ISSN 2676-9042

Vol 5, No 1, 2023.

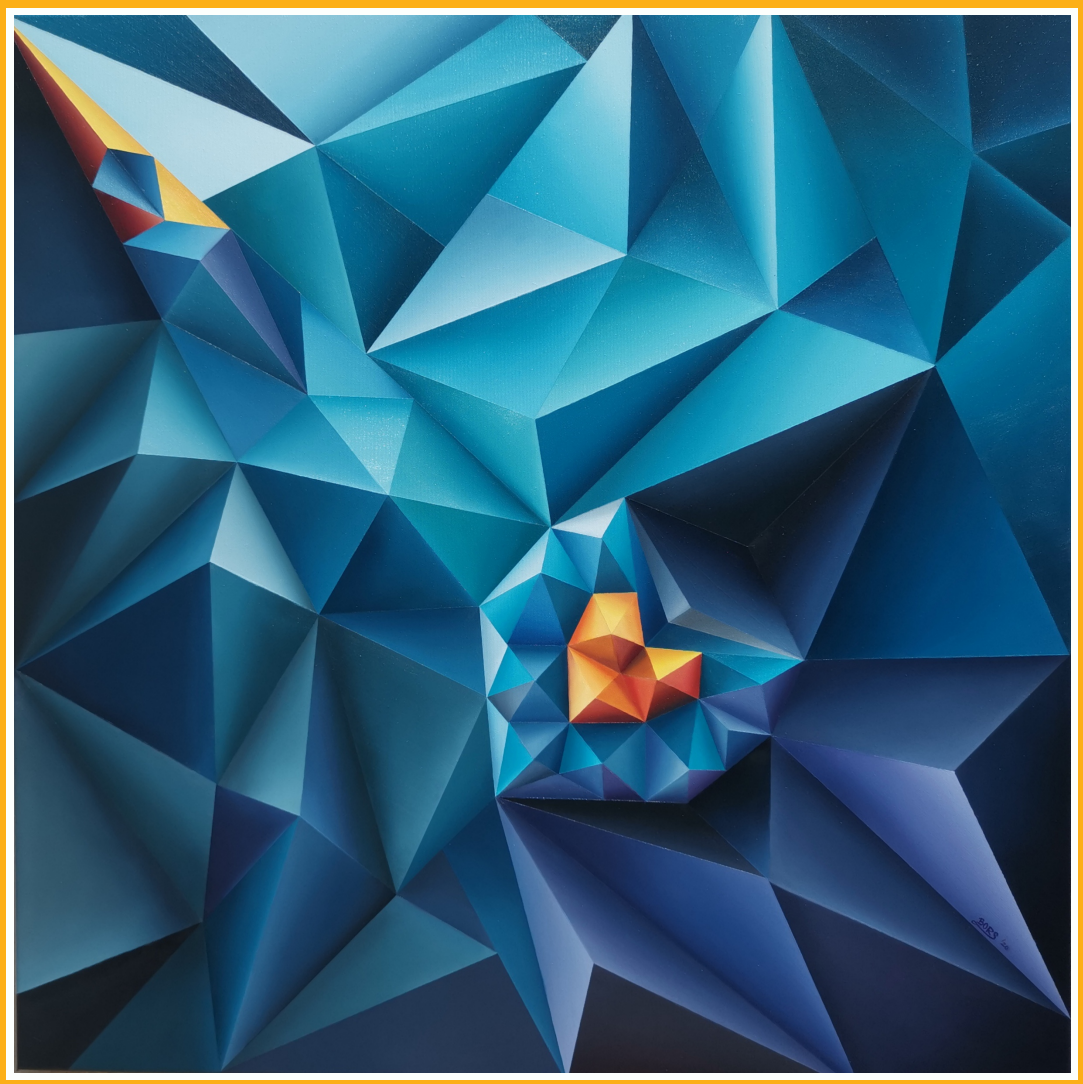
2023, V. évf. 1. szám

Safety and Security Sciences Review

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

Biztonságtudományi Szemle

a biztonságtudomány nemzetközi, lektorált, szakmai és tudományos folyóirata



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

On the cover can be seen | A borítón
BORS Györgyi
painter/festőművész
Hope | **Remény**
painting | című festménye látható

Our journal is indexed by the following databases | **Folyóiratunkat a következő adatbázisok indexelik**

EBSCO

epa.oszk.hu

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

MATARKA

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

Ó D A Óbudai Egyetem Digitális Archívum

Digital Archives of Óbuda University | Óbudai Egyetem Digitális Archívum

dk Országos Széchényi Könyvtár - Digitális Könyvtár

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

ULRICHSWEB™ GLOBAL SERIALS DIRECTORY

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

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

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 5, No 1, 2023. | **2023. V. évf. 1. szám**

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

BARNA Bianka Rita

biankabarna81@gmail.com

Bianka Rita BARNA is a security engineer and a graduate fire safety lecturer, whose research interests include the understanding and use of social engineering techniques for security purposes and the impact of artificial intelligence on everyday life. She is a member of the Artificial Intelligence Workshop at the University of Óbuda. Participated in Artificial Intelligence Workshop's ''The Past, Present and Future of Artificial Intelligence from the Perspective of Senior and Junior Experts'' as a junior expert.

BARNA Bianka Rita RITA biztonságtechnikai mérnök, végzett tűzvédelmi előadó. Kutatási területe a social engineering technikák megismerése és felhasználása biztonsági célokra, valamint a mesterséges intelligencia hatásai a mindennapi életre. Az Óbudai Egyetem Mesterséges Intelligencia Műhely tagja. Részt vett a Mesterséges Intelligencia Műhely „A mesterséges intelligencia múltja, jelene és jövője a senior és a junior szakértők szemszögéből" című kutatásában, junior szakértőként.

BODOR Károly

bodor.karoly@ek-cer.hu

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

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

CSERCSA Klaudia

csercsa.klaudia@phd.uni-obuda.hu

I am currently continuing my doctoral studies at the Obuda University in the Doctoral School of Security Studies. My research topic: Introduction of cybersecurity certification frameworks on the digital

Jelenleg az Óbudai Egyetemen folytatom doktori tanulmányaimat a Biztonságtudományi Doktori Iskolában. Kutatási témám: Kiberbiztonsági tanúsítási keretrendszerek bevezetése a Z generáció által alkal-

(online) educational platforms used by Generation Z. My supervisor is Prof. Dr. Zoltán RAJNAI. At the University of Óbuda, I taught Project Management, PR and Press Relations and Consumer Behavior subjects. I won a MNB Scholarship in 2021 and a National Higher Education Scholarship in 2020. I won 1st place at the Scientific Student Conference in 2021 and a Special Prize in 2020. I also worked as a demonstrator and tutor at Óbuda University. I performed official duties at Jánossy Ferenc Vocational College.

mazott digitális (online) oktatási platformokon. Témavezetőm Prof. Dr. RAJNAI Zoltán. Az Óbudai Egyetemen oktattam Projektmenedzsment, PR és sajtókapcsolatok, illetve Fogyasztói magatartás tárgyakat. 2021-ben MNB Ösztöndíjat, 2020-ban Nemzeti Felsőoktatási Ösztöndíjat nyertem. Tudományos Diákköri Konferencián 2021-ben 1. helyezést, 2020-ban Különdíjat nyertem. Ezenkívül demonstrátori, korrepetitori tevékenységet is végeztem az Óbudai Egyetemen. A Jánossy Ferenc Szakkollégiumban tisztségviselői feladatokat láttam el.

ERDŐDI László

erdodi.laszlo@nik.uni-obuda.hu

Dr. László ERDŐDI is Assistant Professor at the John von Neumann Faculty of Informatics and he is the head of the Ethical Hacking Training Center at Óbuda University. He is also Associate Professor at the University of Oslo and the head of the Hacking Arena in Norway. László Erdődi is the lecturer of several ethical hacking courses such as the Ethical hacking master course at the University of Oslo and organizer of various cyber security events such as the Hungarian Cyber Security Challenge (HCSC) and the Norwegian Cyber Security Challenge (NCSC). His research field is ethical hacking and within that software vulnerability exploitation, automation of hacking and power grid security. His mission is to combine the up-to-date practical hacking methods with scientific theories.

Dr. ERDŐDI László a Neumann János Informatikai Kar adjunktusa és az Óbudai Egyetem Etikus Hacker Oktatási Központjának vezetője. Emellett az Oslói Egyetem docense és a norvégiai Hacking Arena vezetője. Erdődi László több etikus hacker kurzus, például az Oslói Egyetem Ethical hacking mesterkurzusának előadója, valamint különböző kiberbiztonsági rendezvények, például a Hungarian Cyber Security Challenge (HCSC) és a Norwegian Cyber Security Challenge (NCSC) szervezője. Kutatási területe az etikus hackelés, azon belül is a szoftveres sebezhetőségek kihasználása, a hackelés automatizálása és az elektromos hálózatok biztonsága. Küldetése, hogy a korszerű gyakorlati hackelési módszereket tudományos elméletekkel ötvözze.

HEGYI Henrietta

hegyi.henrietta@uni-obuda.hu

Henrietta HEGYI is a student at the Doctoral School of Safety Sciences at the Bánki Donát Faculty of Mechanical and Safety Engineering, University of Óbuda. She holds a degree in Information Security from the National University of Public Service, Faculty of Electronic Information Security Management and the Ethical Hacker course at the University of Óbuda. His research interests include cybersecurity, information security, IT security, geopolitics. Besides his studies, he works as an IT security consultant and project manager.

HEGYI Henrietta az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Karán lévő Biztonságtudományi Doktor Iskola hallgatója. Információbiztonsági végzettségét a Nemzeti Közszolgálati Egyetem Elektronikus információbiztonsági vezető szakán és az Óbudai Egyetem Etikus Hacker tanfolyamán szerezte. Kutatási területei a kiberbiztonság, információbiztonság, informatikai biztonság, geopolitika. Tanulmányai mellett IT-biztonsági tanácsadóként és projektmenedzserként dolgozik.

KÓCZI Dávid

koczid@mk.u-szeged.hu

Dávid KÓCZI is a mechatronics and mechanical engineer, currently working as an assistant lecturer at the Faculty of Engineering of the University of Szeged, in the Department of Mechatronics and Automation.

KÓCZI Dávid okleveles mechatronikai mérnök, illetve gépészmérnök, jelenleg a Szegedi Tudományegyetem Mérnöki Kar, Mechatronikai és Automatizálási Intézet tanársegéde. A Robert Bosch Kft tech-

He is also a technical project manager at Robert Bosch Kft., where he is responsible for the development of electric vehicle steering systems. He is currently pursuing his PhD studies in the field of safety engineering at the Doctoral School of Safety Sciences at the University of Óbuda, with a focus on "Collaborative robot safety". Within this field, he actively researches possible forms of human-robot collaboration and the potential for safe implementation. His main areas of teaching include industrial robotics, industrial image processing, and control engineering, but he also teaches courses on the safety of machines and collaborative robots.

nikai projektvezetője, ahol elektromos autók kormányművének fejlesztésért felel. Műszaki tudományok területén folytat PhD tanulmányokat az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában, melynek témája a „Kollaboratív robotok biztonságtechnikája”, tématerületén belül aktívan kutatja az ember-robot együttműködés lehetséges formáit, azok biztonságos megvalósításának lehetőségeit. Fő oktatási területe, az ipari robotrendszerek, ipari képfeldolgozás, valamint az irányítástechnika, de oktatott tárgyai közé tartozik a gépek és kollaboratív robotok biztonságtechnikája is.

KOLLÁR Csaba

kollar.csaba@uni-obuda.hu

Csaba KOLLÁR communications engineer, certified communications specialist, head of electronic information security, doctor of economics (PhD), cybernetic, consultant, coach, mediator. His research interests include the social aspects and economic impacts of the digital age, in particular the human dimension of information security, the development of information security awareness, human-robot interaction, smart city, artificial intelligence, social credit system, and domotics. He is a senior research fellow at the Óbuda University, leader of Artificial Intelligence Workshop, lecturer and supervisor at the Doctoral School on Safety and Security Sciences, and at the National University of Public Service Doctoral School of Military Engineering. He is an examiner for professional qualification exams. He is a senior consultant, mediator and coach of PREMA Consulting, expert of the Hungarian Military Society and the National Association of Human Professionals. He has been a member of the Artificial Intelligence Consortium since Q4 2018.

KOLLÁR Csaba kommunikációtechnikai mérnök, okleveles kommunikációs szakember, elektronikus információbiztonsági vezető, a közgazdaságtudományok doktora (PhD), kibernetikus, tanácsadó, coach, mediátor. Kutatási területe a digitális kor társadalmi vetületei és gazdasági hatásai, kiemelten az információbiztonság humán aspektusa, az információbiztonság-tudatosság fejlesztése, az ember-robot interakció, az okosváros, a mesterséges intelligencia, a társadalmi kredit rendszere, a domotika. Az Óbudai Egyetem tudományos főmunkatársa, a Mesterséges Intelligencia Műhely vezetője, az Egyetem Biztonságtudományi Doktori Iskolájának és a Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskolájának az oktatója, témavezetője. Elnök a szakmai képesítő vizsgákon. A PREMA Consulting vezető tanácsadója, mediátora és coacha, a Magyar Hadtudományi Társaság és a Humán Szakemberek Országos Szövetsége szakértője. 2018. negyedik negyedévétől a Mesterséges Intelligencia Konzorcium tagja.

MÉSZÁROS Attila

m-attila@mk.u-szeged.hu

Attila MÉSZÁROS is a certified mechanical engineer, assistant lecturer at the Faculty of Engineering of the University of Szeged, in the Department of Mechatronics and Automation. He is completing his PhD studies at the Doctoral School of Safety Sciences of the University of Óbuda, his research topic is "Application and safety engineering examination of systems equipped with soft-robotic elements". Within his research he examines the application and development possibilities of soft-actuators in exoskeleton-type and industrial gripping technology systems. His

MÉSZÁROS Attila okleveles gépészmérnök, a Szegedi Tudományegyetem Mérnöki Kar, Mechatronikai és Automatizálási Intézet egyetemi tanársegéde. PhD tanulmányai az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában folytatja, kutatási tématerülete a „Soft-robotikai elemekkel ellátott rendszerek alkalmazási és biztonságtechnikai vizsgálata”. Kutatásain belül a soft-aktuátorok alkalmazási és fejlesztési lehetőségeit vizsgálja exoskeleton típusú, valamint ipari megfogástechnikai rendszerekben. Oktatási területe a mérés- és irányítástechnika, valamint a

field of study is measurement and control technology, as well as pneumatic and hydraulic controls. He is member of the Pneumatic systems and soft actuators research group.

pneumatikus és hidraulikus vezérlések. Tagja a Pneumatikus rendszerek és soft aktuátorok kutatócsoportnak.

OROSZI Eszter Diána

oroszi.eszter@silentsignal.hu

Eszter Diána OROSZI, CISA, CRISC, CISM is business informatics specialist, senior information security specialist and works as Head of Information Security Consulting Department of Silent Signal Ltd. She has 15 years'experience in the field of information security, with a special interest in human-based attacks, social engineering audits and security awareness improvement. She is PhD student at National University of Public Services, Hungary, her research area is measuring and improving security awareness level of users using gamification, especially applying her self-developed security awareness boardgame.

OROSZI Eszter Diána, CISA, CRISC, CISM gazdaságinformatikusként végzett, vezető információbiztonsági tanácsadó, a Silent Signal Kft. Információbiztonsági tanácsadás üzletágának a vezetője. 15 éves tapasztalata van az információbiztonság terén, kifejezetten a human-alapú támadások, Social Engineering auditok és a biztonságtudatosság fejlesztésének témakörében. Jelenleg PhD hallgató a Nemzeti Közszolgálati Egyetemen, kutatási területe az emberi tényező biztonságtudatosságának mérése és fejlesztése gamifikációs eszközökkel, kifejezetten a saját fejlesztésű biztonságtudatossági társasjátékával.

PÁL Anita Brigitta

pal.anita@hm.gov.hu

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

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

SÁROSI József

sarosi@mk.u-szeged.hu

Prof. Dr. József SÁROSI has diplomas in computer science and mechanical engineering for the food industry, currently he is the deputy dean for strategy and development at the Faculty of Engineering of the University of Szeged, and the head of the Department of Mechatronics and Automation. He obtained a doctorate (PhD) degree in the field of technical sciences by successfully defending the thesis Static and Dynamic Modelling and Accurate Positioning of Pneumatic Artificial Muscles at the Doctoral School of Technical Sciences of Szent István University in 2013, and obtained a habilitation doctorate from the same institution in 2019. From September 1, 2022, he is a full professor at the Faculty of Engineering at the University of Szeged. He is responsible for the bachelor's and master's degree programmes in mechatronic engineering. His main teaching area is measurement technology, his research areas cover soft actuators and the industrial and medical devices operated with them, as well as non-linear controls (e.g. sliding mode control). He is the head of the Pneumatic Systems and Soft Actuators research group.

Prof. Dr. SÁROSI József okleveles mérnök-informatikus, illetve élelmiszeripari gépészmérnök, jelenleg a Szegedi Tudományegyetem Mérnöki Kar stratégiai és fejlesztési dékánhelyettese, valamint a Mechatronikai és Automatizálási Intézet intézetvezetője. Műszaki tudományok területén szerzett doktori (PhD) fokozatot a Pneumatikus mesterséges izmok statikus és dinamikus modellezése, nagypontosságú pozicionálása c. értekezés sikeres megvédésével a Szent István Egyetem Műszaki Tudományi Doktori Iskolában 2013-ban, ugyanitt habilitált doktori címet szerzett 2019-ben. 2022. szeptember 1-jétől a Szegedi Tudományegyetem Mérnöki Kar egyetemi tanára. Szakfelelőse a mechatronikai mérnök alap- és mesterszaknak. Fő oktatási területe a méréstechnika, kutatási területei a soft aktuátorokra és az azokkal működtetett ipari és orvosi eszközökre, illetve a nemlineáris szabályozásokra (pl. csúszómód szabályozás) terjed ki. Vezetője a Pneumatikus rendszerek és soft aktuátorok kutatócsoportnak.

STEIN Vera

stein.vera@bgk.uni-obuda.hu

Vera STEIN is a certified engineer-economist, assistant lecturer and deputy director of the Institute of Mechatronics and Vehicle Engineering at the Bánki Donát Faculty of Mechanical and Safety Engineering, Óbuda University. Currently PhD student at the Doctoral School of the Safety and Security Sciences at the Óbuda University. Her research theme is the development of methods to support project-based education for safety, mechanical and mechatronic engineering study programs at Óbuda University.

STEIN Vera okleveles mérnök-közgazdász, az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar Mechatronikai és Járműtechnikai Intézetének oktatási intézetigazgató helyettese, tanársegéd. Jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskolájának PhD hallgatója. Kutatási témája a Projektalapú oktatást támogató módszerek fejlesztése az Óbudai Egyetem biztonságtechnikai, gépész- és mechatronikai mérnöki képzéseihez.

SZŰCS Gábor

szucs.gabor@phd.uni-obuda.hu

Gábor SZŰCS certified economist, wastewater treatment project manager. His research interest is the analysis of the safety technology of wastewater treatment networks (wastewater treatment plants and sewer networks) and their energy security, especially the development of a unified safety method for the analysis and evaluation of the protection of wastewater treatment plants as critical infrastructure elements according to the identification of plant

SZŰCS Gábor okleveles közgazdász, szennyvízkezelési projektmenedzser. Kutatási területe a szennyvíztisztító hálózatok (szennyvíztisztító telep és csatornahálózatok) biztonságtechnikájának, valamint ezek energiabiztonságának elemzése, kiemelten a szennyvíztisztító telepek, mint kritikus infrastruktúrai elemek védelmének elemzése, értékelése kapcsán egységes biztonságtechnikai módszer kidolgozása teleptípusok és méreteik azonosítása szerint. Az Óbudai

types and sizes. He is a second-year PhD student at Óbuda University's Doctoral School for Safety and Security Sciences, project manager at the Wastewater Treatment Department of the Deputy State Secretariat for the Implementation of the Prime Minister's Office, Transport, Environmental and Energy Efficiency Development Programs, Department of Public Works Development and Waste Management, and has been managing wastewater treatment and development projects for more than eight years.

Egyetem Biztonságtudományi Doktori Iskolájának másodéves doktorandusz hallgatója, a Miniszterelnökség Közlekedési, Környezeti és Energiahatékonysági Fejlesztési Programok Végrehajtásáért Felelős Helyettes Államtitkárság Közműfejlesztési és Hulladékgazdálkodási Végrehajtási Főosztály Szennyvíz kezelési Osztályán projektmenedzser. Munkája keretében több, mint nyolc éve lát el szennyvízkezelési és fejlesztési projektek menedzselését.

TAKÁCS-GYÖRGY Katalin

takacsnegyorgy.katalin@kgk.uni-obuda.hu

Prof. Dr. Katalin TAKÁCS-GYÖRGY is a professor in Károly Keleti Faculty of Economics, Institute of Organization and Management, Obuda University. She is also a member of Hungarian Academy of Science. Her research area is innovation, safety management of enterprises, risk of enterprise innovation, economics precision production.

Prof. Dr. TAKÁCS-GYÖRGY Katalin az Óbudai Egyetem Keleti Károly Közgazdaságtudományi Karának, Szervezési és Menedzsment Intézetének professzora. A Magyar Tudományos Akadémia tagja is. Kutatási területe az innováció, a vállalkozások biztonságmenedzsmentje, a vállalati innováció kockázata, a közgazdaságtan precíziós gyártás.

WU Yue

wuyue.budapest@gmail.com

WU Yue is a Ph.D. student at Doctoral School on Safety and Security Science, Obuda University. Her research interest is food security and sustainable agriculture. She is the president of Chinese Students and Scholars Association in Hungary at Obuda University.

WU Yue az Óbudai Egyetem Biztonság- és Biztonságtudományi Doktori Iskola hallgatója. Kutatási területe az élelmezésbiztonság és a fenntartható mezőgazdaság. Az Óbudai Egyetem Magyarországi Kínai Diákok és Tudósok Egyesületének elnöke.

ZAGYVAI Péter

Peter.Zagyvai@eli-alps.hu

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

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

sultant, to the working units of the International Atomic Energy Agency (IAEA) involved in emergency management and response, and the decommissioning of facilities.

International Atomic Energy Agency (IAEA) baleset-elhárítással és létesítmények leszerelésével foglalkozó munkacsoportjaiban.

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 5, No 1, 2023. | **2023. V. évf. 1. szám**

CONTENT | TARTALOM

Security Systems column | Biztonságtechnika rovat

Food Safety column | Élelmiszer-biztonság rovat

Information Security column | Információbiztonság rovat

Industrial and Operational Safety column | Ipar- és üzembiztonság rovat

Private Security column | **Magánbiztonság rovat**

MECHANICAL PROTECTION FOR WASTE WATER TREATMENT PLANTS

MECHANIKAI VÉDELEM A SZENNYVÍZTISZTÍTÓ TELEPEK ESETÉBEN

SZŰCS Gábor[1]

Abstract

The article starts with an examination of the situation of wastewater treatment plants, clarifying what kind of wastewater treatment plants exist. In the following section, I will review the complex asset protection of wastewater treatment plants. I will examine which element of mechanical protection is the first to contribute to asset protection in the case of a WWTP, highlighting the fences and gates that are part of mechanical protection. In the remainder of the article, I will carry out a study of the fences of some wastewater treatment plants, based on images on Google Earth and Maps. Based on this analysis, I draw conclusions.

Keywords

waste water treatment plant, mechanical protection, fence, gate, test, overview

Absztrakt

A cikk a szennyvíztisztító telepek helyzetének vizsgálatával kezdődik, melyben tisztázásra kerül, hogy milyen szennyvíztisztító telepek vannak. A további részben áttekintem a szennyvíztisztító telepek komplex vagyonvédelmét. Megvizsgálom, hogy a mechanikai védelem melyik eleme az első, amely hozzájárul a vagyonvédelemhez a szennyvíztisztító telep esetében, melyben kiemelem a mechanikai védelemhez tartozó kerítéseket és a kapukat. A cikk további részében a Google Earthn és Mapsn látható képek alapján néhány szennyvíztisztító telep kerítésének vizsgálatát végzem el. A vizsgálat alapján következtetéseket vonok le.

Kulcsszavak

Szennyvíztisztító telep, mechanikai védelem, kerítés, kapu, vizsgálat, áttekintés

[1] szucs.gabor@phd.uni-obuda.hu |ORCID: 0000-0002-3489-3391| PhD student, Óbuda University Doctoral School on Safety and Security Sciences |doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

BEVEZETÉS

Mindennapi tevékenységeink során szennyvíz keletkezik. A szennyvíz a környezetünkből csatornarendszeren keresztül távozik, ha erre nincs lehetőség házi emésztőgödrökbe[2] kerül. A házi emésztőgödrökből költségtérítés ellenében a szennyvíz elszállítás megtörténik a tisztítás helyére. Az elvezetett, elszállított szennyvíz tisztítását el kell végezni, hogy ne legyen belőle probléma. Tisztítást az erre a célra épített szennyvíztisztító telepen végzik el.

A cikkben megvizsgálom a szennyvíztisztító telepek helyzetét, hogy milyen fenyegetettségnek vannak kitéve. Áttekintem a mechanikai vagyonvédelem elemeit kiemelten közülük a kültéri védelem részét képező kerítéseket, kapukat. A kutatás a Google Earthn és a Google Mapsn elérhető képeken megjelenő információk alapján végzem el, rámutatok a különböző kialakítási lehetőségekre.

A SZENNYVÍZTISZTÍTÓ TELEP HELYZETÉNEK VIZSGÁLATA

A zavartalan létezésünk egyik fontos eleme a szennyvíz kezelés rendelkezésre állása. A rendelkezésre állás biztosítása az állam feladata, melyet azzal biztosítja, hogy megalkotja azokat a jogszabályokat, amelyek megteremtik az alapokat. Az alapok kijelölése után kezdődhet meg a konkrét megvalósítás, melyhez az Európai Unió irányelvet fogadott el.

A települési szennyvíztisztításról szóló, 91/271/EGK uniós tanácsi irányelv megfogalmazta a felszíni vizek minőségének helyreállításával, a szennyező anyagok koncentrációjának csökkentésével, valamint a felszín alatti vizek szennyeződésének visszaszorításával kapcsolatos célokat. Kimondja, hogy az önkormányzatoknak kötelessége gondoskodnia az adott városban/településen a megfelelő szennyvízkezelésről, meg kell szüntetniük a ”laza” vízelvezető rendszereket. Az irányelv tartalmazza, hogy a legalább 2000 lélekszámmal rendelkező települések önkormányzatának szennyvízcsatorna-hálózatot kell kialakítania. [3]

Az irányelv tehát a 2000 fős önkormányzatok feladatává teszi a szennyvíztisztítás elvégeztetését, melynek része a szennyvízcsatorna-hálózat megterveztetése, kiviteleztetése és működtetése.

A zavartalan rendelkezésre állást több tényező is akadályozhatja, mint például a rendkívüli időjárási viszonyok következményei, vagy a terrorista támadások.

A terrortámadások valószínű célpontjai között vannak a kritikus infrastruktúra elemek, melyet alátámasztanak a spanyol vasút és a brit közút ellen elkövetett támadások.

A kritikus infrastruktúra hazai meghatározása a Kritikus Infrastruktúra Védelem Nemzeti Programjáról szóló 2080/2008. (VI. 30.) Korm. határozat [4] 1. sz. melléklet 3.2. pont szerint melynek a lényege, hogy a kritikus infrastruktúrák a különböző hálózatok és annak elemei, az erőforrások és szolgáltatások, termékek, a fizika vagy információtechnológiai rendszerek és azok alkotó elemei, részei, melyek egymásra hatással vannak és ennek következtében működésük kiesése vagy megsemmisülésük azonnal vagy késleltetve rövid vagy hosszú ideig súlyos hatást fejthetnek ki hazánk életére ezen belül a nemzetgazdaságra, a szociális helyzetre, a közegészségügyre, a közbiztonságra, a kormányzat (beleértve az települési önkormányzatokat is) működésére és a nemzetbiztonságára. [1.]

[2] A házi emésztőgödrök olyan területen vannak, ahol a szennyvízcsatorna hálózat nincs kiépítve.

A meghatározás alapján az olyan rendszerek, amelyek működésének fenntartása az állampolgárok zavarmentes életének biztosítását szolgálják létfontosságúak.

Az Országgyűlés a létfontosság fenntartása érdekében törvényt alkotott, amely a 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről. [5]

A törvény tehát már a létfontosságú rendszerek és létesítmények megfogalmazást alkalmazza. A létfontosságú rendszerek és létesítmények között van nevesítve ágazatként a víz és a hozzátartozó alágazatként a szennyvízelvezetés és -tisztítás.

A szennyvíztisztító telepek közül a létfontosságú vízgazdálkodási rendszerelemek és vízilétesítmények azonosításáról, kijelöléséről és védelméről szóló 541/2013. (XII. 30.) kormányrendelet a következőket rögzíti a 2.§ "(2) A szennyvízelvezetés és -tisztítás területén nemzeti létfontosságú rendszerelemként kell azonosítani a) azt a szennyvíztisztító telepet, amelynek kapacitása meghaladja a 250 000 lakosegyenérték szennyezőanyag-terhelést, és működésképtelenné válása a felszíni víz jelentősen kedvezőtlen állapotát eredményezi, b) azt a közműves szennyvízelvezetést és -tisztítást biztosító víziközmű-rendszert, amelynek a felhasználói egyenértéke a Vksztv. szerinti működési engedélyben foglaltak szerint meghaladja a százezret." [6]

Magyarország települési szennyvíz-elvezetési és -tisztítási helyzetét nyilvántartó Településsoros Jegyzékről és Tájékoztató Jegyzékről, valamint a szennyvíz-elvezetési agglomerációk lehatárolásáról szóló 379/2015. (XII. 8.) kormányrendelet 1. számú melléklet 5. Műszaki, gazdasági szempontok és követelmények rész 5.6. Szennyezőanyag-terhelések számítása alrész ba)-be) pontok tartalmazzák a lakosegyenérték meghatározást, mely szerint az egyes települések névleges terhelését az alább felsorolásra kerülő terhelések jelentik.

- "a helyben lakó népesség,
- egyéb népesség (üdülő stb.),
- az Irányelv 11. cikkében szereplő ipari kibocsátások,
- vállalkozásokból és gazdasági tevékenységekből (beleértve a kis- és középvállalkozásokat) származó, olyan ipari szennyvíz, amelyet a szennyvíztörzshálózatba vagy települési szennyvíztisztító telepre bocsátanak ki, vagy oda tervezik kibocsátani,
- az összes fennmaradó települési szennyvíz és szennyvíziszap függetlenül attól, hogy szennyvíztörzshálózatokkal összegyűjtésre kerül vagy nem, de az agglomerációban keletkezik és amely nem foglalja magában az olyan ipari szennyvíz okozta terhelést, amelynek tisztítása külön történik, és a tisztított szennyvizet más szennyvízzel történő keveredés nélkül bocsátják a befogadóba." [7]

A szennyvíztisztító telepek közül tehát nem mindegyiket azonosítják a jogszabály szerint létfontosságú rendszerelemnek. Az azonosított szennyvíztisztító telep védelmét meghatározott követelmények szerint kell biztosítani, de a nem azonosított szennyvíztisztító telep esetében is fontos a megfelelő védelem. A nem azonosított telep védelmének követelményeit az üzemeltetőnek kell meghatározni.

A szennyvíztisztító telepet különböző veszélyek fenyegethetik, amelyek az alábbiak lehetnek.

- betöréses lopás,
- rongálás,

- belső lopás,
- engedély nélküli szennyvíz elhelyezés (leeresztés),
- baleset (például munkavállaló műtárgyba esése),
- terrorista támadás.

Az azonosított szennyvíztisztító telep esetében a legnagyobb kockázatot a terrorista támadás jelenti, míg a nem azonosított szennyvíztisztító telep esetében a belső lopás, vagy baleset is jelentős kockázat lehet. Minden szennyvíztisztító telep esetben kockázatértékelést kell készíteni, melynek az eredménye meghatározó lesz a mechanikai vagyonvédelem kialakítására is.

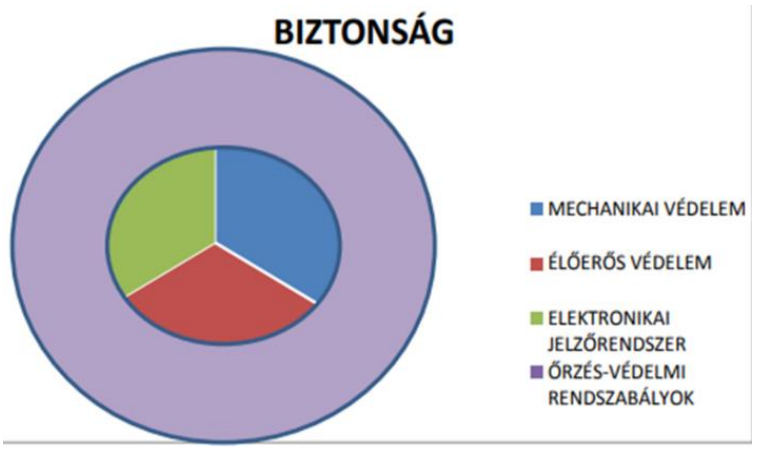
A SZENNYVÍZTISZTÍTÓ TELEP KOMPLEX VAGYONVÉDELME

A jogszabályban elrendelt védelemnek a telep vagyonelemeit, illetve a szennyvíztisztítás folyamatos fenntartását kell biztosítani.

A szennyvíztisztító telep őrzését és védelmét komplex vagyonvédelmi rendszerrel lehet biztosítani.

A komplex vagyonvédelmi rendszer részei:

- a mechanikai védelem,
- az elektronikai jelzőrendszer,
- az élőerős védelem,
- az őrzés-védelmi rendszabályok,
- és a biztosítás.



1.ábra A védelmi erőforrások és az alkalmazott rendszabályok kapcsolata [2. 89.o.]

Az ábrán látható a vagyonvédelem négy eleme, amelyek erőforrások és rendszabályok kapcsolatát jelenítik meg. A biztosítás nincs jelölve az ábrán, mert biztosítás köthető az elemek közül a mechanikai védelem, elektronikai jelzőrendszer eszközeire, az élőerő személyeire, de nem lehet biztosítást kötni őrzés-védelmi rendszabályokra. A körcikkek mérete nem minden esetben azonos arányú, mert az arányuk a kockázatértékelés alapján megállapított veszélyeztetettség szint alapján dönthetjük el, tehát az egyik körcikk kisebb, míg a másik nagyobb lesz.

Ez nagyban függ attól, hogy milyen jellegű objektum őrzéséről-védelméről kell gondoskodnunk. A szennyvíztisztító telepek között tehát vannak azonosítottak és nem azonosítottak, melyek komplex vagyonvédelme akkor valósítható meg, ha megállapítjuk az elemek közötti arányokat.

A cikkben csak a szennyvíztisztító telepek komplex vagyonvédelmének részét képező mechanikai védelem két elemét a kerítést és a kaput vizsgálom a többi elemet a következő cikkekben tekintem át.

Mechanikai védelem

Az egyik legősibb védelmi forma. Kutatások bebizonyították, hogy már az ősember is használta különböző kerítéseket készített kőből, fából, melyek távol tartották tőle és a megszerzett zsákmányától a vadállatokat, valamint a nem közvetlen társait is.

Mára már a mechanikai védelem egyik elengedhetetlen része lett a komplex vagyonvédelemnek, több területet foglal magába:

- a kültéri védelmet,
- az építményvédelmet,
- a tárgyvédelmet.

A felsorolt védelmi elemek mindegyike meg van a szennyvíztisztító telepen.

Kültéri védelem

A kültéri védelem a mechanikai védelem első eleme. Hatékony megelőző védelmi eszköz, mert már a szennyvíztelep ellen jogellenes cselekedet elkövetőt akadályozza, illetve nehezíti, késlelteti a behatolásban.

A kültéri védelem elemei az alábbiak.

- kerítések,
- kapuk,
- sorompók,
- árkok,
- töltések.

A kerítés jelölheti – az esetek többségében így is van - a telekhatárt és egyben az őrzés-védelem határát. A kerítések közül nagy sok fajta áll rendelkezésre, melyek jellemzően a készítésük anyagaiban különböznek. A szerkezeti felépítésük hasonló.

A kerítések fajtái az alábbiak lehetnek az anyaguk alapján:

- fa,
- kő,
- beton,
- tégla,
- alumínium,
- kovácsoltvas,
- drótháló,
- acélháló,
- műanyag.

A kerítések késleltetőképessége függ:

- a fajtától,
- a magasságtól.

A kerítés akadályozó és késleltetőképessége meghatározható azzal, „*hogy beton alappal rendelkezzen és a magassága 1,8- 2,8 m legyen*” [2. 22.o.], valamint *„magasságának és megbízhatóságának növelésére hatékonyan alkalmazható a sorokban kifeszített, vagy a tekercs spirál alakban széthúzott és rögzített tüskés, vagy pengés drót.”* [2. 22.o.]

Az akadályozó és késleltetőképesség akkor biztosított, ha a kerítés megfelelően van elkészítve. A beton alap esetén kettő féle megoldás van alkalmazásban. Az egyik az előre gyártott betonelemek, míg a másik az öntött beton felhasználása. Mindkét esetben az időjárás hatásait figyelembe kell venni, hogy a beton alap állékonysága megmaradjon. A beton alap elkészítése főleg az öntött változat esetében célszerű, ha fagyhatár alatti mélységet (hazánkban ez 60 centiméternél mélyebb) meghaladja. [8]

A továbbiakban tehát csak a kerítések, kapuk megvalósítási formáit vizsgálom meg néhány hazai és egy külföldi szennyvíztisztító telep esetében. A vizsgálatot a fenti idézetben olvasható anyagra és méretekre vonatkozó adatokat alapján végzem el. A beton alapok megítélését a képek alapján nem lehet elvégezni.

A kerítések akadályozó képességének a fokozása a magasságuk növelésével valósítható meg. A magasság növelése a többsoros tüskés vagy pengésdrót felhelyezése biztosítja. A kétféle drót közül a pengésdrót akadályozó képessége a nagyobb, mert a kialakítása a fémpengékkel történik. A pengék nagyon élesek és komoly sérülés okozására képesek. A pengésdrótok látványa is visszatartó tényező. A pengék az alábbi ábrán láthatók.

1.számú kép Pengésdrót (forrás: https://digitalbau.hu/arak/drot-keritesek/oszlopok-rogzito-elemek-drotfonatokhoz/nato-drot-penges-huzal-10-fm

A szennyvíztisztító telepek kerítéseit, kapuit a Google Earth-ön és Maps-on látható képek alapján vizsgáltam meg, melyek az alábbiak.

Szennyvíztisztító telep Ausztriában a 63-s számú főút mellett Őriszigettől délre.

