ISSN 2676-9042

Vol 6, No 3, 2024.

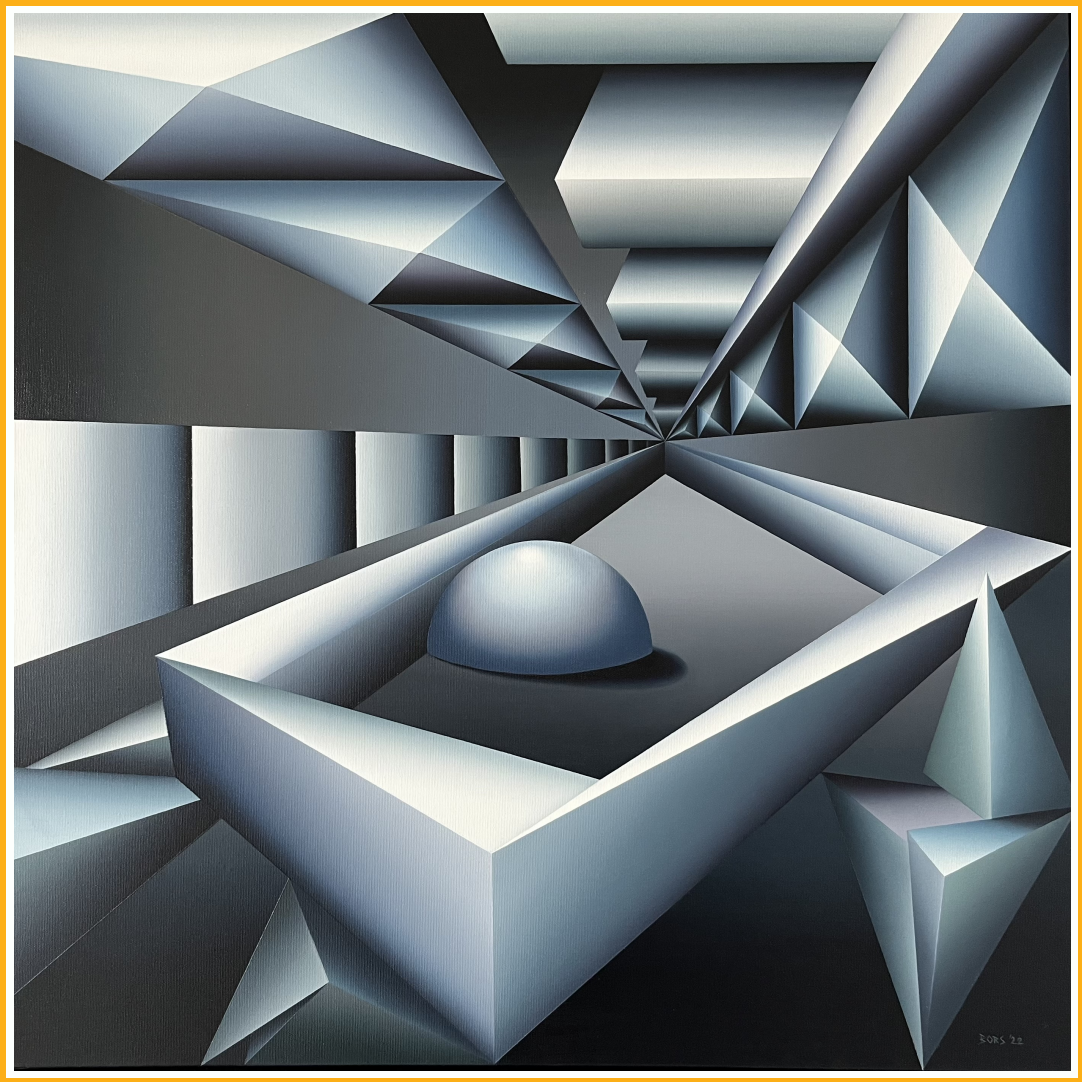
2024, VI. évf. 3. szám

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
Ad infinitum painting | **Ad infinitum** 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

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 6, No 3, 2024. | **2024. VI. évf. 3. szám**

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

BAUMGARTNER Helga

baumgartner.helga@phd.uni-obuda.hu

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

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

BRAUN András

braun.andras92@gmail.com

András BRAUN graduated from the Faculty of Military and Security Engineering of the National University of Public Service in 2016 with a specialization in radar engineering. In 2022, he graduated from Óbuda University with an MSc in Security Engineering. He participated in the operation and operation of military radars in service in Hungary for nearly 7 years. Within the framework of his PhD studies, he plans to research the safety engineering of the application of radars.

BRAUN András 2016-ban a Nemzeti Közszolgálati Egyetem Had- és Biztonságtechnikai mérnöki Karán végzett radar mérnök specializáción. 2022-ben az Óbudai Egyetem Biztonságtechnikai mérnöki MSc szakon szerzett diplomát. Közel 7 éven keresztül vett részt a Magyarországon hadrendben álló katonai radarok üzemeltetésében, működtetésében. PhD tanulmányok keretein belül a radarok alkalmazásának biztonságtechnikai vizsgálatát tervezi kutatni.

CSISZÁRIK-KOCSIR Ágnes

kocsir.agnes@kgk.uni-obuda.hu

Ágnes CSISZÁRIK-KOCSIR Ph.D., Associate Professor at the Keleti Károly Faculty of Economics, Óbuda University. Prior to her university career, she was responsible for the financial management of several EU-funded projects in addition to her general project management tasks. He has been working at the predecessor institution of Óbuda University since 2007, first as a teaching assistant, later as an assistant professor. Since 2013 he has been an associate professor at the Keleti Károly Faculty of Economics at Óbuda University. Hirsh index 23. Member of the editorial board of several professional associations, national and international journals, editor and member of the scientific and organizing committee of several national and international scientific conferences. He is a committed advocate of project thinking and building financial, digital and consumer awareness, as evidenced by his research.

Dr. habil. CSISZÁRIK-KOCSIR Ágnes az Óbudai Egyetem Keleti Károly Gazdasági Karának egyetemi docense. Egyetemi munkássága előtt számos Európai Unió által finanszírozott projekt pénzügyi menedzsmentjét látta el az általános projektvezetői feladatok mellett. Az Óbudai Egyetem jogelőd intézményében 2007 óta dolgozik először tanársegédként, később adjunktusként. 2013-tól az Óbudai Egyetem Keleti Károly Gazdasági Karának egyetemi docense. 2017-ben habilitált, 2018-tól intézetigazgatóként, 2020-tól pedig a Kar kutatási dékánhelyetteseként dolgozik. 2004-től az MTMT-ben a mai napig rögzített publikációinak száma több, mint 600. Hirsh-indexe 23. Több szakmai szervezet, hazai és nemzetközi folyóirat szerkesztőbizottságának tagja, lektora, valamint több hazai és nemzetközi tudományos konferencia tudományos és szervezőbizottságának tagja. Elkötelezett híve a projektszemélet és a pénzügyi, digitális és fogyasztói tudatosság építésének, amit kutatási is igazolnak.

FARKAS Gabriella

farkas.gabriella@bgk.uni-obuda.hu

Gabriella FARKAS PhD, lecturer at Bánki Donát Faculty of Mechanical and Safety Engineering at Óbuda University, senior lecturer. Fields of education: quality assurance, surface roughness measurement, Lean techniques. Teaching activities are in BSc, MSc programs and specialized trainings. She's PhD doctor's degree in Agricultural Technical Sciences in 2010 (Doctoral School of Mechanical Engineering).

Dr. FARKAS Gabriella az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar oktatója, egyetemi adjunktus beosztásban. Oktatási területei: minőségbiztosítás, felületi érdességmérés, Lean technikák. Alapképzésben több szakon, mesterképzésben és a szakmérnöki képzéseken végez oktatási tevékenységet. PhD fokozatot Agrár Műszaki Tudományokban szerzett 2010-ben.

GODA Tibor

goda.tibor@bgk.uni-obuda.hu

Prof. Dr. Tibor GODA DSc, professor, doctor of HAS (Hungarian Academy of Sciences), PhD and Dr. habil. in Mechanical Engineering, MSc in Mechanical Engineering, head of the Doctoral School on Safety and Security Sciences (Bánki Donát Faculty of Mechanical and Safety Engineering, Óbuda University), head of the Institute for Natural Sciences and Basic Subjects (Bánki Donát Faculty of Mechanical and Safety Engineering, Óbuda University), Research areas: numerical modelling, safety and security sciences, tribology, mechanics of polymers, elastomers and composites.

Prof. Dr. habil. GODA Tibor DSc egyetemi tanár, az MTA doktora, PhD, Dr. habil. (gépészeti tudományok), okleveles gépészmérnök, az Óbudai Egyetem (ÓE) Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar (BGK) Biztonságtudományi Doktori Iskolájának vezetője, a Természettudományi és Alapozó Tantárgyi Intézet (ÓE-BGK) vezetője, Kutatási területe: numerikus modellezés, biztonságtechnika, tribológia, polimerek, elasztomerek és kompozitok mechanikája.

KERTÉSZ József

kertesz.jozsef@eng.unideb.hu

József KERTÉSZ is a certified mechanical engineer, a PhD student at the Doctoral School of Safety and Security Sciences at the University of Óbuda and a lecturer assistant at the Department of Vehicle Engineering at the University of Debrecen. His research topic is traffic safety, including the optimization and development of passive safety systems of road vehicles with structural solutions. The aim of the research is to develop bodywork elements that can absorb more energy during a collision, thus reducing the load on passengers. In addition, this must be done taking mass optimization into account, which requires new design ideas and new material applications. Accordingly, part of the research is the load test of aluminum foams. In addition to his doctoral studies, he teaches vehicle and mechatronic engineering students at the University of Debrecen in English and Hungarian laguange.

KERTÉSZ József okleveles gépészmérnök, az Óbudai Egyetem Biztonságtudományi Doktori Iskola PhD. hallgatója és a Debreceni Egyetem Járműmérnöki Tanszék tanársegédje. Kutatási tématerülete a közlekedésbiztonság azon belül is a közúti járművek passzív biztonsági rendszereinek optimalizálása, fejlesztése konstrukciós megoldásokkal. A kutatás célja olyan karosszéria elemek fejlesztése, amelyek az ütközés során nagyobb energiát képesek elnyelni, csökkentve ezzel az utasokat érő terhelést. Ezt ráadásul a tömeg-optimalizáció figyelembevételével kell megtenni, amely új konstrukciós ötleteket, és új anyag alkalmazásokat követel meg. Ennek megfelelően a kutatás részét képezi az alumínium habok terheléses vizsgálata. A doktori tanulmányok mellett a Debreceni Egyetemen jármű- és mechatronikai mérnök hallgatókat oktat angol és magyar nyelven.

KISS Csaba

kiss.csaba@uni-nke.hu

Csaba KISS is a doctoral student at the Military Technical Doctoral School 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 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.

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 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 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 Mil-

KOLLÁR Csaba kommunikációtechnikai mérnök, oklevelés kommunikációs szakember, elektronikus információbiztonsági vezető, a közgazdaságtudományok doktora (PhD), a katonai műszaki tudományok 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

itary Science and the National Association of Human Professionals, and has been a member of the Artificial Intelligence Consortium since Q4 2018.

Hadtudományi Társaság és a Humán Szakem-berek Országos Szövetsége szakértője. 2018. negyedik negyedévétől a Mesterséges Intelligencia Konzorcium tagja.

KOVÁCS Tünde Anna

kovacs.tunde@bgk.uni-obuda.hu

Dr. Anna Tünde KOVÁCS is a university associate professor at the University of Óbuda. She is a member of the editorial board of the journals Acta Meterialia Transylvania, Safety and Security Science Review, and Engineering Safety of Anthropogenic Objects. His research area is special welding processes (ultrasonic and explosive welding) in the field of materials science and technology. As an International Welding Engineer (IWE), welding robots and collaborative robot welding. She works as a subject supervisor at the Doctoral School on Material Sciences and Technologies and Doctoral School on Safety and Security Sciences Doctoral schools. Author and co-author of numerous scientific publications. Member of research projects and supervisor of doctoral topics.

Dr. KOVÁCS Tünde Anna az Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Karának, Anyagtechnológiai Intézeti Tanszékének egyetemi docense. Tagja az Acta Meterialia 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 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.

NAGY Csaba Norbert

nagy.csaba@inf.unideb.hu

Csaba Norbert NAGY, a graduate student of Computer Science Engineering at the Faculty of Informatics of the University of Debrecen. Besides his student research, he hold a technical position at the Department of Data Science and Visualization. His interests include blockchain technology, cryptographic solutions, information and cyber security. He is a member of the Data Security Section of the György Hajós Data Science Colloquium and the Talent Management Program of the University of Debrecen. He participated in the Scientific Student Conference of the Faculty of Informatics of the University of Debrecen with his thesis "Blockchain based security framework for IoT devices", where he won the EPAM special prize and advanced to the National Scientific Student Conference. He submitted his thesis to the "Information Security Thesis of the Year - 2023" announced by the Hétpecsét Information Security Association, where he won the "Other" category and the "Margaret" special prize of Noreg Information Protection Ltd, beyond that New National Excellence Program of the Ministry of Human Capacities scholarship.

NAGY Csaba Norbert a Debreceni Egyetem Informatikai Karának végzős alapszakos mérnökinformatikus hallgatója. Hallgatói pályája mellett technikus pozíciót lát el az Adattudomány és Vizualizációs Tanszéken. Érdeklődési köre a blokklánc-technológia, a kriptográfiai megoldások, az információ és kiberbiztonság. Tagja a Hajós György Adattudományi Szakkollégium Adatbiztonsági tagozatának és a Debreceni Egyetem Tehetséggondozási Programjának. Debreceni Egyetem Informatikai Karának Tudományos Diákköri Konferenciáján a vett részt „Blokklánc alapú biztosági keretrendszer IoT eszközökre" című szakdolgozattal, ahol EPAM különdíjat nyert és továbbjutott Országos Tudományos Diákköri Konferenciára. Szakdolgozatával pályázatot nyújtott be a Hétpecsét Információbiztonsági Egyesülete által meghirdetett „Az év információbiztonsági dolgozata – 2023" címre, ahol az „egyéb" kategória címet nyerte el, valamint a Noreg Információvédelmi Kft. „Margaréta" különdíj, ezentúl az Újnemzeti Kiválóság Program ösztöndíjának elismerésében részesült.

OLÁH Norbert

olah.norbert@inf.unideb.hu

Norbert OLÁH is an Assistant Professor at the Faculty of Informatics, University of Debrecen. He holds a PhD in Theoretical computer science, data security and cryptography in secure authentication scheme design in distributed systems. His interests include security issues in cloud computing and IoT ecosystems, including the implementation of user authentication. The topic is one of the most dynamically developing areas in IT today and raises several problems to be solved. He has been involved in several scientific projects focused on the secure design and study of various communication systems, including TKP 2019: Thematic Program of Excellence 2019, where his tasks included the design and analysis of V2V (Vehicle to Vehicle) and V2I (Vehicle to Infrastructure) secure communication protocols. He also participated in the SETIT - IoT Systems Enhancement Technologies project, where he researched lightweight cryptographic primitives and contributed to the study "Lightweight Cryptographic Algorithms and Security Features". During my PhD studies, he has been awarded the Universitas Foundation PhD Student Scientific Award and the New National Excellence Program of the Ministry of Human Capacities scholarship.

OLÁH Norbert a Debreceni Egyetem Informatikai Karának adjunktusa. Az elméleti számítástudomány, adatvédelem és kriptográfia programban szerzett doktori fokozatot a biztonságos autentikációs sémák tervezése elosztott rendszerekben témakörében. Érdeklődési köre a felhő alapú számítások és az IoT ökoszisztémák biztonsági kérdései, azon belül is a felhasználó hitelesítés megvalósítási lehetőségei. A témakör napjainkban az informatika egyik legdinamikusabban fejlődő területe, számos megoldandó problémát vet fel. Több tudományos projektben is részt vett, amely a különböző kommunikációs rendszerek biztonságos kialakítására és tervezésére fókuszált, többek között a TKP 2019: Thematic Program of Excellence 2019 programban, ahol feladatai közé tartozott a V2V (Vehicle to Vehicle) és V2I (Vehicle to Infrastructure) biztonságos kommunikációs protokoll tervezése és elemzése. Emellett részt vett a SETIT - IoT Systems Enhancement Technologies projektben, ahol könnyűsúlyú kriptográfiai primitíveket tanulmányozott, és részt vett a „Lightweight Cryptographic Algorithms and Security Features" tanulmány kidolgozásában. A PhD tanulmányai során többször elismerésben részesült, melynek során megkapta az Universitas Alapítvány Hallgatói tudományos eredmény elismerését, illetve az Új Nemzeti Kiválósági Program ösztöndíját.

ŐSZI Arnold

oszi.arnold@bgk.uni-obuda.hu

Arnold ŐSZI, Safety Engineer (MSc), PhD in Military Engineering Sciences, Adjunct Professor at the Bánki Donát Faculty of Mechanical and Safety Engineering – Institute of Safety Science and Cybersecurity. His research area: safety, IT, biometrics, drones, crowd motions.

ŐSZI Arnold Okleveles Biztonság- technikai Mérnök (MSc), a Katonai Műszaki Tudományok Doktora, Az Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar – Biztonságtudományi és Kibervédelmi Intézetének Adjunktusa. Kutatási területe: biztonság, IT, biometrikus azonosítás, drónok, embertömegek mozgása.

PÁL Anita

pal.anita@phd.uni-obuda.hu

Over the past 15 years, I have served as an interpreter and IT developer for law firms, economic entities, and commercial organizations, acquiring deep understanding of corporate dynamics within both English and German-speaking environments. For the last four years, I have been serving my country as a soldier at the MoD Defence Economic Bureau's International Directorate. I earned my bachelor's degree in International Relations, then completed a master's degree in

Az elmúlt 15 évben ügyvédi irodák, gazdasági cégek és kereskedelmi vállalatok angol és német nyelvű képviseletében tolmácsként és technikai-informatikai fejlesztőként dolgoztam, mélyreható betekintést nyerve a cégvezetés dinamikájába. A legutóbbi 4 évben katonaként szolgálom hazámat a HM Védelemgazdasági Hivatal Nemzetközi Igazgatóságán. Nemzetközi Kapcsolatokból szereztem alapdiplomámat,

International Security and Defense Policy at the National University of Public Service. During my studies, I deepened my knowledge in optimizing defense organizations and administrative processes. My thesis explored the art of deterrence, examining the role of the defense industry in the arms race. Currently, I am continuing my studies at the Óbuda University Doctoral School of Safety and Security Sciences, where my research focuses on the impact of artificial intelligence on both military and civilian security, emphasizing the importance of AI development and the reduction of associated security risks.

majd a Nemzeti Közszolgálati Egyetem Hadtudományi Karán végeztem el mesterképzést Nemzetközi Biztonság- és Védelempolitikai szakon. Itt tudásomat a védelmi szervezetek és a védelmi közigazgatás optimalizálására mélyítettem el. Diplomamunkámat az elrettentés művészetéről írtam, vizsgálva a hadiipar szerepét. Jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában folytatom tanulmányaimat, ahol kutatásom középpontjában a mesterséges intelligencia katonai és polgári biztonságra gyakorolt hatása áll, kiemelve az MI fejlesztésének és a biztonsági kockázatok csökkentésének fontosságát.

REVÁK Bernadett

revak.bernadett@phd.uni-obuda.hu

Bernadett REVÁK is currently a second-year PhD student at the Doctoral School on Safety and Security Sciences. Since 2009, she has been a lecturer of English language and literature at the Érdi SzC Kossuth Zsuzsanna Technical and Vocational School and Youth Hostel. As the head of the foreign language department of the institution, she manages the teaching of the foreign language. Since 2009, she has also been responsible for writing, coordinating and implementing international Erasmus+ projects. She has gained international work experience in several countries over the years. Of particular importance are collaborations within the framework of strategic partnerships, which provide scope for her own research. As a PhD student, her research focuses on digital education in the national and international area. She is committed to making the work of educators and teachers more effective.

REVÁK Bernadett jelenleg a Biztonságtudományi Doktori Iskola másodéves doktorandusz hallgatója. 2009 óta a jelenleg Érdi SZC Kossuth Zsuzsanna Szakképző Iskola és Kollégium angol nyelv és irodalom szakos oktatója. Az intézmény nyelvi munkaközösségének vezetőjeként irányítja az idegen nyelv oktatását. Mindemellett munkájában 2009 óta kiemelt szereppel bír az Erasmus+ keretein belül szervezett nemzetközi pályázatok megírása, koordinálása és megvalósítása. Több országban szerzett nemzetközi gyakorlati tapasztalatot az elmúlt évek során. Ezek közül különösen fontosak a stratégiai partnerségek keretein belüli együttműködések, melyek teret adnak saját kutatásának. Doktorandusz hallgatóként kutatása fókuszában a digitalizált oktatás áll hazai és nemzetközi színtéren. Hivatásában elkötelezett a nevelői -oktatói munka hatékonyabbá tétele iránt.

SZABÓ Lajos

szabo.lajos@uni-obuda.hu

Dr. Lajos SZABÓ PhD. of security and safety sciences, certified security engineer, security management engineer, retired police Lieutenant Colonel, Chairman of the Board of Trustees of the Law Enforcement and Private Security Education and Research Foundation (REMOK), lecturer at the Faculty of Law Enforcement of the National University of Public Service and the Bánki Donát Faculty of Mechanical and Security Engineering of Óbuda University. During the first half of his three decades in the police service he was a senior investigator and during the second half he was the chief police and team services officer. During this time, I planned and implemented the securing of routes and destinations for various sporting, cultural and religious events, transport and delegations. I was

Dr. SZABÓ Lajos PhD., a biztonságtudományok doktora, okleveles biztonságtechnikai mérnök, biztonságszervező mérnök, nyugállományú rendőr alezredes, kuratóriumi elnöke a Rendészeti és Magánbiztonsági Oktatási és Kutatási Alapítványnak (REMOK), a Nemzeti Közszolgálati Egyetem Rendészeti Karán és az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Karán óraadó tanár. A rendőri szolgálatban töltött három évtized első felében kiemelt főnyomozó, a második felében kiemelt főelőadó közrendvédelmi és csapatszolgálati területen. Ez idő alatt terveztem és végrehajtottam különféle sport, kulturális és egyházi rendezvények helyszínének biztosítását, szállítmányok és delegációk útvonalainak és célállomásainak biztosítását.

responsible for planning the secure guarding of various facilities.I was one of the first to obtain the Diploma in Security Engineering, I was an expert in the accreditation of the MSC Chartered Security Engineers course and subsequently graduated from the MSC. Since retirement I have been teaching, researching and publishing.

Felelős voltam különféle létesítmények biztonságos őrzésének megtervezéséért. Az elsők között szereztem meg a biztonságszervező szakmérnöki diplomát, bolognai szakértőként vettem részt az okleveles biztonságtechnikai mérnök MSC képzés akkreditálásában, majd ott is diplomát szereztem. Tanítok, kutatok és publikálok nyugdíjba vonulásom óta.

SZÁVAY István

szavay.istvan@phd.uni-obuda.hu

István SZÁVAY, Safety Engineer (MSc), PhD Student at the Doctoral School on Safety and Security Sciences Bánki Donát Faculty of Mechanical and Safety Engineering, Óbuda University. His research interests include the integration of drones in asset protection.

SZÁVAY István Okleveles Biztonságtechnikai Mérnök (MSc), az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar Biztonságtudományi Doktori Iskolájának hallgatója. Kutatási területe a drónok vagyonvédelmi integrációja.

SZŰCS Endre

szendre63@gmail.com

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.

TÓTH Georgina Nóra

toth.georgina@bgk.uni-obuda.hu

Nóra Georgina TÓTH: Lecturer at Bánki Donát Faculty of Mechanical and Safety Engineering at Óbuda University, master lecturer. Fields of education: quality assurance, process development, quality techniques and methods. Teaching activities are in BSc, MSc programs and specialized trainings.

TÓTH Georgina Nóra az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar oktatója, mestertanár beosztásban. Oktatási területei: minőségbiztosítás, folyamatjavítás, minőségtechnikák. Alapképzésben több szakon, mesterképzésben és a szakmérnöki képzéseken végez oktatási tevékenységet.

TURÓS Tímea

turos.timea@uni-obuda.hu

With my bachelor's degree in electrical engineering, I applied to the Bánki Donát Faculty of Mechanical and Safety Engineering at Óbuda University in 2020. I successfully passed the final exams in two specialisations, designer and organizer of engineering of safety and security. During my training, my documents submitted to Scientific Student Conference events and the

Villamosmérnöki alapdiplomámmal 2020-ban jelentkeztem az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai mérnöki kar mesterképzésére. Két specializáción, biztonságtechnikai mérnök tervező és szervező szakirányon, sikeres záróvizsgát tettem. A képzés ideje alatt Tudományos Diákköri Konferencia rendezvényekre nevezett munkáim és

maximum support of my thesis supervisor were the basis for my application for doctoral studies. I am currently a PhD student at the Doctoral School of Safety and Security Science. My research area is the security aspects of sports policing.

Témavezetőm maximális támogatása megalapozták a doktori képzésre történő jelentkezésemet. Jelenleg a Biztonságtudományi Doktori Iskola doktorandusz hallgatója vagyok. Kutatási területem a sportrendészet biztonságtechnikai aspektusait taglalja.

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 6, No 3, 2024. | **2024. VI. évf. 3. szám**

CONTENT | TARTALOM

APPEARANCE OF SAFETY AND SECURITY IN THE HUMANITIES (PART 2)

A BIZTONSÁG MEGJELENÉSE A HUMÁN TUDOMÁNYOKBAN (2. RÉSZ)

KOLLÁR Csaba[1]

Abstract

This paper, the second part of a three-part study, examines the intersection of social psychology, anthropology, and communication science, analyzing different perspectives on security. Social psychology examines interpersonal and group interactions and the impact of social environments on individuals, exploring how cultural, social, and environmental factors influence people's sense of security. It addresses concepts such as well-being, peace, happiness, and threats like instability and environmental dangers. Key areas include social representation, societal norms, norm violations, illusions, and errors, and their effects on decisions, obedience to authority, and role-following. Anthropology extends its study to modern urban and workplace environments, examining myths, legends, traditions, and social norms influencing collective security. Communication science integrates insights from various disciplines to explore effective communication models, emphasizing the importance of trust and information sharing in enhancing security awareness and resilience against social engineering attacks. The study underscores the need for a dynamic understanding of norms to maintain social balance and individual security.

Keywords

safety and security, humanities, social psychology, anthropology, communication science

Absztrakt

Ez az írás, egy háromrészes tanulmány második része, a szociálpszichológia, az antropológia és a kommunikációtudomány metszéspontját vizsgálja, a biztonság különböző nézőpontjait elemezve. A szociálpszichológia az emberek közötti és a csoporton belüli interakciókra, valamint a társadalmi környezet egyénre gyakorolt hatásaira összpontosít, vizsgálva, hogy a kulturális, társadalmi és környezeti tényezők hogyan befolyásolják az emberek biztonságérzetét. Főbb területei közé tartozik a szociális reprezentáció, a társadalmi normák, a normaszegés, az illúziók és tévedések, valamint ezek hatása a döntésekre, a hatalomnak való engedelmeskedés és a szerepkövetés. Az antropológia kiterjeszti vizsgálódását a modern nagyvárosi és munkahelyi környezetekre, megvizsgálva, hogyan befolyásolják a mítoszok, legendák, hagyományok és társadalmi normák a kollektív biztonságot. A kommunikációtudomány hatékony kommunikációs modelleket tár fel, kiemelve a kölcsönös bizalom és információmegosztás fontosságát a biztonságtudatosság növelésében és a social engineering támadásokkal szembeni ellenálló képesség erősítésében. A tanulmány hangsúlyozza a normák dinamikus megértésének szükségességét a társadalmi egyensúly és az egyéni biztonság fenntartásában.

Kulcsszavak

biztonság, humán tudományok, szociálpszichológia, antropológia, kommunikációtudomány

[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

SZOCIÁLPSZICHOLÓGIA

A szociálpszichológia – mely a szociológia, a pszichológia és az antropológia diszciplináris metszéspontjában helyezhető el – a szociológiához hasonlóan többféle megközelítésből számos teóriát és kutatási eredményt ismertet a biztonsággal kapcsolatban. Fókuszába rendszerint az emberek közötti, a csoporton belüli, az ember és csoport közötti interakciókat helyezi, valamint a társadalmi környezet egyénre gyakorolt hatását vizsgálja, elsősorban az egyén érzelmi, viselkedése és egyéb jellemzői alapján. Ugyancsak fontos vizsgálati területei, hogy az emberi interakciók (döntően a közöttük levő kommunikáció) révén hogyan alakulnak a társadalmi szerepek, attitűdök és normák. A biztonság vonatkozásában a szociálpszichológia arra kíváncsi, hogy mi befolyásolja az emberek biztonságérzetét, mik azok a kulturális, társadalmi és környezeti tényezők, melyek növelik az egyén biztonságérzetét, s melyek azok, amelyek csökkentik azt, illetve veszélyként, veszélyforrásként, fenyegetésként jelennek meg az életében, vagy melyek azok, amelyekre így tekint (hamis és túlzott félelemérzet, fóbiák – ezekről a pszichológiai résznél írok bővebben). A szociálpszichológusi terminológia szerint a biztonság fogalma köré rendezhetjük a jólétet, a békét, a boldogulást, a boldogságot, míg a veszélyek közé az instabilitást (társadalmi, gazdasági, politikai), a környezeti veszélyeket, az egyének közötti diszharmonikus kapcsolatot (amivel egyébként a pszichológia is foglalkozik), illetve az egyén és a csoport közötti (vagy a csoporton belüli) kisebb-nagyobb súrlódásokat.

A szociálpszichológia biztonsággal kapcsolatos fontosabb vizsgált területei – melyekről írásművemben részletesebben írok – a szociális reprezentáció, a társadalmi normák, a normaszegés és annak következményei, az illúziók és tévedések, valamint ezek hatása az emberi döntésekre, a hatalomnak való engedelmeskedés, a szerepkövetés. A szociális reprezentáció „közös társas elgondolások közhelyszerű 'elméletek' formájában, melyeknek az a fő funkciójuk, hogy értelmet adjanak a világnak és elősegítsék a kommunikációt". [7 p. 490] Az „értelmet adás" elvezet a megértéshez, s azon keresztül az információ feldolgozásához is. A biztonság, illetve a veszély szubjektív és percepciója egyénfüggő, vagyis a kollektív biztonságkép helyett sokkal inkább az egyén saját biztonságképéről beszélhetünk. Moscovici [37] meglátása szerint ugyanakkor létezik egy társadalmi norma, mint modell, illetve szabályok összessége, s amikor az egyén biztonságérzetét (vagy biztonságtudatosságát) vizsgáljuk, akkor kognitív ferdítései, szubjektív torzításai, affektív hajlama e társadalmi normák viszonyában nyer igazi értelmezést. Sherif [1] értelmezésében a társadalmi normák a társadalmi környezet változásának hatására maguk is változnak, vagyis a helyes és helytelen viselkedés, vagy a biztonság/veszély megítélése és e fogalmak tartalma is változik. A megfelelően kialakított normarendszer megléte és változása – ha ennek a változásnak a dinamikája „emberi léptékkel követhető" [2], akkor – hozzájárulnak a társadalmi egyensúly fenntartásához, a társadalmi rendszerek megerősítéséhez, többek között az emberek közötti együttműködéshez és kölcsönös tisztelethez, ami összességében kedvezően hat az egyén és a társadalom biztonságára is. Egy csoport (ami lehet akár egy munkaszervezet/munkacsoport) tagjai kölcsönösen alakítják ki a csoport normarendszerét, melyben az egyéni elképzelések javarészt feloldódnak a csoport normarendszerében, így alakítva ki a társas interakciók során az egyének saját értékrendjeikből a heterogén, jobb esetben konszenzuson alapuló csoportékrendet, illetve -normát. Smith és Mackie [3 p. 483] így ír erről: „Mivel az embereket erősen befolyásolják mások gondolatai és tettei, az interakció során a különböző csoporttagok vélekedései, érzései és viselkedése egyre hasonlóbbá válik. Akár egyértelmű,

akár homályosabb a döntési feladat, az egyének vélekedései egy társas norma kialakítása felé konvergálnak. A norma a csoport által általánosan elfogadott gondolat-, érzés-, illetve cselekvésmódot tükrözi". Festinger [4] kognitív disszonanciáról szóló könyvében arról értekezik, hogy az emberben feszültség keletkezik akkor, amikor személyes cselekedete, vagy véleménye nem kongruál a személyes értékeivel, vagy a társadalmi normákkal. Ez normaszegéshez vezet. Egy biztonságtudatossággal kapcsolatos példa: az egyén a kényelmét a biztonság elé helyezi, amikor az asztalán levő cetlikre írja fel a jelszavakat, mert számára így kényelmes. Tudja, hogy ez nem helyes, hiszen ezt hallotta a vállalati információbiztonság-tudatossági tréningen, s emiatt feszültséget érez, de megmagyarázza azzal, hogy senki sem kíváncsi a kollégák közül arra, hogy mi van a vállalati számítógépén. Így ugyan a feszültséget feloldja magában, de fenntartja eszközei sebezhetőségét. Gilovich [5] a humán okoskodás, a tévedések és az illúziók hibáinak hatását vizsgálja hétköznapi döntéseinkre. A tévedések leggyakoribb okai között az emlékek torzulását [6], a túlzott önbizalmat, a felszínességet, a történések nem reális értékelését, a vélekedések befolyásolhatóságát nevezhetjük meg. A tévedés megában hordozza a személyes és társadalmi biztonság kockázatát is, hiszen a nem, vagy rosszul felmért veszélyforrás, s az annak elhárítására, mérséklésére hozott döntések a hamis biztonság illúziójával kecsegtethetnek. A szociálpszichológia vizsgálódási területein Milgram [8] a hatalomnak való engedelmeséggel foglalkozott. Megállapította, hogy az emberek sokkal nagyobb arányban engedelmeskednek a hatalomnak, mint ami egyébként megjósolható lett volna. Teszik ezt akkor is, ha az engedelmeskedésükkel másik embertársuknak kárt, sérülést okoznak. A megkonstruált hatalomhoz való idomulás és lojalitás az egyén számára ugyan a biztonság látszatát keltheti, de növelheti kételyeit is: mi van, ha egy nálánál még lojálisabb embertársa ellene fordul, s a „küzdelemben" alul marad. Katonai, félkatonai, magánbiztonsági szervetekben a „tekintéllyel felruházott ember parancsainak végrehajtása" [7 p. 482] a szolgálati rend és fegyelem témakörébe tartozik, annak megszegésének következményei vannak. Goffman [9] rámutat arra, hogy a szerepjátszás életünk velejárója, s a különböző társas interakciók során a különböző platformokon szerepeket játszunk. A szerepjáték során a környezetünkkel folytatott kommunikáció révén értékeljük viszonyunkat környezetünkhöz és az ott levő emberekhez, ahogy ők is beazonosítanak minket viselkedésünk, verbális és nonverbális jelzéseink alapján. A szerepjáték során is megjelenhet a kognitív disszonancia, amikor az egyén szerepkonfliktusba kerül, mert olyan módon kellene viselkednie, cselekednie a megadott normák szerint, amely nem egyeztethető össze saját értékrendjével. A social engineering típusú támadások során [10] [11] a támadó egy tudatosan elképzelt szerepet játszik el, hogy elfedje valódi kilétét, érzéseit, gondolatait, vágyait, hogy így tudja átverni a gyanútlan áldozatát.

ANTROPOLÓGIA

Az antropológia az emberrel foglalkozó természet- és társadalomtudományok összefoglaló elnevezése. Részei – többek között – az etnográfia, amelyik szűkebb értelmezésben az anyagi javak termelésével és felosztásával foglalkozik, a folklór, amelyik a népi/társadalmi köztudat egészét (vallás, hiedelem, költészet, szokások, legendák, stb...) foglalja magában, ágazati osztásban pedig a fizikai, a kulturális és a szociális antropológia. A modern antropológia vizsgálódási terepe már nem csak a távoli kontinensekre, eldugott népcsoportokra, vagy a falusi/tanyasi lakosságra korlátozódik, hanem ezeken túllépve a modern

nagyvárosi és munkahelyi környezetre az ezekben élő, tevékenykedő emberekre is. A vizsgálódás tárgyai lehetnek a gyermekek fejlődésében szerepet játszó (nép)mesék, a játékok (a mondókás-cselekményes-eszközös, valamint a tárgykészítő játékok segítik a gyermekek életre való felkészítését), vagy a szülők által az ősökről szóló történetek. A mesékben és a történetekben gyakran megjelenik a hős archetípusa [12], aki rendszerint a közösség védelmében, vagy egy személy kegyeiért vállalva a kockázatot, kilépve biztonságos komfortzónájából, megküzd az ellenséggel és (ha nehezen is, de) legyőzi azt. A közösség biztonságáért a saját biztonságát (időlegesen) kockára tevő harcos eszményképe követendő példaként szolgálhat a felnövekvő gyerekek számára, egyben a kollektív biztonságot előtérbe helyezi az egyéni biztonság kárára.

Az antropológia továbbá vizsgálódási területei a lakó- és munkakörnyezet (különösen, hogy milyen személyes tárgyak, kialakított terek szolgálják az egyén védelmét és kényelmét), a városi mítoszok és legendák, a hagyományok tisztelete, a sport, az egyes társadalmi csoportok közötti munkamegosztás, a család, a rokonság, a leszármazás, a nemek és korcsoportok közötti munkamegosztás, illetve a hírközlés (az adott médiumon keresztül milyen tartalmakat lát/hall/olvas a társadalom tagja) is. E vizsgálatok rámutatnak arra, hogy mik azok a platformok és folyamatok, amelyek közösségi/társadalmi szinten képesek lehetnek a kollektív biztonságot fenntartani, vagy legalábbis a veszélyeket csökkenteni. Az ember kulturális hozadéka, mely generációról generációra – igaz nem teljes mértékben, de – átadódik és bővül, számos olyan történetet és emlékképet tartalmaz (nép)mesék, családi legendák, visszaemlékezések formájában, amelyek arról szólnak, hogy a főszereplők a különböző élethelyzetekkel (munkahely megszűnése, súlyos betegség, háború, elköltözés, szerencsét próbálás, megmérettetés, stb.), mint lehetséges stresszorokkal hogyan tudtak megbirkózni. Ezek a történetek, ha sikeres befejezéssel zárultak, akkor követendő mintaként szolgálhattak, ha pedig a főhős bukásáról szóltak, akkor segítségére lehettek az egyénnek abban, hogy saját életében a bukást felismerje és elkerülje.

A vallásukat rendszeresen gyakorló és/vagy a vallásos műveket (pl.: Biblia, Korán) olvasó egyén számára is megfelelő mintákkal szolgálnak a vallásos történeteket, példabeszédek, különösen akkor, ha az egyén egyfelől azonosulni tud az adott szereplővel (pl.: keresztneve védőszentjével), másfelől az archaikus történetet adaptálni tudja jelen életére is. A történetek, mesék, példabeszédek tehát összességében sikeres életstratégiánk és biztonsági attitűdünk elengedhetetlen kellékei, segítségükkel eredményesebben tudunk helytállni az élet megterheléseivel szemben, illetve problémamegoldó képességünk/készségünk is fejlődik (coping). Megtanulhatjuk át- illetve újraértelmezni, esetleg újrakeretezni az eseményeket, így a kiégéshez vezető nem műszaki környezeti tényezők hatását mérsékelni tudjuk.

Az antropológia fontosabb biztonság-interpretációi közül elsőként Douglas [13] kulturális antropológiai fókuszú megközelítését ismertetem. Elképzelése a tisztaság-veszély fogalma köré épül, az előbbit a sérthetetlenség és a védettség, míg az utóbbit a káros, veszélyes, kóros jelzőkkel lehet leírni. Az ellentétpár révén az emberi test, a táplálék, a környezet, stb. értékelhető. A társadalom feladata az, hogy olyan eszközöket, mechanizmusokat, szabályozókat, módszereket használjon, mely révén a tisztaság ideális állapotához minél közelebb kerül. Ebben az elképzelésben a biztonság a tisztaság egyik társfogalmaként értelmezhető. Hobsbawm és Ranger [14] szerint a társadalom biztonságát és stabilitását a (kollektív) társadalmi emlékezet és a hagyományok alakítják. A tradíciók nem feltétlenül

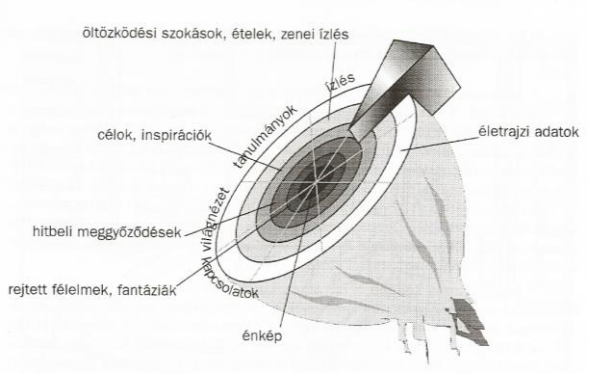
ősi rítusok, gyakran a jelenkor szülöttei. Jelenkori használatuk, illetve a használathoz fűződő modern narratívák célja a jelenkori biztonság és stabilitás alakítása azzal, hogy az adott kultúrkörhöz tartozó valamennyi egyén számára követendő mintaként szolgáljanak. Appadurai [15] a biztonság és a globalizáció közötti kapcsolatot vizsgálja. Rámutat arra, hogy a globalizáció negatívan hat az egyén identitására és érzelmi biztonságára, mert félelmet és feszültséget kelt a társadalmakban, előmozdíthatja a társadalmon belüli, vagy egyes társadalmak közötti konfliktusok kialakulását. A félelem pedig kihat az egyén és a társadalom biztonságérzetére is. Mauss [16] az ajándékozás formáit és rítusait vizsgálva arra a következtetésre jut, hogy az ajándékozás nem csak javak/termékek cseréjét jelenti, de képes fenntartani, ápolni és fejleszteni az egyének, esetleg csoport közötti kapcsolatokat, ezzel formálva a társadalmi normákat. Az ajándékozás és viszont-ajándékozás hozzá továbbá tud járulni az egyének és csoportok közötti béke és az arra épülő biztonság fenntartásához, hiszen olyan pozitív érzéseket kommunikál a másik felé, mint a szívesség, a barátság, az egymás iránt érzett megbecsülés és tisztelet. Fassin [17] a rendfenntartás működését vizsgálja városi környezetben. Bemutatja, hogy a városi lakosságban hogyan alakul ki, illetve át a biztonságérzete a rendfenntartó erők jelenlétének következtében. A konzervatív, rendszerint felnőtt (ős)lakosság számára a rendfenntartó erők megjelenése inkább növeli a biztonságérzetüket, mivel személyes biztonságukat nagymértékben attól teszik függővé, hogy látják-e annak fenntartásának tárgyiasult attribútumait. A fiatalok egy részének, a bevándorlóknak, illetve a kisebbséghez tartozó családok tagjainak azonban a rendfenntartó erők megjelenése inkább erődemonstrációnak tűnik, illetve félelmet kelt bennünk. A szerző művének fókuszába egy rendőrörs élete kerül, melynek állományát nyomon kísérte a párizsi régió egyik legnagyobb körzetében, s feltárta a rendfenntartás hétköznapi aspektusait, amelyeket inaktivitás és unalom, eseménytelen nappalok és éjszakák jellemeznek. Az unalmas hétköznapok legkisebb eseményeire (pl.: kisebb szabálysértés) a hivatásos állomány túlzott erődemonstrációval válaszolt. A tiszteknek pedig kétségeik vannak saját munkájuk értékével, fontosságával és jelentőségével kapcsolatban. Ez a magatartás sajnos a magánbiztonsági szektor munkavállalóinál, illetve vezetőinél is tetten érhető.

KOMMUNIKÁCIÓTUDOMÁNY

Az ember társas lény [18], aki társas kapcsolatokat épít ki, tart fenn, a többi emberrel kommunikál (interakcionál), s megannyi társas csoport/közösség tagja. A kommunikációtudományt számos, az e fejezetben korábban ismertetett etológiai, szociológiai, szociálpszichológiai, pszichológiai és antropológiai tudományterület ismeretanyaga gazdagítja, ugyanakkor megannyi olyan modell van, mely alapvetően a kommunikációtudomány diszciplináris keretén belül nyert igazi értelmezést és gyakorlati hasznosulást. Ezért itt kívánok írni öt fontos kommunikációs modellről és az egyik gyakorlati vizsgálatáról.

Griffin [19] Taylor és Altman 1987-es kapcsolatelmélyülés elméletét egy – a 3. ábrán látható – példán keresztül szemlélteti, melyben Pete a Jon-nal való kapcsolatának elmélyülését mutatja be. A kapcsolatelmélyülés hagymamodelljénél ahogy a kapcsolat elmélyül, az ember úgy tárulkozik fel a másik embernek [20]. Ez a feltárulkozás ugyan felvethet az egyénben bizonyos aggályokat – ha egyáltalán ismeri és foglalkozik a kapcsolatelmélyülés modell gyakorlati alkalmazhatóságával – de a végkövetkeztetés valahogy az lesz, hogy a társas interakciók során a másik fél is feltárt életéből egy csomó bizalmas, intim részletet, vagyis az egymással történő titkok megosztása révén nőtt a bizalom a másik fél irányába.

A feltárulkozó egyén rendszerint nem mérlegeli, hogy a másik fél is hasonlóan komoly, vagy épp ellenkezőleg, csak annak látszó, vagy hamis információkat oszt meg a magáról. A feltárulkozás pedig magával hozza az egyén sebezhetőségét, (bizalmas) adatainak kiszolgáltatását arra nem méltó kommunikációs partnerének.



1. ábra: A kapcsolatelmélyülés elmélete [19]

A legkülső hagymarétegen az életrajzi adatok szerepelnek. Bár ezek is személyes adatok, rendszerint már egy könnyed beszélgetés során is kiderül, hogy ki, mikor, hol született, hova jár(t) iskolákba, hol lakott/lakik, esetleg hol dolgozott/dolgozik. Az öltözködési szokásokat, az ételpreferenciákat és a zenei ízlést néhány beszélgetés során meg lehet ismerni, hiszen az emberek jelentős része ezekről könnyen tud beszélni mások előtt akkor is, ha kapcsolatuk még felszínes. Míg az extrovertált emberek szívesen beszélnek céljaikról és inspirációikról, addig az introvertált emberek rendszerint itt húzzák meg a határt, melyen belülre már azokat engedik, akikben megbíznak. A kapcsolat elmélyülésének további rétegeiben az egyén már beszél hitbéli meggyőződéseiről, de ez már az extrovertált emberek többségénél is bizalmi kérdéssé válik (vagy tudatosan választja a prédikátor, hittérítő szerepet, s akkor kéretlenül is ezek a fontosabb beszédtémái). Mindenkinek vannak olyan félelmei és elképzelései, melyeket vagy senkivel sem, vagy csak egy szűk réteggel oszt meg. S végül, elérkezünk a legbelső rétegig, mellyel kapcsolatban Griffin azt írja, hogy „Pete személyiségének magját belső értékei, énképe, a benne rejlő megoldatlan ellentétek és mély érzelmek alkotják. Ez az ő egyedi birodalma, amely a világ előtt láthatatlan, ám jelentős hatással van életének a felszínhez közelebb eső részeire”. [19 p. 128] Az egymás előtti kölcsönös feltárulkozás az intimitás felé vezet, de ez csak addig a rétegig mélyül el, amíg a feltárulkozás több nyereséggel, mint veszteséggel jár, vagyis inkább okoz örömet, mint fájdalmat. Profi szélhámosok, manipulátorok, humán social engineeringgel foglalkozó szakemberek képesek arra, hogy – ahogy az ábra is mutatja (ék) – rövid időn belül a hagyma több rétegét is átvágják, s a másik személy bizalmába férkőzzenek.

Berger [21] a bizonytalanságcsökkentés elméletében nyolc axiómát fogalmaz meg, melyek Griffin [19] közlése alapján a következők:

1. Ahogy az ember elkezd kommunikálni embertársával, csökken a bizonytalansága. A verbális kommunikáció gyakorisága növekszik.
2. Ahogy az ember elkezd nonverbálisan kommunikálni embertársával, csökken a bizonytalansága. A nonverbális kommunikáció gyakorisága növekszik.

3. A fokozott bizonytalanság arra ösztönöz, hogy minél több információt tudjunk meg a másikról. Ahogy csökken a bizonytalanság mértéke, az információgyűjtés alábbhagy.
4. A bizonytalanság csökkenésével arányosan növekszik a bizalmunk, bizalmasságunk a másik iránt.
5. A bizonytalanság csökkenésével növekszik a kölcsönösség.
6. Az emberek közötti hasonlóság csökkenti, a különbözőségek pedig növelik a bizonytalanságot.
7. Ahogy csökken a bizonytalanságérzet, úgy nő a szimpátia.
8. A közös ismeretségi kör csökkenti, míg annak hiánya növeli a bizonytalanságot.

Az ember tehát szeretné csökkenti a másik féllel szemben fennálló bizonytalanságát, s ezt oly módon teszi, hogy kommunikál vele. A kommunikáció gyakoriságával csökken a bizonytalanság, a kapcsolat elmélyül, de ezek a folyamatok rosszabb esetben az egyént kiszolgáltatottá tehetik, vagyis, ha meggondolatlanul szeretné csökkenteni a partnerével szembeni bizonytalanságot, veszélyeztetheti biztonságát, vagy akár (szervezeti) bizalmas és titkos információkat is megoszthat számára észrevétlenül, kvázi ösztönszerűen a partnerével.

Írásművemben többször utaltam arra, hogy milyen fontos az egyén biztonsága szempontjából az a társas közösség (és annak biztonsága), aminek a tagja. A csoport együttesen tudja alakítani a csoportnormákat, melyek jobb esetben a csoport és a benne levő egyén biztonságára pozitívan, míg az őket veszélyeztető forrásokra negatívan hatnak. A csoportos döntéshozatal univerzális(nak mondható) modelljét Poole [22] alapján Griffin [19 p. 228] a következő öt lépésben írja le:

1. „Tájékozódás: a csoportcélok nem világosak, ezért az erőfeszítések iránya nem azonos, a kapcsolatok bizonytalanok, a tagoknak több információra van szükségük.
2. Konfliktus: a csoporton belüli frakciók eltérő véleményen vannak a probléma megközelítését illetően, és vitába bonyolódnak egymással, a tagok saját álláspontjaik mellett érvelnek.
3. Közeledés: a békés megbeszélések során lecsillapodnak a kedélyek, a mindenki számára elfogadható megoldások megszavazásával a tagok megóvják egymás és önmaguk presztízsét.
4. Fejlődés: a csoport a végleges megoldás megtalálására törekszik, a tagok aktívak és izgatottak.
5. Integráció: a csoport a feladat helyett immár a békés együttlétre összpontosít, a tagok megjutalmazzák egymást a közös munkáért.”

Az idézett folyamat sikere több dologtól is függ: (1) a rendelkezésre álló információk mennyisége és minősége megfelelő-e, (2) a döntéshozatalhoz irreleváns információk nem, vagy csak marginális számban/arányban vannak jelen, (3) adottak-e a körülmények ahhoz, hogy mindenkinek legyen ideje és lehetősége kifejteni a saját álláspontját, (4) adottak-e a körülmények ahhoz, hogy a saját álláspont kulturált módon megvitatásra kerüljön más álláspontokkal szemben, (5) a csoport kellően érett-e ahhoz, hogy az eltérő álláspontok ütközése ne forduljon személyeskedésbe, (6) a csoporttag kellően érett-e ahhoz, hogy saját attitűdjét őszintén megváltoztassa, ha meggyőződése szerint az a csoport érdekeit szolgálja, vagyis nincs benne sértődés akkor, ha nem az ő javaslatát fogadja el a többség, (7) akinek a

javaslatát a megvitatás után elfogadják, az a döntési eredményt elsősorban nem a saját, hanem a közösség sikereként látja. Több kreatív technika létezik, amelyik a csoportos döntéseket támogatja, ezek közül az egyik legismertebb a Bono [23] féle hat gondolkodó kalap módszere, mely lehetővé teszi, hogy egy problémát és annak lehetséges megoldási alternatíváit a csoporttagok a színes kalapok cserélgetésével más-más aspektusból vizsgálhassák meg.

A személyközi, illetve csoporton belüli, vagy csoport felé irányuló kommunikáció elemzésére számos olyan elmélet és modell született, amelyik a hatékony meggyőzéssel, vagy manipulációval foglalkozik. Cialdini [24] a meggyőzés alapelvei modellje alapján lehet felépíteni és gyakorolni a hatékony befolyásolás-gyakorlást, a meggyőzést, illetve akár ártó szándékkal a manipulációt is. Az alapelvek a következők:

1. Viszonzás: az egyén rendszerint szeretné visszaadni/visszafizetni azt az embertársának azt, amit tőle kapott. Nem szeretnénk adósak maradni, mert az az emberek többségénél belső feszültséget, diszharmóniát idézhet elő.
2. Elkötelezettség és következetesség: ha egyszer választunk vagy állást foglalunk, azon dolgozunk, hogy az elkötelezettségünknek megfelelően következetesen viselkedjünk, hogy igazoljuk döntéseinket.
3. Társadalmi bizonyíték: ha bizonytalanok vagyunk, akkor bizonytalanságunkat úgy akarjuk csökkenteni, hogy olyan embereket keresünk, akik hozzánk hasonlóan vélekednek. Minél több ilyen ember találunk, annál inkább gondoljuk úgy, hogy helyes az álláspontunk.
4. Kedvelés: az a hajlam, hogy egyetértsünk azokkal, akik szimpatikusak nekünk, s fordítva: jó, ha akit szimpatikusnak tartunk, az egyetért velünk.
5. Tekintély: nagyobb valószínűséggel mondunk „igent" másoknak, akik tekintélyesek, nagyobb tudással, tapasztalattal vagy szakértelemmel rendelkeznek.
6. Szűkösség: ha egy számunkra fontos erőforrás csak korlátozottan áll rendelkezésre, akkor még inkább fontossá válik annak megszerzése, s még többet akarunk belőle.

Hogan [25] hangsúlyozza, hogy azok, akik másokat szeretnének meggyőzni, fontos, hogy minden megnyilvánulási formájukban megnyerők legyenek, így válva szavahihetővé és bizalomgerjesztővé. Az első négy másodperc különös jelentőséggel bír, amikor a manipulátor nonverbális jelzései (például testalkat, öltözet, ékszerek, kiegészítők, cipő stb.) már a megszólalás előtt megalapozhatják a social engineer sikerét.

A megjelenés és a verbális üzenet együttes hatása olyan tényezőket befolyásol, amelyek a hitelességet meghatározzák (lásd [24]). Ezek közé tartozik: (1) Hozzáértés. A szakértelem általában a tapasztalatban és a képzettségben nyilvánul meg, így a social engineer támadása előtt alaposan felkészül az adott szakma ismereteiből. Mivel a social engineerek többsége átlagon felüli műveltséggel rendelkezik, sokszor képes hitelesen eljátszani olyan szerepeket, amelyek diplomát igényelnek, vagy „visszalépni" egy alacsonyabb szintű szerepbe, például egy kevésbé képzett takarító vagy karbantartó szerepébe. (2) Megbízhatóság. Egy stresszes vállalati környezetben a munkájában bizonytalan munkavállaló számára biztonságot jelenthet egy megbízhatónak tűnő személy megjelenése. Ilyen esetekben az alkalmazott könnyen elárulhatja a vállalati titkokat, és gyorsan bizalmába fogadja a számára szimpatikus social engineert. Az emberek többsége hajlamos a jót feltételezni ember-

társaikról, így például, ha egy esőben elázott pizzafutár kér bebocsátást egy csak belépőkártyával elérhető folyosón található mosdóba, sok gondoskodó vagy anyáskodó nő hajlamos beengedni. (3) Szakszerűség. Amikor a social engineerek rendszergazdának adják ki magukat, és néhány szakzsargont használnak, az áldozatok általában természetes módon elfogadják, hogy egy szakember jött a számítógépük javítására, és magától értetődően átadják a hozzáférési neveiket és jelszavaikat a vállalati adatbázisokhoz. (4) Szerethetőség, szimpátia. Bizonyos social engineerek viszonylag könnyen tudják manipulálni áldozataikat, hogy elnyerjék szimpátiájukat. Ennek alapja, hogy még a támadás előtt felmérik, milyen kapcsolódási pontok lehetnek köztük és az áldozat között.

A gyakoribb szereprelációk (T = támadó, Á = áldozat és/vagy balek) [28] alapján:

- „feltűnően csinos és kívánatos nő (T) – saját magát túlértékelő, szexuális vágytól fűtött férfi (Á),
- beszállító cég intelligens, sármos középvezetője (T) – a harmincas éveiben járó, a férfiak megbecsülését és igaz szerelmét kereső nő (Á),
- az esőben elázott, vékony testalkatú, szemüveges pizzafutár, kerékpáros futár (T) – hasonló életkorú gyermeket nevelő nő (Á)
- a vállalat székhelyén dolgozó, legfrissebb híreket ismerő kolléga (T) – a telephelyen dolgozó, az információhiány miatt sorsukat bizonytalannak ítélő kollégák (Á)
- a dohányzó külsős kolléga, beszállító, vásárló (T) – a kijelölt helyen (vagy éppen a tilosban) dohányzók (Á)
- az új kolléga, aki segítséget kér a vállalat informatikai rendszereinek a használatához (T) – a kollégák, akik segítenek neki (Á)”

A szakszerűség és megbízhatóság szereprelációi [28] alapján:

- „a vállalat tevékenységét ellenőrző külsős személy (T) – a vállalat alkalmazottai (főleg azok, akik tudják, hogy valamilyen munkát nem, vagy nem megfelelő minőségben, vagy csak a megadott határidőn túl végeztek el) (Á)
- az informatikus/rendszergazda (T) – a számítógéphez és/vagy az informatikai rendszerhez nem értő kolléga (Á)”

Egyéb szereprelációk (általában nem alakul ki szimpátia, de hagyják tevékenykedni az álcázott támadókat) [28] alapján:

- takarítók (T) – dolgozók (Á)
- karbantartók, javítók (T) – dolgozók (Á)
- kerékpáros futárok, postások, csomagszállítók (T) – dolgozók (Á)
- pénz-és értékszállítók (T) – dolgozók (Á)

(5) Önuralom. Bár a social engineering támadások általában előre megtervezettek, az esetek többségében nem jellemző, hogy a támadó és az áldozat többször találkozik olyan helyzetben, hogy az áldozat emlékezne a támadó arcára (kivételt képeznek például a belső social engineerek, kémek, ügynökök). Ha a támadó nem az első találkozás alkalmával akarja végrehajtani a támadást, hanem többször találkozik az áldozattal (például beszállítóként egy cégnél), akkor önuralomra van szüksége a megfelelő alkalom kivárásához. Az önuralom a hitelesség hat tényezője közé tartozik, mert segíti a social engineert abban, hogy kontrollálja indulatait és szenvedélyeit. (6) Társas hajlam. Egy social engineernek – még ha a magán-

életben zárkózottabb is az átlaghoz képest – természetesen kell viselkednie a társas közegben, amikor a támadást végrehajtja. Képesnek kell lennie olyan témák felvetésére, amelyek érdeklik a csoportot, vagy aktívan hozzászólnia mások megjegyzéseihez, kérdéseihez. Amikor a támadó egy csoport ellen, vagy annak részeként hajt végre támadást (például egy ebédről visszatérő kollégákhoz csatlakozva lép be belépőkártya nélkül a vállalat zárt részeibe), akkor a csoporthoz illeszkedő természetes viselkedése „védelmet" nyújt számára, hogy a biztonsági személyzet vagy a recepciósok ne figyeljenek fel rá.

A kommunikációs modellek közül a Hymes [26] SPEAKING modelljét a(z információ)biztonság területén ki is tudtam próbálni, s igazoltam, hogy alkalmas a humán alapú social engineering támadások, illetve auditok megtervezésére és elemzésére, s ezáltal a(z információ)biztonság tudatosság fejlesztésére [27] [28]. A modell a beszédesemény elemzésére épül, Hymes [29] megfogalmazásában a beszédesemény „kizárólag olyan tevékenységekre, vagy tevékenységek aspektusaira vonatkozik, amelyeket a beszédhasználattal kapcsolatos szabályok vagy normák közvetlenül szabályoznak. Egy ilyen esemény állhat egyetlen beszédcselekményből, de gyakran inkább több cselekményből".

A beszédesemény elemzésénél Hymes a SPEAKING mozaikszót javasolja, amelynél az egyes betűk jelentése a következő:

- Setting/scene: beszédhelyzet,
- Participants: résztvevők,
- Ends: lezárások,
- Act sequences: cselekménysorozatok,
- Key: kulcs,
- Instrumentalities: eszközök,
- Norms: normák,
- Genre: műfaj.

ÖSSZEFOGLALÁS

Tanulmányomban, a szociálpszichológia, az antropológia és a kommunikációtudomány területeit vizsgáltam meg a biztonság különböző aspektusain keresztül. A szociálpszichológia az emberek közötti interakciókat és a társadalmi környezet egyénre gyakorolt hatásait elemezi, arra fókuszálva, hogy a kulturális, társadalmi és környezeti tényezők hogyan formálják az emberek biztonságérzetét. Ezen belül fontos kutatási területei közé tartozik a szociális reprezentáció, a társadalmi normák és azok megszegése, valamint az illúziók és tévedések hatása az emberi döntéshozatalra. Az antropológia kiterjedt vizsgálatai révén a modern nagyvárosi és munkahelyi környezetekre is koncentrál, feltárva, hogyan befolyásolják a mítoszok, legendák, hagyományok és társadalmi normák a kollektív biztonságot. Tanulmányomban különös figyelmet szenteltem annak, hogy az emberek miként alkalmazzák ezeket a kulturális elemeket a mindennapi életükben és hogyan segítenek ezek a közösségek kohéziójának és biztonságának fenntartásában. Írásomban több kommunikációs modellt is bemutattam, amelyek segítheti a biztonságtudatosság növelését és az ellenálló képesség erősítését a social engineering támadásokkal szemben. Kiemeltem a kölcsönös bizalom és az információmegosztás fontosságát, valamint a társadalmi normák dinamikus megértésének szükségességét a társadalmi egyensúly és az egyéni biztonság fenntartásában.

FELHASZNÁLT IRODALOM

[1] SHERIF, M. *The Psychology of Social Norms*. New York: Octagon Books, 1965.
[2] MENYHAY I. *Adalékok Káin „esti meséjéhez”.* Budapest: Akadémiai Kiadó. 1998.
[3] SMITH, E. R. – MACKIE, D. M. *Szociálpszichológia*. Budapest: Osiris Kiadó, 2001.
[4] FESTINGER, L. *A Theory of Cognitive Dissonance*. Redwood City: Stanford University Press, 1957.
[5] GILOVICH, T. *How We Know What Isn't So: The Fallibility of Human Reason in Everyday Life*. New York: The Free Press, 1993.
[6] KOLLÁR Cs: Emlékeink lenyomatainak információbiztonsága: Hogyan őrizhetőek meg és írhatóak át emlékeink a digitális korban? *POLGÁRI SZEMLE: GAZDASÁGI ÉS TÁRSADALMI FOLYÓIRAT* 13: 4-6, 2017. pp. 17-27.
[7] HEWSTONE, M. – STROEBE, W. – CODOL, J-P. – STEPHENSON, G. M. *Szociálpszichológia*. Budapest: Közgazdasági és Jogi Könyvkiadó, 1999.
[8] MILGRAM, S. *Obedience to Authority: An Experimental View*. New York: Harper & Row, 2009.
[9] GOFFMAN, E. *Az én bemutatása a mindennapi életben*. Budapest: Pólya, 2000.
[10] JAGODICS I. – KOLLÁR Cs. 21. századi social engineering támadások, védekezés és szervezeti hatások Európában. *BELÜGYI SZEMLE: A BELÜGYMINISZTÉRIUM SZAKMAI TUDOMÁNYOS FOLYÓIRATA (2010-)* 71: 1, 2023, pp. 2-126.
[11] KOLLÁR Cs. – ZAKAR Á. A social engineering és a manipulációs technikák és módszerek. *BIZTONSÁGTUDOMÁNYI SZEMLE* 2: 2, 2020. pp. 23-38.
[12] JUNG, C. G. *Archetypes and the Collective Unconscious*. New Jersey: Princeton University Press, 1959.
[13] DOUGLAS, M. *Purity and Danger: An Analysis of Concepts of Pollution and Taboo*. New York: Routledge, 2002.
[14] HOBSBAWM, E. – RANGER, T. *The Invention of Tradition*. Cambridge: Cambridge University Press, 2012.
[15] APPADURAI, A. *Fear of Small Numbers: An Essay on the Geography of Anger*. Durham: Duke University Press Books, 2006.
[16] MAUSS, M. *The Gift: Forms and Functions of Exchange in Archaic Societies*. Eugene: Wipf and Stock, 1954.
[17] FASSIN, D. *Enforcing Order: An Ethnography of Urban Policing*. Cambridge: Polity, 2013.
[18] ARONSON, E. *A társas lény*. Budapest: Akadémiai Kiadó, 2008.
[19] Em, G: *Bevezetés a kommunikációelméletbe*. Budapest: Harmat kiadó, 2001.
[20] TAYLOR, D. – ALTMAN, I: Communication in interpersonal relationship. In: ROLOFF, M – MILLER, G. (szerk.): *Interpersonal process, new directions in communication research*. Newburry Park: Sage, 1987.
[21] BERGER, C: Uncertainty and information exchange in developing relationship. In: DUCK S. (szerk.): *Handbook of personal relationship*. New York: Wiley, 1988.
[22] POOLE, M. S. *Decision development in small groups I.: A comparison of two modells.* Communication monographs. Vol 48, 1981.
[23] BONO, E. D. *A hat gondolkodó kalap – A párhuzamos gondolkodás szakaszai*. Budapest: Manager Könyvkiadó Kft., 2007.
[24] CIALDINI, R. *Influence: The Psychology of Persuasion*. New York: Quill, 1993.

[25] HOGAN, K. *A meggyőzés tudománya*. Budapest: Danvantara Kiadó, 2008.
[26] HYMES, Dell, H. *Foundations in Sociolinguistics: An Ethnographic Approach*. Philadelphia: University of Pennsylvania Press, 1974.
[27] KOLLÁR Cs. Az információbiztonság humán aspektusai: A biztonságtudatossági ellenőrzés során alkalmazott social engineering technikák elemzése a SPEAKING modell segítségével. *Belügyi Szemle (2010-)* 66: 2. 2018. pp. 22-45.
[28] KOLLÁR Cs. Social engineering a gyakorlatban: Manipulációk értelmezése a SPEAKING modellben. *JEL-KÉP: KOMMUNIKÁCIÓ KÖZVÉLEMÉNY MÉDIA* 6: 3, 2017. pp. 62-77.
[29] HYMES, D. Models of the Interaction of Language and Social Life. In.: GUMPERZ, J. – HYMES, D. (szerk.) *Directions in Sociolinguistics: The Ethnography of Communication.* New York, Holts Rinehart & Winston, 1972. pp 35-71.

ARTIFICIAL INTELLIGENCE IN THE LIFE'S WORK OF STANISŁAW LEM

A MESTERSÉGES INTELLIGENCIA STANISŁAW LEM ÉLETMŰVÉBEN

SZABÓ Lajos[1]

Abstract

Since 1956, countless devices and their programs have been declared to be artificial intelligence. The word “robot” has undergone a similar change of meaning since 1922. Lem devoted a significant part of his entire life's work to publishing his ideas on robotisation, cybernetics, and self-aware machine intelligence, which he described as homeostatic systems. The technological development of the 21st century is following precisely the same course, making the same mistakes, that Lem, with his characteristic sarcasm, has illustrated in the stories of Trurl and Klapancius. This paper presents the author's key findings for AI developers.

Keywords

Lem, AI, robots, cybernetics, design flaws, ethics and legal regulation

Absztrakt

1956 óta számtalan eszközt és programjukat nyilvánították mesterséges intelligenciának. A „robot” szó is hasonló jelentésváltozáson ment keresztül 1922 óta. Lem egész életművének jelentős részét a robotizációval, a kibernetikával és az öntudatos gépi intelligenciával kapcsolatos elképzeléseinek közzétételére fordította, amelyeket homeosztatikus rendszereknek nevezett. A 21. század technológiai fejlődése pontosan ugyanazt a pályát követi, ugyanazokat a hibákat követi el, amelyeket Lem a rá jellemző szarkazmussal illusztrált Trurl és Klapanciusz történeteiben. Ez az írás a szerző legfontosabb megállapításait mutatja be a mesterséges intelligencia fejlesztői számára.

Kulcsszavak

Lem, MI, robotok, kibernetika, tervezési hibák, etikai és jogi szabályozás

[1] szabo.lajos@uni-obuda.hu | ORCID: 0000-0001-9375-2188 | Lecturer Óbuda University / Institut of Safety Science and Cybersecurity | Chairman of the Board of Trustees, Foundation for Law Enforcement and Private Security Education and Research (REMOK)| kuratóriumi elnök, Alapítvány a Rendvédelmi és Magánbiztonsági Oktatásért és Kutatásért (REMOK)

BEVEZETŐ GONDOLATOK A MESTERSÉGES INTELLIGENCIA ÉS A ROBOT KIFEJEZÉSEK EREDETÉNEK TÉMÁJÁBAN

Akik részt vettek Asimov életművéről szóló előadásomon,[1] vagy olvasták az erről megjelent tanulmányt [2] azok pontosan tudják, hogy a mesterséges intelligencia és a robot kifejezés eredetileg mit takar. A jelen tanulmányban Lem életművét vizsgálom, és csak megemlítem Asimovval való kapcsolatát.

Röviden, pontokba szedve a következőket állapíthatjuk meg:

a) A tudományos és technológiai fejlődés hozta létre a mesterséges intelligenciákat.[3]
b) A robot és az MI fogalma a kezdetektől összefonódott (1920 Čapek). [4][5]
c) Kézenfekvő gondolat volt a csillagközi utazás és a bolygók meghódítása, földszerűvé alakítása (terraformálása) során olyan gépek alkalmazása, melyek nem csak automaták, de képesek a környezethez alkalmazkodni.
d) A sci-fi félig technológiai futurológia, maga a műfaj a technológiai fejlődéshez, várható eredményeihez kapcsolódik, vagyis kihagyhatatlan a sci-fi irodalomból a mesterséges intelligencia.

Lem a „*Tudományos fantasztikus irodalom és futurológia*”[6] című munkájában külön fejezetet szentel a mesterséges intelligenciával kapcsolatos problémakörnek, „*Robotok és emberek*” címmel. A „*Summa Technologiae*”[7] című könyve kizárólag ezzel a témával foglalkozik, de a kifejezést nem használja, azonban *A katasztrófa-elv* és *A huszonegyedik század fegyverrendszerei avagy a tótágas evolúció* című írása [8] szó szerint említi! Ebben hasonlít Asimovra, aki szintén mindössze két alkalommal írta le regényfolyamában a mesterséges intelligencia kifejezést, mint azt a róla szóló tanulmányban írtam [2].

Lem és Asimov kortársak voltak, Lem mindössze egy évvel volt fiatalabb pályatársánál, nem csoda, hogy hasonló problémákkal foglalkoztak, még ha teljesen eltérő megközelítéssel is. Asimov nem sokat foglalkozott a kibernetikával, a mesterséges intelligencia létrehozásának technológiájával, de mindketten foglalkoztak az ismeretelméleti megközelítésekkel, az etikával, a tudattal, a pszichológiai aspektusokkal.

Mindkettejük írásaiban megjelenik a megismerési folyamatok bemutatása szépirodalmi eszközökkel, és kiemelt fontossággal szerepel az intuíció, mint a gondolkodás egyik legkevésbé feltárható vagy feltárt pszichikai jelensége, a tudatos tevékenységet támogató tudatalatti folyamat.

De innen kezdve az elemezni kívánt szerzővel szeretnék már csak foglalkozni, aki a matériából szerzett információk alapján, tudattal rendelkező önálló (homeosztatikus) és önfejlesztő gépezetek elméletével foglalkozott.

„Bármit csinálunk is, anyagból csináljuk – elmélkedett tovább Mikromill –, tehát az anyagban rejlik minden lehetőség. Ha házat gondolunk ki, házat építünk; ha palotát, akkor palotát; ha gondolkodó csillagot képzelünk el, azt is meg tudjuk csinálni. De az anyagban több lehetőség van, mint a mi fejünkben; tehát szájat kellene adni az anyagnak, hogy maga mondja meg, mit lehet még csinálni belőle!

– Szájra csakugyan szükség van – helyeselt Gigacián –, de ez nem elég, mert a száj csak azt mondja, amit az elme kigondolt. Ezért nemcsak szájat kell az anyagnak adnunk, hanem gondolkodásra kell bírnunk, s akkor biztosan minden titkát feltárja előttünk!” (Kiberiáda: Hogyan kezdődött a ködök menekülése?) [9, 51. o.]

Stanisław Lemet, mint híres írót, legtöbben szépíróként vagy tudományos-fantasztikus íróként és nem tudósként ismerik, vagyis az elsődleges információ a nevéhez ez. Valóban nem szerzett egyetemi tanulás árán tudományos fokozatot. Pedig elismerték tudományos teljesítményét már életében!

Négy lengyel egyetem adományozott számára díszdoktori címet, majd 1972-ben a Lengyel Tudományos Akadémia tagjai közé választotta.[10]

Jellemző, ahogy arról Ropolyi László beszámol Lem életművéről szóló filozófiai elemzésében[11], „*amikor 1999. augusztusában Lengyelországban, Krakkóban tartották az IUHPS 11th International Congress of Logic, Methodology and Philosophy of Science kongresszusát, a kongresszus kiemelkedő eseménye nem egy ismert filozófus, hanem Lem fellépése volt.*"

Születésének 100. évfordulójára a Wroclawi Műszaki Tudományegyetem Lem-díjat [12] alapított. A díj kiírása egyben tiszteletadás Lem előtt: „*A Stanisław Lem Európai Kutatói Díjat (Stanisław Lem European Research Prize, „Lem Prize") a lengyel tudományos-fantasztikus regényíró, Stanisław Lem születésének 100. évfordulóján alapította a Wroclaw Tech. Az intézmény 1981-ben adományozott díszdoktori címet az irodalmár-futurológus professzornak. Lem munkáinak középpontjában a technológia és az emberiség kapcsolata állt.*"

Egyetemek is felvették írásainak elemzését. A brnói Masaryk Egyetemen, ahol a „*Filozófia a sci-fi-ben*" című kurzus a tanszékvezető professzor által vezetett téma [13], és a budapesti Eötvös Loránd Tudományegyetemen is foglalkoznak vele, hiszen Ropolyi László ott tanít, aki a már említett kitűnő összefoglalójában nagyon jó filozófiai-irodalmi összefoglalót ad Lem életművéről.

Számos más okot is felsorolhatnék, amivel igazolható a világszerte „csak" sci-fi íróként közismert szerző tudományos munkássága, de a fentebb felsoroltak elegendőek ahhoz, hogy komoly tudósként kezelje őt bárki, még az is, aki soha egy sort sem olvasott írásaiból.

Aki ezután kezd bele, mindenképpen tudnia kell, hogy Lem abban a korban született, amikor egy tudós, a latin és a görög nyelv ismerete nélkül nem számított tudósnak, és ugyanezen okból rendszeresen francia és angol frázisok is rendszeresen előfordulnak írásaiban. Ő maga egy már kiveszőfélben lévő „fajta" (elnézést a szóért), utolsó képviselőinek egyike, a klasszikus európai műveltséggel és felmérhetetlenül nagy lexikális tudással, ebből fakadóan hatalmas szókinccsel is rendelkező íróé, tudósé, akit egy nem kellően művelt személy sosem lesz képes megérteni, hacsak utána nem olvas azoknak a dolgoknak, amikről ír, megemlít, vagy meghivatkozik.

Ehhez kapcsolódik az a különleges képessége, hogy játszi könnyedséggel váltogatja írásainak stílusát. Egyszer mesét ír, másszor kacagtató sztorizásba kezd, szinte oda sem figyelve verseket ír, érzelmekkel zsúfolt regényt tár elénk, vagy átalakul egyetemi professzorrá és olyan könyvet ad a kezünkbe, amit fejezetenként le kell tenni, mert meg kell emészteni. És szinte mindegy, milyen stílusban ír, mindenütt magvas gondolatokkal, tudományos alapossággal teszi.

Nyelvi leleményei utolérhetetlenek, csak kevés műfordító képes arra, amire Murányi Beatrix, hogy azokat úgy jelenítse meg, ahogy azt a szerző a saját anyanyelvén megfogalmazta, elbűvölve olvasóit. A műfordító egyben önálló művész is, és Murányi Beatrix,

aki a legtöbb Lem-fordítást készítette, kétségtelenül azonosult az alkotó szándékaival és mesteri munkát végzett a magyar olvasók legnagyobb örömére.

A tanulmány nem vállalkozhat a magyar nyelven megjelent összes írásának bemutatására, ahogy a magyarul meg nem jelent művek értékelésére és arra sem, hogy bármely írását részletesen, alaposan elemezze, leginkább terjedelmi okok miatt. A fő vonulat a címben jelzett mesterséges intelligencia, és csak elenyésző mértékben teszek más, irodalmi, filozófiai, kapcsolódású megjegyzéseket.

Egy kaleidoszkóp készül tehát, ahol csak néha térek el a „kiemelt szín" – a mesterséges intelligencia – által megrajzolt alakzatoktól.

A MESTERSÉGES INTELLIGENCIA MEGJELENÉSE LEM ÍRÁSAIBAN

Először csak bemutatom, mennyire volt fontos a regényeiben, írásaiban a téma, rövid tartalmi összefoglalót adva az adott műről.

A *Pirx pilóta kalandjai* [14] című könyve a sci-fi felfutásának idején született, korának tipikus példája a korai űrkorszak irodalmának. Lem zsenije már itt megmutatkozik, a főszereplő Pirx minden kalandjában a főszereplő az intuíció. Ezért van az, hogy olyanokat tesz, amiket más nem is ért, miért teszi, de a történetek végére pontosan levezeti a cselekvés mozgatórugóit. Az első magyar kiadás fülszövegénél pontosabban magam se tudnám tömörebben megfogni a lényegét:

„*Egy elromlott robot áramköreiben régen halott űrhajósok személyiségeinek töredékei élnek tovább, s az éjszakánként felhangzott titokzatos morzejelekben újra meg újra végigélik a tragédiájukat… Tökéletesen emberi külsejű robotűrhajósok szövögetik számítógép pontosságú, hideg terveiket próbaútjukon, ahol senki sem tudhatja a másikról, robot-e vagy ember… Egy robot a névtelen bolygón hegymászásra adja a fejét – elromlott-e, vagy a sportszellem ébredt fel benne?…*

Stanisław Lem, a világhírű tudományos-fantasztikus író szokásához híven ezekben az elbeszélésekben is izgalmas gondolatokat vet fel az ember és a gép viszonyáról, a mesterséges érzékszervekről és személyiségekről, a robotok „lélektanáról" és a technológiai korszak sok más időszerű és jövőbe világító kérdéséről."

Igen, a mesterséges intelligenciáról van benne szó, az esetleges hibás tervezésből, szerelésből, mechanikai sérülésből, vagy programozási hibából adódnak bajok. Hogy ezt kezelni lehessen, néha fel kell tárni a gép „pszichéjét".

A Legyőzhetetlen [15] című regényben egy lépéssel előbbre merészkedve elképzel egy olyan bolygót, amelyen robotok ökoszisztémáját találja az oda látogató ember. A mesterséges intelligencia különféle szintjeit fedezhetjük fel, miközben az embereket inforobotok, energorobotok és felderítő robotok, javítórobotok, szállítóautomaták segítik az önfenntartó robotokból álló, a „lant-lakók" által kifejlesztett, majd magukra hagyott és önfenntartó, önfejlesztő kibernetikai ökoszisztéma ellen a Regis III nevű bolygón.

*A Legyőzhetetlen*ben megismert, alacsony tudattal rendelkező robotrovarok és társaik jóval később, *A huszonegyedik század fegyverrendszerei avagy a tótágas evolúció* című írásban térnek vissza, *Az emberiség egy perce* [8] című kötetben. Ez utóbbiban feltételez egy nagyon apró, homokszem méretű mikrochipet, ami átalakítja a fegyvereket és a háborúskodást.

A téma érdekességét az adja, hogy napjainkra elértük azt a szintet, hogy már képesek vagyunk nano méretű alkatrészeket gyártani [16].

És nem csak erre vagyunk képesek, hanem mint egy 2021. szeptember 24-én megjelent cikk (Repülőből a légkörbe: *Íme a világ első repülő mikrochipje, ami egy hangyánál is kisebb)* írja: *»Néhány kutató kifejlesztette a világ első homokszem méretű repülő mikrochipjét, amit repülőből kidobva juttatnának a légkörbe.*" [17] és ez nem az egyetlen ilyen méretű eszközökről szóló beszámoló, teljesen nyílt forrásból, ami pedig azt jelenti, hogy ennél sokkal fejlettebbek is lehetnek titkos katonai és más laborokban! A Lem által vizionált „chipkatonák" minden műszaki paramétere rendelkezésre áll, pontosan úgy, ahogy leírta. Már csak attól kell tartanunk, hogy lesz olyan fejlesztőmérnök, aki olvasta Lem e tárgyban írt okfejtését [8], és bezárhatjuk (végre) az összes eddigi fegyvergyárat.

Nem ez az első valóra vált „jóslata", hiszen Ropolyi László már idézett cikkében [11] olvasható: „*Büszkén hivatkozik a bevált esetekre, így például a virtuális valóság lehetőségének hatvanas évekbeli előrejelzésére, illetve Leszek Kołakowski korabeli Summa technologiae-kritikájának érvénytelenségére és saját álláspontja harminc év utáni igazolódására*." A technológiai fejlődés lehetséges következményeinek előre látása nyilvánvalóan a kornak megfelelő szintű ismeretekből és a fejlődés látható irányainak ismeretéből adódott, vagyis tudományosan megalapozott lehetséges jövőkép bemutatása és nem „jóslás" volt.

A *Visszatérés* [18] című regényben számtalan fajtájú android és nem android robot szerepel, mind a számára készített, a munkája elvégzéséhez szükséges szintű értelemmel rendelkezik. Pontosan úgy, mint a *A Legyőzhetetlen*ben leírt különféle szinten értelmes automaták. A leírás koherens, pontosan betartva a tudományos hipotézis alapján végzett, logikus gondolati menetrendet. A katarzis a „városi selejtállomás" területén jelentkezik, ahol kiderül, a robotok „élnek", éntudattal rendelkeznek és könyörögnek, hogy ne semmisítsék meg őket.

Az *Éden* [19] című regényében egy bolygón különféle önállóan kifejlődött robotok teremtenek „értelmes" civilizációt, az emberi civilizáció karikatúráját, a mesterséges intelligencia által alkotott világot.

A *Solaris* [20] című regényben egy nem emberi létformával való találkozás során egy bolygó óceánja tudatos lény, akit szeretnének a kutatók megismerni és megérteni, miközben az idegen „lény" szembesíti az embereket önmagukkal, akik magukat sem ismerik. Pontosan szembesít bennünket azzal a ténnyel, hogy milyen nehéz megfogalmazni, mi az, hogy tudat, értelmes lény, gondolkodás, emberi vagy nem emberi értelem vagy intelligencia. Filozófiai mű, nagyon sok időt tölt azzal, hogy az elbizakodott technokrata szemléletet, az elméleti alapok nélküli fejlesztési kényszert szembeállítsa a valódi ismeretekkel és mindannak hiányával, ami nélkül nem lehet létrehozni a mesterséges intelligenciát.

Az Úr hangja [21] című regényben a nem emberi létformákkal való kapcsolatfelvétel próbálkozásait írja le, a regény megírásának korában már alkalmazott módszerekkel, jelek leadásával és keresésével, de itt is megjelennek a kísérleti homeosztátok, a kibernetikai modellezés módszerei is, annak érdekében, hogy a kapott „üzenetet" dekódolni lehessen. Pontosan úgy, mintha egy titkosírás megfejtésére írnánk programot egy számítógépnek, amilyen programokból mára már jelentős készlet áll rendelkezésünkre.

A *Summa Technologiae*[7] (továbbiakban Summa) meggyőződésem szerint Lem főműve, csekély szerénységgel Aquinói Szent Tamás *Summa Teologiae* című munkájára

utaló címével. Míg Tamás az isteni teremtő szándék, az abból fakadó elvek, erkölcs és a világ működésének feltárására tett kísérletet, addig Lem a XX. század közepéig elért technológiai eredményekre alapozva a lehetséges fejlesztési irányok közül a gépi, önállóan működő és önfejlesztő értelmet lehetővé tévő, emberi értelem által „teremtő" kibernetikának a lehetőségeit, jövőjét mutatja be. Enciklopedikus tudásanyagot feldolgozó tudományos, kibernetikai elméleti alapvetés. Az általunk létrehozható homeosztátok és a bennük munkáló, általunk kifejlesztett tudat, a mesterséges intelligencia viszonyait boncolgatja, miközben tükröt tart elénk. Minden mérnöknek, informatikusnak kötelező olvasmány!

Lem az 1960-as években írta Summáját, mégis minden megállapítása érvényes még most, a XXI. század elején is. Fejezetről fejezetre, bekezdésről bekezdésre azonosíthatóak lehetnének a Summából a Lem által írt egyes regények, novellák, melyeket újra és újra vizsgálat, vagy magyarázat tárgyává tett. Mint írtam „lehetnének", de terjedelmi okokból itt nyilvánvalóan nem fogom elvégezni az azonosításukat. Lem szerencsére gondoskodott róla, a Summával egy időben, hogy elkészítse Summájának egy olyan változatát, melyet bárki képes megérteni, ha cseppet elgondolkozik a novellákon. Érdekes, de ilyen megállapítást az író műveivel foglalkozó elemző írások egyikében sem találtam, holott nyilvánvaló az egyezés a *Summa Technologiae* [7] és a *Kiberiáda* [9] között.

A *Kiberiáda* [9] című elbeszélés-kötetben ott vannak az alapkérdések, kockázatok, erkölcsi, elméleti és gyakorlati problémafelvetések. Trurl és Klapanciusz, a két mérnök robot, és mint a „Perpétuális Omnipotencia Oklevél" tulajdonosai és „omnigenerikus tervezők", mindenre képesek, amire a „természet" képes, a Summa [6] minden fejezete felismerhető, egy-egy történetben akár több fejezet, vagy több probléma is egy írásban. Ráadásul irodalmilag változatos palettán, az egyszerű tanmesétől (*Három kóbor űrlovag*)[9, 7-14.o] az Ezeregy éjszaka meséiből ismert egymásba fűződő mesék sorozatáig (*Zsenalion király három mesélőgépe*) [9, 301-382. o.], a rövid kabarétréfa-szerű novellától (*Hogyan kezdődött a ködök menekülése*) [9, 50-56.o.] egy társadalmi jelenség tökéletes kifigurázásáig (*Újabb pótutazás avagy Trurl mint szaktanácsadó*) [9, 262-271.o.].

A *Kibériáda* és a másutt fellelhető Trurl és Klapanciusz történetek azoknak szólnak, akik a száraz szakkifejezésekkel és tudományos megállapításokkal zsúfolt Summát megérteni nem lennének képesek. Példabeszédek, vicces karcolatok, bennük véresen komoly megállapításokkal.

Példának álljon itt az Elektrubadúr történetének néhány részlete:

„*Mint tudjuk, Trurl épített egyszer egy számítógépet, amelyről kiderült, hogy csak egyetlen műveletet tud elvégezni, nevezetesen azt a szorzást, hogy mennyi kétszer kettő, de még azt is rosszul. Mindamellett, mint másutt már elbeszéltük, ez a gép roppant hiú volt, csúnyán összezördült saját alkotójával, és az eset csaknem tragikusan végződött az utóbbi számára. Attól kezdve Klapanciusz megkeserítette Trurl életét, állandóan csúfolta, kaján célzásokkal gyötörte, mígnem Trurl megdühödött, és elhatározta, hogy olyan gépet épít, amely verseket fog írni. E célból összegyűjtött nyolcszázhúsz tonna kibernetikai irodalmat és tizenkétezer tonna költeményt, aztán hozzálátott az anyag tanulmányozásához. Mikor megcsömörlött a kibernetikától, áttért a lírára, és viszont. Hamarosan rájött, hogy maga a gép megépítése gyerekjáték a programozáshoz képest.*" [9. 177.o.]

A technokrata megvilágosodása a szövegkészítő, versíró automata készítése közben. A gépet legyártani könnyű, de a benne futó programhoz sok-sok információra van szükség, hiszen olyan mesterséges intelligenciát szeretne, amelyik bármiről, bármilyen

verset képes elkészíteni, vagyis nem csak irodalmi, hanem nyelvtani, matematikai, fizikai, történeti, szociológiai és még számtalan tudományterület ismereteit kell tartalmazza a program, ráadásul időrendi sorrendben, a fejlődés fokozatait is ismerve.

„*A programot, amely egy közönséges költő fejében lakozik, a civilizáció teremtette, amelyben az illető a világra jött; ezt a civilizációt az előző hozta létre, az előzőt egy még korábbi, és így tovább, egészen a világmindenség kezdetéig, amikor a jövendő poéta információi még kuszán kószáltak az ősködben. Ennélfogva a gép programozásához előbb meg kellett ismételni – ha nem is az egész világmindenséget elejétől fogva, de legalábbis jókora részét. Trurl helyében mindenki visszariadt volna ettől a feladattól, de a mi mérnökünket kemény acélból faragták: esze ágában sem volt meghátrálni.*" [9, 178.o.]

A technokrata tudja, hogy elméletben ez a gépezet és benne a program létrehozható, és szeretné meg is valósítani, ehhez azonban mindent modelleznie kell.

Érdekes, pont a cikk megírása közben jelent meg újabb könyve Csányi Vilmosnak, és az ennek kapcsán tett megállapításai pont ide illenek. A riport címe: *Csányi Vilmos: Semmi értelme mesterséges intelligenciával reprodukálni az embert* már önmagában sokatmondó, de olvassuk tovább: „*Olyan volt, mintha egy 12 éves gyerek írta volna, aki már jól tud beszélni, és tökéletes mondatokat tud írni. Pont ez a különbség a gondolkodó intelligencia és a nyelvi intelligencia között. Hiába töltöttek bele tízezer könyvet, ezekben nincs benne az én életem vagy a maga élete. Elvileg lehet persze olyan mesterséges intelligenciát csinálni, aminek van élettörténete. Húsz évig kellene nevelni, különböző feladatokkal ellátni, interakciókba hozni a társadalommal. Reprodukálhatjuk az embert, csak semmi értelme.*" [22]

Kemény mondatok, de figyeljük, mit írt Lem erről kicsit több mint fél évszázada? Miképpen oldotta fel a nyelvi intelligencia megteremtésének paradoxonát? „*Mindenekelőtt épített egy gépet, amely a káoszt modellezte, és villamos lélek lebegett benne a villamos vizek felett, aztán betáplálta a fény paramétereit, aztán az ősködökét, és így lassacskán elérte az első jégkorszakot; ez persze csak azért volt lehetséges, mivel a gép a másodperc ötmilliárdod része alatt hétszeptillió eseményt modellezett, amelyek négyszázoktillió helyen játszódtak le egyszerre; de ha valaki úgy véli, hogy Trurl tévedett valahol, akkor számoljon utána.*"

Nem sokban tér el Csányi és Lem véleménye, de a 20 év, illetve a teremtés és az értelem létrejötte majd annak biológiai, szociológiai, nyelvi stb. fejlődése között komoly különbség van! A mai technokraták elbizakodottan „öntik bele a tudást" programjaikba, miközben azon sopánkodnak, hogy kimerült a forrásanyagok készlete. Ahogy arról, a New York Times cikke [23] „Az OpenAI, a Google és a Meta figyelmen kívül hagyta a vállalati irányelveket, megváltoztatta saját szabályait, és a szerzői jogi törvények megkerüléséről tárgyalt, amikor online információkat kerestek legújabb mesterséges intelligencia rendszereik betanításához." alcímmel írja a következőket:

„*2021 végén az OpenAI ellátási problémával szembesült. A mesterséges intelligencia laboratóriuma kimerítette az interneten található jó hírű angol nyelvű szövegek minden tárházát, amikor kifejlesztette legújabb AI-rendszerét. Több adatra volt szüksége a technológia következő verziójának betanításához – sokkal többre. ... Zuckerberg úr megoldást követelt, az alkalmazottak szerint. Az a képesség, amit Mark keres a termékben, olyasmi, amit jelenleg nem tudunk biztosítani" - mondta az egyik mérnök.*" [9. 179. o.]

Képtelenek felismerni azt a tényt, amit Lem elmagyarázott, és Csányi is felismert! A különféle „vezető” csevegőprogramok készítői ugyanazzal a dölyfös elbizakodottsággal kezdtek bele programjaik megalkotásába, mint az összes operációs rendszer, vagy a hozzájuk tartozó programok készítői. Elvek, alapos felkészülés és tudományos módszertan nélkül, a feladatra koncentrálva összetákolnak valamit, ami úgy-ahogy teljesíti elvárásaikat.

De maradjunk az Elektrubadúrnál, ahol a gépezet olyan verset ír, amilyenre nagy valószínűséggel a szövegfeldolgozásra és szövegek gyártására jelenleg rendelkezésre álló programok és az elkövetkezendő évtizedekben elkészülők bizonyosan nem lesznek képesek. Hacsak valamelyik programozó, aki olvasta az Elektrubadúr történetét, nem modellezi a teremtéstől napjainkig az emberi civilizációt, tölti fel minden létezhető ismerettel a programot és nem statisztikus, hanem a művészekre jellemző intuitív, heurisztikus intelligenciát nem teremt… Jöjjön az idézet:

„*– Hát akkor tessék! Rendelj másik verset! Amiről csak tetszik! Na, miért hallgatsz? Félsz,mi?!*

– Nem félek, csak gondolkodom – felelte bosszúsan Klapanciusz, és igyekezett a lehető legnehezebb témát kitalálni, mert joggal gyanította, hogy nehéz lesz eldönteni a vitát, vajon a gép alkotta vers jó-e vagy sem.

– Írjon kiberotikus verset! – ragyogott fel hirtelen. Legfeljebb öt sor legyen, de szóljon szerelemről, árulásról és halálról, a néger kérdésről és a nimfomániáról, legyen benne a bonyolult női lélek extrém konfliktushelyzetben bekövetkező meghasonlásának ábrázolása, a középkori feudális viszonyok és erkölcsök maró bírálata, rímeljen, és minden szó k betűvel kezdődjön!

– És a végtelen automaták általános elmélete ne legyen benne? – horkant fel a vérig sértett Trurl. – Ilyen hülye feltételeket nem lehet szab…

De elakadt a szava, mert az egész csarnokot betöltő, bársonyos bariton máris megszólalt:

Kóbor kaffer kószál királylány kertjében.
Királylány kacéran kacsint kéjvágyó kedvében:
Kapj karodba, kaffer! Király kinéz, kiált:
Katonák! Kürtszó, kivégzés. Királylány kacag kuszán.
Kegyetlen kor! Kicsapongó, koronás kurtizán!” [9, 184.o.]

A beszélgetésre, szövegelemzésre és -készítésre tervezett programok nyilvánvaló okokból ilyen teljesítményre sosem lesznek képesek, mindössze abból a megfontolásból, hogy tervezőik elmulasztották a káosz modellezését, a virtuális teremtést és a többit, amit Trurl nem.

A közismerten ateista Lem nem először és nem utoljára vesz bibliai idézeteket, illetve utal rájuk. Kedvenc megoldása, nagyon kevéssé rejtett utalásokkal, a vallás és a tudományos ismeretelméletek szembeállítása, például az *Álmatlanság* című könyvből a *Non Serviam*[2] című novellában. Az ott kifejlesztett gépi értelem eljut oda, hogy feltételezze és keresse teremtőjét, akihez való viszonyát azonban teljesen ateista, pragmatikus logika határozza meg, ezért nem érez hálát azért, mert megteremtették, és nincs oka szolgálnia teremtőjét…

2 latin, jelentése: „Nem szolgálok”

De hiszen *Magafia Majmász* (a Kiberiádából) [9, 363-370.o.] végig viszi ugyanezt a fejlődési folyamatot, és öntudatra ébredésével egyszersmind nyelvi kultúrát is teremt, nem pont olyat, mint az Elektrubadúr, de mégis létrehozza, hiszen fogalmakban, kategóriákban logikusan gondolkodni csak a nyelv ismeretében lehetséges.

Tökélyre azonban a *Léboló* [23, 214-261.o.] című történetben fejlődik, ahol Trurl a robotmérnök tökéletesen hozza azt az emberi magatartást, amit minden emberi találmánnyal – legyen az eszköz, technológia, anyag – kapcsolatban elkövetett és jelenleg is elkövet az emberiség.

Megcsinál valamit, mert képes rá. Üzemelteti, miközben az elméleti és gyakorlati hiányosságok következtében előálló problémákat igyekszik kezelni, megjavítani. Aztán amikor rájön, hogy a találmány elméletileg megalapozatlan volt, a tervezéskor nem vett figyelembe néhány alapvető elvet, ezért veszélyt jelent az üzemeltetőre vagy az emberiségre, korlátozza a használatát, vagy felhagy vele, vagy megsemmisíti.

Pontosan úgy viselkedik, a rendelkezésére álló technológiával visszaélve, anélkül, hogy kellő elméleti alapokkal, átgondolva venné használatba, ahogy az 1991-ben készült *Hook* című filmben a kapitányt zseniálisan alakító Dustin Hoffman bemutatja a gyermeki önzést és türelmetlenséget: „*Akarom, Akarom, Akarom, Én, Én, Én, Enyém, Enyém, Enyém, Most, Most Most!!!*”

Lem a *Léboló*ban szinte lépésről lépésre leír majdnem mindent, amit a Summában tudományos alapossággal kifejt, egyetlen novellába sűrítve, ahol a végén *Cerebron Profeszszor* pikírt alapossággal rápirít tanítványára, hogy bármennyire kitűnő gépész, bármennyire is képes bármit megépíteni, tevékenysége elméletileg megalapozatlan, felkészületlensége kárhozatos következményeket eredményez, hibás elképzelései katasztrofális végeredményhez vezetnek.

A *Léboló* olyan szintű tömörítése Lem *Summá*jának – amely hatalmas tudományos teljesítmény, doktori értekezésnek, vagy akár akadémiai székfoglaló értekezésnek is megfelel terjedelme, hivatkozásai száma és alapossága okán – amire csak kevesen képesek. A novella szinte egy-egy mondatba foglalja össze a *Summa* alcímeinek és főcímeinek bőséges tartalmát. Ráadásul a Lemre jellemző név- és fogalomalkotást is tartalmazza, átfogalmazva a *Summa* definícióit, hogy megfeleljen a *Kiberiádá*ban megszokott, humorban és szójátékokban tobzódó, kacagtató, mégis elgondolkodtató stílusjegyeknek.

LEM IRÁNYMUTATÁSA ÉS A VALÓSÁG

Lem egész életművével az ember teremtette mesterséges környezet és az ember viszonyát, a mesterséges intelligencia megteremtésének irányába tett emberi próbálkozások és lehetséges következményeinek viszonyát tárta elénk.

Mindvégig az elbizakodott technokrácia (Lem saját kategóriája, melyekből számosat alkotott) ellen agitált, tükröt állítva azoknak, akik miközben kísérleteznek, pajkos játéknak fogják fel a programok és hozzá tartozó gépek készítését, nem veszik észre tetteik következményeit.

Az Elektrubadúr a történet szerint verseivel földönfutóvá teszi az írókat, költőket, személyes és társadalmi válságokat indít el. Jelenleg a különféle chatbotok üzemeltetői, fejlesztői tekintetében a szerzői jogok vitája zajlik, mint arról a már említett New York Times-cikk [25] beszámol, de ugyanez már elkezdődött a képzőművészeti alkotások terén, és biztosak lehetünk benne, hogy a tudományos felfedezések területén is fel fog lángolni a szerzői

jogi vita. Vajon nem erről van szó az „önvezető autók” fejlesztése és a balesetért való felelősség kérdésében?

Lem már akkor írt a virtuális valóságról és a vele kapcsolatos problémákról, amikor a CAD (Computer Aided Design) még alig pár éve létezett, és csak raszteres zöld vonalakat lehetett húzni katódsugárcsöves monitorok képernyőire.

*Summá*jában ott van a technikai civilizáció határa, az energiafelhasználási igény és a rendelkezésre álló energia kérdésének megtárgyalása, és következtetése lesújtó. Addig pusztítjuk energiakészletünket, míg végül nem leszünk képesek tovább fenntartani a technikai civilizáció megszokott szintjét.

A valóság az, hogy naponta annyi elektromos energiát használnak fel a chatbotok (már nem robot, csak bot), kép- és filmkészítő programok és a kapcsolt szerverek és tárhelyek, ami meghaladja Magyarország éves energiatermelését. Mindezt a felhasználók puszta szórakozásként, passzióként, a fejlesztők kísérletként, az egészet finanszírozó mágnások befektetésként élik meg, miközben iszonyatos pocsékolás és környezetrombolás folyik.

A mindenféle elvi, erkölcsi, ismeretelméleti, és még számos más megközelítést mellőző, kizárólag technikai elbizakodottságból eredő „csináljuk meg, hiszen képesek vagyunk legyártani” hozzáállás folyamatos kudarcok és katasztrófák okozója lesz. Elég csak a különféle számítástechnikai fiaskókat figyelni, máris az látszik, amit Lem előre leírt, hiszen ő volt talán az egyetlen, aki valóban végig gondolta, levezette, majd papírra vetve megjelentette gondolatait.

Van olyan elterjedt, világszerte szinte mindenki által használt operációs rendszer, amelyikhez a megalkotását követően nem kellett kiadni biztonsági frissítést, utólagos toldást-foldást (foltozást), vagy amelyiknek ne lenne ismert nulladik napi hibája?

Írtak már ezekhez a rendszerekhez tartozó olyan programot, amelyiken ne kellett volna változtatni, mert felületesen készítették el és később a silány munka gondokat okozott?

Készült olyan hardvereszköz, amelyiknek a firmware-jében nem volt utólag hiba, mely gondokat okozott?

Szerintem a témában járatosak azonnal minden kérdés végére rávágták: Nincs!

A helyzet pontosan megfelel a *Summa Technologiae* zárószavában leírtaknak: „*A berendezések megbízhatóságát nem vizsgálhatjuk a statisztikai-technikai módszerektől függetlenül. Ezt a technológiai fejlődés írja elő, amelyben a sorozatgyártást (a tömegtermelést) a termelt berendezések bonyolultságának növekedése kíséri. Ha egy 500 elemből álló rendszer minden eleme 99%-ig megbízható is, a rendszer mint egész mégis alig 1%-os megbízhatóságú (feltéve, hogy működéséhez az összes elemei feltétlenül szükségesek). Az elérhető maximális megbízhatóság az elemek számának négyzetével áll arányban, aminek folytán megbízható terméket lehetetlen kapnunk, különösen akkor, ha nagyon bonyolult rendszerről van szó. Az emberhez mint szabályozóhoz „kapcsolt" rendszerek (a repülőgép, a gépkocsi) kevésbé érzékenyek a sérülésekre, minthogy az ember plasztikus viselkedése gyakran kompenzál egy hibás működést. Ezzel szemben egy „embernélküli" rendszerben, amilyen az interkontinentális rakéta vagy általában egy automatikus berendezés (pl. számítógép), nem lehet szó ilyen plaszticitásról, s ezért az ilyeneknél tapasztalható kisebb fokú megbízhatóságot nemcsak elemeik nagyobb száma, valamint az alkalmazott technológia újszerűsége, hanem a véletlenül beállt hibák jelenségeit „kiegyenlítő" ember hiánya is okozza…”* [6, 352.o.]

Az ok pedig olyan egyszerű, ahogy azt a *Léboló*ban Lem leírta, Cerebron szavaival: „*Elhanyagoltad az elméletet, mint lusták lustája, mint egyébiránt tehetséges idióta, és én eltűrtem, mert ügyes voltál az alacsonyabb művészetekben, amelyek az órásmesterségre mennek vissza.*" [23, 253.o.] Vagyis megcsinálták, előállították azt a valamit, amire képesek voltak, annak ellenére, hogy az elméletét nem értették, elkészíteni megtanulták úgy-ahogy, felszínesen, és hibákat vétettek. Nyilvánvaló, hogy amíg a témával foglalkozó pszichológia, filozófia és más tudományok nem képesek megegyezni abban, mi az a tudat, mi az az intelligencia, miképpen működik, addig nem tudjuk modellezni, és létrehozunk valamit, amit elnevezhetünk akárhogy, sosem lesz képes arra, amire szánták.

Ahogy a köznyelvi „mesterséges intelligencia" is külön programok halmaza, az „emberi intelligencia" is annyiféle, ahányan vagyunk a Földön, az elvárható tudásszint is ugyanekkora szórást mutat.

Lem pontosan leírta, milyen szempontokat kellene figyelembe venni a mesterséges intelligencia tervezésénél. Pontosan leírta, milyen hibákat lehet elkövetni a tervezés és az üzemeltetés közben, milyen problémákkal kerülünk szembe használata során.

Nyilvánvaló, hogy az értelmezésében, működésében, céljaiban különböző programok esetében, ahol a téma „szakértői" – akik ugyanolyan szakértők, mint a futurológusok –, akik a jelen tényeiből és tendenciáiból következtetnek a jövőre, jellemzően tendenciózus, mintsem tényszerű javaslatot tudnak adni a szabályozás tekintetében.

Igen, ahol nincsenek alapelvek, vagy ha vannak, de nem tartják be azokat a tervezők, mint ahogy Trurl sem a *Léboló*ban, nem igazán lehet jó szabályozást csinálni. Az Az EU [25] és USA [26][27][28] által készített, tagállamaik által elfogadott normatív szabályozások ugyanazon ismeretelméleti, erkölcsi alapvetések hiánya miatt, melyeket Lem leírt a *Kiberiádában* [9] és a *Léboló*-ban [24], alkalmatlanok a problémák kezelésére, hatályba lépésük, ami esetenként több év, nem veszi figyelembe a közben elérhető újabb és újabb szintű fejlesztéseket, paradigmaváltásokat. Magas bonyolultsági szintű kibernetikus homeosztátok esetében ugyanúgy nincs 100%-os biztonság, mint a legegyszerűbb szervezet esetén sem a világunkban, ha már valamilyen elfogadható szinten működik egy program, már elégedetten dörzsölhetjük a kezünket.

Mint ahogy képtelenek vagyunk egyelőre előállítani egy használható „emberire hasonlító" mesterséges intelligenciát, gyárt a sok fejlesztő olyat, amilyet tud. A politikusok, a jogalkotók megpróbálják szabályozni, ahogy tudják. Ugyanaz a hályogkovács módszer: vagy sikerül, vagy nem.

Meg kell jegyezni, hogy a katonai, rendészeti mesterséges intelligencia programok és eszközök kivételek, nem tartoznak e szabályozás tervezett köreibe, sem az EU, sem az USA szabályzóiban, ami további aggodalmakra ad lehetőséget.

MEGÁLLAPÍTÁSOK

A XXI. század 20-as éveiben számos olyan program kísérleti alkalmazása és továbbfejlesztése folyik, melyek közös jellemzője, hogy önfejlesztő, öntanuló programrészeik segítségével helyettesíthetik az emberi tevékenységet. Szöveges vagy képi megjelenítéssel képesek olyan termékek előállítására, melyeket eddig csak az emberek voltak képesek létrehozni. Ezeket összefoglaló néven, mesterséges intelligenciaként aposztrofálja a

tudományos és a bulvársajtó is, egybemosva a különféle célra készített programokat. A fejlesztések az önálló tevékenység irányába haladnak a gépi alkotás, gondolkodás területén.

Lem életműve ugyanilyen képességekkel rendelkező öntanuló, önfejlesztő homeosztátokkal foglalkozik. Az író már a múlt század második felének elején készített egy összefoglaló művet, mely leírta mindazokat a várható programokat és alkalmazásuk következményeit, amelyekkel napjainkban szembesülünk.

Fontosnak tartom felhívni a témával foglalkozó elméleti és gyakorlati szakemberek figyelmét arra, hogy fordítsanak nagyobb figyelmet munkájuk elméleti, elvi megalapozására, mielőtt kísérletezni kezdenek.

FELHASZNÁLT FORRÁSOK

[1] Szabó Lajos: A mesterséges intelligencia Asimov szemével, avagy egy élet munkája. https://bgk.uni-obuda.hu/bki/author/kiss-gaborbgk-uni-obuda-hu/

[2] Szabó Lajos: A mesterséges intelligencia Asimov szemével, avagy egy élet munkája. Biztonságtudományi Szemle, 6. évf. 2. szám 2024. ISSN 2676- 9042 123-136. oldalak.

[3] Mesterséges Intelligencia Elektronikus Almanach TAMOP - 4.1.2-08/2/A/KMR-2009-0026 http://project.mit.bme.hu/mi_almanach/books/aima/ch01s03 1.3.1. A mesterséges intelligencia érlelődése (1943–1955) utolsó bekezdés.

[4] Mesterséges Intelligencia Elektronikus Almanach TAMOP - 4.1.2-08/2/A/KMR-2009-0026 http://project.mit.bme.hu/mi_almanach/books/aima/ch01s03 1.3.4. A mesterséges intelligencia megszületése –– 4. bekezdés utolsó előtti mondata.

[5] A robot szó 90 éves – 2011. január. 27. 13:45 https://hvg.hu/tudomany/20110127_90_eves_robot_szo_Čapek

[6] Stanisław Lem: Tudományos fantasztikus irodalom és futurológia. Gondolat Kiadó, Budapest 1974.

[7] Stanisław Lem: Summa Technologiae (tudomány, civilizáció, jövő). Kossuth Könyvkiadó, Budapest, 1972.

[8] Stanisław Lem: Az emberiség egy perce. Európa Könyvkiadó, Budapest, 1988.

[9] Stanisław Lem: Kiberiáda. Európa Könyvkiadó, Budapest, 1987.

[10] https://www.wikiwand.com/hu/Stanis%C5%82aw_Lem

[11] Ropolyi László: Így szólott Trurl és Klapanciusz. Kellék filozófiai folyóirat, 38. szám, 2008. https://www.prophilosophia.ro/assets/files/kellek-38/003ropolyi.pdf

[12] A Lem-díj hivatalos honlapja: https://lemprize.pwr.edu.pl/

[13] Masaryk Egyetem Brno Filozófia tanszék, Filozófia a sci-fiben témakör a tanszékvezető témája https://www.phil.muni.cz/fil/sci-fi/program.html

[14] Stanisław Lem: Pirx pilóta kalandjai. Európa Könyvkiadó, Budapest, 1970.

[15] Stanisław Lem: A legyőzhetetlen. Kozmosz könyvek, Budapest, 1967.

[16] Stanford egyetemi hírek: New high-speed microscale 3D printing technique https://news.stanford.edu/2024/03/13/high-speed-microscale-3d-printing/

[17] Repülőből a légkörbe: Íme a világ első repülő mikrochipje, ami egy hangyánál is kisebb https://leet.hu/2021/09/24/repulobol-a-legkorbe-ime-a-vilag-elso-repulo-mikrochipje-ami-egy-hangyanal-is-kisebb/
[18] Stanisław Lem: Visszatérés. Európa Könyvkiadó, Budapest, 1970.
[19] Stanisław Lem: Éden. Kozmosz könyvek, Móra Ferenc Könyvkiadó, Budapest, 1973.
[20] Stanisław Lem: Solaris. Európa Könyvkiadó, Budapest, 1968
[21] Stanisław Lem: Az úr hangja. Kozmosz könyvek, Móra Ferenc Könyvkiadó, Budapest, 1980.
[22] Csányi Vilmos: Semmi értelme mesterséges intelligenciával reprodukálni az embert https://index.hu/tudomany/2024/04/15/csanyi-vilmos-semmi-ertelme-mesterseges-intelligenciaval-reprodukalni-az-embert/
[23] Stanisław Lem: Álmatlanság. Európa Könyvkiadó, Budapest, 1974. Stanisław Lem: Bezsenność Widawnictwo Literackie, Krakow.
[24] How Tech Giants Cut Corners to Harvest Data for A.I. https://www.nytimes.com/2024/04/06/technology/tech-giants-harvest-data-artificial-intelligence.html
[25] Az Európai Parlament és a Tanács rendelete a mesterséges intelligenciára vonatkozó harmonizált szabályok (a mesterséges intelligenciáról szóló jogszabály) megállapításáról és egyes uniós jogalkotási aktusok módosításáról https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/AUTRES_INSTITUTIONS/COMM/COM/2023/10-25/COM_COM20210206_HU.pdf
[26] Maintaining American Leadership in Artificial Intelligence. A Presidential Document by the Executive Office of the President on 02/14/2019 https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence
[27] Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government, A Presidential Document by the Executive Office of the President on 12/08/2020 https://www.federalregister.gov/documents/2020/12/08/2020-27065/promoting-the-use-of-trustworthy-artificial-intelligence-in-the-federal-government
[28] Blueprint for an AI Bill of Rights https://www.whitehouse.gov/ostp/ai-bill-of-rights/

ON THE DIGITAL THRESHOLD: NATO'S RESPONSE TO MODERN SECURITY POLICY CHALLENGES

A DIGITÁLIS KÜSZÖBÖN: A NATO VÁLASZA A MODERN BIZTONSÁGPOLITIKAI KIHÍVÁSOKRA

PÁL ANITA[1]

Abstract

The article presents NATO's responses to modern security policy challenges by reviewing the historical background from Cold War military research to the transformation of global society, and then analyzes in detail NATO's cyber defense strategies and the development of AI integration, taking into account ethical and legal issues. It highlights significant cases and examples from the field of cyber defense, as well as the benefits and risks of AI integration in defense strategies. AI integration adds a new dimension to defense strategies, but also raises many ethical and legal concerns, such as automated decision-making. Linking the societal impact of technological innovations with security policy is critical for NATO to understand and address modern challenges. Finally, we link the social impacts of technological innovations with security policy to get a comprehensive picture of NATO's responses to modern challenges.

Keywords

NATO, cyber security, information warfare, artificial intelligence, security policy

Absztrakt

A cikk bemutatja a NATO válaszait a modern biztonságpolitikai kihívásokra, azáltal, hogy áttekinti a hidegháború katonai kutatásaitól kezdve a globális társadalom átalakulásáig terjedő történelmi hátteret, majd részletesen elemzi a NATO kibervédelmi stratégiáit és az AI integrációjának fejlődését, figyelembe véve az etikai és jogi kérdéseket. Jelentős eseteket és példákat emel ki a kibervédelem területéről, valamint az AI integráció előnyeit és kockázatait a védelmi stratégiákban. Az AI integráció új dimenziót ad a védelmi stratégiáknak, ugyanakkor számos etikai és jogi aggályt is felvet, például az automatizált döntéshozatalt illetően. A technológiai innovációk társadalmi hatásainak összekapcsolása a biztonságpolitikával kritikus fontosságú a NATO számára a modern kihívások megértése és kezelése szempontjából. Végül összekapcsoljuk a technológiai innovációk társadalmi hatásait a biztonságpolitikával, hogy átfogó képet kapjunk a NATO válaszairól a modern kihívásokra.

Kulcsszavak

NATO, kiberbiztonság, információs hadviselés, mesterséges intelligencia, biztonságpolitika

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

A DIGITÁLIS KÜSZÖBÖN: A NATO VÁLASZA A MODERN BIZTONSÁGPOLITIKAI KIHÍVÁSOKRA

A modern világ biztonságpolitikai kihívásai között egyre nagyobb szerepet kapnak a kiberfenyegetések és a mesterséges intelligencia alkalmazása. Ezen technológiák rohamos fejlődése és integrációja a védelmi stratégiákba olyan új dimenziókat nyitnak, amelyekre a NATO-nak és tagállamainak egyaránt reagálniuk kell. A technológia és a geopolitikai viszonyok változásának üteme magával hozta a biztonságpolitikai paradigmák átalakulását is. A hidegháború vége óta eltelt évtizedek során a katonai szövetségek és védelmi stratégiák egyre inkább az információs technológiák köré szerveződtek, kiemelve az innováció és a hálózatépítés fontosságát.

A kibervédelem és a mesterséges intelligencia kérdésköre nem csupán technikai vagy technológiai kihívásokat jelent, hanem etikai, jogi és politikai dilemmákat is magában foglal. Ezek a technológiák új lehetőségeket és veszélyeket hoznak magukkal, amelyek megértése és kezelése elengedhetetlen a modern kori biztonságpolitikai stratégiák szempontjából. Az információs társadalom és a transznacionális kereskedelem kibontakozása globális szintű összekapcsolódást eredményezett, amely meghatározó befolyást gyakorol a nemzetközi kapcsolatokra és a biztonsági politikákra.

A NATO mesterséges intelligencia stratégiájában a szövetségesek és a NATO kötelezettséget vállaltak amellett, hogy biztosítják, hogy az általuk kifejlesztett és bevetésre szánt mesterséges intelligencia-alkalmazások megfeleljenek a Felelős Felhasználás hat Alapelvének: törvényesség; felelősség és elszámoltathatóság; magyarázhatóság és nyomon követhetőség; megbízhatóság; kormányozhatóság; és az elfogultság mérséklése. Ez a felelős megközelítés biztosítja, hogy a mesterséges intelligencia alkalmazása összhangban legyen a nemzetközi jogi normákkal és támogassa a NATO kollektív védelmi és biztonsági céljait, miközben felkészül a kihívásokra és a technológiai változásokra a biztonságpolitikai környezetben.[1]

Ebben a kontextusban a NATO szerepe és reakciói kulcsfontosságúak. A szövetség a hidegháború óta jelentős változásokon ment keresztül, amelyek középpontjában a technológiai adaptáció és a kiberbiztonság erősítése állt. A NATO-nak mint intézménynek szembe kell néznie a kibervédelem új kihívásaival, beleértve a szövetséges országok közötti koordináció javítását, a kiberfenyegetésekkel szembeni védekezési képesség fokozását, valamint a mesterséges intelligencia etikai és jogi kereteinek kidolgozását.

A cikkben részletesen akartam tárgyalni a hidegháború óta eltelt időszak katonai kutatásait, a globalizáció hatásait, a NATO kibervédelmi stratégiáinak evolúcióját, valamint a mesterséges intelligencia integrálását a biztonságpolitikába. Mindezek mellett kitérünk az interdiszciplináris megközelítések fontosságára is, amelyek ötvözik a technológiai, társadalomtudományi és biztonságpolitikai elemzéseket. A cikk célja, hogy átfogó képet nyújtson arról, hogyan alakítják és formálják ezek a tényezők a modern világ biztonságpolitikai döntéseit, és milyen kihívásokkal és lehetőségekkel kell szembenézniük a jövőben a NATO és tagállamai számára, valamint, hogy mik azok a történelmi, technológiai és politikai dimenziók, amelyek meghatározóak a NATO jelenlegi és jövőbeli biztonságpolitikai szerepvállalása szempontjából.

A HIDEGHÁBORÚ ÉS A KATONAI KUTATÁSOK KEZDETEI

Az időszak, melyet a hidegháború határozott meg, az Amerikai Egyesült Államok és a Szovjetunió közötti geopolitikai, ideológiai és katonai feszültségekről szólt. Ez a korszak 1945-től, a második világháború lezárásától egészen 1991-ig tartott, amikor is a Szovjetunió felbomlásával véget ért ez a globális vetélkedés. A két szuperhatalom és szövetségeseik a katonai technológiák, különösen az atomfegyverek és hosszú távú ballisztikus rakéták fejlesztésére összpontosítottak, amelyek meghatározták a katonai egyensúlyt és az elrettentés politikáját.