2.számú kép A fentnevezett szennyvíztisztító telep déli és nyugati kerítés szakasza (forrás: https://www.gogle.com/maps/@47.2521511,16.2784515,3a,66.5y,359.99h,87.11t/data=!3m6!1e1!3m4!1sZ-3Gbfi6zkBKxYgDMupS6Q!2e0!7i16384!8i8192?hl=hu

3.számú kép A fentnevezett szennyvíztisztító telep északi és nyugati kerítés szakasza (forrás: https://www.google.com/maps/@47.2535197,16.2766551,3a,90y,96.08h,106.78t/data=!3m6!1e1!3m4!1sGeuB2HCCcR-28J2dJ-bHDQ!2e0!7i16384!8i8192?hl=hu

Az 2. és 3.számú képeken látható, hogy dróthálóból készült a kerítés, amelyet fémoszlopok közé rögzítettek. Az oszlopok merevítése a töréspontokban biztosítja a kerítés szakasz stabilitását. A fémoszlopok ellenálló képessége nem olyan, mint a betonoszlopoké. A kerítés tetején két sor tüskésdrótot feszítettek ki. A 2. képen látható a telep főbejárata. A főkapu fémből készült elektromos működtetésű tolórendszerű, de a tetején nincs kétsoros tüskésdrót. A kerítés és a kapu megakadályozza a könnyű behatolást, mert a vizsgálati szempontok közül a méretek közül a magassági méretnek megfelel. A kiegészítő kétsoros tüskésdrót is fokozza a biztonságot, de csak kerítések esetében.

Bajánsenye szennyvíztisztító telep

4.számú kép A szennyvíztisztító telep északi szakaszának egy része (forrás: https://earth.google.com/web/@46.7925724,16.41176458,212.45225029a,0d,15y,181.3190533h,85.56393002t,0r/data=IhoKFlFLTUc2X1BZNmk3SzdHbGplVzY2SWcQAg

A telep északi részén a kerítés faoszlopok, míg a telep többi oldalán betonoszlopok között rögzített drótháló. A kerítés tetején nincs többsoros tüskésdrót. A telep természetvédelmi területen van ezért kellett az északi oldalon faoszlopokat és fából készített kaput elhelyezni. Az 1996. évi LIII. törvény a természetvédelemről 7.§ (2) c) „a település-, a területrendezés és fejlesztés, különösen a területfelhasználás, a telekalakítás, az építés, a használat során kiemelt figyelmet kell fordítani a természeti értékek és rendszerek, a tájképi adottságok és az egyedi tájértékek megőrzésére;" [9] rendelkezésének betartása alapján készítették a kerítés oszlopokat és a kaput fából. A kerítés (elsősorban a telep északi részén a kapu környezetében) és a kapu kismértékű akadályozó és visszatartó tényezőt valósít meg, mert a magassági mérete nem éri el az 1,8 métert és nincs a jelzett kerítésszakasz és a kapu tetején kiegészítő többsoros tüskésdrót.

Balassagyarmat szennyvíztisztító telep

5.számú kép A szennyvíztisztító telep bejárat és a déli kerítés szakaszának egy része (forrás: https://earth.google.com/web/@48.07045495,19.26718791,143.61010742a,0d,15y,11.50778623h,85.61352453t,0r/data=IhoKFmFpd0dsQnZ4M3JNRnZXSWN5UHB1MGcQAg

6.számú kép A szennyvíztisztító telep nyugati és a déli kerítés szakaszának egy része (forrás: https://earth.google.com/web/@48.07045495,19.26718791,143.61010742a,0d,15y,11.50778623h,85.61352453t,0r/data=IhoKFmFpd0dsQnZ4M3JNRnZXSWN5UHB1MGcQAg

A 5. és 6.számú számú képen a déli oldalon lévő főkapu látható, amely mellett jobbra és balra beton alapra épített keretes acélrács a kerítés anyaga. A szennyvíztisztító telep többi kerítés szakasza betonoszlopok között rögzített dróthálóból készült. A kerítés tetején nem látható több soros tüskésdrót. A kerítés és a kapu akadályozó és visszatartó tényezőt valósít meg, mert a főkapu környezetében a kerítés betonalapra van helyezve, illetve a magassági mérete is megfelelő.

Szabadbattyán szennyvíztisztító telep

7.számú kép A szennyvíztisztító telep bejárat és a keleti kerítés szakaszának egy része (forrás: https://earth.google.com/web/search/Szabadbatty%c3%a1n/@47.11949087,18.38336751,101.19302697a,0d,21.86874171y,136.11371527h,86.71579074t,0r/data=CigiJgokCbOLWjcTskdAEdYNTTOWjkdAGYQ_Qpns_jJAIT7q3KDpJzJA

A 7. számú képen az északi oldalon lévő főkapu látható, mellette a keleti oldal kerítés szakasza. A kétszárnyas kapu zárszelvénykeretben rögzített dróthálóból készült, de a tetején nincs kettő sor tüskésdrót. A kerítés szakaszok betonoszlopok (a töréspontokban a merevítésük megfelelő) között rögzített dróthálóból lettek kialakítva a tetején kettő sor tüskésdróttal. A kerítés és a kapu akadályozó és visszatartó tényezőt valósít meg, mert a magasság megfelelő, illetve a kerítés tetején rögzítve van a biztonságot fokozó kétsor tüskésdrót.

ÖSSZEFOGLALÁS

A szennyvíztisztító telepek vagyonvédelmének fontos része a mechanikai védelem, melyet a cikkben vizsgáltam. A mechanikai védelem elemei között a kapuk és a kerítések fontos helyet foglalnak el, az anyaguk, az építési módjuk hozzájárul a védett objektum biztonságához annak fenntartásához. A kerítések csak akkor töltik be szerepüket, ha az idézett méreteknek megfelelő a méretük, valamint a kiegészítő több soros tüskés- vagy pengésdrót megtalálható a kerítés tetején. A vizsgált külföldi és hazai szennyvíztisztító telephelyek kerítési közül csak több esetben a bajánsenyei esetében alacsonyabb a mérete a kerítésnek, míg a balassagyarmati kerítés tetején nincs kettő sor tüskésdrót. A vizsgált kerítések anyagai dróthálók, vasbeton oszlopok, illetve beton alap melyek hozzájárulnak az akadályozás megvalósításához. A megvizsgált szennyvíztisztító telepek esetében megállapítottam, hogy célszerű a kerítések módosítása, melyet a kerítések esedékes (az időjárás viszontagságai következtében a kerítés anyaga elgyengül) karbantartásakor meg lehet valósítani. A módosítás minden esetben a beton alap elkészítése, valamint a biztonságot fokozó tüskés, illetve a pengésdrót felhelyezése.

A kapukat minden vizsgált szennyvíztisztító telep esetében megfelelőnek tartom, mert megvalósítják az akadályozást és a késleltetést. A kapuk esetében is szükségesnek látom az akadályozó képesség növelését. A növelést szintén a tüskés, illetve a pengésdrót felhelyezése teszi lehetővé.

A következő cikkben helyszíni bejárás során gyűjtött információk feldolgozása alapján vizsgálom meg más szennyvíztisztító telephelyek mechanikai védelmét biztosító elemeket.

FELHASZNÁLT IRODALOM

[1] Laczik, B. A kritikus infrastruktúra védelem elveinek, céljainak és a veszélyes ipari üzemek biztonságának összefüggései, kapcsolatuk. Hadmérnök. VI. Évfolyam 2. szám - 2011. június
[2] Berek, L. Szerk. Személy- és vagyonbiztonság. ÓE-BGK 3071 jegyzet, Budapest, 2016.
[3] 91/271/EGK uniós tanácsi irányelv a települési szennyvíztisztításról.
[4] 2080/2008. (VI. 30.) Korm. határozat Kritikus Infrastruktúra Védelem Nemzeti Programjáról.
[5] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.
[6] 541/2013. (XII. 30.) Korm. rendelet a létfontosságú vízgazdálkodási rendszerelemek és vízilétesítmények azonosításáról, kijelöléséről és védelméről.
[7] 379/2015. (XII. 8.) Korm. rendelet Magyarország települési szennyvíz-elvezetési és -tisztítási helyzetét nyilvántartó Településsoros Jegyzékről és Tájékoztató Jegyzékről, valamint a szennyvízelvezetési agglomerációk lehatárolásáról.
[8] Kerítés alap beton. Beton-Dimenzió, Mixerbeton. https://betonozz.hu/kerites-alap-beton/
[9] 1996. évi LIII. törvény a természetvédelemről

THE CHALLENGES OF FOOD SECURITY - FROM THE PERSPECTIVE OF FOOD LOSS AND FOOD WASTE

AZ ÉLELMEZÉSBIZTONSÁG KIHÍVÁSAI – AZ ÉLELMISZERVESZTÉSÉG ÉS -PAZARLÁS SZEMSZÖGÉBŐL

WU Yue[1] – TAKÁCS-GYÖRGY Katalin[2]

Abstract

Food loss and waste is a relatively new crucial research topic accounting for food insecurity, but getting more and more attention nowadays. To better understand the links between food loss and waste and food security, we conducted this research by content analysis, secondary literature review, and report and news study from FAO and the UN. We concluded in our research that food loss and waste include qualitative and quantitative perspectives along the food supply chain at all stages, including the primary or agricultural production, sorting and grading to meet retailer standards, processing and storage, huge waste in households, and waste due to date labeling misunderstanding. All the participnants of food chain has their responsiblitiy in reducing food loss and waste.

Keywords

Food security, Food safety, Sustainability, Food supply chain, Digital education

Absztrakt

A kutatás célja az élelmiszer-veszteség és a pazarlás, valamint az élelmezésbiztonság közötti összefüggések feltárása tartalomelemzéssel, szakirodalom feldolgozásával, továbbá a FAO és az ENSZ jelentések felhasználásával. Kutatásunk során arra a következtetésre jutottunk, hogy az élelmiszerveszteség és -pazarlás minőségi és mennyiségi szempontból vizsgálandó az élelmiszer-ellátási lánc minden szakaszában, beleértve magát a mezőgazdasági termelést, a terméklánc mentén a kereskedelmi szabványoknak megfelelő válogatást és osztályozást, a feldolgozást és tárolást, továbbá a háztartásokban nagy mennyiségben keletkező hulladékot. Az élelmiszerlánc minden szereplőjének kimutatható a felelőssége a veszteség csökkentésében.

Kulcsszavak

Élelmiszerbiztonság, Élelmiszerbiztonság, Fenntarthatóság, Élelmiszer-ellátási lánc, Digitális oktatás

[1] wuyue.budapest@gmail.com | ORCID: 0000-0003-0349-5654 | PhD. student, Óbuda University Doctoral School on Safety and Security Science | PhD. hallgató, Óbudai Egyetem Biztonságtudományi Doktori Iskola

[2] takacsnegyorgy.katalin@kgk.uni-obuda.hu | ORCID: 0000-0002-9129-7481 | Prof. Dr., Óbuda University Keleti Faculty of Business and Management, Department of Business Development and Infocommunications | egyetemi tanár, Óbudai Egyetem Keleti Károly Gazdasági Kar

1. INTRODUCTION

The three most basic elements for human being survival are water, air, and food (food safety and food security), which are also essential to a state's safety. There are two main concerns in food are food safety and food security, which are linked closely with each other. Food safety means the available food for humans is safe, not harmful, and there is no contamination of food. If we talk about food security, we have to highlight that if there is no food safety, there will be no food security. In our research, we mainly focus on the topic of food security.

It is estimated that the world population will increase to 9.1 billion, 34% higher than today in 2050 [1]. When most of us are given enough food, we take it as granted. However, according to the data from 2020, on the same planet, 811 million people are suffering from hunger, and 3.1 billion people do not have access to a healthy diet, 132 million people are threatened by food and nutrition insecurity because of the COVID-19 pandemic [2], [3]. What is worse, the ongoing war started in February 2022 between two important world food suppliers, Russia and Ukraine, depressed world food security [4]. These two countries are the top producers of world foodstuffs and fertilizers, besides Russia is also the main supplier of oil and gas [5]. The so-called "World's bread basket" around the Black Sea has been in trouble since the war outbreak [4], [6]. But these two rigorous and unpredictable problems are not the start of the world food security alarm, catalyst instead [7]. For example, global climate change and extreme weather threaten agriculture through their influence on ecology, the environment, the geographical situation of crop and crop production, the resources and supply chain of agriculture, and the market price [8]. The chronic climate change or extreme weather [9], [10], natural resources scarcity (arable lands and water) [10], [11], agriculture facilities issues (aging farmers and fewer farmers because of urbanization) [11]–[13], food market fluctuation [14] are the main causes of agricultural risks.

Food security is a multi-dimensional topic (in correspondence with SGDs 2: Zero hunger). However, usually, we are used to addressing it by one aspect of the broad food security problem. Food security was defined firstly in the 1970s by World Food Conference and later improved to a more accurate concept by FAO (Food and Agricultura Organization), World Bank, and World Food Summit. Today, the widely accepted definition of food security contains three main dimensions: food availability, food access, utilization, and stability. Food availability means an adequate quantity of food supply with proper safe food. Food access promises all people to access sufficient and nutritional food at the individual, regional, or national levels. Utilization refers to the food supplied to all people to meet nutritional requirements. Food stability requires food availability and stable access for all people, even in the shock of economic crises, climate crises, or seasonal food insecurity [15].

The risks to food security come from agricultural production, market, income, food quality and safety, clean water resources, sanitation issues, and governmental and political stability. The two general types of food insecurity can be understood as Chronic and transitory food insecurity based on the duration and other causes. The intermedia type of food insecurity is seasonal food insecurity, which is similar to chronic food insecurity as it usually can be predicted and follows a sequence of known events, such as extended periods of poverty, lack of assets, and inadequate access to productive or financial resources. But it can also be regarded as recurrent and transitory food insecurity due to the limited duration. The concerns are not only the duration but also the severity, which describes how intense

or severe the problem is on food security and nutrition. The indicator as energy intake (measured in calories) below a threshold of 2,100 kcal per day can be used to classify the intensity of food insecurity to: Food secure, Energy intake (measured in calories), Mild food insecurity, Moderate food insecurity, Severe food insecurity. Besides, a range of livelihood needs (Crude Mortality Rate, Malnutrition prevalence, Food Access/ Availability, Dietary Diversity, Water Access/Availability, Coping strategies, Livelihood Assets) can be used as indicators to calssify food security and humanitarian crises: Generally food secure, Chronically food insecure, Acute food and livelihood crisis, Humanitarian emergency, Famine / humanitarian catastrophe (Integrated Food Security and Humanitarian Phase Classification Framework) [8].

Food loss and waste is a broader topic related to global food security, food safety, quality, and sustainability. From a worldwide view, every year, the food loss and waste is approximatey14%, valued at $400 billion after harvest and before market. And 17% or 931 million tonnes of food is lost between market and consumption, such as households, restaurants, retailers, and other food service types, especially households (11 percent in households, 5 percent in the food service, and 2 percent in retail) [2], [3], [16]–[18]. And 8-10 percent of global greenhouse gas emissions (GHGs) are from food loss and waste, which worsen the unstable climate and extreme weather. Vice versa, the more unstable climate change, and extreme weather negatively impact crop production and crop yields [3], [17]. The greenhouse gas emission ranks after China and the US (figure 1.) [19]. According to the estimation of FAO, every year, lost and wasted food can feed 1.26 billion hungry people. It is obvious to see reducing food loss and waste is a triple win for food security, climate change, and sustainability [17].

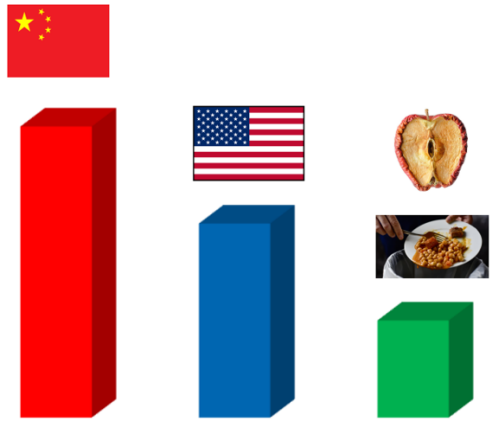


Figure 1: Ranking of greenhouse gas emission
Source: UNEP, 2021

When we learn from the 2030 Agenda for Sustainable Development, it is a great milestone to mention that all the 193 Member States of the United Nations adopted 17 goals on 25 September 2015 [20]. It is a universal action goal including three-dimensional sustainability: economic, social, and environmental for the international community to end

poverty in 2030 [21], where especially highlighted in Goal 2 (End Hunger) and Goal 12.3, „ By 2030, half per capita global food waste at the retail and consumer levels and reduce food losses along production and supply chains, including post-harvest losses", under the Goal 12 „ Ensure sustainable consumption and production patterns" [22], [23]. Today, we have eight years to achieve the SDGs. It is urgent for action to be aware food loss and waste reduction is an efficient method to ease the climate change burden and other risks on agriculture to achieve sustainability.

We are warned as personnel consuming food every day that the food insecurity issue is very serious for present and future generations. However, food security is usually regarded as a broader problem [8]. Therefore, in our research, we simplify the food insecurity issues and focus on a small but important point: food loss and waste.

2. RESEARCH METHODOLOGY

Food security is usually regarded as a broader problem, but contributed by small points. To better understand these small points, which made food insecurity, we simplify the food insecurity issues and focus on a small but important point: food loss and waste by content analysis and secondary literature review. The literature study also focuses on extensive reports and news from FAO and the UN website.

3. RESEARCH RESULTS

The 29 November International Day of Awareness of Food Loss and Waste (IDAFLW) was designed by the United Nations General Assembly in 2019, calling all the public and private sectors to work together on cutting food loss and waste to use the limited natural resources more efficiently, mitigate the burden from climate change, and obtain sustainable food and nutrition [18]. As food loss and waste reduction is a crucial topic now and later accounting for sustainable food security, we explored the questions: what is food loss and waste, how it happened, and what are our suggestions for mitigating food loss and waste.

3.1 Definition of food loss and waste

As the State of Food and Agriculture (2019) report from FAO, food loss and waste refer to a decrease in the quantity or quality of food along the food supply chain [24]. The distinctions between food loss and food waste exist in the conceptual framework and a policy aspect. Food loss comes from the food supply chain, excluding any consuming step, including retail, food service offers, and consumers, where there is reducing of food in quantity and quality. The food supply chain contains these steps:

- Agricultural production and harvest/slaughter/catch
- Post-harvest/slaughter/catch operations
- Storage
- Transportation
- Processing
- Wholesale and retail
- Consumption by households and food services

Food waste refers to the step of consuming step where food is decreased in quantity and quality, including the retailers, consumers, and other food service providers.

Quantitative food loss and waste, also called physical food loss and waste means the decrease in the mass of food for human consumption: food is removed from the food supply chain (food loss), and food is decreased from the behaviors and decisions of consumers, retailers and food service providers (food waste). Qualitative food loss and waste mean decrease in food value for the intended use (nutrition and economic value): food value decreases from the food supply chain (food loss), and food value decrease from decisions of consumers, retailers and food service providers (food waste). The conceptual framework (Figure 2) explains the relationship between the intended use of plants and animal products, fragmentation, and destination:

- Intended use: only the loss and waste of animal and plant products that are eaten by people is considered as food loss and waste, excluded the intended use that is eaten by animals, used as seeds, or used in industry.
- Fragments from intended use for human food: only fragments for human consumption from plant and animal products intended use for humans are considered food loss and waste, excluding other fragmented use, such as in inedible parts, feeding animals, and other economic and productive intentions.
- Destination of edible food from fragments: finally, edible food is used for human eating, but there are qualitative food loss and waste or other uses (feeding animal, industrial use, and other non-food economic use). But there may also be quantitative food loss (by suppliers) and food waste (by consumers, retailers, and food service providers). These quantitative food losses and waste will be put into a trash bin or managed by incineration, composting, and anaerobic digestion.

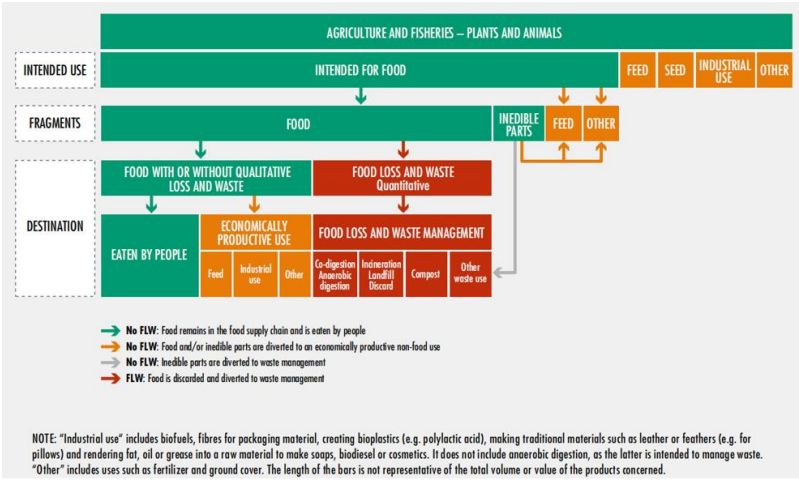


Figure 2: A conceptual framework of food loss and waste (FLW)

Source: FAO

FAO. 2019, p. 31. In Brief: The State of Food and Agriculture 2019. Moving forward on food loss and waste reduction. Rome.

3.2 The scenarios that food and waste are happening

We have introduced the definition of a food supply chain above. In this chapter, we will discuss how food loss and waste happen in the food supply chain. It is estimated that the food lost and wasted along the food supply chain reaches 30% of the food intended for human consumption [25].

3.2.1 Along the food supply chain, exclude retail

In post-harvest, the fresh food products have to be removed from to supply chain during the sorting operations if they are not optimal at different criteria, such as shape, color, and size [17]. For example, vegetable and fruit loss is in a dominant position in industrialized zone. The losses happen in harvesting, sorting, and grading. Especially in grading, the most loss of vegetables and fruits is due to the deviation of quality standards set by retailers [25]. The losses in developing countries at processing is 14%-21%, while the percentage is less than 2% in developed countries. Improving processing technologies have the opportunity to reduce food loss of vegetables and fruits, such as drying technology (replace sun-drying by hot air, fluidized bed, infrared and solar, freeze-drying).

Another example is taken from the consumer cereal (mainly wheat and rye grain) in Poland, which is one of the most important cereal producers in Europe. It was investigated that during 2017-2018, 219,600 tonnes of consumer cereals were lost at primary or agricultural production, which is 1.7% of annual consumer cereal production and accounts for 608,000 tonnes of CO_2 eq. The main causes of consumer cereal grain loss at the production and storage step are moisture, grain damage, pest disturbance, and weather uncertainty [26].

3.2.2 At customer service

As European Commission estimated that there are 88 million tonnes of food waste generated annually in the EU, and 10% of it is because of the date marking on food products [27]. There are three terms confusing for consumers, which are the cause of date labeling for food loss and waste [27]–[29]:

- Use by Date or Expiration Date: about food safety – foods can be eaten until this date but not after any storage condition due to safety and quality reasons, even if they look and smell fine.
- Best Before Date or Best Quality Before Date: about food quality of the unopened shelf-stable product– the food will be safe to eat after this date but may not be at its best. For example, its flavor and texture, freshness, taste, aroma, or nutrients might not be as good.

However, food products that are close to or beyond „Best Before Date" and „Best Quality Before Date" are usually discarded by retailers and consumers [17].

Besides the date labeling misunderstanding, the waste in households is also very harmful. Huge amounts of wholesome editable food are left over or not used and discarded in households and eating establishments [17].

3.2.3 At household and individual levels – example in Hungary

As we highlighted above that, household food waste is taking a big percentage of food waste at the customer service level [2], [17], [18]. In this subchapter, we take an example from Hungary.

From the data in 2020, the official of Hungary announced that the food waste is more than 300,000 tonnes every year, equal to over 170 billion forints (EUR 480m) and 18,000 HUF per person [30]. The data in 2020 showed that the annual food waste is up to 68 Kg per person [31]. In 2019, the food waste was 65.49 kg per capita annually, and 48.81% of it could have been avoided [32]. While in 2016, the food waste was 68.04 kg per capita annually, and 48.7% of total food waste equals 33.14 kg/per capita/year could be avoidable [33]. It is obvious that food waste is still a crucial issue in Hungary, but we have hope for food waste reduction. Similarly to other countries, the largest food waste percentage is from household throwing away, which is not only a social, environmental, or economic issue but also an ethical problem highlighted by the government [30]. Among the food waste types, the most frequent is meals, bakery, dairy products, vegetable, and fresh fruits [33].

3.3 Suggestions for tackling food loss and waste

We have explored and discussed what food loss and waste is and how and why food loss and waste is a serious problem for food security in our research. In this sub-chapter, we shortly suggested the future to tackle food loss and waste.

3.3.1 Importance of individual behavior in reducing food waste

First of all, due to the fact that everyone consumes food, where the food waste comes from. It can not be overemphasized that individual behavior plays an important role in reducing food waste.

Let us look at it deeply through the example of Hungary. It is proved by a series of surveys that most of the population in Sopron and its surroundings have an awareness of selective waste collection, which, combined with reducing waste, contributes to a circular economy. But their behavior on selective waste collection is influenced by gender and the place of residence, including the village, urban agglomeration, and city center [34]. Income is also a factor influencing Hungarian consumers' food waste behavior [33]. The investigated Hungarian also suggested that buying high quality, good duration, and environmentally friendly products with reasonable and packaging-free is also the way to favor a circular economy [34]. Food waste in households and individual is a bad habit in everyday life, which is hard to improve if it is paid attention to when they are already adults [31]. Therefore, education and attitude information should start from childhood.

3.3.2 From the view of digital education or e-learning

Agrifood is a vital industry related to everyone, as all different fields of people are consumers of agrifood. Especially food waste education should be from childhood, as food waste mainly comes from households and individuals, which is a bad daily habit [31].

According to Roger's Diffusion of Innovation Theory (DOI), the crucial step to make people execute the implementation of food loss and waste reduction is to make people

perceive it [35], [36]. Strengthening the learning and knowledge diffusion is the way to aware all consumers about the necessity to reduce food loss and waste and educate all the consumers to take measures in daily life to execute food loss and waste reduction. And also the other important roles in the food value chain, such as farmers in production, operations in food processing in industries, practitioners in food logistic process, and retailers in the food market. With the rapid development of industry 4.0, advanced and digital technologies penetrate all industries, including agriculture and food [37]–[39]. Digital education means any type of digital technology used in education for any age of the student. Thanks to the development of the internet and other technologies, students can study anytime and anywhere. The same for teachers, they can teach anytime and anywhere as long as there is internet and suitable facilities [40], [41].

Let us take the successful practice from FAO. There is abundant and useful e-learning and training materials in FAO free for anyone who is concerned with the topic of food loss and waste. These e-learning courses aid countries in reducing food losses along production and supply chains. The lessons cover the index and its components, along with strategies and guidelines for collecting, integrating, and modeling the necessary data from a variety of sources [18]. The topics refer to „Food Security Concepts and Frameworks" for those audiences: mid-level managers, technical staff, field personnel who are involved in the collection, management, analysis, and reporting of food security information, and planners, policy formulators and program managers who are involved in monitoring progress in poverty reduction, and meeting food security goals and targets [8], „ Food Loss Analysis Case Study Methodology" for those audiences: field level program officers who wish or need to design, organize, coordinate and implement a food loss analysis, and technical advisors and academics who want to learn more about the topic in order to teach others [42], and so on. Any audience could download the course materials and learner notes and learn them anytime and anywhere [43].

Besides, the UN offers an e-learning course, „Food Waste Prevention" for individual practice in daily life [44]. These education strategies should focus on the food supply chain, such as the producers or farmer communities, processers, logistician operators, retailers, and consumers, reducing on-farm food loss and consumption waste [25], [45].

3.3.3 From the view of research agenda

The links between food loss and food security were investigated by Nyambo in 1993 [46]. The claim of this investigation is that food security can be enhanced by reducing food loss because of post-harvest grain handling technology. Food loss and waste is getting more and more attention nowadays. Food loss and waste seem to be and should be on the research agenda in the next decades. The research needs on food loss and waste and the food security nexus have been emphasized by many researchers in recent years. The research topics are suggested to focus on: understanding the interrelations between food loss and waste and food security by reliable, relevant, and timely data, evidence-based analysis[47], improve harvest techniques in order to reduce food loss in production level [25], manage the food loss and waste and food security nexus, scenario analysis on approach green and circular economy [48], multi-disciplinary research on post-harvest, inter-supply chain, knowledge exchange and skill building on reducing food loss and waste [49], collaborative research on identifying crops with high loss percentage relatively [45].

The research on food loss and waste favors policymakers on better decisions to achieve a sustainable environment, economy, and society [47]. Even this research topic is paid more and more attention in recent years [32], but it is not common among all the world. For example, the topic about household food waste dominates in developed countries [50]. Therefore, we still have space to tackle food waste by enhancing the investment in research on food waste related topic.

3.3.4 From the view of policy and regulations

Reducing food loss and waste is the mission of the country members of the UN, which set up the SDGs 12.3, „ By 2030, halve per capita global food waste at the retail and consumer levels and reduce food losses along production and supply chains, including post-harvest losses" , under the Goal 12 „ Ensure sustainable consumption and production patterns" [22]. Achieving this national and global goal needs corresponding policies and regulations to support it at a regional and national level. In the 2022 United Nations Climate Change Conference (COP27) [51], all governments, businesses, and institutions are called to make voluntary commitments to reduce food loss and waste [17].

Nevertheless, food loss and waste is a highly debated topic that needs effective and sufficient policies and regulations to support and implement. Governments should adopt legislative and non-legislative solutions to reduce food loss and waste to accelerate the transition to a more sustainable and resilient agrifood system and favor the food supply chain to ensure food security through a more green and circular economy [47], for instance, the 3R policy: reduce, reuse, and recycle [52], support the on-farm storage facilities and cooling chains to reduce the food loss from the perspective of post-harvest, and the transportation infrastructure [25], encourage coordinated research on identify crops with high loss percentage relatively [45].

4. CONCLUSIONS, SUGGESTIONS

4.1 Conclusion

World food security has been threatened by many aspects: chronic climate change or extreme weather [9], [10], natural resources scarcity (arable lands and water) [10], [11], agriculture facilities issues (aging farmers and decreasing farmers because of urbanization) [11]–[13], food market fluctuation [14], additionally the unpredicted shock from COVID-19 pandemic and war in Ukraine. Besides, the pressure on food security is also derived from the rapidly increasing population [1] and eight years left to achieve SDGs, especially target SDG 2 and SDG 12.3 [21]. Food loss and waste is a broad topics related to food security. The lost and wasted food can feed 1.26 billion hungry people. It is obvious to see reducing food loss and waste is a triple win for food security, climate change, and sustainability [17]. The topic of food loss and waste is highly debated to favor sustainable economics, environment, and society, and mitigate climate change and extreme weather.

We concluded in our research that the links between food security and food loss and waste. Food loss and waste include qualitative and quantitative perspectives along the food supply chain at all the stages [25], including the primary or agricultural production, sorting and grading to meet retailer standards [17],[25], processing and storage [26], huge waste in households [17] and waste due to date labeling misunderstanding [27].

In the end, we suggested three dimensions to reduce food loss and waste from enhancing digital education on reducing food loss and waste to all the actors in the food chain [8], [18], [42]–[45], investing in research or collaborative research on understanding and reducing food loss and waste [25], [45], [47]–[49], and appeal governments and policymakers to build legislative and non-legislative initiatives on reducing food loss and waste to accelerate agriculture transition to more resilient and sustainable mode [17], [22], [25], [45], [47], [51], [52].

According to the FAO report on „The State of Food Security and Nutrition in the World 2022" [53], our world is moving back to the target of 2030 SDG 2, End Hunger, but we have only eight years left to achieve. It is more challenging for governments to obtain sustainability and achieve SDGs target 2. However, not only the government and other public sectors but also private sectors (business and individual) have to take urgent action to tackle food loss and waste.

4.2 Limitations of the research

We have explored the relationship between the challenges of food security and food loss and waste. Unfortunately, due to the page limitation, we could not extend our research to discuss in depth how we can tackle this issue to obtain a sustainable food future at a personal, regional, national, and global level. For example, the green economy and circular economy is an effective approaches. Food will not be wasted if there is a circular practice implemented. For example, harmful methane emissions can be avoided if lost and wasted food is used for compost or biogas [17]. And how to implement waste management to ease the burden of food loss and waste in food security [19]. But we listed a few general suggestions shortly. Here, we also appeal to more and more researchers to stand on this point to achieve sustainable food and agriculture and planet for future generations.

5. SUMMARY

Food loss and waste are crucial food insecurity topics along the whole food chain, including the supply chain from agricultural production to retailers and retailers, consumers, and other food service providers. We suggest all the actors along the food chain be aware and take urgent actions to reduce food loss and waste, as we mentioned via digital education, extending research, and strengthening policy and regulations.

Achieving a sustainable future is never an independent mission for random personnel or a nation. In contrast, it is a shared project for everyone who is living on this planet and cares about his or her future generations. So here, we appeal not only to the researchers but everyone to pay attention to food loss and waste and take daily actions to reduce it.

REFERENCES

[1] 'How to feed the world - 2050: High-level Expert Forum, Rome 12-13 Oct 2009 - Investment - World', *ReliefWeb*. https://reliefweb.int/report/world/how-feed-world-2050-high-level-expert-forum-rome-12-13-oct-2009-investment (accessed Apr. 20, 2022).

[2] FAO, 'Stop food loss and waste. For the people. For the planet.', FAO, Roma, Italy, 2021. [Online]. Available: https://www.fao.org/3/cb6236en/cb6236en.pdf

[3] 'International Day Food Loss and Waste| Technical Platform on the Measurement and Reduction of Food Loss and Waste | Food and Agriculture Organization of the United Nations', *FoodLossWaste*, 2022. https://www.fao.org/platform-food-loss-waste/flw-events/international-day-food-loss-and-waste/en (accessed Nov. 11, 2022).
[4] 'How will Russia's invasion of Ukraine affect global food security? | IFPRI : International Food Policy Research Institute', Feb. 24, 2022. https://www.ifpri.org/blog/how-will-russias-invasion-ukraine-affect-global-food-security (accessed May 27, 2022).
[5] Arif Husain, Friederike Greb, and Stefan Meyer, 'Projected increase in acute food insecurity due to war in Ukraine', Mar. 2022. Accessed: May 26, 2022. [Online]. Available: https://docs.wfp.org/api/documents/WFP-0000138155/download/
[6] K. Vlamis, 'How Russia's assault on Ukraine, the "world's breadbasket," could lead to famine in Yemen', *Business Insider*, May 17, 2022. https://www.businessinsider.com/russia-assault-ukraine-could-lead-to-famine-in-yemen-2022-3 (accessed May 27, 2022).
[7] 'Conflict and food security - Security Council, 9036th Meeting | UN Web TV', May 19, 2022. https://media.un.org/en/asset/k10/k10mjpv1u3 (accessed May 27, 2022).
[8] 'Food Security Concepts and Frameworks', *FAO elearning Academy*, 2008. https://elearning.fao.org/course/view.php?id=131 (accessed Nov. 11, 2022).
[9] C. Agrimonti, M. Lauro, and G. Visioli, 'Smart agriculture for food quality: facing climate change in the 21st century', *Critical Reviews in Food Science and Nutrition*, vol. 61, no. 6, pp. 971–981, Mar. 2021, doi: 10.1080/10408398.2020.1749555.
[10] 'Sustainable and Digital Agriculture | United Nations Development Programme', *UNDP*. https://www.undp.org/sgtechcentre/sustainable-and-digital-agriculture-1 (accessed Oct. 26, 2022).
[11] 'Challenges for modern agriculture', *Syngenta*. https://www.syngenta.com/en/innovation-agriculture/challenges-modern-agriculture (accessed Oct. 26, 2022).
[12] S. Somosi and G. Számfira, 'Agriculture 4.0 in Hungary: The challenges of 4th Industrial Revolution in Hungarian agriculture within the frameworks of the Common Agricultural Policy', p. 28.
[13] 'Digital Agricultural Academy of Hungary to take farmers into new age'. https://www.freshplaza.com/latin-america/article/9428745/digital-agricultural-academy-of-hungary-to-take-farmers-into-new-age/ (accessed Oct. 04, 2022).
[14] *FAO publications catalogue 2022*. FAO, 2022. doi: 10.4060/cc2323en.
[15] FAO, 'Policy Brief-Food Security'. FAO's Agriculture and Development Economics Division (ESA), 2006. [Online]. Available: https://www.fao.org/fileadmin/templates/faoitaly/documents/pdf/pdf_Food_Security_Cocept_Note.pdf
[16] 'Food loss and waste', *Food and Agriculture Organization of the United Nations*. http://www.fao.org/nutrition/capacity-development/food-loss-and-waste/en/ (accessed Nov. 11, 2022).
[17] 'Tackling food loss and waste: A triple win opportunity', *Newsroom*, Sep. 29, 2022. https://www.fao.org/newsroom/detail/FAO-UNEP-agriculture-environment-food-loss-waste-day-2022/en (accessed Nov. 12, 2022).

[18] U. Nations, 'Food Loss and Waste Reduction', *United Nations*. https://www.un.org/en/observances/end-food-waste-day (accessed Nov. 12, 2022).
[19] U. N. Environment, 'UNEP Food Waste Index Report 2021', *UNEP - UN Environment Programme*, Apr. 03, 2021. http://www.unep.org/resources/report/unep-food-waste-index-report-2021 (accessed Nov. 12, 2022).
[20] '193 Member States Archives', *United Nations Sustainable Development*. https://www.un.org/sustainabledevelopment/blog/tag/193-member-states/ (accessed May 11, 2022).
[21] R. Neshovski, 'Home', *United Nations Sustainable Development*. https://www.un.org/sustainabledevelopment/ (accessed May 11, 2022).
[22] 'A/RES/70/1 Transforming our world: the 2030 Agenda for Sustainable Development', p. 35, 2030.
[23] 'Food waste reduction | Community of Practice on food loss reduction (CoP) | Food and Agriculture Organization of the United Nations | Food Loss Reduction CoP | Food and Agriculture Organization of the United Nations'. https://www.fao.org/food-loss-reduction/resources/foodwastereduction/en/ (accessed Nov. 12, 2022).
[24] FAO, *In Brief: The State of Food and Agriculture 2019: Moving forward on food loss and waste reduction*. Rome, Italy: FAO, 2019. Accessed: Nov. 12, 2022. [Online]. Available: https://www.fao.org/documents/card/en/c/ca6122en
[25] M. Rezaei and B. Liu, 'Food loss and waste in the food supply chain', p. 2, 2017.
[26] H. De Groote *et al.*, 'Consumer Acceptance and Willingness to Pay for Instant Cereal Products With Food-to-Food Fortification in Eldoret, Kenya', *Food Nutr Bull*, vol. 41, no. 2, pp. 224–243, Jun. 2020, doi: 10.1177/0379572119876848.
[27] '"Use by" or "best before"? |Food Loss Reduction CoP| Food and Agriculture Organization of the United Nations'. https://www.fao.org/food-loss-reduction/news/detail/en/c/1335014/ (accessed Nov. 12, 2022).
[28] 'DRAFT REVISION TO THE GENERAL STANDARD FOR THE LABELLING OF PREPACKAGED FOODS (CODEX STAN 1-1985) (At Step 6)'. 1985. [Online]. Available: https://www.fao.org/fao-who-codexalimentarius/sh-proxy/en/?lnk=1&url=https%253A%252F%252Fworkspace.fao.org%252Fsites%252Fcodex%252FMeetings%252FCX-714-44%252FWD%252FREP%2B16_FL%2BAPPENDIX%2BII.pdf
[29] 'Best before date vs. expiry date'. https://home.liebherr.com/en/mys/apac/why-liebherr/magazine/best-before-date-vs-expiry-date.html (accessed Nov. 12, 2022).
[30] 'Over 300,000 Tonnes of Food Wasted in Hungary Annually', *Hungary Today*, Oct. 16, 2020. https://hungarytoday.hu/hungary-food-waste-value-300000-tonnes/ (accessed Nov. 14, 2022).
[31] 'Annual Food Waste In Hungary Amounts To 68 Kg Per Person', Aug. 06, 2020. http://xpatloop.com/channels/2020/8/annual-food-waste-in-hungary-amounts-to-68-kg-per-person.html (accessed Nov. 14, 2022).
[32] G. Kasza, A. Dorkó, A. Kunszabó, and D. Szakos, 'Quantification of Household Food Waste in Hungary: A Replication Study Using the FUSIONS Methodology', *Sustainability*, vol. 12, no. 8, p. 3069, Apr. 2020, doi: 10.3390/su12083069.

[33] B. Szabó-Bódi, G. Kasza, and D. Szakos, 'Assessment of household food waste in Hungary', *BFJ*, vol. 120, no. 3, pp. 625–638, Mar. 2018, doi: 10.1108/BFJ-04-2017-0255.
[34] Németh, N. and ;Mészáros, K., 'Vidéki háztartások a körforgásos gazdaság megvalósulásáért: A háztartási hulladékok kezelése és a környezettudatos vásárlási döntések vizsgálata Sopronban és környékén', *GAZDÁLKODÁS*, vol. 66, no. 3, pp. 260–294, 2022.
[35] E. Rogers, 'The diffusion of innovations model', *Nato Asi Series D Behavioural And Social Sciences*, 1993.
[36] 'Diffusion of Innovation Theory'. https://sphweb.bumc.bu.edu/otlt/mph-modules/sb/behavioralchangetheories/behavioralchangetheories4.html (accessed Oct. 17, 2022).
[37] M. Maciejczak, K. Takacs-Gyorgy, and I. Takacs, 'USE OF SMART INNOVATIONS FOR DEVELOPMENT OF CLIMATE SMARTAGRICULTURE', *Annals PAAAE*, vol. XX, no. 2, pp. 117–124, May 2018, doi: 10.5604/01.3001.0011.8125.
[38] K. Takács-György and I. Takács, 'Towards climate smart agriculture : How does innovation meet sustainability?', *Ecocycles*, vol. 8, no. 1, pp. 61–72, 2022, doi: 10.19040/ecocycles.v8i1.220.
[39] 'Agriculture 4.0: Why it is important to evolve from precision farming', *AFN*, Nov. 05, 2021. https://agfundernews.com/agriculture-4-0-why-it-is-important-to-evolve-from-precision-farming (accessed Oct. 14, 2022).
[40] 'What is the difference between digital education and traditional education?' https://www.qnextech.com/people-also-ask/What-is-the-difference-between-digital-education-and-traditional-education (accessed Oct. 07, 2022).
[41] 'Bridging the digital divide and ensuring online protection | UNESCO', Jul. 18, 2022. https://www.unesco.org/en/education/right-education/digitalization (accessed Oct. 07, 2022).
[42] 'Food loss analysis case study methodology', *FAO elearning Academy*, 2018. https://elearning.fao.org/course/view.php?id=374 (accessed Nov. 12, 2022).
[43] 'FAO elearning Academy: About the Academy'. https://elearning.fao.org/mod/page/view.php?id=4534 (accessed Nov. 12, 2022).
[44] 'Food Waste Prevention'. https://unccelearn.org/course/view.php?id=129&page=overview (accessed Nov. 12, 2022).
[45] D. Campbell and K. Munden-Dixon, 'On-Farm Food Loss: Farmer Perspectives on Food Waste', *The Journal of Extension*, vol. 56, no. 3, Jun. 2018, [Online]. Available: https://tigerprints.clemson.edu/joe/vol56/iss3/23
[46] B. T. Nyambo, 'Post-harvest maize and sorghum grain losses in traditional and improved stores in South Nyanza District, Kenya', *International Journal of Pest Management*, vol. 39, no. 2, pp. 181–187, Jan. 1993, doi: 10.1080/09670879309371787.
[47] F. G. Santeramo, 'Exploring the link among food loss, waste and food security: what the research should focus on?', *Agric & Food Secur*, vol. 10, no. 1, pp. 26, s40066-021-00302-z, Dec. 2021, doi: 10.1186/s40066-021-00302-z.
[48] F. G. Santeramo and E. Lamonaca, 'Food Loss–Food Waste–Food Security: A New Research Agenda', *Sustainability*, vol. 13, no. 9, p. 4642, Apr. 2021, doi: 10.3390/su13094642.

[49] M. del C. Alamar, N. Falagán, E. Aktas, and L. A. Terry, 'Minimising food waste: a call for multidisciplinary research: Minimising food waste', *J. Sci. Food Agric*, vol. 98, no. 1, pp. 8–11, Jan. 2018, doi: 10.1002/jsfa.8708.
[50] J. Oláh, G. Kasza, B. Szabó-Bódi, D. Szakos, J. Popp, and Z. Lakner, 'Household Food Waste Research: The Current State of the Art and a Guided Tour for Further Development', *Front. Environ. Sci.*, vol. 10, p. 916601, May 2022, doi: 10.3389/fenvs.2022.916601.
[51] I. S. K. Hub, 'Event: Sharm El-Sheikh Climate Change Conference (UNFCCC COP 27) | SDG Knowledge Hub | IISD', Nov. 2022. https://sdg.iisd.org:443/events/2021-un-climate-change-conference-unfccc-cop-27/ (accessed Nov. 12, 2022).
[52] S. Sakai *et al.*, 'International comparative study of 3R and waste management policy developments', *J Mater Cycles Waste Manag*, vol. 13, no. 2, pp. 86–102, Aug. 2011, doi: 10.1007/s10163-011-0009-x.
[53] *The State of Food Security and Nutrition in the World 2022*. FAO, 2022. doi: 10.4060/cc0639en.

THE PLACE OF SOCIAL ENGINEERING IN THE INFORMATION SECURITY AUDIT

A SOCIAL ENGINEERING HELYE AZ INFORMÁCIÓBIZTONSÁGI AUDITBAN

BARNA Bianka Rita[1] – KOLLÁR Csaba[2] – OROSZI Eszter Diána[3]

Abstract

In the information security audit, it is possible to use several methods and techniques, in this study we focused on social engineering. After the theoretical parts of the topic (audit, information security audit, expectations of the auditor, the importance of the audit, application of social engineering), we present the structure, process, and public results of an information security audit conducted in a real, large company environment. The name of the company will not be mentioned in our study. Based on the results, we formulate proposals for the development of information security awareness, and we also cover the presentation of the more important awareness development methods.

Keywords

audit, information security audit, social engineering, development of security awareness, case study

Absztrakt

Az információbiztonsági auditban többféle módszer és technika használatára van lehetőség, jelen tanulmányunkban a social engineeringre fókuszáltunk. A téma elméleti részei (audit, információbiztonsági audit, auditorral szembeni elvárások, az audit fontossága, social engineering alkalmazása) után egy valós, nagyvállalati környezetben végzett információbiztonsági audit felépítését, folyamatát, illetve publikus eredményeit mutatjuk be. A vállalat neve kérésére tanulmányunkban nem kerül megemlítésre. Az eredmények ismeretében javaslatokat fogalmazunk meg az információbiztonság-tudatosság fejlesztésére, illetve kitérünk a fontosabb tudatosság fejlesztési módszerek bemutatására is.

Kulcsszavak

audit, információbiztonsági audit, social engineering, biztonságtudatosság fejlesztése, esettanulmány

[1] biankabarna81@gmail.com | ORCID: 0009-0001-9367-3882 | information security technology specialist, Citibank | információtechnológiai biztonsági szakértő, Citibank

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

[3] oroszi.eszter@silentsignal.hu | ORCID: 0000-0001-8048-9034 | Head of Information Security Consulting Department, Silent Signal Ltd. | információbiztonsági tanácsadás üzletágvezető, Silent Signal Kft.

ELMÉLETI ALAPVETÉS

Az audit

Az audit egy olyan ellenőrzési folyamat, mely során különböző eljárások és tesztek alapján kivizsgálják, hogy az adott vállalat bizonyos részei, területei, (tanulmányunkban az információbiztonsági rendszerekben alkalmazott intézkedések) megfelelnek-e az elvárásoknak, mind a vállalat belső, mind a külső szabályozásokra tekintettel. Ezek az ellenőrzések biztosítják a vezetőséget arról, hogy minden folyamat a megfelelő módon történik a vállalatnál. Például ez egy tökéletes lehetőség arra, hogy a vezetés egy tisztább képet kapjon egy pártatlan személytől arról, hogy az alkalmazottak hogyan tartják be a vállalati irányelveket, a szabályozásokat és hogyan tartják magukat a velük szemben támasztott elvárásokhoz. Ugyan így, fény derülhet arra is, ha esetleg a munkatársak sorozatosan hibát követnek el valamely területen. Ilyen lehet például, ha biztonsági adatmentéseket elmulasztják megtenni, vagy ha a vállalat nem megfelelően vezeti a könyvelést. [1]

Egy adott vállalat szinte bármely részét auditálhatják. Az ellenőrzést ott szokták legtöbbször elvégezni, amely területek: magasabb prioritásúak, régen voltak felülvizsgálva vagy épp pont egy új program/ rendszer kerül bevezetésre az adott területen, melyet felül kell vizsgálni a helyes működés érdekében. [2]

Az audit legfontosabb követelménye, a független auditor személye. Ezért alakultak ki olyan széles körben elismert és elfogadott szervezetek, amelyek meghatározzák a követendő szabványokat és szabályokat az auditokat illetően. Ilyenek például az ISACA, az auditorok nemzetközi szakmai szervezete. Szinte minden országban (és államban) megtalálható valamilyen tagszervezete, például Magyarországon is. Az ISACA alapvető célja, hogy az információs rendszereket ellenőrizni és irányítani lehessen egy megadott keretrendszer szerint. [2]

Az auditálásnak több különböző típusa is van, tanulmányunkban elsősorban a belső auditokkal foglalkozunk részletesebben. A belső audit a szervezet saját szabályainak és követelményeinek betartását ellenőrzi. Ezek a felülvizsgálatok megtervezett időközönként ismétlődnek annak érdekében, hogy a vezetőség minél átfogóbb és naprakészebb információkkal bírjon a szervezete működéséről. Miután az időpontot kijelölték, fontos, hogy egy előre elkészített auditprogram szerint dolgozzanak, és megfogalmazzák az audit kritériumokat. Az auditorok kiválasztása is fontos feladat az objektív és teljesen pártatlan véleményformálás miatt. Ha a vizsgálatokat lefolytatták, az audit eredményeket jelentik a vezetésnek, és ha vannak, akkor a szükséges helyesbítéseket is végre hajtják. Ezután egy hivatalos dokumentumként az auditprogram és az audit eredményei megőrzendők. [1][2]

Az információbiztonsági audit

Az információbiztonsági auditok ugyan úgy lehetnek belső és külső auditok is. Ebben az esetben a belső információbiztonsági auditok néhány jellemzőjét ismertetjük. Ezeket az auditokat egy kiválasztott személy folytatja le, mely a szervezet egyik saját alkalmazottja, vagy egy a szervezet által megbízott alvállalkozó. Ezen auditok célja a lehetséges jövőbeli fejlesztések megismerése, és a követelményeknek való megfelelések vagy épp nem megfelelőségek észrevétele. Az eredményük pedig, egy auditjelentés mely részletesen ismerteti a megfelelőségeket, (vagy azok hiányát) és akár javaslatot is tehet a fejlesztési tervekhez és egyéb intézkedésekhez. Általában az ilyen auditok évente követik egymást. Ezek

ekkor teljeskörű vizsgálatot jelentenek, azonban lehetséges soron kívüli auditot is indítani. (Erre indok lehet például egy új jogosultságkezelő program használatba vétele a vállalatnál.) [2]

Minden belső audit a rá vonatkozó ISO szabványt, esetleg egy partner vállalt követelményeit, illetve az adott intézmény saját, belső követelményeit és elvárásait követi. Az információbiztonságra vonatkozó legismertebb szabvány melyet egy kissé bővebben ismertetünk, az MSZ ISO/IEC 27001:2014 [12].

Az ISO/IEC 27001:2014, a szabvány mai napig Magyarországon hatályos kiadása. A legújabb kiadást 2022 októberében publikálták, azonban hazánkban a honosítás miatt jelenleg is a 2014-es változatot használták a tanulmány készítésének időszakában. [3]

A legtöbb szervezet komoly struktúrát igényel, ha az információbiztonságról és annak ellenőrzéséről van szó. Az ISO/IEC 27001 erre ad megoldást, hiszen gyakran ad megoldás konkrét helyzetekre, és ez alapján majdnem felépíthető egy vállalat Információbiztonsági Irányítási Rendszere (IBIR). A benne szereplő ellenőrzések leginkább az IT (információtechnológia) és az adatbiztonság témakörét öleli fel, azonban a nem IT vonatkozású eszközök (ahogy a papírmunka és a védett nyomtatványok) kevésbé kerültek kidolgozásra, így kevésbé védettek. [2]

A vállalati vezetés meghatározhatja az IBIR hatáskörét és akár egyetlen egy helyszínre vagy üzleti egységre is korlátozhatja azt [6] [7]. Ezért, ha ismert, hogy egy szervezet egy bizonyos részen alkalmazza az ISO/IEC 27001-et, az nem jelenti az, hogy kijelenthető, a vállalat egyöntetűen megfelelést vár el ehhez a szabványhoz képest. Az ISO/IEC 27000-es szabványcsalád a többi elemével együtt további útmutatást adnak az IBIR tervezéséhez, megvalósításához és a működtetési szempontokhoz. [2]

A szabvány legfontosabb része az „A melléklet”, mely a következő kérdésekre ad útmutatást [12]:

„A5. Információbiztonsági szabályok
A5.1. Az információbiztonság vezetői irányítása
A6. Az információbiztonság szervezete
A6.1. Belső szervezet
A6.2. Mobil eszközök és távmunka
A7. Az emberi erőforrások biztonsága
A7.1. A munkaviszony kezdte előtt
A7.2. A munkaviszony fennállása során
A7.3. A munkaviszony megszűnése és megváltozása
A8. Vagyonelemek kezelése
A8.1. A vagyonelemekért viselt felelősség
A8.2. Információosztályozás
A8.3. Adathordozók kezelése
A9. Hozzáférés-felügyelet
A9.1. A hozzáférés-felügyelettel kapcsolatos üzleti követelmények
A9.2. A felhasználói hozzáférések kezelése
A9.3. Felhasználói felelősségek
A9.4 Rendszer- és alkalmazás-hozzáférés felügyelete
A10. Titkosítás
A10.1 Titkosítási intézkedések

A11. Fizikai és környezeti biztonság
A11.1 Biztonsági területek
A11.2. Berendezés
A12. Az üzemeltetés biztonsága
A12.1. Üzemeltetési eljárások és felelősségek
A12.2. Védelem a rosszindulatú szoftverek ellen
A12.3. Mentés
A12.4. Naplózás és megfigyelés
A12.5. Az üzemeltető szoftverek felügyelete
A12.6. A műszaki sebezhetőségek felügyelete
A12.7 Az információs rendszerek auditálásával kapcsolatos megfontolások
A13. A kommunikáció biztonsága
A13.1. A hálózatbiztonság biztosítása
A13.2. Információátvitel
A14. Rendszerek beszerzése, fejlesztése és karbantartása
A14.1. Az információs rendszerek biztonsági követelményei
A14.2. Biztonság a fejlesztési és támogatási folyamatban
A14.3. Tesztadatok
A15. Szállítói kapcsolatok
A15.1 Információbiztonság a szállítói kapcsolatokban
A15.2. A szállítói szolgáltatásnyújtás irányítása
A16. Az információbiztonsági incidensek kezelése
A16.1. Az információbiztonsági incidensek és javítások kezelése
A17. A működésfolytonosság biztosításának információbiztonsági vonatkozásai
A17.1. Az információbiztonság folytonossága
A17.2. Tartalékok
A18. Megfelelés
A18.1. Megfelelés a jogi szerződéses követelményeknek
A18.2. Információbiztonsági vizsgálatok”

Ezen szempontok alapján tanúsítják a vállalatokat, és írja meg sok vállalat az IBIR-t.

Az auditorral szemben elvárt követelmények

Egy audit előkészítésekor fontos, hogy az auditor megfelelő kapcsolatot tartson az auditáltakkal. Ezzel biztosítja, hogy a lehető legjobban az adott vállalathoz viszonyítva ellenőriz. Így pontosítja az elvárásokat az összes résztvevő között, mely többek között magában foglalja a releváns információkat az audit célját illetően, a vizsgálat hatásköréről és kritériumairól, az alkalmazott módszerekről és az ellenőrzési csoport összetételéről is. Az auditor a legtöbb esetben hozzáférést kér az audithoz szükséges releváns információkhoz, melyek tartalmazzák a szervezet által meghatározott kockázatokat, valamint azok kezelését is. [1][2]

Az auditornak felül kell vizsgálnia az auditált vállalat irányítási rendszerének dokumentációit. Ezeknek tartalmaznia kell az irányítási rendszer korábbi audit jelentéseit, saját dokumentumait. Erre azért van szükség, hogy a releváns információkat összegyűjthesse,

és készítsen saját részére egy áttekintést, a lehetséges megfelelések, vagy épp nem megfelelések előre vetítése érdekében. A felülvizsgálatot követően meg kell tervezni az auditot. Ez segít betartani az ütemtervet és a tevékenységek összehangolását. [4]

Az auditornak külön figyelmet kell fordítania arra, hogy a terv elkészítésének folyamata, a terv tartalma eltérhet különböző külső tényezők miatt. Ilyen lehet például, ha vannak már megelőző auditokról feljegyzések, vagy ha épp ez az első. Illetve az is számít, hogy külső, avagy belső auditról van szó. Egyéb előreláthatatlan okok miatt az elkészült tervezetnek elég rugalmasnak kell lennie ahhoz, hogy a később, a felülvizsgálat előrehaladtával felmerülő változásokat eszközölni lehessen. [4]

Azonban az auditornak nem csak tankönyvekben meghatározott elvárásoknak kell megfelelnie. Az ő helyzetében nagyon fontos az is, hogy megfelelő első benyomást tegyen és a lehető legszimpatikusabban (de határozottan) prezentálja magát az auditáltak előtt. Ilyenkor döntő szerepet játszik a külső megjelenés, valamint a helyes verbális és nonverbális kommunikáció alkalmazása. A folyamatos jelenlét, a lelkes munkavégzés és a szakmai jártasság egyaránt fontosak ahhoz, hogy a felülvizsgálatot végző személy a vállalat minden területén megfelelő kapcsolatot tudjon kialakítani az auditáltakkal.[2][4]

Információbiztonsági audit fontossága

Az információbiztonsági audit fontossága véleményem szerint az összetettségében rejlik. Ekkor az auditor nem csak a vállalat folyamatait kell megfigyelje, de betekintést nyer a munkatársak biztonság-tudatosságába is a mindennapokban. Ezt az összetettséget nagyon jól szemlélteti Baglyos írása:

„Az információbiztonsági audit a szervezetek informatikai infrastruktúrájának átfogó felülvizsgálatát jelenti. Ezek a fajta auditok biztosítják, hogy a megfelelő irányelveknek, eljárásoknak, jogszabályoknak eleget tettek és ezáltal hatékonyan működnek. A vizsgálatok célja, hogy olyan sebezhető pontokat azonosítsanak, amelyek adatvédelmi incidenseket idézhetnek elő. Ezek lehetnek azok a sebezhetőségek, amelyeket a támadók kihasználhatnak a jogosulatlan hozzáféréshez. Az információbiztonsági audit elvégzésének fő oka a biztonsági és megfelelőségi hiányosságok azonosítása, valamint azok kezelése. Egy alapos felméréssel a szervezet átfogó képet kaphat a rendszereiről, és betekintést nyerhet a sebezhetőségek kezelésének legjobb módszereibe. A szervezeteknek nem csak az üzleti tevékenység megszakadásának és a hatósági bírságoknak a veszélye miatt kell aggódniuk, mivel egy biztonsági incidens (különösen, ha az megelőzhető lett volna a megfeleléseknek eleget téve) valószínűleg a beszállítók és az ügyfelek bizalmát is csökkentheti. Ha az incidens elég súlyos volt, ezek az érdekeltek akár úgy is dönthetnek, hogy nem kívánnak továbbra is együtt dolgozni az adott szervezettel. Ugyanez vonatkozik a szabályozási hibákra is. Ha a szervezet bizonyítani tudja, hogy megfelelő lépéseket tett az adatvédelemmel kapcsolatban, a szabályozó hatóságok nem fognak jelentős bírságokat kiszabni. Ha azonban az incidens gondatlanságból következett be, a szervezetekre súlyosabb büntetések várhatnak. Ha ezek a büntetések nem is közelítik meg a GDPR által megengedett maximumot (20 millió euró vagy a szervezet éves globális forgalmának 4%-a), egy viszonylag enyhe bírság is katasztrofális lehet a szervezet jövőjére nézve.

Az információbiztonsági audit során az eddig említetteken túl, vizsgálják még:

- az adatbiztonságot: hálózati hozzáférés, adattitkosítás;
- a működési biztonságot: irányelvek, eljárások, ellenőrzések;

- a hálózati biztonságot: vírusvédelem, hálózatfelügyelet;
- a rendszerbiztonságot: javítás, privilegizált fiókok kezelés;
- valamint a fizikai biztonságit: külső, belső területvédelem, eszközök, vagyontárgyak védelme." [5]

Ebben a cikkben a szerző referál a 2013. évi L. törvényre, mely hazai viszonylatban igen meghatározó, a vállalatok adatvédelmi, információbiztonsági struktúráinak kialakításakor. Ezért is annyira fontos a helyes információbiztonsági auditálás, mivel ez a törvény olyan elengedhetetlen pontokat érint, mint a biztonsági események kezelése; biztonsági osztályba sorolás; védelem kialakítása; stb.

Az említett pontok által világosan látszik az információbiztonsági audit relevanciája. Összességében, az információbiztonsági audit segít betartani a szabványokat és jogszabályokban meghatározott előírásokat, valamint bepillantást enged a vállalat információbiztonsági szemléletébe.

A social engineering alkalmazása az audit során

Az információbiztonság világában igyekszünk lehető legkevesebb támadási felületet hagyni a támadók számára. Azonban amíg az online világban több lehetőségünk is van az esetleges támadások kivédésére, (akár egy vírusírtó segítségével, egy tűzfallal vagy néhány korlátozás bevezetésével) a valóságban létezik egy olyan biztonsági rés, melyet bárki, bármelyik adandó pillanatban kihasználhat. Ez pedig nem más, mint az a tény, hogy a munkatársak bizony „csak" emberek.

Mivel a social engineering számos technikával kivitelezhető [11] a munkatársak felkészítése egy ilyen esetre sokkal nehezebb. Azonban, ha egy auditba építve számon tudják kérni a vállalatot, az rá lesz kényszerítve arra, hogy megfelelően „bizalmatlanná" tegyék a munkatársakat, ezzel felkészítve őket egy esetleges social engineering támadásra.

Egy megfelelően kidolgozott kötelező információbiztonság-tudatossági oktatással, amely meghatározott időnként megismétlésre kerül, jól szinten tartható a kellő óvatosság a munkatársak körében.

A TÉMA EMPIRIKUS VIZSGÁLATA

A következőkben esettanulmányként egy nagyvállalatnál végzett információbiztonsági auditot és annak eredményeit ismertetjük.

A vállalati környezet ismertetése

Az adathalász kampányt nagyvállalati környezetben végeztük. Az energiaszektor egyik kiemelt szereplőjeként a cég nagy figyelmet fordít a biztonságra. Ahhoz, hogy a megfelelő információbiztonság-tudatossági oktatást biztosíthassák munkavállalóik számára, fontos, hogy mindig naprakész adataik legyenek arról, milyen a vállalat általános teljesítménye egy éles helyzetben.

A vállalatnak több telephelye is van, a fővárosban és az ország minden területén egyaránt. Ahogy az majd később az adathalász e-mail eredményeiben is megmutatkozik, jelenleg 6946 munkavállaló dolgozik összesen a vállalat telephelyein. Ez a szervezet követi a tipikus nemzetközi nagyvállalatok felépítését. Megkülönböztet vezérigazgatót és -helyetteseket, valamint igazgatóságot és osztályokat (ezeken belül néha csoportokat) is. Ezek a

jól elválasztott rétegek, gyakran még inkább megkönnyítik az adathalászok dolgát, hiszen egy kevés utánajárás után (például LinkedIn segítségével) könnyen találhat a céljainak megfelelő áldozatot, akire a támadást irányítani fogja. Az általában a legjobban veszélynek kitett pozíciók közül néhány példa lehet: a vezérigazgatóság tagjai, az üzemeltetés vagy a kontrolling tagjai, bármilyen humánpolitikai vonatkozású beosztás, vagy akár a kommunikációs munkatársak, hiszen ők még szorosabb kapcsolatban vannak a közösségi oldalakkal és a sajtóval.

A vállalaton belül kiforrott intézkedések működnek egy esetleges adathalász kampány bekövetkeztének esetére. Egyaránt használnak spam-szűrőket, tűzfalakat, különböző végpontvédelmi megoldásokat (kötelező VPN használat a vállalat saját hálózatán kívül), illetve akár egy esetleges gyanús e-mail vagy telefonhívás kapcsán bárki felkeresheti az illetékes incidenskezelő csoportot. Habár az igazán kifinomult adathalász támadások pontosan ezeket az intézkedéseket kerülik ki észrevétlenül, hiszen pszichológiai manipulációt és mindenki számára elérhető nyílt információkat felhasználva férkőznek olyan munkavállalók közelébe, akik egy esetleges gyanús tartalmú e-mailt nem ismernek fel, és megteszik, amit a levélben írnak, ha az épp elég meggyőző és neki szól.

Az audit során kiküldött adathalász e-mailt az információbiztonsági csapat készítette, majd felügyelte az esetleges visszajelzéseket is. Például, ha valaki bejelentette, hogy gyanús levelet kapott, választ kellett visszaküldeni, melyben elmagyaráztuk, hogy ez csak egy általunk kreált adathalász levél, de köszönjük, hogy jelezte.

A szimuláció célja

Az általunk megalkotott adathalász e-mail egy adathalász kampány részét képezte. Ez a kampány részben az októberi kiberbiztonsági hónap előzetes felmérése miatt jött létre, részben pedig a közelgő belső audit miatt. Évente négyszer tartunk általában ehhez hasonló belső adathalász kampányokat (lokálisan) és másik négy alkalommal anyavállalati szinten kerülnek kiküldésre ilyen e-mailek. Ezek száma változhat például nagyobb globális adatszivárgások esetén, mivel ilyenkor felfrissítjük a munkatársaink biztonságtudatosságát, vagy esetleges magasabb linkre kattintási arányt eredményező kampány esetén (mely meghaladja a 10%-ot) újabbal készülünk a biztonságtudatosság fenntartása érdekében.

Minden biztonságtudatosságot célzó kampány legfontosabb mozzanata a cél megnevezése. Ez azért nagyon fontos, mivel a célkitűzésnek illeszkednie kell a vállalat saját biztonságtudatossági stratégiájához. Ezt időnként módosítják, felülvizsgálják, illetve bővítik, így más és más időszakokban végzett kampányok célkitűzései ezek szerint változnak.

Az adott adathalász kampányt megelőző kampányok mindig fontos szerepet játszanak az újabb tervezésében. Amennyiben egy adathalász kampány eredménye (lokális vagy vállalati csoport szinten) eléri a 10%-os kattintási arányt további tudatossági akciókat szerveznek (cikkek megjelentetése a belső intranet hálózaton, egyéni tudatosítási előadásokat szerveznek, vagy akár megkeresik a rosszabbul teljesítő vállalati területeket és direkt képzést nyújtanak).

Az adathalász e-mailünk jelenlegi célja kisebb részben volt a kiberbiztonsági hónap. Nagyobb részben a cél nem volt más, mint a közelgő belső auditra való felkészülés. Egy belső audit során a legfontosabb, hogy a vállalat tisztában legyen a saját, és a követelményeknek való megfeleléseivel (vagy épp a nem megfelelőségekkel), valamint lehetséges

jövőbeli fejlesztésekkel. A hasonló kampányoknál évente meghatározzuk, hogy milyen biztonságtudatosítási tevékenységeket végzünk (például adathalász kampányok száma, oktatások száma és témája, októberi „kiberhónap” eseményei).

Az általunk vizsgált esetben kampányunk célját akkor érjük el, amint megkapjuk a végleges adatokat arról, hogy a kiküldött e-mailek közül hány esetben lett volna éles helyzetben sikeres a támadásunk. Mivel ez megmutatja, hányan nem ismerik, illetve nem tartják be a vállalat információbiztonsági szabályzatát.

Az adathalász kampány

A teszt lefolytatásához a vállalat által ilyen esetekben használt Lucy Security szoftvert használtuk. A svájci Lucy Security egy kiberbiztonsági tudatosság fejlesztő szoftver. A kiberbiztonsági tudatosságot növelő tréning innovációi lehetővé teszik a szervezetek számára, hogy mérjék, javítsák és teszteljék alkalmazottaik biztonság-tudatosságát. Több támadássablon és sok testre szabható, képzési modul közül választhatunk. Első lépésként egy új kampányt, azon belül pedig egy új forgatókönyvet hoztunk létre. Mikor ezzel elkészültünk, különböző előre gyártott sablonok közül válogathattunk, de akár kreálhattunk is egy saját tematikájú kampányt. Fontos szempont volt, hogy az általunk használt sablon rendelkezzen magyar nyelvű „landing page-dzsel”, és üzenettel. A mi esetünkben egy Google értesítés alapú kampányt választottunk, hiszen a vállalatnál fontos szabály, hogy a Google egyik szolgáltatását sem használják a kollégák, adatvédelmi szempontok miatt. Így az első intő jel lehetett az olvasóknak az, hogy Google-fiók értesítőt kaptak a céges e-mail címükre. Az általunk kiküldött üzenet az 1. ábrán látható:


Google

Kedves Google felhasználó!

Google-fiókjának helyreállítási telefonszáma nemrég megváltozott. Ha végrehajtotta ezt a módosítást, akkor nem kell többet tennie.

Ha nem Ön változtatta meg helyreállítási telefonszámát, előfordulhat, hogy valaki feltörte a fiókját. További információért látogassa meg ezt a linket: https://support.google.com/accounts/bin/answer.py?answer=2450236.

Ha problémái vannak a fiókjához való hozzáféréssel, állítsa vissza jelszavát az alábbi gombra kattintva:

Jelszó törlése

Üdvözlettel,
The Google Support csapat

This email can't receive replies. For more information, visit the Google Accounts Help Center.

You received this mandatory email service announcement to update you about important changes to your Google product or account

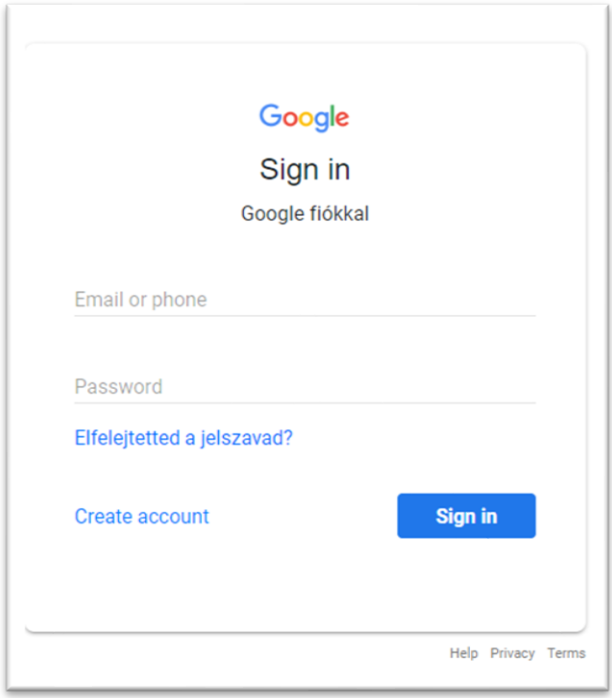
©2018, Google Inc., 160 Amphitheatre Parkway, Mountain View, CA 94043, USA

Please note that the third-party logos and trademarks used in this email or landing page are used for illustrative or instructional purposes only and there is no connection or relationship between the trademark owner and Lucy Security or the LUCY Security customer.

1. ábra A kiküldött üzenet (saját szerkesztés)

Az e-mail feladójaként egy általunk kreált e-mailcím jelent meg, mely goggle.sup@cloudserver185.com volt. A tárgymezőben pedig „Valaki feltörhette a Google fiókodat” szerepelt. Azok a kollégák, akik figyelmesen elolvasták a feladó e-mail címét, már a levél megnyitása előtt rájöhettek, hogy gyanús e-mail érkezett a postafiókjukba, hiszen a Google-re nem jellemző e-mailcím a feladó. A szöveg tartalmi része a mi esetünkben különösen testhezállónak bizonyult, mivel a vállalatnál nemrégiben telefonszolgáltató váltás történt, így a figyelmetlenebb kollégák könnyen összekapcsolhatták a SIM kártyák cseréjét ezzel az üzenettel.

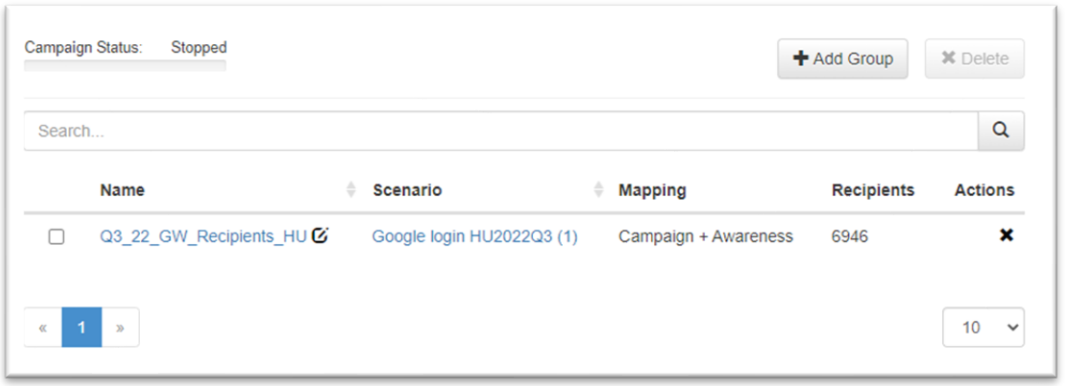
Azonban, ha valaki végig olvasta az apróbetűs részt is az üzenet alján, egyértelműen látszik, hogy a Lucy Security program által generált adathalász szimulációról van szó. Abban az esetben, ha a megadott linkre kattintottak, egy új böngészőoldal nyílt meg, mely a 2. ábrán látható.



2. ábra Az oldal, melyre a link vezetett (saját szerkesztés)

A képen jól látszik, hogy a felugró bejelentkező ablak félig magyarul, félig angolul van, ami szintén gyanús lehetett a kollégáknak.

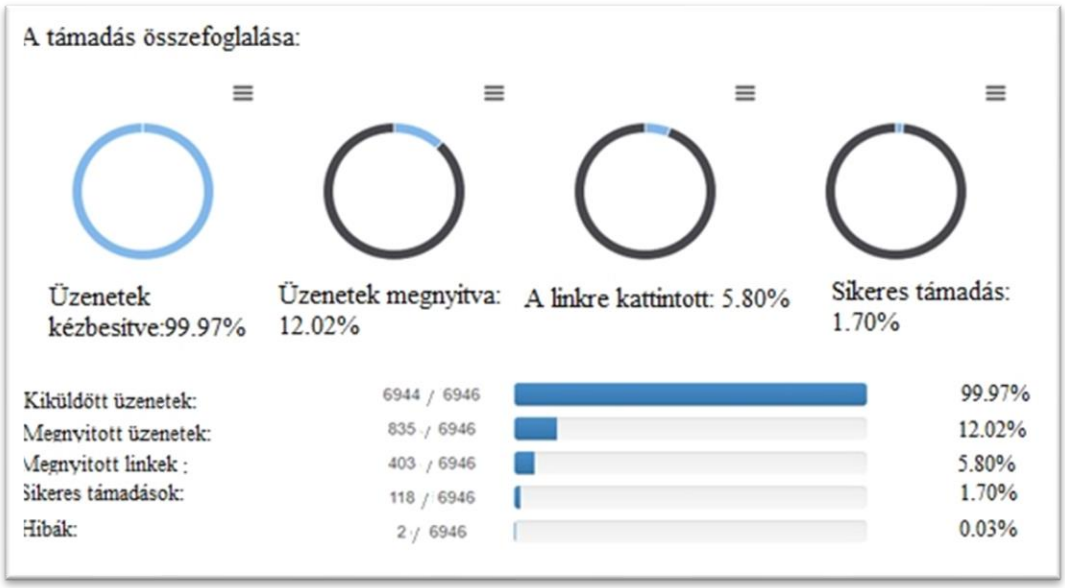
Miután elkészültünk az ál e-maillel, megadtuk a kampánnyal tesztelni kívánt dolgozók csoportját. A mi esetünkben ez a vállalat összes magyarországi dolgozóját magában foglalta. A 3. ábrán azt a felhasználói csoportot mutatjuk be, mely a vállalat által kiadott összes e-mail címet tartalmazza. (A felső vezetőktől a gyakornokokig) Ahogy az a 3. ábrán is látszik, végül az e-mail 6946 címre került kiküldésre.



3. ábra A vállalati csoport kiválasztása (saját szerkesztés)

Az eredmények

Az adathalász kampányunk nagyjából egy hétig tartott. Az e-mailek kiküldését követő két napban volt észlelhető a legtöbb linkre kattintás és sikeres támadás. Ezt követően a számuk drasztikusan csökkent. Végül a szoftver által egy hét múlva megkaptuk az adathalász szimuláció eredményét, melyet a 4. ábra mutat be:



4. ábra A támadási szimuláció eredményei (saját szerkesztés)

Jól látszik, hogy a kiküldött 6946db e-mail közül 6944 db sikeresen kézbesítve lett. A két meghiúsult kézbesítés valószínűleg épp a kilépés folyamatában levő kollégát, vagy már nem létező e-mailcímet jelöl. A levelet megkapó kollégák alig több mint 12%-a nyitotta meg a levelet, így elmondható, hogy szerencsére a dolgozók többsége tisztában van vele, hogy a vállalat semmilyen formában nem használja a Google szolgáltatásait. Még kevesebb,

a megnyitók csupán 5.8%-a kattintott a linkre, melyből 1.7% volt sikeres támadásnak tekinthető, azaz a kollégák megadták személyes adataikat.