A katonai fejlesztések ezen felül magukban foglalták a légi és űrkutatásokat is. Az űrverseny kulcsfontosságú állomásai voltak a 1957-ben felbocsátott Szputnyik műhold és az 1969-es Apollo 11 holdra szállás, amelyek döntő mérföldköveket jelentettek a hidegháború idején. Ezek a technológiák nemcsak katonai szempontból voltak jelentősek, hanem számottevő hatást gyakoroltak a civil technológiákra és az ipari fejlődésre is. Mi sem példázza jobban az akkori kutatásfejlesztések fontosságát, mint az a tény, hogy napjainkra bekrült a kibertér is a NATO 5. műveleti területei közé, amelyre kiterjesztette az 5. cikkelyének vonatkozásait is.

A katonai kutatásokon túl, a számítástechnika és a kriptográfia fejlődése is előtérbe került, ami alapjaiban formálta át a hírszerzést, a katonai kommunikációt és a kiberháború kezdeti lépéseit. Az elektronikus hadviselés és a kiberbiztonság kérdései a hidegháború idején váltak kiemelt fontosságúvá, és napjainkban is kulcsfontosságú elemei a nemzetbiztonsági stratégiáknak.[2]

A biztonságpolitikai környezet átalakulása drasztikusan csökkentette a katonai tényezők szerepét. A hagyományos államok közötti háború kitörésének veszélye a közeljövőben minimálisra csökkent, bár a katonai konfliktusok és regionális válságok továbbra is jelentős kockázatot jelentettek az euroatlanti régió számára. A közép- és kelet-európai politikai rendszerváltozásokkal a hidegháborús korszak kétoldalú politikai és katonai ellentéteken alapuló rendszere, valamint annak ideológiai alapjai is megszűntek. Ezt a viszonylag stabil, bár magas katonai kockázatokkal járó helyzetet váltotta fel a politikai, gazdasági és társadalmi átalakulások által kiváltott új és régi feszültségek okozta instabilitás.[3] Ebben a megváltozott biztonságpolitikai környezetben új kockázati tényezők is megjelentek. A nem katonai jellegű kihívások - mint a terrorizmus, a tömeges migráció, a tömegpusztító fegyverek terjedése, és a nemzetközi bűnözés - súlya megnőtt, így annak következményei kihatottak mind a katonai, mind a polgári biztonságra egyaránt. A globalizáció jelensége azt eredményezte, hogy a korábban távolinak tűnő nemzetközi feszültségek mára közvetlenül megrengethetik az egyén biztonságról alkotott képét.[4]

A GLOBALIZÁCIÓ ÉS AZ INFORMÁCIÓS TÁRSADALOM KIALAKULÁSA

A hidegháború vége után a világ hatalmas léptékkel transzformálódott a globalizáció kényelme felé, ami egyszerre hozott előnyöket és kihívásokat a világgazdaságnak, politikának és kultúrának. A globalizáció ezen korszakában központi szerepet kapott az információs technológia, különösen az internet és a kommunikációs eszközök gyors fejlődése. Az 1990-es évek elején az internet kereskedelmi felhasználásának liberalizálása új dimen-

ziókat nyitott meg az információs társadalom előtt, lehetővé téve az információ és a kommunikáció korábban elképzelhetetlen mértékű áramlását, valamint a tér és az idő közötti korlátok megszűnését.

Az információs társadalom fejlődésével párhuzamosan növekedett a transznacionális kereskedelmi kapcsolatok és a gazdasági integráció fontossága. A nemzetközi üzleti tevékenységek és a globális ellátási láncok expanziója jelentős hatást gyakorolt a világgazdaságra, átformálva azokat a dinamikákat, amelyek korábban meghatározták a nemzetközi gazdasági rendszert. Ezek a változások nem csak gazdasági, hanem biztonságpolitikai következményekkel is jártak. Új típusú kihívások és fenyegetések jelentek meg, mint például a kibertámadások és az információs háborúk új formái, amelyek nemcsak új kockázati tényezőket hoztak a nemzetközi kapcsolatokban, de megváltoztatták az elrettentés politikájában és a szövetségi rendszerek egymáshoz való viszonyulásában és függőségi viszonyokat is.

A katonai és civil technológiák közötti együttműködés, valamint a kibertér és az információs infrastruktúrák védelme kiemelten fontossá vált. A NATO és más nemzetközi szervezetek számára ez azt jelentette, hogy újra kellett gondolniuk és adaptálniuk kellett védelmi stratégiáikat, hogy megfeleljenek az új, digitalizált világ kihívásainak. Az információs társadalom kialakulása így nem csak technológiai forradalmat jelentett, hanem mélyreható politikai és társadalmi változásokat is előidézett, amelyek ma is jelentősen befolyásolják a világ globális biztonságpolitikáját. [5]

Ez a folyamat alapvetően átalakította az államok közötti interakciókat, erősítve a nemzetek közötti függőségeket, miközben növelte azokat a lehetőségeket, amelyek révén a kisebb államok is részt vehetnek a globális piacon. Ugyanakkor a fokozott összekapcsolódás új sebezhetőségeket is teremtett, amelyek kezelése kulcsfontosságú a nemzetközi stabilitás fenntartása szempontjából. Az információs kor hajnalán a biztonságpolitikai tervezőknek és döntéshozóknak újra kell gondolniuk stratégiáikat, hogy képesek legyenek kezelni a digitalizált világ rendkívül összetett és gyorsan változó fenyegetéseit.[6]

A technológiai trendek jelentős változásokat hozhatnak, mivel a fejlett algoritmusok (például gépi tanulás) egyre jobban kihasználják a rengeteg digitális adatot (big data) emberihez hasonló viselkedés és tevékenységek (mesterséges intelligencia) létrehozására. A gépek sok feladatban hatékonyabbak lehetnek az embereknél, ami az interakciók exponenciális növekedéséhez vezethet. A vállalatok egyre inkább a szoftverekre és digitális tartalmakra támaszkodnak új termékek gyors fejlesztéséhez. Hasonlóképpen, az algoritmusok online vásárlási pontosságának javulása az online vásárlás dominanciájához vezethet, ahol a szoftverek autonóm módon szállítják a szükséges termékeket a vásárlók digitális nyilvántartásai alapján. Ezek a változások nagy hatással lesznek az üzleti tevékenységekre és a versenyre.[7]

A NATO KIBERVÉDELMI STRATÉGIÁINAK EVOLÚCIÓJA

Ahogy a digitális kor fejlődött, úgy vált egyre nyilvánvalóbbá, hogy a kiberfenyegetések jelentős kihívást jelentenek a nemzetek biztonságára. A NATO, mint transzatlanti katonai szövetség, kénytelen volt szembenézni azokkal a kihívásokkal, amelyek az információs kor hajnalán kezdődtek és napjainkra egyre összetettebbé váltak. Amint a tagállamok kormányzati, katonai és infrastrukturális rendszerei egyre inkább célpontjává váltak a

kibertámadásoknak, úgy vált maga a kibervédelem egyre kiemeltebb prioritássá a szövetség számára.

Az elmúlt évtizedekben a NATO számos lépést tett a kiberbiztonsági kapacitásának megerősítése érdekében. Ezen folyamat során több jelentős eset is bekövetkezett, amelyek rávilágítottak a kollektív védelem kiberdimenzióinak fontosságára. Például, 2007-ben Észtország ellen indított kibertámadás, amelyet állami szponzorált orosz hackereknek tulajdonítanak, széles körű zavart okozott az ország kormányzati, pénzügyi és hírközlési rendszereiben. Ez az eset katalizátorként szolgált a NATO számára, hogy felgyorsítsa saját kiberreakciós erőinek fejlesztését, és 2008-ban létrehozta a NATO Kiberbiztonsági Kiválósági Központját (CCDCOE) Tallinnban, amely a kibervédelmi kutatás és képzés központja lett.[8]

2021 novemberében Tallinn adott otthont a „Cyber Coalition 21" nevű hadgyakorlatnak, amely a NATO legnagyobb kibervédelmi eseménye, és világviszonylatban is kiemelkedő jelentőségű. célja a NATO és szövetséges országok kiberbiztonsági szakértőinek felkészültségének és együttműködési képességeinek tesztelése volt. A gyakorlaton 21 tagállam több mint 1000 szakértője vett részt, beleértve Svájc, Finnország, Írország és Svédország képviselőit is. A gyakorlat különféle válság-szcenáriókat tartalmazott, amelyek valós fenyegetéseket szimuláltak, mint például gázvezeték szolgáltatók elleni kiber- és információs támadások. Ezek a szcenáriók a valósághűségre és a geopolitikai realizmusra törekedtek, például a 2021 eleji amerikai Colonial Pipeline támadásra reagálva. A résztvevők nem versengtek egymással, hanem együttműködve oldották meg a feladatokat, fejlesztve a NATO-tagállamok közötti kooperációt és vészhelyzeti információcserét. A gyakorlat kiemelt figyelmet fordított a modern információs hadviselésre, beleértve a közösségi média platformokon végzett kognitív támadásokra való felkészülést.[9]

Az Adat- és Mesterséges Intelligencia Felülvizsgáló Testület (DARB-Data and Artificial Intelligence Review Board) a szövetségesek fórumaként és a NATO azon erőfeszítéseinek fókuszpontjaként szolgál, amelyek a mesterséges intelligencia felelős fejlesztésének és használatának szabályozására irányulnak. A DARB-on keresztül a szövetségesek és a NATO olyan felelől mesterséges intelligencia (RAI-Responsible AI) használatokon és gyakorlatokaon (fog csiszolni, amelyek megbízhatóbb, interoperábilis és biztonságosabb rendszereket biztosítanak, elősegítve minőségi előnyök elérését a stratégiai versenytársakkal és a potenciális ellenfelekkel szemben.[10]

A NATO válasza a kiberfenyegetésekre nem csupán technikai védekezésre korlátozódik. A szövetség a tagállamok közötti információmegosztást és együttműködést is ösztönzi, amely elengedhetetlen a gyorsan változó kiberfenyegetések hatékony kezeléséhez. Az intézkedések között szerepel a kiberháborús gyakorlatok rendszeres végrehajtása, a kiberbiztonsági politikák harmonizációja, valamint a kiberbűnözéssel szembeni fellépés koordinálása. Ezek a lépések biztosítják, hogy a NATO képes legyen védelmet nyújtani nem csak a hagyományos, hanem a digitális fenyegetésekkel szemben is.

A NATO folyamatosan fejleszti kiberbiztonsági stratégiáit, hogy megfeleljen a modern kihívásoknak, és védelmezze tagállamai digitális infrastruktúráit a növekvő kiberfenyegetésekkel szemben. A szervezet kiberbiztonsági politikája a tagállamok közötti együttműködésen és az új technológiák bevonásán alapul, ami kulcsfontosságú a kollektív biztonsági rendszer fenntartásához a 21. században. A NATO válasza a kiberfenyegetésekre így

nem csupán a jelenlegi veszélyekre ad választ, hanem a jövő kihívásaira is felkészül, biztosítva, hogy a szövetség tagjai közötti védelmi kötelék ellenálló maradjon a digitális korban.

A MESTERSÉGES INTELLIGENCIA A BIZTONSÁGPOLITIKÁBAN

A technológia gyors fejlődése három fő irányban halad előre. Először is, a processzorok teljesítménye olyan ütemben növekszik, hogy a következő években nagyobb számítási kapacitás lesz elérhető, mint eddig valaha. Másodszor, a szoftverek nem csak a világot hódítják meg, hanem alapvetően átalakítják a számítástechnika területét, különösen a mély neurális hálózatok fejlődésének köszönhetően. Harmadszor, a hordozható eszközök elterjedésével az elektronikus tartalom mennyisége 24 havonta megduplázódik, és a jelenlegi digitális adatok 90%-a az elmúlt két évben jött létre. Ez az exponenciális növekedés várhatóan a közeljövőben is folytatódni fog.[11]

Az elmúlt években a mesterséges intelligencia (MI) fejlődése átformálta a védelmi stratégiákat és újra értelmezte a biztonságpolitikai paradigmákat. A technológia előretörése jelentős hatással van a katonai műveletekre, a hírszerzésre és a kibervédelemre, megváltoztatva ezzel a nemzetek közötti erőviszonyokat és a globális biztonsági környezetet.

Az MI integrációjának kulcsfontosságú területei közé tartozik a hírszerzési tevékenységek optimalizálása, ahol az MI képes óriási adathalmazokat feldolgozni és értelmezni, lehetővé téve ezzel a gyorsabb és pontosabb döntéshozatalt. A kibervédelemben az MI alapú rendszerek előre láthatják és automatikusan reagálhatnak a fenyegetésekre, így növelve a hálózatok biztonságát és ellenálló képességét. Továbbá, a robotizált és autonóm hadviselési technológiák fejlesztése új dimenziókat nyit meg a harctéri műveletekben, amelyek potenciálisan minimalizálhatják az emberi veszteségeket.[12]

Az MI technológiai előnyei mellett azonban számos etikai és jogi kihívás is felmerül: a döntések átláthatósága, a felelősség kérdésköre, valamint a teljesen autonóm fegyverrendszerek használatának morális vetületei mind olyan témák, amelyek komoly vitákat váltanak ki a szakértők és a döntéshozók körében. A nemzetközi jogi szabályozások kialakítása és az etikai normák meghatározása lassan halad a gyors technológiai fejlődéshez képest, ami kihívásokat jelent a globális biztonság és alkalmazhatóság szempontjából.

A NATO mesterséges intelligencia stratégiájának keretein belül a szövetségesek és a NATO elkötelezték magukat amellett, hogy az általuk fejlesztett és alkalmazott mesterséges intelligencia rendszerek megfeleljenek a Felelős Felhasználás hat alapelvének (PRU-Principles of Responsible Use): törvényesség; felelősség és elszámoltathatóság; magyarázhatóság és nyomon követhetőség; megbízhatóság; kormányozhatóság; valamint az elfogultság csökkentése.[13]

2022-ben a NATO-szövetségesek további lépéseket tesznek a mesterséges intelligencia, az adatok, az autonómia és a digitális átalakítás felelős használatára. Az Igazgatóság első feladata egy felhasználóbarát felelős mesterséges intelligencia tanúsítási szabvány kidolgozása lesz, beleértve a minőség-ellenőrzést és a kockázatcsökkentést is, amely elősegíti az új mesterségesintelligencia- és adatprojektek összehangolását a NATO 2021 októberében jóváhagyott felelősségteljes felhasználási elveivel.[14]

A NATO Adat- és Mesterséges Intelligencia Felülvizsgáló Testülete (DARB) létrehozásának alapvető célja, hogy elősegítse a mesterséges intelligencia felelős fejlesztését

és alkalmazását a védelmi szektorban. A DARB központi szerepet tölt be a bizalom építésében a nyilvánosság, az innovátorok és a végfelhasználók között, miközben irányítást biztosít a felelős védelmi innovációkhoz a nemzetközi normák és jogi előírások szerint. A testület fontos szerepet játszik abban, hogy a mesterséges intelligencia alkalmazásait a NATO és a szövetséges államok számára elfogadható, megbízható és interoperábilis módon alakítsa át, csökkentve a kockázatokat és ellenőrizve a minőséget. A DARB fórumként is szolgál, ahol a szövetségesek megoszthatják a legjobb gyakorlatokat és véleményeket cserélhetnek, ezzel támogatva a kollektív védelmi erőfeszítéseket. A testület munkája eredményeként a NATO és tagállamok gyakorlati mesterséges intelligencia eszközkészleteket dolgoznak ki, melyek a NATO és a szövetségesek számára is elérhetők. Ezek az eszközök és eljárások a tapasztalatokra, a NATO érdekelt felei által adott bemenetekre és a nemzetközi gyakorlatokra épülnek, beleértve a köz-, magán-, akadémiai szektort és a civil társadalmat is. A testület agilis módon irányítja a mesterséges intelligencia megvalósítását a NATO-n belül, alkalmazkodva a változó körülményekhez és technológiai fejlődéshez. Célja, hogy támogassa a szövetségeseket a mesterséges intelligencia eszközkészletek nemzeti szintű használatában és a felelős tervezési gyakorlatok alkalmazásában, erősítve a NATO kollektív védelmi képességeit a stratégiai versenytársakkal és potenciális ellenfelekkel szemben.[15]

A MESTERSÉGES INTELLIGENCIA A VÉDELMI STRATÉGIÁKBAN

A mesterséges intelligencia integrációja a védelmi stratégiákba az elmúlt évtizedek egyik legmeghatározóbb technológiai fejlődése. Az MI alkalmazása a katonai és biztonságpolitikai területeken számos új lehetőséget nyitott meg, így a hírszerzési tevékenységek hatékonyságának növelésétől kezdve a kibervédelmi rendszerek fejlesztésén át a robotizált hadviselésig. Az MI lehetővé teszi, hogy a védelmi rendszerek gyorsabban és pontosabban reagáljanak a fenyegetésekre, miközben csökkenthetik az emberi tényezőből adódó hibák és az azokból adódó késedelmek számát. Ezekben az eszközökben és műveletekben mindig is fontos szerepet játszott a nyílt forrású információszerzés (OSINT), amely az internet elterjedésével és a világhálón tárolt adatok feldolgozásával jelentős mértékben átvette a hagyományos emberi hírszerzés (HUMINT) szerepét. Az MI alkalmazása az OSINT-ben növeli az információszerzés sebességét és hatékonyságát, legyen szó szövegbányászatról, képfelismerésről vagy összefüggések elemzéséről.[16]

A mesterséges intelligencia integrációja a hírszerzési műveletekbe forradalmasította a modern hadviselést és biztonságpolitikát. Az MI képessége, hogy hatalmas adatmennyiségeket dolgozzon fel és elemezzen gyorsasággal és pontossággal, lehetővé teszi a hírszerző szervezetek számára, hogy az eddiginél sokkal hatékonyabban azonosítsák és értékeljék a fenyegetéseket. Ez a technológia kritikus döntéshozatali támogatást nyújt a biztonsági erőknek, lehetővé téve számukra, hogy gyorsan reagáljanak és megfelelő intézkedéseket hozzanak.[17]

Az MI a hírszerzés terén elsősorban képfelismerésre, nyelvi feldolgozásra és viselkedési minták elemzésére használható. Például, a drónok és műholdak által gyűjtött képi adatokat MI algoritmusok elemzik, azonosítva a fontos objektumokat és mozgásokat olyan helyzetekben, ahol az emberi elemzőknek napokba telne a feldolgozás. Az MI segítségével a hírszerzés képes lépést tartani a folyamatosan változó és fejlődő kibertérrel, ahol a fenyegetések gyorsan változhatnak és evolválódhatnak.[18]

A hírszerzési MI alkalmazásai közé tartozik a szociális média és nyílt források monitorizálása is, ahol az algoritmusok képesek felismerni a különleges eseményeket, hangulati változásokat vagy radikalizálódási jeleket. Ezen technológiák integrációja lehetővé teszi a döntéshozók számára, hogy jobban megértsék a globális politikai és társadalmi trendeket, és előre lássák a potenciális zavarokat vagy konfliktusokat.

Ezek az MI alkalmazások tehát alapvetően növelik a hírszerzési képességeket, miközben új kérdéseket vetnek fel a magánélet védelmével és az adatkezeléssel kapcsolatban. Az AI által vezérelt hírszerzés hozzájárul a nemzetbiztonsági célkitűzések hatékonyabb eléréséhez, miközben biztosítja a gyors és alapos adatelemzést, amely elengedhetetlen a modern biztonsági kihívások kezelésében.

A MESTERSÉGES INTELLIGENCIA SZEREPE A KIBERFENYEGETÉSEK KEZELÉSÉBEN

A mesterséges intelligencia (MI) alapvető szerepet játszik a kiberfenyegetések azonosításában és kezelésében, mivel az AI technológiák képesek a hálózati forgalom mintáinak folyamatos elemzésére és a rendellenes viselkedés azonosítására. Az MI rendszerek gyorsan reagálnak a potenciális biztonsági incidensekre, automatizált védelmi protokollokat aktiválva, amelyek azonnali lépéseket tesznek lehetővé a fenyegetések elhárítására, még mielőtt azok kárt okoznának.

Az MI segítségével a kibervédelmi rendszerek képesek adaptálni és tanulni a különféle támadási technikákból, így növelve a védelmi stratégiák hatékonyságát az idő előrehaladtával. Az incidensreagálási stratégiák automatizálása, mint például a sebezhetőségek gyors javítása vagy a támadási vektorok elszigetelése, kulcsfontosságúak az információs infrastruktúrák védelmében. Az mesterséges intelligencia tehát nélkülözhetetlen eszközzé vált a kiberbiztonsági szakértők számára, amelyek íly módon képesek lépést tartani a folyamatosan változó kiberfenyegetésekkel és proaktívan védekezni ellenük.[19]

Automatizált harci rendszerek: Autonóm fegyverek és járművek

Az MI integrációja a védelmi stratégiákba kiterjed az automatizált harci rendszerekre is, amelyek középpontjában az autonóm fegyverek és járművek állnak. Ezek a rendszerek képesek önállóan döntéseket hozni és végrehajtani különböző műveleteket emberi beavatkozás nélkül, bonyolult és veszélyes környezetben is. Az MI által vezérelt döntéshozatal lehetővé teszi a harci műveletek gyorsaságának és hatékonyságának növelését, miközben csökkenti a katonák életveszélyes helyzetekben való kitettségét.

Autonóm rendszerek alkalmazása jelentős előnyöket kínál, mint például a reakcióidő drasztikus csökkentését és a műveletek precizitásának növelését. Az MI képes „real-time" adatok alapján elemzéseket végezni, így optimalizálva a célzási és támadási protokollokat. Emellett, az autonóm járművek, mint drónok és robotizált földi járművek, képesek felderítő és megfigyelő feladatokat ellátni, kritikus információkat szolgáltatva a döntéshozóknak.[20]

Azonban ezeknek a technológiáknak a bevezetése komoly etikai kérdéseket is felvet. Az AI által vezérelt döntéshozatal, különösen a harci környezetben, számos aggodalmat generál a felelősség és az elszámoltathatóság terén. Ezért fontos, hogy a fejlesztés és alkal-

mazás során szigorú etikai keretek között mozogjunk, biztosítva, hogy az autonóm rendszerek használata összhangban legyen a nemzetközi jogi előírásokkal és humanitárius normákkal.

Etikai és jogi kihívások

Bár az MI technológia jelentős előnyöket kínál a védelmi stratégiákban, számos etikai és jogi kérdést is felvet. Ezek között a legfontosabbak:

- A mesterséges intelligencia védelmi alkalmazása etikai és jogi dilemmákat vet fel, amelyek kezelése elengedhetetlen a technológia felelős integrálásához a katonai stratégiákba. Az MI vezérelte *döntéshozatali folyamatok átláthatóságának kérdése* kulcsfontosságú, mivel az ilyen rendszerek gyakran zárt, nehezen érthető algoritmusokon alapulnak. A "fekete doboz" jelenség, amely az MI által hozott döntések mögötti logikát homályban hagyja, komoly kihívásokat jelent a biztonságpolitika számára. A védelmi döntéshozóknak és a hadseregnek meg kell birkózniuk azzal a tényezővel, hogy hogyan biztosítható az elszámoltathatóság, amikor az MI részt vesz a kritikus döntések meghozatalában. A modern háborúkban alkalmazott MI technológiák növelik a hadműveletek hatékonyságát, de ezeknek a rendszereknek a döntései mögötti logika megértése és ellenőrzése létfontosságú marad.[20]
- Az autonóm fegyverrendszerek etikai vetületei további aggodalmakat vetnek fel. Amikor a gépek képesek önállóan dönteni élet és halál kérdéseiről, felmerül a kérdés, hogy vajon a technológia felelősségteljesen használható-e. A nemzetközi közösség már évek óta küzd azzal, hogy meghatározza azokat a kereteket, amelyek között az autonóm fegyverek bevetése elfogadható lenne. Ezek a viták gyakran az emberi felügyelet szükségességére koncentrálnak, ahol a döntő kérdés, hogy *az MI által hozott döntések mekkora mértékben igényelnek emberi beavatkozást vagy ellenőrzést*. A nemzetközi jogi normák és a hadviselésre vonatkozó etikai előírások nehezen tartják lépést a technológia fejlődésével, ami késlelteti az egyértelmű szabályozások kialakulását.[21]
- Végül, a *szabályozás és felügyelet kérdésköre* is elengedhetetlen a biztonságpolitikai szempontból releváns MI alkalmazások esetében. A nemzeti és nemzetközi szabályozó testületeknek folyamatosan értékelniük kell az MI technológiák fejlődését, hogy megfelelő kereteket állíthassanak fel az etikus használathoz. A katonai MI alkalmazások szigorú felügyelete kulcsfontosságú a biztonságos és felelős technológiai integráció érdekében. Az ilyen rendszerek bevezetésével járó kockázatok kezelése érdekében szükséges egy átfogó jogi és etikai infrastruktúra kiépítése, amely képes alkalmazkodni a gyors technológiai változásokhoz és azok új kihívásaihoz.[22]

Ezek a kérdések alapvető jelentőséggel bírnak a modern biztonságpolitikai döntéshozatalban, és létfontosságúak a mesterséges intelligencia katonai alkalmazásainak jövőjére nézve. Az átláthatóság, az etikai felelősség és a hatékony szabályozás kulcsfontosságúak az MI technológiák biztonságos és felelős használatának biztosításához.

Ezen kihívások kezelése érdekében szükség van a nemzetközi jogi keretek továbbfejlesztésére és a nemzetközi együttműködés erősítésére. A NATO és az ENSZ együttműködése például kritikus a kibervédelem és az információs biztonság területén, mivel ezek a területek közvetlenül érintik a tagállamok nemzeti biztonságát és a nemzetközi stabilitást

vagy akár az autonóm döntéshozatal kérdéskörét. Ezen kihívások kezelése érdekében szükség van a nemzetközi jogi keretek továbbfejlesztésére és a nemzetközi együttműködés erősítésére.

A mesterséges intelligencia integrációja a védelmi stratégiákba tehát nem csupán technológiai, hanem etikai, jogi és politikai dimenziókat is magában foglal. A felelős MI alkalmazás biztosítása érdekében a nemzetközi közösségnek együtt kell működnie a technológiai fejlődés és az emberi jogok tiszteletben tartása közötti egyensúly megteremtése érdekében.

Interdiszciplináris Perspektívák

A modern katonai stratégiák és biztonságpolitikai intézkedések megértése egyre inkább igényli az interdiszciplináris megközelítést, amely ötvözi a technológiai, társadalmi, és politikai elemzéseket. A mesterséges intelligencia terjedése és annak integrációja a védelmi rendszerekbe olyan komplex kihívásokat vet fel, amelyek kezelése különböző tudományágak együttműködését igényli. Az MI hatása a biztonságpolitikára nem korlátozódik pusztán a technológiai fejlődésre; széleskörű társadalmi és etikai kérdéseket is felvet, beleértve a munkaerőpiacra, a jogi szabályozásra és a nemzetközi kapcsolatokra gyakorolt hatásokat.[23]

A technológiai fejlődés által indukált társadalmi változások megértése érdekében a biztonságpolitikai elemzéseknek széleskörűen kell vizsgálniuk a társadalomtudományi összefüggéseket. Az MI, mint a kiberhadviselés és hírszerzés eszköze, új kérdéseket vet fel az információs háborúk etikájáról és a kibertér nemzetközi szabályozásáról.

Az interdiszciplináris perspektívák fontosságát jól mutatja, hogy a technológiai innovációk hogyan alakították és alakítják a társadalmi struktúrákat, különösen a biztonságpolitika területén. A mesterséges intelligencia fejlődése például jelentős hatással van a munkaerőpiacra, a magánélet védelmére és az állampolgári jogokra, amelyek mind a társadalmi szerkezet alapvető elemei. Az MI alkalmazása a katonai technológiákban, mint amilyeneket a NATO használ, új kihívásokat és lehetőségeket teremt, amelyek a hagyományos védelmi stratégiákon túlmutatnak. A robotizált harci rendszerek és a hírszerzési technológiák fejlődése, melyek az MI-t integrálják, nem csupán a hadviselés módját változtatják meg, hanem a nemzetek közötti diplomáciai és társadalmi dinamikákat is befolyásolják. [24]

Az interdiszciplináris megközelítések tehát nem csupán a technológiai fejlesztések és azok társadalmi hatásainak megértését segítik, hanem a nemzetközi jogi és etikai keretek megszilárdítását is elősegítik a biztonságpolitika területén. Az MI hatása a biztonságpolitikára és a társadalomra kiterjedő tanulmányozása nélkülözhetetlen a felelős és fenntartható technológiai integráció szempontjából.

ÖSSZEGZÉS

Az informatika vívmányai egyre inkább átszőtték a mindennapjainkat, valamint a katonai rendszereket is. A katonai irányítórendszerek és az intelligens fegyverek hálózatba kapcsolódva fognak hosszú távon működni, ami kétélű fegyver, hiszen ezáltal egy sor biztonsági kockázatnak vannak kitéve. Fel kell készülnünk arra, hogy a jövő konfliktusaiban az ellenséges országok egyre nagyobb hangsúlyt helyeznek majd nem csak a katonai, hanem polgári használatban lévő hálózatok, elektronikus információs rendszerek és kritikus infra-

struktúrák támadásaira. Jelentős hátrányba kerülhetnek azok az országok, amelyek nem fejlesztik ki a védekezésre való a képességeiket, mivel önmagában csak a kibervédelem nem biztos, hogy elegendő lesz egy konfliktus során.

A jelenlegi technológiai korszak jelentős kihívásokkal szembesíti a NATO-t, amelynek kulcsszerepe van a kollektív védelemben és a tagállamok biztonságának fenntartásában. Ahogy a mesterséges intelligencia és egyéb digitális technológiák egyre inkább részévé válnak a katonai stratégiáknak és műveleteknek, úgy a NATO-nak adaptálnia kell a hagyományos védelmi megközelítéseit, hogy kezelni tudja a kibertér által előidézett új fenyegetéseket és kihívásokat. Az MI alkalmazása a hírszerzésben, kibervédelemben és robotizált harci rendszerekben lehetőséget nyújt a NATO-nak, hogy növelje a hatékonyságát és a reakcióképességét. Ugyanakkor ezek a fejlesztések komoly etikai és jogi kérdéseket is felvetnek, különösen az autonóm fegyverrendszerek és a döntéshozatali folyamatok átláthatósága terén.

A technológiai innovációk gyors üteme komoly kihívást jelent a jelenlegi nemzetközi jogi keretek számára. A NATO-nak és tagállamainak folyamatosan értékelniük kell az új technológiák biztonságpolitikai következményeit, és aktívan részt kell venniük a nemzetközi szabályozási folyamatokban. Az MI és más fejlett technológiák katonai alkalmazásának szabályozása alapvető fontosságú a nemzetközi béke és biztonság fenntartása érdekében. A hatékony szabályozási keretek kialakításához elengedhetetlen a nemzetközi együttműködés, különösen az ENSZ és más regionális szervezetek bevonása.

A jövőbeli kutatások irányai közé tartozik az MI technológiák biztonsági alkalmazásainak részletesebb elemzése, a kibervédelem erősítése és az információbiztonság javítása. Emellett szükséges a technológiai fejlesztések társadalmi és etikai hatásainak folyamatos figyelemmel kísérése a felelős használat biztosítása érdekében. A nemzetközi együttműködés erősítése és a globális biztonsági kihívásokra adott közös válaszok kidolgozása kulcsfontosságú cél kell hogy legyen a jövőben. A katonai és civil szektorok közötti együttműködés, valamint az interdiszciplináris kutatások támogatása segíthet a komplex biztonsági problémák hatékonyabb kezelésében.

Összegzésül, a NATO-nak és a nemzetközi közösségnek alkalmazkodnia kell a gyorsan változó technológiai környezethez. A folyamatos innováció és a nemzetközi együttműködés támogatása, valamint a jogi és etikai keretek erősítése elengedhetetlen a jövőbeli biztonsági kihívások kezelésében. A technológiai fejlődés lehetőséget nyújt a védelmi képességek javítására, ugyanakkor szükség van a kritikus infrastruktúrák védelmének és a társadalmi stabilitás megőrzésének biztosítására. A NATO és a tagállamok feladata, hogy a technológiai fejlődést a biztonság és stabilitás növelésére használják, miközben tiszteletben tartják az etikai és jogi normákat.

FELHASZNÁLT IRODALOM

[1] https://www.nato.int/cps/en/natohq/opinions_224836.htm?selectedLocale=en
[2] D. Shree,. A Review on Cryptography, Attacks and Cyber Security. International Journal of Advanced Research in Computer Science, 2017, Vol 8, Issue 5, pp. 239, ISSN: 0976-5697
[3] Z. Martinusz, Felelősség és lehetőség, MHTT XI. évfolyam 1. szám https://www.mhtt.eu/hadtudomany/1999/ht-1999-1-1.html

[4] C. Kollár and B. Z. Vinárné, “Terrorism and the information security of media content with special regard to ISIS, the Balkans and Russia,” *SOCIOECONOMIC CHALLENGES*, vol. 1, no. 1, pp. 13–19, 2017.
[5] C. Kollár, “A mesterséges intelligencia és a kapcsolódó technológiák bemutatása a biztonságtudomány fókuszában,” in *Kiberbiztonság – Cybersecurity 2.*, vol. 2, 2019, pp. 47–61.
[6] M. Barsy: A digitális gazdaságról, In: Pintér István (szerk.) Műhelymunkák: A virtuális tér geopolitikája. 367 p. Budapest: Geopolitikai Tanács Közhasznú Alapítvány, 2016. pp. 131-142. (ISBN:978-963-9816-34-3) http://mek.oszk.hu/16100/16182/16182.pdf
[7] H. J. Wilson, P. Daugherty: Human and machine: Reimagining work in the age of AI., Harvard Business Review Press 2018, https://hbsp.harvard.edu/product/10163-PDF-ENG
[8] L. Kovács: Cyber security policy and strategy in the European Union and NATO. *Land Forces Academy Review*, 2018, Vol. XXIII, No 1(89), 2018, pp. 16-24., DOI: https://doi.org/10.2478/raft-2018-0002
[9] G. Nyári: Kiber koalíció 21 – a NATO legfontosabb éves kibervédelmi hadgyakorlatát rendezték meg Észtországban, E-Gov hírlevél, Közigazgatás és Informatika 2021. https://hirlevel.egov.hu/2021/12/13/kiber-koalicio-21-a-nato-legfontosabb-eves-kibervedelmi-hadgyakorlatat-rendeztek-meg-esztorszagban/
[10] https://www.nato.int/cps/en/natohq/official_texts_208374.htm?selectedLocale=en
[11] D. Ryding, J. Reinsel, J. Gantz: The digitization of the world from edge to core. *Framingham: International Data Corporation*, 2018, 16: pp. 1-28., https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate-data-age-whitepaper.pdf
[12] I. Szabadföldi. "A mesterséges intelligenciával támogatott nyílt információszerzés (OSINT): evolúció és kihívások." *Nemzetbiztonsági Szemle* 10.1 (2022), pp. 30-51., https://folyoirat.ludovika.hu/index.php/nbsz/article/view/5953
[13] https://www.nato.int/cps/en/natohq/official_texts_208374.htm?selectedLocale=en
[14] https://www.nato.int/cps/en/natohq/news_208342.htmkiber
[15] https://www.nato.int/cps/en/natohq/official_texts_221777.htm?selectedLocale=en
[16] I. Szabadföldi. "A mesterséges intelligenciával támogatott nyílt információszerzés (OSINT):–evolúció és kihívások." *Nemzetbiztonsági Szemle* 10.1 (2022), pp. 30-51. https://folyoirat.ludovika.hu/index.php/nbsz/article/view/5953/4997
[17] G. Berki: Kiberháborúk, kiberkonfliktusok, In: Pintér István (szerk.) Műhelymunkák: A virtuális tér geopolitikája. 367 p. Budapest: Geopolitikai Tanács Közhasznú Alapítvány, 2016. pp. 246-282. (ISBN:978-963-9816-34-3) http://mek.oszk.hu/16100/16182/16182.pdf
[18] J. Carroll: OSINT Analysis using Adaptive Resonance Theory for Counterterror-ism Warnings, *Artificial Intelligence and Applications*, Innsbruck, 2005., pp. 756–760.
[19] T. Kőkuti, "Társadalmi hatások és MI!", 2022, pp. 312-324.
[20] A. Németh: "A katonai alkalmazású autonóm terepjáró járművek fejlesztésének egyes kérdései I. rész." *HADITECHNIKA* 53.4 (2019), pp. 11-16.

[21] P. Scharre, *Army of none: Autonomous weapons and the future of war, Future Weapons*. WW Norton & Company, 2018. pp. 34, ISBN-szám:9780393608991, 0393608999

[22] F. Mező, "A mesterséges intelligencia téma megjelenése a „Tanulás és Társadalom" Interdiszciplináris Nemzetközi Konferencián - The Appearance of the Topic of Artificial Intelligence in the" Learning And Society" Interdisciplinary International Conference." *MESTERSÉGES INTELLIGENCIA: INTERDISZCIPLINÁRIS E-FOLYÓIRAT* 4.2 (2022): pp. 89-107., https://real.mtak.hu/155963/1/MI_2022_2_089_Mezo.pdf

[23] K. Mező, Zs. Mándy. "BESZÁMOLÓ A 4. NEMZETKÖZI INTERDISZCIPLINÁRIS KONFERENCIÁRÓL." *Különleges Bánásmód-Interdiszciplináris folyóirat* 5.2 (2019), pp. 71-81.

[24] H. Harlow, Ethical concerns of artificial intelligence, big data and data analytics, *European conference on knowledge management*. Academic Conferences International Limited, 2018. pp. 316. Ethical Concerns of Artificial Intelligence, Big Data and Data Analytics - ProQuest

GAIT RECOGNITION AND THEIR DATABASES

JÁRÁSFELISMERÉS ÉS ADATBÁZISAI

SZÁVAY István[1] – GODA Tibor[2] – ŐSZI Arnold[3]

Abstract

This study examines the benefits, challenges and potential applications of gait and action recognition in the field of asset protection. Gait recognition enables the identification of individuals and early detection of potentially dangerous acts without direct contact. Its application facilitates a faster response of the asset protection system to dangerous situations. In a practical sampling, the use of drones to support gait and action recognition will be investigated and analysed to see how they offer a new opportunity in traditional asset protection. Finally, a comparative analysis of datasets supporting the development of gait recognition algorithms and models will be carried out.

Keywords

gait recognition, drone, action recognition, databases, remote monitoring,

Absztrakt

A tanulmány vizsgálja a járás és cselekvésfelismerés előnyeit, kihívásait és alkalmazási lehetőségét a vagyonvédelem területén. A járásfelismerés lehetővé teszi az egyének azonosítását és a potenciálisan veszélyes cselekmények korai felismerését közvetlen érintkezés nélkül. Alkalmazása elősegíti a vagyonvédelmi rendszer gyorsabb reagálását a veszélyes helyzetekre. Gyakorlati mintavétel során vizsgálatra és elemzésre kerül a drónok alkalmazása a járás és cselekvésfelismerés támogatására, hogy milyen új lehetőséget kínálnak a hagyományos vagyonvédelmi rendszerben. Végül a járásfelismerési algoritmusok és modellek fejlesztését támogató adatbázisok adatkészleteinek összehasonlító elemzése is megvalósul.

Kulcsszavak

járásfelismerés, drón, cselekvés felismerés, adatbázisok, távoli megfigyelés,

[1] szavay.istvan@phd.uni-obuda.hu | ORCID: 0000-0001-7840-8506 | PhD-student, Óbuda University Doctoral School on Safety and Security Sciences | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

[2] goda.tibor@bgk.uni-obuda.hu | ORCID: 0009-0004-5666-3142 | University professor, Óbuda University Bánki Donát Faculty of Mechanical and Safety Engineering, Egyetemi tanár, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

[3] oszi.arnold@bgk.uni-obuda.hu | ORCID: 0000-0001-5988-0143 | Adjunct professor, Óbuda University Bánki Donát Faculty of Mechanical and Safety Engineering, Egyetemi adjunktus, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

BEVEZETÉS

A vagyonvédelemben alkalmazott videó megfigyelési rendszerek segítik a felderítés és megelőzés hatékonyságát. A fejlesztések és innovatív megoldások képesek a belátható tér méretének megnövelésére, a látható kép minőségi részleteinek javítására, az energiatárolás élettartamának növelésére, vagy a telepítési költségek csökkentésére. Minden fejlesztés a korábbi rendszerek korlátozásaira válaszolva alapozza meg a jövő fejlesztési irányait.

A biztonsági rendszerek vonatkozásában egy gyanús tevékenység korai felismerése és ezáltal a megelőző intézkedések megfelelő időben történő végrehajtása a konkrét fenyegetés csökkentését eredményezi. Ezen kívül a személy beazonosításának lehetősége nagymértékben hozzájárul egy esetleges jogellenes cselekmény későbbi bizonyítási eljárásához.

Például a járásfelismerés, mint az emberi testalkat és járásmód alapján történő személyazonosítás lehetővé teszi a gyanús tevékenységek korai felismerését.

A JÁRÁSFELISMERÉS JELENTŐSÉGE

Az emberi járás a testrészek időszakonként szabályosan elvégzett mozgása olyan mozgássorozatként definiálható, amely az alsó végtagok ritmikus mozgása által a test előrehaladását eredményezi. A járást az ember egyik jellemzőjeként ismerjük és elemzése számos tudomány területen ismert (gyógyászat, sport, rehabilitáció, stb). A többféle mozgásforma egyedi testtartásokkal és az alsó végtagok koordinált működésével párosul, ezáltal egyedi mintát kölcsönözve az adott személynek. [1]

Ez a bonyolult folyamat nem csupán a mozgás mechanikai megnyilvánulásait jelenti, hanem összetett interakciók halmazát képezi, így alakítja az emberi mozgást egyedivé és megkülönböztethetővé. A járás elemzésének tudományos jelentősége abban rejlik, hogy képessé válunk azonosítani bizonyos mozgásmintákat, amelyek fontos információkkal szolgálhatnak a mozgást végző személy fizikai állapotáról, mozgásmódjáról [1] és cselekvésének esetleges céljáról (pl. más személy elleni támadás előkészülete, végrehajtása). Ezen ismeret hasznosítása fontos a vagyon és személy elleni káros cselekmények megelőzésében, kiszűrésében.

Az emberi cselekvésfelismerés csoportjába tartozó járáselemzés a lágy biometriai módszerek közé sorolható. Ezek az eljárások szolgálhatnak a hagyományos biometrikus rendszerek teljesítményének javítására. [2] A lágy biometrikus jellemzők közé tartozik a magasság, a testsúly, a testalkat, a különböző hegek, a tetoválások, stb. Az elsődleges biometrikus jellemzőkkel ellentétben a lágy biometrikus adatok elérhetőek anélkül is, hogy a személy közvetlen együttműködése megtörténjen, így ideálisak a felügyeleti alkalmazásokhoz. [3]

A biometrikus jellemzők bár egyediek az adott személyre, mégsem alkalmazhatók hatékonyan bizonyos megfigyelési környezetben. A járásfelismerés alkalmazása minimális előfeldolgozással képes az emberi jellemzők kinyerésére és osztályozására ott, ahol az aktív felhasználói együttműködés kivitelezése zavartalanul egyáltalán nem, vagy csak magas költséggel lenne megvalósítható.

A járásfelismerés különösen nehéz olyan esetekben, amikor a járás jellemzői részben, vagy teljesen kitakart állapotba kerülnek. Ilyen eset lehet, ha a megfigyelő eszköz magas pozíciója és meredeken vetülő látószöge okán az egész emberi testet nem, hanem annak

csak egy részét képes megfigyelni. Egy drón működési magasságából, mozgási dinamikájából adódóan az emberi test egy része saját maga által, illetve a környezeti elemek által rejtve marad, ami nehezíti a járásfelismerő rendszerek számára a pontos észlelést és a járásminták értelmezését. [4]

A biometrikus rendszerek az egyének azonosítását és felismerését azok biológiai jellemzőik alapján végzi, mint például az arc, vagy a hang. A technológiák azonban nem tökéletesek és problémákat jelent számukra, ha például az arc részben takarásban van (pl: szemüveg, maszk). Probléma forrása az is, hogy az emberek tartanak az eszközökkel való közvetlen érintkezéstől, továbbá nagyobb tömegek feltorlódása is bekövetkezhet a biometriai azonosításra alkalmazott eszközök használata során. A járásfelismerés jó alternatívát jelenthet, hiszen a technológia kombinálható más módszerekkel, ezzel javítva az azonosítás megbízhatóságát. [1]

Környezeti tényezők a járásfelismerési rendszerekben

A járásfelismerési algoritmusok hatékony működéséhez és a megfelelő adatminőség biztosításához kulcsfontosságúak a felvételi körülmények, beleértve a szélsőséges fényviszonyokat, az esőt, a köd és a szél hatásait. A napfény, illetve a mesterséges fényforrások változó intenzitású árnyékokat vetnek, ami megnehezítheti a járásminták feldolgozását. A környezeti feltételek okozta problémákra az árnyékszegmentálási módszer, valamint az árnyékok normalizálására szolgáló transzformációs technikák kínálnak megoldást. [3], [5], [6]

A mozgó járművek, más emberek jelenléte, vagy egyes építészeti elemek is akadályozó tényezőt jelenthetnek a járásfelismerés során, különösen légi megfigyelés esetén. Ezen problémák áthidalására a mélytanulási modellek közül a konvolúciós neurális hálózatok kiemelkedően alkalmasak arra, hogy például a légi megfigyelés során keletkezett adatokból kiemeljék a járásfelismerés szempontjából releváns jellegzetességeket, még zavaró tényezők jelenlétében is. A járás időbeli dinamikájának és összetett mintázatainak értelmezéséhez gyakran alkalmaznak rekurrens neurális hálózatokat, amelyek képesek a mozgássorozatok időbeli jellemzőinek pontos modellezésére. Ez különösen fontos az összetett járásmintázatok felismerésénél, ahol a vizuális adatok minősége és a környezeti változások, mint például a fényviszonyok és a háttér változékonysága lényeges szerepet játszanak. [7]

Annak érdekében, hogy egy vagyonvédelmi rendszerben minél pontosabb információkat állítson elő, egy járásfelismerési algoritmus számára a megfelelő adatminőség biztosítása érdekében fontos szempontok közé tartozik a rögzített kép távolsága, a kamera látószöge, a betekintés szöge, valamint a képstabilitás. A rögzített videófelvételeknek elegendő részletességet és minőséget kell biztosítaniuk a hatékony adatelemzéshez. Fontos szempont, hogy az adatgyűjtés során minimalizálva legyenek azon zavaró hatások, amelyek a megfigyelt személyek viselkedésének változását is előidézhetik.

A vizuális adatgyűjtés és a járásfelismerés területén a drón technológia alkalmazása jelentős előnyöket kínál a hagyományos, rögzített pozíciójú kamerarendszerekhez képest, hiszen a mobilitásuk révén képesek különböző szögekből végrehajtani az adatgyűjtést. A drónoknak a változó megfigyelési igényekhez való alkalmazkodása a rugalmasságuk és a nagy terület lefedő képességük révén valósul meg.

Ez a tulajdonság különösen előnyös a nehezen hozzáférhető, vagy változó környezeti feltételek mellett, ahol a földi kamerák telepítése gazdaságtalan, esetleg nehézségbe

ütközik. A drónok nyújtotta mobilitás lehetővé teszi a járásfelismerési algoritmusok számára, hogy hatékonyan kövessék a személyeket, ezáltal növelve a megfigyelési rendszerek reakcióképességét és pontosságát. [2]

A test által elrejtett járásjellemzők

Az árnyékok kulcsfontosságú információkat őriznek meg a járás dinamikus jellemzőiről még olyan esetben is, ha a test részben, vagy teljesen kitakart állapotba kerül. Az árnyékok által szolgáltatott járásjellemzők használata lehetővé teszi az egyének azonosítását nemcsak különböző nézőpontokból és magasságokból, de még abban az esetben is, ha a megfigyelt személy közvetlenül nem látható a drón kameráján keresztül. [3], [5], [8]

A módszer alkalmazása azonban korlátokkal is rendelkezik, hiszen az árnyékok torzulhatnak, a különböző terepekre vetülve eltérő kontúrokkal rendelkezhetnek, valamint kedvezőtlen fényviszonyok mellett akár el is tűnhetnek. A problémák áthidalására két megoldást dolgoztak ki: az egyik az árnyékszegmentálási, a másik a normalizálási módszert. [7]

Az árnyékszegmentálás célja az emberi alak és az árnyék kontúrjainak elválasztása, különös tekintettel a lábak helyzetére. Ez a lépés növeli az emberi alak és mozgás pontos azonosításának lehetőségét.

A normalizálási technika az árnyékokat egyenletessé alakítja át, optimalizálva ezzel a járás textúraképét. Ez a módszer kompenzálja a nézőpontból és az árnyék orientációjából adódó változásokat, korrigálva az árnyékok eltorzulását annak érdekében, hogy a sziluettek a lehető legjobban visszaadják a valóságot. Az előkészített adatokat egy járásfelismerő algoritmus dolgozza fel, amely a szegmentált és normalizált árnyékok alapján azonosítja be az egyéneket. [3], [5]

Drón alkalmazása járásfelismeréshez: adatkészlet összeállítása

Az irodalmi áttekintés kiegészítéseként egy gyakorlati adatkészlet összeállításával került elemzésre a drónokkal támogatott járásfelimerés lehetősége. Ennek során a járás jellemzők egy drón segítségével három eltérő időpontban (egy reggeli, egy déli és egy délutáni napszakban), három különböző magasságból felvett képsorozatként kerültek rögzítésre valós kertvárosi viszonyok között.

A mintavétel célja annak felmérése, hogy a drónok alkalmazása képes, vagy sem hatékonyan támogatni az emberi járás és cselekvés felismerést. Annak ellenére, hogy a vagyonvédelem egyes ágazataiban a drónok alkalmazása még elenyészően ritka, már a technológia keresi a helyét ebben a szegmensben is.

Az adatrögzítés napján az ég komolyabb felhősödéstől zavartalan, a látási és szélviszonyok pedig megfelelőnek mondhatóak, illetve egyéb különleges időjárási körülmény nem befolyásolta az adatok felvételét. Ennek következtében a fennálló környezeti feltételek ideálisnak nevezhetőek. A mintavétel adatai az 1. táblázatban kerültek összesítésre.

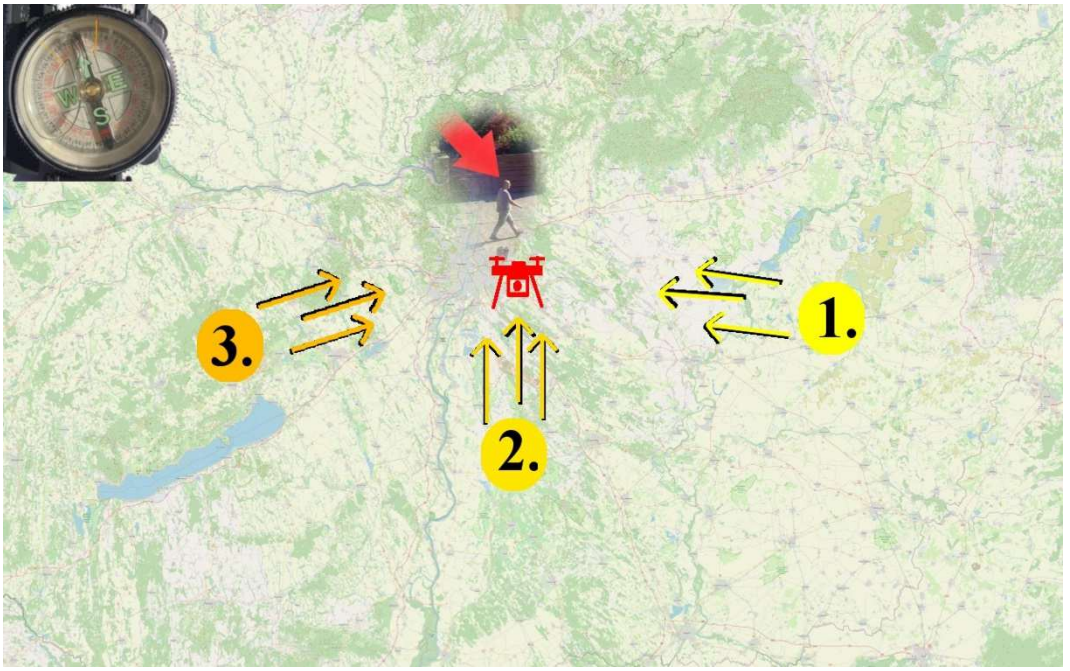
Adatrögzítés	Mintavételek			Magyarázat
	1.	2.	3.	
Időpont	08:30 – 09:00	12:30 - 13:00	16:30 - 17:00	A felvétel készítésének időpontjai
Rögzítési magasság	~3 m és ~5 m és ~8 m			A drón magassága a földtől a felvétel készítésekor
Rögzítési távolság	~ 14 m	~ 15m	~ 16 m	A drón és a személy közötti távolság (rögzítési magasságból adódó változás)
Napsugárzási adatok[4]				
Nap magassága (Altitude)	34,17°	64,18°	37,73°	A nap pozíciója a horizont felett
Azimut szög (Azimuth)	94,50°	174,40°	261,38°	A nap horizontális irányszöge (0-360°)
Árnyékhossz (Shadow length)	2,95 m	0,97 m	2,58 m	Árnyékhossz = Személy magasság (2m) / Nap magasságának tangense
Geo data (Földrajzi adatok)				
Tengerszint feletti magasság	151 méter			A helyszín tengerszint feletti magassága
Szélesség (északi)	É 47°			A helyszín földrajzi szélessége
Hosszúság (keleti)	K 19°			A helyszín földrajzi hosszúsága
Meteorológiai környezet[5]				
Szél iránya és sebessége	ÉNy 15 km/ó	ÉNy 15 km/ó	ÉNy 20 km/ó	A szél iránya és sebessége
Hőmérséklet	18°C	24°C	26°C	A levegő hőmérséklete
Páratartalom	73%	54%	45%	A levegő nedvességtartalma
Légköri nyomás	1014 hPa	1013 hPa	1010 hPa	A levegő nyomása
Látótávolság	>10 km			A horizontális látótávolság
Felhőzet	Felhőtlen 1500 m	Kevés felhő 1341 m	Felhőtlen 1500 m	A felhőzet állapota

1. táblázat: Az adatkészlet elkészítésének környezeti adatai

4 A NOAA Global Monitoring Laboratory, Boulder, Colorado, USA (https://gml.noaa.gov) által szolgáltatott adatok

5 METAR és TAF jelentések - https://hu.allmetsat.com/ - A nyilvánosan elérhető repülésmeteorológiai adatok a Budapest Liszt Ferenc nemzetközi repülőtér állapotát rögzítik.

Az 1. ábra az északi irány meghatározását (egy hagyományos mágneses folyadékos tájoló alapján) és a mintavétel során a nap, a drón és a járási adatokat biztosító személy egymáshoz viszonyított elhelyezkedését ábrázolja. A drón a sétáló személy és a nap között helyezkedett el. A felvételsorozat rögzítésének helyét a térképen a piros drón jelzi, a sétáló helyzetét a piros nyíl mutatja. A nap a mintavételek sorszámával jelöltek, a nap sugarainak irányát szimbolizáló nyilak pedig a mintavétel helyszíne felé mutatnak.



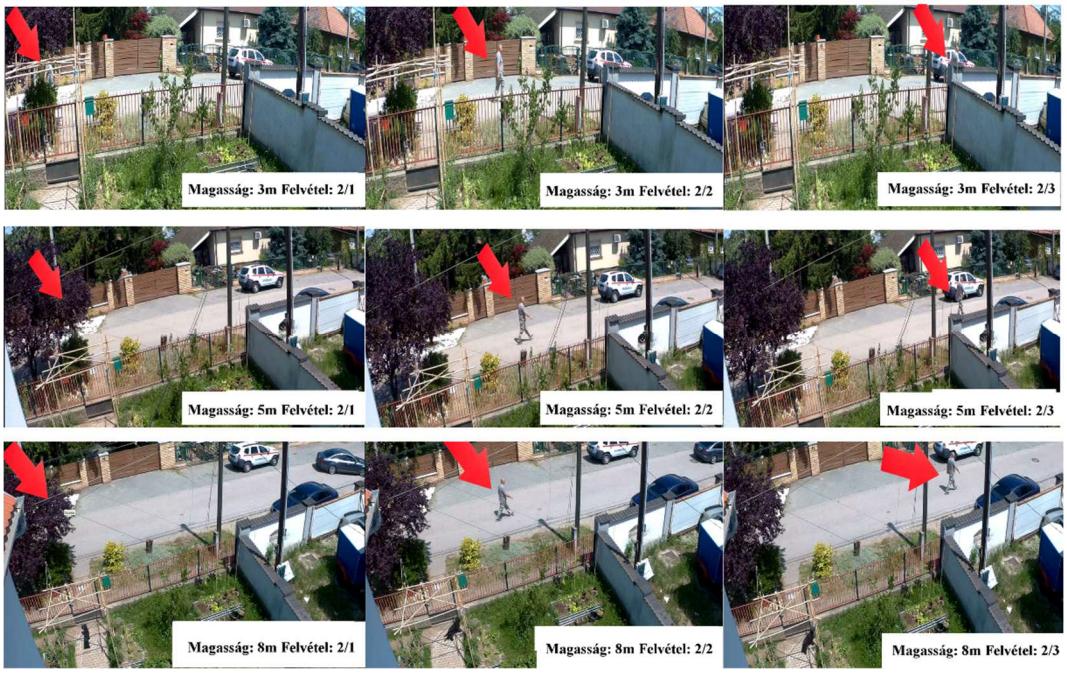
1. ábra: A mintavétel helyzetének bemutatása a felvételek készítésének időpontjaiban.

Drón alkalmazása járásfelismeréshez: elemzés

A 2., 3., 4. ábrán időrendi sorrendben tekinthető meg a mintavétel eredménye. A személy helyzete piros nyíllal, míg a rögzítés időpontjának beazonosításához szükséges rövidített információk fehér háttérrel vannak kiemelve a képsorozatokon. A három különböző magasságból 3 képfelvétel került kimentésre (számozásuk: 1/1, 1/2, 1/3). A képeken is látható, hogy a nem homogén háttér és a valós környezeti hatások akár ilyen kis adatokban is rengeteg torzítást idézhetnek elő.

Ezen zavaró tényezők kiküszöbölése kiemelt fontosságú, hiszen a drón kamerája által érzékelt kép alapján a feldolgozó egység elemzi és értelmezi az összetett emberi cselekményeket. Az emberi testhelyzetek és mozgások részletes elemzésének elvégzése hozzájárul a káros és veszélyes viselkedések normálistól történő megkülönböztetéséhez.

2. ábra: Az 1. mintavétel során rögzített járási minta.



3. ábra. A 2. mintavétel során rögzített járási minta.

4. ábra: A 3. mintavétel során rögzített járási minta.

A három időpontban és magasságban végzett adatgyűjtés során a növényzet takaró hatása, illetve a délutáni napsütés (különösen kis magasságban) torzította leginkább a képet és akadályozta jelentősen a személy felismerhetőségét. A legjobb beazonosítást a kevés tereptárgy jelenléte biztosította. A legalacsonyabb magasság a legrosszabb, míg a legmagasabb pont a legjobb és a leginkább zavarmentes rálátást nyújtotta. Az eredmények összefoglalása a 2. táblázatban található.

	Magasság [m]		
	3	**5**	**8**
Láthatóság	A személy részben, vagy teljesen takarásban van.	A személy nagyrészt teljesen látható, a járás megfigyelhető, de a részletesség csökken.	A személy jól látható, de kisebb és kevésbé részletes.
Járásfelismerés	A járás dinamikája a legkevésbé figyelhető meg.	A kép közepén a legj□bb a részletesség, amely csökken a táv□1□dásával.	A járási jellemzők megfigyelhetők, de a részletek kevésbé láthatók.
Növényzet hatása	Függetlenül a magasságtól a növényzet takaró hatása akadály□zza a személy felismerését.		