Az általunk az előbbiekben referált szabályzat a vállalat saját információbiztonsági szabályzata. Épp ezért konkrétumok nélkül térhetünk csak ki rá. A szabályzat először meghatározza saját hatókörét és a fogalmakat és rövidítéseket melyek a dokumentumban szerepelnek. Ezután ismerteti a munkavállalók felelősségét, mely egyértelműen kijelenti, hogy minden munkavállaló az általa kezelt információk biztonságáért felel és felelősségre vonható. Az információk biztonsági besorolásának ismertetése fontos része a szabályzatnak. Ez alapján lehet: nyilvános, belső, bizalmas vagy szigorúan bizalmas egy adat. A besorolás alapján részletesen leírja az adott információk kezelésére vonatkozó előírásokat. A minősített adatok fogalmának és kezelésének szerves részét képezi a 2009. évi CLV törvény a minősített adat védelméről; valamint a GDPR adatvédelme és megfelelései. Ezek után a szabályzat ismerteti a jelszóhasználati szabályokat, hogy a lehető legbiztonságosabb, nehezen feltörhető jelszavakkal legyenek biztosítva a céges felhasználói fiókok.

A következő részben pedig az általunk előbbiekben említett szabályt ismerteti, miszerint a vállalat eszközeire csak és kizárólag a vállalat által jóváhagyott szoftverek és fájlok telepíthetőek vagy tölthetőek le. A vállalat által kiadott IT eszközök kizárólag üzleti célokra használhatóak egészen addig amíg a munkavállaló vezetője máshogy nem rendelkezik. (Egy ilyen döntésbe azonban kötelező a hozzáértő IT-s személyzet véleményét kikérni.)

A szabályzat a továbbiakban ismerteti:

- a biztonságos internet használatot,
- a biztonsági mentések fontosságát,
- a „tiszta asztal” elvet,
- az információ biztonságos megosztására vonatkozó szabályokat (például titkosított e-mailek)
- az információkezelést, információs rendszer fejlesztést és bevezetést
- a külső állományra, szolgáltatókra és partnerekre vonatkozó biztonsági előírásokat
- a naplózásra, jelentésekre és ellenőrzésekre vonatkozó előírásokat
- a gyanús viselkedés, biztonsági incidensek jelentését és az ehhez szükséges kapcsolattartási elérhetőségeket

Ezek után az utolsó részben bemutat egy rövid kockázat elemzést, a szabályozott tevékenységek felügyeletét, és ismerteti a szabályzatra vonatkozó hivatkozásokat és kapcsolatokat.

Mivel az általunk kapott a számadatok a 10%-os vállalat által meghatározott linkre kattintási határ alatt vannak, így annyiban tér el az eredmény a megszokottól, hogy nem volt szükség plusz tudatossági akciókat bevezetni. Úgy döntöttünk elég egy cikket írnunk róla, a munkatársak tájékoztatásának érdekében. Amennyiben az eredmény meghaladta volna a 10%-t, egyéni tudatosítási előadásokat szerveztünk volna, vagy megkerestük volna a roszszabbul teljesítő területeket és területre szabott képzést nyújtottunk volna nekik.

JAVASLATOK AZ INFORMÁCIÓBIZTONSÁG-TUDATOSSÁG FEJLESZTÉSÉRE

Egy nagyvállalati rendszerben a biztonság mindig kulcsfontosságú kérdés. Mind fizikai mind információbiztonsági oldalról. A következőkben az utóbbi témát mutatjuk be,

pontosabban azt, hogy milyen eszközökkel lehet és érdemes az információbiztonság-tudatosságot fejleszteni egy nagyvállalati környezetben.

Információbiztonság-tudatosság fejlesztése és javaslatok

Minden vállalat (vagy vállalkozás) életében nagy szerepet kap a munkavállalók felkészítése az esetleges webes fenyegetésekre, adat- vagy információlopásokra. De a vállalat növekedésével (és minél fontosabb pozíciójával) könnyen célkeresztbe kerülhet. Gyakrabban lehet kitéve social engineering támadásoknak, hacker támadásoknak, és egyéb fenyegetettségeknek, melyek célja az információszerzés, a vállalat hírnevének rombolása, vagy akár a teljes megsemmisítés.

Ezek miatt kap hatalmas szerepet és figyelmet az információbiztonság-tudatossági oktatás. Mivel a legkönnyebben kihasználható információbiztonsági rés maga az ember, mint tényező, a támadók bármilyen eszközt bevethetnek, hogy megszerezzék amire szükségük van. A rendszeres információbiztonsági oktatásokkal azonban a munkatársakban rejlő kockázat csökkenthető. Minél többször találkoznak valós támadásokhoz hasonló helyzetekkel, annál felkészültebben éri őket egy igazi élesben zajló támadás. Az információbiztonság-tudatossági tréning sikerét nagyban befolyásolja az oktatás minősége és a módszerek. A munkatársak az alábbi alapvető elvárásokkal kell megismerniük a tréning során:

- Tiszta asztal elv alkalmazása
- Tiszta képernyő használata
- Kulcsok, kártyák rendeltetésszerű kezelése
- Hardver eszközök és adathordozók kezelése, valamint tárolása
- A jelszavakkal kapcsolatos előírások betartása
- Iratmegsemmisítés helyes elvégzése
- Adathalász-gyanús e-mailek és egyéb technikák felismerése
- Vírusvédelem megfelelő alkalmazása
- Közösségi média használata (a vállalt területén és a magánéletben)
- Okos eszközök rendeltetésszerű, biztonságos használata
- Egyéb az adott vállalatra érvényes szabályok [8][9][10]

A tiszta asztal és tiszta képernyő: Az iroda kialakításakor arra kell törekedni, hogy a dolgozók és más esetlegesen a szobában tartózkodó személyek minél kevésbé lássanak rá a monitorokra. Az íróasztalon nem szabad látható helyen érzékeny adattal bíró dokumentumokat, feljegyzéseket tárolni. Ugyan így tilos a jelszavakat kiragasztani az asztal környékén, az irodában és bárhol, ahol illetéktelen személyek felhasználhatnák. Ugyan így nem tanácsos naplóban vagy kis könyvben tartani sem. Inkább használjuk valamely jelszókezelő programot melyhez a hozzáférést a vállalat biztosítja. A munkaidő lejártával az ehhez hasonló dokumentumokat elzárt helyen kell tartani. Mikor elhagyjuk a munkaállomást, a számítógépet lezárt (mai Windows operációs rendszereknél például a Windows-gomb és „L” együttes lenyomásával) vagy kikapcsolt állapotban kell az irodában hagyni. Ekkor külön figyelmet kell fordítani arra is, hogy a fénymásológépekben, nyomtatókban ne hagyjunk érzékeny iratot. Ha valamilyen okból kifolyólag vendég van az irodában, semmi esetre se hagyjuk egyedül, hiszen alkalma nyílhat kutakodni a dokumentumok között, illetve a fiókokban, szekrényekben. Az utolsó munkatárs, aki a nap folyamán elhagyja az irodát, ha van lehetősége, kulccsal zárja az irodát.

Kulcsok, kártyák rendeltetésszerű kezelése: A kulcsok és belépőkártyák kizárólag illetékes személyeknek adhatók ki. Amennyiben vendég érkezik az irodába, például egy megbeszélés miatt, érdemes megkérni a kollégát, akihez jött, hogy együtt közlekedjenek a látogatás idején az épületben. A kulcsok vagy kártyák kiadásáról, visszavételéről, esetleges cseréjéről vagy bevonásáról és megsemmisítéséről minden esetben nyilvántartást kell vezetni, mely a lehető legnaprakészebb állapotban kell legyen. Fontos, hogy a munkavállalók ismerjék a kulcsok és belépőkártyák használatának szabályait (például, hogy nem adhatják oda vagy nem adhatják kölcsön senki másnak stb.). A szabályok ismertetése, ha elmarad, komoly következményei lehetnek.

Hardver eszközök és adathordozók kezelése, valamint tárolása: A munkatársaknak kiemelt fontosságú megismernie a különböző hardverek és adathordozók helyes használatát. Ezek egyik első és talán legfontosabb szabálya, hogy ha a vállalat nem a „hozd a saját eszközöd" alapján működik, akkor saját adathordozót nem csatlakoztathat senki a vállalat hálózatán működő gépekre. Ez a szabály ugyan úgy vonatkozik okostelefonokra, táblagépekre és egyéb okos eszközökre is.

A jelszavakkal kapcsolatos előírások betartása: Sok esetben a vállalatok saját elvárásokat támasztanak a munkavállalókkal szemben arra vonatkozóan, hogy milyen jelszavakat kell bizonyos felületen használniuk. A könnyebb megjegyezhetőség és a maximális biztonság érdekében, a legtöbb cég ma már saját jelszókezelő szoftvert ad a dolgozók kezébe, így a hosszabb, biztonságosabb jelszavakat nem szükséges megjegyezni, sem pedig papírcetlikre írva kiragasztani valahova. Fontos tudatosítani a kollégákban, hogy a jelszavakat ne osszák meg se egymással, se senkivel. Egymás belépési kulcsait pedig szintén ne használják és ne engedjék másnak sem, hogy így tegyenek.

Iratmegsemmisítés helyes elvégzése: Egy cég életében mindig keletkeznek olyan dokumentumok, melyekre már esetleg nincs is szükség, azonban még mindig tartalmazhatnak olyan adatokat, melyek illetéktelen személy kezébe kerülve kárt okozhatnának. Ezeket mindig a megfelelő körültekintéssel kell tárolni s megsemmisíteni. Fontos tudatosítani a kollégákban, hogy ilyen esetben nem csak papírlapokra kell gondolni. lehetek ezek borítékok, belépőkártyák, külső adathordozók is. Az iratmegsemmisítés mindig olyan mértékű kell legyen, hogy az adott tárgy helyreállítása többe kerüljön (akár időben akár pénzben) mint az általa hordozott információ értéke.

Adathalász-gyanús e-mailek és egyéb technikák felismerése: A munkatársak érzékenyítése az ilyen szituációkra nagyon fontos. Akár egy egész vállalat sorsa is múlhat egy adathalász támadáson. Ezért lényeges, hogy a gyanús e-maileket és egyéb kétes megkereséseket (mobiltelefonos hívás, SMS, személyes beszélgetéssel stb.) gyorsan felismerjék, valamint tudják, hogy hol kell bejelenteniük. Ez minden vállalatnál más lehet, de biztosan az információbiztonsági osztályhoz van köze.

Vírusvédelem megfelelő alkalmazása: A munkatársak gyakran értesítést kapnak a legújabb frissítésekről, melyeket a számítógépen eszközölniük kell. Ezt semmiképp sem szabad elmulasztaniuk, hiszen az IT részleg kifejezetten azért küldi ezeket az értesítéseket,

hogy a vállalat összes használatban lévő eszközét friss, naprakész szoftverrel használjuk. Ezzel igyekeznek csökkenteni az esetleges sérülékenységekből adódó támadások kialakulásának esélyeit.

Közösségi média használata: Napjainkban szinte már nincs olyan személy, aki valamilyen formában nem lenne jelen a közösségi médiában. Sajnos emiatt a legtöbben tudtukon kívül is áldozatául eshetnek egy támadónak, aki épp kiválasztja ki legyen az áldozata a következő social engineering támadás során. Ezért fontos a munkavállalókban tudatosítani, hogy mit lehet és mit nem lehet közzétenni a közösségi média oldalakon.

Íme néhány példa:

- ne osszuk meg a helyzetünket
- ne tegyünk közzé képet melyek az irodában vagy a vállalat telephelyein belül készülnek
- ne osszunk meg belső vállalati adatokat
- ne osszunk meg a jelszavakra utaló képeket, szövegeket
- semmiképp se osszuk meg a lakcímet, telefonszámot, és egyéb olyan személyes adatokat melyekkel esetleg valaki visszaélhet
- ne adjunk ki anyagi helyzetünkre utaló képeket, videókat

Abban az esetben, ha egy munkavállaló mégis megoszt a fentiekhez hasonló tartalmakat, veszélybe sodorhatja a vállalatot. Ezért fontos, a helyes oktatás és az ott hallott információk elsajátítása. Pont a fent említett okok miatt egyes vállalatok megtiltják a közösségi média oldalak látogatását a saját hálózatukról.

Okos eszközök rendeltetésszerű, biztonságos használata: A közösségi média mellett, az okos eszközök használata szintén népszerű manapság. Azonban fontos a munkavállalók tudtára adni hogyan lehet egy adott vállalati környezetben használni őket. Amennyiben saját, és nem céges eszközről van szó, még nagyobb odafigyelésre van szükség. Többek között fontos ismertetni a kollégákkal, hogy hol és mikor lehet az eszközöket telefonálásra, video hívásra, vagy akár fényképezésre használni. Ez vállalatonként változhat, annak függvényében, hogy milyen pozícióban dolgozik az illető, és mivel foglalkozik maga a cég. Az ilyen eszközök töltése is fontos, hogy említést tegyünk róla, mivel akár vírussal fertőzöttek is lehetnek. Így semmiképp sem javasolt a vállalati hálózathoz csatlakoztatott céges eszközökről tölteni őket. Ugyan ezen okból kifolyólag fontos az is, hogy nem csak a vállalat által kiadott laptopokra és asztali gépekre, de a céges okoseszközökre sem javasolt ismeretlen vagy nem megbízható forrásból származó applikációkat letölteni. (Például játékokat és más alkalmazásokat a Play Áruházból vagy az Appstore-ról.)

Egyéb az adott vállalatra érvényes szabályok: Minden vállalat maga írja elő a fent említett pontokkal szemben támasztott elvárásait. Ezek nagyban függenek a cég profiljától, és attól, hogy pontosan mivel is foglalkoznak. Ez azért fontos, mert a különböző ágazatokban más és más fenyegetettségek fordulhatnak elő. Ilyenek lehetnek például a know-how adatbázis védelme egy gyár esetében, vagy akár egy energiaszolgáltató vállalat komplex védelme, mely energiával látja el az egész országot.

A fentiek ismeretében már megfogalmazható egy a vállaltra szabott információbiztonság-tudatossági oktatás. Azonban az oktatás sikere nem csak a belső tartalmától függ, hanem az oktatás természetétől is. Ahhoz, hogy a legmegfelelőbbet válasszuk, ismernünk kell a lehetőségeinket, melyek a következők:

- Hagyományos, személyes oktatás
- E-learning kurzus
- Online oktatás (Microsoft Teams, Zoom stb.)
- Kampány
- Szabadulószoba
- Társasjáték

A **hagyományos, személyes oktatás** pozitívuma lehet, hogy van kapcsolat a résztvevők és az oktató közt. Azonban hátránya, hogy egy klasszikus frontális tanteremi (vagy tárgyalói) helyzet nem ösztönzi a munkatársakat az interakcióra. Ezáltal unalmassá válhat az oktatás, és így a résztvevők kevésbé figyelnek oda, sajátítják el a leadott anyag lényegét. Ez azért számít nagy hátránynak, mivel az információbiztonság-tudatossági tréningek egyik leglényegesebb része, hogy a megfelelő gondolkodásmódot sajátítsák el a munkavállalók, mellyel könnyebben eldönthetik, hogy az adott helyzetben szükséges-e támadásra gyanakodniuk.

Az **e-learning kurzus és az online oktatás** sok szempontból hasonlít egymásra. Pozitívumai, hogy nem szükséges a fizikai részvétel, így akár home officeból, vagy a pandémia miatt a megfelelő távolságtartással is elvégezhetőek ezek a kurzusok. Az e-learning kurzusok jó megoldást jelentenek akkor, ha csak általános ismétlő jellegű figyelemfelhívásra van szükség a munkatársak körében. Azonban hátránya lehet, hogy ezeket gyakran nem a kellő odafigyeléssel végzik el a kollégák, így az eredménye ilyen esetben ugyan az lehet, mint a személyes oktatásnak. Az online oktatásra is ugyan ez vonatkozik, azonban itt még az is nehezítheti a kollégák koncentrációját, hogy ha egy olyan előadáson vesznek részt, melyben nincs szükség arra, hogy kérdésekre válaszoljanak, interakcióba lépjenek egymással, könnyen elterelődik a figyelmük. Ez főleg abban az esetben igaz, ha home office-ból csatlakoznak be a hívásba.

A **biztonságtudatossági kampányok** célja, hogy az információbiztonság-tudatosság teljesen beépüljön a vállalati kultúrába. Ez azt jelenti, hogy minden alkalmazott automatikusan figyelembe veszi a biztonsági szempontokat minden döntésében és minden, a vállalat érdekében tett intézkedésében. Ahhoz, hogy ezt elérjék, az információbiztonságnak mindennapos témává kell válnia, amely gyakran foglalkoztatja a kollégákat. A kampányok egyszerre több csatornán is futtathatóak, így a leghatásosabb, ha a vállalat által használt belső „hírportálon" és a valóságban is minden nap találkoznak ezzel a témával a munkavállalók. Hátránya az, hogy nem fenntartható állandóan a figyelem, amit erre tudnak fordítani a munkavállalók. Például megszokják a kiplakátolt figyelemfelhívásokat és nem olvassák el őket egy idő után.

Abban, hogy a munkavállalók érdeklődését egy oktatás alatt fenntartsuk, sokat segíthet a **gamifikáció**. A gamifikáció, azaz „játékosítás" a játékszerű ösztönző elemek beépítését jelenti a mindennapi vagy nem játék jellegű tevékenységekbe. Bármikor, amikor játékszerű funkciókat vagy a játéktervezés szempontjait alkalmazzák nem játék jellegű kontextusban, játékosítás történik. Így nem csak élvezhető, de könnyebben tanulható is az elsajátításra szánt tananyag. Oroszi Eszter munkája során sokszor alkalmazza a gamifikációt különböző információbiztonság-tudatossági oktatások keretein belül. Erre példa lehet a szabadulószoba és a társasjáték. Ezekkel a technikákkal játékosan, unalom és „felesleges ismétlés" (mivel sajnos sok kolléga így tekint a kötelezően ismétlődő oktatásokra) nélkül a gyakorlatban tanulják meg és alkalmazzák a munkatársak az információbiztonsági szabályokat. A szabadulószoba és a társasjáték hatékony tud lenni, hiszen leköti és elgondolkodtatja a munkatársakat. Azonban hátránya lehet például, hogy a személyes oktatáshoz hasonlóan kevésbé rugalmas megoldás szervezési szempontból, valamint lehetséges, hogy ebben a formában nem lehet minden témát olyan alapossággal ismertetni, mint például egy jól megszervezett kampánysorozattal, vagy esetleg egy személyes oktatás során.

ÖSSZEFOGLALÁS

Tanulmányunkban bemutattuk, hogy mi az audit és milyen fontos a helyes auditálás, valamint az, hogy milyen nagy szerepe van az információbiztonsági auditoknak egy vállalat sikerében és biztonságában. Említést tettünk arról, milyen tulajdonságokkal rendelkezik egy jó auditor, és választ adtunk a kérdésre miért fontos, hogy a social engineering technikák részét képezzék az információbiztonsági auditoknak. A téma empirikus vizsgálatát egy esettanulmány segítségével és a kapott eredmények elemzésével végeztük el. A lezajlott adathalász kampány és a kutatás eredményeként, írásművünk végén ismertettük az információbiztonság-tudatosság fejlesztési eszközeit majd egy rövid javaslatot tettünk arra vonatkozóan, hogy mivel lehet még hatékonyabbá tenni a munkatársak oktatását az információbiztonsági-tudatossági tréningeken.

FELHASZNÁLT IRODALOM

[1] Molnár B. – Kő A. *Információrendszerek auditálása. Az informatika és az információrendszerek ellenőrzési és irányítási módszerei*. Budapest: Corvinno Technology Transfer Kft. 2009.
[2] Horváth Zs. L. *Információbiztonsági belső auditor* (jegyzet), 2016. megtekintve: 2022.07.28
[3] Ködmön I. *Hétpecsétes történetek: Információbiztonság az ISO 27001 tükrében*, 2008. megtekintve: 2022.09.15
[4] Kerti A. *Az audit tevékenységek előkészítése*, (belső oktatási anyag). megtekintve: 2022.05.25
[5] Baglyos S. *Az információbiztonsági auditálás fontossága* (https://www.ludovika.hu/blogok/cyberblog/2022/06/23/az-informaciobiztonsagi-auditalas-fontossaga). megtekintve: 2022.10.16
[6] Oroszi E. *Információbiztonsági stratégia és vezetés*. Budapest: Nemzeti Közszolgálati Egyetem. 2014.

[7] Michelberger P. – Lábodi Cs: *Vállalati információbiztonság szervezése*. Budapest: Óbudai Egyetem. 2012.
[8] Oroszi E. *Időutazás a Social Engineering auditok korában, avagy mi változott az elmúlt 10 év alatt?* (https://silentsignal.hu/docs/S2_ISACA_Konferencia_Oroszi_Eszter_20220616.pdf). megtekintve: 2022.10.12
[9] Oroszi E. *Biztonságtudatossági játékok, avagy a felhasználók információbiztonsági ismereteit fejlesztő módszerek hatékonyságának vizsgálata* (https://silentsignal.hu/docs/S2_ISACA_masodik_szerda_OE_20220112.pdf). megtekintve: 2022.10.12
[10] Oroszi E. – Bálint B: *Biztonságtudatossági szabaduló szoba, avagy a felhasználók biztonságtudatosságának új fejlesztési eszköze* (https://www.witsec.hu/sites/default/files/WITSEC2019/4_3_witsec_szabadulo_prezi_20191010.pdf). megtekintve: 2022.10.12
[11] Kollár Cs. *Hackerpszichológia*. Az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar „Kutatók éjszakája 2017" rendezvényen elhangzott előadás prezentációja. https://www.slideshare.net/drkollarcsaba/hackerpszichologia. megtekintve: 2022.10.15.

FELHASZNÁLT SZABVÁNYOK

[12] MSZ ISO/IEC 27001:2014

DIGITAL BUSINESS CONTINUITY ON MODERN DIGITAL EDUCATIONAL PLATFORMS AT OBUDA UNIVERSITY

ÜZLETMENET FOLYTONOSSÁG A KORSZERŰ DIGITÁLIS OKTATÁSI PLATFORMOKON AZ ÓBUDAI EGYETEMEN

CSERCSA Klaudia[1]

Abstract

During the outbreak of the coronavirus epidemic, a decision had to be made immediately to switch to a digital form of education. The unexpected situation in education presented a great challenge to all involved participants. The time has come for feedback, for the subsequent analysis of what happened and for determining a possible educational method for the future based on previous experiences. Within the framework of qualitative research methodology, the study examined the business continuity of BigBlueButton, a digital educational platform, using expert interviews. The study also assessed the opinions of university students within the framework of quantitative research methodology. The study seeks an answer to what is the most preferred teaching method by students in the future, online vs. in terms of personal education.

Keywords

business continuity, BigBlueButton, online education, Obudai University, Covid

Absztrakt

A koronavírus járvány berobbanása idején azonnal kellett döntést hozni a digitális oktatási formára való átállásra. A nem várt helyzet az oktatásban minden érintett részvevőt nagy kihívás elé állított. Elérkezett az idő a visszacsatolásra, a történtek utólagos elemzésére és a jövő egy lehetséges oktatási metódusának meghatározására a korábbi tapasztalatok alapján. A tanulmány kvalitatív kutatási módszertan keretein belül, szakértői interjú alkalmazásával egy digitális oktatási platformnak a BigBlueButton-nak az üzletmenet folytonosságát vizsgálta. A tanulmány kvantitatív kutatási módszertan keretein belül egyetemi hallgatók véleményét is felmérte. A tanulmány választ keres arra, hogy mi a jövőben a hallgatók által leginkább preferált oktatási metódus online vs. személyes oktatás tekintetében.

Kulcsszavak

üzletmenet folytonosság, BigBlueButton, online oktatás, Óbudai Egyetem, Covid

[1] csercsa.klaudia@phd.uni-obuda.hu | ORCID: 0000-0003-2800-9106 | PhD student, Óbuda University Doctoral School for Safety and Security Sciences| doktorandusz hallgató, Óbudai Egyetem Biztonságtudományi Doktori Iskola

BEVEZETÉS

A digitalizáció megváltoztatja világunkat. A negyedik ipari forradalom gyors technológiai fejlődésének hatásai óriási kihívások elé állítják a társadalmat és a politikai döntéshozókat. [1] Ezek a kihívások hatványozottan jelentek meg az oktatás világában a pandémia idején, ahol nagyon gyors, radikális változásokat kellett érvénybe léptetni az oktatás és az egészségvédelem közös meglétének érdekében. Az egészségügyi krízis lezajlott és az online jelenlét előnyeit kellene megtartani a személyes jelenlétet kívánó oktatási formával vegyítve, mindkettőnek az erősségeit szem előtt tartva. Jelen kutatásban egyetemi hallgatók véleménye alapján felmérést készítettem a korszerű digitális platformokon történt online oktatás és hagyományos tantermi kereteken belül zajló oktatással kapcsolatos véleményekről, tapasztalatokról. Hallgatói oldalról mutatkozik-e igény az online oktatási formára és ha igen milyen módon, mekkora arányban a hagyományos tantermi oktatáshoz képest. A hallgatói vélemények megismerése mellett kvalitatív módszertan segítségével szakértők véleményét vizsgáltam az online oktatás üzletmenet folytonosságának vetületében. Szakértői mélyinterjú keretében a BigBlueButton rendszer üzemeltetőjét kérdeztem ennek az online oktatási platformnak a bevezetésével, használatával, üzletmenet folytonosságával kapcsolatos kérdésekben. A téma teljesebb körű megismerése érdekében egyéni interjúkat készítettem egyetemi oktatókkal, akik a BigBlueButton rendszer bevezetésekor aktív oktatói tevékenységet folytattak és személyes tapasztalatokkal rendelkeznek ennek kapcsán. Szekunder adatgyűjtés során a témában releváns kutatók eredményei kerültek ismertetésre, a témához kapcsolódó alapfogalmak és definíciók ismertetésével mind nemzetközi, mind hazai tekintetben.

ÜZLETMENET FOLYTONOSSÁG

Az információs társadalom rohamos térnyerése és a mögötte lévő exponenciális technológiai fejlődésnek az eredményeként a kibertér műveleteinek jelentős a felérékelődése. [2] Az üzletmenet-folytonosság célja, hogy nem várt események hatása alatt is lehessen fenntartani a szervezet működőképességét. Fel kell készülni az esetleges vészhelyzetekre, csökkenteni kell a kockázatokat és törekedni kell a mielőbbi visszaállításra és a zavar elkerülésére. „Az üzletmenet folytonosság esetében a szervezet folyamatai zavartalanul és hibamentesen működnek és az azokhoz szükséges erőforrások megfelelő helyen és időben rendelkezésre állnak. A szervezetek elsősorban információbiztonsági vonatkozásban használják a fogalmat.” [3]

Az üzletmenet folytonosságra vonatkozó szabvány az ISO 22301:2019, mely tartalmazza a Magyarországon érvényes szabványokat a társadalmi biztonság, üzletmenetfolytonossági irányítási rendszerek, követelmények tekintetében. [4]

Az online oktatási platformok tekintetében oktatói oldalról megközelítve az üzletmenet folytonosságot, az online órát zökkenőmentesen, zavartalanul és technikai hibák, illetve malőrök nélkül tudja az oktató megtartani a virtuális térben. Ehhez bizonyos feltételeknek a megléte elengedhetetlen. A megfelelő műszaki tudással rendelkező személyi számítógép megléte, stabil internetkapcsolat, esetlegesen használandó szoftverek licencei és az oktatók megfelelő felkészültsége nem csak a szaktantárgyuk, hanem informatikai tudásuk tekintetében is. Ha ezek mind adottak és megfelelő időben rendelkezésre állnak akkor van

az oktatónak lehetősége egy minőségileg biztosított online órát tartani és az üzletmenet folytonosságot biztosítottnak tekinteni.

Napjainkban egyre nagyobb hangsúlyt kap az üzletmenet-folytonosság (Business Continuity), mely egy átfogóbb és az összes működési feltételnek a folyamatos biztosítására koncentrál a hagyományos IT-központú katasztrófavédelemmel (Disaster Recovery) szemben. [5]

Az üzletmenet folytonosság biztosítása során olyan kritikus folyamatoknak a leállására készül fel egy szervezet, amely nélkül mondhatni megállna az élet. Első lépésként fel kell deríteni, hogy mik a kritikus erőforrások, illetve folyamatok, majd a továbbiakban a rendszert folyamatosan tesztelni és karbantartani szükséges. [6]

Ez a gyakorlatban nagyon sok dokumentációval jár és sok erőforrást igényel a szervezettől, ezen okból kifolyóan gyakran nem is veszik kellőképpen komolyan az üzletmenet-folytonosság biztosítását. Legtöbbször csak egy megfelelőségi követelményként tekintenek rá és nem gyakorlatban is alkalmazható tervként. Ez esetben, ha nem várt esemény következik be, mindenki kapkod és senki sem tudja, mi a teendője. Éppen ezért fontos a jól kipróbált eljárás, hogy vészhelyzet esetén az improvizálást elkerülje a szervezet. Tudatos tervezésnél mindenki tudja, hogy mit kell csinálni. A terveket muszáj folyamatosan karbantartani és aktualizálni, sőt tesztelni is. Fontos, hogy megtörténjen a felelősök meghatározása és mindenki tudja, hogy szükség esetén mi a feladata. Legyen egy úgymond parancsnoki lánc, amely segít a nemkívánatos események megtörténtekor higgadtan kezelni a helyzetet, a felelősök irányításának segítségével. Fontos tisztában lenni a felszabadítható erőforrásokkal, amikre támaszkodhat a szervezet szükség esetén. A bajt mindig jobb megelőzni, mint kezelni, de ha megtörténik akkor tudjuk megtenni a szükséges lépéseket higgadtan és amennyire csak lehetséges felkészülten. [7]

Az üzletmenet-folytonosság tervezés alapvető céljai az alábbiak:

- Erőforrás kiesés esetén a kritikus üzleti folyamatok az előre meghatározott szinten működni tudjanak
- A kritikus üzleti folyamatok kieséséhez tartozó kockázatok, károk csökkentése
- Egy esetleges kiesés esetén a legkisebb veszteség mellett, költségek szempontjából a leghatékonyabb megoldás alkalmazása

Kapcsolódó rendelkezések, szabványok, ajánlások:

- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról és végrehajtási rendelete (41/2015. (VII.15.) BM rendelet
- 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
- A Magyar Nemzeti Bank 7/2017. (VII.5.) számú ajánlása az informatikai rendszer védelméről
- ISO 27001 szabvány
- ISO 22301 szabvány

[8]

KORSZERŰ DIGITÁLIS OKTATÁSI PLATFORMOK

A pandémia miatt szinte egyik napról a másikra kellett átállni a teljesen digitális felületen történő oktatásra. Ez rendkívül megterhelő volt hallgatóknak és oktatóknak egyaránt. Azokban a kutatásokban, melyek a pandémia idején mérték fel a hallgatók véleményét, egyértelműen tükröződött a hosszú elszigetelődés hatása és vélhetően emiatt születhettek olyan kutatási eredmények, hogy a hallgatók döntő többsége nagy mértékben elutasítja a digitális oktatást. [9]

Napjainkra már nem jellemző a hallgatók ilyen irányú elutasítása az online térben történő oktatásnak. Az viszont egyértelműen kirajzolódott, hogy a kizárólag digitális oktatás nem kívánatos. Ugyanakkor az online tanulási formának számos előnye van, amennyiben megfelelő körültekintéssel és felkészültséggel alkalmazzák, és bizonyos tantárgyakra korlátozzák használatát. A hibrid rendszerű munkavégzésre való átállás legfeljebb kezdetben okozott problémát. [10]

Több egyetemen is végeztek kutatást a digitális formában zajló oktatásról a zavartalan folytonosságot és minőséget szem előtt tartva. [11] [12] [13] [14] [15]. A kutatások végső eredményeként elmondhatjuk, hogy nincs egy egzakt digitális oktatási metódus. Minden tantárgy, oktató és egyetem a saját profiljához leginkább illeszkedőt alkalmazza az oktatási tevékenységük során.

Elsősorban nem a technikai nehézségek váltottak ki egyfajta ellenérzést a hallgatókban, hanem a személyes kapcsolatok elcsökevényesedése. A korábbi tapasztalatokra alapozva kellene felépíteni egy gyakorlati alkalmazásra megfelelő metodikát, mely támpontot nyújthatna az oktatóknak a hibrid oktatás hatékony működéséhez.

EREDMÉNYEK

A kvalitatív és a kvantitatív kutatási eredmények külön alfejezetekben kerülnek ismertetésre.

Kvalitatív kutatás, szakértői mélyinterjú eredménye

Kvalitatív kutatás keretében készítettem szakértői mélyinterjút a BigBlueButton rendszer egyik üzemeltetőjével. A kutatásban való részvétel önkéntes alapon történt, online felületen, félig strukturált interjúvázlat segítségével. Az interjú körülbelül 50 percet vett igénybe.

Az interjúalany elmondása alapján, a BigBlueButton egy nyílt forráskódú webkonferencia-rendszer, amelyet online tanulásra terveztek. Ez egy szabad felhasználású program és amikor egyik napról a másikra kellett digitális oktatásra váltani, ezt a programot preferálták kezdetben az Óbudai Egyetemen. Nem voltak korábbi tapasztalatok a BBB használatával kapcsolatban, ahogyan más oktatási platformokkal kapcsolatban sem. A koronavírus világjárvány berobbanását követően azonnal kellett cselekedni a digitális oktatásra való átállásban az országban mindenhol. Ekkora felhasználói igényre a szolgáltatók és a platformok sem voltak felkészülve. Ez nagyban befolyásolta az üzletmenet folytonosságot. Gyakoriak voltak a működési hibák. Az egyszerre 100-200 fős leterheltséget, ami az Óbudai Egyetemen egy előadással járt, nem tudta kezelni a rendszer. Igyekeztek a működési feltételek optimális megteremtését biztosítani és a hatékonyabbá tenni. Vettek egy több processzoros szerver gépet is, hogy a lassú és akadályoztatott működést problémamentessé tegyék.

Az idő múlásával egyre több frissítés érkezett a BBB-hoz és a felülete egyre inkább felhasználóbaráttá vált. A folyamatbiztonság zökkenőmentes biztosítása érdekében a rendszerbe való belépés során 3 szintű felhasználó csoport kerül megkülönböztetésre, különböző jogkörök biztosításával. Az alapjogokat biztosító felhasználó csoport a user. Ezt a jogot kapják a hallgatók amikor belépnek és órán vesznek részt. A manageri vagy középkategóriás jogokat biztosító szinten a jogosult belenézhet a felhasználók listáiba és felvételeibe, azokat le tudja játszani, de szerkesztési, törlési joggal nem rendelkezik. Ő a moderátor, aki megnyitja a szobát, le tudja némítani a kurzuson résztvevőket, akár el is távolíthat a kurzusról résztvevőket. Ilyen hozzáférési jogot kapnak az oktatók. A legmagasabb jogot az adminisztrátor kap. Ő telepíti a programot, frissíti, karbantartja. Ő a rendszergazda. Bele tud nyúlni az adatbázisokba, felhasználót törölhet, jogokat adhat, bármikor beléphet az előadások vagy órák során. A folyamatbiztonság vizsgálata szempontjából további releváns információ, hogy a BBB korábbi verziója nem volt kompatibilis, illetve átjárható a különböző oktatási félévek feltöltött anyagai tekintetében. Az oktató elkészítette egy adott oktatási félévre a digitális tartalmakat és azokat nem tudta újra felhasználni a következő félévben. Ez fölösleges plusz terhet jelentett az oktatóknak. A frissítések során már megoldódott ez a probléma.

Az interjúalany a vizsgálat során nagyon együttműködő volt és hasznos információkat osztott meg. Szuverén véleménye szerint a jövőben hasznos lenne megtartani a digitális oktatás előnyeit is, és hibrid oktatási tevékenységet folytatni. A rendszer zavartalan működésének biztosításához az Óbudai Egyetem biztosított egy több processzoros szervergépet, hiszen a hirtelen bekövetkezett felhasználói igényre nem voltak kezdetben felkészülve és gyakran előfordultak működési hibák az üzletmenet folytonosságban. A digitális oktatásra jelentkező igény fellépésekor azonnal kiképeztek az egyetemen egy rendszergazdát, aki kézben tartotta a rendszer üzemeltetését és kezelte az esetlegesen jelentkező problémákat. Folyamatos rendszerfrissítésekkel egyre inkább felhasználóbarát platformot alakítottak ki, hogy az oktatókat tehermentesíteni tudják. A feltöltött tananyagot a különböző félévekben már át tudja emelni az oktató és nem kell újra kezdeni az egész folyamatot, minden tanítási félév elején. Az üzembiztonság megfelelő biztosításához különböző jogosultsággal ruházták fel a felhasználókat. A kezdeti nehézségek után a BigBlueButton rendszer már zavartalanul működik és biztosított a zavartalan üzemeltetés az Óbudai Egyetemen. A teljes bezártság eltörlésével és a kizárólag digitális formában történő oktatás kényszerének enyhítésével a rendszer terheltsége is jelentős mértékben csökkent, lényegesen kisebb igénybevételnek van kitéve.

Kvalitatív kutatás, oktatói interjúk eredménye

Négy oktató véleményét ismertetem összegezve, akik aktív oktatói tevékenységet folytattak az Óbudai Egyetemen a pandémia idején, amikor teljes digitális oktatási forma bevezetése történt. Mind a négy interjúalany egyetértett abban, hogy a digitális oktatási formának vannak előnyei, ezek közé sorolták például az időmegtakarítást, ami az utazás hiányából fakad, az egészségük védelmét és a kényelmet. A diploma és szakdolgozatot készítő hallgatókkal rugalmasabban lehetett időpontot egyeztetni digitális keretek között. Kezdetben mindegyik oktatónak kihívást jelentett a digitális oktatásra való átállás és a BigBlueButton rendszer hiányosságai mindegyik oktatónál nehézségeket okozott. Nem érezték kom-

fortosnak a rendszer használatát és nem is használták a továbbiakban a BBB-t. Az megosztotta a négy interjúalany véleményét, hogy kezdetben nem volt egy egységesen használandó platform az oktatási tevékenységhez. Volt, aki úgy érezte, hogy nagyobb szabadságot nyújt, hogy használhatja, amit már valamennyire ismert korábbról és volt, akit elbizonytalanított. Mindannyian fárasztóbbnak és mentálisan megterhelőbbnek élték meg a kizárólag digitális formában történő oktatást. Az egyik interjúalanynak három gyermeke tanult otthonról és a házastársa is oktató, így komoly nehézséget okozott, hogy mindenkinek legyen saját eszköze és a lakáson belül az egymástól megfelelően elkülönített tér, hogy ne zavarják egymás óráit. A négy interjúalany közös véleménye továbbá, hogy nem tartanák üdvözítő megoldásnak, ha a jövőben kizárólag digitális formában történne az oktatás. A megfelelő műszaki feltételek megteremtésével egy hibrid oktatási formát tartanának a legmegfelelőbbnek, hiszen számos előnye van a digitális oktatásnak, amit feltétlenül célszerű lenne megtartani.

KVANTITAÍV KUTATÁS

Kvantitatív kutatás keretén belül készítettem kutatást egyetemi hallgatók körében sztenderdizált kérdőív segítségével. A kitöltés teljesen anonim volt és önkéntes alapon történt. A kérdőívet összesen 215 fő töltötte ki hólabda mintavételi eljárással. A kérdőív egy szűrőkérdéssel kezdődött annak érdekében, hogy a kizárólag online oktatási formában tantárgyat teljesítő hallgatók véleményét tudjam értékelni. Adattisztítást követően összesen 186 fő válasza bizonyult értékelhetőnek. Pearson-féle korrelációs együttható vizsgálatával végeztem adatelemzést a kapott válaszok alapján.

Hallgatók véleménye a digitális oktatásról 2022-ben

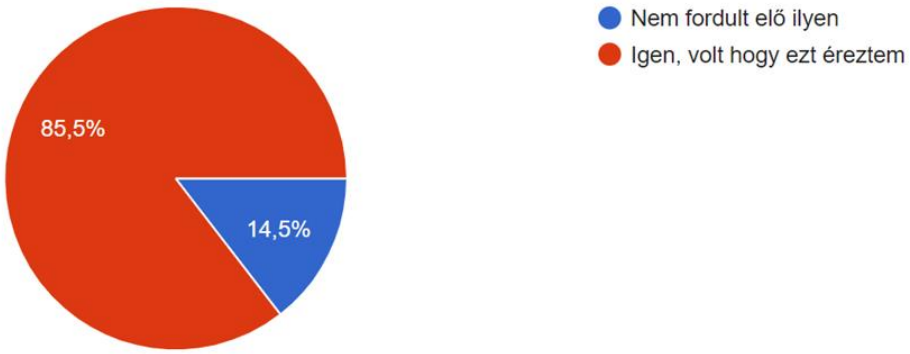
Az első ábrán a hallgatók véleményét látjuk annak tekintetében, hogy inkább az online, vagy a személyes esetleg egy hibrid oktatási módot preferálják-e leginkább.

1. Ábra: Hallgatók online és személyes jelenléti oktatással kapcsolatos véleménye, saját szerkesztés, saját kutatás alapján, 2022, N=186.

A kérdőívet kitöltő hallgatók közel 76%-a tartaná a legelőnyösebbnek, ha a személyes jelenlétet kívánó és az online módon történő oktatás is jelen lenne olyan tárgyaknál, ahol az megoldható.

Ez arra enged következtetni, hogy nagy mértékben csökkent a hallgatóknak az ellenállása az online oktatással szemben, amely a pandémia idején volt tapasztalható.

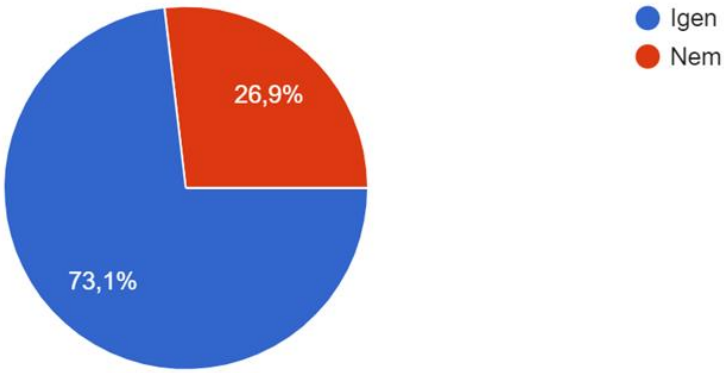
A második ábra azt szemlélteti, hogy a kitöltőknek hiányoztak-e a személyes kontaktuson alapuló találkozások a kizárólag online oktatás idején.



2. Ábra: Hiányoztak-e a személyes találkozások a kizárólag online oktatási formában? saját szerkesztés, saját kutatás alapján, 2022, N=186

A 186 kitöltőnek közel 86%-a érezte azt a pandémia idején, hogy hiányoznak számára a személyes emberi kapcsolatok. Ez a szignifikáns különbség arra enged következtetni, hogy a kizárólag online oktatás nem lenne ideális megoldás. A fiataloknak szükségük van társas kooperációra.

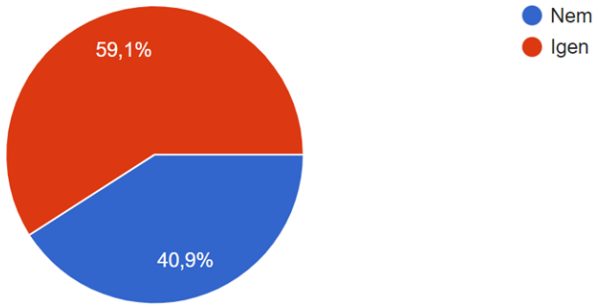
A harmadik ábra azt szemlélteti, hogy társas kapcsolataik tekintetében érezték-e azt valaha is a kitöltők, hogy hátrányos számukra a kizárólag online oktatási forma.



3. Ábra: Társasági élet tekintetében hátrányosnak érzi a kizárólag online oktatási formát, saját szerkesztés, saját kutatás alapján, 2022, N=186.

A válaszok itt is egyöntetűen azt támasztják alá, hogy a hallgatók hátrányosnak érezték a pandémia idején a teljes bezártság alatt a társas kapcsolataik hiányát. Az online oktatásnak számos előnye van, de a kizárólag digitális oktatási formának komoly hátrányai vannak szociális jólétünk tekintetében.

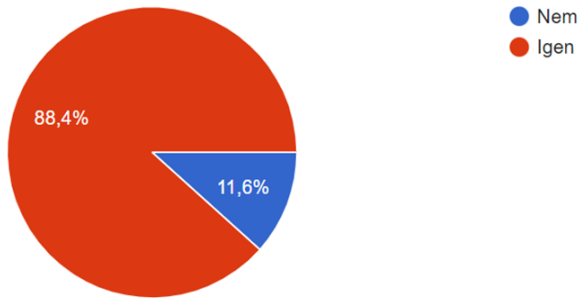
A negyedi ábrán már nincs szignifikáns eltérés a válaszok eredményei között. A következő ábra azt illusztrálja, hogy hiányozna-e a kitöltőknek a digitális oktatás a jövőben.



4. Ábra: Hiányozna a digitális oktatás, saját szerkesztés, saját kutatás alapján, 2022, N=215

A kitöltők 59%-ának hiányozna a digitális oktatási forma, ha ezután már kizárólag személyes részvétellel lehetne tanulni. Az online oktatási formát hiányolná a hallgatók többsége.

Az ötödik ábrán az előző kérdésnek az inverzére adott válaszokat látjuk. Vagyis, hogy a személyes találkozások hiányoznának-e a kitöltőknek.



5. Ábra: Hiányoznának a személyes találkozások kizárólag digitális oktatás esetén, saját szerkesztés, saját kutatás alapján, 2022, N=215

A kitöltők több, mint 88%-ának hiányoznának a személyes találkozások, ha újra kizárólag digitális oktatási formában tanulnának. A két kérdés párhuzamos vizsgálata a kizárólag digitális oktatás a kitöltők 59%-ának hiányozna, míg a személyes találkozások a kitöltők 88%-ának. Ez arra enged következtetni, hogy a hagyományos oktatás megléte, a jövőben kívánatos jelenség és a fiatal egyetemistáknak szüksége van a társaik jelenlétére az egyetemi órák alatt, ugyanakkor a digitális oktatás által nyújtotta előnyöket is szeretnék élvezni.
A Pearson-féle korreláció elemzés során 2 vizsgáltnál jelentkezett szignifikáns érték. A 22. és a 24. kérdés vizsgálata során a Pearson-féle korreláció eredménye 0,87 értéket mutatott. A két vizsgálandó kérdés: Melyik oktatási formát preferálja és a társasági élet szempontjából okozott-e hátrányt az online oktatás. A korreláció erős, vagyis akik az online oktatást preferálják, azoknak az online oktatás nem okozott társadalmi szempontból hátrányt. Illetve a 24. és 25. kérdésnél a Pearson-féle korreláció eredménye 0,82 lett. A két vizsgálandó kérdés: A társasági élet szempontjából okozott-e hátrányt az online oktatás és hiányoznának-e

a személyes találkozások. A kapcsolat erős, vagyis akik társadalmi szempontból aktívak voltak, azoknak nem okozott hátrányt az online oktatás.

ÖSSZEGZÉS, KONKLÚZIÓ

Az üzletmenet folytonosság biztosítása az oktatási platformokon kezdetben komoly kihívások elé állította az üzemeltetőket is és ez hatással volt a felhasználókra, hallgatókra és oktatókra egyaránt. A koronavírus járvány hatására, azonnali intézkedésként beállt online oktatás felkészületlenül ért minden érintett részvevőt. Egy kevésbé extrém körülmények között történő digitális oktatás bevezetése valószínűleg csökkentette volna a kezdeti nehézségek számát, könnyebb lett volna a digitális oktatási alkalmazások használata, megszokása, viszont a folyamat nem lett volna ennyire turbulens. A rendkívüli állapot megszűnésével csökkent az extrém nagy leterheltsége a különböző digitális oktatási platformoknak. A kezdeti nehézségek után egyre inkább üzembiztosan működtek a különböző online oktatási programok. Az üzletmenet folytonosság biztosítása egyre hatékonyabban működött és a felhasználói felületek is egyre inkább felhasználóbaráttá váltak. Az oktatók és a hallgatók egyre jobban tudták zökkenőmentesen használni ezeket a felületeket. A személyes kontaktuson alapuló szociális kapcsolatok korlátozásának elmúlásával a hallgatók egyre inkább értékelik az online oktatás nyújtotta előnyöket és kényelmet. Az egyetemi hallgatók és oktatók, illetve a digitális oktatási platformokat üzemeltető rendszergazdák egyöntetű véleménye alapján a jövőben leginkább egy hibrid oktatási formát lenne célszerű alkalmazni, ahol meg lehet tartani a digitális és a személyes oktatás előnyeit is. Ennek mikéntjét egy további, célzottan erre fókuszáló tanulmány keretein belül lehetne további vizsgálat tárgyává tenni.

FELHASZNÁLT IRODALOM

[1] Rajnai Zoltán and I. Kocsis, "Labor market risks of industry 4.0, digitization, robots and AI," 2017 IEEE 15th International Symposium on Intelligent Systems and Informatics (SISY), 2017, pp. 000343-000346, doi: 10.1109/SISY.2017.8080580
[2] Kralovánszky Kristóf, 2021, A kibertér fejlődése – Kiberműveletek és kritikus infrastruktúrák egyes kapcsolatai, Hadmérnök, 16. évfolyam, 1. szám pp. 145-160
[3] Michelberger Pál, Információ-, folyamat- és vállalatbiztonság, 2022, 131 p., ÓE KGK, Budapest ISBN: 9789634492894
[4] MSZ EN ISO 22301:2020 Társadalmi biztonság. Üzletmenet-folytonossági irányítási rendszerek
[5] Godányi Géza, Katasztrófavédelem és üzletmenet-folytonosság az információtechnológiában (A DR/BC tervezés alapjai). Híradástechnika, LIX évf. 2004/4. pp. 47-52
[6] Haig Zsolt, 2018, Információs műveletek a kibertérben, Dialog Campus Kiadó, Budapest
[7] Krasznai Csaba, Kiberbiztonság a negyedik ipari forradalom korában, 2019, Híradástechnika: Hírközlés-informatika LXXIV: 1 pp. 25-29. Paper: 6, 5 p.
[8] njt.hu https://njt.hu/jogszabaly/2013-50-00-00.0 letöltés: 2022.04
[9] Viktor Patrik, Kárpáti-Daróczi Judit, 2020, Innovatív e-learning rendszerek elemzése, Óbudai Egyetem 51. Tudományos Diákköri Konferenciakötet pp. 82-82, 1p

[10] Tóth István Márk, Csiszárik-Kocsir Ágnes, 2021, A koronavírus világjárvány agilis projektmenedzsmentre gyakorolt hatásának vizsgálata, Vállalkozásfejlesztés a XXI. században 2021/1. kötet: Óbudai Egyetem KGK 209 p. pp.170-184., 15 p
[11] Hargitai Dávid Máté - Sasné Grósz Annamária - Veres Zoltán (2020) Hagyományos és online tanulási preferenciák a felsőoktatásban – A COVID-járvány kihívásai. Statisztikai Szemle, 98 (7). pp. 839-857. ISSN 0039-0690
[12] Sipos Norbert–Jarjabka Ákos–Kuráth Gabriella–Venczel-Szakó Tímea: Felsőoktatás a COVID-19 szorításában: 10 nap alatt 10 év? Gyorsjelentés a digitális átállás hatásairól a munkavégzésben a Pécsi Tudományegyetemen. Civil Szemle, Oktatás, Digitalizáció, Civil Társadalom. Különszám 2020.pp. 73-92. ISSN 1786-3341
[13] Kálmán Botond-Tóth Arnold: A COVID-19 hatása a felsőoktatásr oktatói vélemények kérdőíves felmérése alapján. 12th International Conference of J. Selye University, Economics Section. https://doi.org/10.36007/3754.2020.209 p.17
[14] Rajcsányi-Molnár Mónika - Bacsa-Bán Anetta: Úton a digitalizáció felé - egy felsőoktatási intézmény digitális oktatásának hallgatói tapasztalatai (2021) (Towards Digitalisation - Student Experiences in Online Education at a Higher Education Institution.) Journal of Applied Technical and Educational Sciences, 11(1), pp. 88-110. https://doi.org/10.24368/jates.v11i1.245
[15] Buda András - Szabó József - Erdei Gábor: A pandémiás helyzet hatása az oktatásra a Debreceni Egyetemen. Opus et Educatio 7. évfolyam 4. szám (2020) pp. 423-431. ISSN: 2064-9908

THE POTENTIAL USE OF PASSENGER CAR DATA TRAFFIC FOR RECONNAISSANCE PURPOSES

SZEMÉLYGÉPJÁRMŰVEK ADATFORGALMÁNAK MEGFIGYELÉSI CÉLÚ FELHASZNÁLÁSI LEHETŐSÉGEI

HEGYI Henrietta[1] – ERDŐDI László[2]

Abstract

As a by-product of the fourth industrial revolution, smart devices are also gaining ground in the home. As well as simple IoT devices, advanced passenger vehicles can be considered as such smart devices. As network communication functions become commonplace in vehicles, the opportunities for targeting them are also expanding. This paper will briefly describe the infocommunication systems of vehicles, illustrate through case studies its vulnerabilities and some of the ways in which the data can be exploited, and then attempt to sketch a situation that adequately exemplifies the possible consequences by means of a theoretical scenario.

Keywords

IoT, passenger vehicle, information security, botnet, reconnaissance

Absztrakt

A negyedik ipari forradalom egyik mellékhatásaként az okoseszközök egyre nagyobb teret nyernek a lakossági felhasználás terén is. Az egyszerű IoT eszközök mellett a fejlett személygépjárművek is ilyen okoseszközöknek tekinthetők. Ahogyan a járművek esetén a hálózati kommunikációs funkciók mindennapossá válnak, az őket célzó támadási lehetőségek is kiszélesednek. Jelen tanulmány röviden bemutatja a járművek infokommunikációs rendszereit, esettanulmányokon keresztül szemlélteti annak sérülékenységeit, illetve az adatok felhasználásának néhány módját, majd kísérletet tesz rá, hogy egy elméleti szituáció segítségével felvázoljon egy olyan szituációt, mely megfelelően példázza a lehetséges következményeket.

Kulcsszavak

IoT, személygépjármű, információbiztonság, botnet, megfigyelés

[1] hegyi.henrietta@uni-obuda.hu | ORCID: 0000-0002-7731-840X | Doctoratal Student, Bánki Donát Faculty of Mechanical and Safety Engineering, Óbuda University | Doktorandusz, ÓE Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, Óbudai Egyetem

[2] erdodi.laszlo@nik.uni-obuda.hu | ORCID: 0000-0002-4910-4228 | Senior Lecturer, John von Neumann Faculty of Informatics, Óbuda University | Adjunktus, Neumann János Informatikai Kar, Óbudai Egyetem

IOT ESZKÖZÖK ELTERJEDÉSE ÉS ADATGYŰJTÉSI TENDENCIÁK

A 4. ipari forradalom folyományaként az egész világon egyre elterjedtebbé válnak az okoseszközök. A negyedik ipari forradalom kifejezés Klaus Schwab nevéhez köthető, aki így foglalta össze:

„Mint ahogy az első ipari forradalom gőzzel működtetett gyárai, a másodiknál a tömeggyártás tudományának alkalmazása, továbbá a harmadik ipari forradalom során a digitalizáció elkezdése, addig a negyedik ipari forradalom olyan technológiái, mint a mesterséges intelligencia, a genomszerkesztés, a kiterjesztett valóság, a robotika és a 3D nyomtatás, gyorsan megváltoztatják azokat a folyamatokat és módszereket, ahogy az emberiség az értékeket létrehozza, cseréli és elosztja. Ahogy az az előző forradalmak során is történt, ez a változás is mélyen átalakítja az intézményeket, iparágakat és a magánszemélyeket is. Ennél is fontosabb azt észrevenni, hogy ezt a forradalmat az emberek ma meghozott döntései vezérlik. A világ 50–100 év múlva nagymértékben függ majd attól, hogy hogyan gondolkodunk ma ezekről a befektetésekről, és hogyan vezetjük be ezeket a nagy teljesítményű új technológiákat."

A negyedik ipari forradalom magával hozta az olyan újításokat is, amik mindannyiunk életét meghatározzák: az okostelefonok által irányítható okos lakberendezési tárgyakon át az okosórákig. Ahogyan Krasznay Csaba rámutat [1], akár már egy egyszerű kábel is tartalmazhat mikroprocesszorokat, melyekről nem feltétlenül tudjuk, hogy konkrétan milyen adatforgalmat bonyolítanak. A „digitális társadalom" létéhez ma már elengedhetetlenül hozzátartozik az, hogy egyre több internetre csatlakozó eszközzel vesszük körül magunkat. [1] Az IoT-eszközökkel, rendszerekkel és szolgáltatásokkal kapcsolatos veszélyek és kockázatok sokrétűek, és gyorsan fejlődnek, ráadásul rendkívül széles területet ölelnek fel. Ezért fontos megérteni, hogy pontosan milyen elméleti keretekkel, szabályozási környezettel lehetséges az ilyen eszközöket biztosítani és milyen operatív intézkedéseket kell kidolgozni, amelyek segítenek megvédeni őket a különböző fenyegetésektől. Ahogyan ezt az Európai Uniós Kiberbiztonsági Ügynökség, az ENISA is kiemeli, az IoT eszközök esetében éppen a komplexitás miatt jelent kihívást. [2]

Az egyre több tiszta, szenzorok általi adatot gyűjtő okoseszköz elterjedésével párhuzamosan a XXI. században kibontakozó másik fontos tendencia az egyes állami és nemállami szervezetek egyre nagyobb mértékű adatgyűjtési folyamatai. Világszinten az Egyesült Államok ellen indított 2001. szeptember 11-i terrortámadás jelentett olyan fordulópontot, melynek köszönhetően a kibertérből származó információk szerepe felértékelődött. Miután a globális szempontból is sokkoló terrortámadás körülményeit sikerült tisztázni, az Egyesült Államok lassan megkezdte a tömeges adatgyűjtési programjának elindítását, amelyről az Edward Snowden által nyilvánosságra hozott adatokból értesült a világ. Snowden és más, kevésbé ismert aktivisták és hackerek csoportjai rámutattak az átfogó programmal kapcsolatos szabályozási hiányosságokra. [3], [4]

2017-ben a CIA által kiszivárgott hacker eszközökről készült egy „Vault 7" nevű, a Wikileaks dokumentum. A leírás rávilágított, hogy a szervezet aktívan keresi a sebezhetőségeket olyan okoseszközökben, mint például az okostelefonok, okostelevíziók, vagy éppen a személygépjárművek. [1], [5]

PÉLDA AZ IOT ESZKÖZÖKKEL VALÓ VISSZAÉLÉSRE: A MIRAI BOTNET BEMUTATÁSA

Annak ellenére, hogy az IoT eszközök nem tekinthetnek vissza hosszú múltra, a több kompromittált eszközből álló hálózatok, melyeket szinkronizált támadásokhoz használnak, már ma sem számítanak újdonságnak. Az elsősorban beágyazott és IoT-eszközökből, főként webkamerákból álló Mirai botnet 2016 végén jelent meg az interneten, amikor több nagynevű célpontot hatalmas elosztott szolgáltatásmegtagadási (DDoS) támadásokkal sújtott.

M. Antonakakis et al. [6] *„Understanding the mirai botnet”* című tanulmányban hét hónapos visszatekintő elemzésben mutatja be a Mirai 600 ezer fertőzött eszköz csúcsra történő növekedéséről szóló, és a DDoS áldozatainak történetét. A 2016 szeptemberétől kezdődően tömeges elosztott szolgáltatásmegtagadási (DDoS) támadások sorozata ideiglenesen megbénította a Krebs on Security [7], az OVH[3] és a Dyn [6] működését. A Krebs elleni kezdeti támadás volumene meghaladta a 600 Gbps-ot [7] - ez az eddigi legnagyobbak közé tartozik. Figyelemreméltó, hogy ez az elsöprő forgalom az internet néhány százezer, az összes lehetséges host közül a legkevésbé „erősekről” – IoT eszközökről - származott, amelyek a Mirai nevű új botnet irányítása alatt álltak. A kutatók megállapították, hogy a botnet az első 20 órában közel 65 000 IoT-eszközt fertőzött meg, mielőtt elérte volna a 200 000-300 000 fertőzéssel járó stabil állapotot. [6] Ezek a botok a földrajzi régiók és autonóm rendszerek egy szűk sávjába estek, Brazília, Kolumbia és Vietnám aránytalanul nagy arányban jelentek meg a fertőzések forrásának helyszíneként, 41,5%-ot téve ki az összes lokációból.

A Mirai működése a következőképpen foglalható össze: a command and control szerver két socket listenert futtatott: egyet a Telnet-kapcsolatokhoz, egyet pedig egy programozott API-hoz. A Telnet socket a 23-as portot figyelte, és minden érvényes kapcsolatot a megfelelő bot vagy admin kezelőhöz irányított. Az API socket a 101-es portot figyelte, és a hozzá küldött érvényes támadási parancsokat továbbította a csatlakoztatott botokhoz. Továbbá, minden egyes csatlakoztatott bot új sebezhető eszközök után kutatott az interneten. Amint felfedeztek egyet, a hitelesítő adatait, IP-címét, és a hozzáféréshez használt portot elküldték a loader szervernek. Ez lehetővé tette az adatok fájlban történő eltárolását, majd rosszindulatú szoftver futtatását az eszközön. [8]

Bár Mirai a DVR-ektől kezdve az IP-kamerákon és routereken át a nyomtatókig számos eszközt megcélzott, a kutatók felfedezték, hogy végső eszközösszetételét erősen befolyásolta egy maroknyi fogyasztói elektronikai gyártó piaci részesedése és tervezési döntései. [8] Ennek egyik mutatója, hogy miközben a megfertőzött eszközök folyamatosan szkennelték az internetet, újabb és újabb gyenge eszközöket keresve találták meg például a beépített gyenge jelszavakat. Az ehhez hasonló sérülékenységeket kihasználva birtokba vették az új eszközt, majd a központtól érkező utasításokat alapján szinkronban hajtottak végre olyan támadásokat, amelyek többek között globális digitális szolgáltatásokat céloztak. [1]

A személygépjárművek adattovábbítási mechanizmusaik miatt szintén alkalmasak lehetnek a botnetek kialakítására, amennyiben a támadóknak többféle sérülékenységet egy-

[3] https://twitter.com/olesovhcom/status/778830571677978624

idejűleg sikerül kiaknázniuk. Az ehhez hasonló lehetőségekről már jelenleg is több tanulmány olvasható – ilyen például egy elektromos személygépjárművekből létrehozott botnetnek a villamos hálózatra gyakorolt lehetséges hatásairól szóló 2021-es tanulmány. [9]

SZEMÉLYGÉPJÁRMŰVEK ADATTOVÁBBÍTÁSI MECHANIZMUSAI ÉS SÉRÜLÉKENYSÉGEI

A modern járművek olyan összekapcsolt elektronikai rendszereket tartalmaznak, amelyek a kibertérben jelenlévő különböző fenyegető szereplők potenciális célpontjai lehetnek. Az személyautók ma már képesek interakcióba lépni környezetükkel azáltal, hogy adatokat cserélnek az városok lakosságának nyújtott szolgáltatások széles skáláját biztosító vezérlőállomásokkal. Ez ráadásul nem csak okosvárosokra vonatkozik – gondoljunk csak a telekommunikációs hálózattal való összeköttetésre. A járművek ezenkívül kifinomult vezérlőket tartalmaznak, amelyek valós időben kezelik az érzékelők hálózatán keresztül gyűjtött adatokat. Ennek köszönhetően hasonló szerephez jutnak a kibertérben, mint a mobiltelefonok vagy a számítógépek. Amennyiben a gyártó, azaz az úgynevezett OEM (original equipment manufacturer) és alvállalkozói nem gondoskodnak a megfelelő védelemről a hackerek átvehetik a jármű irányítását azáltal, hogy a CAN-buszon nagyszámú vezérlőhálózati csomagot (normál és diagnosztikai csomagokat egyaránt) küldenek a belső alkatrészeknek. Ha a rosszindulatú csomagok a jogos csomagok előtt érkeznek az ECU-khoz (engine control unit), az alkatrészek érvényesnek tekintik azokat.

A normál csomagokat a támadók többféle komponens manipulálásának céljából küldhetik, beleértve az autó sebességmérőjét, kilométer-számlálóját, a fedélzeti navigációs rendszert, a kormányzást, a kamerarendszert, a fékeket és a gyorsítást. A diagnosztikai csomagokkal a jármű néhány komponensének viselkedésének megváltoztatása idézhető el, mint például a fékek kezelése, a motor leállítása, a lámpák villogása, az ajtók zárása/kioldása és az üzemanyagszint-mérő módosítása. A normál csomagokkal ellentétben az ECU-nak küldött diagnosztikai tevékenységeket hitelesíteni kell. A hitelesítési folyamat gyenge végrehajtása azonban komoly kockázatot jelent a felhasználók számára.

Támadás formája	Leírás
Telematikai rendszerek elleni támadások	A telematikai rendszerek lehetővé teszik, hogy a járművek egy távoli központtal kommunikáljanak, telemetriai adatokat és egyéb információkat cseréljenek vele. Egyes autógyártók már most is kínálnak ügyfeleiknek telemetriai szolgáltatásokat távdiagnosztikai célokkal, amelyekkel megelőzhetők a véletlen balesetek és az elektronikai hibák. A támadók kihasználhatják e rendszerek sebezhetőségeit, hogy potenciálisan beavatkozzanak a fedélzeti alkatrészekbe és módosítsák azok paramétereit, megváltoztassák a jármű reakcióját a vezető utasításaira.
Rosszindulatú programok kihasználása	Egy támadó személyre szabott rosszindulatú szoftvereket juttathat be egyes autóalkatrészekbe, módosítva azok viselkedését, vagy szolgáltatásmegtagadási állapotot idézhet elő. Egy rosszindulatú programot kü-

Támadás formája	Leírás
	lönböző módokon lehet bejuttatni a rendszerbe. Például egy MP3-olvasóba dugott USB-stick segítségével vagy vezeték nélküli technológián (Wifi, Bluetooth, mobilkommunikáció) keresztül.
Jogosulatlan alkalmazások	A fedélzeti számítógépek alkalmazásokat és a kapcsolódó frissítéseket tölthetnek le és hajthatnak végre. Egy fenyegető szereplő saját céljai elérése érdekében módosíthatja ezeket az alkalmazásokat. Egy klasszikus ellátási lánc elleni támadás során a hackerek olyan hamisított frissítést juttathatnak be az autóba, amely a járműre telepítve és végrehajtva lehetővé teszi a támadók számára, hogy további rosszindulatú tevékenységeket hajtsanak végre.
OBD porton keresztüli hozzáférés	A testreszabott szoftverek kihasználhatják az OBD-II (fedélzeti diagnosztikai) portot a telepítéshez. Ha a csatlakozóhoz a CAN-buszon keresztül hozzáférnek, lehetőség nyílik a csatlakozóhoz csatlakoztatott minden alkatrész megfigyelésére.
Ajtózárak és kulcstartók	Egy támadó utánozhatja a kulcscsomók és ajtózárak által a zárak vezérlésére és az autómotorok indítására/leállítására használt hozzáférési kódot.

1. Táblázat - Gyakori személygépjárműveket érő támadástípusok, saját szerkesztés.

Jelen tanulmány szempontjából az első három támadástípus bír relevanciával, mivel ezekhez van szükség internetcsatlakozásra. Ahhoz azonban, hogy a lehetséges veszélyeket jobban megértsük, érdemes áttekinteni a személygépjárművek belső hálózatának sajátosságait is. A következő generációs elektromos architektúráinak, azaz EEA (Electrical/Electronic Architecture) egyik legjelentősebb kihívása a jármű elektronikus alkatrészei közötti nagysebességű kommunikáció kezelése a költségek szinten tartása mellett. Az alábbi táblázat a főbb belső hálózati protokolltípusokat foglalja össze:

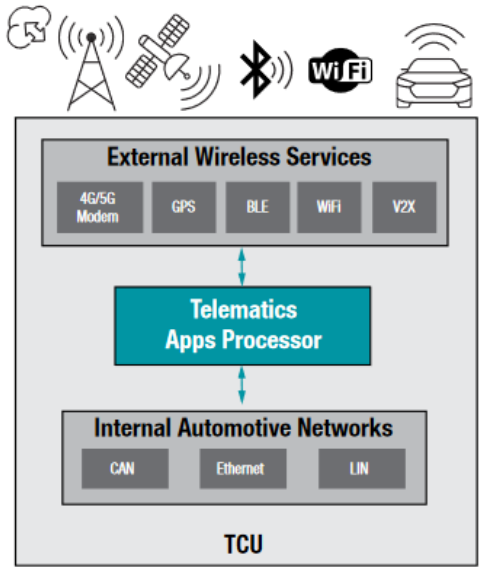
Protokoll neve	Leírás
CAN (Controller Area Network)	A jelenlegi autóipar legsikeresebb kommunikációs hálózata a CAN protokoll. A CAN protokollt a Bosch vállalat fejlesztette ki, és 1986-os megjelenése óta a legszélesebb körben használt szabvány a járműhardverek kommunikációjának területén. [10] Más hálózati technológiákhoz képest a CAN kiemelkedő előnyökkel rendelkezik a költséghatékonyság és a rugalmasság terén. A CAN egyik változata a rugalmas adatátviteli sebességű (CAN-FD) [11], [12] amely akár 8 Mb/s sávszélességű [13]. A CAN egy többmesteres hálózat, amelyben min-

Protokoll neve	Leírás
	den csomópont egyformán és egymástól függetlenül fogadhat és sugározhat információt. Ezzel a tulajdonságával a CAN szinte „plug-and-play" módon működik: új ECU-k vagy diagnosztikai eszközök könnyen csatlakoztathatók a hálózathoz a hálózat külön módosítása nélkül. Ez azonban a kommunikációs rendszert is sebezhetővé teszi a támadásokkal szemben. [13]
LIN (Local Interconnect Network)	A helyi összekötő hálózat (LIN) lehetővé teszi az alacsony költségű és rugalmas vezetékkötegek kialakítását, és könnyen megvalósítható speciális támogatási követelmények nélkül. A LIN sávszélességi kapacitása azonban csak 20 kb/s. Általában az ablakok tekerését és az ülések vezérlését végző kapcsolókban és motorokban használják.
FlexRay	A FlexRay protokollt úgy tervezték, hogy támogassa a jármű biztonságkritikus funkcióinak ellátására szolgáló elektromos/elektronikus rendszerek használatát, beleértve a "brake-by-wire", "suspension-by-wire", "steer-by-wire" és általában az "x-by-wire" elven működő kapcsolatokat. [14] A beépített időszinkronizációs mechanizmusnak köszönhetően a FlexRay kis időbeli késleltetés mellett is képes biztosítani a biztonságkritikus komponensek közötti valós idejű kommunikációt.
MOST (Media Oriented Systems Transport)	A MOST (Media Oriented Serial Transport) egy másik járműfedélzeti hálózat. A MOST-ot a járművekben található infotainment eszközök és kapcsolódó alkalmazások támogatására fejlesztették ki. [15], [16], [17] Fizikai rétegként műanyag optikai szálakat használ, így a hálózat el van szigetelve az elektromágneses interferenciától (EMI), ami megakadályozza az olyan problémákat, mint a zúgó hangok az infotainment rendszerben. [17]
Ethernet – TCP/IP	Ahogy az autók egyre inkább összekapcsolódnak, egyre több adatra van szükségük, ami miatt az Ethernet egyre elterjedtebbé vált az autókban – az átjárók ennek az igénynek a kielégítésére fejlődtek ki. Míg a régebbi átjárók kisebb, egyszerűbb mikrokontrollereket (MCU-kat) használtak vezérlőként, az újabb átjárók processzorokat használnak, néha egy kiegészítő MCU-val kiegészítve. A processzor és az MCU közötti különbség a memóriában rejlik - a processzorok külső memóriával rendelkeznek, míg az MCU-k mindent a chipen tárolnak. A processzorokra való áttérés oka részben a támogatási szempontokban keresendő. Sok processzorban az Ethernet és az azt támogató szoftver is integrálva van. A több memóriával rendelkező processzorok népszerű

Protokoll neve	Leírás
	operációs rendszereket, például Linuxot futtatnak, ami nagyobb hordozhatóságot tesz lehetővé, és csökkenti a fejlesztési időt. [18], [19]

2. Táblázat - Személygépjárművek belső hálózatának jellemző protokollja, saját szerkesztés.

A fent felsorolt belső hálózatokat egyre több jelenleg is forgalmazott személygépjármű esetében egy beépített „router", a TCU (Telematics Control Unit) [20] köti össze a telekommunikációs hálózattal – a TCU tehát tulajdonképpen egy olyan ECU, amely kapcsolatot biztosít az internethez. Az internethez és a felhőhöz csatlakozó autók egyre inkább mindenütt jelen vannak, mivel az autógyártók a járműveket Wifi, Bluetooth és mobil adatátviteli lehetőségekkel szerelik fel. Az ilyen csatlakoztathatóság lehetővé teszi a segélyhívást (eCall). valamint a szórakoztató és egyéb tartalmak elérését online hozzáféréshez utazás közben, valamint az OTA-szolgáltatás mellett szoftverfrissítéseket biztosít az autóban lévő digitális tartalomhoz. [20] Hogy a jármű szórakoztatóelektronikai eszközeire a gyártó „over-the-air", azaz OTA frissítéseket küldhessen, azért van szükség, mert így anélkül teszi lehetővé a szoftverek naprakészen tartását, hogy a tulajdonosnak fel kéne keresnie egy szervizt. Ez természetesen nem csak kényelmi funkció, hanem olyan szempontból is hasznos lehet, ha éppen biztonsági rések kijavítását kell minél gyorsabban megoldani. Mivel azonban a járművek a mobiltelefonokhoz hasonlóan egyszerű HTTPS protokollon keresztül kommunikálnak, így ezekhez hasonlóan kitettek a különböző sérülékenységeknek.



1. ábra - Egy telematikai rendszer sematikus rajza, Subbu Venkat 2020. [20]

Az 1-ábra egy telematikai rendszer sematikus rajzát mutatja. A TCU-k a csatlakoztathatóság biztosításához mobil vagy Wifi modemmel, a modemtől kapott adatok feldolgozásához pedig alkalmazásprocesszorral rendelkeznek. A feldolgozás magába foglalja az adatok dekódolását, az adatok érvényesítését és továbbítását az átjáróhoz vagy egy másik

tartományi ECU-hoz. A jelenlegi architektúrákban a modem és a processzor egyetlen félvezető eszközbe van integrálva. Mivel azonban a modemszabványok folyamatosan fejlődnek, az autógyártók egyre inkább olyan architektúra felé fordulnak, amely elválasztja a modemet a processzortól. Ezenkívül mind az autóipari átjárók és a TCU-k is egyre inkább Ethernet-alapúvá válnak. A modemnek a processzortól való elválasztásának előnye, hogy az ECU gyorsan átállítható egy új modemszabványra mindössze a modem cseréjével, megőrizve a processzort és az összes kapcsolódó és rajta futó szoftvert. [20] Bár a biztonság és a védelem ebben a tekintetben is egyre fontosabbá válik, sajnos gyakran még mindig a költségek döntenek. Egy dedikált beágyazott biztonsági processzor vagy alrendszer segíthet megvédeni a jármű biztonsági kulcsaihoz való hozzáférést, a kommunikációs csatornák biztonságának fokozását. A biztonsági funkciók jellemzően diszkrét MCU-kban valósulnak meg, amelyek tanúsítvánnyal rendelkeznek. Az alkalmazásprocesszorokat és a biztonsági MCU-t is integráló SoC (system-on-chip) azonban alacsonyabb anyagköltséget kínál az autóipari OEM-eknek. [20]

2016-ban a Keen Security Lab, kínai biztonsági kutatók egy csoportja felfedezett egy módszert a Tesla modellekben található CAN-busz feltörésére, amely a kijelzőket és a fékeket vezérli. [21] A kutatók képesek voltak távolról hozzáférni a központi vezérlőegységhez, és beállítani a tükröket, bezárni az ajtókat, manipulálni a műszerfalat, sőt még a fékeket is be tudták kapcsolni. Ezt jelentették a Teslának, a cég pedig egy újonnan kiadott frissítéssel reagált a bejelentésre. Ez az esemény azonban egyértelműen rávilágított arra, hogy az alkalmazott elavult szoftverrel valóban probléma van. Néhány évvel később szintén a Keen Security Lab egy másik csapata 14 sebezhetőséget fedezett fel a BMW által gyártott járművekben. [22] Felfedezték, hogy egy hiba kihasználásával hozzáférhetővé válik a telematikai vezérlőegység, valamint a CAN-busz. A Teslához hasonlóan a BMW válasza az volt, hogy frissítéseket vezetett be az érintett modellekhez. Ezeket OTA (over-the-air) megoldással, az interneten kapcsolaton keresztül vagy a BMW márkakereskedésekben tették elérhetővé az ügyfelek számára. Hasonlóan, holland kutatók felfedeztek egy módszert, amellyel meg lehet kerülni a rádiófrekvenciás azonosításon (RFID) alapuló kulcsos indításgátlókat, [23] amelyeket 1996 óta számos autógyártó elsődleges biztonsági funkcióként használ. A szerzők egy olyan módszert alkalmaztak, amely megkerüli a kriptográfiai hitelesítést, miközben kevesebb mint 6 perc alatt, speciális hardver nélkül elvégezhető.

Egy másik példa a személygépjárművek feletti irányítás megszerzéséhez Sam Curry webalkalmazások biztonságával foglalkozó kutató 2023 január 3-i esettanulmánya [24], melyben részletes leírást ad több ismert márka rendszereihez való távoli hozzáférésének lehetőségeiről. A teszt során Curry és csapata a következő adatokhoz fért hozzá a teljesség igénye nélkül: a tulajdonos elérhetőségei, email címe, telefonszáma (pusztán az alvázszám ismeretében) és a következő rendszereket volt képes távolról irányítani: elektromos zár, motor (indítás is), precíziós lokáció, fényszórók, duda, a felhasználói fiók lecserélése (azaz a felhasználó kizárása az autóból), hozzáférés a 360 fokos kamerához élő felvételek készítésével, távoli kódok futtatása, hozzáférés a memóriák tartalmához, illetve egyes márkák esetében hozzáférés a vállalat dolgozóinak adataihoz.