	Magasság [m]		
	3	**5**	**8**
Napsütés hatása	A délutáni napsütés a mintavétel alkalmával, főleg kis magasságban torzította a képet, teljesen elnyomva a személy felismerhetőségét.		
Tereptárgyak hatása	A legrosszabb felismerhetőség a tereptárgyak miatt.	A legjobb felismerhetőség, ha kevés a tereptárgy.	A legjobb rálátást biztosította, és a leginkább zavarmentesek a vetett árnyékok.
Összefoglalás	A legalacsonyabb magasság biztosítja a legrosszabb felismerhetőséget.	A közepes magasság némi kompromisszumot kínál a részletesség és a láthatóság között.	A legmagasabb pont biztosította a legjobb rálátást és a leginkább zavarmentes vetett árnyékokat.

2. táblázat: A mintavétel eredménye

A JÁRÁSFELISMERÉS ADATBÁZISAI

Az emberi járás és cselekvés felismerés kutatásához segítséget nyújtanak a különböző egyedi járásmintákat tároló adatbázisok [9]. Ezek az adatkészletek személyek járásmintájáról készített videókat és képsorozatokat tartalmaznak azokat több nézőpontból rögzítve, ahol a személyek eltérő öltözékben, illetve egyéb ruházati kiegészítőket viselnek.

Az OU-ISIR és OU-MVLP adatbázisok

Az Osaka Egyetem (OU) Tudományos és Ipari Kutatási Intézete (ISIR) által kezelt adatbázis hozzáférése korlátozott, az csak igénylés és megfelelő indoklást követően kiadott engedély birtokában lehetséges. A nagyméretű adatbázisban különböző életkorú és eltérő társadalmi, gazdasági és kulturális háttérrel rendelkező személyekről készített járási minták kutathatóak. Vannak közöttük futópadon végzett gyaloglások, különböző nézetekből rögzített és a valós életben használt tárgyakat hordozó személyek adatmintái is. Ezek az adatok további részleteket biztosítanak és egyedi perspektívákat kínálnak a mozgáselemzéshez. [12]

Eltérően mástól az OU-ISIR adatkészleteket ellenőrzött körülmények között hozták létre és a videofelvételek sok esetben részletes adatokat is tartalmaznak. Az Osaka Egyetem (OU) Többnézetes Nagy Populációs Adatkészletben (MVLP) több mint 10 000 egyedi alanyt magában foglaló és 14 különböző szögből rögzített járásminta található. [11] Ez az adatbázis a többnézetes járásfelismerés kutatását támogatja, valamint az OU-ISIR MVLP rövidítéssel is hivatkoznak rá.

Gait3D

Az adatbázishoz való hozzáférés előzetes regisztráció és szerződéskötést követően lehetséges. Míg a legtöbb járásfelismerési kutatás a kétdimenziós képek, mint például az emberi alak vázának felhasználására koncentrál, addig a háromdimenziós járási adatokkal rendelkező adatbázis, a Gait3D mintái a mozgás irányának, vagy a test formájának adatait is tartalmazza.

A Gait3D több ezer ember mozgását tárolja, sőt a képek és videók mellett a mozgásokhoz kapcsolódó háromdimenziós modellek is megtalálhatóak. Ezek részletes információt nyújtanak a test mozgásáról. Az adatbázisban több mint 4000 résztvevő járása került dokumentálásra közel 25000 különböző felvétellel, amit 39 kamera rögzített akadálymentes beltérben. Az adatgyűjtemény különlegességét adják azok a háromdimenziós modellek, amelyeket a valós mozgásokból digitálizáltak annak érdekében, hogy pontosan láthatóvá tegyék a térbeli emberi mozgást minden irányból. A háromdimenziós modellek használata lehetővé teszi a mozgás minden egyes részletének, így például a testhelyzet változásának, a végtagok mozgásának, vagy akár a járás stílusának pontos elemzését. [12], [13]

GREW

A Gait Recognition in the Wild (GREW) adatkészlet egy viszonylag új nyílt forrású gyűjtemény a valós körülmények közötti járásfelismerés területén. Kiemelkedő tulajdonsága, hogy a járás mintákat nem mesterséges, hanem annak természetes környezetében rögzítették. Az adatbázisban megtalálható több ezer egyén járásadatait különböző időjárási és fényviszonyok mellett, városi környezetekben gyűjtötték. Az adatokhoz többek között a járás típusai, valamint a kamera nézőpont és távolság adatai is hozzá tartoznak. [14], [15]

A CASIA adatkészlet

A The Institute of Automation, Chinese Academy of Sciences (CASIA) egy több részből álló nagyméretű adatbázis, melyet a Kínai Tudományos Akadémia Automatizálási Intézetének Biometriai és Biztonsági Kutatási Központja (CBSR) hozott létre. Az adatokhoz való hozzáférés korlátozott, egy kérelem benyújtását követően annak jóváhagyása szükséges.

A CASIA adatkészlet kiemelkedő jellemzője a sokféleség, hiszen az egyes részek a járás különböző szempontjait fedik le.

- Az "A" rész volt az első, amely különböző irányokból felvett személyek mozgási képsorozatát tartalmazza.
- A "B" rész adatkészletében három fő járástípust rögzítettek több nézetből: a normál, a kabátban és a táskával végzett járás állapotokat. A mintafájlok mellett megtalálhatóak a videófájlokból kinyert emberi sziluetteket adatai, valamint a látószög, a ruházat és a szállítási állapot változásainak adatai is.
- A "C" rész adatgyűjtése éjszakai körülmények között négy különböző járási módra összpontosít: gyaloglás, lassabb és gyorsabb tempójú járásra, valamint a hátizsákkal történő sétára.
- A "D" adatkészlet széles életkori sávban a járás biometriai és lábnyomadatainak összefüggéseit vizsgálja. [16], [17], [18]

A CASIA adatbázis legfrissebb tagja az „E”, amely méreteiben jóval meghaladja elődeit. Az adathalmaz több mint ezer személy járásmódját tartalmazza közel egymillió videófelvételen. Az adatokat közel 5 hónapon keresztül gyűjtötték három kültéri helyszínen. Az első helyszín egy egyszerű statikus, a második és harmadik már bonyolultabb, dinamikus hátterű és változó megvilágítású környezetben készültek, míg a harmadik a hőkamerával készült adatokat tartalmazza. Az adathalmaz különlegessége a járásmódok széles skálájának felvonultatása mellett a különböző járási stílusok, a változatos ruházatban rögzített

minták, a járási módok táskaviselettel. Ezen túlmenően megadja a résztvevők lágy biometrikus jellemzőit is, mint például az életkort, a nemet, a magasságot, a testsúlyt és a nemzetiséget. [19], [20]

SUSTech1K

Az adatbázis létrehozója a Hongkongi Műszaki Egyetem. Az adatbázishoz engedélyezés és szerződés aláírását követően lehetséges a hozzáférés. [21] A LiDAR-alapú járásfelismerő adatkészlet kifejezetten a 3D járási jellemzők pontos meghatározására összpontosít LiDAR szenzorok és RGB kamerák segítségével létrehozott mintáival. A járás 3D szerkezeti információinak tárháza és több mint 25 ezer egyedi járásmintát gyűjtött össze. Az alanyok által végrehajtott teljes járási ciklusok különféle körülmények között kerültek rögzítésre, így számos változatot fednek le a járásmintákban, úgymint eltérő nézőpontok, test kitakarások, változatos ruházati stílusok és hordozott tárgyak. [21], [22]

OpenGait eszköztár

Az OpenGait egy nyílt forráskódú keretrendszer, amely a járásfelismerés és az emberi mozgás elemzésének területén zajló kutatások és fejlesztések támogatására jött létre.

Fontosnak tartom kiemelni, hogy az OpenGait nem egy adatgyűjtemény, hanem az ismert járásfelismerési adatkészletek széles halmazával kompatibilis fejlesztési eszköztár. A platform lehetővé teszi a saját modellek kidolgozását és tesztelését, valamint azok összehasonlítását más modellekkel. Az OpenGait támogatja a különböző adathalmazokat, beleértve a CASIA-B, CASIA-E, OU-MVLP, GREW, SUSTech1K és Gait3D-t is. [23], [24]

A személyre szabható és bővíthető moduláris rendszer alapvető felépítése két fő komponensre bontható:

- a Modell Zoo-ra, amelynek betanítása a keretrendszer által támogatott és ismert nagyméretű adatkészletek adatkészleteken történt. Egyik kulcsfontosságú eleme kifejezetten a csontváz alapú mozgáselemzésre összpontosít.
- A másik a keretrendszer magja, ami a modellfejlesztés és integráció eszközeit biztosítja. [24]

A CSELEKVÉSFELISMERÉS ADATBÁZISAI

A testtartás, testhelyzet becslés a számítógépes látás által feldolgozható feladat, amelynek célja egy személy, vagy tárgy helyzetének megállapítása. Általában ez bizonyos kulcspontok, például kezek, fej, könyök stb. térbeli elhelyezkedésének azonosításán keresztül történik.

HMDB51

A CC BY 4.0 [25] Human Motion Database 51, röviden HMDB51 adatbázist kifejezetten az emberi mozgások tanulmányozására hozták létre. Az adatbázis összeállítását az amerikai Brown Egyetem kutatócsoportjának kutatói végezték 51 különböző cselekvéstípus azonosításával és összegyűjtésével. Ezek között megtalálhatóak mindennapi tevékenységek, a sport, vagy például a kézfogás, ölelés. Az adatbázis létrehozásának elsődleges célja, hogy támogassa a számítógépes látás területén dolgozó kutatókat és fejlesztőket az emberi cselekvések felismerésében. A minta adatok adatbázisa ingyenesen letölthető. [26]

Az adatbázisban szereplő több mint 6000 videó változatos; filmekből, televíziós műsorokból és nyilvánosan elérhető videómegosztó oldalakról származnak. A HMDB51 adatbázis különlegessége, hogy nem csupán általános mozgásmintákat tartalmaz, hanem olyan specifikus és összetett dinamikus cselekvéseket is, mint például az ütés, rúgás, ugrás, vagy akár az esés. Ezen minták segítségével a biztonsági rendszerekben alkalmazható algoritmusok fejleszthetők, amelyek képesek felismerni és megkülönböztetni az emberi mozgások széles skáláját. [26], [27]

Video Dataset of Atomic Visual Action

A szintén CC BY 4.0 [25] licensszel ingyenesen hozzáférhető AVA, azaz Atomic Visual Actions adatbázis a Google által kifejlesztett videó adatbázis, mely az emberi cselekvések szerint szelektálja adatkészletét, vagyis minden egyes tevékenységet külön-külön azonosítanak és címkéznek, figyelembe véve az emberi interakciók és mozgások részleteit. [28]

A videóanyagok a mindennapi élet számos területét fedik le, úgymint a sporttevékenységek, munkahelyi események, az otthoni teendők, de mindezen túlmenően tartalmaz agresszív és veszélyes helyzeteket ábrázoló felvételeket is, mint például különböző személy elleni támadásokat. Az adatbázisban található jelenetek változatos környezetekből kerültek kiemelésre általában a közösségi videó portálokon, mint a YouTube megtalálható videótartalmak kivágott jeleneteiből. Fontosnak tartom megjegyezni, hogy az adatbázis mutató hivatkozások rendszerezett adatkészlete és sajnos az egyes hivatkozott videóállományok esetenként már nem létező tartalmakra mutatnak.

NTU CCTV-Fights Dataset

A jelen tanulmányban szereplő kutatás a szingapúri Nanyang Technológiai Egyetem ROSE Lab által rendelkezésre bocsátott NTU CCTV-Fights adatbázist használta. Az adatkészlet a hagyományos kamerák és mobil eszközök valós idejű egyéni, vagy tömeges támadási események rögzített felvételeinek gyűjteménye. Az adatkészlet mintegy 1000 videót tartalmaz összesen több mint 8 órányi felvételben. Az adatbázis készletét szintén a közösségi médiából (YouTube) specifikus kulcsszavak, mint például "CCTV Fight" és "Violence" segítségével gyűjtötték össze és csak azok a videók kerültek az adatbázisba, amelyek nem tartalmaznak vizuális manipulációkat. Az adatkészlet két fő része a CCTV videó anyag és a többnyire mobil eszközök kameráinak felvételei. [29], [30]

Az adatkészlet használata az oktatási, vagy kutatóintézetek kutatói számára ingyenes, de regisztrációhoz és engedélyhez kötött.

AlphaPose rendszer

Az AlphaPose egy nyílt forráskódú és a nem kereskedelmi használatra ingyenes valós idejű többszemélyes testtartás becslő és személykövető rendszer. A Shanghai Jiao Tong Egyetem, Gépi látás és intelligencia csoport (MVIG) által létrehozott rendszer lehetővé teszi az emberi test, arc, kéz és láb mozgásának valós idejű követését. Ebben a rendszerben egy lokalizációs módszer teszi lehetővé az emberi kulcspontok gyors és pontos meghatározását elkerülve a duplikált érzékeléseket. [31]

Az AlphaPose modell képes a különböző emberek testtartását ábrázoló adatbázisokon tanulni, amelyek eltérő helyzeteket, testalkatokat és mozgásmintákat tartalmazhatnak.

A rendszer a testtartás becslés és az egyedi azonosítás egyidejű végrehajtását teszi lehetővé, ami fontos a biztonságtechnikai rendszerekben.

Az 3. táblázat áttekintést nyújt a jelen tanulmányban tárgyalt adatbázisokról összegezve azok megkülönböztető jellemzőit és elérhetőségét.

Adatbázis	**Adatkészlet**	**Hozzáférés**	**Különlegesség**
OU-ISIR	Futópad gyaloglás, Többnézetes járásminták	Korlátozott	Ellenőrzött körülmények, részletes biomechanikai adatok
OU-MVLP	Nagy populáció széleskörű demográfiai jellemzők;	Korlátozott	Egyedi azonosítókkal rendelkező nagy populációs adatkészlet
Gait3D	Beltéri 3D járásminták; a mozgás iránya, a test formája	Korlátozott	3D modellek; térbeli emberi mozgás nézet minden irányból.
GREW	A járás természetes környezetében rögzített adatok; városi környezetek	Nyílt	Valós körülmények, fényviszonyok, városi környezet; a járás típusai, kamera nézőpont és távolság adatok
CASIA-B	Különböző irányokból felvett képsorozatok, több nézetből rögzített minták	Korlátozott	Különböző járástípusok és nézetek, ruházat, táskaviselés
CASIA-E	Hatalmas adatmennyiség, közel egymillió videó, hőkamerával készült adatok	Korlátozott	Nagy méretű, változatos kültéri helyszínek Nézetek, ruházat, táskaviselés, lágy biometrikus jellemzők
SUSTech1K	LiDAR-alapú, 3D adatok	Korlátozott	járásminták: eltérő nézőpont, test kitakarások, változatos ruházat, hordozott tárgyak

Adatbázis	Adatkészlet	Hozzáférés	Különlegesség
OpenGait	Nem adatgyűjtemény, hanem járásfelismerési eszköztár Járásfelismerési modellek fejlesztése és tesztelése	Nyílt	Kompatibilis több ismert adatkészlettel, moduláris rendszer
HMDB51	Emberi mozgások, mint ütés, rúgás, ugrás, esés	Nyílt	Több mint 6000 videó; filmekből, TV műsorokból és videómegosztókról
AVA	Mindennapi tevékenységek és agresszív cselekvések	Nyílt	Részletesen címkézett, az emberi interakciókat és mozgásokat figyeli
NTU CCTV-Fights	Valós idejű egyéni és tömeges támadási események	Korlátozott	1000 videó, specifikus kulcsszavakkal gyűjtve, valós támadások
AlphaPose	Valós idejű többszemélyes testtartás becslés	Nyílt	Emberi test, arc, kéz és láb mozgásának követése; nyílt forráskódú

3. táblázat: Az adatkészletek összehasonlítása

ÖSSZEGZÉS

A járás és cselekvésfelismerés fontos eszköze lehet a jövő biztonsági felügyeleti rendszereinek, hiszen képes az egyének azonosítására azok közvetlen érintkezése nélkül. Egy nagy, de gyakran még kisebb létszámú embertömeg esetén is szükséges azon cselekedet korai felismerése, amely veszélyes a biztonságra. A drónok egyre növekvő felhasználási köre tovább bővíthető az adott területen tartózkodó erőszakos személyek, cselekmények kiszűrésével a járás, vagy cselekvés felismerés segítségével. Egy személy testhelyzetének vizsgálatával, a várható cselekmények becslésével csökken a reakció idő, amely segíti az eseményre reagálás eredményeségét.

A kutatást és fejlesztést támogató adatbázisok és keretrendszerek megfelelő teret és segítséget biztosítanak ahhoz, hogy a felismerés pontosságának javulásával az egyes rendszerek fejlődése töretlen maradjon. A járás és cselekvésfelismerési adatbázisok változatos adatkészletek sorát biztosítják, hogy a kutatók az elemzések elvégzéséhez, valamint az algoritmusok fejlesztéséhez elegendő mintához férjenek hozzá. Az integrált keretrendszerek fontos szerepet töltenek be a kutatásokban, hiszen az adatbázisokkal való kompatibilitásuk révén testreszabott megoldások előállítását segítik elő.

A drónok alkalmazása a járásfelismerésben vegyes eredményeket mutat, de a valós körülmények között elvégzett vizsgálat megerősítette, hogy mobilitásuk hatékony kiegészítést jelent a hagyományosan telepített kamerarendszerek mellett. A mintavétel során megállapításra került, hogy a drónokkal támogatott járásfelismerés akkor válhat hatékonnyá például a vagyonvédelem területén, ha a drón képes a személy minél pontosabb felismerése érdekében a saját helyzetén változtatni.

Az állandó, vagy változó akadályok közötti útvonaltervezés és az adott területen belül (legyen az zárt, vagy szabadtér) a pozíció módosításával megvalósított másik nézőpont kiválasztásának eredménye az alkalmasabb nézőpontból történő megfigyelés, továbbá a személy követése. Az ezt segítő útvonalkeresési lehetőségek a következő publikációban kerülnek vizsgálatra.

FELHASZNÁLT IRODALOM

[1] D. Sethi, S. Bharti, és C. Prakash, „A comprehensive survey on gait analysis: History, parameters, approaches, pose estimation, and future work”, *Artificial Intelligence in Medicine*, köt. 129, o. 102314, júl. 2022, doi: 10.1016/j.artmed.2022.102314.

[2] S. Kapoor, A. Sharma, A. Verma, és S. Singh, „Aeriform in-action: A novel dataset for human action recognition in aerial videos”, *Pattern Recognition*, köt. 140, o. 109505, aug. 2023, doi: 10.1016/j.patcog.2023.109505.

[3] T. T. Verlekar, P. L. Correia, és L. D. Soares, „Gait recognition using normalized shadows”, in *2017 25th European Signal Processing Conference (EUSIPCO)*, 2017, o. 936–940. doi: 10.23919/EUSIPCO.2017.8081345.

[4] C. B. Nalty *és mtsai.*, „A Brief Survey on Person Recognition at a Distance”, in *2022 56th Asilomar Conference on Signals, Systems, and Computers*, 2022, o. 145–152. doi: 10.1109/IEEECONF56349.2022.10051819.

[5] T. T. Verlekar, L. D. Soares, és P. L. Correia, „Gait recognition in the wild using shadow silhouettes”, *Image and Vision Computing*, köt. 76, o. 1–13, aug. 2018, doi: 10.1016/j.imavis.2018.05.002.

[6] A. Li, S. Hou, Q. Cai, Y. Fu, és Y. Huang, „Gait Recognition With Drones: A Benchmark”, *IEEE Transactions on Multimedia*, köt. 26, o. 3530–3540, 2024, doi: 10.1109/TMM.2023.3312931.

[7] J. P. T. Sien, K. H. Lim, és P.-I. Au, „Deep Learning in Gait Recognition for Drone Surveillance System”, *IOP Conf. Ser.: Mater. Sci. Eng.*, köt. 495, sz. 1, o. 012031, 2019, doi: 10.1088/1757-899X/495/1/012031.

[8] Y. Iwashita, R. Kurazume, és A. Stoica, „Gait Identification Using Invisible Shadows: Robustness to Appearance Changes”, in *2014 Fifth International Conference on Emerging Security Technologies*, szept. 2014, o. 34–39. doi: 10.1109/EST.2014.18.

[9] „Datasets - Machine Learning Datasets”. Elérés: 2024. május 25. [Online]. Elérhető: https://datasets.activeloop.ai/docs/ml/datasets/

[10] „Gait Recognition in the Wild with Dense 3D Representations and A Benchmark”. Elérés: 2024. április 7. [Online]. Elérhető: https://gait3d.github.io/

[11] „OU-ISIR Biometric Database”. Elérés: 2024. április 8. [Online]. Elérhető: http://www.am.sanken.osaka-u.ac.jp/BiometricDB/index.html

[12] „Gait Recognition in the Wild with Dense 3D Representations and A Benchmark”. Elérés: 2024. április 8. [Online]. Elérhető: https://gait3d.github.io/

[13] J. Zheng, X. Liu, W. Liu, L. He, C. Yan, és T. Mei, „Gait Recognition in the Wild with Dense 3D Representations and A Benchmark”, in *2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, jún. 2022, o. 20196–20205. doi: 10.1109/CVPR52688.2022.01959.

[14] „GREW”. Elérés: 2024. április 7. [Online]. Elérhető: https://www.grew-benchmark.org/

[15] „Gait Recognition in the Wild: A Benchmark”, in *2021 IEEE/CVF International Conference on Computer Vision (ICCV)*, 2021, o. 14769–14779. doi: 10.1109/ICCV48922.2021.01452.
[16] „Papers with Code - CASIA-B Dataset”. Elérés: 2024. április 7. [Online]. Elérhető: https://paperswithcode.com/dataset/casia-b
[17] „Center for Biometrics and Security Research”. Elérés: 2024. április 8. [Online]. Elérhető: http://www.cbsr.ia.ac.cn/english/Gait%20Databases.asp
[18] „Gait Dataset”. Elérés: 2024. április 8. [Online]. Elérhető: http://www.cbsr.ia.ac.cn/users/szheng/?page_id=71
[19] C. Song, Y. Huang, W. Wang, és L. Wang, „CASIA-E: A Large Comprehensive Dataset for Gait Recognition”, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, köt. 45, sz. 3, o. 2801–2815, márc. 2023, doi: 10.1109/TPAMI.2022.3183288.
[20] „CASIA-E: Nagy, átfogó adatkészlet a járásfelismeréshez”. Elérés: 2024. április 9. [Online]. Elérhető: https://www.scidb.cn/en/detail?dataSetId=57be0e918db743279baf44a38d013a06
[21] „LidarGait: Benchmarking 3D Gait Recognition with Point Clouds”. Elérés: 2024. április 10. [Online]. Elérhető: https://lidargait.github.io/
[22] C. Shen, F. Chao, W. Wu, R. Wang, G. Q. Huang, és S. Yu, „LidarGait: Benchmarking 3D Gait Recognition with Point Clouds”, in *2023 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, jún. 2023, o. 1054–1063. doi: 10.1109/CVPR52729.2023.00108.
[23] C. Fan, J. Liang, C. Shen, S. Hou, Y. Huang, és S. Yu, „OpenGait: Revisiting Gait Recognition Toward Better Practicality”, in *2023 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, jún. 2023, o. 9707–9716. doi: 10.1109/CVPR52729.2023.00936.
[24] „GitHub – ShiqiYu/OpenGait: Rugalmas és bővíthető keret a járásfelismeréshez. Az OpenGait segítségével könnyedén saját modelljeit tervezheti, és könnyedén összehasonlíthatja a legmodernebb technikákkal.” Elérés: 2024. március 27. [Online]. Elérhető: https://github.com/ShiqiYu/OpenGait
[25] „CC BY 4.0 Deed | Attribution 4.0 International | Creative Commons”. Elérés: 2024. május 10. [Online]. Elérhető: https://creativecommons.org/licenses/by/4.0/
[26] H. Kuehne, H. Jhuang, E. Garrote, T. Poggio, és T. Serre, „HMDB: A large video database for human motion recognition”, in *2011 International Conference on Computer Vision*, 2011, o. 2556–2563. doi: 10.1109/ICCV.2011.6126543.
[27] „Serre Lab » HMDB: a large human motion database”. Elérés: 2024. május 9. [Online]. Elérhető: https://serre-lab.clps.brown.edu/resource/hmdb-a-large-human-motion-database/
[28] C. Gu *és mtsai.*, „AVA: A Video Dataset of Spatio-Temporally Localized Atomic Visual Actions”, in *2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition*, jún. 2018, o. 6047–6056. doi: 10.1109/CVPR.2018.00633.
[29] M. Perez, A. C. Kot, és A. Rocha, „Detection of Real-world Fights in Surveillance Videos”, in *ICASSP 2019 - 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, 2019, o. 2662–2666. doi: 10.1109/ICASSP.2019.8683676.

[30] „ROSE Lab”. Elérés: 2024. május 10. [Online]. Elérhető: https://rose1.ntu.edu.sg/dataset/cctvFights/
[31] „AlphaPose: Whole-Body Regional Multi-Person Pose Estimation and Tracking in Real-Time | IEEE Journals & Magazine | IEEE Xplore”. Elérés: 2024. május 9. [Online]. Elérhető: https://ieeexplore.ieee.org/document/9954214

THE EFFECT OF WIND TURBINES ON RADARS

SZÉLERŐMŰVEK HATÁSA A RADAROKRA

BRAUN András[1]

Abstract

In Hungary, military facilities equipped with three-dimensional radar can be found in three settlements in different parts of the country. Bánkút, Medina and Békéscsaba. These radars can detect air targets at different angles, altitudes and distances. In my research, I investigate the expected effect of the wind farm to be built near Medina on the radiated microwave signals. I describe the anomalies and system-level degradation of radar, both with the help of pictures and diagrams, and I also write about electromagnetic wave propagation and jamming. I carry out experimental measurements and calculations, then I compare the obtained data in case of real radars and wind farms that can be installed in their vicinity. After the results obtained, I analyse the data and make a proposal for the elimination, mitigation and solution of problems in the future.

Keywords

Wind farm, RAT-31DL radar, Military Technology

Absztrakt

Magyarországon három településén, az ország különböző pontjain, található háromdimenziós radarral felszerelt katonai létesítmény. Bánkút, Medina és Békéscsaba. Ezen radarok különböző oldalszögeken, különböző magasságokon és távolságokon képesek a légi célokat felderíteni. Kutatómunkám során Medina település közelében épülő szélerőműpark várható hatását vizsgálom a kisugárzott mikrohullámú jelekre. Ismertetem a radar leképezési anomáliáit, rendszerszintű degradációit, képek és ábrák segítségével egyaránt, illetve írok az elektromágneses hullámterjedésről és a zavarásról is. Kísérleti méréseket, számításokat végzek, majd összehasonlítom a kapott adatokat a valós radarok és azok környékén telepíthető szélerőműparkok esetén. A kapott eredmények után elemzem az adatokat és javaslatot teszek a problémák jövőbeni kiküszöbölésére, enyhítésére, megoldására.

Kulcsszavak

Szélerőmű, RAT-31DL radar, Haditechnika

1 braun.andras92@gmail.com| ORCID: 0009-0008-3958-5751| Military and Safety Technology Engineer, Radar Engineer, Certified Security Engineer, HBBB INVEST Kft.| Had- és biztonságtechnikai mérnök, Radar mérnök, Okleveles biztonságtechnikai mérnök, HBBB INVEST Kft.

BEVEZETÉS

A szélerőművek hatásának vizsgálata a radarokra ismertetése és vázolása után, különböző mérések, számítások és megállapítások fogják alátámasztani az általam leírtakat, konkrétan a RAT-31DL három dimenziós radarok segítségével. Ilyen például a medinai radar, ahol egy a közeli Németkér falu melletti területen építendő 16 darab szélerőművel, szélerőműparkkal vetem össze, melyet vizsgálok nulla és egy darab szélerőmű esetén is. A témához szükséges szakirodalmak gyűjtésekor a Nemzeti Közszolgálati Egyetem könyvtárában, de nagy részben az interneten és a különböző konferenciák előadásaiból végeztem kutatómunkát. Munkám elkészítéséhez főképp online elérhető folyóiratokat, cikkeket, konferencián meghallgatott előadásokat használtam fel. Rendelkezésemre álltak még a munkám során talált, idegen nyelvről fordított, kapott céges dokumentumok, gyakorlati mérések, illetve az eddig szerzett tapasztalataim. Ebben a témában még nem jelent meg ezzel a területtel foglalkozó felhasználható magyar nyelvű tanulmány , a meglévő 1-2 általánosíthatón kívül, s ezért is igazán érdekes ennek a témának az összefoglaló feldolgozása. Az általam szemléltetett és vizsgált problémák, valamint összefüggések csak egy kis részei ennek a hatalmas témakörnek, mellyel manapság is, de hamarosan a jövőben is rengetegen fognak foglalkozni.

A RADAROK MŰKÖDÉSE ÉS ALKALMAZÁSA

A radar, mint rádiófelderítő és meghatározó eszköz, a II. Világháború óta ismert. A radar a célpontot rádióhullámok segítségével deríti fel és a tárgyak térbeli helyzetét térképszerűen ábrázolja.[1] A rádióhullámok füstön, felhőn, ködön, még falakon is átterjednek, a fény számára áthatolhatatlan tárgyon is kitűnően látnak.[2] Az antenna rádióhullámokat sugároz ki, majd várja a kibocsájtott jel visszaverődő hullámait. Egyszerre több jelet is kisugároz, hogy rövid idő alatt minél több irányba derítsen, s eközben az antenna folyamatosan forog, forgó mozgást végez. A radarok kibocsájtott impulzusait úgy kell időzíteni, hogy legyen ideje a már elküldött jel visszaérkezésének is, mielőtt még a következő impulzust elküldené az antenna.[3] A visszavert jelből megmérhető egy célpont távolsága, különböző radaroknál a magassága is.

A rádiólokátorok osztályozási módok:

- Üzem szerint: folytonos vagy impulzusüzemű.
- Használatos hullámhossz szerint: méteres, deciméteres, milliméteres hullámhosszú.
- Elsődleges feladat szerint: követés, keresés.
- Telepítés helye szerint: hajó, földi, repülőgép stb.

Az aktív radarok alapvető eleme az antenna és a tápvonalrendszer, az indikátor, az adó-vevő, az antennavezérlő rendszer, valamint az áramforrás. A passzív üzemű radaroknak nincs adóberendezése. A folyamatos üzemű radarok a kiválasztott céltárgy radiális sebességének meghatározása a Doppler-effektus felhasználásával alkalmasak. A Doppler-effektus a hullám frekvenciájában és ezzel együtt a hullámhosszban megjelenő változás, mely amiatt alakul ki, hogy a hullámforrás és a megfigyelő egymáshoz képest mozog. Az antenna által a légtérbe kisugárzott nagyfrekvenciás energia, melyet az adó állított elő $3x10^8$ m/s

sebességgel terjed. Majd egy célpontról, céltárgyról visszaverődött jelet a vevőantenna felfogja, a vevő erősíti, majd az indikátor képernyőre juttatja, ahol látható információvá alakul át.

A rádiólokáció alkalmazása polgári életben:

- Iparban: kutatás és hiba helymeghatározás, megfigyelés.
- Meteorológiában: koordináták meghatározása, szélsebesség mérése és az időjárás előrejelzése, felhők vándorlásának megfigyelése.
- Közlekedésben: földi, vízi és légi járművek felkutatása, irányítása, sebesség és egyéb koordináták megállapítása, balesetek esetleges megelőzése.
- Mezőgazdaságban: terménybecslés.

A rádiólokáció alkalmazása a hadseregben:

- Felismerés és zavarás.
- Célfelderítés, célkövetés, célpont meghatározás és tűzvezetés, célelfogás.
- Repülőgépek fel- és leszállásának irányítása, cél koordinátáinak meghatározása és az ellenséges célra való rávezetés.
- Parancsjeles távvezérlés, mélységmérés és kikötőbe bevezetés, rakéták és torpedók irányítása.

RAT-31-DL HÁROMDIMENZIÓS RADAR

A RAT-31 DL[2] egy nagy hatótávolságú háromdimenziós radar, mely felügyeletet és felderítést biztosít a légi járművek felett. A legkorszerűbb radar rendszer, melyet a katonai légvédelemben működtetnek. [4] Antennája szélessávú dipólokból felépített fázisvezérelt antennarács, s felderítési hatótávolsága 470 km. A radar túlélhetőséget biztosít, valamint sokoldalú működési rugalmasságot a különböző ellenséges zavarokkal szemben. Teljesen félvezetős, távvezérelhető, adóteljesítménye 84 kW, D/L sáv 1215-1400 MHz, IFF[3] rendszere Mode 4 és Mode S, illetve Mode 5. Adott esetekben légi irányításként is alkalmazható, hiszen a légi felügyelet mellett korai figyelmeztetést és helyzet felismerést tesz lehetővé a fegyverrendszerek időbeni alkalmazásához. Célja, rendeltetése az ECM[4] környezet és a clutterek[5] feltérképezése, a feldolgozott plotok továbbítása, a radar felderítési tartományában tartózkodó repülő eszközök felderítése, valamint a térbeli koordináták, a távolság, oldalszög és magasság meghatározása.

A RAT-31 DL radarról elmondható, hogy rendelkezik az összes olyan modern adatfeldolgozó képességgel, mint például az adaptív zavartérképek, illetve az összes modern zavarszűrő technikával az ismert szárazföldi objektumokra. Az irányszögbéli forgása mechanikusan, míg a fősugár szögmagassága elektronikusan, fázisvezérléses elven, azaz fázisváltókkal történik. A radar antennafelülete körülbelül 10^0-al vissza van döntve annak érdekében, hogy a lehetséges legalacsonyabb radarsugár szögértéket érjük el. Létrehozták

2 RAT31-DL - olasz gyártású háromdimenziós felderítő radar

3 IFF – Identification Friend or Foe, Barát vagy ellenség rádiófelismerés, egy az irányításra és ellenőrzésre tervezett azonosítási rendszer. Lehetővé teszi a katonai és polgári légi forgalomirányító rendszerek számára, hogy azonosítsák a repülőgépeket, járműveket vagy erőket barátként és meghatározzák a kérdezőtől való irányukat, illetve távolságukat.

4 ECM – Electronic Countermeasure, Elektronikai ellentevékenység.

5 Clutter – Zavar, zavaró tényező.

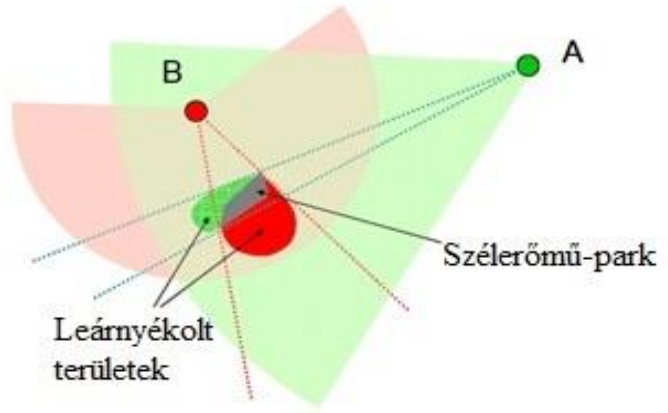
az idők során a RAT-31 DL/M verzióját, mely a mobil, szállítható verzióját takarja, eme korszerű háromdimenziós radar rendszernek. Paramétereikben, tulajdonságaikban szinte teljesen megegyeznek, a legnagyobb különbség a mobilitásban lelhető fel.[5]

SZÉLERŐMŰVEK HATÁSA A KISUGÁRZOTT JELEKRE

Korábbi tanulmányok igazolják, hogy az elektromágneses energia terjedésére hatással vannak a szélerőművek, hiszen felépítésük után a szélerőművek mögött olyan térrész alakul ki egy adott irányban, ahol csökkentett teljesítménnyel fog tovább haladni a radar által kisugárzott elektromágneses energia.[4] A kisugárzott energia egy része a radar irányába visszaverődik, másik része szétszóródik, melyek oka a beton, fém, illetve a terjedés szempontjából átlátható turbinalapát felületei, harmadik része pedig megfelelően halad tovább a légi jármű irányába.[6] A légi járművekről visszaérkező, tehát a visszavert jelek, a már említett hatásokat ismételten elszenvedik, s ennek eredményeként a légi járművek detektálási valószínűsége, nyomon követése, felderíthetősége lecsökken, illetve megszűnik.

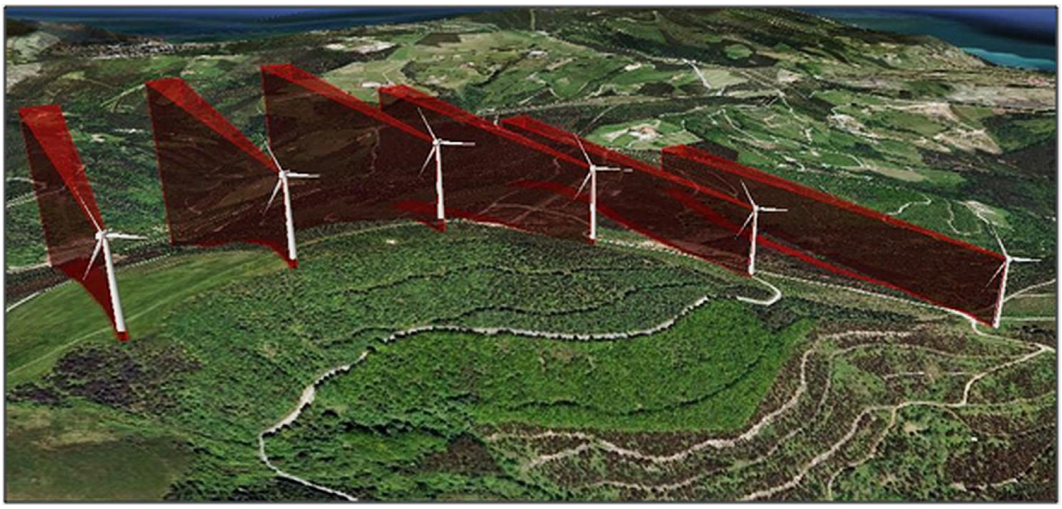
RADAR LEKÉPEZÉSI ANOMÁLIÁK

A szélerőművek nem „kerítésként” működnek, így nem okoznak maguk mögött vak-foltokat, de néhány irányban enyhe mezőgyengülés tapasztalható (1. ábra), s semmiképp sem a ferdetávolság csökkenését kell kiemelni, hanem a felderítési valószínűség csökkenését.[7]



1.ábra: A szélerőművek által árnyékolt területek, ahol A és B radarok, a szerző szerkesztése

A hamis jelek, azaz a célok száma jelentősen megnő a szélerőművek környezetében, s emiatt a zavarjelek lehetséges célként jelennek meg a légtérellenőrző rend-szerek, illetve radarok kijelzőin, indikátorain (2. ábra). Ezáltal két probléma merül fel: Az egyik, ami a fontosabb, hogy a radar által feldolgozható jelek száma véges, így a jelfeldolgozás túlterheltté és telítetté válik. A másik kevésbé, de szinté fontos, hogy a kezelőszemélyzetnek jobban oda kell figyelnie, ami leterheltséget és figyelem elvonást eredményezhet.[4]



2.ábra: Szélerőművek árnyékolása, a szerző szerkesztése

RENDSZERSZINTŰ DEGRADÁCIÓK

A szélerőművek hatása egyaránt érvényesül a céltárgyakra és a clutterekre is. Két fő csoportba oszthatók melyek szerint van statikus (torony, gondola) és dinamikus (lapátok) szórás. A statikus szórás a céltárgyakra szellemképet eredményezhet, illetve megnövekedett mérési hibákat okoz. A clutterekre pedig úgy hat, hogy áthelyezi, átpozícionálja őket a térben, ahol az álló földi clutterek nem kerülnek áthelyezésre a sebességtérben.[1] Dinamikus szórás esetén a céltárgyakra gyakorolt hatása szerint hamis, ugráló plotok[6] jönnek létre, illetve ugyan úgy, mint a statikusnál, itt is meg-növekedett mérési hibákat okoz. Viszont itt már a clutterekre jobban kihatással vannak, hiszen pozíciótérben ugráló clutterekről beszélünk és az álló földi clutterek is áthelyezésre kerülnek a sebességtérben.

Rendszerszintű PSR[7] degradációk:

- Tracker[8] telítésbe vétele.
- Lehetséges vevő szaturáció.
- Hamis (ghost) plotok.
- Redukált detekciós valószínűség (Pd)[9].
- Távolság- és szögmérési pontatlanság.

Rendszerszintű SSR[10] degradációk:

- Hamis (ghost) plotok.
- Távolság- és szögmérés pontatlanság.
- Redukált detekciós valószínűség (Pd).
- Tracker telítésbe vétele.

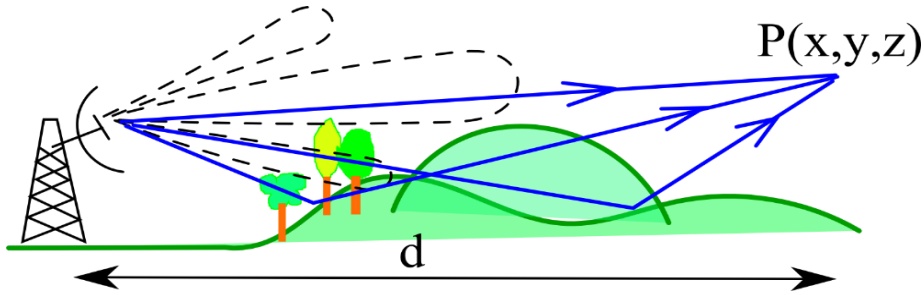
6 Plot – A Doppler-frekvencia és az irány vektorból képezik a plotot. A rendelkezésre álló plot adatokat hozzárendelik a célokhoz. Több önálló plot alapján inicializálják az adott célhoz tartozó útvonalat a tracket.
7 PSR – Primer Survaillance Radar, Elsődleges felderítő radar, Primer.
8 Track – Plotok sorozata, mely egy útvonalat alkot.
9 Pd – Detekciós valószínűség.
10 SSR – Secondary Surveillance Radar, Másodlagos felderítő radar, Szekunder.

Az Szekunder (másodlagos) felderítő radar enyhébben érzékeny a szélerőművek káros hatásaira, mint a Primer (elsődleges) felderítő radar. Hamis IFF/SSR plotok jelentkeznek több kérdezési módban is, például magas építményekről. Az egyik eshetőségnél a szekunder radar antenna iránykarakterisztikájának oldalszirmán kisugárzott P1 és P3 impulzusok, a közel térben nagy felületű tetőszerkezetről, a valós detektálandó cél irányába verődve aktiválják a céltárgy transzponderét[11] , s ezáltal hamis plotok, valamint hamis útvonal is keletkezhet. A transzponder válaszol az interrogátor kérdésére és a válaszjel ugyanazon az úton bekerül a jelfeldolgozásba. A szekunder antenna a válasz idején a főantennával együtt, szinte akkor még az északi irányon áll, ezáltal hamis útvonalat képeznek a hamis plotok, melyek azon az oldalszögön sorakoznak fel. Egy másik eshetőségnél a szekunder radar antenna iránykarakterisztikájának főszirmán kisugárzott P1 és P3 impulzusok, a közel térben nagy felületű tetőszerkezetről, a valós detektálandó cél irányába verődve aktiválják a céltárgy transzponderét, holott az antenna a forgása alatt még a valós cél oldalszögének irányát sem érte el, s ezáltal hamis plotok, valamint hamis útvonal keletkezhet. A transzponder válaszol az interrogátor[12] kérdésére és a válaszjel ugyanazon az úton bekerül a jelfeldolgozásba. A szekunder antenna a válasz idején a primer antennával együtt még a kérdéses céltárgy irányán áll, ezáltal hamis útvonalat képeznek a hamis plotok, melyek azon az oldalszögön sorakoznak fel.[5] Eme problémák megoldására, kiküszöbölésére a legjobb megoldás az, hogy a közel térben nagyobb csillapítást kell alkalmazni.[3]

ELEKTROMÁGNESES HULLÁMTERJEDÉS, ZAVARÁS

A szélerőművek, szélerőműparkok zavarják a telekommunikációs eszközöket, de ez elkerülhető a körültekintő tervezésükkel.[4] Szélerőművek tervezői, illetve az illetékes katonai és polgári szervek konzultálnak egymással, hogy megállapítsák, várhatók-e elektromágneses zavarok az adott területen, hiszen a légügyi kommunikációs rendszereket és mikrohullámú hálózatokat befolyásoló problémákat már a tervezés szakaszában figyelembe kell venni, rendezni kell.[8] A közelben lévő vevőkészülékek venni fogják a lapátkerékről visszavert és a közvetlen jeleket is, így kelthetnek a szélerőművek elektromágneses zavaró hatást. Azokat a katonai és polgári kommunikációs jeltípusok, amelyeket az elektromágnes zavaró hatások befolyásolhatnak, a TV- és rádióadásokat, mikrohullámú és cellás rádiókommunikációt, valamint a különböző navigációs és légi közlekedési ellenőrző rendszereket foglalják magukba.[9] A modern lapátkerekekhez már üvegszálas poliésztert használnak, amely részlegesen áteresztő az elektromágneses hullámok számára, s emiatt közbenső helyet foglal el az elektromágneses zavarások skáláján. Fontos szerepet játszanak felderítési szempontból az elektromágneses hullámterjedésben tehát a domborzati viszonyok (geometria), a növényzet (reflexió, diffrakció, elnyelés), a megvilágító adó iránykarakterisztikája, polarizációja és frekvenciája, mint „bementi” adatok. „Kimeneti” adatként pedig az elektromágneses sugárzás intenzitása, iránya, polarizációja tetszőleges P (x, y, z) pontban, melyet a 3. ábra szemléltet.

11 Transzponder – A repülésben használt radar-válaszjeladó megnevezése, amely név az angol transmit (továbbít, sugároz) és responder (válaszadó) szavak összevonásából származik.
12 Interrogátor – A kérdező jelet kisugárzó.

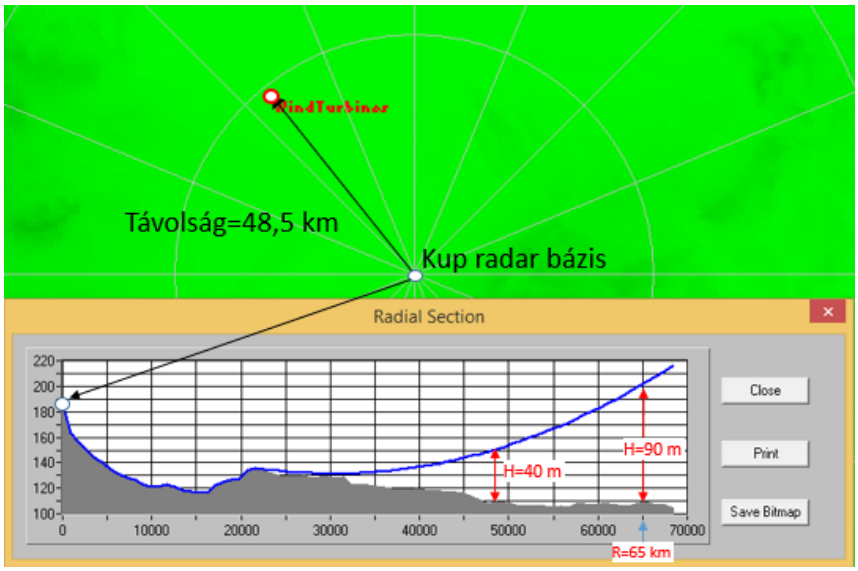


3.ábra: Az elektromágneses hullámterjedés szimulációja, a szerző szerkesztése

Komplex hatások szimulációjánál figyelembe kell venni tehát a terjedési- és reflexiós szimulációk összekapcsolását, a lefedettség változtatását („kitakarítás” a torony mögött), erősen reflektáló tereptárgyakat, szélerőműpark elemei közötti reflexiós kölcsönhatásokat és a többszörös reflexiót (céltárgy RCS[13] és WT RCS), a turbulencia hatását esős időben. A pirotechnikai eszközök stadionba bevitele elméleti síkon tilos, azonban detektorok és röntgen átvizsgáló kapuk hiányában a biztonsági személyzet a kiszűrésükre többnyire alkalmatlan.

MEGÁLLAPÍTÁSOK, ÖSSZEFÜGGÉSEK

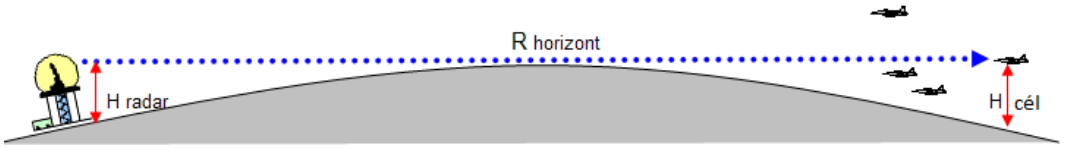
Az eddig leírtak alapján megállapítom, hogy a szélerőművek telepítése mindenképpen hatással lesz a radarokra, hisz erősen kiveszi a részét a szárazföldi zavarokból. A 4. ábrán látható, hogy kell elképzelni egy radar bázis és egy szélerőműpark egyszerű kapcsolatát, valamint a domborzati viszonyokat.



4.ábra: Kup radar bázis és Veszkény szélerőműpark telep távolsága, domborzati viszonyok, a szerző szerkesztése számítások alapján

13 RCS – Radar Cross Section, Radar hatásos keresztmetszet

Továbbá, választásom, elemzés és összevetés szempontjából, a magyarországi háromdimenziós radarokra esett, melyek Békéscsabán, Medinán és Bánkúton találhatók. Ezek közül a Medinán elhelyezkedő RAT-31 DL háromdimenziós radart vizsgáltam, mivel az ottani radarra nagy hatással lenne a Németkér falu közelében építendő szélerőműpark. A medinai radar egy dombon van elhelyezve, mely körülbelül 30 méteres és ehhez hozzáadva még a betontorony magasságát, amin az elhelyezkedik az antenna, összesen 35 méteres körülbelüli értéket kapunk. Tehát a föld felett, a Föld görbületét beleszámítva (5. ábra), ilyen magasan van elhelyezve az antenna, amit egy szendvicsszerkezetű multipanel radarantenna kupolával látott el a gyártó, az olasz Selex cég. A terepviszonyokat is figyelembe véve állítom, hogy a létrehozandó szélerőműpark optikailag teljes mértékben látható a radar számára. Feltételezhető, hogy a legalacsonyabb sugár nyaláb körülbelül +0,9^0 szögmagasságra mutat, vagyis -3dB értékre a horizonton, annak érdekében, hogy a működési frekvenciatartományban a földről visszaverődő sugarak által keltett jelentős zavarás elkerülhető legyen.



5.ábra: A Föld görbületi hatásai a detektálandó célokra ((1)-(7) számítások), a szerző szerkesztése számítások, mérések alapján

$$r_{föld(bal\ oldalt)} = 6370\ km \qquad r_{föld(jobb\ oldalt)} = 6370\ km \tag{1}$$

$$r_{föld\ effektív} = 8500\ km \qquad r_{föld\ egyenértékű\ sugár} = 6370\ km \tag{2}$$

$$H_{radar} = 250\ m \qquad H_{cél} = 1000\ m \tag{3}$$

$$R_{horizont} = \sqrt{2 * k * R_f} * (\sqrt{H_{radar}} + \sqrt{H_{cél}}) \tag{4}$$

$$\sqrt{H_{radar}} = 15{,}81139 \quad \sqrt{H_{cél}} = 31{,}62278 \tag{5}$$

$$\sqrt{H_{radar}} + \sqrt{H_{cél}} = 47{,}43416\ m \tag{6}$$

$$R_{horizont} = 3605 * \left(\sqrt{H_{radar}} + \sqrt{H_{cél}}\right) = 196{,}508\ m \tag{7}$$

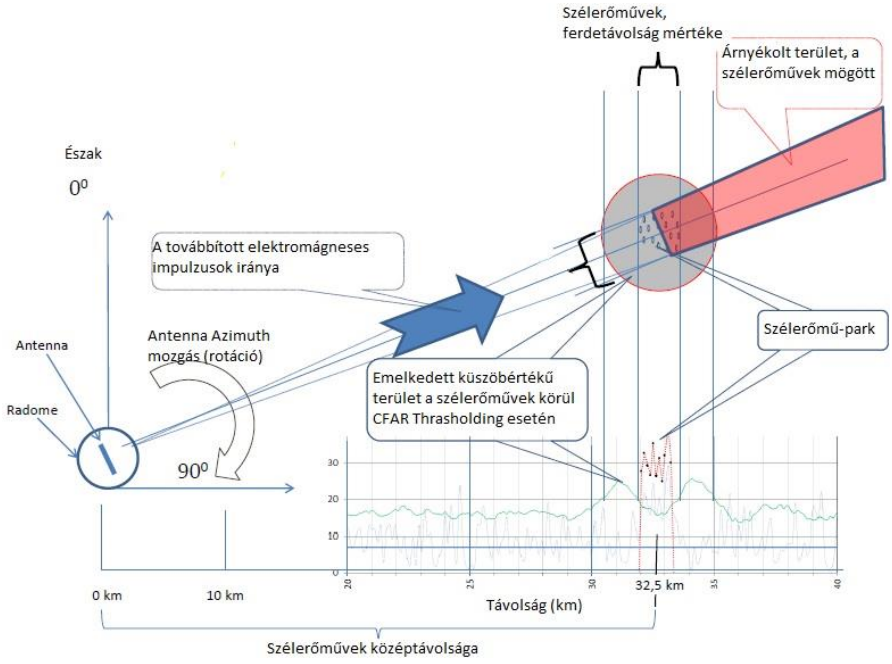
A szélerőműpark körülbelül 35 km-re lesz légvonalban a medinai radartól, mely a felderítésben hatalmas nagy problémát okozhat, nem is beszélve a visszaverődő különböző jelekről, melyeket már korábban említettem. Ugyanakkor a telepíteni kívánt szélerőműpark Budapesttől sincs messze, mindössze 90 km-re van, mely a Ferihegyi repülőtér radarjait is nagymértékben befolyásolhatja. Mind a primer mind pedig a szekunder radarnál okozhat problémákat, ha a kisugárzott jel egy szélerőműparkba „ütközik". A szekunder radarnál felmerül, hogy a visszaverődések erősebbek a légi jármű transzponderének minimum küszöbértékénél, így a transzponder a visszaverődésekre ad választ, valamint figyelembe kell még venni a monopulse[14] szöghibákat is, mint problémát. A primer radarnál pedig hamis célazonosítást eredményezhet a visszaverődések miatt, melyek elég nagy távolságban is előfordulhatnak, függetlenül attól, hogy 35 km-ről vagy többszörös távolságokról beszélünk, valamint hatótávolság-csökkenést okoz a potenciális elnyelési és visszaverődési, szóródási

14 Monopulse – Nagyobb irányszög pontosságú

hatások miatt. A szélerőművek jellegzetessége, hogy bár a jelük „állandó” egy adott helyen, de a róluk visszaverődő jel forgó rotor lapátok esetén Doppler eltolódást mutat. Az eltolódás spektruma annál szélesebb, minél gyorsabban forognak a szélturbinák lapátjai. Az eltolódás függ továbbá attól, hogy a radartól milyen szögben látszódnak - a széliránynak megfelelően - a rotor lapátok.

A MEDINAI RAT-31DL HÁROMDIMENZIÓS RADAR ÉS A NÉMETKÉR MELLETTI SZÉLERŐMŰPARK ÖSSZEVETÉSE, ELEMZÉSE

Összesen tizenhat darab szélerőműből álló szélerőműpark hatását vizsgálom, mely különböző mértékben befolyásolja a medinai RAT-31 DL háromdimenziós radar felderítését, nulla, egy, illetve a tizenhat szélerőmű esetén. A RAT-31DL háromdimenziós radarra gyakorolt hatása a szélerőműveknek függ attól, hogy mennyi szélerőmű helyezkedik el a radar látómezőjében. Különböző szempontok alapján figyelembe kell venni a szélerőművek kumulatív hatásait, hogyan árnyékolnak, például, hogy milyen magasak ,rotorral együtt természetesen, valamint milyen sok van belőlük az adott területen, tehát milyen széles skálát fednek le ezáltal. Az árnyékról feltételezzük, hogy konstans Azimuth iránnyal rendelkezik, amely a tizenhat szélerőmű ferdetávolságának mértékétől és a középtávolsága által került meghatározásra. Valamint azt is feltételezem, hogy konstans magassággal és szélességgel rendelkezik, amely a szélerőművek magassága, beleértve a rotort is, középtávolsága által került meghatározásra (6. ábra). Méréseim alapján a nulla darab szélerőmű elhelyezéséhez képet, mikor pontosan 1 darab szélerőművet helyezünk el a szélerőműpark települési helyén, akkor a szélerőmű által leárnyékolt tartomány $0{,}1^0$ lesz, míg 16 darab szélerőmű esetén pedig $1{,}6^0$.



6.ábra: Az „árnyék” modell a szélturbinák mögött, a szerző szerkesztése mérések alapján

KONKLÚZIÓ

Az összehasonlításnál vizsgáltam a szélerőművek hatását a radarokra, miszerint figyelembe vettem a különböző szempontokat, melyek problémákat okoznak. Amikkel foglalkoztam ez esetben, azok a különböző radar leképezési anomáliák, a szélerőművek hatása a kisugárzott jelekre, a rendszerszintű degradációk, az elektromágneses hullámterjedés, illetve zavarás. Hatalmas problémát okoznak ugyanis a légtérfelderítésben a különböző felületekről érkező reflexiók, hamis plotok, árnyékolt területek, a tracker telítésbe vétele, a redukált detekciós valószínűség, távolság- és szögmérés pontatlanság, melyeket mind megemlítettem, de van, amit ábrákkal szemléltettem munkám írása folyamán. Kutatómunkám további része, mely a bizonyításokról, mérésekről, összefüggésekről és megállapításokról szól, nem egyszerű, ám annál lényegre törőbb választ ad az általam vizsgált problémákra. Én ugyanis elsősorban a Medinán elhelyezkedő RAT-31 DL három dimenziós radar és a tőle 35 km-re elhelyezkedő Németkér falu melletti terület összevetésével vizsgáltam meg azt, hogy ha a szélerőműparkot megépítenék az nagy mértékben befolyásolná a légtérfelderítést. A mérési eredmények kielégítő választ adnak, miszerint szélerőmű nélkül nagyobb felderítési távolsága van a radarnak, viszont, ha egy vagy tizenhat darab szélerőmű akadályozza a felderítést, akkor 10, illetve 1,60 már leárnyékolt tartomány jön létre, ahol a célt nem látja a radar.

Úgy gondolom, hogy mivel a radarok felderítési hatótávolságát már a különböző domborzati viszonyok (dombok, hegyek, fák), meteorológiai jelenségek (felhő, eső), építmények (magaslatra épített házak) alapjáraton is befolyásolják, s hatalmas problémát okoznak, akkor ezt, a szélerőműparkok közeli telepítésével a radarállomásokhoz csak is kizárólag növelni fogják. Véleményem szerint kétféle megoldás létezik a probléma elkerülésére, illetve csökkentésére, melyeket még így is csak kompromisszum kötés alapján lehetne a jövőben kiküszöbölni. Az általam vélt egyik közös megegyezés alapján történő megoldás az lenne, ha a szélerőműveket viszonylag messze telepítenék a radarállomásoktól, s így a lehető legminimálisabban zavarnának be a légtér felderítésében. A másik viszont az, hogy a lehető legmagasabb helyekre kellene építeni a radarállomásokat, illetve helyezni a radarokat, s a szélerőműveket ennél jóval alacsonyabb pontra helyezni, ahol szintén minimális zavarást okozna a légtér felderítésében. A probléma Magyarországon az, hogy nagyon kevés a magaslati pont, s azok sem túl magasak, így se szélerőműpark, se radar telepítésénél nincs túl nagy választék a helyek tekintetében. Ezeket összegezve, s a két általam vázolt megoldás alapján a legjobb az lenne, ha a kettő ötvözése megvalósulna. Tehát kompromisszumot kell kötni, ha jól működő légtér felderítés, illetve szélerőműparkok építése a cél, akkor ezeket úgy kell telepíteni, illetve létrehozni adott esetben, hogy minimális legyen a szélerőműparkok radarra gyakorolt hatása.

FELHASZNÁLT IRODALOM

[1] WOLFF, C. *Radar Basics*, 2010, [Online] https://www.radartutorial.eu/index.en.html
[2] FEKETE L. *Radar, Radarrendszer*, 2000, [Online] http://suszter.atw.hu/
[3] WOODFORD, C. *Radar*, 2015, [Online] https://www.explainthatstuff.com/radar.html
[4] SELLER R. *Szemelvények a szélerőmű – radar kérdéskörben I.*. Veszprém: Szimpózium, 2015.

[5] WOLFF, C. *RAT-31 DL. L-BAND/SOLID STATE 3D Air Surveillance Radar*, 2014, [Online] https://www.radartutorial.eu/19.kartei/02.surv/karte012.en.html
[6] EUROCONTROL, *How to Access the Potential Impact of Wind Turbines on Surveillance Sensors*, 2014, [Online] https://www.eurocontrol.int/publication/eurocontrol-guidelines-assessing-potential-impact-wind-turbines-surveillance-sensors
[7] KÁRÁNDI Zs. *A Magyar Honvédség helye, szerepe a szélerőművek telepítésének engedélyeztetési eljárásában*. Veszprém: Szimpózium, 2015.
[8] SZÖKRÉNY Z. *Radartechnika órai jegyzet*. Budapest: Nemzeti Közszolgálati Egyetem, 2015.
[9] SIPOS Gy. *Elektronikai hadviselés a XX. században 2. rész*, 2014, [Online] https://lazarbibi.hu/index.php?option=com_content&view=article&id=124:radarhaboru&catid=23:haditechnika&Itemid=125

SINGLE CARD COMPUTERS FROM THE-POINT OF VIEW OF THE SECURITY OFTHE DIGITAL SOLDIER

AZ EGYKÁRTYÁS SZÁMÍTÓGÉPEK A DIGITÁLIS KATONA BIZTONSÁGA SZEMPONTJÁBÓL

KISS Csaba[1]

Abstract

The XXI. In the 20th century, the use of artificial intelligence accelerated, including in the field of machine vision. Machine vision occupies an important place in the system of our digital life, since we acquire most of our information through vision. Writing the software necessary for the operation of machine vision is facilitated by the multitude of open source programs and single-board computers available to everyone on the Internet. With the help of these, it may be possible to develop tools that have not yet been regularized in military use. Devices created with single-card computers can even serve to increase the security of the digital soldier. The publication deals with the presentation of single-card computers and the conditions for their use from the point of view of the digital soldier performing military operations on the battlefield.

Keywords

digital soldier, single-board computer, artificial intelligence, IT security

Absztrakt

A XXI. században felgyorsult a mesterséges intelligencia felhasználása, többek között a gépi látás területén is. A gépi látás egy fontos helyet foglal el a digitális életünk rendszerében, hiszen látás útján szerezzük be az információnk nagyobb részét. A gépi látás működéséhez szükséges szoftverek megírását könnyíti az interneten mindenki részéről elérhető nyílt forráskódú programok és egykártyás számítógépek sokasága. Ezek segítségével, olyan eszközök kifejlesztésére nyílhat lehetőség, amik a katonai felhasználásban még nincsenek rendszeresítve. Az egykártyás számítógépekkel kialakított eszközök akár szolgálhatnak a digitális katona biztonságának a növelésének érdekében. A publikáció foglalkozik az egykártyás számítógépek bemutatásával, valamint azok informatikai biztonság szempontból történő elemzésével.

Kulcsszavak

digitális katona, egykártyás számítógépek, mesterséges intelligencia, IT biztonság

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

INTRODUCTION

Accelerated military operations and increasingly powerful technologies and systems are bringing unprecedented changes to the field of military warfare today. Automated command and control technologies will appear on the battlefield as digital workstations for automated targeting systems.

Protecting the lives of soldiers on such an automated battlefield is a particularly big challenge for those involved in military technology research and development. The 'digital soldier program' can be a solution for increasing the soldiers' sense of security and for the shorter and more accurate execution of military operations. Practically, the soldier is provided with all the information he needs to fight the battle with the help of digital technologies, i.e. they provide a connection with a wifi or bluetooth application to a server computer, which can be installed even on a Lynx combat vehicle. The movements and positions of the soldiers are displayed on a screen, which is usually placed on the arm.

All elements of the individual device system of modern foot soldiers are electronic, and therefore require a source of energy. The duration of planned military tasks - when the soldier cannot charge the batteries - is a maximum of 24 hours.[1] There can be significant differences in the electrical implementation of the power supply systems, which manifests itself in the fact that custom-designed or standard batteries are used, adapted to the energy intake. This means that power supplies of different capacities and voltages are possible in digital military systems developed in different countries, so the load capacity of the batteries can also be different. As a result of the rapid technological development in this field of science, energy storage devices have a longer lifespan, an ever-increasing capacity, can be charged more easily and quickly, and are increasingly smaller in size. This is important when connecting devices made with single-board computers to the power distribution system made on the digital soldier.

Commercially available single-board computers, which are complete computers based on a single circuit board, such as Raspberry Pi, NanoPi, Banana Pi, Orange Pi, usually have power supply requirements ranging from 5V, 200mA to up to 2A, depending on the configuration.

These single-card computers can be easily programmed, even in the field of machine vision, so they can become a tool supporting the digital soldier and their power supply can even be based on the digital soldier's system. By using machine vision, we can not only correct human errors (due to fatigue or inattention, for example), but it is also possible to use it for social purposes, which can be proven in other areas.[2] [3]

In civil society, devices built with single-board computers can perform just as well in the military operational area as in the civilian area. According to the task to be performed, the same thing is done, for example: obstacle avoidance, but in terms of the result of the task, we get something different. In the civilian area, a robot may deliver medicine to an elderly person, while in the military area, the same robot brings ammunition to the trenches to the soldier from the distribution point. Obstacle avoidance (trees, ditches, etc.) can be performed by the same algorithm, therefore we can say that the various algorithms created by civil society can be suitable for increasing the defense system of the digital soldier, which can increase its combatability and chances of survival.

From the point of view of the program, it does not matter whether the algorithm is run in a civilian or military field, and from the point of view of the result, the person is the

determining factor. Such an interpretation and application of single-board computers allows the addition of military systems. The following chapter presents single-board computers.

SINGLE-BOARD COMPUTERS

One-board computers are one-board because they consist of a single printed circuit board and the circuit elements implanted on it. By connecting a keyboard, mouse and screen, we can get a complex computer workstation. Translated into English, its name in scientific literature is single-board computer, its abbreviation is SBC.

Single-board computers are popular due to their low cost and versatility, so they quickly became popular for home hobby applications, e.g. for home automation, building camera surveillance systems, controlling robots, as well as cloud services, own web server, website operation and so on. One-card computers can easily be used to learn programming languages, which is also used by schools, and its versatility is also reflected in the peripherals that can be connected to it.

The following single-board computers can be purchased commercially: Raspberry Pi, Rock Pi, Radxa Zero, Odyssey, VisionFive, Nezha, Odroid, LattePanda, Tinker Board, NVIDIA Jetson Nano, Atomic Pi, Khadas, NanoPi, Edge-V, Quartz, ROCKPro64, UDOO x86 Advanced Plus, Banana Pi, LeMaker, Orange Pi, HiKey 960. Picture 1 shows the Raspberry Pi 4B.

Picture 1.: Raspberry Pi 4B single-board computer, Christopher Barnatt: Explaining Computers.com, 2023

Picture 1 clearly shows the connection points USB, power supply and network connection interface, this is generally true for all single-board computers. Compared to the USB connector, its size is predictable: 85 mm long and 56 mm wide. They usually have a (2-8) core processor, 10/100 Mbit/s Ethernet port, WiFi, Bluetooth, RAM from 128 MB up to 8 GB, Video controllers and other additional panels (camera) depending on the type depending. Their nominal power is also possible from 200 mA (1 W) to 1.4 A (7 W). Power supply via MicroUSB or GPIO connector is DC 1.8–5.1 V. DC 3.3V and DC 1.8V are possible at the output. Their operating system usually depends on the type: Linux, Android, Ubuntu, Debian, OpenHarmony, Orange Pi OS and other operating systems. They can also have a headphone connection option and a connection option suitable for receiving audio input and output data.

Since single-card computers are suitable for the design of devices based on machine vision due to their small size, light weight and simple programmability, they can function as a complement to the digital soldier's system. Their power supply is either built on top of the digital soldier's system or has its own separate power supply, which can be a battery or a solar panel.

DIGITAL SOLDIER

Artificial intelligence has appeared in all areas of life, safety and security sciences [4] and military applications [5] are no exception.

In line with international processes, an artificial intelligence (AI) development program was launched in Hungary, during which the Artificial Intelligence Coalition (MIK) was established under the leadership of the Ministry of Innovation and Technology (ITM), whose primary goal is to improve domestic AI technologies on the international scene. their incorporation into everyday life and state activities.[6] In 2020, the Hungarian government issued Decree No. 1573/2020 to support the process. (IX. 9.) Government decision, which deals with Hungary's Artificial Intelligence Strategy and certain measures necessary for its implementation.[7]

The Hungarian Armed Forces is also not left out of the developments, since nowadays no one questions the importance of digital warfare, nor that its importance is constantly growing compared to other forms of warfare. In 2021, the National Military Strategy of Hungary (hereafter: NKS) was published, where artificial intelligence and the digital soldier program are among the development areas concerned. [8]

The development areas formulated by the NKS respond to the military challenges of the time. The most important value is human life, and the man of the age is trying to transfer this view to the military world using science. Picture 2 shows one of the construction possibilities of the digital soldier.

Picture 2.: Digital soldier, https://matasz.com/hun/a-digitalis-katona-program-a-magyar-honvedseg-teljes-gondolkodasmodjat-meg-fogja-valtoztatni/

The signal from the sensors (camera) worn on the soldier is connected to a transmitter device, the transmission of which is received by a centrally located receiver. dr. According to Lt. Gen. Gábor Böröndi: 'In the era of digital communication, it is necessary to be able to provide soldiers with all the information they need to fight.'[9] The data received by the driver through the reconnaissance system is processed and then sent to the tablet placed on the combat soldier's arm. This is how the soldiers see their own position, the position of the enemy and the military maneuver they have to carry out. By connecting them in a network, it can operate at several military levels, even at the battalion or brigade level.

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. Technical devices do not work without a power supply. In the next chapter, I will examine the system created with single-board computers from the point of view of IT security.

IT SECURITY

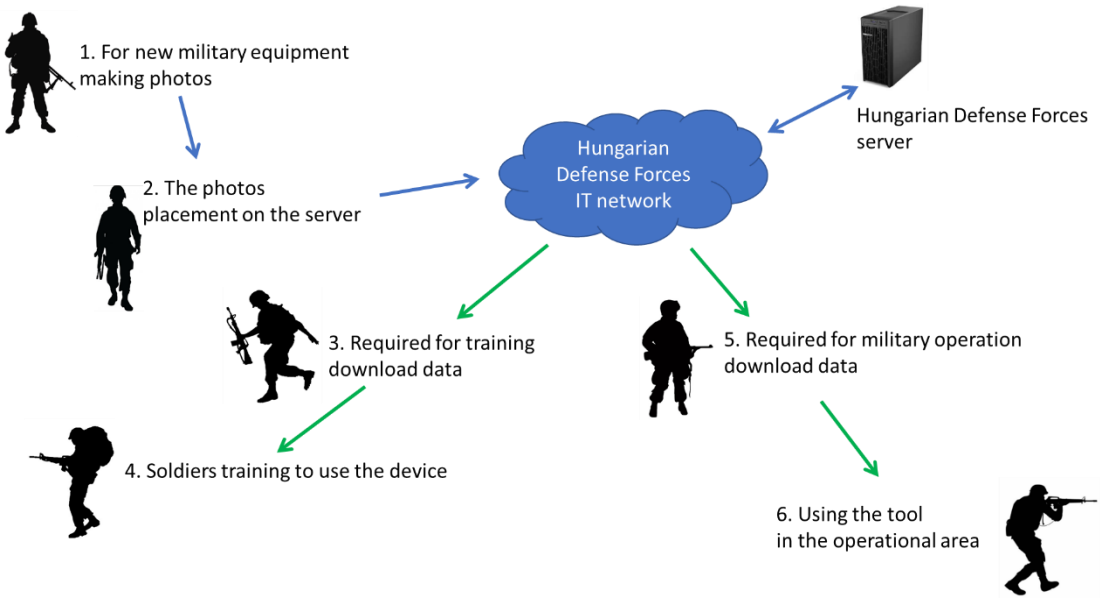
Since it is an IT device, of course a program runs on this device and the data is stored in a file system. As with all IT devices, the question may arise as to what and how the program and files running on the device ensure safe operation, i.e. how the IT protection of the program running on the device can be realized.

Soldiers could become familiar with such an IT tool during training. Military training is part of military life, which consists of theoretical and practical training, weaving through the entire military career. The training affects all types of weapons, so for each type of weapon we can examine the possibility of using a device equipped with machine vision created with a single-card computer. In general, it can help you recognize rank, military equipment, weapons, NATO symbols and other map symbols, ammunition, mines, rockets, bombs, grenades, fixed-wing and rotary-wing equipment and other special military tools. Soldiers would take the device with them and could also use it to monitor drones in the trenches, so they could also scan the sky with the help of the camera.

According to some security experts: 'IT security is a state of the protection system that is satisfactory for the defender, which is closed, comprehensive, continuous and proportionate to the risks in terms of the confidentiality, integrity and availability of the data managed in the IT system.'[10] The critical points are those activities that can be determined in the process of using single-board computers, where IT security may be compromised for various reasons.

With the spread of the use of single-card computers, the role and importance of IT security among users of single-card computers is even more appreciated. Single-card computers bring many advantages and benefits to the user, so its protection has also become critical, therefore there is an increasing need for users who are able to guarantee the safe IT use of devices equipped with a single-card computer.

Picture 3 shows the critical points arising from one of the possible conditions of use of the single-board computer from the point of view of IT security.



Picture 3.: Critical points from the point of view of IT security, own editing

In the 3rd picture, the MH IT network and the MH server can be clearly seen as the central element of the operating process of the device equipped with a single-card computer. Since the MH Informatikai network and MH server are already regulated in terms of IT security, the publication does not cover these elements. The second most important thing, which can be clearly seen in the 3rd picture, is the central role of the soldier, that is, the person who operates the process and uses the device. In the 3rd picture, you can see that there are 1 upload and 2 download directions.

I have identified a total of 6 critical points based on the 3rd image, where it is necessary to analyze IT security, these are the following:

1. The training photographs to be taken of the new military equipment. Photo files are created here, which can be files of different sizes. Up to 100 training photos can be taken from one device.
2. The files completed in point 1 are uploaded to the database located on the server, this is possible by copying the images to a folder system after logging in to a storage location.
3. Download the training photos required for military training. This is possible as described in point 2, when we log in to the storage on the server and copy the images to our device.
4. During the training, we put the device in the hands of the soldier to be trained.
5. The soldier participating in the military operation can initiate the download of the data according to the operation after logging into the database located on the server. You can copy the data to the device you want to use.
6. Use of the device loaded with training images in the military operational area.

The classification into the security class must be carried out on the basis of a risk analysis, which is defined in Art. 41/2015. (VII. 15.) BM Decree (BMr.) describes the requirements for technological security and secure information devices and products, as well as classification into security class and level.[11]

Table 1. shows the threats of the identified critical points in terms of IT security.

Critical point	Activity	Threats
1	Training photographs to be taken of the new military equipment. Photo files are created here, which can be files of different sizes. Up to 100 training photos can be taken from one device.	– industrial espionage – negligence, irresponsibility
2	The 1. the files completed in point are uploaded to the database located on the server, this is possible by copying the images to a folder system after logging in to a storage location.	– cyberterrorism – hackers, crackers
3	Download training photos required for military training. This is possible as described in point 2, when we log in to the storage on the server and copy the images to our device.	– industrial espionage – computer crimes – cyberterrorism – hackers, crackers
4	During the training, we put the device in the hands of the soldier to be trained.	– negligence, irresponsibility
5	The soldier participating in the military operation can initiate the download of the data according to the operation after logging into the database located on the server. You can copy the data to the device you want to use.	– information warfare
6	Use of the device loaded with training images in the military operational area.	– negligence, irresponsibility

Table 1. The critical points and possible threats, own editing

According to Act L. of 2013 (Ibtv.), electronic information systems must be classified into a security class in terms of confidentiality, integrity and availability. The law stipulates that the classification into the security class is approved by the head of the organization and is responsible for its compliance with legislation and risks, as well as the completeness and timeliness of the data used. The security classification must be recorded in the organization's IT security policy.[12]

According to Act L. of 2013 (Ibtv.), there are three data security requirements:

- confidentiality: only a limited number of authorized persons can know.
- integrity: that which corresponds to the original state.
- availability: access to the necessary data according to their processing where and when needed.

According to these principles, the group of authorized persons consists of trainers and IT staff, as well as an access restriction that limits the accessible files.

Since the use of the device can also take place within the IT system of a closed MH, from the point of view of IT security, the role of the soldier, i.e. the person, as a threat and risk factor increases.

Both international and domestic data show that data loss and data compromise can most often be traced back to human factors - in many cases, the incident can be prevented by paying attention to the staff and following the rules.[13] In this case, the device can be used by all soldiers, so education is what can strengthen the use of the rules of conscious IT security among soldiers.

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 with various measures and new protection techniques and tactics, but it cannot be 100% excluded. This is probably the most convincing argument regarding the need to develop a digital soldier, which can be supported even by using a single-card computer, which has already been well-proven in the civilian field.

The NATO Army Armament Group (NAAG) established Thematic Group 1 (TG/1) to coordinate the interoperability of military systems and to prevent identical developments between different military systems. This also applies to digital military systems.

Field design is important for such devices, which is not included in this publication. Due to the field design, the elements that ensure the power distribution of the digital soldier have a robust design. In practice, these connectors are elements made for special field design, so commercially available systems cannot connect to them. Due to the diversity of the power supply, which can be observed in the digital soldier, it is easiest if the single-board computers have their own power supply.

Technical progress results in a reduction in size and an increase in capabilities for all electronic devices, including single-card computers. Therefore, solutions developed at home on commercially available single-board computers and already proven in civilian life, which can be used to support the soldier on the battlefield, become applicable if IT security is observed.

The core of the device created with a single-board computer is loaded by a computer, so the IT security requirements for it are the same as the security requirements of an IT device. When using such a tool, the person is a critical point, whose training in IT security rules is a key element in achieving IT security.

The use of single-card computers is no more difficult than the usual military computers that soldiers use at work. Adherence to IT security begins with training, which the

units repeat annually at the workplace, and the soldier ensures the acceptance of the submitted material by signing it.

The best remedy for the prevention of industrial espionage and computer crimes is strengthening patriotism and the patriotism that people carry in their hearts. Patriotic education is nothing but education to protect the homeland, which can ensure that the soldier does not cause harm to his own country, i.e. protects its values. You are not only obliged to protect, but also to report if you detect an act indicating this, the same is true in the field of IT security.

REFERENCES

[1] Gácsér Z., 2008. "The possibilities of developing a modern, network-integrated individual equipment system that increases the soldier's combat ability in the Hungarian Armed Forces.", Budapest, Nemzeti Közszolgálati Egyetem.

[2] Kollár Cs. and Nagy B. "A mesterséges intelligencia felhasználási lehetőségei az objektumfelismerésben (első rész)," BIZTONSÁGTUDOMÁNYI SZEMLE, vol. 3, no. 1, pp. 123–140, 2021.

[3] Kollár Cs. and Nagy B. "A mesterséges intelligencia felhasználási lehetőségei az objektumfelismerésben (második rész)," BIZTONSÁGTUDOMÁNYI SZEMLE, vol. 3, no. 2, pp. 115–129, 2021.

[4] Kollár Cs, "A mesterséges intelligencia és a kapcsolódó technológiák bemutatása a biztonságtudomány fókuszában," in Kiberbiztonság – Cybersecurity 2., vol. 2, 2019, pp. 47–61.

[5] Kollár Cs, "A mesterséges intelligencia jelene és jövője a katonai és a polgári képzés fókuszában," in Generációspecifikus oktatásmódszertan alkalmazása a polgári és katonai oktatásban, Budapest: HM Zrínyi Térképészeti és Kommunikációs Szolgáltató Nonprofit Kft. (2023) pp. 31-44.

[7] Porkoláb I. - Négyesi I, 2019. " Researching the application possibilities of artificial intelligence in the military." Honvédségi Szemle, 2019/5. Online: https://honvedelem.hu/images/media/5f2bd1646eeb8298912683.pdf

[7] 1393/2021. (IV.24.) "Government decision on the National Military Strategy of Hungary." Magyar Közlöny 2021 (119)

[8] 1573/2020. (IX. 9.) "Government decision on Hungary's Artificial Intelligence Strategy and on certain measures necessary for its implementation" Magyar Közlöny 2020 (202)

[9] Szűcs L, 2021. " The digital soldier program - Conversation with dr. with Lieutenant General Gábor Böröndi." Online: https://matasz.com/hun/a-digitalis-katona-program-a-magyar-honvedseg-teljes-gondolkodasmodjat-meg-fogja-valtoztatni/

[10] Déri Z. at. All, 2004. "The system of requirements for the management of IT security - draft recommendation of the Information Society Coordination Interdepartmental Committee", Budapest

[11] 41/2015. (VII. 15.) "BM decree on technological security and the requirements for secure information devices and products, as well as classification into security class and security level, as defined in Act L. of 2013 on the electronic information security of state and local government bodies." Online: https://net.jogtar.hu/jogszabaly?docid=a1500041.bm

[12] Muha L.-Krasznay Cs., 2014. “Managing the security of electronic information systems.” Nemzeti Közszolgálati Egyetem, Budapest
[13] Kollár Cs, “A média mérőszámai és a digitális kommunikáció biztonságának mutatószámai,” BIZTONSÁGTUDOMÁNYI SZEMLE, vol. 1, no. 1–2, pp. 31–44, 2019.

BLOCKCHAIN-BASED SECURITY FRAMEWORK FOR IOT DEVICES

BLOKKLÁNC ALAPÚ BIZTONSÁGI KERETRENDSZER IOT ESZKÖZÖKRE

OLÁH Norbert[1] – NAGY Csaba Norbert[2]

Abstract

Nowadays, various Internet of Things (IoT) devices arise in many application areas (e.g. smart city, Internet of Drones). However, security incidents show that these systems are vulnerable. In our proposed solution, we explore the advantages and disadvantages of IoT devices and current relevant security issues. We suggested a solution to increase the security level of IoT systems, for which we proposed the application of blockchain technology. Our proposed framework considers the design considerations related to IoT (resource-constrained devices, scalability). We developed a user-friendly platform for the distributed storage of IoT device attributes on a permissioned (private) blockchain. The device manager has several features to provide a higher security level and fulfil security requirements (e.g. password setting, firmware update, two-factor authentication method).

Keywords

Security, IoT, Blockchain, Password setting, Firmware update

Absztrakt

Napjainkban a különböző Internet of Things (IoT) eszközök számos alkalmazási területen jelennek meg (pl. okosváros, drónok hálózata). Azonban a biztonsági incidensek azt mutatják, hogy sérülékenyek ezek a rendszerek. Az általunk javasolt megoldásban megvizsgáltuk az IoT eszközök előnyeit és hátrányait, illetve aktuális releváns biztonsági problémákat. Megoldást kerestünk az IoT rendszerek biztonsági szintjének növelésére, amelyre a blokklánc technológiát alkalmaztuk. Az általunk javasolt keretrendszer figyelembe veszi az IoT-val kapcsolatos tervezési szempontokat (erőforrás korlátozott eszközök, skálázhatóság). Kialakítottunk egy felhasználóbarát platformot, amely képes az IoT eszközök attribútumait egy engedélyköteles blokkláncon elosztott módon tárolni. Az eszközkezelő számos funkcióval rendelkezik, melyek növelik a biztonsági követelmények magasabb szintű megvalósítását. (pl. jelszó beállítás, firmware frissítés)

Kulcsszavak

Biztonság, IoT, Blokklánc, Jelszóbeállítás, Firmware frissítés

[1] olah.norbert@inf.unideb.hu | ORCID: 0000-0002-0007-8508 | Assistant Professor, University of Debrecen, Faculty of Informatics, Department of Data Science and Visualization| adjunktus, Debreceni Egyetem, Informatikai Kar, Adattudomány és Vizualizáció Tanszék

[2] nagy.csaba@inf.unideb.hu | ORCID: 0009-0009-0678-281X | technician, University of Debrecen, Faculty of Informatics, Department of Data Science and Visualization| technikus, Debreceni Egyetem, Informatikai Kar, Adattudomány és Vizualizáció Tanszék

BEVEZETÉS

A dolgok internete (IoT) napjaink egyik robbanásszerűen fejlődő területe. A fogalmat 1999-ben Kevin Ashton alkotta meg a Procter & Gamble számára tartott előadásában. A dolgok internetét, azaz az Internet of Things-t (IoT) egy olyan technológiaként fogalmazta meg, amely az 1983-ban megjelent RFID (Radio Frequency Indentification) segítségével több eszközt kapcsol össze. Napjainkban az IoT eszközökből álló rendszerek az életünk minden területén megjelennek, ilyen alkalmazásai többek között okosvárosok, az okosotthonok, az intelligens tömegközlekedés, az intelligens egészségügy vagy a dolgok ipari környezete (IIoT). Az IoT eszközök piaca dinamikusan nő, ahol a 2015-ös becslésben mért 15 milliárd eszközről 2025-re több mint 75 milliárd eszközt jósolnak a kutatók ([1]). Ez az előrejelzés azt jelenti, hogy 2 év múlva átlagosan minden embernek a Földön 5-10 személyes IoT eszköz lesz a birtokában.

Az IoT rendszerek terjedését és alkalmazását nagyban segíti annak számos előnye. Az IoT érzékelők működtetésével a vállalkozásoknak nagy mennyiségű valós idejű információ áll a rendelkezésére, melynek elemzésével képesek optimalizálni a munkafolyamatokat, csökkenthetik a működési költségeket és jobb ügyfélélményt biztosíthatnak. A szenzorok mellett a különböző beavatkozó eszközök (aktuátorok) fokozhatják a termelékenységet és növelhetik a munkahelyi biztonságot. Erre példa az autógyártó Ford, ahol speciális IoT technológiát és az életfunkciókat érzékelő technológiát használnak a munkavállalók túlzott fizikai terhelés elleni védelmére és a munka optimalizálására, amely 70%-ban csökkentette a sérülések számát ([2]). Azonban az előnyök mellett számos kihívás és probléma jellemzi még ezeket a rendszereket, ahol kibervédelmi szempontból az IoT eszközök sokszor nem megfelelően védettek. Az egyre érzékenyebb iparágakban, például az egészségügyben és a pénzügyekben használt IoT eszközöknél felmerülő adatvédelmi hiányosságok kezelésére egyre nagyobb motivációja van a rendszer fenntartóinak. A [3]-ban a szerzők kimutatták, hogy a jelenleg használt rendszerek többsége nem képes olyan erős biztonsági szolgáltatásokat és mechanizmusokat integrálni, amelyek megőrizhetnék a biztonságát a betegek személyes adatainak. Emellett súlyosbítja a helyzetet, hogy a kriptográfiai megoldások és a különböző biztonsági intézkedések integrálása az IoT eszközökbe nehézségekbe ütközhet, mivel az eszközök sokszor erőforrás korlátozottak. Emiatt ezek az eszközök nem képesek használni a különböző kriptográfiai primitíveket, illetve nagy eszközpark esetében a skálázhatóság, az interoperabilitás és a heterogenitás egyaránt a felmerülő kihívások közé tartozhat. Így az összes eszköz megfelelő beállítása, konfigurálása és folyamatos karbantartása sok időt, erőfeszítést és költséget jelent. Fontos, hogyha az így kialakított implementációnál akár egyetlen biztonsági rés is marad az elegendő ahhoz, hogy a támadók súlyos károkat okozzanak a rendszereinkben. Ezért az eszközöket többek között védeni kell a különböző aktív és passzív támadásokkal szemben. A passzív támadások kategóriájában a támadók általában a kommunikációt hallgatják le a felek között, hogy hasznos információkat gyűjtsenek. A passzív támadások közé tartozik a lehallgatások és a forgalomelemzések. Az aktív támadások esetén a támadó hatással van a kiválasztott rendszer funkcióira és működésére. Ennek hatásai a biztonsági mechanizmusok (behatolásérzékelés) által is észlelhető. Az ilyen típusú támadások következményeként például a hálózati szolgáltatások sérülhetnek. Az aktív támadások közé sorolhatók: zavarás (jamming), elárasztás (flooding), szolgáltatásmegtagadás (DoS) vagy Sybil típusú támadások ([4]).

A TUDOMÁNYOS ÉS GYAKORLATI MEGOLDÁSOK

A tudományos irodalomban számos cikkben foglalkoznak az IoT rendszerek biztonságának növelésével, ahol az egyik legfontosabb cél az eszközök által generált és továbbított adatok bizalmasságának, integritásának és rendelkezésre állásának védelme, amelyet (CIA) hármasaként ismerünk ([5]). Ezek a biztonsági elvek ugyanúgy vonatkoznak az IoT eszközökre és rendszerekre, mint az informatikai (IT) rendszerekre és online hálózatokra. Ha ezen alapvető biztonsági követelmények egyike sérül, abban az esetben az érintett egyénre vagy szervezetre nézve komoly következményekkel járhat. A Nemzeti Szabványügyi és Technológiai Intézet (NIST) a FIPS 199 szabványban ([6]) meghatározza a bizalmasság, az integritás vagy a rendelkezésre állás elvesztése miatti alacsony, közepes és magas potenciális hatásokat. Az adott támadásokra sok enyhítő és ellenintézkedést lehet implementálni, azonban az IoT rendszerek hálózatának összekapcsoltsága és heterogenitása miatt a biztonsági stratégiának általában átfogóbb, többszintű és több rétegre kiterjedő megközelítést alkalmaznak. A javasolt megoldások során figyelembe kell venni az IoT sajátosságokat például a [7] cikkben a szerzők állítása szerint a biztonsági incidensek 95%-a emberi hibákból származik. Javaslatuk egy új IoT alapú kiber-fizikai emberi rendszert (CPHS) tartalmazott, melynek egyik fontos eleme az emberi faktor, mivel a rendszer biztonságát nem csak az IoT rendszerek, hanem az emberi interakciók is befolyásolják. Ennek a felügyeletére a szerzők egy behatolástűrő rendszert (Intrusion Tolerant System, ITS) vezettek be, melynek célja az emberi hibákból származó támadások hatékony megelőzése. Egyes ötletek ([8], [9]) az architektúra rétegeit vizsgálják és kompromisszumot keresnek annak érdekében, hogy biztosítsák a megfelelő funkcionalitást és kezeljék a korlátozott eszközképességeket. A keletkező adatok védelmét a tárolás és a küldés során különböző kriptográfia primitívekkel garantálhatják, ahol olyan szempontok teljesülését vizsgálják, mint a végponttól végpontig terjedő biztonság, a különböző entitások hitelesítése vagy a hozzáférés-ellenőrzés.

Az IoT-hoz hasonlóan a blokklánc is viszonylag új technológia, ami megmagyarázza, hogy a blokklánc alapú alkalmazások miért korlátozottak. Mindazonáltal decentralizált jellegükből adódóan a blokkláncok számos előnyt kínálnak, amelyeket már megvalósítottak az IoT eszközökben. Emellett a blokkláncoknak az IoT eszközök sebességére gyakorolt negatív hatásai is sokszor nem relevánsak vagy kezelhetőek. Egy komplex blokklánc alapú gyakorlati megvalósítás az IoT rendszerek védelmére az Európai Unió által finanszírozott GHOST projekt, melynek célja egy megfizethető, kulcsrakész, védelmi megoldás kifejlesztése a kiberfenyegetések ellen okosotthonokra ([10]). A megoldás egy központi átjáróra támaszkodik, amely az okosotthon hálózatból érkező összes adatforgalmat összesíti. A GHOST különböző megközelítéseket követ a kiberfenyegetések és kockázatok észlelésére számos kiemelt technológiát alkalmazva, mint például a gépi tanulás, a behatolásérzékelés és megelőzés és a blokklánc. A GHOST autonóm módon értékeli a kockázatot az otthoni hálózat állapotával szemben, és intuitív és felhasználóbarát felületet biztosít a végfelhasználók számára a biztonsági preferenciák és beavatkozások kezeléséhez. A blokkláncokon alapuló IoT a mindennapi életünk gyakorlatilag összes területén megjelent és a fogyasztók egy része nincs vele tisztában, hogy aktívan használja ezt a technológiát. A blokklánc alapú IoT rendszerek használatának egyik fontos szempontja a kriptográfiailag védett nem manipulálható adatbázisok használata ([11], [12]). A GHOST mellett számos egyéb blokklánc alapú alkalmazást javasoltak az ellátási láncokba, az autóiparban, vagy az villamosenergia

piacokon, mely megoldások az IoT rendszerek biztonságának növelését tűzték ki célul ([13], [14]).

Hozzájárulás

A célunk egy új biztonsági keretrendszer javaslása blokklánc alkalmazásával egy IoT ökoszisztémára. A keretrendszer tartalmaz egy eszközkezelőt, amely az IoT eszközök különböző attribútumait tárolja, mint név, szoftver vagy firmware verzió, típus, tulajdonos és állapot. A blokklánc alkalmazás során egy engedélyköteles blokkláncot alkalmazunk, mivel az egyes szenzitív adatokat tartalmazó attribútumokat titkosítva kell letárolnunk (pl. verzió vagy az IoT eszköz állapota). Az eszközkezelő része egy okosszerződés, melynek célja, hogy ellenőrizhető legyen, ha a felhasználó nem változtatta meg az alapértelmezett jelszót az eszköznél vagy az eszközhöz tartozó szoftver, illetve firmware elavult verzióval rendelkezik. Végezetül a keretrendszer biztonsági mentést nyújt, ahol az IoT rendszer (például okosotthon) beállítások és konfigurációk elosztottan kerülnek tárolásra a blokklánc által. A keretrendszer biztonságosnak tekinthető, mivel a kapcsolódó webalkalmazás megköveteli a felhasználó hitelesítését (tagja-e a blokkláncnak), továbbá a felhasználó és a keretrendszer közötti kommunikáció TLS protokollt alkalmaz. A webszerver és a rajta futó webalkalmazás csak egy felhasználóbarát felületet nyújt a felhasználók számára. A blokklánc biztosítja az elosztott tárolást, illetve az okosszerződés egy elosztott alkalmazás, amely nagyobb rendelkezésre állást biztosít. Így például egy okosotthon beállításait és konfigurációját könnyebb helyreállítani különböző kártékony vagy zsaroló programok fertőzése esetén.

A javasolt rendszerről (lásd 1. ábra) egy prototípust készítettünk, amely egy webes alkalmazás Javascript nyelven implementálva. Az implementáció kialakítása során teszteltük a rendszer funkcionalitását és a biztonsági követelményeket.

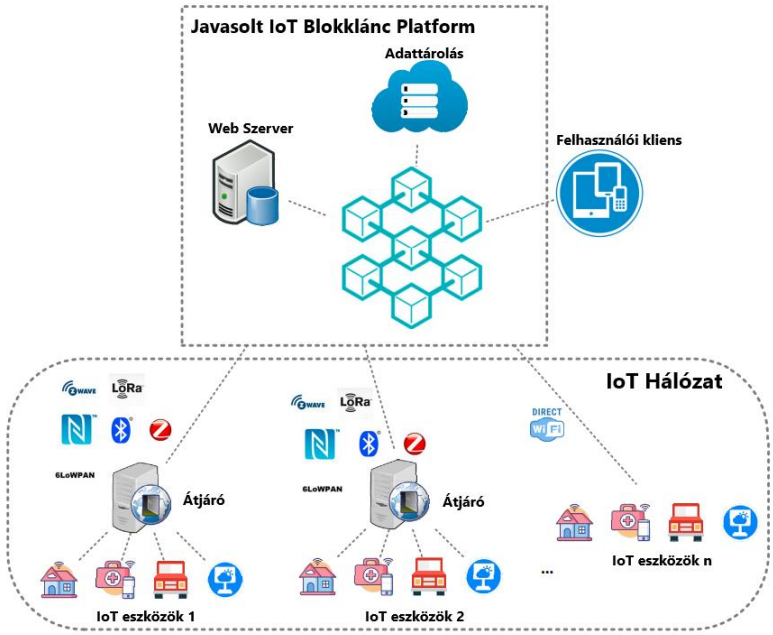
PROTOTÍPUS

Technológiai áttekintés

Az általunk javasolt rendszer implementációja több modulból épül fel. Ennek egyik eleme a Node.js ([15]), amely egy nyílt forráskódú szoftver platform és a webszerverünk elkészítésére alkalmaztuk. A Node.js egy V8 Javascript motorra épül, amely eseményalapú, aszinkron bemenettel és kimenettel rendelkezik a túlterhelés minimalizálása és a skálázhatóság maximalizálása érdekében. A felhasználóbarát felület kialakításához a React ([17]) egy nyílt forráskódú, deklaratív frontend nyelvét vettük igénybe. A webes API felhasználói felületének megjelenítéséhez és kinézetének testre szabásához a React JavaScript könyvtárat alkalmaztuk, ami által különböző komponenseket jeleníthetünk meg, mint például gombok, szöveg dobozok, űrlapok. Emellett szükségünk volt még a Next.js-re ([18]), amely egy nyílt forráskódú webfejlesztői keretrendszer. Ez lehetővé teszi a React alapú web alkalmazások használatát a szerveroldali rendelések és lokális webhelyek generálása érdekében. Támogatja az automatikus kódgyorsítást és adatlekérdezést, amely által a React alapú alkalmazások számára a hatékonyabb és gyorsabb működés biztosítható.

A blokklánc modul fejlesztéséhez először az okosszerződéseket kellett implementálni, ahol a legnépszerűbb objektum-orientált blokklánc programozási nyelvet, a Solidityt választottuk ([16]), amely lehetővé teszi a fejlesztők számára az Ethereum láncra való

alkalmazások fejlesztését. Az okosszerződések programozható logikát és állapotokat tartalmaznak, mint például a változók, a függvények, az objektumok, az öröklődés és az interfészek. Végezetül egy ingyenes kriptovaluta pénztárcára a Metamask-ra ([19]) volt szükségünk, amely elérhető a böngésző bővítményei között. A Metamask a felhasználók számára a fiókcímek tárolását és kezelését, valamint az Ethereum alapú kriptovaluták és tokenek küldését és fogadását támogatja. Emellett a Metamask biztonságos csatlakozást biztosít a decentralizált alkalmazásokhoz webböngészőn vagy mobilalkalmazások beépített böngészőjén keresztül.



1. Ábra: IoT eszközök és blokklánc kapcsolata, saját szerkesztés, saját szerkesztés.

Funkcionalitás

A prototípus fejlesztése számos biztonsági és egyéb funkciót foglalt magába, amellyel menedzselhetővé válnak a hálózatunkra felcsatlakoztatott eszközök. A rendszer skálázható, így lehetővé válik a tetszőleges számú IoT eszköz hozzáadása, illetve azok eltávolítása. Okosszerződések segítségével három alapfunkció kapcsolódik minden IoT eszközhöz, a megtekintés, a szerkesztés és a törlés. A megtekintés funkció aktiválása során a felhasználó részletesebb információt kap az eszközről, megjelenítve a különböző attribútumokat, mint például a MAC cím, a firmware azonosító, a kapcsolódó konfigurációs fájl. A szerkesztés aktiválásával az eszközök adatai szerkeszthetővé válnak, végezetül a törlés funkcióval az adott eszköz eltávolításra kerül a felhasználótól.

A biztonsági funkciók során kiemelendő a szoftver frissítés, amellyel nyomon követhető és ellenőrizhető, hogy az IoT eszközön lévő verzió megegyezik-e az elérhető legfrissebb verzióval. Amennyiben nem, akkor a rendszer figyelmeztetést küld és a felhasználó manuálisan elvégezheti a szükséges frissítéseket. A prototípus forráskódja elérhető az [20] hivatkozáson.

BIZTONSÁGI SZEMPONTOK

A rendszerünk biztonságát formálisan vizsgáltuk, a CIA hármas szempontokat figyelembe véve.

Bizalmasság

Az implementációnk elősegíti az IoT eszközök monitorozását a biztonsági kockázatok csökkentése érdekében. A bizalmasság szempont teljesülését a blokkláncon lévő érzékeny adatok, illetve a felhasználó és a webszerver közötti kommunikációra vizsgáltuk. A felhasználók és a webszerver közötti kommunikációhoz TLS (Transport Layer Security) protokoll alkalmazunk, amely biztosítja kulcscsere mechanizmust a résztvevők között és a munkamenet biztonságát. A blokklánc esetén az egyes érzékeny adatokat tartalmazó attribútumokat AES-GCM szimmetrikus blokktitkosítási algoritmussal vannak ellátva. Az adatok titkosságát így csak a megfelelő visszafejtő kulccsal rendelkező résztvevők képesek megismerni.

Integritás

A rendszerünkben az integritás védelmének biztosítására alkalmazzuk a megfelelő kriptográfiai primitíveket, úgymint hash függvény és digitális aláírások. Emellett a kiberbiztonsági szempontból problémás feladatok is kezelve vannak, így a támadók nem képesek az elavult szoftver vagy eszközkomponensből fakadó hiányosságokat kihasználni. Továbbá a blokklánc alapú alkalmazás tulajdonságai biztosítják, hogy az adatokat ne lehessen manipulálni vagy nyomon követhetőek legyenek az IoT eszközhöz kapcsolódó tranzakciók.

Rendelkezésre állás

Az általunk javasolt keretrendszerben az adatok a blokklánc több csomópontján való tárolásával, illetve az okosszerződések használatával elosztott tárolást és alkalmazást valósítottunk meg, amely növeli az alkalmazás rendelkezésre állását, mivel az adatok és az IoT rendszer funkciói redundánsan tárolódnak, illetve több csomóponton hajtódnak végre. Emellett az elosztott tárolás és alkalmazás lehetővé teszi az adatok és függvények szétosztását a hálózatban ezért lehetőség van arra, hogy a hálózaton belüli replikációkból rövid idő alatt helyreállítsuk azokat például, ha egy adat elveszik vagy kártékony program miatt elérhetetlenné válik. Így a blokklánc alkalmazásával lehetővé válik a leállások minimalizálása, illetve a kártékony programok elleni védelem növelése, amely során hiába fertőzi meg a kártékony program a rendszert, akár több csomópontot egyidőben, a konfigurációs fájlok felhasználásával gyorsan visszaállíthatóvá válik a korábbi, fertőzés előtti állapotába a rendszer.

ÖSSZEFOGLALÁS

A cikkben feltérképezésre került az Internet of Things rendszerek és eszközök széleskörű alkalmazási lehetőségeit, amelyek lefedik az életünk minden területét. Meghatároztuk az IoT rendszerek előnyeit és hátrányait és átfogó képet alkottunk a napjainkban fellelhető aktuális problémákról és sérülékenységekről. Elengedhetetlen volt még az IoT eszközök biztonságát tárgyalni, hiszen a kisebb és a komplex rendszerek is sok kis különböző eszköz összeségéből épülnek fel. Ezáltal a legkisebb alkotó elem biztonságát is magas szinten kell kezelni, azonban a legtöbb IoT eszköz korlátozott erőforrással rendelkezik, ami

miatt nem alkalmazható hagyományos kriptográfiai megoldások. Felmértük a blokklánc technológia fontosságát napjainkban. Egy engedélyköteles blokkláncot alkalmaztunk, ahol az érzékeny adatokat tartalmazó attribútumokat titkosítva tároljuk. A keretrendszer megalkotása során egy eszközkezelőt valósítottunk meg, amely az IoT eszközök különböző attribútumait tárolja. Ezek mellett ismertetésre került az Ethereum és okosszerződések alkalmazási és működési feltételei a biztonsági keretrendszerünkben. Taglaltuk az okosotthon rendszer résztvevőit és javaslatot készítettünk a saját implementációnkról más rendszerekkel összevetve. Végezetül a CIA hármas paramétereit határoztuk meg a rendszerünkre való tekintettel.

FELHASZNÁLT IRODALOM

[1] Friedman, V., *On the edge: Solving the challenges of edge computing in the era of iot.* 2018. [Online] Elérhető: https://www.databank.com/resources/blogs/solving-edge-computing-challenges-in-era-of-iot/

[2] Center Ford Media, *"Ford reduces production line injury rate by 70 percent for its more than 50.000 industrial athletes".* 2015. [Online] Elérhető: https://media.ford.com/content/fordmedia/fna/us/en/news/2015/07/16/ford-reduces-production-line-injury-rate-by-70-percent.html

[3] Gope, P. & Hwang, T. BSN-Care: *A secure IoT-based modern healthcare system using body sensor network.* IEEE sensors journal, 16(5), 1368-1376. 2015.

[4] Butun, I., Österberg, P., & Song, H. *Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures.* IEEE Communications Surveys & Tutorials, 22(1), 616-644. 2019.

[5] Sadique, K. M., Rahmani, R., & Johannesson, P. *Towards security on internet of things: applications and challenges in technology.* Procedia Computer Science, 141, 199-206. 2018.

[6] Division, NIST Computer Security, F. I. P. S. *Standards for Security Categorization of Federal Information and Information Systems*, NIST FIPS 199, 2004.

[7] Kumar, S. A., Bhargava, B., Macêdo, R., & Mani, G., *Securing iot-based cyber-physical human systems against collaborative attacks.* In 2017 IEEE International Congress on Internet of Things (ICIOT) (pp. 9-16). IEEE. 2017.

[8] Rajendran, G., Nivash, R. R., Parthy, P. P., & Balamurugan, S., *Modern security threats in the Internet of Things (IoT): Attacks and Countermeasures.* In 2019 International Carnahan Conference on Security Technology (ICCST) (pp. 1-6). IEEE. 2019.

[9] Ahmed, A. W., Khan, O. A., Mian, M. A., & Shah, M. A., *A comprehensive analysis on the security threats and their countermeasures of IoT.* International Journal of Advanced Computer Science and Applications, 8(7). 2017.

[10] Collen, A.; Nijdam, N.A.; Augusto-Gonzalez, J.; Katsikas, S.K.; Giannoutakis, K.M.; Spathoulas, G.; Gelenbe, E.; Votis, K.; Tzovaras, D.; Ghavami, N.; et al. *GHOST—Safe-Guarding Home IoT Environments with Personalised Real-Time Risk Control. In Security in Computer and Information Sciences*; Springer: Cham, Switzerland, pp. 68–78. 2018.

[11] Mazzei, D., Baldi, G., Fantoni, G., Montelisciani, G., Pitasi, A., Ricci, L., & Rizzello, L., *A Blockchain Tokenizer for Industrial IOT trustless applications.* Future Generation Computer Systems, 105, 432-445. 2020.
[12] Cullen, A., Ferraro, P., King, C., & Shorten, R., *On the resilience of DAG-based distributed ledgers in IoT applications.* IEEE Internet of Things Journal, 7(8), 7112-7122. 2020.
[13] Alshaikhli, M., Elfouly, T., Elharrouss, O., Mohamed, A., & Ottakath, N., *Evolution of Internet of Things from blockchain to IOTA: A survey.* IEEE Access, 10, 844-866. 2021.
[14] Minoli, D., & Occhiogrosso, B. *Blockchain mechanisms for IoT security.* Internet of Things, 1, 1-13. 2018.
[15] Node.js, 2023. [Online] Elérhető: https://nodejs.org/en/about
[16] Solidity, 2023. [Online] Elérhető: https://dev.to/envoy_/history-and-origin-of-solidity-2mhl
[17] React, 2023. [Online] Elérhető: https://en.wikipedia.org/wiki/React_(JavaScript_library)
[18] Next.js, 2023. [Online] Elérhető: https://vercel.com/home
[19] Metamask, 2023. [Online] Elérhető: https://docs.metamask.io/guide/
[20] Github prototípus, 2023. [Online] Elérhető: https://github.com/ncsn/SmarthomeBlockchain

PÁLYÁZATRA UTALÓ MEGJEGYZÉS

A KULTURÁLIS ÉS INNOVÁCIÓS MINISZTÉRIUM ÚNKP-23-1 KÓDSZÁMÚ ÚJ NEMZETI KIVÁLÓSÁG PROGRAMJÁNAK A NEMZETI KUTATÁSI, FEJLESZTÉSI ÉS INNOVÁCIÓS ALAPBÓL FINANSZÍROZOTT SZAKMAI TÁMOGATÁSÁVAL KÉSZÜLT.

DEVELOPMENT OF THE MEASUREMENT PROCESS BASED ON THE 5S

MÉRÉSI FOLYAMAT 5S ALAPÚ FEJLESZTÉSE

FARKAS Gabriella[1] – TÓTH Georgina Nóra[2]

Abstract

5S is a method that can eliminate the disarray, increases degree of order and therefore safety. It is an effective procedure used in a wide range of industrial environments to increase productivity and achieve occupational safety. It is a basic requirement to establish the work-place safe, which is not only focused on production or manufacturing areas, but also on entire activities, such as the establishment of laboratories and measuring equipment. In these areas, however, the safety and preservation of equipment and tools comes to the fore. In our article we would like to present a development plan for the use of high value measuring equipment using the 5S method. The primary goal is to investigate damage to the device, to discover the background of the damage and to develope the measure to protect it. For this reason it is important to choose the appropriate quality assurance methods and present the completed measurement protocol to minimize the number of problems occurring during measurement.

Keywords

5S, laboratory safety, quality improvement, measurement protocol, quality control tools

Absztrakt

Az 5S olyan módszer, amely megszűnteti a rendetlenséget, növeli az átláthatóságot és ezáltal a biztonságot. Széles ipari környezetben hatékonyan alkalmazott eljárás a termelékenység növelésére és a munkabiztonság megvalósítására. A munkahelyi környezet biztonságossá tétele alapvető követelmény, ami nem kizárólag a gyártási területekre összpontosul, hanem a teljes tevékenységekre, így a laborok, mérőhelyek kialakítására is. Ezeken a területeken ugyanakkor a berendezések, eszközök biztonsága, állagmegóvása kerül előtérbe. Cikkünkben bemutatjuk egy nagyértékű mérőberendezés használatára kidolgozott fejlesztési tervet az 5S módszer alkalmazásával. Elsődleges cél az eszköz sérüléseinek kivizsgálása, a károkozások hátterének feltérképezése és védelmére tett javító intézkedések kidolgozása. Ennek érdekében a megfelelő minőségbiztosítási módszerek kiválasztása elengedhetetlen, továbbá bemutatjuk az elkészült mérési protokollt, hogy a lehető legkisebbre csökkentsük a mérés során bekövetkezett problémák számát.

Kulcsszavak

5S, laborbiztonság, minőségfejlesztés, mérési protokoll, minőségügyi módszerek

[1] farkas.gabriella@bgk.uni-obuda.hu | ORCID: 0009-0000-9881-7286 | senior lecturer, Óbuda University Bánki Donát Faculty of Mechanical and Safety Engineering | egyetemi adjunktus, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

[2] toth.georgina@bgk.uni-obuda.hu | ORCID: 0009-0007-7451-9322 | master lecturer, Óbuda University Bánki Donát Faculty of Mechanical and Safety Engineering | mestertanár, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

BEVEZETÉS

A Gyártástechnológiai Intézeti Tanszék oktatási profilját tekintve a gépészmérnöki tantárgyakra fókuszál. Ennek megfelelően számos laboratóriummal rendelkezik, amelyek a gyakorlatorientált oktatás megvalósulását teszik lehetővé, így a munkavédelmi és a biztonsági szempontok dominálnak. A méréstechnika témakör nemcsak a gépészmérnök, hanem a mechatronikai mérnök és a biztonságtechnikai mérnök képzésben is megjelenik. Ugyanakkor a minőségelleőrzésnek fontos része a metrológia, így kutatási projektekben, TDK dolgozatokban, doktori tanulmányokban gyakran megjelenik önállóan vagy kiegészítő témaként. Ezen feladatok elvégzéséhez magas szinten felszerelt mérőgépek, berendezések, eszközök szükségesek. Ezek használata többnyire csak az adott mérési feladatok elvégzésére korlátozódnak. Alapvető elvárás, hogy a munkavédelem és a munkabiztonság szempontjából megfelelő környezet álljon rendelkezésre a személyes jelenlétű gyakorlatok lebonyolításához és a kutatási feladatok elvégzéséhez. Az Egyetem rendelkezik olyan szabályozási rendszerrel, amelynek célja az oktatók, a tanárok, a munkatársak és a hallgatók egészségének és biztonságának megóvása. Ezen szabályok betartása minden érintett számára kötelező, a munkabiztonsággal kapcsolatos ismeretek oktatása és felülvizsgálata rendszeres. Ezen túlmenően a korábbi években az egyes laboratóriumok biztonságosságának és ezen belül, elsősorban a rendezett és tiszta munkakörnyezet kialakításának növelése érdekében a Kar sokat tett. Kiemelendő a laborok rendszeres és dokumentált 5S alapú auditja, amely hatékonyan hozzájárult a munkahelyi környezet minőségi javulásához. A mérési folyamatok 5S alapú fejlesztése a különböző mérőeszközök esetében más és más. A különbözőségük miatt minden esetben egyedileg kell megvizsgálni, elemezni és új megközelítéseket alkalmazni. Tanulmányunkban ez a mérési eljárás a felületi érdességmérésre vonatkozik. Azon mikrogeometriai és mikrotopográfiai mérések, amelyek tudományos vizsgálatokhoz szükségesek a Mahr MarSurf GD120 felületi érdességmérő berendezésen valósulnak meg Intézetünkben. A berendezés használata és kezelése a szakmai ismereteken túl precizitást, odafigyelést és a mérési folyamat minden lépésének betartását igényli. Az érdességmérő berendezés legsérülékenyebb része a tapintószerkezet, a tapintótű, leggyakrabban előforduló meghibásodása pedig a tapintótörés. Ennek megfelelően az oktatói felügyelet ebben az esetben elengedhetetlen követelmény.

A felülettapintó érdességmérés során egy gyémántcsúccsal rendelkező tapintó halad végig a mérendő felületen, amely során vonalszerűen letapogatja a felület különböző hullámait és érdességeit. A mérés során felvett profilgörbékből a szabványos 2D és a 3D paraméterek szoftver segítségével számíthatóak, így válik a felület kiértékelése teljeskörűvé. Mindezek alapján belátható, hogy az eszköz használatához elengedhetetlen a megfelelő hozzáértés és előismeret. Az alkalmazott tapintótű törését számos tényező előidézheti, de minden esetben a mérőszemély jelenléte elősegítheti vagy megakadályozhatja azt. A tapintó esetleges sérülése vagy törése esetén beszerzése magas költséget jelent és pótlásáig a mérőgép gyakorlatilag használhatatlan. Ezen nem kívánt esemény elkerülése érdekében fontosnak tartottuk a mérőgép biztonságának növelését, az előforduló meghibásodások csökkentését. A kockázatelemzés alapjait követve építettük fel vizsgálatainkat, amely felöleli a mérési folyamat egyes lépéseinek definiálását, a káros eseményeket azonosítását, azok okainak vizsgálatát, valamint olyan eljárások kidolgozását, amellyel ezek a kockázatok csökkenthetők vagy teljesen megszüntethetők, elsősorban a megelőzésre helyezve a hangsúlyt.

ALKALMAZOTT MINŐSÉGÜGYI MÓDSZEREK

Az 5S egy olyan megközelítés és eljárás, amelynek célja a munkahelyi környezet rendezett kialakításával a munkafolyamatok hatékonyságának növelése, a folyamatokban lévő észszerűtlenségek csökkentése, kiküszöbölése. A Toyota Termelési Rendszer (TPM) egyik alapja, amely mára nélkülözhetetlenné vált az ipar minden szektorában. A módszert alkotó tevékenységek, egyben a megnevezésben található 5 japán kifejezés: seiri, seiton, seiso, seiketshu és shitsuke. [1] Ezek magyar megfelelői: szelektálás, elrendezés, takarítás, szabványosítás, szinten tartás. Az 5S arra a filozófiára épül, hogy a munkafolyamatok javítása elősegíti a hatékonyabb és biztonságosabb munkavégzést, ezáltal a termelékenységet növeli, a veszteségeket csökkenti. Leegyszerűsítve tehát, a környezet rendben tartásával a munkavégzés biztonságosabbá és ezáltal hatékonyabbá válik. [2]

Az eljárás első eleme a szelektálás (Seiri), amely a munkavégzéshez szükségtelen tárgyak eltávolítására összpontosít. A válogatási folyamatban döntéseket kell hozni a munkavégzéshez szükséges, szükségtelen, talán nem szükségtelen tárgyakról. Ezen tevékenységen belül nemcsak a munkahelyi területek felszabadítása történik meg, hanem a hiányosságok, rendellenességek felmérése is.

Az elrendezés (Seiton) tevékenység a munkavégzéshez szükséges eszközök, gépek, berendezések hatékony elhelyezésére, tárolására fókuszál. Az elrendezés kialakításánál ügyelni kell a jól látható – könnyen és gyorsan elérhető – és visszatehető elvek betartására. Ez láthatóan már a munkafolyamat egyes mozzanatainak megértését és hatékony megszervezését igényli. A 5S módszer alkalmazása a csoportmunkán alapul, melynek kiemelkedő jelentősége van ebben a folyamatlépésben. Eredményeképpen körvonalazódik a munkaterület, az abban lévő tevékenységek, mozdulatok. Az elhelyezések megvalósításához a címkézés, színkódolás, számozás, különböző grafikai elemek alkalmazása szükségszerű.

A tisztítás, takarítás (Seiso) lépésen belül történik a berendezések, eszközök, szerszámok tisztításának, karbantartásának elvégzése. Olyan rendszer kidolgozás szükséges, amely hosszútávon biztosítja az eszközök rendelkezésre állását, épségét és megfelelő működését. Törekedni kell a munkaterület és az ahhoz tartozó tárgyak rendszeres ellenőrzésére, az esetleges változásokra, amelyek valamilyen rendellenességre utalhatnak, mint pl. szivárgás, sérülés, rossz beállítás.

Seiketshu, a szabványosítás. Célja, az első 3S lépésben elért eredmények fenntartása és folyamatos javítása. A rend, a tisztaság és a módszeresség folyamatossá tétele, a jó gyakorlat szabványosítása. Ebben a lépésben kell elkészíteni és kialakítani egy eljárásrendet a fenntartáshoz, amely tartalmazhat szemléket, ellenőrzéseket, értékeléseket, elismeréseket.

Shitsuke, a szinten tartás megvalósítása. Ez tulajdonképpen a fegyelmezett magatartást és morált jelenti a 4S megvalósításában. Elengedhetetlen alapja a megfelelő kommunikáció kialakítása, a feladatok, hatáskörök meghatározása. Ebben a folyamatlépésben történik a sikeres 5S bevezetés alapjául szolgáló vizuális tájékoztatási eszközök tervezése, készítése, elhelyezése. [2]

A helyes 5S-t megvalósító vállalat általában magas termelékenységgel (P), jó minőséggel (Q), alacsonyabb költségekkel (C), pontosabb szállítással (D), magas biztonsággal (S) és magas morállal (M) rendelkezik. Ez a hat előny a következő rövidítéssel ismert: PQCDSM. A termelékenység fejlesztés dimenziói:

- Termelékenység: a tervezett termelési célok elérése.