A támadás kiindulópontja lehet maga a személygépjármű is, de jellemzőbben az OEM (gyártó) vagy forgalmazó központi szerver webes felületeinek valamelyike számít alkalmas célpontnak, ahonnan egyidejűleg több jármű felé is továbbíthatóak az utasítások. Tekintettel arra, hogy az adattovábbítás nem feltétlenül csak a gyártó felé folyhat, hanem

más telematikai vállalatok is részt vehetnek annak valamelyik szakaszában, így a potenciális támadási felület is kiterjedt. A sérülékenységek eredhetnek félrekonfigurált webalkalmazásokból, hozzáférhető API végpontokból (különösen figyelemreméltó példa erre a leírásban szereplő TOTP generálást lehetővé tevő végpontra vonatkozó rész). [24] Amennyiben a támadó hozzáfér a vállalaton belüli kommunikációs csatornákhoz és/vagy a vállalat forráskód repository-jaihoz, olyan információk megszerzésére lesz képes, melyekkel könnyen megértheti a fedélzeti rendszer biztonsági funkcióinak működését és megtalálhatja a további sérülékenységeket, melyek az egyes járművekkel való közvetlen kommunikációt lehetővé teszik számára.

További példa a Tesla Kínai Népköztársaság egyes területeiről való kitiltásának története. Az Állampárt a Tesla sanghaji gyárának megnyitását követően aggodalmát fejezte ki azzal kapcsolatban, hogy a járművek korlátlanul készíthetnek felvételeket még az olyan magas biztonsági besorolású helyekről is, mint például a katonai bázisok – amennyiben bejutnak egy ilyen területre. [25] Figyelemreméltó az a tény, hogy a párt egy magasszintű, zárt, éves megbeszélésének időpontjával kapcsolatban a márka járművei teljesen kitiltásra kerültek „legalább két hónapos időtartamra" a teljes helyszínül szolgáló pekingi városrészből. [26] Ez az információ abban a tekintetben is különlegesnek számított, mert a rendszeresen megtartott találkozó dátumát hagyományosan nem szokták nyilvánosságra hozni. Hasonló helyzet alakult ki Csengduban is, ahol a kitiltás tényéről sem látott napvilágot hivatalos információ, egyszerűen a Tesla tulajdonosok figyeltek fel rá, hogy bizonyos városrészekre nem engedik be őket a rendőrök. A kínai esetekkel kapcsolatban Elon Musk úgy nyilatkozott, hogy a Tesla autói nem kémkednek sem Kínában, sem máshol, és hogy a céget bezárnák, ha ez megtörténne. [27] Hónapokkal később a vállalat közölte, hogy az általa Kínában értékesített autók által generált összes adatot az országban tárolják. Az iparág és a szabályozó hatóságok számára világszerte egyre nagyobb kihívást jelent annak ellenőrzése, hogy ezeket a képeket hogyan használják fel, hová küldik és hol tárolják. 2021-ben a Tesla sanghaji üzemében készült az amerikai autógyártó által világszerte leszállított 936 000 jármű mintegy fele.[4], [26] Kína ráadásul hatalmas piac is a Tesla és az elektromos járművek számára.

EGY MEGFIGYELÉST CÉLZÓ TÁMADÁS LEHETSÉGES FORGATÓKÖNYVÉNEK BEMUTATÁSA

Az fejlett személygépjárműveket különböző fenyegető szereplők vehetik célba, például olyan személyek, akik megpróbálnak megtámadni egy adott autót, hogy annak rendszereit valamilyen célból a saját szolgálatukba állítják vagy éppen magánadatokat szerezzenek a jármű rendszereiből. Jelen tanulmányban a kifinomultabb támadástípusokra összpontosítunk, amelyek az intelligens járművek hálózatát és adatfolyamát használják. Az általunk elemzett forgatókönyvben feltételezzük, hogy a fenyegető szereplőnek több autóhoz is hozzáférése van, és a rendszeres adatkommunikációt használja titkos csatornaként a rosszindulatú tevékenység végrehajtására. Megközelítésünk az személygépjárművet a korábbi fejezetekben bemutatott információkra építve speciális IoT eszköznek tekinti, amely rendszeres hálózati kommunikációval rendelkezik.

[4] https://carsalesbase.com/china-tesla/

A több járműhöz és azok adataihoz való hozzáférés egyedülálló lehetőséget biztosít a fenyegetést okozó szereplők számára. Vélelmezzük, hogy a fenyegető szereplő hozzáférhet az összes szükséges intelligens járműadathoz, mint például a következőkhöz:

- a jármű GPS-koordinátái az időbélyegzőkkel együtt;
- a jármű által belülről és kívülről készített kameraképek, azok időbélyegzőjével együtt;
- a jármű belsejében zajló hangkommunikáció, szintén az időadatokkal együtt.

Azt is figyelembe vesszük, hogy a jármű rendelkezik a következőkkel:

- rendszeres kommunikáció az akkumulátorra vonatkozó naprakész adatok szolgáltatása érdekében;
- rendszeres kommunikáció a szoftverfrissítések ellenőrzésére;
- rendszeres kommunikáció az önvezető adatok megszerzésére és jelentésére;
- rendszeres kommunikáció a gépjármű-biztosítóval.

Feltételezésünk szerint a fenyegető szereplő képes ezen adatcsatornák egyikét használatba venni és a kommunikációt rejtett csatornaként használni a rosszindulatú tevékenység elrejtésére. Az alábbiakban tehát azt feltételezzük, hogy a járművek egy jelentősebb csoportjához egy külső szereplő hozzáfér, ezáltal lehetősége van egy előre meghatározott algoritmus alapján adatokat lekérni. Ilyen adat lehet pl. az autó külső kameráinak felvételei. Ezek alapján néhány elméleti lehetőséget vizsgálunk. A különböző lehetőségek vizsgálatánál két alapvető jellemzőt figyelembe kell vennünk:

- az algoritmus komplexitása, amit a személygépjárműnek végre kell hajtania a megfigyelő művelet során;
- a többletadatok mennyisége, amit a személygépjárműnek továbbítania kell a támadó (megfigyelő) felé.

Mivel a fenti körülményeket vizsgáló, az itt bemutatott elméleti modellhez hasonló leírás a tanulmány írásának időpontjában nem állt rendelkezésre, így a továbbiakban ismertetett információk során a szerzők által kikalkulált értékek bemutatására kerül sor.

Kijelölt területek megfigyelése

Egy elméleti lehetőség a kijelölt objektumok környezetének megfigyelése. Egy ilyen jellegű támadásnál a jármű GPS koordináták alapján aktiválja a megfigyelést. Az algoritmus tehát annak aktuális pozícióját figyeli és abban az esetben, ha egy meghatározott pozícióba kerül, fényképeket készít a külső kamerák segítségével. Ezen fényképeket a telekommunikációs hálózaton keresztül képes továbbítani a támadó felé. A támadó algoritmus komplexitása ebben az esetben alacsony. A rejtett funkciók az alábbi elemeket tartalmazzák:

- folyamatos helypozíció figyelés, adott pozíciókban az extra funkciók aktiválása és deaktiválása;
- aktivált állapotban fényképek készítése;
- az elkészített képek azonnali vagy késleltetett rejtett továbbítása.

Az általunk alkalmazott modell a kontrollált autók számából mint bemenő adat és a forgalom nagyságából kiindulva vizsgálja a támadó lehetőségeit. Vizsgálatunkhoz egy Budapest nagyságú várost feltételeztünk 500.000 autóval. Az autók eloszlása a városban

nem egyenletes, illetve a gépjármű tulajdonosának lakhelye, munkahelye és egyéb életvitelszerű mozgása befolyásolja az autó lehetőségeit. Mindezektől függetlenül egyszerűsített módon azt feltételeztük, a városban lévő autók egyenletesen járják a várost. További feltételezéseink a megfigyelt épülettel kapcsolatosak. Az elkészített vizsgálatunkban azt feltételezzük hogy a megfigyelt épületben emberek dolgoznak vagy laknak. Egy ember legalább napi 4 percet az épületen kívül, de az épület környezetében van, az okos autók által vizuálisan elérhető területen (2 perc érkezéskor, 2 perc távozáskor).

A forgalom nagyságát percenkénti áthaladó autószámmal vesszük figyelembe. Egy egysávos úton 50-es tempóval 10 autó halad át percenként egy sávban. Az autók száma természetesen függ a napszaktól, a sávok számától és az esetleges közlekedési dugóktól, lámpáktól és a megengedett sebességtől. A vizsgálatunk másik bemenő paramétere a kontrollált autók száma. Megvizsgáltuk a lehetőséget azokban az esetekben ha a támadó 1, 100, 1000, 10.000 illetve 100.000 gépjármű adataihoz fér hozzá:

autók száma melyekhez a támadó hozzáfér	**5 gépjármű percenként / napi 5000**	**10 gépjármű percenként / napi 10000**	**20 gépjármű percenként / napi 20000**	**40 gépjármű percenként / napi 40000**
1 gépjármű	kb. évente 2 fotó	kb. 3 havonta egy fotó	kb. havonta egy fotó	kb. 2 hetente 1 fotó
100 gépjármű	kb. naponta egy fotó	kb. naponta 2 fotó	kb. 4 óránként egy fotó	kb. 2 óránként egy fotó
1000 gépjármű	kb. 2 óránként egy fotó	kb. óránként egy fotó	kb. fél óránként egy fotó	kb. 15 percenként egy fotó
10.000 gépjármű	10 percenként egy fotó	5 percenként 1 fotó	2-3 percenként egy fotó	1-2 percenként egy fotó/teljes megfigyelés
100.000 gépjármű	percenként egy fotó / teljes megfigyelés	teljes megfigyelés	teljes megfigyelés	teljes megfigyelés

3. Táblázat - Kijelölt területek megfigyelése, saját szerkesztés.

Kijelölt személyek megfigyelése

A kijelölt személy megfigyeléshez tartozó algoritmus komplexitása ebben az esetben lényegesen magasabb. Ebben az esetben a gépjárműnek folyamatos arcfelismerést kell végeznie a kamerák képeiből. A rejtett funkciók az alábbi elemeket tartalmazzák:

- folyamatos arcfelismerés a vizuálisan elérhető személyekre, adott személy beazonosítása esetén a további szükséges funkciók aktiválása;
- aktivált állapotban fényképek tárolása és a GPS adatok lementése;
- az elkészített képek és GPS adatok azonnali vagy késleltetett rejtett továbbítása.

A kijelölt személy megfigyeléséhez azt feltételezzük hogy a célszemély napi 20 perc és 2 óra közötti időtartományt tartózkodik az utcán, az okos gépjárművek által vizuálisan elérhető területen:

autók száma amihez a támadó hozzáfér	**napi 20 perc az utcán**	**napi 40 perc az utcán**	**napi 1 óra az utcán**	**napi 2 óra az utcán**
1 gépjármű	kb. 100 naponta egy detektált pozíció	kb. 50 naponta egy detektált pozíció	kb. 20-30 naponta egy detektált pozíció	kb. 10-20 naponta egy detektált pozíció
100 gépjármű	kb. naponta 1 detektált pozíció	kb. naponta 2 detektált pozíció	kb. naponta 3 detektált pozíció	kb. naponta 6-8 detektált pozíció
1000 gépjármű	naponta 10 detektált pozíció	teljes megfigyelés	teljes megfigyelés	teljes megfigyelés
10.000 gépjármű	teljes megfigyelés	teljes megfigyelés	teljes megfigyelés	teljes megfigyelés
100.000 gépjármű	teljes megfigyelés	teljes megfigyelés	teljes megfigyelés	teljes megfigyelés

4. Táblázat - Kijelölt személyek megfigyelése, saját szerkesztés.

ÖSSZEGZÉS

Jelen tanulmányban a személygépjárművekhez kapcsolódó megfigyeléssel kapcsolatos kibertámadások lehetőségeit vizsgáltuk. Elemeztük a rendelkezésre álló információkat, az egyes autótípusok sajátosságait, az eddig publikált támadásokat és egyéb ezzel kapcsolatos kiszivárgott információkat. Megvizsgáltunk néhány elméleti lehetőséget feltételezve hogy a támadó hozzáfér egy vagy több okos személygépjármű erőforrásaihoz.

A vizsgáltaok alapján arra jutottunk, hogy egy (vagy főként több) személygépjármű belső rendszereihez való hozzáférés természetesen nagyobb feladat, mint a korábbiakban bemutatott IoT botnetek létrehozása. Azonban a megfelelő erőforrások birtokában egyáltalán nem tűnik lehetetlennek. Egy az általunk kidolgozott forgatókönyvhöz hasonló eset megvalósulása komoly személyi biztonsági, vagy adott esetben nemzetbiztonsági kockáza-

tot is jelenthet. Míg a tanulmányok túlnyomó része kifejezetten az automata járművek, illetve a V2x technológiák biztonságának kérdésköreit járja körül, fontos, hogy a már jelenleg is elterjedt és használatban lévő rendszerek biztonságára is megfelelő figyelem irányuljon.

Az adatokhoz való hozzáférés révén okozott károk nagysága és típusa nagyban függ a támadó kapacitásaitól és céljaitól is, így további kutatás alapját képezheti ezeknek a céloknak az ismertetése. Amennyiben a támadó olyan nagy erőforrásokkal rendelkező szervezet, mint például egy állami támogatást élvező hacker csoport, abban az esetben a támadás akár szofisztikáltabb módon, annak napvilágrakerülése nélkül is véghezvihető.

További kutatási lehetőséget ad a potenciális célpontok szerinti vizsgálat is. Az OEM-en és a kereskedőkön túl célponttá válhatnak a különböző flották adatainak kezelésére specializálódott telematikai vállalatok. Az ilyen szolgáltatók különböző eszközöket biztosítanak ügyfeleik számára, hogy azok pontosan nyomon követhessék a gépjárműflottájuk egyes elemeinek mozgását, helyzetét vagy bármilyen más, az igényeknek megfelelő információt, akár kameraképekkel is. Amennyiben egy flotta esetében alkalmazott fejlett telematikai rendszerhez fér hozzá a támadó, akkor az hasonló aggodalmakra adhat okot, hiszen ezek az eszközök kifejezetten nyomkövetési célt, illetve az autóról és környezetéről folyó adatgyűjtést szolgálják. A flotta alatt ráadásul nem csak logisztikai vállalatokat érthetünk, hanem például a rendőrség vagy egyéb hatóságok, mentők, tűzoltók járműveit is, akik esetlegesen szenzitív helyekre is beléphetnek.

Az okosgépjárművek robbanásszerű elterjedése a közeljövőben bekövetkezik. Amellett, hogy a kényelmi szolgáltatások egy élvezhetőbb, biztonságosabb és környezetbarátabb jövőt hoznak az emberiségnek, számos olyan elméleti lehetőség rejlik a technológiában, amely nemzetbiztonsági kockázatot jelent. A megfelelő szabályozás, átláthatóság kierőltetése jelentősen mérsékelni tudja ezen veszélyforrásokat.

FELHASZNÁLT IRODALOM

[1] C. Dr. Krasznay, *Kiberbiztonság a XXI. században*, Budapest: Katonai Nemzetbiztonsági Szolgálat, 2022.

[2] ENISA, „IoT," 2020. [Online]. Elérhető: https://www.enisa.europa.eu/topics/iot-and-smartinfrastructures/iot. [Hozzáférés dátuma: 28 02 2023].

[3] R. Deibert, „The Geopolitics of Cyberspace after Snowden," *Current History*, vol.: 114, szám:768, pp. 9-15., 2015.

[4] E. Snowden, *Rendszerhiba*, Budapest: XXI. Század, 2019.

[5] Wikileaks, „Vault 7: CIA Hacking Tools Revealed," Wikileaks, 2017. [Online]. Elérhető: https://wikileaks.org/ciav7p1/. [Hozzáférés dátuma: 28 02 2023].

[6] M. Antonakakis, T. April, Bailey Michael, M. Bernhard, E. Bursztein, J. Cochran, Z. Durumeric, A. J. Halderman, L. Invernizzi, M. Kallitsis, D. Kumar, C. Lever, Z. Ma, J. Mason, C. Seaman, N. Sullivan, K. Thomas és Y. Zhou, „Understanding the Mirai Botnet," in *Usenix*, Vancouver, BC, Canada, 2017.

[7] C. B. Krebs, „Krebs On Security Hit With Record DDoS," KrebsOnSecurity, 2017. [Online]. Elérhető: https://krebsonsecurity.com/2016/09/krebsonsecurity-hit-with-record-ddos/. [Hozzáférés dátuma: 28 02 2023].

[8] J. Margolis, T. T. Oh, S. Jadhav, Y. H. Kim és J. N. Kim, „An In-Depth Analysis of the Mirai Botnet," in *2017 International Conference on Software Security and Assurance (ICSSA)*, Altoona, PA, USA, IEEE, 2017, pp. 6-12.

[9] O. G. M. Khan, E. El-Saadany, A. Youssef és M. Shaaban, „Impact of electric Vehicles Botnets on the Power Grid," in *2019 IEEE Electrical Power and Energy Conference (EPEC)*, Montreal, QC, Canada, IEEE, 2019, pp. 1-5.

[10] A. Fodor, D. Fodor, K. Dr. Bíró és L. Dr. Szabó, „A CAN mint ipari kommunikációs protokoll," Kolozsvár: Kolozsvári Műszaki Egyetem, 2007.

[11] M. Afsin, K. W. Schmidt és E. G. Schmidt, „C3: configurable CAN FB Controller: Architecture, design and hardware implementation Industrial Embedded Systems (SIES)," in *2017 12th IEEE International Symposium On*, IEEE, 2017, pp. 1-9.

[12] F. Hartwich és et al., „CAN with flexible data-rate," in *iCC*, 2012, pp. 1-9.

[13] M. Dibaei, X. Zheng, K. Jiang, R. Abbas, S. Liu, Y. Zhang, Y. Xiang és S. Yu, „Attacks and defences on intelligent connected vehicles: a survey," *Digital Communications and Networks*, vol.: 6, szám: 4, pp. 399-421, 2020.

[14] F. Consortium, Flexray Communication System Protocol Specification 3.0.1, 2010.

[15] S. Khurshid, C. Păsăreanu és W. Visser, „MOST 150 development and production launch from an OEM's perspective," in *11th MOST Intercon-Nectivity Conference*, Dél-Korea, 2010, pp. 553-568.

[16] A. Grzemba, „Most Book from Most 25 to Most 150," in *MOST Cooperation FRANZIS*, 2011.

[17] E. Zeeb, „Optical data bus systems in cars: current status and future challenges," in *27th European Conference on Optical Communication (ECOC)*, IEEE, 2001, pp. 70-71.

[18] H. Lothamer, „Automotive gateways: the bridge between communication domains," Texas Instruments, 2017.

[19] J. Taube, F. Hartwich és H. Beikirch, „Comparison of CAN Gateway Modules for Automotive Industrial Control Applications," iCC, 2005.

[20] S. Venkat, „Evolving Automotive Gateways for Next-Generation Vehicles," Texas Instruments, 2020.

[21] A. Perring, R. Canetti, J. D. Tygar és D. Song, „The Tesla Broadcast Authentication Protovol vol. 5," *CryptoBytes*, vol.: 5, szám: 2, pp. 2-13, 2002.

[22] Z. Zorz, „Researchers hack BMW cars, discover 14 vulnerabilities," Helo Net Security, 2018. [Online]. Elérhető: https://www.helpnetsecurity.com/2018/05/23/hack-bmw-cars/.

[23] R. Verdult, F. Garcia és J. Balasch, „Gone in 360 Seconds: Hijacking with Hitag2," Usenix, 2012.

[24] S. Curry, „Web Hackers vs. The Auto Industry: Critical Vulnerabilities in Ferrari, BMW, Rolls Royce, Porsche, and More," Samcurry.net, 2023. [Online]. Elérhető: https://samcurry.net/web-hackers-vs-the-auto-industry/. [Hozzáférés dátuma: 28 02 2023].

[25] S. Loveday, „China Resort Town Bans Tesla's EVs Over Spying Concerns," InsideEVs, 2022. [Online]. Elérhető: https://insideevs.com/news/593257/tesla-cars-banned-china-spying-concerns/. [Hozzáférés dátuma: 38 02 2023].

[26] Reuters, „Tesla cars barred for 2 months in Beidaihe, site of China leadership meet," Reuters, 2022. [Online]. Elérhető: https://www.reuters.com/business/autos-transportation/chinas-beidaihe-district-bar-tesla-cars-driving-july-local-police-2022-06-20/. [Hozzáférés dátuma: 28 02 2023].

[27] K. Lyons, „Elon Musk says Tesla would be 'shut down' if its cars were used for spying in China," The Verge, 2021. [Online]. Elérhető: https://www.theverge.com/2021/3/21/22343018/elon-musk-tesla-shut-down-cars-spying-china. [Hozzáférés dátuma: 28 02 2023].

[28] H. Mukundhan, „Anatomy of an IoT DDoS Attach and Potential Policy Responses," *ISACA JOURNAL,* vol.: 5, 2017.

INFORMATION OPERATIONS AND INFORMATION WARFARE

INFORMÁCIÓS MŰVELETEK ÉS INFORMÁCIÓS HADVISELÉS

PÁL Anita Brigitta[1]

Abstract

Information warfare has become crucial in the art of war and military practice of the 21st century. With the results of the fourth industrial revolution, our imagination of war and the primary goals set in warfare, have also changed. Information has become one of the biggest value before impact measurements. In part, disinformation and sabotage have also entered the arenas of the games in the art of war, controlled by algorithms. Parallel with technological development, information warfare has been redefined. Automated weapon systems, drones, firewalls, viruses, radars, and programs that can be used to influence the physical and virtual battlefield have become an essential part of cyber warfare. The current four-dimensional battlefield (air, land, water and space) is connected by the information battlefield.

Keywords

information warfare, virtual warfare, digital revolution, cyber warfare, military leadership, information operations

Absztrakt

Az információs hadviselés döntő jelentőségűvé vált a 21. század hadművészetében és katonai gyakorlatában. A negyedik ipari forradalom hozadékaival a háborúról alkotott képünk és a hadviselésben kitűzött elsődleges célok is megváltoztak. Az információ lett a legnagyobb érték a csapásmérések előtt. Részint a dezinformáció és a szabotálás is bekerült a játszmák színterei közé az algoritmusok által vezérelt harcok művészetében. A technológiai fejlődéssel párhuzamosan újra definiálták az információs hadviselést. A kiberhadviselés elengedhetetlen részévé váltak az automatizált fegyverrendszerek, a drónok, tűzfalak, vírusok, radarok, valamint az olyan programok, amelyekkel befolyásolni lehet mind a fizikai- mind a virtuális hadszínteret. A jelenkori négydimenziós hadszínteret (levegő, szárazföld, víz és űr) az információs hadszíntér kapcsolja össze.

Kulcsszavak

információs hadviselés, információs műveletek, virtuális hadviselés, digitális forradalom, kiberháború, katonai vezetés

[1] pal.anita@hm.gov.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

GLOBALIZÁCIÓ

„Veszélyektől, vagy bántódástól mentes, zavartalan állapot. A biztonság fogalma mára általánosabb és összetettebb lett, és a biztonsági kockázatok elemzése során a terület specifikus sajátosságait is figyelembe kell venni. A biztonság megértése ma már sokkal összetettebb, mint korábban, és a különböző területeken alkalmazott biztonsági intézkedések és protokollok eltérőek lehetnek egymástól" [1]

A globalizáció folyamatai egy sor fenyegetéssel járulnak hozzá a biztonságpolitika és a nemzeti biztonsági stratégiák mihamarabbi integrációjához. A külpolitikán keresztül a védelempolitikáig, a legnagyobb kihívást szerintem az adat-, illetve az információbiztonság jelenti. Világunkat és egymáshoz való kapcsolódásunkat láthatatlan hálózatok sorai övezik. Világunk globalizációs folyamati között a technológiai fejlődés olyan ütemben halad, amit nem látott még a világ.

Az információs műveletekben meghatározó szerep jut a műveleti tervezések folyamatainak. Az információs technológia gyors fejlődése új szerepet határozott meg a katonai földrajz területén. Az állami vezetés művészetében a geopolitika és geostratégia fontos szerepet játszik, míg a földrajz a logisztika, térképészeti elemzés és műveleti tervezés szempontjából meghatározó tényező. Ugyanakkor a stratégiai földrajz, amely elsődlegesen határozza meg a nemzetvédelmi és a nemzeti biztonsági magatartást, súlya az idők folyamán csökkent. [2]

A globalizáció hatására a biztonság fogalma megváltozott, és már nem csak a területi érdekek mentén alakul. Az államoknak figyelmet kell fordítaniuk az összekapcsolódás és a kölcsönös függőség kérdéseire, nem csak a saját területükön zajló eseményekre koncentrálva. A belbiztonsági kérdések tekintetében a helyi konfliktusok mellett egyre fontosabbak a regionális és globális összefüggések, amelyek között a tömeges bevándorlás és a terrorizmus elleni harcok különösen kiemelkedőek.

Az információs technológia fejlődése számos új kihívást jelent a hadviselésben, amelyek tovább alakítják a korábbi területi határokat. A kiberháború és az információs hadviselés által teremtett új hadszínterek nem ragaszkodnak a hagyományos földrajzi határokhoz, és jelentősen átformálják a nemzetbiztonsági szemléletet. Az információs technológia fejlődése által az új hadszínterek (levegő, szárazföld, víz és űr) határai tovább bővültek és összemosódnak az információs hadszíntér határaival. Az egyre növekvő kibertér már teljes mértékben globálissá vált, és a szakértők egyetértenek abban, hogy a hagyományos, lineáris hadviselési formák kiegészítésére szükség van a nem lineáris konfliktusokkal keleten és nyugaton egyaránt. Azáltal, hogy a társadalmak közötti kapcsolatok dimenziói sokrétűvé váltak (politikai, gazdasági, infrastrukturális, média- és pszichológiai dimenziók), a nemzeti biztonság már nem csak határokkal határozható meg, és az ellenük irányuló támadások sem csak a terület elfoglalásával vagy megtartásával jellemezhetők. [3]

DIGITÁLIS FORRADALOM

Kereken fél évszázada hódít teret Moore törvénye, miszerint az integrált áramkörök összetettsége exponenciális teljesítménynövekedést mutat. A digitális forradalom, amit "harmadik és negyedik ipari forradalom" néven is ismerünk, az áttörést jelenti, amit a számítógépek és a digitalizáció hozott az élet számos területére a 20. század végétől kezdve.

Az integrált áramkörök és mikrocsipek feltalálása megnyitotta az utat a digitális fejlődés előtt. A technológiai eszközök teljesítményének folyamatosan növekedése lehetővé tette a termelés rugalmas automatizálását. Az internet, amely egy globális kommunikációs hálózatként működik, mára megszüntette a tér és idő korlátait.

Az informatikai forradalom, melyet a számítógép és a mikroprocesszorok bevezetése elindított, olyan mértékű hatást gyakorolt a társadalmi életre, hogy ma már az informatikai eszközök használata szinte mindenhol magától értetődőnek tekinthető - legyen szó munkahelyről, otthonról, vagy akár az oktatásról. Minden olyan digitális szolgáltatást amit ingyen használunk, ott gyakorlatilag mi magunk válunk áruvá a titkainkkal és az életünk privát részeivel fizetünk, amit aztán a mesterséges intelligencia által futatott algoritmusok fognak felhasználni, hogy még célozottabb reklámokat kaphassunk.

Az ún. „digitális javak", azaz a szoftverek és a „digitalizált információk" kiemelt jelentőséget kaptak. A digitális forradalom hatására ma már az állami és magánszféra egyaránt elkötelezett a digitális technológiák világa iránt, amelynek használatával egy sor előny és árnyoldal is társul.

Az egyre növekvő globális kibertér az új típusú fenyegetések egyre bővülő kínálatát nyújtja, valamint a nemzetközi és állami szinteken egyaránt új fajta szervezetek és kibervédelmi jogszabályok megszületését eredményezték.[4] Azonban nem szabad figyelmen kívül hagynunk, hogy a digitális javak jelentős előnyei alapvetően új szemléletet követelnek meg, amelynek eredményeként komoly jogi és szerzői jogi kihívásokat kell megoldani. [5]

Ha az információs műveletek során lehetőségünk van információs és vezetési előnyre szert tenni a ellenfelekkel szemben, akkor az újonnan létrejövő információk új módon való felhasználása hatékony eszköze lehet a katonai műveletek sikeres végrehajtásának.

Az információs kor és az XXI. század hadviselése szervesen összefonódik, amely megköveteli az információs műveletek elméleti és gyakorlati kérdéseinek fokozott figyelmét.[6] Ezek a műveletek természetes evolúciója során bonyolult, integrált és komplex katonai tevékenységekké válnak, amelyek az információs hadszíntéren megoldandó feladatokhoz különböző tudományterületeket ötvöznek.

A Magyar Honvédség vezetése is felismerte az információs műveletek fontosságát, aminek következményeként külön figyelemmel szenteltek egy fejezetet a MH Összhaderőnemi Doktrínájában, hasonlóan a NATO tagországokhoz. [7]

INFORMÁCIÓS MŰVELETEK HATÁSÁNAK KIHASZNÁLÁSA

Az információs kor és az információs társadalom fejlődésével olyan intellektuális és anyagi erőforrások váltak hozzáférhetővé, amelyek újraértelmezték a hadviselési stratégiákat. Az információs technikai és technológiai forradalom vívmányai gyökeres átalakítást hoztak mindazon elvek és eljárásokat illetően, amelyeket idáig vallottunk és alkalmaztunk a hadügy területén. A fejlődés során egyértelműen kirajzolódott, hogy a korszerű katonai műveletekben, az információ megléte és hiánya, döntő jelentőséggel bír. Az információ hatékony megszerzése és felhasználása komoly előnyöket biztosít a haderő számára, így mindkét fél nagy erőfeszítéseket tesz annak érdekében, hogy információs rendszerei hatékonyabban működjenek, és teljes mértékben kihasználják azok képességeit. E cél érdekében az

információ már nem csak a vezetés és fegyverirányítás során használatos, hanem mint egy nem-kinetikus energia alapú fegyver is alkalmazható. Az új kihívások számos magasabb követelményt állítanak a társadalom és a katonák számára. [8]

Az adat megőrzése és azok helyes felhasználása prioritássá válik olyan hierarchizált és kereszthivatkozásokat tartalmazó struktúrákban, amelyek lehetővé teszik, hogy az adatból információ, abból pedig bölcsesség alakuljon ki. Az internet sokrétű funkcionalitása nemcsak az információ megosztását és a közösségi média használatát teszi lehetővé, hanem egyben a pénzügyi csalások és a kiberbűnözés olyan platformjává vált, amelyet a hálózatba kapcsolt bűnözői csoportok és terrorista szervezetek is nagymértékben ki tudnak használni. [9]

Világunkban minden tevékenységünkkel szinte már adatot generálunk. Takács Gergely, a „Big Data (adatvezérelt) elemzési módszerek alkalmazása a nemzetbiztonsági szférában" című tanulmányának a bevezetésében úgy írja le a Big Data jelenségét, ami olyan exponenciális és folyamatosan keletkező adatok mennyiségét generálja, amelyeket a hagyományos eszközökkel már nem lehet menedzselni, feldolgozni vagy tárolni. Etikai szempontból ráadásul a rendszernek vannak hiányosságai. Stigmatizálás híján egy algoritmus nehezen tud különbséget tenni kódok és igazságok között.

A Big Data módszerek és technológiák lehetővé teszik a rendkívül nagy adatmennyiségek feldolgozását az adatkezelés és feldolgozás párhuzamosítása révén. Ennek lényege az olyan logikailag összekapcsolt géphálózatokon működő algoritmusok alkalmazása, melyek tér- és időbeli korlátok nélkül képesek tevékenykedni. Íly módon az előrejelző elemzések és a predektív analítika alapján hozzásegíthet a bűnmegelőzésben, vagy akár a terrorelhárításban is. [10]

A koalíciós műveletek tapasztalatainak értékelés során a NATO vezetői megállapították, hogy a győzelem elérése érdekében az információs műveletek növekvő jelentőséggel bírnak, míg a precíziós felderítés és fegyverek használata minden haderőnem számára létfontosságúvá vált. Az információs műveletek azonban stratégiai szinten is megnőtt jelentőségre tettek szert, és ezáltal az ezekre adott válaszok is hasonló komolysággal bírnak, különösen azok, amelyek számítógépes hálózatokat céloznak meg. Ezt jól példázza, hogy Oroszország néhány évvel ezelőtt figyelmeztette az Amerikai Egyesült Államokat, hogy a számítógépes hálózati támadásokat egyenértékűnek tekintik a nukleáris támadással, és ennek megfelelően válaszolnak majd rá.

„A katonai létesítményeknek tudomásul kellene venniük, hogy a csata harctere változik. Az információ, mint a konfliktusok és a verseny dimenziója, felcsigázta a jövőbeni nemzetbiztonsági szférák változatosságának palettáját. Legalább olyan fontos élenjárója, és legalább annyira egyenértékű, mint a levegő, a föld, a tenger és az űr dimenziója. Olyan elméletek kidolgozásához kezdtek, mely alátámasztja az Információs műveletek szellemi szükségességét, amely választ ad háborús kérdésekben napjaink digitális korában." [11]

Az új kor hadseregeinek lényeges jegyei közé tartoznak az automatizált irányítási funkciókkal ellátott, nagy pontosságú fegyverek, valamint hatékony felderítési, navigációs és információfeldolgozási módszerek, amelyek integrált alkalmazása már napjainkban is alapvető fontosságú az eredményes hadviseléshez.

Az aktív tevékenységek dinamikusan változó környezetében az információs fölény kialakítása és fenntartása létfontosságú a kitűzött célok eléréséhez. Ennek megfelelően, az információs műveletek (information operations) és az információs hadviselés (information

warfare) fogalmait használják annak érdekében, hogy meghatározzák azokat az eljárásokat, amelyek az információs fölény megteremtéséhez és megtartásához szükségesek.

INFORMÁCIÓS HADVISELÉS

„Az információs hadviselés az információs fölény elérése érdekében végrehajtott, a szemben álló fél információi, információalapú folyamatai, információs rendszerei és számítógépes hálózatai befolyásolására, illetve a saját információk, információalapú folyamatok, információs rendszerek és számítógépes hálózatok védelmére irányuló tevékenységek összessége.”[12]

Az információs hadviselés az ellenféllel szembeni információelőny megszerzése érdekében végrehajtott művelet. Ez abból áll, hogy ellenőrzik a saját információs terüket, megvédik a saját információkhoz való hozzáférést, miközben megszerzik és felhasználják az ellenfél információit, megsemmisítik az információs rendszereiket és megzavarják az információáramlást. Az információs hadviselés nem új jelenség, mégis innovatív elemeket tartalmaz a technológiai fejlődés hatása, amelynek eredményeként információkat terjesztenek gyorsabban és nagyobb léptékben.[13]

Az információs hadviselés önálló katonai fogalmaként az 1990-91-es Öböl-háborúk és az azt követő balkáni, majd afganisztáni konfliktusok során jelent meg először a hadviselés színterén. Később, az aszimmetrikus háború kapcsán, ahol kiderült, hogy a katonai és nem katonai szakterületek szoros kapcsolatban vannak egymással és több helyen átfedik egymást. Az éles háttér elmosódik a harctér és a hátország között. Továbbá a vezetékes és a vezeték nélküli, valamint űrkommunikációs hálózatokba kapcsolt, számítógép által vezérelt kritikus infrastruktúrák működésének korlátozása már nem csak kinetikus tűzeszközökkel (pusztító hatású légi, tüzérségi vagy rakétacsapásokkal) lehetséges, hanem nem kinetikus számítógép hálózati eszközökkel (korlátozó programokkal) is.

A hidegháború óta rendkívüli jelentősége van a technikai-hírszerzési és a technikai együttműködési rendszerek kapcsolata között, hogy ellenőrizni lehessen a szemben álló fél tevékenységét és kommunikációját. Az amerikai és brit szolgálatok kifejlesztették a tömeges lehallgatás képességét, amely lehetővé tette, hogy az Öböl-háború során először az információs hadviselés szabályai érvényesüljenek. Az újonnan megalakulkó információs háborúval, más néven vezetési háborúval (information war - command and control war), egy újszerű és teljesen eltérő módszer alakult ki a háború lefolytatására, amelyben az információs erőforrások használata kulcsfontosságúvá vált. Az úgynevezett információs hadviselés (information warfare) tartalmazza az integrált tudást tartalmazó információk megszerzését és felhasználását, valamint a küzdő felek is ezek védelme érdekében vívják meg a harcot.

Az enyhülő hidegháború és az atomerő visszaszorításával egyre fontosabbá váltak a hagyományos robbanóanyaggal felszerelt fegyverek, melyek fejlett irányítási rendszerekkel rendelkeznek, így nagy távolságról célzottan alkalmazhatóak. A rendszerek zavarása, befolyásolása vagy bénítása stratégiai előnyhöz vezethet valamelyik küzdő fél számára, mivel lehetővé teszi az érzékeny mélységi objektumok megsemmisítését. Ebben az összefüggésben azonban egy ország fegyveres agresszivitása korlátozottá válhat, mivel a saját területén lévő objektumok könnyen célpontjává válhatnak a korszerű repülő- és rakétatechnikai eszközöknek. A hidegháború alatt ez a tényező biztonsági szempontból is fontos volt, mivel elkerülte a közvetlen fegyveres konfliktus kialakulását a két nagyhatalom között és a jövőben is fontos visszatartó erőként szolgálhat. [14]

TERRORIZMUS

Az elmúlt évtizedek információs forradalma főként a csúcstechnológiával foglalkozó "infokommunikációs" szektorban tapasztalható. Az egyik ilyen példa a dróntechnológia gyors fejlődése, amely felveti a nemzetbiztonsági kockázatok és a drónok legitim felhasználásának kérdését. A terroristák gyakran használják a dróntechnológiát támadásokra, megfigyelésre, propagandavideók készítésére vagy zavarásra. Jelenleg 4 terrorszervezet rendelkezik azonosítható drónprogrammal: a Hezbollah, a Hamász, az Iszlám Állam és a Jabhat Fateh al-Sham.[15] Fontos kiemelni, hogy a terrorizmus növekedése szorosan összefügg a globalizáció és a technológiai fejlődés jelenségeivel. Az átfogó összekapcsolódásuk gyorsította az elektronikus pénzügyi átutalásokat, amelyek radikálisan átalakították a pénzügyi szektor működését, és hatással voltak a társadalmi tevékenységekre is. Az új technológiai vívmányok elterjedése széles körűvé vált, így az 1990-es évek posztindusztriális társadalmaiból az első információs társadalmak jöttek létre.

A terrorizmus elleni háború frontvonala nem mindig a háborús helyeken zajlik, hanem európa fővárosaiba, a szervereken, az összeköttetésekben. A modern harcmező mindent behálóz. Vagyis többé nem kell lövészárkokban megbújni meg bombákat kerülgetni. Minden generációnak megvan a maga hézaga amiből a következő nemzedék korrigálva a hiányosságokat prevenciós előnnyel indulhat neki a fejlesztéseknek. A cél mindig a rendszer biztonságos működésének biztosítása kell, hogy legyen.