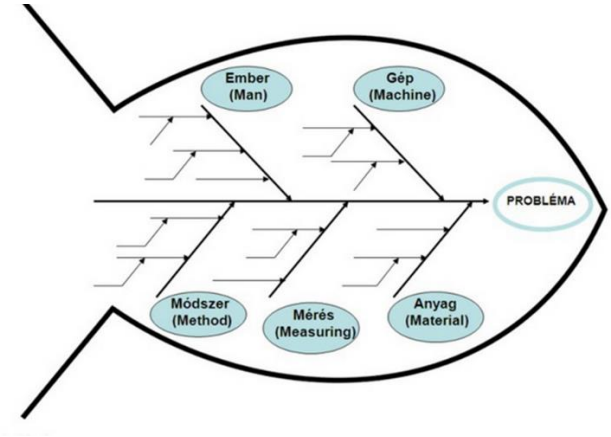
- Minőség: a termék és a folyamat minőségének javítása.
- Költség: a ráfordítási, karbantartási, javítási költségek csökkentése.
- Szállítás/határidő: a szállítási célok megismerése.
- Biztonság: a munkahelyi biztonság fenntartása.
- Morál/közszellem: a munkahelyi morál javítása, magasabb szintre emelése. [3, 4]

Összefoglalva a folyamat lépéseinek teljesítése nagy mennyiségű munkát igényel, ugyanakkor a befektetett erőforrások rövid idő alatt megtérülnek. Ipari, termelési környezetben az 5S módszer alkalmazásával csökkenthetők az átállási idők, a hibák, a keletkező hulladék, a késedelmes teljesítések, a munkahelyi balesetek, a meghibásodások. Mindezek hatalmas költségmegtakarítást jelentenek, a munkaszervezési folyamatok hatékonyságának javulása mellett. A munkaterületek biztonságos és ergonomikus kialakítása elősegíti a munkahelyi egészségvédelmet és biztonságot. Az eljárás megfelelő kialakítása, bevezetése mellett rendkívül fontos annak folyamatos fejlesztése, melynek alapja a rendszeres felülvizsgálat.

Gyökérok elemzés módszere

A minőségügyben alkalmazott minőségtechnikák különbözőképpen csoportosíthatóak attól függően, hogy milyen területen, milyen célra, milyen eredmények elérése érdekében alkalmazzák. Közös jellemzőjük, hogy alkalmazásuk csoportmunkán alapul. A problémamegoldás területén az úgynevezett hét régi, egyszerű minőségtechnika ismeretes, amelyek szisztematikus alkalmazásával a problémák nagy része megoldható, ezáltal a folyamatok javításában van nagy szerepük. A kockázatelemzés területén a minőségügyi eljárások a három egymást követő lépéshez rendelten alkalmazhatóak, ezek: kockázatazonosítás, kockázatelemzés és kockázatértékelés. A gyökérok elemzés (Root Cause Analysis) hatékony módszer a kockázatok elemzésének elvégzése során. Célja az okok feltérképezése és elemzése, az okok kapcsolatrendszerének megismerése, amely iránymutató a hibák előfordulásának csökkentésében és újbóli előfordulásuk megakadályozásában. Többféle minőségtechnika alkalmazható gyökérok feltárására, ezek közé tartozik az Ishikawa-diagram, a fa-diagram, az 5Miért? módszer stb.

Az egyik legelterjedtebb ok-okozati elemző módszer mindezek közül a halszálka-diagram, vagy más néven Ishikawa-diagram, melyet Dr. Kaoru Ishikawa 1943-ban publikált. Célja, hogy egy adott problémában szerepet játszó okokat feltérképezze. Az ehhez alkalmazott diagram leginkább egy hal testfelépítésére hasonlít, innen ered a halszálka-diagram elnevezése. Az 1. Ábrán látható grafikus megjelenítése miatt könnyen átlátható és értelmezhető. A megfelelő eredmény érdekében a csoportmunka ebben az esetben szükségszerű, hiszen a probléma vagy hiba létrejöttét széleskörűen feltérképezni úgy lehet, ha minél több szempontot, megközelítést figyelembe veszünk. Ezt úgynevezett keresztfunkcionális csoportösszetétel alkalmazásával lehet elérni, amely azt jelenti, hogy a csoport minden tagja más-más megközelítésből szemléli, elemzi az adott problémát. Így biztosítható a teljeskörű analízis. Az ok-okozati elemzés során meghatározásra kerülnek azok az okok, amelyek kapcsolatban állnak a következő elemekkel: ember, gép, módszer, mérés, környezet stb. [5]



1. Ábra: Halszálka-diagram, saját szerkesztés.

Az egyes kategóriákban fellelhető okokat a brainstorming módszer alkalmazásával kell meghatározni. Ezen úgynevezett főokok kerülnek az első szintre. Ezek további elemzésével folytatódik az alokok feltérképezése. A témával foglalkozó szakirodalmak többnyire az 5Miért? illetve az 5W+2H módszer alkalmazását javasolják. [6] A halszálka diagram általában más folyamatjavítási, -fejlesztésben ismeretes módszerekkel együtt hatékony, mint például a hibamód és -hatáselemzés, a különböző problémamegoldó módszerek (8D, A3). Eredményét tekintve hátránya, hogy nem mutatja a különböző kategóriákban lévő okok egymáshoz való viszonyát, kapcsolatát. [7]

A FELÜLETI ÉRDESSÉGMÉRÉS FOLYAMATÁNAK ELEMZÉSE

A felületi érdességmérés során a tapintótű törése meglehetősen gyakori. Mivel ez egy régóta fennálló probléma, igen nagy hangsúlyt kell fordítani annak megoldására. A probléma feltérképezéséhez elengedhetetlen a mérőgépet használó személyek véleményének, tapasztalatainak megismerése. Vizsgálatainkban azon oktatók és hallgatók véleményének megismerése és értékelése történt, akik az elmúlt időszakban használták a berendezést. Az oktatói felügyelet az első néhány mérés során, valamint a beoktatás során jellemző. Mindezek mellett a mérőgép használatára vonatkozó előírás, használati útmutató nem áll rendelkezésre, amely komoly probléma a tapasztalatlan mérőszemélyek esetében. A mérési folyamat teljeskörű elemzése és vizsgálata azért fontos, mert a felületi érdességmérés első pillanatától az utolsóig működésben van a tapintótű. Egy apró figyelmetlenség is komoly problémákhoz vezethet, amely eredménye lehet a tű sérülése. A nem kívánatos esemény – esetünkben a tapintótű sérülése, törése – létrejöttében szerepet játszó tényezők teljeskörű vizsgálatához ki kell terjeszteni az elemzést a mérési folyamatról a mérőgép közvetlen környezetére és a laborban alkalmazott szabályokra, szokásokra.

Célkitűzéseink között szerepelt a felületi érdességmérés kockázatainak csökkentése, a mérési folyamat javítása, a problémák csökkentése és a gép környezetére vonatkozó ajánlások kidolgozása az 5S módszer elvei alapján. Ezen szempontok alapján végeztük el az állapotfelmérést és annak dokumentálását. A Mahr Perthometer Concept mérőberendezés (2. Ábra) a koordináta méréstechnika laboratóriumban található. Az eszköz márványasztalon van elhelyezve, használaton kívüli állapotban portól és szennyeződéstől védeni

szükséges. A felületi érdességi paramétereket tartalmazó táblázat a mérést végző segítségére szolgál. A mérőeszközhöz tartozó számítógép kizárólag a méréshez szükséges szoftvert és adatokat tartalmazza. A mérőhely és annak környezete összességében jó állapotúnak minősíthető, a rendezettség megfelelő.

2. Ábra: Felületi érdességmérés környezete, saját szerkesztés.

A mérőhely közvetlen környezetének vizsgálati alapját az 5S módszer első lépésének szempontjai adták. A mérőhely és annak asztalán csak a méréshez elengedhetetlen tárgyak lehetnek. Ennek megfelelően a méréshez szükséges elemek meghatározása történt meg a mérőhely közvetlen környezetében. A könnyebb áttekinthetőség érdekében a felsorolt tárgyakat táblázatos rendszerbe rendeztük, amely a továbbiakban akár az ellenőrzések során is felhasználható (1. Táblázat).

Ssz.	Megnevezés	Méréshez szükséges?	Megfelelő helyen van?
1.	felületi érdességmérő berendezés	igen	igen
2.	számítógép és hardver eszközök	igen	igen
3.	paramétertáblázat (Mahr)	igen	igen
4.	instrukció alapvető mérési beállításokhoz	igen	nem
5.	csavarok, alkatrészek	nem	nem
6.	forgácsoló szerszámok	nem	nem
7.	fóliazsák	igen	igen
8.	íróeszközök	igen	nem

1. Táblázat: Szelektálás adatfelvétele a mérőhely környezetéről, saját szerkesztés.

A felmérés során megállapítottuk, hogy sok olyan tárgy található a mérőgép közvetlen környezetében, amelyeket a mérések során nem szükséges használni vagy egyáltalán nem tartoznak a mérőeszközhöz. Nem használt, régi alkatrészek, szerszámok, esetlegesen

szemét sok esetben akadályozza vagy lassítja a megfelelő (szükséges) eszközök, szerszámok megtalálását. Zárható dobozban tárolt eszköz kevéssé jellemző, továbbá a meglévők nem megfelelően feliratozottak. Gyakorlatilag a megfelelő eszközök kiválasztása azon alapul, hogy általában hol találjuk. Az egyedi mérések esetében azonban komoly kockázatot jelent a használónak, ha nem a megfelelő tapintótű, alkatrész, szerszám kerül alkalmazásra, ezzel kockáztatva a biztonságos mérés megvalósítását. Fontos megemlíteni azokat az alkatrészeket, melyek a géphez tartozó pótalkatrészek. A Mahr cég által gyártott gépek saját hatáskörben nem szerelhetők, javíthatók. Ugyanakkor a mindennapi munka során előfordulhatnak olyan apró állapotmegóvási céllal alkalmazott karbantartási feladatok melyek megengedettek. Pl. a mérőasztal csúszásának megakadályozását elősegítő csavarok kicserélésére. Akadnak ellenben olyan eszközök is melyek sérülékenyek még sincsenek megfelelő körülmények között tárolva. A rendezettség kialakításának érdekében az 5S módszer minden lépéséhez meghatároztuk azokat a feladatokat, amelyek elősegítik a jelenlegi állapot javítását.

- 1S – szelektálás: A mérőberendezéshez és a mérési folyamathoz tartozó eszközök összeállítása. Ezen listában méréshez szükséges, vagy feltételesen szükséges elemek vannak felsorolva. A formai kialakításnak lehetővé kell tennie, hogy bármely mérőszemély könnyen és gyorsan ellenőrizhesse, hogy az előírtaknak megfelelő eszközök rendelkezésre állnak. A mérőhelyhez tartozó fiókos rekeszek tartalmáról fényképes piktogramok felhelyezése javasolt. Így már kinyitás nélkül kívülről is láthatóak a benne lévő elemek. Minden egyéb eszköz, alkatrész, szerszám, munkadarab stb. eltávolítása következik a mérőhely rendezettségének kialakítására.
- 2S – elrendezés: A mérőgép kialakítása meghatározott, csak azok az elemek tárolását kell megoldani, amik a különböző mérési feladatok miatt más-más eszközt igényelnek, így a tapintótű, a mérendő munkadarab felhelyezésére és rögzítésére szolgáló alkatrészek, a kalibrálási folyamat elvégzéséhez szükséges etalonok. A mérőasztal tehát alap állapotban üres, minden más a méréshez szükséges darabot a mérőasztal fiókjai tartalmaznak. A szelektálás befejezése után az egyes darabok jól elkülöníthető módon, tárolódobozokban, feliratozva, fényképpel ellátva tárolandók. A mérőeszköz tapintói és a tapintó felszereléséhez tartozó szerszámok elhelyezése a megfelelő információtartalommal erre a célra kialakított formázott szivacsbetétekben történjen.
- 3S – tisztítás: a mérések többnyire forgácsolással megmunkált felületeken történik. A munkadarabok fémek vagy műanyagok. A mérendő felületet minden esetben meg kell tisztítani az esetleges forgácsdaraboktól, ezért előfordul, hogy a mérőhely forgáccsal szennyezett. A mérőgép és az alkatrészasztal tisztítására és a mérőeszköz megfelelő tárolására vonatkozóan készül egy karbantartási előírás, ami minden esetben kötelező.
- 4S – Szabványosítás: Az egyes dokumentációk kidolgozásánál törekedtünk az egyszerűségre. Ennek alapvető oka, hogy az 5S rendszer bevezetésével nem célunk a mérési folyamat lassítása, esetleges akadályozása, a túlzott adminisztráció. A vizuálmenedzsment egyes elemei nagyon hatékonyan alkalmazhatók ilyen esetekben.
- 5S – Szinten tartás: Az elért rendezettség és annak szisztematikus betartása csak úgy valósítható meg, ha a mérőszemélyek minden esetben megismerik a szabályokat. Így a mérőeszköz oktatásánál az 5S rendszer elemeire is ki kell térni. Továbbá

a rendszeres ellenőrzés növeli a rendezettség hosszútávú fennmaradását, amelynek felelőse a laborvezető.

Az 5S rendszer alapján kidolgozott ajánlások nagy mértékben növelhetik a mérések hibamentességét, biztonságosságát és hatékonyságát, amelyekkel minimalizálhatók vagy elkerülhetők a környezeti hatásokból adódó hibák. Alkalmazásuk könnyen, gyorsan kivitelezhető és költséghatékony.

Felületi érdességmérés folyamata és elemzése a tapintótörés szempontjából

A felületi érdességmérő berendezés használatának folyamatát 23 lépésben határoztuk meg, amelyek alapvetően az alábbi három fő szakaszra osztható:

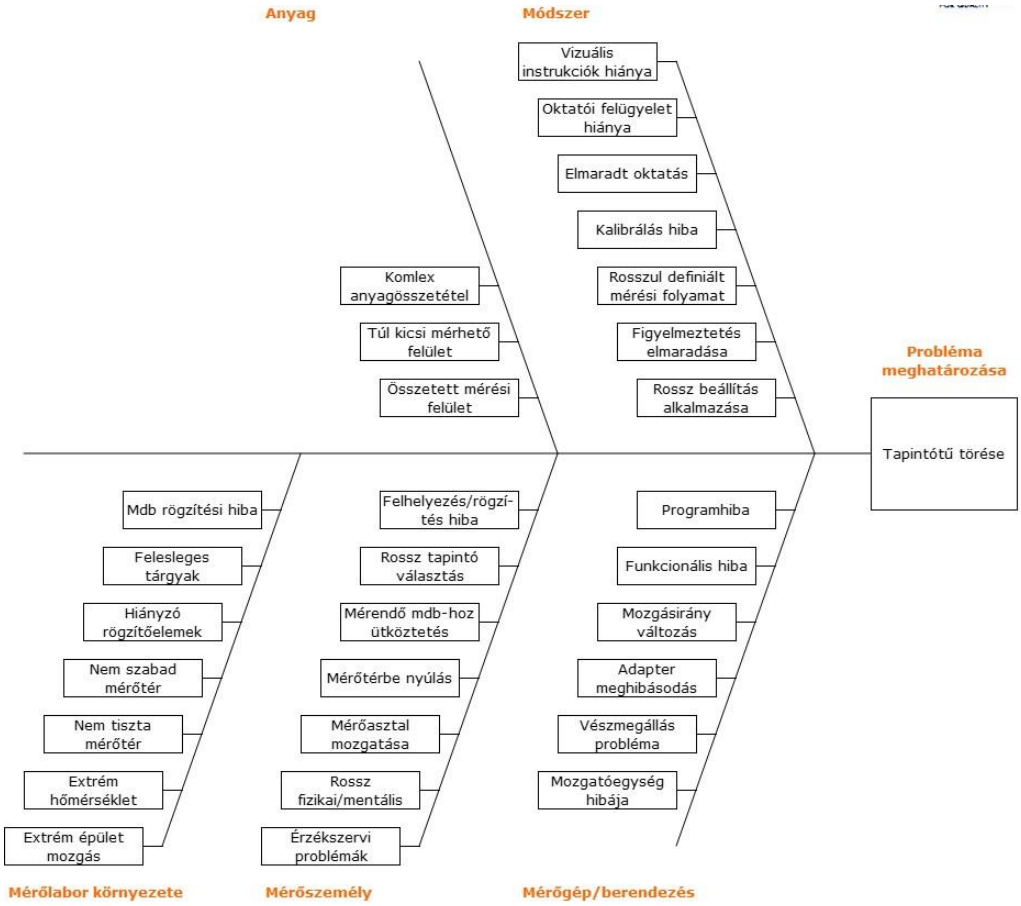
- A mérés előkészítése (mérőhely, mérőberendezés, mérendő alkatrész).
- Mérés (beállítási feladatok, programkezelés).
- A mérés befejezése (mérőgép lezárása, mérendő alkatrész eltávolítása, mérőhely).

Az első szakaszban a mérés előkészítése történik meg, amely magában foglalja a mérőeszköz és annak környezetének szemrevételezéssel történő ellenőrzését, a takarófólia eltávolítását, valamint a munkadarabasztal előkészítését. Attól függően, hogy milyen típusú érdességmérés következik, a méréshez megfelelő tapintó kiválasztását és beszerelését kell elvégezni. A munkadarab mérendő felületét meg kell tisztítani és a megfelelő pozícióba fel kell helyezni. A mérés megkezdése előtt az ellenőrzés elengedhetetlen, mely során meg kell győződni a tapintó és a munkadarab megfelelő helyzetéről, az ütközés elkerülése érdekében.

A következő folyamszakasz a mérések elvégzése. A Mahr Perthometer Concept működése számítógépes programmal segített. A rendelkezésre álló programok alkalmasak a felület 2D-s és 3D-s érdesség vizsgálatára. A szoftver magyar nyelven is elérhető, így a mérőszemély lépésről lépésre elvégezheti a műveleteket és a mérési eredmények kiértékelését is. A kritikus lépések ebben a szakaszban a referenciapontra járatás és a tapintótű felületre helyezése. Ez nagy figyelmet és óvatosságot kíván meg a mérőszemélytől. A mérőgép kezelő program lehetőséget ad az automatikus a tapintásra, ezzel a tapintó csúcsa a mérendő felületre fekszik fel. A mérési paraméterek beállítása során lehet kiválasztani az előfutást, a tapintás hosszát és az utánfutást. Szükséges meggyőződni arról, hogy a beállított mozgásokhoz elegendő hely áll rendelkezésre majd, ezt követően indítható a mérés. Amennyiben a mérőtű elő- vagy utánfutásához nincs elegendő hely, két megoldás alkalmazható. Az egyik, hogy a mérendő felületet más helyről közelítjük meg, a másik, hogy az előfutás lehetőségét kikapcsoljuk. A rendkívül érzékegy szerkezet miatt a tapintótű képes felvenni az épület vagy a mérőasztal rezgését, lengését, és azt a mérés során a felületre rámásolni, amellyel a mérés pontossága, precizitása torzul. Ezért a mérés ideje alatt az asztalhoz érni vagy azt mozgatni tilos.

A mérés befejezése során elkészíthető a mérési jegyzőkönyv és kiemelhető a tapintó biztonságos magasságba. Az alkatrésztartó asztal kihúzása során ügyelni kell arra, hogy az alkatrész biztonságosan eltávolítható legyen. Ezután a tű horizontális visszahúzása következik pozitív irányba, azaz az alkatrésztartó asztallal ellentétesen. A mérőgép leállása automatikusan történik, a mérőszemély feladata a tapintó kiszerelése és alaphelyzetbe állítása. A mérőhely környezetét a tisztaság és a biztonság szempontjait szem előtt tartva megfelelő módon kell lezárni.

A gyökérok elemzés alapját az előbb ismertetett folyamat adta. Az elemzés során a folyamat minden egyes lépését megvizsgálva rögzítettük a lehetséges okokat, majd azokat halszálka-diagramban ábrázoltuk (3. Ábra).



3. Ábra: Tapintótű törésének ok-okozati elemzése, saját szerkesztés.

Az elemzéshez meghatározott kategóriák jól illeszkednek a felületi érdességmérés folyamatához, melyek: anyag, módszer, környezet, személy, berendezés voltak. A mérőberendezés és a program esetleges hibája potenciális okként szerepel, de jelentőségét tekintve nem meghatározó, ugyanis az ilyen jellegű problémák bekövetkezésének valószínűségét a program biztonsági funkciói minimalizálják. Az egyes kategóriákon belül felvett okok vizsgálata során arra a megállapításra jutottunk, hogy a mérőszeméllyel kapcsolatos problémák nagy jelentőséggel bírnak a tapintó törésének bekövetkezésére. A mérés módszerének és a labor környezetének kialakításához emberi beavatkozás szükséges, úgyhogy bár külön kategóriába tartoznak, összefüggés tapasztalható a mérést végző személlyel. Elemzéseink alapján, melyhez figyelembe vettük az elmúlt évek tapasztalatait is, arra a következtetésre jutottunk, hogy a probléma előidézésében szerepet játszó okok között a legnagyobb befolyással az emberi tévedés, mulasztás, figyelmetlenség, esetlegesen szándékosság áll. A kutatómunkánk további részében tehát erre összpontosítottunk.

JAVASLATOK A PROBLÉMA MEGOLDÁSÁRA

A felületi érdességmérés ok-okozati elemzés összhangban állt a korábbi időszakban tapasztaltakkal és egyértelműan kijelenthető, hogy az emberi tényező áll első helyen a probléma leggyakoribb okai között. A következő lépésben sorra vettük azokat a megoldási lehetőségeket, amelyek csökkenthetik a tapintó törését befolyásoló tényezőket és több szempont alapján a mérési protokoll kidolgozása mellett döntöttünk. A mérési protokoll célja, hogy a felület érdességmérő gépen történő mérés menetét bemutassa, kiemelje azon kritikus pontokat, ahol fokozott figyelem szükséges, és ezeken a pontokon információt és tanácsot nyújtson a hibák megelőzésére, elkerülésére. Összeállításakor fontos szempont volt, hogy odafigyeljünk annak szerkezetére, könnyű értelmezhetőségére. Egy átlátható, jól követhető folyamatleírás hathatós segítséget jelenthet minden felhasználó számára. Javaslataink a kidolgozásra vonatkozóan a következők voltak:

- A folyamat egyes lépéseit leíró folyamatábra értelmezhetőségét jól látható, könnyen értelmezhető ábrák, képek segítsék. A kritikus lépéseknél figyelmeztető jelzések jelezzék a felhasználó számára a hibázás elkerülésének módját. A fontosnak vélt információkat kiemelése szükséges, például a „FONTOS!” vagy „FIGYELEM!” feliratok elhelyezésével.
- A jellegzetes mérési folyamatokra, mint például a forgácsolt felület mikrogeometriai vagy topográfiai mérése, általános útmutató készült, amely a számítógépen megtalálható. Tekintettel arra, hogy a mérőeszközt nem csak magyar nyelvű hallgatók is használhatják, ezen leírások angol nyelven történő biztosítása is szükséges.

A folyamatjavításban alkalmazott minőségügyi módszerek nagyon hatékonyak lehetnek, ha a célnak megfelelőt alkalmazzuk. A mérési folyamat elemzése és a tapintó törés okainak kivizsgálására alkalmazott halszálka diagram jól illusztrálta, hogy az emberi figyelmetlenség minimalizálásával sok esetben kiküszöbölhető a probléma. A folyamatábra hathatós segítséget nyújtott a mérési folyamat részletes megismerésében és irányt mutatott a kritikus lépések meghatározásában. A rendezett környezet kialakítása és fenntartása pedig jó alapot szolgáltat a javasolt intézkedések meghozatalára. Annak érdekében, hogy az ember által okozott hibákat visszaszorítsuk, a mérőgépen méréseket végző személyek oktatására nagyobb hangsúlyt kell fektetni. Jelenleg a program kezelésére szolgáló útmutató áll rendelkezésre, amely elsősorban az egyes beállítások jellemzőire fókuszál. A gép használatát megelőző oktatóanyag nem elegendő a megfelelő szaktudás elsajátításához. Szükség van ezen túlmenően bővebb oktatási segédletre, melyeket nem csak biztosítani kell, hanem számon is kell kérni valamilyen formában. Egy olyan segédlet, amely az előzetes oktatást alapul véve elmélyíti az egyéni tudást. Továbbá, melyben maga a gép használata sokkal körültekintőbben részletezett, a gyakorlati mérések menetét erősíti és a hibák elkerülését hangsúlyozza.

ÖSSZEFOGLALÁS

Cikkünkben azt problémát elemeztük, amely az Intézményünkben található Mahr Perthometer Concept felület érdességmérő gép tapintóegységének meghibásodására vonatkozik. Vizsgálataink céljai között szerepelt a tapintó töréséhez vezető hibák, hibaokok feltárása, továbbá ezek kiküszöbölésére tett javaslatok kidolgozása annak érdekében, hogy a mérési folyamatot biztonságossá és hibamentessé tegyük, a mérés során bekövetkezett

problémák számát csökkentsük. A mérés folyamatát lépésről lépésre elemezve megállapítottuk a lehetséges okokat, amelyek a tapintó töréséhez vezethetnek. Majd kidolgoztunk javaslatokat, amelyekkel megelőzhetőek, csökkenthetőek vagy megszüntethetőek, egyszersmind biztonságossá tehetők a mérések. Az 5S módszer hatékony a rendezett környezeti kultúra kialakításához, ezért célravezető a labor környezetének javításához ezen módszer alkalmazása. A mérési folyamatok egyedi azonosítására is van lehetőség saját profil létrahozásával. Ezen belül egyedi mérési beállítások, jegyzőkönyvformátumok készíthetők, a szoftver automatikusan naplózza a mérések időpontjait. Ahhoz, hogy mindig a megfelelő programot és annak beállításait használja a felhasználó elengedhetetlen, hogy pontosan megismerje a mikrogeometriai (2D) illetve a mikrotopográfiai (3D) mérési eljárásokat. A folyamat kritikus lépéseinél a mérőszemély hibázási lehetősége mindig megjelenik. A mérőszemély képzetlensége, tapasztalatlansága, figyelmetlensége meglehetősen sok veszélyt hordoz magában. Ez az a terület, amire különös figyelemmel kell lenni. A használat előtti oktatásra és segédlet kidolgozására nagyobb hangsúlyt kell fektetni. Továbbá a mérési protokoll kidolgozása és alkalmazása folyamatos segítséget nyújt a mérés során is. E két fejlesztési terület hatékonyan segít a tapintó törések elkerülésében. A mérőlabor használatára kidolgozott 5S rendszer elősegíti a mérőgépek és tartozékainak biztonságosságát, egyben biztosítja az átláthatóságot és az ellenőrizhetőséget. Költséghatékony megoldás és mindemellett elősegíti a súlyos károkozás bekövetkezésének csökkentését is.

FELHASZNÁLT IRODALOM

[1] D. F. Gomes, M. P. Lopes, and C. Vaz de Carvalho, “Serious Games for Lean Manufacturing: The 5S Game”, *IEEE revista iberoamericana de tecnologias del aprendizaje*, vol. 8, no. 4, pp. 191–196, Nov. 2013, doi: 10.1109/RITA.2013.2284955

[2] M. Jiménez, L. Romero, M. Domínguez, M. Espinosa, “5S methodology implementation in the laboratories of an industrial engineering university school”, *Safety Science*, vol. 78, pp. 163–172, Oct. 2015, doi: https://doi.org/10.1016/j.ssci.2015.04.022.

[3] A. Mittal, P. Gupta, V. Kumar and C. Chun Ki Chan, “The application of quality control circle to improve the PQCDSM quality parameters: a case study”, *International Journal of Productivity and Quality Management*, vol. 40, issue 1, pp. 102–119, Sept. 2023, doi: https://doi.org/10.1504/IJPQM.2023.133422

[4] L. Liliana, “A new model of Ishikawa diagram for quality assessment”, In: 20th Innovative Manufacturing Engineering and Energy Conference (IManEE 2016), IOP Conf. Ser.: Mater. Sci. Eng. 161 012099, doi: 10.1088/1757-899X/161/1/012099

[5] B. Neystani, “Seven Basic Tools of Quality Control: The Appropriate Techniques for Solving Quality Problems in the Organizations”, *Quality Problems in the Organizations*, pp. 1–10, 2017, doi: http://dx.doi.org/10.2139/ssrn.2955721

[6] V. M. Magar and Dr. V. B. Shinde, “Application of 7 Quality Control (7 QC) Tools for Continuous Improvement of Manufacturing Processes”, *International Journal of Engineering Research and General Science*, vol 2, issue 4, pp. 364–371, June-July 2014, ISSN 2091-2730

[7] M. Agrawal, “Impact of Ishikawa on the analysis of data in mechanical industries”, Materials Today: Proceedings, vol. 81, part 2, pp. 1040–1045, 2023, doi: https://doi.org/10.1016/j.matpr.2021.04.376.

OPTIMIZED MULTI-STAGE CRASHBOX STRUCTURE FOR LOW SPEED COLLISION

ALACSONY ÜTKÖZÉSI SEBESSÉGRE OPTIMALIZÁLT TÖBBTAGÚ CRASHBOX SZERKEZET

KERTÉSZ József[1] – KOVÁCS Tünde Anna[2]

Abstract

One of the most common collisions is the head-on collision, which occurs mainly on congested inner-city and access roads. These are mostly low-speed collisions, but can cause personal injuries to vehicle occupants that can lead to long-term health damage, such as whiplash injuries. More efficient impact energy absorption can improve the safety of vehicle occupants. This paper presents the design and application potential of an optimised multi-member crashbox for use in bumper systems and underrun protection systems. The structure is integrated with an absorber filler (e.g. metal foam) and is suitable for deformation transmission. Thanks to the multi-member design, the peak crushing force typical of conventional thin-walled structures can be significantly reduced, allowing energy absorption to start sooner by the crashbox structure.

Keywords

crashbox, bumper system, metal foam, absorption, crashworthiness

Absztrakt

Az egyik leggyakoribb ütközés a ráfutásos baleset, amely elsősorban a zsúfolt belvárosi és bevezető szakaszokon történik. Ezek legtöbbször alacsony sebességű ütközések, viszont olyan személyi sérüléseket is okozhat a járműben utazókban, hogy azok akár hosszútávú egészségkárosodáshoz is vezethetnek. Hatékonyabb ütközési energia abszorpcióval növelhetjük a járműben utazók biztonságát. Jelen tanulmány egy olyan lökhárító rendszerekben és aláfutásgátló rendszerekben alkalmazható optimalizált többtagú crashbox (gyűrődő elem) konstrukcióját és alkalmazási lehetőségét mutatja be. A konstrukció abszorber töltettel (pl. fémhab) integrált, és deformációs áttétel megvalósítására alkalmas. A több tagú kialakításnak köszönhetően a hagyományos vékonyfalú szerkezetekre jellemző gyűrődési csúcserő jelentősen csökkenthető, így az energia abszorpció hamarabb elkezdődhet a crashbox szerkezet által.

Kulcsszavak

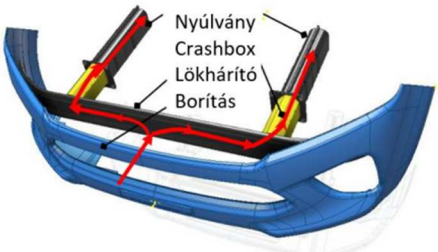
crashbox, lökhárító rendszer, fémhab, abszorpció, ütközésbiztonság

[1] kertesz.jozsef@eng.unideb.hu | ORCID: 0000-0001-9544-3135 | Ph.D. student, Óbuda University Doctoral School on Safety and Security Science | Ph.D. hallgató, Óbudai Egyetem Biztonságtudományi Doktori Iskola

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

BEVEZETÉS

8 km/h és 16 km/h közötti ütközési sebesség tartományában a jármű elejére és hátuljára szerelt lökhárító felel az ütközési energia abszorpcióért. Nemzetközi előírásoknak megfelelően ebben a tartományban a jármű fő részegységei mint pl. az alváz (nyúlvány) nem sérülhetnek [1-5]. Ez azt jelenti, hogy az energia abszorpció jelentős részét a lökhárító rendszer részét képező crashbox szerkezetnek kell megoldania. A lökhárító rendszer könnyen, oldható kötésekkel szerelt és cserélhető passzívbiztonsági konstrukció, melyek nagymértékben gyorsítják a káresemény utáni javítást és a javítási költségek alacsonyabban tarthatók[6-8]. A lökhárító rendszer három fő részre különíthető el: kereszttartó, crashbox szerkezet és felfogatás. Ezek közül az energia abszorpció tekintetében kiemelt fontosságú a crashbox. A crashbox egy vékonyfalú szerkezetnek tekinthető konstrukció, amely alak és méret sajátosságainak köszönhetően programozható gyűrődési jellemzőkkel bír[9-11]. Az 1. ábra a lökhárító rendszer elemeit mutatja.



1. Ábra: Lökhárító rendszer felépítése [Saját szerkesztés]

A crashbox által elnyelt energia függ a szerkezet falvastagságától, keresztmetszeti jellemzőitől és az alkalmazott anyag mechanikai és szilárdságtani jellemzőitől[12-14]. Természetesen az energia elnyelő képesség fokozható a falvastagság növelésével, viszont a passzívbiztonsági rendszerek fejlesztése során, ha nem is primer, de fontos szempont a tömegoptimalizáció is. A crashbox szerkezetek gyűrődési jellemzőiről általánosan megfogalmazható, hogy a lineárisan rugalmas szakasz, egy csúcserőt (folyási értéket) elérve nagy mértékű erő fluktuáció mellett harmonika elven zömül, a teljes roncsolódásig[15-16]. A szerkezet zömítéséhez szükséges energia megegyezik a káreseményben felemésztett energiával.

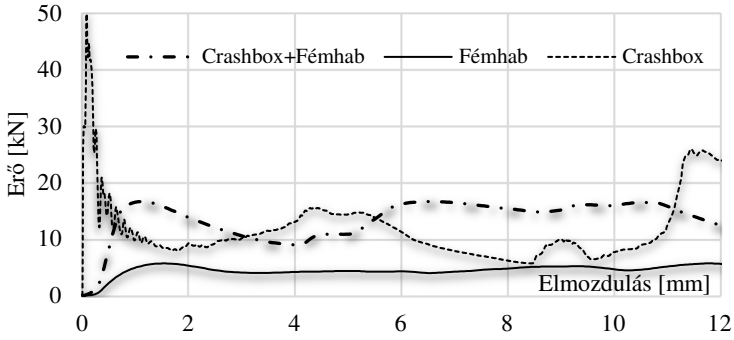
VIZSGÁLATI MÓDSZER

A következőkben bemutatott megoldás egyszerűsített változata (próbadarab) elkészítése és mérése anyagvizsgálati laborban történt. A zömítési vizsgálatot Instron 8801 szervo-hidraulikus anyagvizsgáló gépen végeztem el, ahol vizsgáltam az elnyelt energia mennyiséget és a gyűrődés során jelentkező erőviszonyokat. A megoldást többféle variációban szereltük össze és került lemérésre, hogy a szerkezet működéséről és annak jóságáról információt kapjunk, valamint, hogy a kutatás kezdetén megfogalmazott hipotézist igazolni tudjuk. igazolják. Minden konstrukció változatot többször mértük le, hogy a kapott értékek validálhatók legyenek. A vizsgálatokat 1mm/s-al végeztük, és az erőmérő cellák védelme érdekében 100kN-s erő maximumban limitáltuk. A szerkezetek gyűrődésük során elnyelt

energia meghatározásához az gyűrődési erőt rögzítettük az elmozdulás függvényében 100 Hz mintavételi frekvencia mellett.

FÉMHAB, MINT ENERGIA ABSZORBER

Léteznek olyan anyagok, melyek szerkezeti sajátosságaiknak köszönthetően ideális energiaelnyelőknek tekinthetők. Ilyenek pl. a porózus szerkezetű fémek, kompozitok, úgynevezett fémhabok. Porozitásuk függvényében a lineáris elasztikus szakaszt egy egyenletes energia elnyelési zóna, az úgy nevezett plató szakasz(közel állandó erő melletti deformáció) követ, amely az energia abszorpció szempontjából kiemelten fontos annak egyenletessége miatt [17-19]. A crashbox pl. fémhab tömbökkel helyettesíthető lenne, azonban a szabad zömítéshez képest nagyságrendileg 30%-al több energiát képest megköti, ha deformációja radiálisan gátolva van[20-23]. Ezért gyakran alkalmazott megoldás a zártcellás fémhabokkal integrált crashbox szerkezet, vagyis a fémhabbal töltött crashbox. Gyűrődése során nem csak a crashbox szerkezet folyamatos roncsolódása, de a benne lévő fémhab zömítése is energiát emészt fel, ezzel növelve a konstrukció energia elnyelő képességét[24]. Az elnyelt energia mennyisége ugyan fokozható fémhab integrációval, azonban az alkalmazott abszorber előnyös gyűrődési jellemzőit – mint pl. plató szakasz - elveszítjük, mivel az elsődleges teherviselő a vékonyfalú szerkezet. A vékonyfalú szerkezet törése egy csúcserővel indul, majd jelentős erő fluktuáció mellett folytatódik a zömülése egészen a felkeményedésig[25-26]. Ez a hátrányos erő fluktuáció figyelhető meg a 2. ábrán , ahol azt láthatjuk, hogyan alakulnak az energia görbék önálló hab zömítés és a crashbox-al együttes zömülés esetén.



2. Ábra: Gyűrődési karakterisztika különböző energia elnyelő konstrukció esetén [Saját szerkesztés]

A FEJLESZTETT KONSTRUKCIÓ MŰKÖDÉSI ELVE

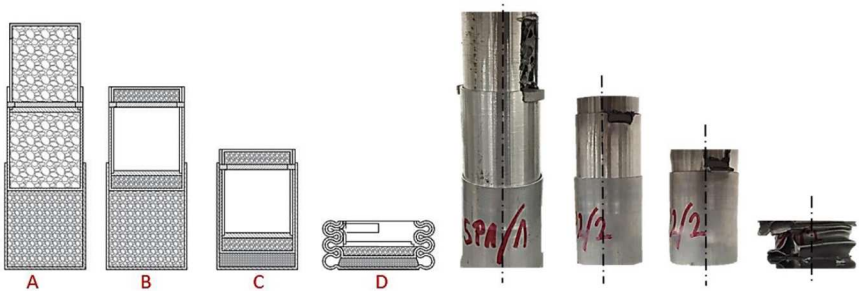
Az optimalizált, abszorberrel (lattice szerkezet, fémhabok, kompozitok) integrált crashbox szerkezet több elemből tevődik össze, ennek köszönhetően az alkalmazott abszorber és a vékonyfalú szerkezet zömülése a törés során elkülöníthető, ezáltal egy modulálható energia elnyelőt kapunk. Mivel az abszorber a crashbox-on belül kerül zömítésre, annak deformációja radiálisan gátolt többtengelyű feszültség állapotnak tekinthető. A crashbox gyűrődése során először a benne található abszorber zömül, majd annak teljes deformációját elérve megkezdődhet a vékonyfalú szerkezet gyűrődése, melynek jellemzőit a gyakorlatban már alkalmazott és ismert alak- és méret optimalizációval befolyásolhatunk, amely a talál-

mány működése szempontjából nem releváns. A szerkezet lehetőséget ad különböző sűrűségű, típusú abszorberek egyidejű és elkülöníthető zömítésére is. A különböző típusú/sűrűségű abszorberek alkalmazásának gyakorlati jelentősége, hogy a nagyobb sűrűségű abszorber csak nagyobb energiájú ütközések esetén lép működésbe. A különböző típusú és abszorpciós képességű abszorbereknek köszönhetően modulálható a crashbox szerkezet és az aktuális jármű tömegéhez és jellegéhez igazíthatjuk. (Nagyobb tömegű jármű, nagyobb mozgási energiát eredményez, vagyis nagyobb energia megkötésre alkalmas abszorber szükséges.) Részleges zömülése mellett elegendő csak az abszorber cseréje, nem szükséges a teljes szerkezetet cserélni/ javítani. Az abszorberek által elnyelt energia arányos azok deformációjával. Ez azt jelenti, hogy egységnyi gyűrődéshez egységnyi abszorber zömülés tartozik a hagyományos, korábban alkalmazott crashbox szerkezetek esetében. Az optimalizált crashbox azonban többtagú teleszkóp szerkezetként működik, ez pedig lehetőséget ad arra, hogy egységnyi gyűrődéssel a konstrukción belül kétszeres zömülést hozzunk létre az abszorberre vonatkozóan növelve ezzel az elnyelt energia mennyiségét, vagyis a jármű lassulása és ezáltal a káresemény következményei csökkenthetők. Az ütközésbiztonságra vonatkozó nemzetközi előírások értelmében átlagosan 8km/h-s ütközési sebességig a jármű nem szenvedhet jelentősebb deformációt. (A felületi karcolásoktól, műanyag elemek repedésétől eltekintve.) Ez a követelmény jelen megoldásban a tagok egymáshoz viszonyított szilárd/átmeneti illesztésével esetleg ragasztásával oldható meg. A szilárd illesztésnek köszönhetően a tagok egymáson való elmozdulása során a köztük ébredő súrlódás is növeli az elnyelt energia mennyiségét. Jelen megoldás alapján két fő konstrukciót fejlesztettünk ,adott konstrukción belül pedig kétféle változatot dolgoztunk ki. Azonban mind a négy a következőkben bemutatott szerkezet működési elve azonos, vagyis modulálhatók, és a deformáció áttételezés elvén működnek.

Konstrukció működés

A fent részletezett megoldás alapján két fő konstrukció született. Adott konstrukción belül pedig kétféle változatot dolgoztunk ki. Azonban mind a négy bemutatott szerkezet működési elve azonos, vagyis modulálhatók, és a deformáció áttételezés elvén működnek.

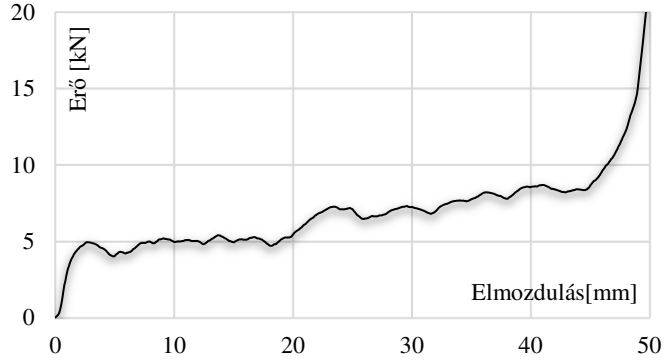
A fejlesztett konstrukció működését a 3.ábra mutatja be, amely 2D nézetben és a validálás során készített fényképeken keresztül is megfigyelhető. A technikai rajzon a ritkább sraffozás alacsonyabb sűrűségű, a sűrűbb sraffozás pedig a nagyobb sűrűségű/teljesítményű abszorbert jelképezi.



3. Ábra: a 1.sz. konstrukció gyűrődési lépései (eltérő abszorberek esetén) [Saját szerkesztés]

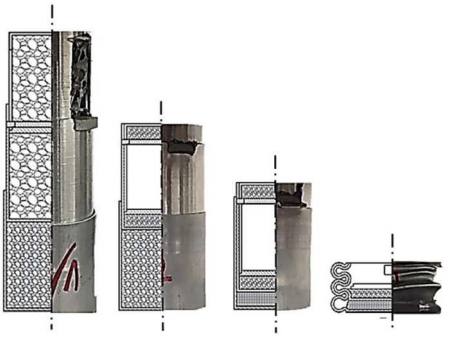
Az alapfázis (A) esetén a felső két tagban alacsonyabb sűrűségű/teljesítményű abszorber, az alsó tagban nagyobb sűrűségű/teljesítményű abszorber található. Az abszorber töltet fajtája nem rögzített, az lehet fémhab, kompozit vagy akár lattice szerkezet, esetleg ezek együttese. A részleges gyűrődés fázisban (B) az alacsonyabb sűrűségű/teljesítményű abszorberek zömülése történik. A teleszkóp szerkezet révén és a konstrukció kialakítása miatt egységnyi crashbox hosszváltozáshoz kétszeres abszorber zömülés tartozik. Ennek részletezése egy későbbi fejezetben olvasható. Ezen fázis végéig a szerkezet szétszerelhető és felújítható marad, az abszorber cserélhető. A részleges gyűrődési fázist a C-zömülési fázis követi, amikoris a „B" szakasz végén a felső abszorberek elérték a teljes zömült állapotot, megkezdődik a nagyobb sűrűségű/teljesítményű abszorber zömülése.

Az alacsonyabb sűrűségű abszorberek felkeményedése egybe esik a nagyobb sűrűségű/teljesítményű abszorber lineáris elasztikus szakaszával. Ezt a jelenséget a fejlesztés részeként végzett fémhab zömítési vizsgálataink is igazolják, ahol különböző sűrűségű alumínium habból készült próbatesteket egymásra helyezve vetettük alá terhelésnek. Az így kapott diagramot az 4. ábra mutatja, ahol jól megfigyelhető és elkülöníthetők az egyes habok zömülési fázisa. 20mm-es elmozdulásig figyelhető meg az alacsonyabb sűrűségű (0,4g/cm^3) plató szakasza, amely ezt követően el kezd felkeményedni. Ez a szakasz azonban már a nagyobb sűrűségű hab (0,7g/cm^3) lineárisan rugalmas deformációjával esik egybe. 23 mm-től megkezdődik a nagyobb sűrűségű hab plasztikus deformációja, vagyis egy magasabb energiaszintű plató szakasz, amely 45mm elmozdulásig tart.

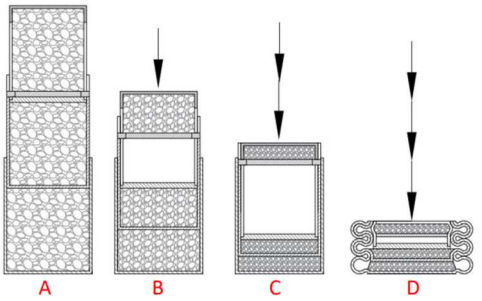


4. Ábra: Különböző sűrűségű fémhabok egyidejű zömítése egymásra helyezve [Saját szerkesztés]

A „C" szakasz a nagyobb sűrűségű/teljesítményű abszorber teljes felkeményedésével zárul, a tagok teljes mértékbe egymásba csúsznak. Ezen fázis végéig a szerkezet továbbra is szétszerelhető és felújítható marad, az abszorber töltet cserélhető. Amennyiben az alsó tagban is azonos sűrűségű/teljesítményű abszorbert alkalmazunk, akkor a „B" és a „C" fázis egybe esik. A „D" szakaszban a vékonyfalú szerkezet gyűrődése kezdődik meg, melynek működőképes falvastagsága immáron a három, egymásba csúszott tag falvastagságának összegével egyezik meg. A vékonyfalú szerkezet plasztikus deformációja már csak akkor valósul meg, ha az előző deformációs fázisokban az energia abszorpció nem teljesült maradéktalanul, vagyis az ütközési energia nagyobb volt, mint amennyit az abszorberek képesek lettek volna elnyelni. A konstrukció működési lépéseit mutatja be a 5. ábra, félnézet-félmetszet formában.



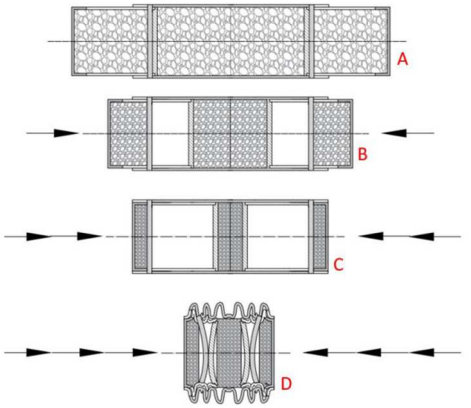
5. Ábra: Az 1.sz. konstrukció működése félnézet-félmetszetben [Saját szerkesztés]



6. Ábra: 1.sz. konstrukció gyűrődési lépései (azonos abszorberek esetén) [Saját szerkesztés]

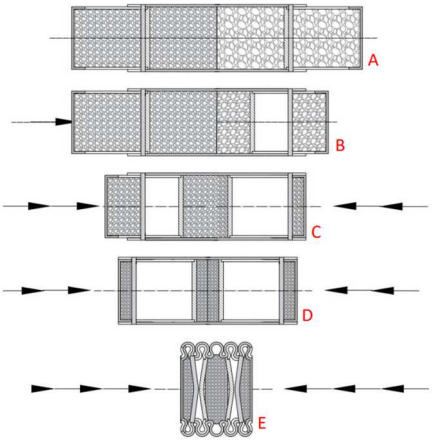
Az 6. ábra olyan változatot mutat, ahol mindhárom tagban azonos sűrűségű/teljesítményű abszorber található. A szerkezet működése azonos, de az egyes fázisokban történő zömülések eltérnek. A „B" részleges gyűrődési fázisban ugyanis mindhárom abszorber zömülése egyidejűleg történik. A „C" szakasz az abszorberek teljes felkeményedésével zárul, a tagok teljes mértékbe egymásba csúsznak. A „D" szakaszban hasonlóan a vékonyfalú szerkezet gyűrődése kezdődik meg az ütközési energia maradvány révén.

A fejlesztés során kidolgoztunk egy olyan konstrukciós változatot is, amely ugyan nagyobb konstrukciós térfogattal bír, azonban az abszorber töltet zömítése két irányból történik. Ezt a koncepciót mutatja be az 7. ábra.



7. Ábra: 2.sz. konstrukció gyűrődési lépései (azonos abszorberek esetén) [Saját szerkesztés]

A két szélső és a középső tagban is egyaránt azonos sűrűségű/teljesítményű abszorber található. A középső és szélső tag átmeneti/szilárd illesztéssel szerelt, vagy ehhez ragasztástechnikai módszer is alkalmazható. Ragasztás esetében az energia abszorpció kezdetét a kötés nyírásához szükséges erő határozza meg, míg szilárd illesztésnél a fedés mértéke. A konstrukció működésbe lépésének és mozgásban való tartásának feltétele a abszorber és a crashbox fala közötti, valamint a tagok közötti nyugvó és dinamikus súrlódás leküzdése. Természetesen ez a konstrukció modulálható különböző abszorberek egyidejű alkalmazásával, ahogy azt a 8. ábra és a 9. ábra is mutatja.



8. Ábra: 2.sz. konstrukció gyűrődési lépései (eltérő abszorberek esetén) [Saját szerkesztés]

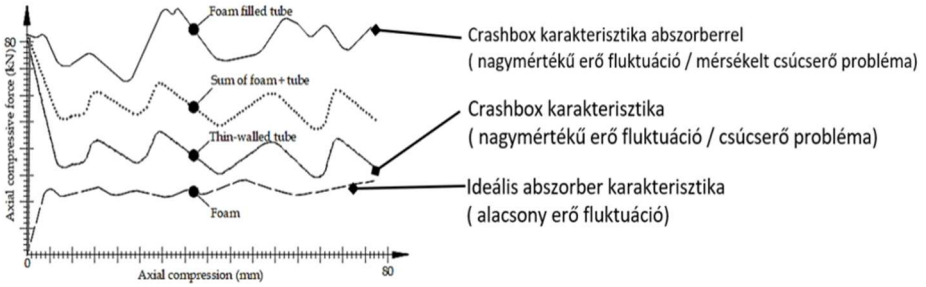
9. Ábra: 2.sz. konstrukció gyűrődési lépései pillanatképekben [Saját szerkesztés]

ÖSSZEHASONLÍTÁS MÁS KONSTRUKCIÓKKAL

A mai technológiák és kutatások alkalmazzák ugyan az abszorber integrációt crashbox-ok esetében azonban ezeknél a megoldásoknál vékonyfalú szerkezet és az abszorber gyűrődése egyidejűleg történik, elveszítve ezzel a töltet előnyös gyűrődési jellemzőit, ahogy az a xx. ábrán is látható. Továbbá részleges gyűrődés során a crashbox belsejében alkalmazott abszorber egy jelentős része zömületlen, vagyis energia abszorpció tekintetében kihasználatlan állapotban marad, ami a szerkezet hatékonysága szempontjából hátrányos. Ez azt jelenti, hogy ezeknél a megoldásoknál az alkalmazott abszorber csak a szerkezet teljes gyűrődése során használható ki maradéktalanul. Ezt a részleges gyűrődésnél jelentkező problémát mutatja a 10. ábra, amelyen a pirossal megjelölt rész jelöli a crashbox belsejében kihasználatlan állapotban maradt abszorbert.

10. Ábra: Zömületlen állapotban maradt abszorber a crashbox belsejében részleges gyűrődés esetén [27]

Az egytagú szerkezetek további hátránya, hogy a gyűrődést és ez által az ütközés pillanatában jelentkező lassulás jellemzői, valamint az elnyelt energia mértékét elsősorban a vékonyfalú szerkezet határozza meg. Illetve ahogy azt a 10. ábra is mutatja részleges gyűrődése során a teljes szerkezet cseréje szükséges.

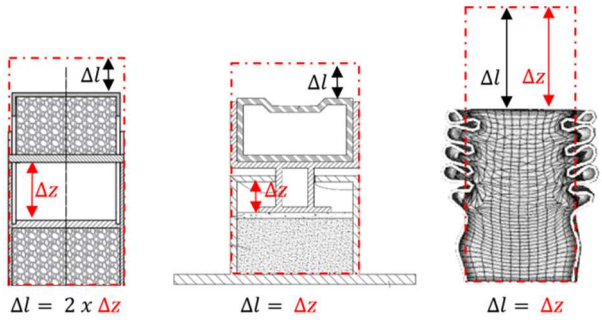


11. Ábra: Erő fluktuáció és csúcserő alakulása az elmozdulás függvényében (Szerkesztve : [28] alapján)

Megoldásunk a jelenleg ismert technológiákhoz képest annak modulálhatóságában is különbözik, vagyis kis energiájú ütközésnél csak az abszorber töltetek szenvednek plasztikus deformációt. Míg a vékonyfalú szerkezet maradó deformációja már csak egy nagyobb energiájú ütközésnél következik be. Továbbá a teleszkóp szerkezetnek köszönhetően különböző típusú és sűrűségű abszorberek egyidejű vagy elkülönített zömítése hozható létre radiálisan gátolt deformációjuk mellett.

DEFORMÁCIÓ ÁTTÉTEL

Természetesen az alkalmazott abszorberek által elnyelt energia arányos a zömülésük mértékével. Az xx. ábrán bemutatott konstrukcióknál egységnyi crashbox hossz-változás(Δl)egységnyi abszorber zömülést (Δz) jelent, tehát $\Delta l = \Delta z$. A jelenlegi megoldásunk azonban a többtagú kialakításának köszönhetően egységi crashbox hosszváltozás (Δl), a szerkezet belsejében kétszeres abszorber zömülést (Δz) képes generálni, vagyis $\Delta l = 2\ x\ \Delta z$. Az 12. ábra összehasonlítás céljából készült, ahol az általunk fejlesztett konstrukció figyelhető meg másik két, gyakran alkalmazott crashbox megoldással összevetve.

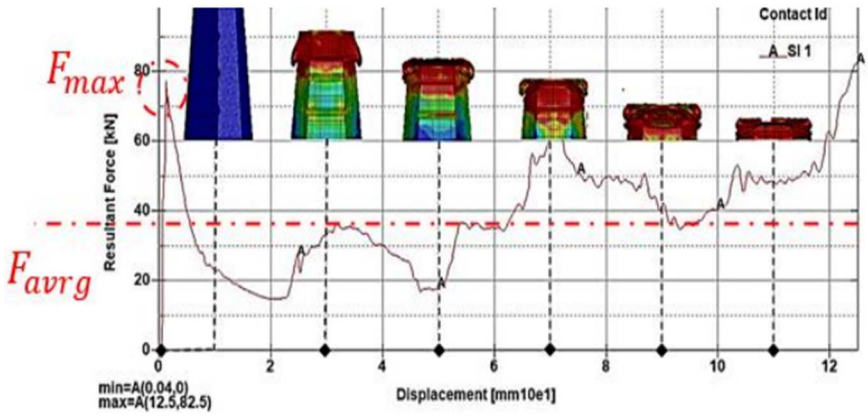


12. Ábra: Deformáció áttétel értelmezése [Saját szerkesztés]

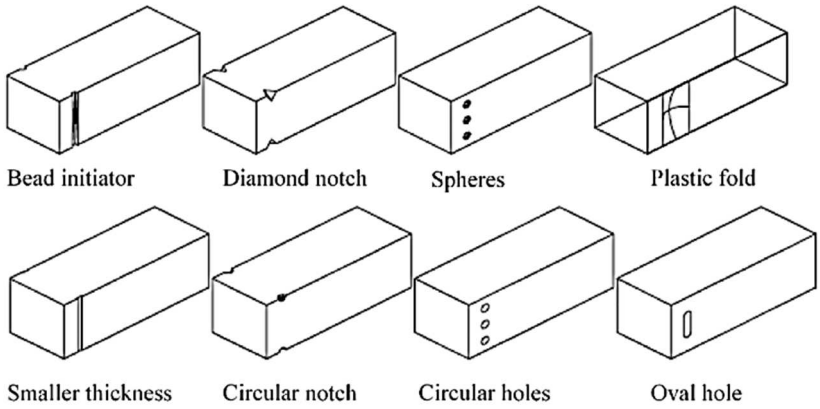
KEZDETI CSÚCSERŐ PROBLÉMA

A crashbox szerkezetek működésbe lépésének mértéke (merevsége) alapvetően meghatározza az ütközés pillanatában jelentkező lassulás mértékét. Túlságosan nagy merevség nagy csúcserőt von maga után, amely fokozza a személyi sérülések és műszaki károk mértékét, hiszen a csúcserőt meghaladva indulhat el a szerkezet plasztikus deformációja. Ezt a csúcserő problémát mutatja a 13. ábra. Hagyományos crashbox szerkezetek esetében a kezdeti csúcserő (F_{max}) többszöröse is lehet az átlagos zömülési erőnek (F_{avrg}), ez nagymértékben rontja a szerkezet törési hatékonyságát (CFE)[29-30]. Az xx. ábra alapján ez egy 50-60%-os hatékonyságot eredményez. A csúcserő jelentősen csökkenthető úgynevezett gyűrődés indító technikai megoldásokkal, amely olyan bordák, kimunkálások, furatok esetleg élletörések alkalmazását jelenti, amelyek a crashbox feszültséggyűjtő pontokként jelennek meg, és a plasztikus deformáció ezáltal hamarabb következik be. Törés indító konstrukciós lehetőségeket mutat be a 14. ábra.

$$CFE = \frac{F_{avrg.}}{F_{max}} \ [\%]$$

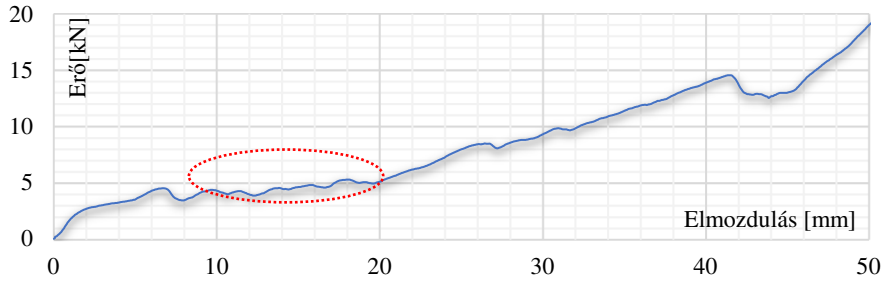


13. Ábra: A kezdeti csúcserő és az átlagos deformációs erő aránya [Saját szerkesztés]

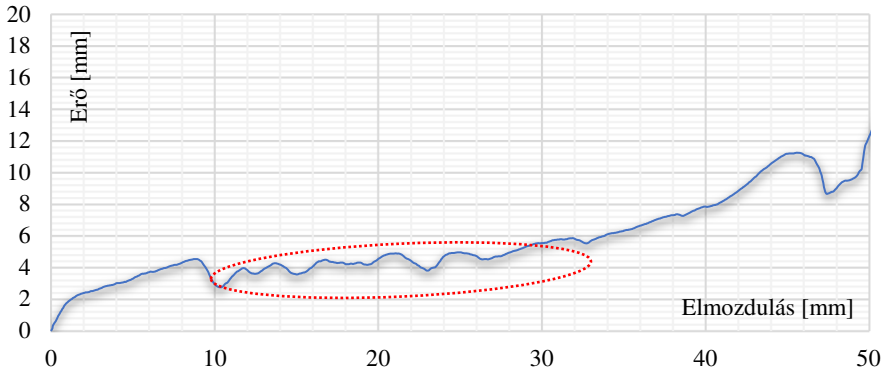


14. Ábra: A kezdeti csúcserő csökkenése érdekében alkalmazható technikai megoldások [31]

Az általunk fejlesztett konstrukció ezen csúcserő problémára is megoldásként szolgálhat, amelyet a fent ismertetett $CFE \cong 80 - 90\%$ hatékonysági értékkel lehet igazolni azonos periódust vizsgálva. Erő-fluktuáció már csak a abszorberek teljes zömülése után jelentkezhet, amikor megindul a crashbox héjszerkezet harmonika szerű gyűrődése. Ez már egy magasabb ütközési energia szintet követel meg, amikoris az alkalmazott abszorberek nem képesek felemészteni a teljes ütközési energiát. A 14.ábra és az 15.ábra a zömítési tesztelés során kapott diagramokat mutatja, melyen jól megfigyelhető, hogy egyenletesebb, lineárisan növekvő karakterisztikát ad az optimalizált crashbox annak gyűrődése során, valamint jól kivehető a platószakasz is, vagyis az abszorber előnyös tulajdonságai megtarthatók. Az 14. ábra az 1.sz. konstrukció azon változatának diagramját mutatja, ahol alacsonyabb sűrűségű (0,4g/cm^3) fémhabbal töltöttük meg az alsó tagot és nagyobb sűrűségű (0,7 g/cm^3) fémhabot használtunk a középső és felső tag tölteteként. A 15. ábrán pedig egy olyan változat erő-elmozdulás diagramja látható, ahol minden egyes tagban azonos sűrűségű(0,4g/cm^3) fémhabot alkalmaztunk. A két ábrát összehasonlítva látható, hogy annál a konstrukciónál, ahol csak egyféle abszorbert használtunk a plató szakasz tovább fenntartható, egészen 33 mm elmozdulásig, amelyet piros színnel jelöltünk. A csúcserő már csak a működés végén jelentkezik, addigra felemésztve az ütközési energia egy jelentős részét.



14. Ábra: Az 1.sz. konstrukció gyűrődési karakterisztikája különböző sűrűségű fémhabok alkalmazása esetén [Saját szerkesztés]



15. Ábra: Az 1.sz. konstrukció gyűrődési karakterisztikája egyféle sűrűségű fémhab alkalmazása esetén [Saját szerkesztés]

KONKLÚZIÓ

Alacsony sebességű ütközések, vagyis 16 km/h sebességig a passzívbiztonsági rendszer részét képező lökhárító berendezésnek kell olyan gyűrődési képességgel rendelkeznie, amely energia abszorpció révén képes megakadályozni a jármű fő alváz elemeinek (pl. nyúlványok) bármilyen mértékű deformációját. Ennek eszköze a lökhárító merevítő és a nyúlványok között elhelyezkedő, úgynevezett crashbox alkatrész plasztikus deformációja. Ezen vékonyfalú szerkezetek energia elnyelő képessége, és gyűrődési tulajdonságai alakoptimalizációval javítható. Másik megoldás az energia hatékonyság növelése céljából a szerkezet abszorberekkel való integrálása, pl. fémhabok, lattice szerkezetek, kompozitok. Viszont, hogy az így alkalmazott ideális gyűrődési karakterisztikákkal rendelkező abszorberek előnyös tulajdonságait ne veszítsük el, a vékonyfalú szerkezet konstrukciós továbbfejlesztése szükséges. Az általunk kidolgozott megoldásunk az ütközési/ütési energia hatékonyabb abszorpcióját hivatott megoldani a tömegoptimalizáció figyelembe vételével, ezért elsősorban járműiparban való alkalmazásra javasolt. Ezen belül személy és kisteherjárművek első-hátsó lökhárító rendszereinek hatékonyságának növeléséhez, valamit tehergépjárművek és pótkocsik hátsó és oldalsó aláfutásgátló rendszereinek kiegészítéséhez növelt energia abszorpció céljából. Felhasználási területe lehet a modern elektromos/hibrid/üzemanyagcellás személyszállító járművek (buszok) azok hátsó részeinek védelmének fokozása céljából. A kutatáshoz kapcsolódó mérések igazolták, mind a fémhabok alkalmasságát mint abszorber töltet, mind pedig a konstrukció működő képességét alátámasztva ezzel a fejlesztés kezdeti szakaszában megfogalmazott hipotéziseket. A tesztelések során kapott diagramok alapján kijelenthető, hogy a fejlesztett konstrukció gyűrődése esetén nem veszítjük el az abszorberek előnyös tulajdonságait.

FELHASZNÁLT IRODALOM

[1] Zhu, Y., Li, L., & Yang, J. (2012, July). Frontal structure improvement on car based on RCAR impact test. In 2012 Third International Conference on Digital Manufacturing & Automation (pp. 434-438). IEEE.

[2] Opperman, C. J. (2012). Study of a simplified bumper system subjected to offset impact loading.

[3] Li, M., Xia, Z., & Shangguan, W. (2018). Analysis and Simulation of Low-Speed Collision of Car Front Bumpers (No. 2018-01-1460). SAE Technical Paper.
[4] Ramon-Villalonga, L., & Enderich, T. (2007). Advanced Simulation Techniques for Low Speed Vehicle Impacts. Sixth LS-DYNA Anwenderforum, Frankenthal, 25-36.
[5] Cheni, R. K., Sinha, A., & Narayan, S. (2013). Enhanced light weight frontal crash box design for low speed and insurance tests (No. 2013-26-0023). SAE Technical Paper.
[6] Morello, L., Rossini, L. R., Pia, G., Tonoli, A., Morello, L., Rossini, L. R., ... & Tonoli, A. (2011). Body Components. The Automotive Body: Volume I: Components Design, 207-437.
[7] Constantin, B. A., Iozsa, D., & Fratila, G. (2016, November). Studies about the Behavior of the Crash Boxes of a Car Body. In IOP Conference Series: Materials Science and Engineering (Vol. 161, No. 1, p. 012010). IOP Publishing.
[8] Lee, K. H., & Bang, I. K. (2006). Robust design of an automobile front bumper using design of experiments. Proceedings of the Institution of Mechanical Engineers, Part D: Journal of Automobile Engineering, 220(9), 1199-1207.
[9] Hou, W., He, P., Yang, Y., & Sang, L. (2023). Crashworthiness optimization of crash box with 3D-printed lattice structures. International Journal of Mechanical Sciences, 247, 108198.
[10] Rayamajhi, M., Hunkeler, S., & Duddeck, F. (2014). Geometrical compatibility in structural shape optimisation for crashworthiness. International Journal of Crashworthiness, 19(1), 42-56.
[11] Ciampaglia, A., Fiumarella, D., Niutta, C. B., Ciardiello, R., & Belingardi, G. (2021). Impact response of an origami-shaped composite crash box: Experimental analysis and numerical optimization. Composite Structures, 256, 113093.
[12] Ghasemnejad, H., Hadavinia, H., Marchant, D., & Aboutorabi, A. (2008). Energy absorption of thin-walled corrugated crash box in axial crushing. SDHM Structural Durability and Health Monitoring, 4(1).
[13] Choi, S. Y., Hong, S. C., Park, S. K., & Jeong, S. W. (2022). Effects of diameter-to-thickness ratio on impact energy absorption capability of CFRP cylindrical crash box. International journal of automotive technology, 23(6), 1663-1671.
[14] Pavlovic, A., & Fragassa, C. (2024). Investigating the crash-box-structure's ability to absorb energy. International Journal of Crashworthiness, 1-15.
[15] Abdullah, N. A. Z., Sani, M. S. M., Salwani, M. S., & Husain, N. A. (2020). A review on crashworthiness studies of crash box structure. Thin-Walled Structures, 153, 106795.
[16] Ma, J., & You, Z. (2011). The origami crash box. Origami, 5(277-290), 587.
[17] Nisa, S. U., Pandey, S., & Pandey, P. M. (2023). A review of the compressive properties of closed-cell aluminum metal foams. Proceedings of the Institution of Mechanical Engineers, Part E: Journal of Process Mechanical Engineering, 237(2), 531-545.
[18] Xia, X. C., Chen, X. W., Zhang, Z., Chen, X., Zhao, W. M., Liao, B., & Hur, B. (2013). Effects of porosity and pore size on the compressive properties of closed-cell Mg alloy foam. Journal of Magnesium and Alloys, 1(4), 330-335.

[19] Movahedi, N., & Mirbagheri, S. M. H. (2016). Comparison of the energy absorption of closed-cell aluminum foam produced by various foaming agents. Strength of Materials, 48, 444-449.
[20] Blazy, J. S., Marie-Louise, A., Forest, S., Chastel, Y., Pineau, A., Awade, A., ... & Moussy, F. (2004). Deformation and fracture of aluminium foams under proportional and non proportional multi-axial loading: statistical analysis and size effect. International journal of mechanical sciences, 46(2), 217-244.
[21] Gioux, G., McCormack, T. M., & Gibson, L. J. (2000). Failure of aluminum foams under multiaxial loads. International Journal of Mechanical Sciences, 42(6), 1097-1117.
[22] Duarte, I., Vesenjak, M., & Krstulović-Opara, L. (2016). Compressive behaviour of unconstrained and constrained integral-skin closed-cell aluminium foam. Composite Structures, 154, 231-238.
[23] Li, C., Li, C., & Wang, Y. (2020). Compressive behavior and energy absorption capacity of unconstrained and constrained open-cell aluminum foams. Advanced Composites Letters, 29, 2633366X20923671.
[24] Wang, G., Zhang, Y., Zheng, Z., Chen, H., & Yu, J. (2022). Crashworthiness design and impact tests of aluminum foam-filled crash boxes. Thin-Walled Structures, 180, 109937.
[25] OKORUGBO, P. A. (2019). Effect of impact velocity on the energy absorption characteristics of crash boxes. PhD diss., NEAR EAST UNIVERSITY.
[26] Kocabaş, İ., & Yılmaz, H. (2021). Crashworthiness performance of Al6061 tubes with stiffened quatrefoil sections under axial and oblique impact conditions. Mühendis ve Makina, 63(706), 23-40.
[27] Zarei, H. R., & Kröger, M. (2008). Optimization of the foam-filled aluminum tubes for crush box application. Thin-Walled Structures, 46(2), 214-221.
[28] Ashby, M.F.; Evans, T.; Fleck, N.A.; Hutchinson, J.W.; Wadley, H.N.G.; Gibson, L.J. Metal Foams: A Design Guide; Elsevier: Amsterdam, The Netherlands, 2000.
[29] Ceyhan, M., & YİLDİZ, B. (2023). Investigation of Crash Performance of Multi-Cell Crash-Boxes. Çukurova Üniversitesi Mühendislik Fakültesi Dergisi, 38(3), 613-621.
[30] Turan, M. K., Ensarioglu, C., Bakirci, A., & Karpat, F. (2024). Impact performance of unconventional trigger holes. Materials Testing, (0).
[31] Harhash, M., Kuhtz, M., Richter, J., Hornig, A., Gude, M., & Palkowski, H. (2021). Trigger geometry influencing the failure modes in steel/polymer/steel sandwich crashboxes: Experimental and numerical evaluation. Composite Structures, 262, 113619.

KÖSZÖNETNYILVÁNÍTÁS

A szerzők köszönetet nyilvánítanak ÚNKP, a Kulturális és Innovációs Minisztériumnak, valamint a Nemzeti Kutatási, Fejlesztési és Innovációs Alapnak, hiszen a kutatást segítette és anyagilag támogatta az Felsőoktatási Doktori Hallgatói Kutatói Ösztöndíj (ÚNKP-23-3) programja.

SZABADALMI NYILATKOZAT

A tanulmányban bemutatott konstrukció szabadalmi bejegyzése megtörtént, így azt szerzői jog védi, annak bármiféle hasznosítása vagy alkalmazása kizárólag a szerzők engedélyével történhet.

ARTIFICIAL INTELLIGENCE IN CRIME PREVENTION AND COUNTER-TERRORISM

MESTERSÉGES INTELLIGENCIA A BŰNMEGELŐZÉSBEN ÉS A TERRORIZMUS ELLENI VÉDEKEZÉSBEN

BAUMGARTNER Helga[1] – ŐSZI Arnold[2]

Abstract

The integration of artificial intelligence and facial recognition technologies into modern security frameworks significantly enhance our ability to identify threats, to take preventive measures, and to improve public safety and security. As threats posed by criminals and suspected terrorists continue to evolve, increasingly sophisticated countermeasures are required to combat the risks posed by such threats. By analysing vast amounts of data in real-time, artificial intelligence can detect patterns that suggest illegal activities, while face recognition can identify individuals of interest without them suspecting surveillance. Furthermore, with rapid evolution and broad applicability within both physical and cybersecurity, these technologies enable continuous improvement, ensuring that security measures follow the recent technological advancement. Artificial intelligence and face recognition play crucial roles in mitigating security risks and in countering terrorism, making them an important component of the global effort to maintain safety in our complex and digital world.

Keywords

artificial intelligence, counter-terrorism, face recognition, cybersecurity

Absztrakt

A mesterséges intelligencia és az arcfelismerő technológiák integrálása a biztonsági rendszerekbe jelentős előrelépést jelent a fenyegetések azonosítására, a megelőző intézkedések megtételére és a biztonság fokozására. Ahogy a bűnözők és a feltételezett terroristák által jelentett fenyegetések egyre fejlődnek, egyre kifinomultabb ellenintézkedések szükségesek ezek leküzdésére. A valós idejű adatelemzés révén a mesterséges intelligencia képes felismerni az illegális tevékenységekre utaló mintázatokat, míg az arcfelismerő rendszerek képesek azonosítani a célszemélyeket természetes közegükben. Gyors fejlődésük és széleskörű alkalmazhatóságuk révén, biztosítják, hogy a fizikai és kiberbiztonsági intézkedések lépést tudjanak tartani a legújabb technológiai fejlesztésekkel. A mesterséges intelligencia és az arcfelismerés kulcsszerepet játszanak a biztonsági kockázatok mérséklésében és hatékony eszközt nyújtanak a terrorizmus elleni globális küzdelemben az összetett és digitális világunkban.

Kulcsszavak

mesterséges intelligencia, terrorizmus elleni védekezés, arcfelismerés, kiberbiztonság

[1] baumgartner.helga@phd.uni-obuda.hu | ORCID: 0009-0003-7938-7614 | PhD Student, Doctoral School for Safety and Security Sciences Óbuda University |Doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola
[2] oszi.arnold@bgk.uni-obuda.hu | ORCID: 0000-0001-5988-0143 | adjunct professor, Óbuda University, Bánki Donát Faculty of Mechanical and Security Technology Engineering |adjunktus, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

ARTIFICIAL INTELLIGENCE

Artificial intelligence is one of the most critical technologies today, playing a significant role in our daily lives. In the past decade, it has undergone significant evolution — the rapid growth of the internet has led to an exponential increase in the volume of data produced, which is a key component in artificial intelligence development. Artificial intelligence is a complex interdisciplinary field, which integrates elements – apart from computer science, mathematics and statistics, engineering – from biology and medicine, psychology, sociology, communication and linguistics, amongst others. With the increase in computing power and the improvement of algorithms that enable the addressing of more complex problems, processing this ever-growing amount of data has become faster and more efficient in response. Moreover, increased financial investment in artificial intelligence has resulted in its rapid spread across various sectors. This widespread adoption is transforming industries. In healthcare, artificial intelligence assists in diagnosing diseases and personalizing treatment plans. In the automotive industry, it advances the development of autonomous vehicles. In national defence it helps analyse the allied and enemy forces' strategy and provides support in military operations. In the financial sector artificial intelligence is used for fraud detection and investment analysis. In education it tailors the learning path based on the individual's learning experience. Smart cities also utilize artificial intelligence to develop a more liveable space by improving traffic management, energy, water and waste management, and infrastructure management. With the help of artificial intelligence, farmers can optimize field usage for better food production, manage natural resources and minimize environmental impact. Furthermore, artificial intelligence-driven chatbots are enhancing customer service. As a result, artificial intelligence is not only changing technology, but also impacting society, leading to new innovations, and making life more efficient, leading to innovation and efficiency: starting a new era where technology and daily life work better together. [1] [2]

Artificial intelligence has become an integral part of our everyday life, aiming to make it easier and more convenient. Despite its undeniable presence and effects, oftentimes we are not truly aware of the way it works, or the potentials it has. The evolution and spread of artificial intelligence have outpaced the public awareness, which can lead to either underestimating the possibilities that artificial intelligence holds or overestimating its capabilities — either way we may fail to explore the potential benefits. As we continue to integrate artificial intelligence into our lives, we must focus on understanding its benefits while simultaneously paying attention to its misuse.

Artificial intelligence has multiple subfields, each representing different technologies, and often they are referred to collectively as artificial intelligence, which, although not necessarily inaccurate, understanding the characteristics of these subfields and their potential applications improves our ability to utilise their strengths effectively across the different sectors and functions. The primary subfield of artificial intelligence is machine learning, which enables machines to learn autonomously and to improve from experience without being specifically programmed to do so. By analysing vast amounts of data, it can identify patterns and trends with more precision and higher effectiveness than a human. This capability allows machine learning to be applied across various industries, leading to significant improvements in efficiency, accuracy, and decision-making processes. Another subfield is deep learning, which employs neural networks inspired by the human brain's structure and

function to process high-dimensional, unstructured data, effectively mimicking human intuition but at a scale and speed that exceeds human capability. Deep learning is able to understand data hierarchy, allowing machines to understand texts, pictures or even sounds, which is a significant progress in areas such as autonomous vehicles, speech recognition, and predictive analytics, revolutionising how machines understand and interact with the world. [1] [3]

This paper focuses on the technical and operational aspects of facial recognition technology and counter-terrorism. While facial recognition technology raises significant concerns regarding privacy, data protection, human rights, and ethics, these are beyond the scope of this study, and therefore, not discussed.

ARTIFICIAL INTELLIGENCE IN SAFETY AND SECURITY

Artificial intelligence has also gained ground in the safety and security sector, where it is applied across various fields, such as in physical security, including access control, fire protection, hazard detection, disaster response and management, as well as in information security, data protection and cybersecurity. These artificial intelligence-driven solutions are used not only by consumers seeking to make everyday life safer and more comfortable, but also by government bodies to enhance national security, and to efficiently identify and assess threats and to mitigate the risks posed criminal activities. These advanced technologies enable a more proactive approach in identifying threats, protecting infrastructure, managing emergencies, facilitating better coordination and response strategies at local, national, and international levels, allowing for a much more effective and efficient allocation of both human and material resources. [4]

In physical safety and security, artificial intelligence can be applied to Closed-Circuit Television Systems (CCTV) where it can enhance their functions and enable proactive monitoring and response, rather than merely reactive actions. Traditional CCTV requires constant human oversight to detect and respond to anomalies. By integrating artificial intelligence into CCTV systems, it can reduce the need for human resources that would perform the same function, decrease overall response time, and increase the efficiency of these systems, overall leading to enhanced safety and security for both people and infrastructure. [5]

Artificial intelligence enhanced CCTV can improve security measures by performing object recognition, which can identify unattended bags in public areas; crucial in restricted areas such as airports, stadiums, or densely populated streets, preventing possible terrorist attack. Object recognition can also be used to identify weapons or other specific items, allowing security personnel for fast reaction. By monitoring the crowd, it is also possible to determine the number of attendees, assess density, and to determine if the headcount reaches a potentially dangerous level. When evacuation is required, artificial intelligence can advise through dynamic exit signs about the optimal evacuation route as the conditions change. [6]

Artificial intelligence is also used in plate number recognition, which is widely applied, especially to manage access to parking lots, ensuring only authorised vehicles can access restricted areas. It is also utilised by law enforcement agencies to monitor traffic for potential violations and to identify and locate stolen or suspicious vehicles.

Another method of utilising artificial intelligence is in motion detection, which can enhance intrusion detection and perimeter security by differentiating between the movements of humans and animals. Traditional motion sensors often react to any kind of movement, disregarding the size of the body detected. By applying artificial intelligence, the system can differentiate whether the motion comes from a human – and therefore a potential intruder – or an animal, and therefore reduce false alarms.

Fire safety can also benefit from the use of artificial intelligence. One known application is in CCTV systems with flame and smoke detection function where visual changes indicating fire can be identified. During firefighting, real-time visual monitoring can inform firefighters of potential flashover, enabling them to leave the building, before it is too late. Artificial intelligence can also be trained to identify the type of burning material or fluid without personnel being exposed to potential harm. Furthermore, artificial intelligence can also be applied to simulations of the spread of smoke and fire in buildings, and with that, evacuation and firefighting plans can be updated, and the ideal location of sprinklers and other fire protection and firefighting devices can be identified for optimal performance. [7]

During a disaster, the primary focus is on minimising the impact of such events as much as possible. Disasters can arise from health crises, natural causes, human negligence, or even acts of terror. Effective disaster management includes prediction, prevention, preparation, mitigation, response and recovery. Of these, prediction plays a crucial role, for which artificial intelligence serves as a powerful tool. By analysing historical data and current measurements, artificial intelligence can predict natural disasters such as floods, volcanic eruptions, or hurricanes, and can advise on effective rebuilding strategies for resource allocation.

Disasters occurring due to human negligence, such as industrial accidents or nuclear disasters, can also be mitigated using artificial intelligence by predicting equipment failure, recognising signs of human negligence and advising on the safety distance for evacuation in case of nuclear disaster based on level of radiation to minimize exposure. Ultimately, artificial intelligence can be applied to all elements of disaster management. [8] [9]

ARTIFICIAL INTELLIGENCE AND CYBERSECURITY

Cybercrime and cyberterrorism pose a great threat nowadays, affecting everyone and every sector from individuals to governmental, private, and public sectors. These activities range from stealing personal data to causing financial fraud or attacking critical infrastructure to a level where cyber criminals or cyberterrorists are capable of shutting down communication and navigation systems, disrupting businesses or government operations.

On one hand, artificial intelligence can be used by malicious actors to identify vulnerable targets or refine their methods to seem more authentic. However, artificial intelligence can also detect threats and offer response solutions to mitigate risk, therefore enhance cybersecurity and reduce potential damage. Machine learning models can analyse and learn the pattern of the users' normal behaviour, and can detect when irregular activities occur, that indicate cyberattack.

Ransomware is also often employed by cybercriminals and cyberterrorists, who block access to systems of individuals or organizations within the private or public sector to demand ransom. Machine learning models can be applied to make ransomwares more sophisticated by learning how the security measures developed against them work, and

adapting accordingly, making them more difficult to detect, therefore posing greater threat to its victims. However, artificial intelligence can also predict potential ransomware attacks based on historical data, foresee future threats and suggest preventive measures based on the profile of the organization. During an attack, artificial intelligence can initiate immediate incident response, such as isolating elements of the system, or shutting down the whole system and therefore minimizing the impact, while informing respective individuals and authorities about the attack. Furthermore, artificial intelligence can be utilized to reconstruct the elements of the attack for further investigations, helping to understand the utilized methods for the attack, and to develop an adequate cyber-defence strategy. [1] [10]

The spread of crypto assets – including crypto currency – has been convenient in the financing of terrorism due to their anonymity and quick transferability across borders. Terrorist groups can receive fundings in crypto currency – ransoms are also often demanded in the form of crypto currency – which then can be used to purchase firearms and explosives, launder money, and to commit further crime or acts of (cyber)terrorism.

The internet and social media serve as a tool for radicalisation of individuals, recruiting potential terrorists, and financing terrorist operations including transactions of weapons.

The adoption of end-to-end encryption in popular messaging platforms enables suspected terrorists to communicate in such way that is almost impossible for law enforcement agencies to detect. Additionally, they often use the dark web to conduct their illegal activities while remaining anonymous and protected by the encryption and anonymity features of the dark web.

ARTIFICIAL INTELLIGENCE AND COUNTER-TERRORISM

Terrorism does not have a universally accepted definition, and the same applies to cyberterrorism, however, the key distinction between "traditional" terrorism and cyberterrorism is that cyberterrorism often does not involve physical harm or direct casualties. Instead, cyberterrorism focuses on disrupting services and causing serious consequences for critical infrastructure, resulting in chaos and significant economic damage.

With the widespread availability of the internet and modern technology, access to the internet has become more available for the many. As such, suspected terrorists as well are adopting new technologies and are shifting their theatre into cyberspace, allowing criminals and suspected terrorists to operate across borders with minimum risk of exposure, spreading terrorist content – including propaganda –, recruiting individuals, and learning about the latest technology for malicious purposes. While the two concepts are similar, they are not the same. [11]

To prevent cyberterrorist attacks, it is crucial to protect online infrastructure adequately by implementing security controls; predictive measures must be in place. Artificial intelligence can quickly and accurately process and analyse vast amounts of data – such as communications metadata, financial transactions, travel patterns, and web browsing activities. artificial intelligence in the context of counter-terrorism could serve multiple purposes, including identifying patterns of terrorist threat, including their intent, capabilities, and opportunity. In turn, a better understanding of the threat would allow counter-terrorism authorities to deploy measures to mitigate the associated risks.

The total data production in 2024 is estimated to reach 147 zettabytes per day, increasing to 181 zettabytes per day in 2025. This includes the creation and collection of digital information across the internet, including, but not limited to social media content, communication, scientific research, and data from Internet of Things (IoT), among others. From a technology and research perspective such growth of available data is welcomed, as it enhances various aspects of human life, however, managing such quantity of data is impossible to be controlled by humans alone, and therefore calls for advanced data management. [12]

To effectively manage this data, employing artificial intelligence to monitor online content in real-time is essential. This approach ensures the timely detection and flagging of terrorist content for removal, thereby preventing its spread and promoting a safer internet environment. However, this method requires a balanced application of technology and human judgment, as utilising this approach for monitoring individuals requires such a large amount of data per person to be effective, which is almost impossible to collect, and also raises significant human rights concerns regarding privacy, discrimination, and the potential for mass surveillance. [1]

It is undeniably easier to analyse written content, however, videos are more commonly used to share information. Advanced algorithms are required to monitor the content of videos, which can be utilised not only for analysing the content – such as speech, sound, images, surroundings.

Numerous tools are available to identify online terrorist content, which can be districted into two main groups: matching and classification. Matching compares new content to existing content that has been previously classified as terrorist content. In this case the content is converted into a fixed-length string of data, or so-called hash value, allowing comparison of whether the newly generated hash value matches any of the existing hash values generated from confirmed terrorist content. When using cryptographic hashing, the same content will always generate the same hash value, which is both a strength and a weakness of this technique. Any alteration of the original content results in a different hash value. Alternatively, perceptual hashing can also be utilized, as this technique can identify visually similar content and patterns despite minor modification. However, matching does not always classify as artificial intelligence, only when machine learning is applied to learn, adapt, and improve over time. [13]

To adequately monitor content on the internet, artificial intelligence tools based on computer vision, speech recognition and audio analysis and Natural Language Processing (NLP) techniques must be applied to sift through texts, images, videos, audios available online, identifying potential terrorist material or connections that can indicate the presence of terrorist groups. NLP is a subfield of artificial intelligence that applies machine learning, and often deep learning as well to analyse texts, and to understand their content and semantics. However, content moderation and classification also heavily rely on computer vision for image and video analysis, as well as speech recognition and audio analysis for processing audio content. matching technique, classification-based content moderation offers a more sophisticated approach.

A sophisticated NLP technology can differentiate between an article about terrorism, and potential terrorist content, preventing the misleading of officials. While these technologies can identify possible terrorist content, they require human assessment and final

decision. No matter how advanced artificial intelligence is, it may identify harmless content as terrorist content, and vice versa. Automated content moderation is used by many well-known social media platforms to identify and filter content that meets pre-defined criteria, helping to prevent spread of terrorist propaganda and radicalisation, however, due to the stylistic nuances of a language, it may fail to adequately recognise the intended message and, therefore, should not be fully automated without human supervision. [3]

One significant limitation of applying artificial intelligence to detect and remove online terrorist content is the lack of available relevant data needed to adequately train the algorithms. While different online platforms provide a large amount of data that has already been identified and removed, this data might not be sufficient to train the algorithms to identify all types of terrorist content, or it might be biased, due to specific event, terminology appearing in the training data, as well as the lack of accepted definition of terrorism. To overcome this limitation, generative artificial intelligence can be used to generate content for training purposes that is similar to already existing, real-world example. This new content is then similar in style, terminology, and characteristics of previous examples, with the aim of filling the gap of lack of sufficient training data. [13]

ARTIFICIAL INTELLIGENCE AND FACE RECOGNITION

Of all the possible applications of artificial intelligence in the field of counter-terrorism, artificial intelligence enhanced face recognition is particularly crucial.

Face recognition in crime prevention was utilised long before the digital era. Historically, until the mid-1900s, identification relied on manual comparison of photographs in documents such as identification cards or early passport versions where photos could be easily falsified, or replaced, and the comparison relied significantly on human intuition. Relying solely on the expertise of law enforcement personnel, it has been, and still is, a liability, as errors may occur due to potential misjudgement and lack of experience of the personnel in charge of the verification of these documents.

When digital pictures replaced analogue, face recognition underwent a significant evaluation. Firstly, as falsification of photographs within identification documents became much more challenging and secondly as sophisticated facial recognition technologies became available.

The origins of face recognition dates back to the 1960s, when a semi-automatic face recognition system was developed by Woody Bledsoe, along with Helen Chan Wolf and Charles Bisson, where the characteristic reference points on the image of a human face were manually marked on a graphic tablet, and then the computer would use these points to recognise faces. In the 1970s, a semi-automated facial recognition system was created by A. Jay Goldstein, Leon D. Harmon and Ann B. Lesk, by establishing 21 marker points on the face, which were then systematically compared by computers. In the late 1980s, face recognition underwent significant development, when Michael Kirby and Lawrence Sirovich, began to apply a method based on linear algebra, which later served as the foundation of the Eigenface technique. The concept is that the positions of reference points on the face relative to each other can be described by vectors, and less than one hundred values are necessary to numerically describe a face for identification purposes. In the early 1990's this method was adopted and further developed by Matthew Turk and Alex Pentland, who created an average face from all the faces in their database. By subtracting this average face

from each individual face and describing the difference with vectors, the characteristic eigenvector, or personal vector, for each face is obtained. [14] [15]

In the mid 1990s, Peter N. Belhumeur, João P. Hespanha, and David J. Kriegman developed a method called Fisherface to address some of the limitations of the Eigenface technique. This method enhances the accuracy of recognition by better distinguishing features of different individuals and reducing unnecessary variations, such as changes in expression or lighting within the same person's images. [16]

From the 1990s onwards, the civilian sector has played a significant role in developing face detection and recognition systems, mostly encouraged by governmental bodies. Among these initiatives are the Facial Recognition Technology Database (FERET) initiated by the Defense Advanced Research Projects Agency (DARPA), or the Face Recognition Vendor Tests (FRVT) launched by the National Institute of Standards and Technology (NIST) in the 2000s. In 2001 Paul Viola and Michael Jones developed a face and object detection system using Haar-like features. This method was capable of analysing a large number of images in real-time to determine whether they contained an image of a face. The Haar-like features scan images, searching for patterns characteristic of faces based on the intensity of contrasts and edges due to facial features. [14] [17]

The methods listed so far worked primarily on basic algorithms, without the use of artificial intelligence.

In the 2010s, as artificial intelligence became more widespread, so did artificial intelligence enhanced face recognition, integrating deep learning to improve its accuracy. These systems began to incorporate deep learning techniques, which use neural networks with multiple layers to analyse various forms of data. This integration marked a pivotal shift in how facial recognition technologies functioned, enabling these systems to achieve unprecedented levels of accuracy and efficiency.

Deep learning models, especially Convolutional Neural Networks (CNNs), learn to detect and differentiate between facial features automatically and accurately. As these systems are fed more data, their ability to recognise faces under varied conditions and from different angles improves. Sophisticated models are also able to differentiate and recognize various facial expressions, coming from different emotions, and categorise people based on that, which allows among others personalised targeting in marketing, other purposes like enhanced security measures, where facial emotions can indicate intent or state of mind.

FACE RECOGNITION AND COUNTER-TERRORISM

The events of 9/11 brought a significant change in safety and security, especially within the aspect of travel and border management. This incident catalysed significant advancements in security measures – countries became more protective, strengthened their borders as well as their entry policies, and travel regulations became unprecedentedly strict. This event also accelerated the integration of biometric data into Machine Readable Travel Documents (MRTDs), and therefore facial recognition technology became a significant tool in countering terrorism. As a result of that, nowadays more than 140 countries issue MRTDs, with integrated biometric data. Integrating facial recognition technology into travel security has revolutionised border control and screening procedures at both land

crossings and airports. This helps prevent suspected terrorists from crossing borders or boarding flights, resulting in enhanced security measures and a significant improvement in safety protocols. [18]

When leaving or entering a country, travellers must present their travel documents to passport control officer, who then verifies the identity of the traveller, checks the validity of the document, and that the individual is not on any watchlist, including known or suspected criminals and terrorists among other entities. Automated Border Control Gates (ABC Gate) operate in a similar way as traditional passport control but replace the passport control official with facial recognition software. Travellers present their travel document – only those with integrated biometrics data – to the ABC gate, which scans and verifies the document, ensures that person is the rightful owner, and checks that they are not wanted by authorities. [19]

Facial recognition technology enhances safety and security in both physical and cyberspace. By integrating it into CCTV systems in public spaces, authorities can improve their situational awareness, enabling them to monitor these areas more effectively, and detect and respond to suspicious activities. These systems can be deployed in crowded places, such as airports, stadiums, train stations and streets. Facial recognition systems are capable of monitoring crowds in real time, searching for potential matches against watchlists. During investigations for criminal cases including terrorist attempts or attacks, reviewing CCTV footage, extracting facial images of the potential perpetrators and using artificial intelligence enhanced facial recognition systems to search for and possibly identify criminals and suspected terrorists are crucial for the success of investigation.

In cyberspace, facial recognition systems can be employed to monitor online content, identifying individuals in terrorist propaganda, or extracting their facial images, similarly to how they operate in physical space. By analysing the content together with the metadata, such as geolocation, time stamp and other technical information, law enforcement agencies have better chance to capture known or suspected criminals and terrorists. [1]

SUMMARY

Artificial intelligence undeniably plays an increasingly significant role in our everyday life – unless we specifically attempt to avoid it – there is hardly a day when we do not meet it in our daily routines. Applying artificial intelligence to safety and security, and especially to crime prevention and counter-terrorism, could immensely enhance global safety and security.

Applying artificial intelligence in these areas is complex; from real-time CCTV with enhanced capabilities to complex data analysis that predicts potential threats before they materialise. These systems are capable of identifying individuals on watchlists in real-time, providing law enforcement agencies with essential information that can prevent terrorist actions. Facial recognition technology, when integrated with extensive surveillance networks, enables continuous monitoring of public spaces, therefore enhancing the detection and response to potential threats.

Artificial intelligence is capable of analysing vast amounts of data, allowing it to identify patterns and connections that human analysts may miss. This includes forecasting potential terrorist attacks by analysing communication, financial transactions, and travel

data. Law enforcement agencies can extract actionable information from this data, preventing possible crime and terrorist acts.

Integrating artificial intelligence into counter-terrorism strategies becomes imperative, this not only ensures a higher level of public safety but also supports a more proactive approach to global security challenges. In a world where threats are becoming more complex and harder to detect, artificial intelligence offers a powerful tool in the arsenal of national security, enhancing international cooperation and coordination for safety and security.

Facial recognition technology supports various aspects of counter-terrorism efforts, including prevention, investigation, surveillance, and monitoring of online environments. As threats continue to evolve, the strategic application of facial recognition technology remains crucial in safeguarding the public and enhancing global security measures.

REFERENCES

[1] United Nations Office of Counter-Terrorism – Counter-Terrorism Centre (UNCCT) – United Nations Interregional Crime and Justice Research Institute (UNICRI) – *Algorithms and Terrorism: The Malicious Use of Artificial Intelligence for Terrorist Purposes – A Joint Report by UNICRI and UNCCT*, 2021, [Online] link

[2] KOLLÁR, Csaba – A mesterséges intelligencia és a kapcsolódó technológiák bemutatása a biztonságtudomány fókuszában – Kiberbiztonság – Cybersecurity 2. – Biztonságtudományi Doktori Iskola, Budapest, 2019, ISBN:9789634491859 [Online] link

[3] United Nations Office of Counter-Terrorism – Counter-Terrorism Centre (UNCCT) – United Nations Interregional Crime and Justice Research Institute (UNICRI) – *Countering Terrorism Online with Artificial Intelligence – An Overview for Law Enforcement and Counter-Terrorism Agencies in South Asia and South-East Asia – A Joint Report by UNICRI and UNCCT*, 2021, [Online] link

[4] NECZ, Dániel – *A mesterséges intelligencia belügyi és biztonsági célú alkalmazása* – SCIENTIA ET SECURITAS 1 : 1 pp. 49-53., 5 p. (2020), , [Online] link

[5] LAHIFF, Mike – *How AI is Disrupting the Business of Physical Security* – Forbes Technology Council, 2023, , [Online] link

[6] ROMAN, Jesse – *Applications of AI* – National Fire Protection Association (NFPA) Journal, 2024 [Online] link

[7] ROMAN, Jesse – *Our AI Future* – National Fire Protection Association (NFPA) Journal, 2024 [Online] link

[8] SAHOTA, Neil – *AI in Disaster Management: AI's Role in Disaster Risk Reduction, 2023,* [Online] link

[9] BARI, Lazima Faiah, AHMED Iftekhar, AHMED Rayhan, ZIHAN Tawhid Ahmed, SHARMIN Sabrina, PRANTO Abir Hasan, and Md. ISLAM Rabiul – *Potential Use of Artificial Intelligence (AI) in Disaster Risk and Emergency Health Management: A Critical Appraisal on Environmental Health* – Sage Journals, 2023 [Online] link

[10] PAUL, Anthony Lawrence – *The Role of Artificial Intelligence in Enhancing Data Security* – May 2024 [Online] link

[11] NADIJA, Madaoui – *The role of artificial intelligence in combating cyber terrorism – El Papel de la Inteligencia Artificial en la Lucha Contra el Ciberterrorismo*, IUS ET SCIENTIA, 2023 Vol. 9 Nº 2, [Online] link

[12] TAYLOR Petroc – *Amount of data created, consumed, and stored 2010-2020, with forecasts to 2025* – Statista, 2023 [Online] link
[13] MACDONALD, Stuart, MATTHEIS, Ashley, WELLS, David – *Using Artificial Intelligence and Machine Learning to Identify Terrorist Content Online* - Tech Against Terrorism Europe - 15 January 2024 [Online] link
[14] NEC New Zealand Limited – *A brief history of Facial Recognition* –2022, [Online] link
[15] Dr. U, Chandni – *The Tale of Facial Recognition Technology* –2022, [Online] link
[16] BELHUMEUR, Peter N., HESPANHA, Joao P., KRIEGMAN, David J – *Eigenfaces vs. Fisherfaces: Recognition Using Class Specific Linear Projection* – IEEE Transaction on Pattern Analysis and Machine Intelligence, Vol. 19, No. 7, July 1997, [Online] link
[17] MAUSS, Ben – *Haar-like Features: Seeing in Black and White, An Introduction to Computer Vision, Part II,* 2021 [Online] link
[18] BAUMGARTNER, Helga – *Biometrikus adatok a géppel olvasható úti okmányokban – Az ICAO Doc 9303,* Safety and Security Sciences Review 6 : 1 pp. 1-8. , 8 p. (2024), [Online] link
[19] Dr. BALLA, József – *A biometrikus adatokat tartalmazó úti és személyazonosító okmányok biztonságnövelő hatása a határ- és közbiztonság alakulására* – Doctoral dissertation, 2019, [Online] link

SECURITY DIMENSIONS OF THE USE OF ARTIFICIAL INTELLIGENCE IN EDUCATION FROM AN INTERCULTURAL APPROACH

A MESTERSÉGES INTELLIGENCIA OKTATÁSBAN VALÓ ALKALMAZÁSÁNAK BIZTONSÁGI DIMENZIÓI INTERKULTURÁLIS MEGKÖZELÍTÉSBEN

REVÁK Bernadett[1] – CSISZÁRIK-KOCSIR Ágnes[2]

Abstract

Today, the importance of information security in education is increasingly emphasised. For members of generations X, Y and Alpha, ICT tools have become everyday objects of use, making it essential that teaching methods adapt and innovate accordingly. In particular, it is important that students learn to use data and devices safely, and the necessary guidelines should be integrated into the educational process. The aim of our study is to examine how young people use the opportunities offered by digitalisation in educational institutions, with a particular focus on the use of AI and the perceptions and visions of its use. This is interpreted through an intercultural lens, comparing the intercultural characteristics and attitudinal differences of Hungarian and Turkish youths based on a questionnaire survey conducted in the two countries.

Keywords

Security, Security Culture, Security Awareness, Critical Information Infrastructure, Artificial Intelligence, Education, Digitalisation

Absztrakt

Napjainkban az információbiztonság fontosságát egyre inkább hangsúlyozni kell az oktatásban. Az X, Y és Alfa generáció tagjai számára az infokommunikációs eszközök mindennapi használati tárgyakká váltak, ami elengedhetetlenné teszi, hogy az oktatási módszerek is ehhez igazodjanak és megújuljanak. Különösen fontos, hogy a diákok megtanulják a biztonságos adat- és eszközhasználatot, amelyhez szükséges iránymutatásokat az oktatási folyamatba kell integrálni. Tanulmányunk célja, hogy megvizsgáljuk, hogyan használják a fiatalok az oktatási intézményekben a digitalizáció nyújtotta lehetőségeket, különös tekintettel a mesterséges intelligencia alkalmazására és az ezzel kapcsolatos véleményekre és jövőképekre. Mindezt interkulturális szemüvegen keresztül értelmezzük, összehasonlítva a magyar és a török fiatalok interkulturális jellemzőit és a hozzáállásbeli eltéréseket a két országban végzett kérdőíves kutatás alapján.

Kulcsszavak

Biztonság, Biztonság Kultúra, Biztonságtudatosság, Kritikus Információs Infrastruktúra, Mesterséges Intelligencia, Oktatás, Digitalizáció

[1] revak.bernadett@phd.uni-obuda.hu| ORCID: 0009-0003-1441-2743 | Ph.D. Student, Óbuda University, Doctoral School on Safety and Security Sciences | Ph.D. hallgató, Óbudai Egyetem, Biztonságtudományi Doktori Iskola

[2] kocsir.agnes@kgk.uni-obuda.hu| ORCID: 0000-0001-5454-7843 | Associate professor, Óbuda University, Keleti Károly Faculty of Business and Management | Egyetemi docens, Óbudai Egyetem, Keleti Károly Gazdasági Kar

BEVEZETÉS

A 21. századi modern társadalomnak folyamatosan kihívásokkal kell szembenéznie, megfelelnie. Ezek a kihívások nagymértékben függenek a technikai és virtuális infrastruktúrától. Elsősorban a számítástechnikai és informatikai rendszerek gyors fejlődésének köszönhetően a mesterséges intelligencia egyre több aspektusban jelenik meg a társadalmi és gazdasági területeken. A kommunikáció módját tekintve a mesterséges intelligencia egyfajta innovatív, kommunikációs ágensként definiálható. A digitalizáció mellett a 21. század vezető fogalma lett az innováció is, amelynek köszönhetően találkozhatunk a mesterséges intelligenciával. A mesterséges intelligencia térnyerése napjainkra megállíthatatlan folyamattá vált. Az OECD által megfogalmazott 6 alapelvben olvasva tisztább képet kaphatunk az információbiztonsági kultúra felépítésének alapjairól, tényezőiről. Ezen elvek vonatkoznak felelősségkörükhöz igazodva diákokra és tanárokra egyaránt. Gyakorlatilag a felhasználók számára egyfajta segítségnyújtást adva ezzel [1]. A biztonság kultúra kialakításában és kialakulásában nagy szerepe van a biztonságtudatosságnak. Mindezek alapján a biztonsági kultúrának tehát szükséges eleme a tudás és kompetenciák mellett a tudatosság és a szándékosság is egyben, ami számos elemből táplálkozik [2].

A biztonság, mint fogalom mindenképpen valamiféle védelmet jelent, védelmet a különféle veszélyektől. Mindenkinek más-más nézőpontja alakul ki a fogalmat végig gondolva. A definíciók és megközelítések a különféle prioritások függvényében alakulnak. A biztonság életünk minden területén szignifikáns tényezőként van jelen. A biztonság megteremtésére minden élőlény egész élete során törekszik. Az oktatás és a biztonság szoros és elválaszthatatlan kooperációban áll egymással. A biztonság kiemelkedő fontossággal bír az oktatás minden területén. A 21. század társadalmának bátran adhatjuk az információs társadalom elnevezést. Az emberiség tagjainak életét előbb vagy utóbb szerves mértékben áthatják, formálják az információs technika és technológia vívmányai. A köztük lévő kapcsolatrendszer a függőség folyamatának köszönhetően folyamatos kölcsönhatásban és körforgásban áll egymással. Gyakorlatilag egy kikapcsolhatatlan kapcsolat áll fenn.

SZAKIRODALMI ÁTTEKINTÉS

A mesterséges intelligencia (MI) biztonsági, oktatási dimenziói

Számtalan definitív megközelítéssel találkozhatunk a mesterséges intelligencia fogalmának meghatározásakor. A mesterséges intelligencia (AI) az általános elnevezése az olyan gépek fejlesztési technológiájának, amelyek teljesen mesterséges eszközökkel jönnek létre, valamint képesek hasonló viselkedést és mozdulatokat mutatni, mint az ember. Tulajdonképpen olyan technikák összessége, amelyek lehetővé teszik a számítógépek számára az emberi viselkedés utánzását [3]. A fogalmat az 1950-es években kezdték el használni, ma számtalan területen alkalmazzák. Számos szektort érint és reformál nap mint nap. Beleértve az oktatást, a katonai területet és mindezek mellett a biztonsági szektorokat. A világ számos részén kiemelt figyelmet kap, új innovatív gyakorlatokkal vezetik és építik be az élet legkülönfélébb színtereibe. Érdekes példa erre az Egyesült Arab Emírségek, ahol még úgynevezett AI minisztériumot is létrehoztak, ezzel is támogatva nyitott szemléletüket a világ felé. Azt hogy nem létezik többé mobilprioritás, olyan világvezető informatikai szervezetek jelentették ki, mint a Microsoft, a Google, az Apple valamint a Facebook. Helyette

bevezették az úgynevezett AI-prioritást. Ennek elsődleges információforrásaként a különböző digitális asszisztenseket határozták meg.

A *humán biztonság* fogalmának meghatározásakor szintén több megközelítést is olvashatunk. Horváth Gergely szavait idézve, az emberi élet védelme és a munkabiztonság mellett azt is jelenti, „*hogy felkészítsük a felhasználókat, a szervezetünk munkatársait arra, hogy felelősen, a biztonságot veszélyeztető tényezők ismeretében végezzék a munkájukat. Továbbá legyenek felkészítve azoknak az eszközöknek és információs rendszereknek a használatára, amely szükséges a munkájukhoz, így is csökkentve az emberi hibákból fakadó biztonsági eseményeket*." [4]. Mógor a humán biztonság összetevőit csoportosítja. Elkülöníti a szakmai oktatás-képzést, a személyes kompetenciát, az ellenőrzést-értékelést-szankcionálását, a nemzetbiztonsági ellenőrzést, a megfelelő mértékű biztonságtudatosságot és a személyiségbeli megfelelősséget [5]. Péczeli Anna az 1994-es United Nations Development Program alapján a következő elveket fogalmazta meg: "*a humán biztonság általános érvényessége, hogy bárkit érinthet. Interdependens jellege szerint, ha bárki biztonságát fenyegetés éri az más emberekre is kihathat. Preventív jellegű, könnyebb megteremteni prevenciós intézkedésekkel, mint helyrehozni korlátozásokkal. Emberközpontúságát tekintve, a fókusz pontba az embert helyezi* "[6].

Az innovációk és fejlesztések beépítése, alkalmazása közvetlenül befolyásolják az országok oktatási és fejlődési szintjét. A mesterséges intelligencia segítheti a személyre szabott tanulási élmények megteremtését, adaptív oktatási rendszerek kialakítását, sőt a diákok teljesítményének elemzésével a hatékonyabb támogatást is.

Valójában az oktatás és maga az új technológiai vívmány kétoldalú kölcsönhatásban van egymással. A mesterséges intelligencia algoritmusainak létrehozásakor alapvető követelmény a megfelelő mennyiségű adatok összegyűjtése. Maga az oktatás folyamata ezt támogatja, illetve lehetővé teszi a különböző személyek, diákok, tanárok, szülők és iskolai alkalmazottak részéről érkező adatok rendszerezését. Ezek az átfogó információk egyrészt alkalmasak arra, hogy az oktatáspolitikában általánosságokon alapuló szakpolitikát hozzanak létre, valamint kiválóan alkalmazhatók a mesterséges intelligencia alapú szoftverek fejlesztésében.

Az oktatás területén számtalan újdonságot, fejlődést hoz magával a mesterséges intelligencia használata. Automatizálja az alapvető oktatási tevékenységet, mint például az osztályozást. Objektívebbé, átláthatóbbá teszi azt. Mindezzel megteremtve és támogatva a humán biztonságot. Megmutatja hol van szükség javításra, gyakorlásra és folyamatos visszajelzést ad. Az oktatási szoftverek a tanulók igényeihez igazíthatók. Egyfajta információs interakciót tanítanak arról hogyan és hol találunk hasznos információkat. mellyel támogatja és fejleszti a tanulók tanulási módszereit. A biztonságtudatosság fogalma ennél a pontnál különleges figyelmet igényel. A felhasználóknak tisztában kell lenni azzal, hogy milyen veszélyek állnak az alkalmazás hátterében, valamint milyen megoldásokkal kerülhetik el azokat.

A mesterséges intelligencia jobban tudja a társadalmi folyamatokat szemléltetni és modellezni. Ez egyfelől a multimédiás kezelőfelületnek köszönhető, melyen keresztül kommunikál a diákokkal. Ez a csatorna közelebb áll a jelenlegi tanulói generáció igényeihez és szemléletmódjához. A digitális bennszülöttek mindennapjainak részei a technológiai eszközök [7].

Biztonság fogalmával kapcsolatos definíciók tudományos források tükrében

A tudományos cikkeket olvasva definíciók tárháza végtelennek tűnik.

A f*izikai biztonság* fogalma több szempontból is definiálható. Jelenti a testi integritás és a vagyon védelmét, gondoljunk csak a mentőrobotokra [8]. A covid-19 világjárvány és más halálos járványok idején kiemelkedően fontos szereppel bírnak az úgynevezett orvosi robotok, melyek feladata a betegségek terjedésének mérséklésében illetve a beteges minőségi ellátásában merül ki [9]. Másfelől az épületek és infrastruktúra fizikai veszélyekkel szembeni védelmét takarja [10]. A *személyes biztonság,* mint a magánélet védelme. A biztonság, mint személyes biztonság a dinamikusan fejlődő technológiai fejlődés miatt kiemelkedő szereppel bír napjainkban. Kiemelt szerep jut a mobil biztonságra és az adatvédelemre, a személyek különféle veszélyekkel szembeni épségét és jólétét helyezve előtérbe . *Számítógépes biztonság* fogalmán az adatok, hálózatok és egyéb információs rendszerek vírusokkal és kibertámadásokkal szembeni védelmét értjük. A különféle eszközök internetes hálózata számos biztonságii kihívást eredményez. Ilyenek például a kriminalisztikai kihívások, a váratlan adathasználat, az egyes meghibásodási pontok, a blokklánc-sebezhetőségek, a gépi tanulás (ML), a mély tanulás (DL). *Egészségügyi biztonság* a betegadatok védelmét, az egészségügyi ellátás minőségét, valamint a páciensek egészségét jelenti. A biztonság és a magánélet védelme fontos szereppel bír az egészségügy területén is. A CIA modell, a titoktartát, integritást és rendelkezésre állást jelenti, az informatikai biztonság modellje. [3] Az elektronikus egészségügy biztonságának biztosítása során felmerülő kihívások közé tartoznak az etikai kihívások, a felhasználói hitelesítés, a titoktartás és integritás, az adatvédelmi politika, az adatvédelem, az adatbiztonság, a kiberbiztonság [11]. A kategóriák tárháza szinte végtelennek tűnik.

Az előzőekben felsorolt meghatározások és szemléletek közül több tényező is összekapcsolható rendszert alkot az oktatással. Valójában az oktatás és a biztonság szoros és elválaszthatatlan kooperációban áll egymással. A biztonság kiemelkedő fontossággal bír az oktatás minden területén. *Fizikai biztonság*nak nevezzük az épületek, a környezet, balesetekkel és bűncselekményekkel szembeni védelmét, mely egyben kiterjed a személyek fizikai biztonságára is. *Mentális-érzelmi biztonság* jelenti a támogató környezetet, mely mentálisan is biztonságos. Ennek kiemelt pontja az érzelmi támogatás, a bizalom és védelem. *A számítógépes biztonság* kiemelkedő szerepet kap a digitális oktatás, eszközök és az internet integrálásával. Ez egyben magába foglalja a diákok és iskolai rendszerek kiberfenyegetettségekkel szembeni online biztonságát. Az oktatás ma a digitális környezetben született és felnövő diákokkal más tanítási módszereket igényel [12]. *Egészségügyi biztonság* fogalmán a diákok és tanárok egészségének védelmét értjük a különböző oktatási intézményeken belül.

A mesterséges intelligencia fontos szerepet tölt be a kockázatkezelésben, illetve a kockázatelemzésben [13]. Innovatív jellegét adja például, hogy képes kockázatok előrejelzésére/predikcióra is, azaz a kockázatok jövőbeli valószínűségére és hatásaira is képes becsléseket tenni. Mindezek mellett a szövegfelismerés és elemzés, a kép és videó felismerés és elemzés, a beszédfelismerés és elemzés területeken is kiemelkedő és új eredményeket jelent. A különféle forenzikus területeken, mint például a felderítés, az adatok gyorsabb és

hatékonyabb elemzésében játszik nagy szerepet. A kapcsolati hálók felderítésével a különféle bűnszervezetek leleplezésében jelent előrelépést. Értékét növeli azon képessége, mely szerint azonosítja, előre jelzi és megelőzi az esetleges biztonsági fenyegetéseket. A kiberbiztonság területén mindenképp előremutató eredményeket vonz. Néhány példával alátámasztva ezt, mint a támadásdetektálás, a riasztáskezelés, a biztonságos felhasználói azonosítás, a spamszűrés, vagy éppen a logfájlok mély elemzése.

A mesterséges intelligencia fejlesztésekor fontos kérdés, hogy mekkora szintű autonómiát adnak a gépnek a fejlesztők [14].

Kritikus infrastruktúra- Kritikus információs infrastruktúra

A kritikus infrastruktúra elemei egymástól nem elkülöníthető szigetet alkotnak, köztük interminiszterális kapcsolat áll fenn. Fizikailag nem határolható el különálló közegekre, mint nép, nemzet. A kritikus infrastruktúra az egymással kölcsönös függésben álló infrastruktúra elemek, létesítmények, szolgáltatások, rendszerek és folyamatok interaktív kölcsönhatásban álló hálózata. A kritikus infrastruktúrák megléte és működése sokszor alapvető és tényszerű a társadalom számára. Sokszor észre sem vesszük azok gyakorlati létezését, mindaddig míg valamilyen hiba nem kerül a gépezetbe. Vegyük példaként egy számítógépes vírus elterjedését. Annak hatása gyakorlatilag életünk apró részeletéig érezhető, zavart okoz [15].

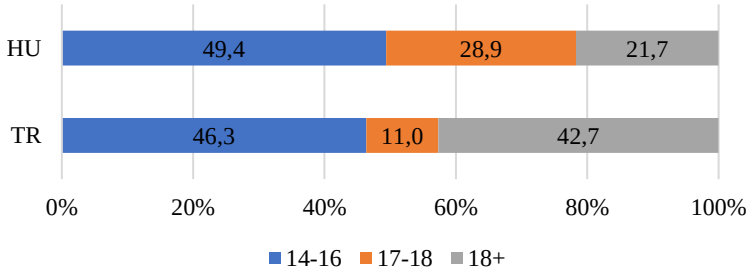
A kritikus infrastruktúra és a kritikus információs infrastruktúra között kölcsönös kapcsolat van, melyben mindkettő hasonló fontossággal bír. A rendelkezésre álló hálózatok összessége biztosítja a kritikus információs infrastruktúrát. A kritikus információs infrastruktúra azokat az infokommunikációs rendszereket jelenti, amelyek önmagukban is kritikus infrastruktúra elemek, vagy lényegesek az infrastruktúra elemei működésének szempontjából, például távközlés, számítógépek és szoftver, Internet, műholdak. Kritikus információs infrastruktúrák például az energiaellátó rendszerek és hálózatok, az infokommunikációs hálózatok, a kormányzati és közigazgatási infokommunikációs hálózatok, a nemzetvédelem működését biztosító infokommunikációs hálózatok [17].

Modern társadalmunkban az oktatás kritikus infrastruktúraként való elismerése egyre fontosabbá válik. Ha a kritikus infrastruktúra fogalmára gondolunk, mely szerint ide tartoznak azok a rendszerek és szolgáltatások, melyek alapvető fontosságúak egy ország működése és biztonsága szempontjából, nem less többé kérdés, hogy az oktatás vajon ide tartozik e. Olyan kulcsfontosságú funkciókat lát el, melyek elengedhetetlenek a társadalom és a gazdaság hosszú távú fejlődéséhez és fenntarthatóságához. Jelentősége több színtéren is megmutatkozik. A társadalom kohéziójának megerősítéséhez hozzájárulva, mindenki számára hozzáférést biztosít a tudás és képességek megszerzéséhez. Gazdasági szinten felkészít a munkaerő piacra, ezzel is is elősegítve a gazdasági fejlődést. Mindezek mellett elősegíti a kritikus gondolkodást, mely napjainkban kulcsfontosságú a biztonság és védelem szempontjából. Kihívásokat és lehetőségeket is rejt magában. Az oktatás digitalizációja szintén szignifikáns tényező napjainkban. Különös tekintettel a távoktatás és az online tanulási platformokon [18],[19],[20]. Tulajdonképpen ez nem csak a járványok miatt kapja ezt a szerepet, hanem az új munkaerőpiaci igényeknek is köszönhető. Az oktatásnak mindenki számára biztosítania kell a hozzáférhetőséget és inkluzivítást. Mindenkinek bárhonnan, bármilyen körülmények közül ugyanazt a minőséget kell elérhetővé tenni. Az oktatási

rendszer fejlesztésével egy biztonságosabb és prosperálóbb társadalom kialakulása érhető el [21][22]. Mindez építően hat a nemzetgazdaságok fejlődésére [23] és vállalkozások versenyképességére is [24][25], illetőleg a társadalmi jólét pozitív alakulására is befolyást gyakorol.