Az új típusú katonai konfliktusok és háborúk ma már a világ szeme láttára zajlanak. Az elmúlt másfél évtizedben a katonai technológia folyamatos fejlesztése az idő és tér összesűrűsödéséhez vezetett, amelynek következtében a távoli akciók helyi hatásokat váltanak ki és fordítva. Az interdependens nemzetközi rendszer egy összekapcsolódott világrendet hozott létre, amelyben a helyi és regionális katonai fejlemények potenciálisan globális hatásúak lehetnek. A szakértők felismerték, hogy a világ bármely pontján kialakuló zűrzavar és konfliktus azonnal elérheti a globális közönséget, az információs technológia robbanásszerű terjedésének köszönhetően. A média fontossága nemcsak a nyugati nagyhatalmak és a feltörekvő államok (például Russia Today, Al Jazeera) számára nyilvánvaló, hanem a terrorista szervezetek (például ISIS) is teljes mértékben kihasználják azt. [16]

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

A terrortámadások és az erőszakkal való megfélemlítés lehetőséget biztosít a politikába való katonai beavatkozásra, az állami intézmények ellenőrzésének átvétele nélkül. Két olyan mechanizmust említ Vincenzo Bove, amelyek révén a terrorizmus befolyásolja a katonai részvételt a politikában: Amikor a terrorizmus elleni küzdelemhez és a nemzetbiztonság megerősítéséhez, valamint a fegyveres erők „bevonásához" a kormányzati hatóságoknak katonai szakértelemre van szükségük a politikához, és amikor az állam fegyveres szereplői kihasználják az információs előnyüket a civilekkel és a hatóságokkal szemben, hogy „belenyomják" magukat a politikai jelenlétbe és a politikaalkotásba.[17]

Azonban, ha az nemzetközi terrorizmus elleni küzdelemről van szó, akkor fel kell ismernünk, hogy a katonai erő alkalmazása csak egy, az összetett stratégiai eszközök között. A terrorizmus elleni küzdelem többdimenziós tevékenység, amelyet mind nemzeti, mind

nemzetközi szinten kellene összehangolni. Ideális esetben ez egy összehangolt válságreagálási stratégia lenne, amely politikai, gazdasági, diplomáciai, titkosszolgálati, adminisztratív, felderítő, rendőri és katonai megoldásokat kombinál. [18]

KIBERHÁBORÚ

A kiberhadviselés az állami szereplők által kezdeményezett kibertámadások összefoglaló neve, amelynek lényege, hogy az államok az információs technológiai fejlődést egyre gyakrabban használják fel a politikai és katonai előnyök elérésére. [19] A NATO a kiberhadviselést hadtudományi szempontból, az információs műveletek részének tekinti, amelyek célja az információs fölény elérése. Az ilyen műveletek lehetnek támadó jellegűek, amikor az ellenséges hálózatokra irányulnak, vagy védekezőek, amikor a saját rendszerek biztonságát kívánják megőrizni. Azonban fontos kiemelni, hogy a kiber-hadviselés nemzetközi jogi szempontból csak akkor értelmezhető, ha az elkövető állam kiléte egyértelműen azonosítható. [20]

Egy nemzetnek a kibertérben megnyilvánuló hatalmát a National Cyber Power Index összetett formula szerint értékeli. Olyan kritikus faktorokat vesz számításba, mint a belső csoportok megfigyelése, a nemzeti kiberbiztonsági erők megerősítése, a nemzetközi normák és szabályok kialakításában való részvétel és azok hatékony definiálása, az információs környezet szabályozása, a nemzetbiztonsági erők külföldi információgyűjtési képessége, az ellenséges kibertámadásokra való hatékony válaszlépés, valamint az ipar és a kereskedelem digitális növekedésének mértéke. [21]

A kibertér és az ehhez kapcsolódó új technológiák fontos területét képezik az információs hadviselésnek. A kiberháborús tevékenységek állhatnak kibertámadásokból, az ellenfél információs rendszereinek megsemmisítéséből, de magukban foglalhatnak úgynevezett társadalmi kibertámadásokat is, azáltal, hogy az emberek tudatában sajátos képet alkotnak meg a világról, összhangban az adott ország által folytatott információs háború céljaival. [22]

Az információs hadviselésnek azon vonatkozásai, amelyek a vezetési-fegyverirányítási és navigációs rendszerek megbontására és védelmére irányulnak, jelenleg az egyik leghatékonyabb hadviselési eljárások közé tartoznak. Az 1990-91-es Öböl-háború tapasztalatai egyértelműen igazolták a több hónapos légi és elektronikai csapások elsődleges célpontjainak - a tömegpusztító fegyvereken, repülőtereken és rakétakilövő-állásokon túl - az ellenséges felderítési (lokátor), kommunikációs és fegyverirányítási képességeinek bénítását. Az információs hadviselés másik jelentős elemének, a saját vezetési rendszer hatékony alkalmazásának köszönhetően, a szárazföldi hadműveletek során az ellenséges erők dezorganizációja, és nem pedig teljes megsemmisítése, segítette a szövetséges erőknek jelentős ellenállással szembeni sikerességüket.

Bár az Öböl-háború nem mutatta meg az információs hadviselés minden aspektusát, így például a polgári célú információs rendszerek zavarásának és bénításának gazdasági károkat okozó hatásait, vagy politikai instabilitást okozó képességeit, az elektronikus felderítésnek a siker döntő tényezőjeként bizonyult. Az elektronikai eszközökkel gyűjtött műholdas és egyéb felderítési információk hatalmas tömege egyértelműen gazdagította a hadművészet elméletét. Az elektronikai felderítés nélkülözhetetlen eleme a korszerű hadviselésnek, és bebizonyította, hogy az információs hadviselés eljárásai között az egyik legfontosabb.

Az információs hadviselés egy újfajta stratégia, amelynek célja azonos a hagyományos hadviseléssel - azaz a struktúrák megtörésével vagy megőrzésével - azonban módszerei és eszközei jelentős mértékben eltérnek a hagyományos hadviseléstől. Míg a hagyományos hadviselés főként a harcoló csapatok, a végrehajtó szakaszok, a műszaki zárrendszerek és a logisztikai bázisok megsemmisítésére összpontosít, addig az információs hadviselés elsődlegesen az alakulatok vezetési és irányítási rendszerének feltérképezésére, támadására, alkalmazására és védelmére irányul sajátos eszköz- és eljárásrendszerével.

A hagyományos és az információs hadviselés egymást kiegészítik és támogatják, azonban az információs hadviselés rendszere - mint a hadművészet egy része - fokozatosan előtérbe kerül és döntő tényezővé válik a háborúk eredményes megvívásában a társadalmak és haderők fejlődésével párhuzamosan.

„Az ellenség harcoló csapatainak pusztítása nélkül háborús körülmények között nem érhető el tartós siker. Az információs hadviselés alkalmazása azonban lehetővé teszi a győzelem kivívását lényegesen kevesebb erőforrás bevonásával, a veszteségek jelentős mérséklését, és a katonai helyzetnek a saját csapatok javára fordítását."[23]

INFORMÁCIÓS HADVISELÉS ÉS A KATONAI VEZETÉS ELMÉLETÉNEK KAPCSOLATA

Az ellenség információs hozzáférési lehetőségeinek megszüntetése önmagában csak korlátozott értékű, ha nem jár együtt a saját információs képességek kialakításának, továbbfejlesztésének és hatékony alkalmazásának szorgalmazásával. [24]

Az információs hadviselés a katonai vezetés elméletének gazdagító eleme, amelynek meghatározó területei az információfeldolgozási rendszerek fejlesztése és üzemeltetése. Az ilyen tevékenységek célja az ellenséges haderő információs folyamatainak támadása és a saját információs képességek védelme. Az információs hadviselés megköveteli a saját információs rendszer fejlesztésének és üzemeltetésének szigorú szabályozását, beleértve az információ típusát, tartalmát és formáját, az információ áramlását, feldolgozását és rendelkezésre bocsátását. A szervezetek az információs hadviselés módszereinek kidolgozásával gazdagítják a katonai vezetés elméletét, hogy hatékonyabban védelmezhessék és használhassák információs képességeiket.

Az összehangolt katonai informatikai rendszereknek képesnek kell lenniük az autonóm működésre, miközben együtt kell működniük a többnemzetiségű összhaderőnemi csoportosítás (CJTF-*Combined Joint Task Force*) más összetevőivel, hogy biztosítsák a művelet sikerét. Ezt az összehangolt rendszert "szövetségnek" nevezik, amely dinamikusan változik az információs környezet változásaihoz igazodva. Az együttműködő információs rendszerek által alkotott szövetségek összetétele nem állandó, és egy adott rendszernek más és más rendszerekkel kell interoperábilis módon együttműködnie a körülményeknek megfelelően. [25]

Specifikus szakértők képzése mellett helye lenne átfogó és központosított információbiztonsági rendszerek és berendezések folyamatos fejlesztésének és erősítésének, mely a szolidarizmus jegyében képesek azonnali végrehajtások megosztására és biztosítani tudják az összehangolt nemzetközi cselekvőképességet a reziliencia, a versenyképesség és a digitális autonómia megerősítése jegyében.

INFORMÁCIÓS HÁBORÚ ÉS AZ INTERNET KAPCSOLATA

Az Internet kibővíti az adatgyűjtés lehetőségeit és spektrumait, illetve az információvédelem és az információ megzavarásának lehetőségeit. Megkönnyíti az adott ország állampolgárainak és a nemzetközi közösség tagjainak a részvételt ebben a játszmában a világ bármely pontjában tekintettel a kommunikáció sebességére.

A közösségi oldalak értékes információforrást jelentenek azokról a célcsoportokról is, amelyeknek a félretájékoztatási szándék címezve van. Ennek megfelelően az Információs hadviselés felhasznál:

- úgynevezett trollgyárakat. Ezek szervezetek, akik a célnak megfelelően lobby kommenteket tesznek közzé hamis profilok felhasználásával a közösségi médiában.
- Felhasznál továbbá botokat. Ez egy úgynevezett automatizált hírlevélküldő program, ami bizonyos kulcsszó megjelenésekre generálja üzeneteit.
- Továbbá felhasznál hamis híreket a médiafelhasználók félrevezetésére/dezinformációjára.[26]

A médiahasználók az úgynevezett hagyományos média segítségével áldozatává válnak az internetes sebezhetőség széles spektrumának az információs háborúban. A propaganda kampányok és a dezinformációk számos médiaüzenetben kódolva vannak, beleértve a hagyományos- és a közösségi médiát is. A médiahasználók egyre inkább tudatában vannak ennek a dezinformációs tevékenységnek, amelyek a valóság felfogásának befolyásolására irányulnak.

Az orosz elképzelésekben az információs hadviselésnek két fő – egymást kiegészítő oldala – létezik: „az információs-technikai és az információs-pszichológiai hadviselés. Az információs-technikai hadviselés döntően a nyugati terminológia szerinti számítógéphálózati hadviselést és az elektronikai hadviselést foglalja magában, beleértve az információs rendszerek technikai eszközökkel történő támadását vagy védelmét. Az információs-pszichológiai hadviselés pedig a közvélemény és a tömegek tudatának befolyásolását, a kognitív folyamatok manipulálását, a politikai és katonai döntéshozatali folyamatok lassítását és bénítását, végül a kedvező politikai hatások kiváltását célozza.” [27]

Talán az Információ a legújabb harci dimenzió a fegyveres erők között. Sok elmélet szól arról, hogy egy információs korszak kezdetén vagyunk. Ugyan megváltoztak a harcászati eszközök, a végső cél ugyanaz maradt: meghódítani az ellenfelet. Az információs kor új lehetőségeket, és ezzel együtt új célpontokat is teremtett, ami megváltoztatja a 21. század háborúinak a harcmódját.

Például mi történik, amikor az új harcmező határvonalává az információ válik, amelyek alapján a parancsnokok meghozzák kritikus döntéseiket? György Gilder, a The Quantum Revolution in Economics and Technology szerzője elmondta: „a legértékesebb tőke napjainkban az emberi elme és a szellemi tőkéje.” [28]

Gordon Sullivan tábornok szerint „az információ, a győzelem valutája a hadszíntéren.”[29] Az információ értékes, de csak akkor hasznos, ha megfelelően kommunikáljuk. A hatékony kommunikáció nem csak azt jelenti, hogy az információhoz hozzáférünk, hanem azt is, hogy megosztjuk a megfelelő emberekkel. A kommunikáció fő célja az információ közzététele, amely meghatározza annak jelentőségét és értékét. [30]

Az információgyűjtés ma már nem csupán az általunk önkéntesen megadott információkból áll. Az internet világában nincsenek ingyenes dolgok - a meséktől kezdve az alkalmazásokon át a szolgáltatásokig mindenért valamilyen formában fizetünk, akár csak az adatainkkal is. A mobiltelefonok rögzítik az általunk felkeresett helyeket, keresési szokásainkat, míg a hűségkártyáink nyomon követik vásárlási szokásainkat. Mindennapi tevékenységeink során jelentős mennyiségű adatot termelünk, amelyek nagy része automatikusan felkerül a felhőbe. Az adatszerver tulajdonosa teljes hozzáférést biztosít az adatokhoz, amelyeket adatbrókerek harmadik felek részére el is adhatnak. [31]

Az elmúlt években bekövetkezett technológiai előrelépés lehetővé tette az információs hadviselés számos formájának alkalmazását, amelyek révén emberek milliói célponttá válhatnak valós időben, bármilyen nyelven és országhatártól függetlenül. A folyamatos technikai fejlődés - kiterjesztett és virtuális valóság technológiája, mesterséges intelligencia fejlesztések, propagandaterjesztés automatizált lehetőségei, úgynevezett personal management szoftverek - valószínűleg növelni fogja az információs technológiák szerepét a stratégiai célok eléréséhez szükséges versengésben. [32]

FELHASZNÁLT IRODALOM

[1] https://www.britannica.com/topic/security

[2] Szenes Zoltán: Katonai biztonság napjainkban. Új fenyegetések, új háborúk, új elméletek 70-104.old. https://m2.mtmt.hu/api/publication/3258112 Finszter G. Biztonsági kihívások a 21. században. (2017) ISBN:9786155680502

[3] U.o.

[4] Az EU Tanácsa: Kiberbiztonság Európában; Infojegyzet, 2016/44; Inforkörkép, 2018
https://www.parlament.hu/documents/10181/1789217/Infojegyzet_2019_49_Kiberhadviseles.pdf/11686cc6-54a5-8388-87db-54233ab8a32d?t=1573810309857 , ORSZÁGGYŰLÉS http://industry4.hu/hu/fogalomtar/digitalis-forradalom

[5] Global Terrorism Index 2020: A terrorizmus hatásának mérése. https://reliefweb.int/sites/reliefweb.int/files/resources/GTI-2020-web-2.pdf

[6] Dr. Haig Zsolt, Dr. Várhegyi István: A vezetési hadviselés alapjai http://www.bibl.u-szeged.hu/bibl/mil/konyvek/elmelet/info/h/haig2_i.html

[7] Dr. Haig Zsolt és Dr. Várhegyi István Információs műveletek: Információs korszak hadügyi forradalma és információs rendszerei, Zrínyi Miklós Nemzetvédelmi Egyetem 2004-es számú egyetemi jegyzet

[8] Takács Gergely: Big Data (adatvezérelt) elemzési módszerek alkalmazása a nemzetbiztonsági szférában, A Terrorelhárítási Központ Tudományos Tanácsának 2018/1- es számú folyóirata, 7. évfolyam 1. szám http://epa.oszk.hu/02900/02932/00016/pdf/EPA02932_terror_elharitas_2018_1.pdf

[9] U.o

[10] Wayne M. Hall, "Information Operations: Military Competition," Cyber Sword: The Professional Journal of Joint Information Operations 4, no. 1 (Spring 2000): 6. http://www.iwar.org.uk/iwar/resources/cybersword/Dragon_R_A_01.pdf

[11] Muha Lajos: Fogalmak és definíciók, 2004 [In.: Az informatikai biztonság kézikönyve (szerk.: Muha Lajos), Budapest: Verlag Dashöfer Szakkiadó, ISBN 963 9313 12 2]

[12] Defence Education Enhancement Programme (DEEP): Media, (Dis)Information and Security https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf
[13] Szabó András: Az információs hadviselés, Magyar Hadtudományi Szemle 1998 VIII. évfolyam 8. szám http://mhtt.eu/hadtudomany/1998/ht-1998-4-5.html
[14] Dr. Kis-Benedek József nyá. Ezredes: A nemzetközi terrorizmus jelenlegi tendenciái Európában, Felderítő Szemle , Katonai Nemzetbiztonsági Szolgálat XVIII. évfolyam 3. szám https://www.knbsz.gov.hu/hu/letoltes/fsz/2019-3.pdf
[15] Finszter G. Biztonsági kihívások a 21. században. (2017) ISBN:9786155680502 https://www.uni-nke.hu/document/uni-nke-hu/3.%20Szenes%20k%C3%B6nyv,%20k%C3%B6nyvr%C3%A9szlet.pdf
[16] Vincenzo Bove: Beyond coups: terrorism and military involvement in politics: European Journal of International Relations 2020, Vol. 26(1), DOI: 10.1177/1354066119866499 https://journals.sagepub.com/doi/pdf/10.1177/1354066119866499
[17] Dr. Szternák György, Dr. Szternák Nóra, Dr. Bolgár Judit: A terrorizmussal kapcsolatos kutatások legújabb eredményei. Felderítő Szemle , Katonai Nemzetbiztonsági Szolgálat 2005 IV. évfolyam 4. szám https://www.knbsz.gov.hu/hu/letoltes/fsz/2005-4.pdf
[18] Szathmáry Zoltán: Bűnözés az információs társadalomban – Alkotmányos büntetőjogi dilemmák az információs társadalomban. PhD értekezés. https://pea.lib.pte.hu/bitstream/handle/pea/16033/szathmary-zoltan-tezis-hun-2013.pdf?sequence=2&isAllowed=y
[19] Berki Gábor: Kiberháborúk, kiberkonfliktusok. In: Pintér István (szerk.) A virtuális tér geopolitikája. Geopolitikai Tanács, 2016. 260–264. old. HU ISSN 1788-7895. ISBN 978-963-9816-34-3. https://mek.oszk.hu/16100/16182/16182.pdf
[20] Julia Voo, Irfan Hemani, Simon Jones, Winnona DeSombre, Dan Cassidy, Anina Schwarzenbach: National Cyber Power Index (NCPI) 2020, Harward Kennedy School Belfer Center for Science and International Affairs, https://www.belfercenter.org/publication/national-cyber-power-index-2020
[21] Defence Education Enhancement Programme (DEEP): Media, (Dis)Information and Security https://www.nato.int/nato_static_fl2014/assets/pdf/2020/5/pdf/2005-deepportal4-information-warfare.pdf
[22] Szabó András: Az információs hadviselés, Magyar Hadtudományi Szemle 1998 VIII. évfolyam 8. szám http://mhtt.eu/hadtudomany/1998/ht-1998-4-5.html
[23] Marc Loi: New equipment gives Reserve MP Soldiers resources to succeedhttps://www.army.mil/article/97665/New_equipment_gives_Reserve_MP_Soldiers_resources_to_succeed
[24] Munk Sándor : Katonai informatikai rendszerek interoperabilitásának aktuális hadtudományi kérdései. MTA Doktori értekezés https://core.ac.uk/download/pdf/35134477.pdf
[25] NATO Standard AJP-6, Allied joit Doctrine for Communication and Informatin Systems, Edition A Version 1. 2017 https://www.coemed.org/files/stanags/01_AJP/AJP-6_EDA_V1_E_2525.pdf

[26] Thomas Timothy L.: Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts? The Journal of Slavic Military Studies, 2014
[27] 3 Joint Pub 6-0, Doctrine for Command, Control, Communications, and Computer (C4) Systems Support to Joint Operations, 30 May 95, I-3 https://nsarchive.gwu.edu/sites/default/files/documents/5628050/Joint-Force-Joint-Pub-6-0-Doctrine-for-Command.pdf
[28] Kranzieritz Veronika Marketing információs rendszerek alkalmazhatósága a pszichológiai műveletek vezetés-irányítási folyamatában1 DOI 10.17047/HADTUD.2019.29.E.11 HADTUDOMÁNY, 2019. ÉVI ELEKTRONIKUS LAPSZÁM http://mhtt.eu/hadtudomany/2019/2019e/2019ekranzieritz.pdf
[29] Haig Zsolt: Információ – társadalom – biztonság. Budapest, NKE Szolgáltató Kft., 2015. 8., https://www.uni-nke.hu/document/uni-nke-hu/kritikus_infrastrukturak.pdf
[30] Horváth-Sántha Hanga1 Milipol Asia Pacific 2019 – A délkelet-ázsiai térség legjelentősebb belügyi és biztonságpolitikai konferenciájának összefoglalója, Hadtudományi Szemle • 12. évfolyam (2019) 4. szám http://real.mtak.hu/109468/1/HSZ_2019_4_05-Horvath-Santha-45-60.pdf
[31] Fekete Csanád: Az információs hadviselés orosz koncepciójának fejlődése a hidegháború végét követően, Hadtudományi szemle 11. évf. 3. sz. (2018.)
[32] Erdész Viktor: A mesterséges intelligencia felhasználási lehetőségei a korszerű nemzetbiztonsági hírszerző elemzés-értékelésében, Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola Doktori értekezés https://hdi.uni-nke.hu/document/hdi-uni-nke-hu/erdesz_viktor_ertekezes_tervezet.pdf

RECOMENDATIONS FOR THE RADIATION PROTECTION OF HIGH PERFORMANCE LASER EQUIPMENT

AJÁNLÁSOK NAGY TELJESÍTMÉNYŰ LÉZERBERENDEZÉSEK SUGÁRVÉDELMÉHEZ

BODOR Károly[1] – ZAGYVAI Péter[2]

Abstract

During laser-matter interactions, accelerated particles may be emitted, which upon leaving the experimental equipment may activate materials/objects in their surroundings, e.g. radiation protection shields. As a result of activation, so-called hotspots may develop, where a higher dose field than that of the background radiation will be measurable in the long run. This is the space where pieces detaching from the target must be found and identified. In this work, I examine the processes occurring in the target and estimate the values of the expected braking radiation by extrapolation. I formulate recommendations and present the training site where searching for hotspots can be practiced under real conditions.

Keywords

Radiation protection, high power laser facility, training site, FOSTER, Reflux

Absztrakt

A lézerfény és az anyag kölcsönhatása során gyorsított részecskék is keletkezhetnek, amelyek a kísérleti berendezést elhagyva felaktiválhatják a környezetükben megtalálható anyagokat, például a sugárvédelmi árnyékolókat. A felaktiválódás hatására ún. forró pontok (hotspot-ok) alakulnak ki, ahol hosszabb távon a háttérsugárzásnál magasabb dózistér mérhető. Ebben a térben kell megtalálni és azonosítani a céltárgyról leváló darabokat. Ebben a cikkben megvizsgálom a céltárgyban létrejövő folyamatokat és extrapolációval becsülöm a várható fékezési sugárzás értékeit. Ajánlásokat teszek, valamint bemutatom a tanpályát, ahol lehetőség van valós körülmények között gyakorolni a hotspot keresést.

Kulcsszavak

Sugárvédelem, nagy teljesítményű lézerberendezés, tanpálya, FOSTER, Reflux

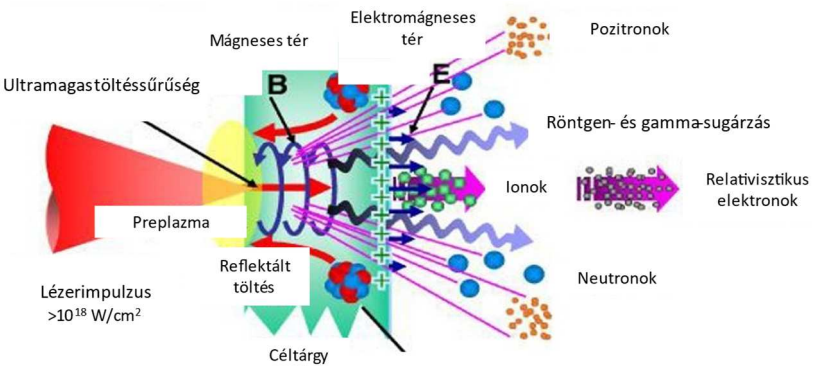
[1]Karoly.Bodor@eli-alps.hu | ORCID: 0000-0002-1612-8207| Radiation protection expert, ELI ALPS, ELI-HU Non-Profit Ltd.| Sugárvédelmi szakértő, ELI ALPS, ELI-HU Nonprofit Kft.
[2]Peter.Zagyvai@eli-alps.hu|ORCID: 0000-0002-8121-8452| Radiation protection advisor, ELI ALPS, ELI-HU Non-Profit Ltd.| Sugárvédelmi tanácsadó, ELI ALPS, ELI-HU Nonprofit Kft.

BEVEZETŐ

A nagy teljesítményű lézerberendezések különleges sugárvédelmet igényelnek, mivel a hagyományos radioaktív sugárforrásokhoz, illetve az ionizáló sugárzást létrehozó, de radioaktív anyagot nem tartalmazó berendezésekhez képest eltérő ionizáló folyamatok játszódnak le. A sugárvédelmi ajánlások pontos meghatározásához fontos tisztában lenni azzal, hogy mi történik a lézerfény-anyag kölcsönhatásakor, mi történik a néhány mikrométer vastagságú céltárgyakkal, illetve milyen felaktiválódási folyamatok mehetnek végbe.

A LÉZERFÉNY-ANYAG KÖLCSÖNHATÁS

Nano-, piko- és femtoszekundumos lézerimpulzusokat már viszonylag régóta használnak az anyagmegmunkálás területén (pl. impulzus lézeres abláció). A lézerimpulzussal való besugárzás hatására a néhány mikrométer vastagságú céltárgy felületéről távozó anyag ún. ablációs felhőt alkot. A gerjesztett elektronok egy része kilép a céltárgy felületéből, egy másik része pedig bediffundál annak belsejébe, így a felületen lokálisan megnő a pozitív ionok sűrűsége. Ha az ionok közötti taszítás meghaladja a rács kötéseinek erősségét, akkor a kötések felszakadnak, és ún. Coulomb-robbanás következik be. A robbanás következtében a felületből nagy energiájú (az ionizáló sugárzások csoportjába sorolandó) részecskék lépnek ki, valamint UV-, röntgen-, valamint látható fény tartományú elektromágneses sugárzás keletkezik (1. ábra), [4 pp. 3-12].



1. ábra: A lézerfény-anyag kölcsönhatásából keletkező másodlagos részecskék [1]

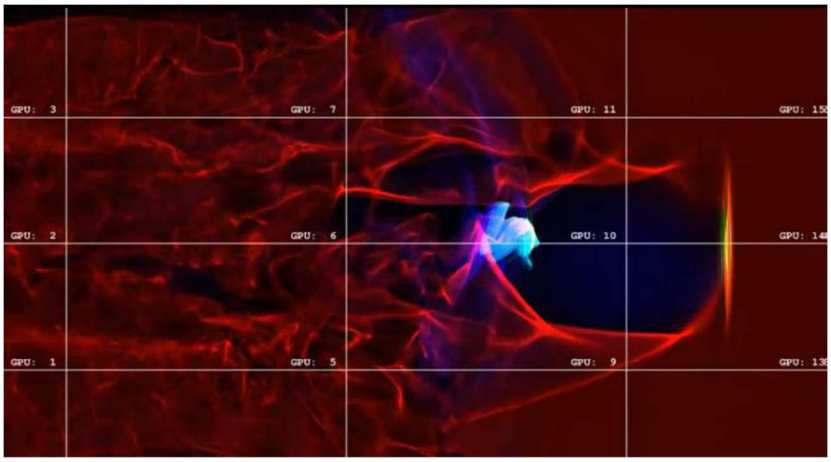
Az attoszekundumos impulzusok előállítása két lépésben történik. A lézerelven kelthető legrövidebb impulzus a femtoszekundumos nagyságrendbe esik, ezt felerősítik és ráfókuszálják a céltárgyra. Amikor az ultrarövid impulzus eltalál egy atomot, az intenzív elektromos tér kiszakítja a leggyengébben kötött elektront a kötött állapotból és eltávolítja az atomtól. Viszont a térerősség irányának fordulásakor az elektron visszatér az atom közelébe és a mag mellett való elhaladásakor egy attoszekundumos röntgen impulzust bocsát ki.

Mi történik a céltárgyban?

A nagy teljesítményű lézerimpulzusok alkalmazásakor a néhány mikrométer vastagságú céltárgyban az abláció folyamán létrejövő, „forró" elektrongáz a részecskegyorsítás kiinduló pontja. A kialakuló gyorsító térerősség eléri a TV/m-es nagyságrendet. A kísérletek során a lézernyalábot egy néhány μm vastagságú céltárgyra fókuszálják. A lézerimpulzus által felgyorsított elektronok kollimált nyaláb formájában áthaladnak a céltárgyon, miközben olyan elektromágneses teret hoznak létre, amely a pozitív töltésű ionokat és protonokat a nyaláb irányában gyorsítja. A kísérlet folyamán a céltárgy lézerrel ellentétes oldalán a felületre merőlegesen kilépő, nagy energiájú, kollimált elektron- és protonnyalábot figyeltek meg. A protonok feltételezhetően a céltárgyban, illetve a felületen jelenlévő vízmolekulák hidrogénjeiből származnak.

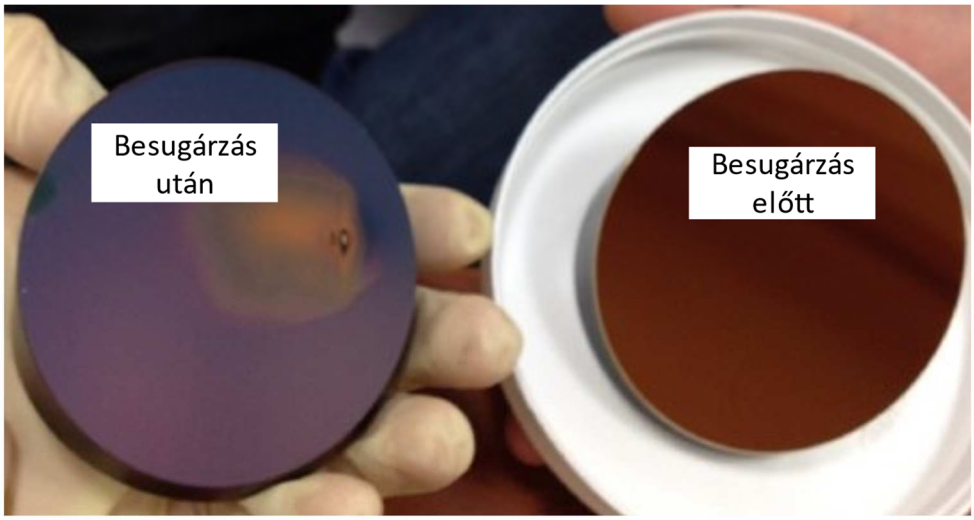
A néhány mikrométer vastagságú céltárgy elektronjainak lézeres gyorsításában több kölcsönhatási folyamat is szerepet játszik. Ahhoz, hogy a részecskék megfelelő mértékben fel tudjanak gyorsulni, a lézer transzverzális elektromágneses terét longitudinális térré kell alakítani, amely hatására az elektronok egy irányban mozogva gyűjtik össze az energiát. Ez a folyamat a plazmában jöhet létre. A lézerfény elektromágneses tere elmozdítja az elektronokat a tér irányában, míg a magok a sokkal nagyobb tömegük miatt mozdulatlannak tekinthetőek. Az elektronfelhő transzverzális irányú oszcillációja miatt periodikus töltéssűrűség változás jön létre, amely nagy sebességű longitudinális plazmahullámként halad tovább. Az így kialakuló sűrűség perturbáció longitudinális irányú elektromos térerősséget hoz létre, ami már képes nyaláb irányában gyorsítani az elektronokat.

A nagy energiájú, kollimált és kvázi-monokromatikus részecskenyaláb előállítását az ún. buborék gyorsítás teszi lehetővé (2. ábra), amelyet 2002-ben fedeztek fel szimulációk alapján, majd ugyanabban az évben kísérletileg is kimutattak. A buborék gyorsítás létrejöttéhez szükséges lézerimpulzus elég nagy ahhoz, hogy a plazmahullám már az első oszcilláció után a tengely felé törjön. A folyamatos törések miatt a hullámfront meggörbül, majd összezáródik és egy „buborék" alakul ki, amely csapdába ejti és felgyorsítja az elektronokat. A lézerimpulzus néhány MeV energiájú elektronokat tol maga előtt, míg a buborék mögött csökken az elektronsűrűség. A buborék közepén csapdába ejtett, kvázi-monokromatikus elektronok sűrűsége a legnagyobb, miközben az energiájuk elérheti a GeV-es nagyságrendet. A buborék igen stabil, a plazma hullámhossz százszorosának megfelelő utat is megtehet. Az anyagi és geometriai jellemzők megfelelő megválasztásával a lézerfény energiatranszfer hatásfoka elérheti a 15%-ot.



2. ábra: A buborék gyorsítás szimulációja, az elektronsűrűség a sötétebb árnyalatok felé csökken, a kékkel jelölt részen „esnek csapdába" az elektronok [2]

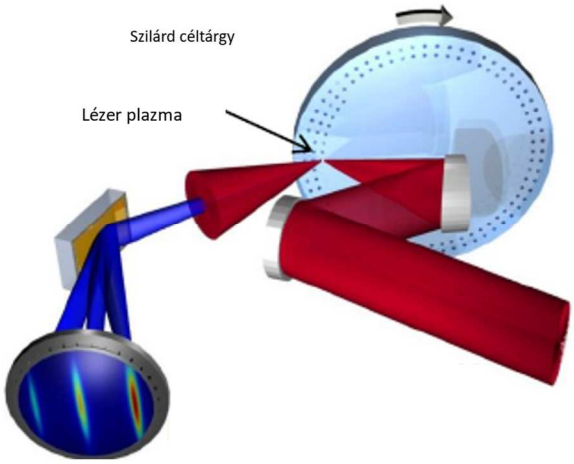
Az alábbi 3. ábrán egy néhány mikrométer vastagságú szilárd céltárgy látható lézerfény általi besugárzás után és besugárzás előtt:



3. ábra: Besugárzás előtti, utáni szilárd céltárgyak [3]

SZILÁRD CÉLTÁRGY BESUGÁRZÁSA

A néhány µm vastag szilárd céltárgyat egy precíziós léptetőmotor forgatja a besugárzások időtartama alatt (4. ábra). A femtoszekundumos lézerimpulzussal való besugárzás hatására a céltárgy felülete megolvad, az anyag egy része el is párolog. Ablációs plazmafelhő alakul ki, ezen felhők paraméterei eltérőek a hosszabb lézerimpulzusok során létrejövő ablációs felhőkétől, [4 pp. 3-12].



4. ábra: Szilárd céltárgy besugárzása [1]

A lézerimpulzus primer energiája a besugárzott céltárgy felületén abszorbeálódik. Az igen rövid lézerimpulzus miatt, a besugárzási pontban keletkező magas hőmérséklet és a céltárgy további része között nincs hőmérsékleti kiegyenlítődés. Hosszabb, pl. nanoszekundumos impulzusoknál már van elég idő a hőmérséklet kiegyenlítődésre. A céltárgy hőmérséklet kiegyenlítődéséhez ezerszer több időre van szükség, mint a femtoszekundumos lézerimpulzus ideje. A besugárzott céltárgy vagy annak részei elpárologhatnak, illetve megolvadnak a hőmérsékletváltozás végett, [4 pp. 3-12].

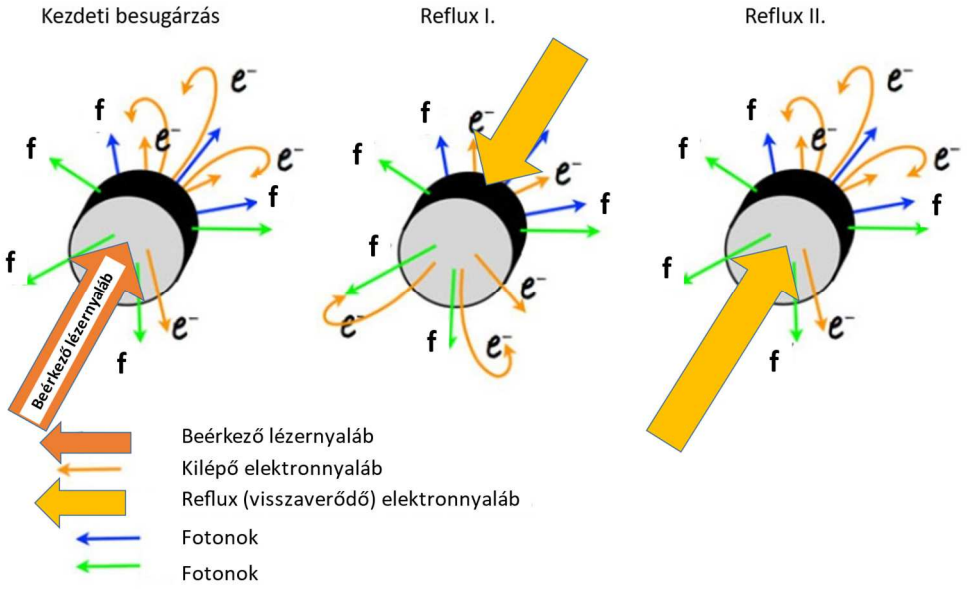
A céltárgyban (pl. amikor a céltárgy anyaga alacsony szublimációs- és olvadáspontú) a folyamatos nagy intenzitású lézerfény besugárzás hatására mechanikai feszültségek alakulnak ki a részleges elpárolgás és olvadás hatására. Az olvadás során a gázként elpárolgó céltárgy darabok az olvadékban csapdába kerülhetnek és a megolvadt céltárgy gázbuborékokat tartalmazhat, mely szintén rideggé teszi a céltárgyat. A „forrásban lévő" céltárgyban keletkező gázbuborékok folyadékcseppeket lökhetnek ki a céltárgyból, a szakirodalom ezt fázisrobbanásnak nevezi, [4 pp. 3-12].

Továbbá a céltárgy deformálódik és belső repedések alakulnak ki. Kellően nagy energiájú lézerfény impulzus hatására a céltárgy felületi rétege elpárolog és a gázállapotú részecskék a besugárzó térben létrehozott vákuumban nagy sebességgel terjedhetnek. Az ablációs felhő keletkezése során először elektronok, ezt követően a pozitív töltésű ionok szakadnak le a céltárgy felületéről. Az abláció során ún. plazma tükör effektus lép fel, mely során a (nagy sűrűségű elektron felhő) ablációs felhő visszaveri a besugárzott lézerfény egy részét, [4 pp. 3-12].