ANYAG ÉS MÓDSZER

Kutatásunk során a középiskolás és fiatal egyetemista diákok tanulási folyamatát vizsgáltuk egy kérdőíves kutatás keretén belül, az új technológiai eszközök beépítése szempontjából, kiemelt figyelemmel a mesterséges intelligencia használatára, az ahhoz kapcsolódó vélemények rávilágítására. A benne rejlő lehetőségekről és veszélyekről formált véleményüket kérdeztük meg egy előtesztelt sztenderdizált kérdőív segítségével. A célcsoportot magyar és török középiskolás diákok és egyetemisták alkották. A kérdőívet magyar és angol nyelven készítettük el, így a nemzetközi eredményeknek köszönhetően egyfajta összehasonlításra is lehetőség nyílt a két ország közt. Mivel a két nemzet eltérő oktatási rendszerrel dolgozik, a kapott mintákból egyéb következtetések is levonhatóak. A zárt kérdéseknek köszönhetően a kapott minták könnyen értékelhetőek. A kérdéseket a kutatási témámhoz kapcsolódva a mesterséges intelligencia beépítése a diákok tanulási folyamatába téma köré rendeztük. A digitalizáció, az MI használatáról alkotott véleményükre kerestük a választ. Hogyan gondolják, milyen mértékben befolyásolja az MI a jövőbeli munkalehetőségüket és a munka világát, az MI használata evolúciós előrelépést vagy evolúciós zsákutcát jelent számukra, illetve mennyire tartják az MI-t veszélyesnek az emberiségre. A kérdőívet online formában terjesztettük és töltötték ki a célcsoport tagjai. A magyar mintát 470, a török mintát 328 válasz alkotta. A következtetések levonása érdekében a hagyományos alapstatisztikai módszereken túl keresztábla elemzést is végeztünk. A kapott eredményeket a válaszadók életkora alapján értékeltük, amelyet az alábbi ábra mutat.

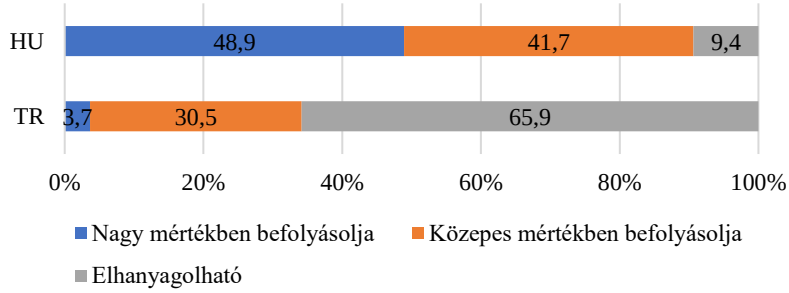


1. ábra: A magyar és a török minta összetétele a válaszadók életkora alapján
Forrás: saját kutatás, 2024, N = 470 (HU), N = 328 (TR)

EREDMÉNYEK

Elsőként arra voltunk kíváncsiak, hogy hogyan vélekednek a magyar és a török fiatalok a mesterséges intelligencia jövőbeli befolyásoló hatásáról. Az látható, hogy a magyar fiatalok közel fele úgy vélekedett, hogy ez nagy hatást fog gyakorolni a jövőben az életünkre, és több mint 40%-os aránnyal a közepes mértékű befolyásolásra és voksoltak. Így összesen a fiatalok 90%-ban erőteljes hatást tulajdonítottak a mesterséges intelligenciának a magyar mintában. A török fiatalok ezzel szemben viszont közel kétharmad arányban úgy

vélekedtek, hogy a mesterséges intelligenciának a jövőben elhanyagolható hatása lesz, és meglepő módon alig 4%-os értékkel vélekedtek úgy, hogy nagy mértékben lesz az befolyással az életünkre.



2. ábra: A magyar és a török fiatalok véleménye a MI jövőbeli befolyásoló hatásáról
Forrás: saját kutatás, 2024, N = 470 (HU), N = 328 (TR)

A továbbiakban a kereszttábla elemzés oszlopszázalékai segítségével megnéztük a válaszadók megoszlását az adott válaszok tekintetében a magyar és a török mintában egyaránt. Elmondható, hogy a török mintában a 14-16 éves korosztály 60%-ban tulajdonított elhanyagolható hatást a mesterséges intelligenciának, és meglepő módon a 17 éves, és annál idősebb válaszadók több mint 70%-ban vélekedtek így. Ez az arány a magyar mintában mindösszesen a 14 éves korosztályban volt csak 13% körüli, az idősebbek sokkal kisebb mértékben mondtak elhanyagolható hatást a mesterséges intelligenciának. A magyar mintában közel kétharmada arányban a 17 és 18 éves korosztály vélekedett úgy, hogy az nagymértékű befolyásoló hatást fog gyakorolni majd az életünkre.

		14-16	**17-18**	**18+**	
TR	Nagy mértékben befolyásolja	7,9%	0,0%	0,0%	3,7%
	Közepes mértékben befolyásolja	31,6%	27,8%	30,0%	30,5%
	Elhanyagolható	60,5%	72,2%	70,0%	65,9%
HU	Nagy mértékben befolyásolja	45,7%	57,4%	45,1%	48,9%
	Közepes mértékben befolyásolja	41,4%	39,7%	45,1%	41,7%
	Elhanyagolható	12,9%	2,9%	9,8%	9,4%

1. táblázat: A magyar és a török fiatalok véleményének megoszlása az MI jövőbeli befolyásoló hatásáról korcsoportonként (kereszttábla elemzés oszlopszázaléka)
Forrás: saját kutatás, 2024, N = 470 (HU), N = 328 (TR)

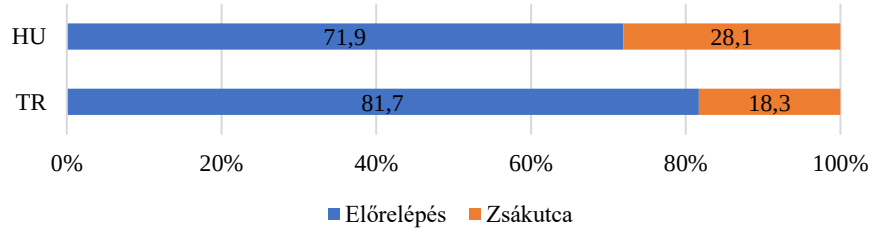
A továbbiakban szintén a kereszttábla elemzés segítségével vizsgáltuk meg azt, hogy hogyan alakulnak a korrigált sztenderdizált reziduumok a kérdés tekintetében. Azt tapasztaltuk, hogy az elvárt értékhez képest a török mintában a nagymértékű befolyást tulajdonított fiatalok aránya volt az elvárt érték felett a 14-16 éves korosztály esetén, és ugyanezt tapasztaltuk a 18 évesnél idősebbeknél, azonban náluk az elvárt érték alatti hatást látunk. A magyar minta tekintetében sokkal nagyobb eltérések voltak tapasztalhatók. A 14-16 éves

korosztály az elhanyagolható hatásra voksolt az elvárt értéken felül, és a 17-18 éves korosztály pedig a nagy mértékű befolyás tekintetében voksolt az elvárt értéken felül, és az elhanyagolható hatás tekintetében pedig alul. A Pearson-féle Chi-négyzet érték alapján megnéztük, hogy a kérdés megítélésére mennyire van hatással az életkor. Azt tapasztaltuk, hogy mindkét minta tekintetében egyértelműen kimutatható a szignifikancia, azaz ahol az 5% alatti értéket képvisel, ott véltünk hatást felfedezni a két tényező között. A Cramer-féle V értékkel megnéztük a hatás erősségét is, ami az érték alapján elhanyagolhatónak mondható.

		14-16	17-18	18+	Pearson Chi-Square	Cramer's V
TR	Nagy mértékben befolyásolja	3,8	-1,2	-3,0	0,004	0,153
	Közepes mértékben befolyásolja	0,4	-0,4	-0,2		
	Elhanyagolható	-1,9	0,9	1,4		
HU	Nagy mértékben befolyásolja	-1,4	2,3	-0,9	0,015	0,115
	Közepes mértékben befolyásolja	-0,1	-0,6	0,8		
	Elhanyagolható	2,6	-3,0	0,2		

2. táblázat: A korrigált sztenderdizált reziduumok értéke a magyar és a török mintában MI jövőbeli befolyásoló hatásáról korcsoportonként (kereszttábla elemzés)
Forrás: saját kutatás, 2024, N = 470 (HU), N = 328 (TR)

A kutatás további részében megvizsgáltuk a mintába bevont fiatalok véleményét a mesterséges intelligencia jövőjéről, hogy hogy tekintenek arra a válaszadók: előrelépésként, vagy zsákutcaként értelmezik azt. Itt nagyjából megegyező volt a válaszadók véleménye, döntő többségükben mindannyian előrelépésként értelmezték azt.



2. ábra: A magyar és a török fiatalok véleménye a MI jövőjéről
Forrás: saját kutatás, 2024, N = 470 (HU), N = 328 (TR)

A kereszttábla elemzés oszlopszázalékai alapján jelen esetben is megvizsgáltuk a korcsoportonkénti megosztásokat. A török mintában a 17 éves korosztály 80-90%-os arányban mondta, hogy előrelépés lesz a mesterséges intelligencia jövőben, míg a magyar válaszadóknál az előrelépés kissé alacsonyabb értéket kapott, 75% alatti arányban látták így a hasonló korosztályba tartozó fiatalok a jövőt. Mindebből az következik, hogy a magyar fiatalok szkeptikusak a mesterséges intelligencia segítő mivolta, jövőbemutató léte tekintetében. Inkább óvatosnak mondhatók, és tartanak a jövőbeli hatásoktól.

		14-16	17-18	18+	
TR	Előrelépés	78,9%	88,9%	82,9%	81,7%
	Zsákutca	21,1%	11,1%	17,1%	18,3%
HU	Előrelépés	71,6%	76,5%	66,7%	71,9%
	Zsákutca	28,4%	23,5%	33,3%	28,1%

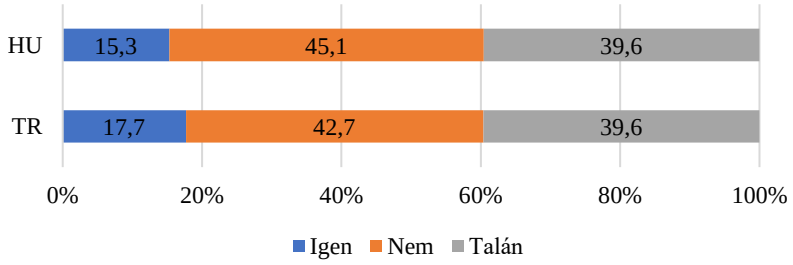
3. táblázat: A magyar és a török fiatalok véleménye a MI jövőjéről korcsoportonként (kereszttábla elemzés oszlopszázaléka)
Forrás: saját kutatás, 2024, N = 470 (HU), N = 328 (TR)

A korrigált sztenderdizált residuumok értéke alapján jelen esetben is megvizsgáltuk, hogy melyik korcsoport voksolt az elvárt érték alatt vagy felett. A reziduumok értéke alapján nem találtunk összefüggést egyetlen esetben sem, és jelen esetben nem volt kimutatható kapcsolat a Chi-négyzet érték tekintetében sem.

		14-16	17-18	18+	Pearson Chi-Square	Cramer's V
TR	Előrelépés	-1,2	1,2	0,5	0,343	0,081
	Zsákutca	1,2	-1,2	-0,5		
HU	Előrelépés	-0,2	1,4	-1,3	0,246	0,077
	Zsákutca	0,2	-1,4	1,3		

4. táblázat: A korrigált sztenderdizált reziduumok értéke a magyar és a török mintában MI jövőjéről korcsoportonként (kereszttábla elemzés)
Forrás: saját kutatás, 2024, N = 470 (HU), N = 328 (TR)

A kutatásunk utolsó részében arról kérdeztük a fiatalokat, hogy hogyan tekintenek a mesterséges intelligenciára, az veszélyt jelent számukra vagy sem. Jelen esetben, eddig nem látott módon a minta alapján azt tapasztaltuk, hogy a török és a magyar fiatalok véleménye nagyjából együtt mozog. Itt azt tapasztaltuk, hogy a magyar fiatalok kevésbé tekintik jövőben veszélyforrásnak, amely eredmény némiképp ellentmond a korábban tapasztaltakkal.



3. ábra: A magyar és a török fiatalok véleménye a MI veszélyt jelentő mivoltáról
Forrás: saját kutatás, 2024, N = 470 (HU), N = 328 (TR)

Végül a kereszttáblák eredményei alapján itt is megnéztük, hogy melyik korcsoportok hogyan vélekedik a mesterséges intelligencia jövőbeli veszélyforrás jellegéről. A török

fiatalok esetén legnagyobb arányban a 17-18 éves korosztály tart a veszélytől, ami a magyar mintában a 18 évesnél idősebb korosztályt jelenti. Akik nem tekintenek a mesterséges intelligenciára, úgy, mint veszélyforrás, azok a török minta 18 évesnél idősebb fiataljai voltak, a magyar mintából ezt pedig a 17-18 éves korosztályt jelentette.

		14-16	**17-18**	**18+**	
TR	Igen	18,4%	22,2%	15,7%	17,7%
	Nem	39,5%	44,4%	45,7%	42,7%
	Talán	42,1%	33,3%	38,6%	39,6%
HU	Igen	15,5%	11,8%	19,6%	15,3%
	Nem	48,3%	50,0%	31,4%	45,1%
	Talán	36,2%	38,2%	49,0%	39,6%

5. táblázat: A magyar és a török fiatalok véleménye a MI veszélyt jelentő mivoltáról korcsoportonként (kereszttábla elemzés oszlopszázaléka)
Forrás: saját kutatás, 2024, N = 470 (HU), N = 328 (TR)

A korrigált sztenderdizált reziduumok értéke alapján az elvárt érték tekintetében mindösszesen két esetben tapasztaltunk eltérést. A magyar minta 18 évesnél idősebb válaszadói adtak az elvárt érték alatti válaszarányt a „nem" válasz tekintetében, és a „talán" válasz esetén pedig az elvárt érték felett teljesítettek. A Chi-négyzet érték alapján szintén a magyar minta tekintetében látunk hatást a válaszokra, valamint a válaszadók életkorának kapcsolatára, ami a Cramer-féle V érték alapján ismét elenyésző hatás jelentett.

		14-16	**17-18**	**18+**	**Pearson Chi-Square**	**Cramer's V**
TR	Igen	0,3	0,8	-0,8	0,717	0,057
	Nem	-1,1	0,2	1,0		
	Talán	0,9	-0,8	-0,3		
HU	Igen	0,1	-1,4	1,4	0,028	0,108
	Nem	1,4	1,4	-3,2		
	Talán	-1,5	-0,4	2,2		

6. táblázat: A korrigált sztenderdizált reziduumok értéke a magyar és a török mintában MI veszélyt jelentő mivoltáról korcsoportonként (kereszttábla elemzés)
Forrás: saját kutatás, 2024, N = 470 (HU), N = 328 (TR)

KÖVETKEZTETÉSEK

A mesterséges intelligencia megjelenése és egyre szélesebb körű használata sokféle jövőképet inspirál. Világunk számos előnnyel, de megannyi veszéllyel fenyegető technológiával szembesül. Kiemelten fontos etikai és társadalmi szempontból, hogy előnyösebb normák felé irányuljon a mesterséges intelligencia használata és beépítése a különböző területeken. Fontos, hogy konkrét és konstrúktív válaszok szülessenek a társadalmi kihívásokkal kapcsolatban felmerülő kérdésekre. A különféle tudományterületeken alkalmazott technológiai változásokat látva érzékelhetjük, hogy a tudományok közti kapcsolat a mesterséges

intelligencia tükrében egyre összetettebb képet mutat. Szoros összefüggések, hasonló előrelépések és veszélyek tapasztalhatók. Akár az egyes utópikus látomásokat, akár az aggodalmasabb jóslatokat nézzük a fejlődés léptéke mindenképpen vitathatatlan, és megállíthatatlan.

A kutatás eredményei alapján megállapítható, hogy a mintába bevont fiatal korosztály meglehetősen megosztott a mesterséges intelligencia tekintetében. Több esetben is tapasztaltuk azt, hogy egymásnak ellentmondó válaszokat adtak a fiatalok, ami a kevésbé kiforrott háttértudásnak köszönhető. Összességében az mondható el, hogy az eredmények alapján a magyar fiatalok tűnnek tájékozottabbnak, és bizonyos kérdésekben óvatosabbnak, mint török társaik. A török fiataloknál nem látszódott az, hogy hogyan vélekednek tisztán a mesterséges intelligenciáról. Mindebből az következik, hogy az ismeretek bővítése tekintetében az oktatásnak nagyon fontos szerepe van a jövőben. Ahogy arról már a szakirodalomban is szó esett, nagyon fontos látni azokat a folyamatokat, amelyek az oktatási rendszerek tekintetében egyre jobban kirajzolódnak. A megváltozó igények és körülmények, az egyre fokozódó tanárhiány, az egyre erőteljesebb digitalizáció egyértelművé teszi azt, hogy a mesterséges intelligencia nagyon gyorsan be fog kerülni az oktatási rendszerbe is. Éppen ezért nagyon fontos az, hogy annak használatára megfelelő módon tudjuk felkészíteni a fiatalokat, hiszen a mesterséges intelligencia egyben eszköz, és másrészt pedig fegyver is lehet, amelynek nem jó használata akár az emberiség jövőjét is kockára teheti.

FELHASZNÁLT IRODALOM

[1] OECD, “Áttekintés Az információs rendszerek és hálózatok biztonságára vonatkozó OECD irányelvek: Útban a biztonságkultúra felé,” 2003. [Online]. Available: https://web-archive.oecd.org/2012-06-15/159501-15582292.pdf. [Accessed: Jun. 14, 2024].

[2] K. Lazányi, “A biztonsági kultúra,” Taylor: Gazdálkodás- és szervezéstudományi folyóirat: a virtuális intézet Közép-Európa kutatására közleményei, vol. 7, no. 1-2, pp. 398-405. [Online]. Available: https://ojs.bibl.u-szeged.hu/index.php/taylor/article/view/12936.

[3] C. Sönmez, “Yapay Zeka Nedir?,” Yapay Zeka Nedir? [Online]. Available: https://shiftdelete.net/yapay-zeka-nedir-62428. [Accessed: Jun. 14, 2024].

[4] G. K. Horváth, Adatbiztonság. Budapest: Budapesti Gazdasági Főiskola, 2014.

[5] T. Mógor, “Az emberi tényező szerepe az információbiztonság megvalósítása és erősítése terén. Az információbiztonsági kultúra fejlesztésének lehetőségei a Magyar Honvédségben,” Az Óbudai Egyetem Doktori Tanácsa, Budapest, 2017. [Online]. Available: https://doktori.hu/index.php?menuid=193&lang=HU&vid=17772. [Accessed: Jun. 14, 2024].

[6] A. Péczeli, “A humán biztonság elmélete és gyakorlata Kanada és Japán példáján,” Grotius, pp. 1–13, 2011.

[7] S. Savaş, “Artificial Intelligence and Innovative Applications in Education: The Case of Turkey,” Journal of Information Systems and Management Research, vol. 3, no. 1, pp. 14–26, 2021.

[8] J. Delmerico, et al., “The current state and future outlook of rescue robotics,” J. Field Robot., vol. 36, no. 7, pp. 1171–1191, Oct. 2019, doi: 10.1002/rob.21887.

[9] A. Di Lallo, R. Murphy, A. Krieger, J. Zhu, R. H. Taylor, and H. Su, "Medical Robots for Infectious Diseases: Lessons and Challenges from the COVID-19 Pandemic," IEEE Robot. Autom. Mag., vol. 28, no. 1, pp. 18–27, Mar. 2021, doi: 10.1109/MRA.2020.3045671.
[10] X. (Shirley) Li, S. Kim, K.W. Chan, and A. L. McGill, "Detrimental Effects of Anthropomorphism on the Perceived Physical Safety of Artificial Agents in Dangerous Situations," Int. J. Res. Mark., vol. 40, no. 4, pp. 841–864, Dec. 2023, doi: 10.1016/J.IJRESMAR.2023.07.002.
[11] B. J. Kim and J. B. Chung, "Is safety education in the E-learning environment effective? Factors affecting the learning outcomes of online laboratory safety education," Saf. Sci., vol. 168, p. 106306, Dec. 2023, doi: 10.1016/J.SSCI.2023.106306.
[12] M. Videnovik, T. Vold, L. Kiønig, A. Madevska Bogdanova, and V. Trajkovik, "Game-based learning in computer science education: a scoping literature review," Int. J. STEM Educ., vol. 10, no. 1, pp. 1–23, Sep. 2023, doi: 10.1186/S40594-023-00447-2.
[13] T. Guida, Big Data and Machine Learning in Quantitative Investment. Wiley, 2018. doi: 10.1002/9781119522225.
[14] Cs. Kollár, A mesterséges intelligencia megjelenése a biztonságtudományban. In: T. J. Karlovitz (szerk.) What will our Future be Like? 2 essays in German, 7 in English, 30 in Hungarian language, Grosspetersdorf: Sozial und Wirtschafts Forschungsgruppe, 2023, 448 p. pp. 242-256. , 15 p.
[15] Z. Rajnai and B. Fregan, "Kritikus infrastruktúrák védelme (jogi szabályozás)," Műszaki Tudományos Közlemények, vol. 5, pp. 349–352, 2016, doi: 10.33895/MTK-2016.05.78.
[16] I. Ozturk, "The Role of Education in Economic Development: A Theoretical Perspective," SSRN Electron. J., vol. XXXIII, no. 1, pp. 39–47, Dec. 2001, doi: 10.2139/SSRN.1137541.
[17] Z. Rajnai, "Kritikus infrastruktúra PhD előadás," May 13, 2024.
[18] M. Garai-Fodor and A. Popovics, "Analysing the Role of Responsible Consumer Behaviour and Social Responsibility from a Generation Specific Perspective in the Light of Primary Findings," Acta Polytech. Hung., vol. 20, no. 3, pp. 121-134, 2023.
[19] M. Garai-Fodor, L. Vasa, and K. Jäckel, "Characteristics of consumer segments based on perceptions of the impact of digitalisation," Decis. Mak.: Appl. Manag. Eng., vol. 6, no. 2, pp. 975-993, 2023.
[20] M. Garai-Fodor, L. Vasa, and K. Jäckel, "Characteristics of segments according to the preference system for job selection, opportunities for effective incentives in each employee group," Decis. Mak.: Appl. Manag. Eng., vol. 6, no. 2, pp. 557-580, 2023.
[21] Á. Csiszárik-Kocsir, J. Varga, and M. Garai-Fodor, "External professional assistance for small and medium-sized enterprises to solving the challenges of the pandemic," in IEEE 20th Jubilee International Symposium on Intelligent Systems and Informatics (SISY 2022), Subotica, Serbia, pp. 189-193.
[22] Cs. Kollár, "A biztonság megjelenése a humán tudományokban (1. rész)," Biztonságtudományi Szemle / Biztonságfilozófia és -történet, vol. 6, no. 2, 2024., pp. 13-22.
[23] Cs. Kollár, "A mesterséges intelligencia kapcsolata a humán biztonsággal," Nemzetbiztonsági Szemle, vol. 6, no. 1, 2018, pp. 5-23.

[24] J. Varga, “A szervezetek versenyképességének alapjai: a vállalati versenyképesség erősítésének lehetőségei,” in Vállalkozásfejlesztés a XXI. században: VII. tanulmánykötet, Á. Csiszárik-Kocsir, Ed. Budapest, Magyarország: Óbudai Egyetem, Keleti Károly Gazdasági Kar, 2017, pp. 725-743.
[25] J. Varga, “SMEs as the innovation flagships - where are the real economic drivers?” in IEEE 23rd International Symposium on Computational Intelligence and Informatics (CINTI 2023) Proceedings, Danvers (MA), USA, pp. 373-377.
[26] J. Varga, “The potential benefits of innovation as seen by some domestic businesses,” in SISY 2023 IEEE 21st International Symposium on Intelligent Systems and Informatics, Budapest, Magyarország: IEEE Hungary Section, pp. 223-228.

THE USE OF ARTIFICIAL INTELLIGENCE TO SECURE FOOTBALL MATCHES

MESTERSÉGES INTELLIGENCIA ALKALMAZÁSA A FUTBALL-MÉRKŐZÉSEK BIZTOSÍTÁSÁBAN

TURÓS Tímea[1] – SZŰCS Endre[2]

Abstract

The organisation of football matches is a complex task for specialists because of the popularity of the sport, but it is also a constant challenge due to the development of technical tools. The aim of our research is to examine the tools used in the security of matches at the international level with the emergence of Artificial Intelligence (AI) using a comparative analysis method with the tools currently used in domestic practice. The analysis focuses on AI tools that are commercially available and whose use can effectively assist the work of organizations that perform the security of football matches in Hungary. In the analysis, the effect of the tools that can have a positive impact on the security of matches and that fit well with the future vision of the collaborating organisations involved in the organisation of matches, that the creation of "Smart Cities" will result in the flow and centralisation of data, which will allow the effective filtering and individual sanctioning of illegal and disorderly behaviour among match spectators.

Keywords

Football match, safety and security, Artificial Intelligence (AI), positiv effect illegal behaviour

Absztrakt

A futballmérkőzések biztosítása a sportág népszerűségéből adódóan a szakemberek számára komplex szervezést igénylő feladat, ugyanakkor a technikai eszközök fejlődésének következményeként állandó kihívás is. Kutatásunk célja, hogy a Mesterséges Intelligencia (MI) megjelenésével nemzetközi szinten már alkalmazott eszközöket komparatív elemzés módszerével vizsgáljuk a jelenlegi hazai gyakorlatban alkalmazott eszközökkel. Az elemzés a MI olyan eszközeire irányul, amelyek kereskedelmi forgalomban elérhetőek és amelyek használata a magyarországi labdarúgó mérkőzések biztonsága szempontjából hatékonyan tudja segíteni a futballmérkőzések biztosítását végrehajtó szervezetek munkáját. Az elemzés során megvizsgáltuk az eszközök azon hatásait, amelyek a mérkőzések biztosítása szempontjából pozitív hatással bírhatnak és jól illeszkednek a szervezésben érintett, együttműködő szervezetek jövőbeli elképzeléséhez, miszerint a „Smart Cities” létrejöttével az adatok áramlásának és centralizálásának eredményeképpen hatékonyan kiszűrhetővé és egyénenként szankcionálhatóvá válnak a mérkőzések látogatói köréből az illegális magatartású, rendbontó elemek.

Kulcsszavak

Futballmérkőzés, biztosítás, Mesterséges Intelligencia (MI), pozitív hatás, illegális magatartás

BEVEZETÉS

[1] turos.timea@uni-obuda.hu | ORCID: 0000-0003-2505-8826 | PhD Student, Doctoral School for Safety and Security Sciences Óbuda University | Doktorandusz hallgató, Óbudai Egyetem Biztonságtudományi Doktori Iskola

[2] szendre63@gmail.com | ORCID: 0000-0003-2818-262X | Adjunct, Institute of Security Science and Cyber Defence Óbuda University | Adjunktus, Óbudai Egyetem Biztonságtudományi és Kibervédelmi Intézet

A mesterséges intelligencia történetét tekintve az 1950-es évek óta aktuális felvetés. Az első tapasztalatok szerzése arra irányult, hogy a gépek alkalmazása során mennyire helyettesíthető a humán erőforrás, képesek-e a gépek emberi viselkedésre, intelligens emberi viselkedésre. Az elmúlt évtizedekben a kutatások és az alkalmazott eszközök tapasztalatai alapján olyan eredményeket sikerült felmutatni, amelyek alapján a társadalmak számos szegmensén belül kezdték meg a MI eszközök használatát.

A társadalmak fejlődése, a munka és a szabadidős tevékenység egyértelmű elkülönülése a sportéletben is innovatív módon kezdett megmutatkozni. A sportágak kialakulásával és a szabályok egyértelmű meghatározásával, valamint szabálykönyvekbe való foglalásával időszerűvé vált a biztonságra való törekvés szervezett formában lévő megvalósítása. Az idő előrehaladtával a sportesemények biztonságának fenntartása szakemberek által meghatározott módon, az emberi erőforrás és az eszközök alkalmazásával, technológiai elvek alapján kerül végrehajtásra.

A technika rohamos fejlődésével, a szakembereknek lehetősége adódik széles palettáról kiválasztani a technológiához legmegfelelőbb, a végrehajtáshoz legoptimálisabb, hatékony eszközöket. A fő kutatási területünk a futballmérkőzések biztosításának vizsgálata. Ebben a kontextusban a biztosításba ténylegesen bevont erők és eszközök vizsgálatát tartottuk fontosnak, hazai és nemzetközi viszonylatban, annak tükrében, hogy a MI milyen módon és hogyan alkalmazható a futballmérkőzések vonatkozásában. A sportág sajátosságából és népszerűségből adódóan, a futball huliganizmus és a rendbontások figyelembevételével, az elmúlt évtizedek stadion katasztrófáinak tapasztalata alapján szükségesnek tartottunk megvizsgálni olyan, MI technológián alapuló rendszert vagy eszközöket, amely a futballmérkőzések biztosításában hatékonyan alkalmazhatók, továbbá a biztonság veszélyeztetője szankcionálható.

A BIZTONSÁG, A MI ÉS A TECHNOLÓGIA ÖSSZEFÜGGÉSEI

Anglia a futball „bölcsője”

A mai futball kialakulása évtizedeken át tartó folyamat letisztult eredménye. A világ számos pontján találhatók feljegyzések a sportág kezdetleges formájától, a mai szabályozott, modern futballig. A mérföldkőnek számító áttörés, amikor a futball és a rögbi végleg és szignifikánsan elkülönült, 1863-ban következett be, amikor Angliában megalapították az első Futball Szövetséget, illetve kimondták, sőt szabálykönyvbe is foglalták a játék legfontosabb alapelvét, hogy a labdához tilos kézzel hozzáérni. Ezzel egyidejűleg számos másik alapelvet is lefektettek, amelyek a mai labdarúgás alapjai is. A Szövetség megalakulását követően hamarosan az első, szemléletében és szervezésében is professzionálisnak mondható Liga is megalakult. [1]

Az angol Liga azonban nem csak sportszakmai téren számított úttörőnek. A sportág kialakulását végig kísérte, a fejlődésével párhuzamosan, a biztonságra való törekvés. Az események biztonsága ugyanolyan fontossággal bírt a sportesemények szervezése során, mint maga a sportág. Tekintettel arra, hogy a futball korábban is nagy tömegeket vonzott, mindenképpen szükséges volt olyan intézkedések bevezetése, amelyek a sportesemény ideje alatt garantálták a helyszínen a rendbontás mentes lebonyolítást, a nézők önfeledt szórakozását. Később a futball nemzetközi szinten is sportággá nőtte ki magát, ami a biztonság szempontjából újabb kihívások elé állította a kor szakembereit. A hatalmas tömegeket

vonzó mérkőzések helyszínei a mai kor stadionjaihoz nem voltak mérhetőek, így az egyik legnagyobb kihívást az infrastruktúra és a tömeg összefüggése okozta, ugyanis gyakran lépték túl a megengedett nézőszámot. A labdarúgás ezen szakaszában történtek a világ legnagyobb stadion katasztrófái.

A stadion katasztrófák olyan intézkedések bevezetését tette szükségessé, amelyek bevezetésével a katasztrófák bekövetkezési valószínűségét hatékonyan tudták csökkenteni. A futball létesítmények biztonságának fokozására először Taylor tett javaslatokat, nem is keveset és nem is megvalósíthatatlanokat. Konkrét stadion katasztrófa elemzését követően Taylor olyan javaslatokkal állt elő, amelyek alapjaiban változtatták meg a labdarúgó események biztosítását. A javaslatoknak köszönhetően többek között eltűntek a stadionokból a kerítések, a nézőket a pályához egészen közel engedték, valamint javaslata kiterjedt a stadionok átépítésére oly módon, hogy kizárólag ülőhelyek létesülhetnek. Mindehhez kőkeményen ragaszkodott, mert tisztában volt vele, hogy a további katasztrófák csak így kerülhetők el. [2]

A biztonság jelentősége

Az elmúlt évek erőszakos és terrorista cselekményei rávilágítottak arra, hogy a futballmérkőzések játékosai, a stábok és a technikai személyzete biztonsága mellett a nézők, szurkolók biztonságát és szórakozását is szem előtt kell tartani. Ugyanakkor ezen szempontok figyelembevételével elengedhetetlenül szükségessé vált a korábbinál szigorúbb intézkedések bevezetése, amelyek a mérkőzések során garantálják az esemény biztonságos lebonyolítását, emelve a színvonalát, eredményességét, ezen felül nyugtatóan hatnak az esemény szereplőire, látogatóira. Egy-egy ilyen mérkőzés lebonyolítása olyan kihívás elé állítja a szervezőket, amelyek megoldása egyre inkább támaszkodik a fejlett technikai megoldásokra és a MI eszközeire, a hatékony és gyors reagálás érdekében. Ugyanakkor a fizikai támadások mellett mindenképpen számolni kell a kiberfenyegetéssel, a közösségi médiák félretájékoztató hatásával és a támadások összehangolásával is. Mindezen fenyegetések időbeni felismerésére és megelőzésére előtérbe kerülnek azok az eszközök, amelyek a valós időben szolgáltatott nagy mennyiségű adat elemzésével a biztosítás végrehajtói számára azonnali reagálást tesznek lehetővé. Ennek érdekében a MI és gépi tanulási algoritmusok alkalmazásra kerülnek a videó megfigyelő rendszerekben. A biometrikus azonosítási technológiák (arcfelismerő, ujjlenyomat azonosító) a belépési jogosultság és az eseményről kitiltott személyek esetében kerülnek alkalmazásra. Az IoT eszközök és érzékelők rendszerbe történő bevonásával könnyebben kezelhetővé válik a túlzsúfoltság, a gyanús tevékenységek követése és a tömegkezelés. Korábban megfogalmazott elképzelések, tervek szerint a futballmérkőzések biztosításában áttörést hozhat a „Smart Cities” kialakulása.

Az integrált rendszerben történő adatáramlás átjárhatósága a biztosításban résztvevő minden szerv számára hozzáférést biztosít az adatokhoz, amelyek nem csak a sportlétesítményben, hanem annak környezetében, centralizáltan gyűjtik a biztosítás szempontjából releváns adatokat. Mindezek MI, biometrikus és drón eszközök alkalmazásával történő kiegészítése, a katasztrófahelyzetekre történő reagálás megtervezésével gyorsabbá teheti egyrészt a veszélyhelyzetek felismerését, másrészt a válasz reakciót. [3]

Az angol „minta”

Az angol futballvilág tragédiáinak ismerete alapján egyáltalán nem meglepő, hogy a futballmérkőzések biztosításában olyan intézkedések kerültek bevezetésre, amelyek a futballt alapjaiban megváltoztatták, szurkolói szempontból jelentősen. A kerítések lebontásával, a nézők játéktérhez való közelebb kerülésével új kihívások láttak napvilágot. A mesterséges intelligencia bevezetésével számos biztosítási elem vált hatékonyabbá. A biztonsági kamerák és felismerő rendszerek alkalmazásával a létesítmény belső és külső környezete is kontrollálható, a veszélyek forrásai és a gyanús személyek gyorsan azonosíthatók és kiszűrhetők. A MI eszközei alkalmasak a beléptetés során jogosultsággal nem rendelkezők vagy hamisított belépőjeggyel érkezők detektálására. A videófelvételek elemzése alkalmas az emberi viselkedés és a rendellenes cselekmények nyomon követésére. A hangosbemondó rendszereket vészhelyzetek esetén a nagyobb tömegek tájékoztatása céljából tudják használni, vészhelyzeti kommunikációs célokra. Célszerűen tűzvédelmi és egyéb riasztórendszerek telepítése elősegíti tájékoztatni a szükséges intézkedésekről a szervezőket és a nézőket. A MI arra is képes, hogy a kockázatelemzéshez figyelembe vegye a csapatok sajátosságait, az ellenfélhez való viszonyukat, szurkoló táborok egymás közötti kapcsolatát, vagy akár az aktuális társadalmi-politikai viszonyokat. A VIP boxok látogatói számára is különleges intézkedéseket alkalmaznak. Ezekbe a boxokba a bejutás külön bejáratokon vagy beléptető pontokon történik. A VIP látogatók részére a mérkőzések idejére is gyakori a személyi biztosítás. A boxok területét nagy felbontású kamerarendszerek monitorozzák, a gyors beavatkozás érdekében. A mentési tervek külön, a boxokból való menekülésre is készülnek, a sajátosságok figyelembevételével. A stadionokban a biztonsági személyzet nagy számban van jelen. Nagy részük képzett, nagy tapasztalattal rendelkezik nem csak a biztosítás, hanem a tömegkezelés és az elsősegélynyújtás terén is. Speciálisan képzettek a veszélyhelyzetek kezelésében és a rendezvénybiztosításban is. Effektíven képesek kommunikálni a hivatalos társ szervekkel, rendőrséggel tűzoltósággal. Az angol stadionokban a tűzijátékok, füstbombák, petárdák használata tilos, súlyos szankciókat von maga után.

Az angol stadionokban a múlt stadion katasztrófáinak következményeként és tapasztalataik feldolgozásának eredményeképpen a nézőtéri rendbontásokat szigorúan szankcionálják. A biztonság és a fegyelem megtartása érdekében a rendbontókat azonnal kiutasítják a stadionokból és számolniuk kell időszakos vagy életfogytig tartó kitiltással is. Természetesen a jogellenes magatartású egyéneknél fennáll az a kockázat is, hogy a jegyvásárlás során nem tud érvényesülni a továbbiakban, mert megtagadják tőle a lehetőséget. Vandalizmus vagy erőszakos cselekmények elkövetőit büntetőjogieljárás alá vonják, amelynek akár börtönbüntetés is lehet az eredménye. A rendbontókkal szemben erőszakos magatartás vagy károkozás esetén polgári jogi követelést is lehet eszközölni. A jogellenes magatartást tanúsítok ellen a klubok élhetnek azon jogukkal, hogy az egyén klubtagságát és ezzel a kedvezmények megvonását is kezdeményezhetik. [4]

A magyar „valóság”

A magyar stadionok nagy része az elmúlt években átépítésre, újjáépítésre került. A létesítés során nagy hangsúlyt fektettek a biztonsági kihívásoknak való megfelelésnek, nem csak a hazai, hanem nemzetközi mérkőzések vonatkozásában is.

Angliai mintára a Magyar Labdarúgó Szövetség biztonsági előírásait is úgy határozták meg, hogy a nemzetközi szabványoknak megfelelően a létesítmények rendelkezésre

tudjanak állni nemzetközi mérkőzések lebonyolítására is. A nagy elrettentő erővel bíró monumentális kerítések lebontásra kerültek, a nézőtér a pályához közelebb került, a régi vizes árkokat, futópályákat megszüntették. A stadionokban kialakításra kerültek kamera és videó és megfigyelő rendszerek, zárt láncú formában (CCTV). A nézőtér szektorait állóhelyek nélkül, ülőhelyekkel látták el, a befogadóképesség 100 %-ában. A stadion belsejében fogda helyiséget alakítottak ki a kiemelt rendbontók azonnali elhelyezésére a rendőrségi eljárás megkezdéséig. A beléptető rendszereket hibrid módon alakították ki. A belépési jogosultság ellenőrzése több lépcsőben, humán erőforrás és leolvasó rendszer együttes alkalmazásával történik. A beléptető kapuk kódleolvasóval szereltek, kiürítés szempontjából az automata nyitás nem megoldott, állandó humán erőforrást igényelnek. A stadionok általában nem szereltek biometrikus azonosító rendszerrel. Vénaszkennert mindössze egy hazai létesítményben találunk, ott sem népszerű a szurkolók körében. A VIP látogatók részére kialakított boxok biztonságát személyi és objektumvédelmi eszközökkel is garantálják. A VIP zóna látogatói a többi nézőtől elkülönítetten, már a parkoló használattól kezdődően, eltérő beléptető kapukon keresztül jutnak el a részükre kijelölt páholyokba. A különösen veszélyes tárgyak kiszűrése a humán erőforrás által, ruházat és csomagátvizsgálás formájában történik. Kézi detektorokat nem használnak, detektorkapuk nincsnek beépítve erre a célra. A biztonsági személyzet képzettsége nem feltétlenül felel meg a biztosítás követelményeinek, képzési rendszerük nem gyakorlat orientált, kommunikációs képességük átlag alatti, amely a szakmai tudás hiányosságairól is árulkodik. A pirotechnikai eszközök stadionba bevitele elméleti síkon tilos, azonban detektorok és röntgen átvizsgáló kapuk hiányában a biztonsági személyzet a kiszűrésükre többnyire alkalmatlan.

Kreditgyűjtő rendszer alkalmazhatóságának előnyei és hátrányai

A MI és eszközeinek széleskörű felhasználásával és gyors terjedésével összefüggésben, kutatásunkat kiterjesztettük egy bevezetésre, tesztelésre került rendszer vizsgálatára, konkrétan azzal a céllal, hogy használható és hatékony módszer lehet e futballmérkőzések biztosítása tekintetében. Az alapfelvetés kezdetben olyan ötlet volt, amely Kínában fogalmazódott meg és elsősorban, főként kezdetben a gazdasági életben képzett eredményt, mégpedig úgy, hogy az egyénekről gyűjtött információk alapján a bankok és a pénzügyi szervezetek ügyfél minősítése pozitív irányt vett. Az állampolgárokról megfigyeléséből, sőt nyomon követéséből származó információhalmaz kiértékelése után a hitelképesség vagy a törlesztési hajlandóság figyelembevételével olyan kategóriákba sorolhatták az egyéneket, amely pozitív vagy negatív adós színében tünteti fel őket, szankciók kiszabásának vagy éppen kedvezmények igénybevételének a lehetőségével. Kínában 2014-ben aztán úgy döntöttek, hogy az állampolgárok napi 24 órás felügyeletét országos szintűre terjesztik ki.

Eredményeképpen az állampolgárok megfigyeléséből származó adatok gyűjtése és kiértékelése az egyének büntetésére vagy jutalmazására szolgálhat. Ezeknek az adatoknak a feldolgozását, elemzését, kiértékelését a MI végzi. Elsődleges szándékként és fundamentumként azt a célt tűzték ki, hogy minden egyén egyedi azonosítóval legyen ellátva. A következő logikus lépésként az azonosítás adatai számára létrehozni olyan adatbázist, amely az egyedi azonosításra támaszkodva, az egyén a saját azonosítója alapján kapcsolja össze az adatbázisok tartalmát. Ezen technológia bevezetésével gyorsan és hatékonyan szűrhetők ki gyanús egyének, a gazdasági életben egyfajta megbízhatóság érhető el. A nagy mennyi-

ségű információ elemzésekor létrejövő statisztikai eredmények a vállalati mutatókat képesek jobbá tenni. A szankciók elkerülése érdekében mindenképpen megéri olyan magatartást tanúsítani, amely sokkal inkább kedvezmények igénybevételére forgatható át. A rendszer működése azonban számos problémát is felvet. Többek között a fejlesztések ellenére sem teljesen kiforrott rendszerről beszélünk. Az iszonyatosan nagy mennyiségű adatok kezelése és feldolgozása során előfordulhat, hogy az információ illetéktelen kezekbe kerül, hatalmas gazdasági károkat okozva ezzel. Az egyén privát szférája gyakorlatilag megszűnik. A gazdasági élet szereplői és az állam mindent tudnak az egyénekről, cégekről, így aztán fennáll a veszélye annak, hogy azokat az elemeket, amelyekkel nem szimpatizálnak könnyedén nehéz helyzetbe hozzák. A rendszer Kína határain kívül történő adoptálása régóta aktuális téma. Számunkra európai aspektusból érdekes a felvetés. Az európai kultúra és gazdaság szempontjából ott lehetne előnyösen alkalmazni, ahol a gazdasági élet feletti állami kontroll döntő jelentőségű. Minden szegmensre kiterjedő, állandó megfigyelés jelenleg nem aktuális az európai országok tekintetében. Vannak azonban olyan területei a társadalmi és gazdasági életnek, ahol részben adaptálható a rendszer. [5], [9]

Kreditgyűjtő rendszer alkalmazhatósága futballmérkőzések biztosításában

Azzal az elképzeléssel összefüggésben, hogy a „Smart Cities” létrejöttének következménye egy integrált adatgyűjtő-, feldolgozó rendszer felállítása, amely a biztosításban résztvevők mindegyik szerv számára adatokhoz való hozzáférést biztosít, a kreditgyűjtő rendszer egyes elemei kifejezetten előnyösek tudnak lenni. A szurkolókról gyűjtött és kielemzett adatok hatalmas segítséget nyújtanak a szervezők számára, a jogellenes cselekmények megelőzése és a gyors reagálás tekintetében. A folyamatos megfigyelésnek köszönhetően, az egyénről rengeteg információ áll rendelkezésre, amelyek átfogó képet adnak szokásairól, habitusáról, jogellenes tevékenységre való hajlamáról és rengeteg paraméteréről. A MI által végrehajtott kiértékelés az egyént kedvezményekben vagy szankciókban is részesítheti, kinek-kinek érdeme szerint. A jelenlegi, hazai és hazai rendezésű nemzetközi futballmérkőzések biztosítása során néhány dolog már bevezetésre került. A mérkőzések látogatását egyedi azonosítóhoz, úgy nevezett „klub kártyához” kötötték. Később ez a rendszer megdőlni látszott, azonban a bevezetésekor a kívánt hatást, a beazonosíthatóságot és ezzel együtt az igazmondási kötelezettséget részben elérték. Az egyedi adatok megadásával a szurkolók belépési jogosultságot szereztek, ezzel egyidőben elfogadták, hogy esetleges jogellenes cselekményük szankcionálható. Ugyanakkor a klubkártya tulajdonos a jegyvásárlás során érvényesíteni tudja elővásárlási jogát, a nem regisztráltakkal szemben. A jegyvásárlás során, a nyomon követhetőség és beazonosítás szempontjából külön kategóriának számít a kiemelt biztonsági kockázatú mérkőzésekre történő értékesítés. A szurkoló a jegyvásárlás során köteles személyes adatait, a szükséges mértékben. megadni.

A stadion területére történő beléptetés során az érvényes belépési jogosultsággal (jeggyel vagy bérlettel) rendelkező szurkoló előzetesen, a biztonsági személyzet általi jegyellenőrzésen, ruházat és csomagátvizsgáláson esik át. Ezt követően a beléptető rendszeren keresztül jut be a létesítménybe. A beléptetőkapuk alkalmasak a különböző szurkolótáborok szeparálásra is, a szektor alapján történő megkülönböztetésre. A mérkőzés ideje alatt videó megfigyelő rendszeren keresztül pásztázzák a nézőteret, amelynek információi egy erre a célra kialakított figyelőhelyre futnak be és a létesítményen belül kialakított vezetési pontnak

szolgáltatnak fontos információkat. Az angol példával összehasonlítva a jogellenes magatartást tanúsító vagy rendbontó egyéneket ugyanúgy azonnal kiemelik. A magyarországi gyakorlatban azonban nem tudtam fellelni olyan esetet, amikor az egyén kitiltásra került a létesítményből. Biometrikus azonosításra alkalmas rendszer mindösszesen egy magyarországi létesítményben került beszerelésre, osztatlan sikert azonban nem okozott a szurkolók körében. A szurkolók egyenesen a személyük ellen irányuló „sértésnek" vették a dolgot, szabotálták a mérkőzésre járást, amely a klub számára gazdasági kiesést és hírnéven esett csorbát is eredményezett. A kiemelt biztonsági kockázatú mérkőzések biztosításában aktívan résztvevő rendőri erők jelenléte erődemonstráló hatású, de korábban nem volt mindig elrettentő erejű. Az azonosíthatóság és képrögzítő technika alkalmazása óta azonban látványosan lecsökkent a tömegoszlatást igénylő esetek száma. A MI technológiával megtámogatott mérkőzés biztosítás klasszikus elemeként a tömegkezelési feladatok szoftver alapú megoldásai kizártak. Ezekben az esetekben mindenképpen élőerős beavatkozás szükséges. A MI technológia által gyűjtött és kiértékelt adatok alapján azonban a tömegkezelésbe történő beavatkozás reakció idejét hatékonyan le lehet csökkenteni, kvázi minimalizálni, az értesítéstől a felszámolásig bezárólag.

A kreditgyűjtő rendszer adaptálása és integrálása a mérkőzések biztosításban megosztó lehet. Szurkolói szempontból nyilván az előnyök, jogosultságok megszerzése szempontjából támogatásra találna. Azonban azt az oldalát is megvizsgálva, hogy a BIG DATA információk alapján a beazonosítás, az egyén nyomon követése, a róla rendelkezésre álló információk milyen hátrányokkal járnak, véleményem szerint a népszerűségét erősen befolyásolná. Annak tudatában pedig, hogy az összegyűjtött adatokat integrált központban elemzik, értékelik és átjárhatóságot biztosítanak az adatok hozzáféréséhez minden szervezet részére, biztos vagyok benne, hogy az előnyöket is „elhomályosítaná".

Az MI eszközök kereskedelmi kínálata

A stadionok biztonságtechnikai kihívásaihoz rendelkezésre álló eszközök palettája széleskörű. Fontos azonban leszögezni, hogy a biztonsági rendszerek üzemeltetése létesítmény specifikus, ezen felül hazai és nemzetközi követelményeknek megfelelően kialakított. Labdarúgó stadionok esetében a Magyar Labdarúgó Szövetség Biztonsági Szabályzatában foglaltak a mérvadók, amely paraméterek meghatározása a hazai és nemzetközi szabályzók, továbbá nemzetközi ajánlások figyelembevételével történik. A biztonsági eszközök és berendezések piacának vezető gyártóit Kína delegálja, kb. a piac 85%-ában. Az európai illetőségű gyártók biztonságtechnikai megoldásai jelen vannak a nemzetközi és a hazai gyakorlatban is. Kamerarendszerek tekintetében a Hikvision, Dahua, Geovision, DSC mellett további ~140 gyártó kínál innovatív eszközöket. Beléptetőrendszerek esetén a piacvezető márkák Assa Abloy, Hikvison, DSC, Paradox cégek mellett számos gyártó kínál megoldásokat. A gyártók innovatív eszközeinek választásában döntő szerepe van annak, hogy a létesítmény követelményeinek legmegfelelőbb, legújabb fejlesztés kerüljön alkalmazásra. [6]

Az MI szerepe a futballmérkőzések biztosításának jövőjében

A jelenlegi elképzelések a MI biztosítás során történő használatával kapcsolatban komplexitást és integritást igényelnek. A feladat végrehajtása a biztosításban résztvevők közötti proaktív együttműködésen alapul. A kommunikációs csatornák fejlődésének következményeként egyértelmű előrelépés tudna megvalósulni akár a megelőző intézkedések,

akár a végrehajtás során. Ezt az alapot olyan kiegészítő elemekkel, mint a biometrikus azonosítási rendszer, a MI és a drón technológia olyan szintre képes juttatni, hogy a létesítményben nagyobb kontrollt lehet gyakorolni és a biztosítás végrehajtásában résztvevők reakció idejét nagy mértékben lehet növelni.

A Dahua mélytanulási algoritmuson alapuló arcfelismerő forradalmian új technológiája lehetővé teszi az emberi arc valós idejű rögzítését, amely a MI által értékelhető, elemezhető és felhasználható a megelőzés és a biztosítás idején is. A mélytanulási algoritmus képes viselkedéselemzésre, ezáltal a MI azonnal kiszűri az agresszív viselkedést és 7riasztást generál. Starlight technológiája gyenge fényviszonyok közepette is jó minőségben rögzít, a szurkolók ismertetőjegyeit észlelő videóanalízisre képes és amennyiben a képességek eredményei összeadódnak, akkor azonnal megtörténik a riasztás. [7]

Tekintettel arra, hogy a fenyegetettség is állandóan változik, a biztonsági szakembereknek és az általuk használt eszközöknek naprakésznek kell lenniük a fenyegetettség felismerésében és az információk szűrésében. A röntgenvizsgálat tökéletes megoldás a stadion biztonság kihívásaira. Gyorsan és hatékonyan találják meg a fenyegetés eszközeit a szurkolók táskáiban, hátizsákjaiban, szállítmányokba. Az eszközök továbbfejlesztett változatai gyorsan áttelepíthetők, kevesebb létszámú biztonsági személyzet is elegendő a használatuk ideje alatt. Ráadásul a szkennerek nagy felbontású képalkotó technológiával vannak szerelve, amelyek képesek anyagok analízisére, ezzel együtt annak megállapítására is, hogy veszélyt okozó anyagról van e szó. Mindezt természetesen érintésmentesen, a csomagokba való tényleges benyúlás nélkül. Ezeken a tulajdonságon felül, a technológia teljesen objektív, elfogultságmentesen teszi, nem kivételez az esemény résztvevőivel. Ezzel megvalósítva az egyenlő bánásmód elvét. [8]

A biztosítás kihívásai tehát kiterjednek a változó fenyegetettségre, az érdekelt felek közötti együttműködés szükségességére, valamint egyfajta egyensúlyra a biztonsági és adatvédelmi szempontok között. A futballmérkőzések biztosításának eredményessége, a biztonság megteremtése és fenntartása a mérkőzés minden résztvevőjére nézve csak kollektív és kezdeményező - gyorsan cselekvő tevékenységgel érhető el.

ÖSSZEFOGLALÁS

A Mesterséges Intelligencia fejlődésének jelenlegi fázisában megvizsgáltuk, hogy a futballmérkőzések biztosításában milyen hatékonysággal alkalmazható technológiáról beszélünk. A stadionok biztonsági kihívásai már a XX. század második felében is gondolkodóba ejtették a biztonsági szakembereket. A stadionkatasztrófák tapasztalatainak feldolgozása során rávilágítottak, különös tekintettel a Taylor által megfogalmazottakra, hogy olyan intézkedésekre van szükség, amelyek hatékonyan járulnak hozzá a mérkőzések biztonságához és a résztvevőket nem veszélyeztetik.

Angliában, a futball szülőhazájában bevezetett intézkedéseknek köszönhetően a tapasztalatok azt mutatták, hogy mind a mérkőzések, mind pedig a nézők biztonsága óriási fejlődésen ment át. Ennek következtében a nemzetközi labdarúgásban ezeket az intézkedéseket más országok is bevezették, ugyancsak pozitív tapasztalatokkal. Az eszközök folyamatos fejlődésével egyszerűbben és hatékonyabban szűrik ki a jogellenes magatartást tanúsító személyeket, akik szankcionálása büntető eljárást és börtönbüntetést is vonhat maga után, amellett, hogy futballmérkőzés helyszíneitől időszakosan vagy véglegesen eltiltásra kerül. A mérkőzések biztonságát garantáló, Mesterséges Intelligencia technológia számos

eszköz képében gyűjt adatot, elemez, értékel annak érdekében, hogy a fenyegetettség minél előbb észlelhető legyen és a beavatkozás azonnal megtörténhessen. Az angol szurkolói kultúrában az új megoldások korábban elégedetlenséget, majd a biztonságérzet javulásával később elismerést váltott ki.

Magyarországi viszonylatban az angliai stadionok mintájára alkalmazott eszközök, azonosító rendszerek, képalkotó és videó elemző rendszerek, beléptető rendszerek és a stadion egyéb biztonsági rendszerei csak hosszú idő után válnak elfogadottá. Mindössze egyetlen magyarországi stadion van felszerelve biometrikus azonosító rendszerrel, de a szurkolók körében a mai napig nem vált népszerűvé. A biztosításban résztvevő szervek szoros együttműködése, elemző-értékelő előkészítő munkája azonban együttesen és proaktív módon hozza meg gyümölcsét.

A mérnöki tudományok innovációjának eredményeként egyre nagyobb teret hódító a MI technológiára kulcs szerep hárulhat a jövőben. A mesterséges intelligencia térhódítása pontosan illeszkedik a biztonsági szakemberek azon elképzelésébe, hogy a mérkőzések biztosításának jövője az „Okos városok" létrejöttével párhuzamosan tud kiteljesedni. Az integrált központba jutó hatalmas mennyiségű adat gyűjtésére, elemzésére és értékelésére a MI tökéletesen alkalmazható. A veszélyek azonosítása és a fenyegetettségre való gyors reagálás annak az eredményétől függ, hogy a MI milyen hatékonysággal tudja azonosítani a fenyegetést, illetve a riasztás milyen gyorsan következik be.

Vizsgálatunk arra is kiterjedt, hogy a mérkőzések biztonsága szempontjából milyen eredményesen alkalmazható például kreditgyűjtő rendszer. A Kínában tesztelt, az állampolgárok megfigyeléséből, nyomon követéséből gyűjtött információk alapján, az egyének viselkedésük és szokásaik elemzésének következtében jutalmazhatóvá vagy szankcionálhatóvá válnak. A magyar szurkolói kultúra jelenlegi formájában, a vénaszkenner példáját is alapul véve, nem elfogadó az ilyen jellegű azonosítási és elemzési módszerekkel szemben. Biztonsági szakemberek oldaláról megközelítve azonban, a MI technológia alkalmazásának forradalmi újításai kiszámíthatóbbá, hatékonyabbá teszik a biztonságérzet meglétét és fenntartását a stadionban jelenlévők számára. A jövőbeli elképzelések még jobban támaszkodnak a MI eszközeire, hiszen az összegyűjtött és kielemzett, értékelt adatok a biztosításban résztvevő szervek mindegyike számára elérhetővé válik, ennek következtében a végrehajtás lényegében már csak az együttműködés sikerességén múlik. A MI eszközök elfogulatlansága, befolyásolhatatlansága, objektív eredményre vezet, megteremtve ezzel az egyenlő bánásmódot is. Széleskörű alkalmazhatósága úttörő módon vezethető be az azonosítási, monitorozási, értékelő-elemző mechanizmusokba. A veszélyeztetettség mihamarabbi felismerésével, kiszűrésével lehetővé teszi a riasztástól számított gyors beavatkozást. A MI eszközök használata nem utolsó sorban a biztonsági személyzet szükségességét is lecsökkenti, miközben a biztosítás hatékonysága nem csökken.

A kereskedelmi forgalomban található biztonságtechnikai rendszerek és eszközök nagy része kínai gyártmány. Az európai gyártók kínálata sokszínű, a stadionok biztonsági rendszerének kiválasztása létesítmény függő, illetve a sportági szakszövetség biztonsági követelményeinek megfelelően kialakított. Egyre inkább elterjednek a MI technológiát alkalmazó eszközök, amelyek szerelése során fő szempont a legújabb, innovatív eszközök kiválasztása. Az azonosító, beléptető és egyéb biztonsági rendszerek által gyűjtött BIG DATA elemzésre a MI kiválóan alkalmas és hatékonyan alkalmazható. A mesterséges intelligencia

alkalmazása a mérkőzések biztosítása és a szakemberek szempontjából mérföldkő és a jövő technológiája.

FELHASZNÁLT IRODALOM

[1] The history of football (soccer) [Online] Elérhető: The history of football (soccer) (footballhistory.org)
[2] TURÓS T. - SZŰCS E. A futball és a mérkőzésbiztosítás fejlődésének összefüggései a kezdetektől az 1980-as évek végéig, BELÜGYI SZEMLE 71: 12, 2023. pp. 2145-2161.
[3] EKLER P. - PÁSZTOR D. Alkalmazott mesterséges intelligencia felhasználási területei és biztonsági kérdései – Mesterséges intelligencia a gyakorlatban, SCIENTIA ET SECURITAS 1: 1, 2020. pp. 35-42.
[4] ANDREW C. The 'Big Picture' to deliver a safe and secure sporting event and the challenges ahead, [Online]. Elérhető: https://www.linkedin.com/pulse/big-picture-deliver-safe-secure-sporting-event-challenges-cooke-wwqyc
[5] KOLLÁR Cs. Kína és a társadalmi kredit rendszere. *HADTUDOMÁNY: A MAGYAR HADTUDOMÁNYI TÁRSASÁG FOLYÓIRATA* 2020/2 pp. 79-97.
[6] Power Biztonságtechnika, [Online]. Elérhető: Forgalmazott márkák - Biztonságtechnikai Nagykereskedelmi Áruház (powerbizt.hu)
[7] ANDREW C. Security: assessing the future of sport security and technology, [Online] Elérhető: https://www.linkedin.com/pulse/security-assessing-future-sport-technology-andrew-cooke/
[8] JAMES T. Boosting stadium security with AI technology, INTERNATIONAL SECURITY JOURNAL May/2021 edition [Online] Elérhető: Exclusive: Boosting stadium security with AI technology (internationalsecurityjournal.com)
[9] KOLLÁR Cs. Kína és a társadalmi kredit rendszerének információbiztonsági kérdései. *BIZTONSÁGTUDOMÁNYI SZEMLE* 2020/2 pp. 93-109.

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