A fentiek alapján látható a besugárzott céltárgy kezelése nagy körültekintést igényel, mivel kisebb rázkódásra, ütésnek, mechanikai behatásnak kitéve a céltárgy apró darabokra töredezhet a besugárzó kamrában, illetve annak környékén a kiszedési procedúra során. A céltárgy darabkák elszennyezhetik ezen területeket. Emiatt fontos a szakemberek számára, hogy besugárzatlan céltárgyak kiszedésével gyakorolhassanak, valamint a baleseti szcenáriókra is felkészülhessenek.

Elektron reflux

A fentiekben ismertetett módon a primer lézerimpulzus plazmát generál a céltárgy felszínén. A céltárgynak a beérkező lézernyalábbal ellentétes oldalon lévő felszínét elérve az elektronok egy része távozik, ezért a fennmaradó töltéskülönbség fékezi a további elektron kiszakadást, illetve visszafordítja az elektronnyaláb „maradékát", a folyamat többször megismétlődik, ún. elektron oszcilláció, reflux alakul ki (5. ábra).



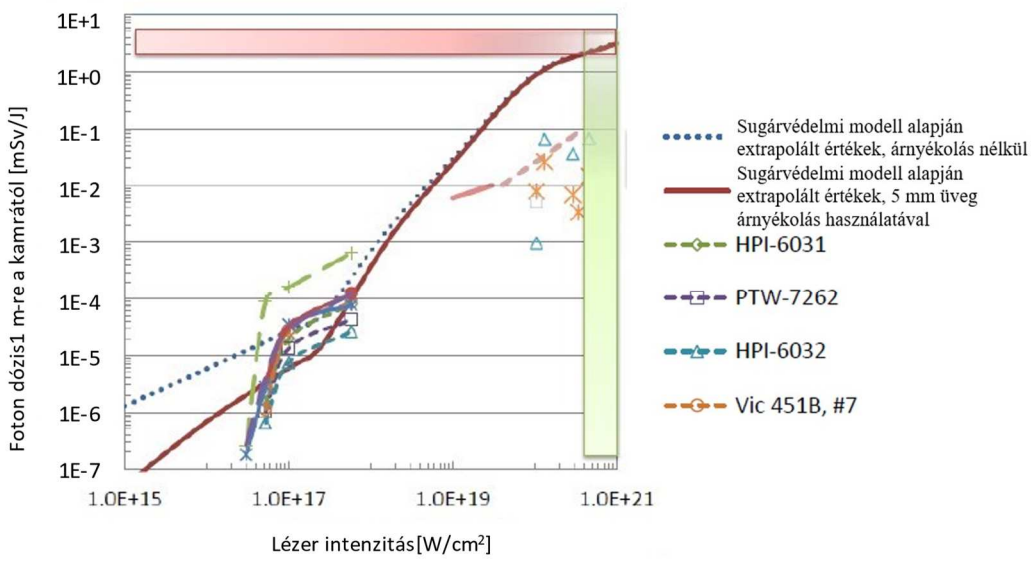
5. ábra: A céltárgyban kialakuló elektron reflux folyamata [saját szerkesztés]

Vékony, hidrogéntartalmú céltárgy esetén (1-2 µm) a gyors elektronok „átrepülnek" a céltárgyon, jelentékeny energiaveszteség nélkül, majd a hátsó felületen lévő felszínből protonokat szakítanak ki.

Vastagabb céltárgy esetén (>10 µm) a céltárgy már nem „átlátszó" az elektronok szemszögéből, az energiaveszteség jelentősebb, ennek során fékezési röntgensugárzás keletkezik. Ha ezek energiája meghaladja az 1,2 MeV-ot, a fotonok útjába eső anyagok (kamrafal, árnyékolás stb.) rendszámától függő mértékben párkeltés is bekövetkezik. Minél nagyobb a reflux mértéke, annál intenzívebb röntgenfluxus is keletkezik. Azaz alacsony elektron energiákon és vastag céltárgy esetén a reflux nem effektív, mivel az elektronok többsége abszorbeálódik az anyagban, és a kiváltott röntgensugárzás sem intenzív. Vékonyabb céltárgy esetén hatékonyabb a reflux, a nagyobb rendszámú anyagok több röntgent generálnak.

A működő berendezéseknél végzett (SLAC National Accelerator Laboratory) $10^{15\text{-}17}$ W/cm^2 lézer intenzitású besugárzások során a lézerfény-anyag kölcsönhatástól 1 méterre elhelyezett detektorokkal mért prompt foton dózisok extrapolációjával becsülhető, amennyiben a kamrák anyaga azonos minőségű és vastagságú a 10^{21} W/cm^2 lézer intenzitásnál várhatóan kialakuló prompt röntgenfoton-dózisterek értéke, a besugárzó kamra környékén a céltárgyban bekövetkező elektron reflux hatására (6. ábra). A 6. ábrán a piros és a kék szaggatott görbe az elméleti extrapolációs értékeket mutatja, míg a többi

jelzés meglévő berendezéseknél különféle termolumineszcens dózismérőkkel (TLD) mért értékeket ábrázol.



6. ábra: 10^{21}W/cm^2 lézer intenzitásnál várhatóan kialakuló prompt röntgenfoton-dózisterek értéke a besugárzó kamra körül [5]

A 6. ábra alapján becsülhető, hogy maximum 6 mSv/J dózis mérhető egy lövéstől a céltárgytól 1 m távolságban. Figyelembe véve a lövésenkénti 40 J energiatartalmat és a 10 Hz-es ismétlési frekvenciát, a prompt foton-dózisteljesítmény a besugárzás alatt elérheti a 2,4 Sv/s értéket! Emiatt a besugárzó termekbe való bejutást a kísérletek alatt meg kell akadályozni, vagy hatékony árnyékolást kell kiépíteni.

A céltárgy és környezetének felaktiválódása

A lézerfény-anyag kölcsönhatás során a lézerfény nagy elektromágneses térereje gyorsított elektron- és protonnyalábokat hoz létre, melyek a céltárgyat körülvevő anyagokkal és az árnyékoló anyagokkal való kölcsönhatásuk során elektromágneses és hadron-kaszkádot hoznak létre. Az elektromágneses kaszkád során ún. óriás rezonancia neutronok is keletkeznek. A hadron-kaszkád során a rugalmatlan ütközések hatására felaktiválódó anyagok minősége, ezáltal felezési ideje igen változatos lehet. A proton aktivációhoz küszöb energia szükséges (>100 MeV), emiatt a protonok és az árnyékoló anyagok és a céltárgyat körülvevő anyagok közötti kölcsönhatásakor jellemzően azok felszínét és felszín közeli részeit aktiválják fel. Az aktivációs hatáskeresztmetszetek anyagonként különbözők. Az anyagi minőség részletes ismerete nélkül is lehetséges azonban közelítő becsléseket tenni. G. R. Stevenson közleményében a nagy energiájú protonok szóródása során várható rugalmatlan ütközések számára (N) és az adott protonhozammal elérhető aktivitás maximumára (A_{max}) adott meg hangsúlyozottan empirikus összefüggéseket, megjegyzendő az aktiváció valószínűsége a besugárzott anyag sűrűségétől is függ, minél nagyobb a sűrűség annál nagyobb az aktiváció valószínűsége [6]:

$$N \sim E_p(GeV) \cdot 3 \qquad (1)$$

$$A_{max}(Bq) \sim E_p(GeV) \qquad (2)$$

A felaktiválódott céltárgy és céltárgy körüli anyagok reziduális (tehát a besugárzás befejezését követően is egy ideig fennálló) dózisteljesítményére (D*(t)) is közölt becslést a szerző. Eszerint D*(t) arányos a besugárzás fluensével, a besugárzási idővel, valamint a besugárzás utáni eltelt relaxációs, ún. hűlési idővel [6].

$$D^*(t) = B \cdot \varphi \cdot ln\ \frac{(T+t)}{t} \ (3),$$

ahol

T: besugárzási idő [s]

t: hűlési idő [s]

B: arányossági tényező [Sv · cm^2/részecske · s]

φ: besugárzási fluens [részecske/cm^2]

Ha t>>T, akkor $D^*(t) = B \cdot \varphi \cdot \left(\frac{T}{t}\right) \sim \frac{1}{t}$, azaz a dózisteljesítmény fordítottan arányos a hűtési idővel.

Ha T>>t, akkor $D^*(t) = B \cdot \varphi \cdot (lnT - lnt)$, azaz, ha nő a besugárzási idő, akkor a dózisteljesítmény logaritmikusan csökken a hűlési idővel.

A kis rendszámú anyagokban az empirikus közelítés szerint főleg rövid felezési idejű pozitron bomló izotópok keletkeznek. Ez alól kivétel a ^{16}O-ből keletkező ^{7}Be [6].

A kaszkád effektus során keletkező óriás rezonancia neutronok is képesek a céltárgyat és annak környékét (pl. besugárzó kamra és a kamrában elhelyezett különféle berendezések, alkatrészek) felaktiválni neutron aktivációval, mely során béta bomló izotópok keletkezhetnek. A felaktivált vékony céltárgy bétasugárzásából fakadó reziduális dózisteljesítmény a felületből kilépő béta-részecskék számával és energiájával arányos, a kilépő részecskék számát az önabszorpció csökkenti. A gamma sugárzás reziduális dózisteljesítménye a felületből kilépő gamma fotonok számával és a fotonok energiájával arányos.

Szintén Stevenson becslése alapján neutron aktivációval a vékony felaktivált céltárgyak esetén a levegőben kialakuló béta- és gamma-dózisteljesítmények (D_{beta} és D_{gamma}) az alábbi egyenletekkel közelíthetők [6]:

$$D^*_{\beta-}\left(\frac{Sv}{s}\right) = 1{,}6 \cdot 10^{-10} \cdot N_\beta \left(\frac{db}{cm^2 \cdot s}\right) \cdot \left(\frac{dE}{dx}\right)_\beta \qquad (4)$$

$$D^*_\gamma\left(\frac{Sv}{s}\right) = 1{,}6 \cdot 10^{-10} \cdot N_\gamma \left(\frac{db}{cm^2 \cdot s}\right) \cdot E_\gamma \cdot \mu \qquad , (5)$$

ahol:

$D^*_{\beta-}$: A céltárgy felületén mérhető béta-sugárzásból származó dózisteljesítmény [Sv/s]

D^*_{γ}: A céltárgy felületén mérhető gamma-sugárzásból származó dózisteljesítmény [Sv/s]

N_β: A másodpercenként 1 cm^2 felületen kibocsátott β- részecskék száma [$\frac{db}{cm^2 \cdot s}$]

N_γ: A másodpercenként 1 cm^2 felületen kibocsátott γ-részecskék száma [$\frac{db}{cm^2 \cdot s}$]

$\left(\frac{dE}{dx}\right)_\beta$: Átlagos energiaveszteség [MeV·cm^2/g]

E_γ: Átlagos fotonenergia [MeV]

μ: A céltárgy súlyozottan átlagolt fotonenergiához tartozó tömeggyengítési együtthatója [cm^2/g]

Például, ha $\frac{N_\beta}{N_\gamma} = 1$ és $\left(\frac{dE}{dx}\right)_\beta$ értéke 2, valamint E_γ=1 MeV és μ=0,03, akkor a becslés szerint $D^*_{\beta-}/D^*_{\gamma}$=70. Azaz a felszínen mért béta-dózisteljesítmény 70-szer nagyobb, mint a gamma-sugárzásból származó dózisteljesítmény.

A béta/gamma reziduális dózisteljesítmény aránya a céltárgy rendszámának, illetve vastagságának növelésével csökken a béta-sugárzás önabszorpciójának növekedése miatt. Igen vékony (vastagság <0,1 mm), kis rendszámú céltárgy esetén az arány a céltárgy felszínén az elvégzett mérések alapján jellemzően 50-szeres is lehet Stevenson megállapítása alapján, melynek érvényességét egy valós helyzetben a keletkező radioaktív anyagok minőségének ismeretében lehet csak igazolni [6]. A céltárgyhoz közeledve a béta-sugárzás értéke többszörösen felülmúlhatja a gamma-dózisteljesítményt, emiatt a céltárgyakat csak távtartóval szabad megfogni, illetve automata robotkarral, valamint a céltárgyat érdemes megfelelő árnyékolással ellátott szállító konténerbe helyezni (7. ábra).

7. ábra: Automata robotkar a céltárgyak elhelyezésére és kivételére a besugárzó kamránál, valamint árnyékolással ellátott szállító konténer [saját szerkesztés]

Indukált (mesterséges) radioaktivitás a céltárgyon kívül

A céltárgyakon kívül a besugárzó termekben elhelyezett berendezések, eszközök, köztük az árnyékoló elemek anyagaiban is keletkezhetnek radioaktív nuklidok a lézerfény-anyag kölcsönhatásából adott esetekben közvetve származó tercier neutron (óriás rezonancia neutron) részecskesugárzás hatására. A neutron indukált felaktiválódás mértéke az alábbi egyenlettel számolható:

$$A(t)=\lambda \cdot N_{rad}(t)=\sigma \cdot \varphi \cdot N_{target} \cdot [1-\exp(-\lambda t)] \quad (6)$$

ahol:

t: besugárzási idő [s],

φ: fluens [részecske/cm^2],

σ: aktivációs hatáskeresztmetszet [barn = 10^{-24} cm^2],

λ: bomlási állandó [s^{-1}],

N_{rad}: keletkező radioaktív magok száma [db],

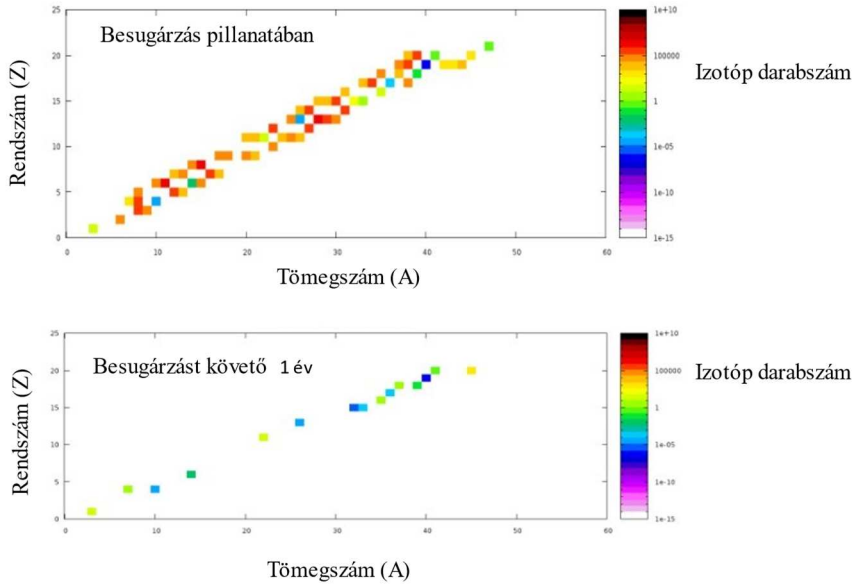
N_{target}: a radionuklid keletkezéséhez vezető reakcióban részt venni képes célmagok száma

A: aktivitás [Bq].

Az árnyékoló elemekbe behatoló másodlagos sugárzások (elektron, proton) a részecske energiája és az árnyékolás anyagát jellemző gyengítési hatáskeresztmetszet függvényében eltérő mértékben képesek behatolni, ahol az erre alkalmas részecskék az anyagot fel tudják aktiválni. Az elektronok kisebb LET-értéküknek megfelelően jellemzően mélyebbre hatolnak, míg a kezdetben hasonló energiájú protonok a felszín közelében nye-

lődnek el, és okozhatnak felaktiválódást. Az elektronok csak közvetve, pl. az általuk keltett fékezési sugárzás elnyelődéséből előálló fotoneutronok révén válthatnak ki magreakciót. Az árnyékoló elemekről szóródó neutron sugárzás a besugárzó termekben lévő egyéb anyagok felszínét, illetve felszínközeli részét is képes lehet felaktiválni. A nyaláb elrendezéstől függően bizonyos területeken nagyobb lesz a felaktiválódás mértéke a neutron fluens inhomogén eloszlása és a neutronok változó mértékű termalizálódása miatt, így hosszabb besugárzásoknál kialakulhatnak hotspotok, ezekből származhat reziduális sugárzás. A reziduális sugárzásból eredő dózisteljesítmény kezdetben gyorsan csökken a kis felezési idejű radionuklidok bomlása miatt, a hosszabb felezési idejűek megmaradnak, és ezek képzik majd a hotspotokat [6].

A különböző anyagok felaktiválódásának mértéke azonos részecskesugárzás hatására a hatáskeresztmetszetek különbözősége miatt eltérő. A 8. ábrán a FLUKA kód segítségével szimulált aktivációval keletkező izotópok láthatóak a tömegszám és a rendszám függvényében nehézbetonra. A felső ábrán a besugárzás pillanatában, míg az alsó ábrán a besugárzást követő 1 év pihentetés után rögzített állapot látható, 1 db 250 MeV-es proton besugárzásra normálva, besugárzási idő 1 óra, lézer frekvencia 10 Hz, indított részecskeszám 10^9 db proton (minden kis négyzet 1-1 izotópot jelöl).



8. ábra: Nehézbeton (Nurad 385) felaktiválódása a besugárzás pillanatában és a besugárzás követő 1 évben (x: tömegszám (A), y: rendszám (Z), színkód: Izotóp darabszám 1 db 250 MeV proton besugárzásra normálva) [saját szerkesztés]

A 8. ábra alapján – a felső és alsó ábrát összevetve – megállapítható, hogy a protonok által generált radioaktív izotópok nagy része igen gyorsan elbomlik, ennek ellenére a hosszú idejű lézerhasználat esetén az anyagban a hosszú felezési idejű radionuklidok feldúsulnak (8. ábra alsó).

MÓDSZERTANI ÚTMUTATÓ, AJÁNLÁSOK

Az ajánlások célja, hogy szakmai segítséget nyújtsanak a nyílt sugárforrásnak minősülő céltárgyról leváló törmelék, az akár néhány µm méretű felaktiválódott (radioaktív) anyagok hatékony kereséséhez, megtalálásához, valamint a besugárzó kamra dekontaminálásához, illetve a termekben kialakuló hotspotok felkutatásához a háttérhez képest nagyobb dózisteljesítményű térben, amit a reziduális aktivitás okoz. Ezt a munkát már az ELI ALPS indulásakor elindítottuk, így a korábbi eredményekből egyetemi szakdolgozat is készült [10].

Mivel a céltárgyak kis mérete (pár µm, szemmel nem látható) megnehezíti a kezelésüket, így ionizáló sugárzások mérésére alkalmas készülékek használata indokolt. Amennyiben ezen apró céltárgy darabkák ellenőrizetlenül kikerülnek a besugárzó kamrából, akkor megnő a környezeti szennyezés (kontamináció) és humán szennyezés (inkorporáció) kockázata.

Az útmutatóban leírtak segítséget adhatnak az operátorok, sugárvédelmi megbízottak számára az elveszett céltárgyak, céltárgy törmelékek, valamint elveszett források felkutatásához.

A sugárveszélyes munkafolyamatokat csak olyan személyek végezhetik, akiknek megfelelő sugárvédelmi képzettségük és tapasztalatuk van, valamint felhatalmazásuk a munkáltató részéről. A sugárvédelmi képesítés feltételei megtalálhatók a 2/2022. (IV. 29.) OAH rendeletben [7]. A sugárforrás keresése begyakorolható az erre a célra kialakított tanpályán valós, illetve virtuális sugárforrásokkal.

Az ilyen munkát végző személyek képzésének kötelező eleme a minimum bővített sugárvédelmi tanfolyam a nagy teljesítményű lézerberendezés sugárvédelmi sajátosságaival kiegészítve, valamint a rendszeres időközönként tartott gyakorlatokon való részvétel.

Sugárvédelmi ellenőrző mérések, monitorozás

A besugárzó termekbe való belépéskor hordozható belégzés monitorral kell meggyőződni arról, hogy a termek kiszellőztek, a levegő a természetes háttérszint felett nem tartalmaz mérhető mennyiségben radionuklidokat.

A besugárzást követően (a besugárzási kamrában vákuumot kell létrehozni a kísérletek alatt) a vákuumot először meg kell szüntetni, majd a kamrát ki kell nyitni, különösen ügyelve arra, hogy a céltárgyról esetlegesen levált mikroszkopikus méretű radioaktív szennyeződések ne juthassanak ki a külső térbe. Nyitás után a sugárvédelmi megbízottnak alfa, béta és gamma felületi szennyezettséget mérő eszközzel végig kell mérnie a besugárzó kamra belső részét, és meg kell találni a céltárgy esetleg levált darabjait.

Radioaktív anyag kezelése

Egy robotkar vagy csipesz segítségével ki kell emelni a besugárzott, aktív céltárgyat, majd egy jól záródó, vonalkóddal (vagy azonosító címkével) ellátott nejlon tasakba kell helyezni. A besugárzott céltárgyról érdemes minden információt digitális archívumba felvezetni (fénykép, besugárzási körülmények, mért gamma-spektrum, egyéb dokumentumok). A későbbiekben a vonalkód és informatikai program segítségével könnyedén megtudható minden információ a céltárgyról.

Radioaktív anyag tárolása

Amennyiben gamma-sugárzó az anyag, akkor ólom tokokban kell tárolni a besugárzott céltárgyakat (levált darabokat) a házon belüli szállítás idejére. A felaktiválódott anyagokat célszerű mindig távfogókkal mozgatni. Végül a céltárgyat egy ólom tároló konténerbe kell helyezni tárolás céljából. A szállító- és tároló konténert sugárveszély bárcával kell ellátni és úgy lezárni, hogy illetéktelenek ne férhessenek hozzá. A tárolást olyan helyen kell biztosítani, ahová csak külön belépési jogosultsággal és sugárvédelmi képzettséggel rendelkező személyek léphetnek be. A besugárzó kamra dekontaminálását és a felaktivált anyagok elszállítását követően a sugárvédelmi megbízott engedélye alapján lehet csak belépni a besugárzó termekbe.

A fenti folyamatokhoz a következő protokoll tartozik: Belépés előtt megfelelő zárt védőruházat, két pár gumikesztyű, szájmaszk, védőszemüveg, tisztatéri cipő felvétele szükséges, valamint hatósági dózismérő és kiegészítő EPD (elektronikus személyi dozimáter) viselése is kötelező (9. ábra). Az öltözetnek meg kell felelnie a tisztatér technológiának a lézertechnológia miatt, illetve a sugárvédelmi előírásoknak is. A védőruházatok fel- és levételét ún. fekete-fehér öltözőben kell elvégezni. A mérőműszereket szintén védőburkolattal kell ellátni az esetleges kontamináció elkerülése végett. Ellenőrizni kell a mérőműszerek kalibráltságát, hitelesítését és a mérőeszközök akkumulátorainak töltöttségi szintjét is.

9. ábra Megfelelő védőruházat [saját szerkesztés]

Két személy (minden ilyen sugárveszélyes munka végzéséhez két fő szükséges) bemegy a kutatási területre felszerelve a személyi dozimetria eszközeivel: hatósági TLD, EPD (Electronic Personal Dosimeter); továbbá a mérésekhez szükséges detektorokkal: felületi szennyezettség mérő, α-β-γ mérők, dózisteljesítmény-mérő, valamint kézi nuklidazonosító készülék, illetve belégzés monitor. A terület határán először háttérsugárzást kell mérni. Ezután a céltárgyról levált szennyeződéseket kell megkeresni: a dózisteljesítménymérő és felületi szennyeződés mérő jelzései alapján a forró pontok meghatározhatók. Amennyiben a nuklidazonosító dózisteljesítmény-mérő része háttérsugárzási szintet jelez

(10. ábra, bal), érdemes a műszert spektrum analizáló üzemmódba kapcsolni, így meghatározhatók a kis gamma-energiájú, felaktiválódott anyagok (10. ábra jobb).

10. ábra: Gamma dózisteljesítmény mérés (bal oldali ábra), spektrum analízis (jobb oldali ábra) RIIDEye-G készülékkel [saját szerkesztés]

Dekontaminálás

A céltárgy elszállítása után a besugárzási kamra dekontaminálása következik. A műszer által mért aktivitás két helyről származhat: a kamra felaktiválódott anyagából, vagy a kamra falára rakódott aktív szennyeződésekből. Ez dörzsmintavétel segítségével határozható meg. Egy etanolba áztatott inaktív vattával át kell dörzsölni az aktívnak vélt felületet, majd a vattát nejlon csomagolásba kell elhelyezni, hogy elkerülhető legyen a véletlen szennyezés. A becsomagolt dörzsmintát a besugárzó termen belül egy erre a célra kijelölt természetes környezeti háttérsugárzású területre kell szállítani. Ott meg kell mérni a felületi szennyezettségét. Ha a műszer emelkedett értéket mutat, akkor megállapítható, hogy lerakódott szennyeződésről van szó, amit dekontaminálni kell. Amennyiben nem mérhető a háttérnél magasabb érték, akkor a kamra anyaga aktiválódott fel, amire fel kell hívni a figyelmet. Ebben az esetben a sugárvédelmi megbízott további utasításáig nem lehet a kamrát megközelíteni. A sugárvédelmi megbízottnak a kamrában lévő felületi szennyezettséget dekontaminálnia szükséges, az irányadó beavatkozási felületi szennyezettség értékek megtalálhatóak az MSZ:62-7/2017 szabvány 5. táblázatában.

Az eljárás során fontos a detektor megfelelő pozicionálása (11. ábra), ugyanis a kizárólag spektrum analízissel detektálható szennyeződések annyira kis aktivitásúak lehetnek, hogy helytelen mérési módszer esetén detektálásuk elmaradhat. A mérőszondát a vizsgált felülethez a lehető legközelebb, merőlegesen tartva kell a mérést elvégezni, mivel az aktivitás kimutatási érzékenysége a távolság négyzetével arányosan romlik.

11. ábra: Megfelelő mérési módszer RIIDEye-G készülékkel [saját szerkesztés]

A dekontaminálást hosszú szárú csipesszel megfogott, dekontamináló szerbe mártott vattával kell elvégezni. A használt vatták veszélyes radioaktív hulladéknak minősülnek, és ennek megfelelően kezelendők. Dekontaminálás után feltétlenül szükséges a védőruházatok vizsgálata felületi szennyezettség mérővel (12. ábra), majd a védőruházatok levétele.

12. ábra: Védőöltözet ellenőrzése, kilépéshez [saját szerkesztés]

A kamra sugárvédelmi ellenőrzésére fordítandó idő legfeljebb fél – 1 óra.

A folyamatról jegyzőkönyv készítése szükséges, amelyben az alábbi adatoknak kell szerepelnie:

- munkafolyamatot végző személyek neve
- munkafolyamat kezdési és befejezési dátuma, ideje
- munkafolyamat helye
- besugárzott anyag
- szennyeződések típusa, aktivitásának mértéke
- munkafolyamat rövid leírása
- anyagfelhasználás
- megjegyzés
- rendkívüli események

A munkafolyamat során használt szerszámokat, alkatrészeket, amelyek szennyeződhetnek, a besugárzó termek melletti sugárvédelmi laboratóriumba kell elhelyezni, illetve használaton kívül ott kell tárolni.

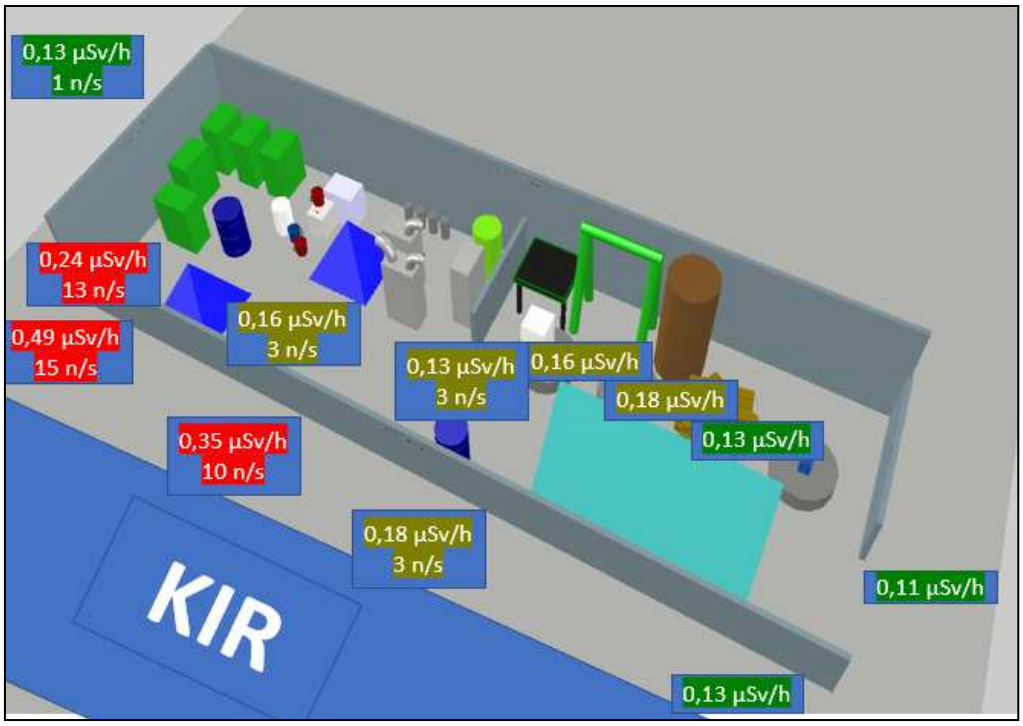
TANPÁLYÁK, GYAKORLATOK, FOSTER

A nagy teljesítményű lézerberendezés hosszabb távú működése során számolni kell a céltárgyak, a besugárzó kamra, az árnyékoló elemek és egyéb berendezések felaktiválódásával, az ún. hotspotok kialakulásával és a háttérhez képest emelkedettebb dózisteljesítményekkel a reziduális sugárzás következtében. Kisméretű és kisebb aktivitású anyagokat még normál háttér-érték mellett is nehéz és hosszadalmas megkeresni, nagyobb háttérnél pedig speciális eszközökre és megfelelő gyakorlatra van szükség.

A 490/2015 (XII.30.) rendelet [8] értelmében, amennyiben sugárforrást találnak vagy foglalnak le a hatóságok az országban, akkor a rendelet és a hatályos jogszabályok alapján esetenként több, elsődleges detektálásra és reagálásra is jogosult és detektálási képességekkel rendelkező hatóság is kivonul(hat) a helyszínre (Katasztrófavédelem, Terror Elhárítási Központ, Nemzeti Nyomozó Iroda). Radioaktív anyag, (pl. zárt radioaktív sugárforrások) esetén az OKI készenléti csapata az OSKSZ (Országos Sugáregészségügyi Készenléti Szolgálat) az illetékes helyszínelő, amennyiben az anyag nukleáris, akkor az OSKSZ, vagy más szervezet értesítése után, az EK SBL (Energiatudományi Kutatóközpont Sugárbiztonsági Laboratórium) feladata az anyag helyszíni vizsgálata, kategorizálása, begyűjtése és elszállítása az EK telephelyére.

A Sugárbiztonsági Laboratórium emiatt létrehozta a MEST (**M**obile **E**xpert **S**upport **T**eam) csapatot, melynek elsődleges feladata felkészülni radioaktív sugárforrások felkutatására az egyszerűtől az igen bonyolult esetekig [9].

A 490-es rendelethez kapcsolódó eljáró szervek kiképzésére létrehoztunk tanpályákat (FOSTER: **F**irst resp**O**nder**S** cen**T**re at **E**nergy **R**esearch on Nuclear Security) az Energiatudományi Kutatóközpontban, ahol igen sokféle szcenáriót lehet begyakorolni. A tanpályák közül a **K**özponti **I**zotóp **R**aktár (KIR) mellett elhelyezkedő hangár speciális, mivel itt normál és emelkedett háttér lett kialakítva (13.-14. ábra) [11]:



13. ábra: A KIR melletti tanpálya dózistérképe [saját szerkesztés]

14. ábra: A KIR és a speciális tanpálya [saját szerkesztés]

Az emelkedetebb háttér miatt ez a terület ideális gyakorlópálya, mivel a remanens dózisteljesítménnyel rendelkező besugárzó termekhez hasonló körülmények lettek kialakítva.

Az SBL forráskeresési eljárásokat dolgozott ki, ezek leírása megtalálható az Országos Atomenergia Hivatal (OAH) honlapján [12]. A MEST csapat számos nemzetközi konferencián demonstrálta a forráskeresést, a helyszínelő rendőrséggel közös eljárásrendet dolgozott ki, továbbá az Országos Katasztrófavédelem Katasztrófavédelmi Mozgó Laboratórium egységeinek tart forráskeresési gyakorlatokat. Az SBL-en és a hozzá tartozó tanpályák segítségével időben fel lehet készülni és meg lehet szerezni a megfelelő gyakorlatot az ELI ALPS sajátos környezetéhez.

ÖSSZEFOGLALÓ

A kutatási célú lézerek maximális intenzitása és teljesítménye az elmúlt húsz év alatt drasztikusan emelkedett. A nagy intenzitású lézerimpulzus és az anyag kölcsönhatása során bizonyos elrendezések mellett a kísérletekben többféle ionizáló sugárzás, szekunder és tercier részecskék is keletkezhetnek. A generált proton- és/vagy neutronsugárzás felaktiválhatja a céltárgyat, a besugárzó kamrát, az árnyékoló elemeket, valamint a besugárzó termek egyéb anyagait.

A nagy teljesítményű lézerberendezések sajátos sugárvédelméhez tett ajánlások segítik az ilyen létesítményben dolgozó sugárvédelmi szakembereket jobban megérteni, milyen fő fizikai folyamatok játszódnak le, melyek a sugárvédelmi szempontból releváns folyamatok, és ezeknek milyen várható hatásai vannak.

A kísérletek után a céltárgyak és törmelékek biztonságos megtalálása, elhelyezése, hotspotok, felületi szennyezettségek felkutatása és dekontaminálása kulcsfontosságú, mivel ezek hiányában a munkavállalók elszennyezhetik a besugárzó kamrát, a kísérleti labort és annak külső folyosóját.

Az EK SBL több éve foglalkozik sugárforrások felkutatásával, és olyan tanpályákat épített ki, ahol ezek a műveletek gyakorolhatók. A KIR melletti hangárban speciális emelkedett háttér található, ami kiváló terep az emelkedett háttérben történő forráskeresés készségeinek elsajátításához.

Az ELI ALPS projekt (GINOP-2.3.6-15-2015-00001) az Európai Unió támogatásával, az Európai Regionális Fejlesztési Alap társfinanszírozásával valósul meg.

FELHASZNÁLT IRODALOM

[1] Osvay Károly: Az ELI-ALPS lézerei és kutatási infrastruktúrája https://www.kfki.hu/elftkisk/61_Anket/61_Eloadasok/Osvay_K.pdf (Letöltés ideje: 2022.09.11.)

[2] https://www.youtube.com/watch?v=MlNxgmPVF6U&t=2s (Letöltés ideje: 2022.09.05.)

[3] J. Bauer, J. C. Liu, A. A. Prinz, S. Rokni, H. Tran, M. Woods, and Z. Xia, E. Galtier, H-J Lee, D. Milathianaki, B. Nagler: Measurements of Ionizing Radiation Doses Induced by High Irradiance Laser on Targets in LCLS MEC Instrument, SLAC PUB-15889, 2013.12.15. https://www.osti.gov/biblio/23082908 (Letöltés ideje: 2022.09.10.)
[4] Jegenyés Nikoletta: Ultrarövid lézerimpulzusok kölcsönhatása fém és félfém céltárgyakkal, http://doktori.bibl.u-szeged.hu/id/eprint/838/10/2010_jegyenyes_nikoletta.pdf (Letöltés ideje: 2022.09.10.)
[5] J. Bauer, J. C. Liu, A. A. Prinz, S. Rokni, H. Tran, M. Woods, and Z. Xia, E. Galtier, H-J Lee, D. Milathianaki, B. Nagler: Measurements of Ionizing Radiation Doses Induced by High Irradiance Laser on Targets in LCLS MEC Instrument, SLAC PUB-15889, 2013.12.15. https://www.osti.gov/biblio/23082908 (Letöltés ideje: 2022.09.10.)
[6] Graham R. Stevenson: Induced activity in accelerator structures, air and water, https://www1.lnl.infn.it/~radprot/index_htm_files/act.pdf (Letöltés ideje: 2022.10.16.)
[7] 2/2022. (IV.29.) OAH rendelet https://net.jogtar.hu/jogszabaly?docid=a2200002.oah (Letöltés ideje: 2022.10.27.)
[8] 490/2015. (XII. 30.) Korm. rendelet: a hiányzó, a talált, valamint a lefoglalt nukleáris és más radioaktív anyagokkal kapcsolatos bejelentésekről és intézkedésekről, továbbá a nukleáris és más radioaktív anyagokkal kapcsolatos egyéb bejelentést követő intézkedésekről: https://net.jogtar.hu/jogszabaly?docid=a1500490.kor (Letöltés ideje: 2022.06.07.)
[9] Dr. Éva Kovács-Széles, István Almási, Ákos Balaskó, Csaba Bíró, Károly Bodor, Csilla Csöme, Izabella Kakuja, Zsuzsanna Kreitz, Kornél Papp, Csaba Tóbi, József Volarics: How to respond a crime scene contaminated with radioactive material? Belügyi Szemle / 2020 / Special Issue 3., https://ojs.mtak.hu/index.php/belugyi-szemle/article/view/4852 (Letöltés ideje: 2022.06.07.)
[10] Vaska-Potharn Henriett: Az ELI-ALPS HTA-beli ionizáló sugárforrások sugárvédelmének elemzése, Diplomamunka, 2015. GAMF
[11] Károly Bodor, Péter Zagyvai: Lost radioactive source exploration training capabilities at the Centre for Energy Research (EK), https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/252/228 (Letöltés ideje: 2023.03.01.), Biztonságtudományi Szemle Évf. 4 szám 4. (2022)
[12] OAH útmutató: Útmutató a hiányzó nukleáris vagy más radioaktív anyagok keresésére http://www.haea.gov.hu/web/v3/oahportal.nsf/708B91804DA53733C1258167002F0F67/$FILE/FV-20v1T_v%C3%A9gleges_korr_tiszta.pdf (Letöltés ideje: 2023.03.01.)

STRUCTURAL AND STANDARDIZATION EXAMINATION OF EXOSKELETONS EQUIPPED WITH SOFT ACTUATORS

SOFT-AKTUÁTORRAL ELLÁTOTT EXOSKELETONOK SZERKEZETI ÉS SZABVÁNYOSÍTÁSI VIZSGÁLATA

MÉSZÁROS ATTILA[1] – KÓCZI Dávid[2] - SÁROSI József[3]

Abstract

The wearable robots are going through a huge transformation from the initial rigid machines to the lightweight robot clothing, which we can hardly distinguish from our everyday clothes. In less than a decade, soft robot clothing has achieved outstanding results in coordinating and assisting human motor movements. This article provides an overview of the evolution and technological development of exoskeletons, as well as current development directions, and presents standards and international initiatives related to exoskeletons that are designed to promote the widespread and safe dissemination of the technology.

Keywords

Exoskeleton, Exomuscles, Exosuits, AMST, FEA, Standard

Absztrakt

A hordható robotok hatalmas átalakuláson mennek keresztül a kezdeti merev gépektől egészen a könnyű robotruházatig, amit aligha tudunk megkülönböztetni a mindennapi ruháinktól. Kevesebb, mint egy évtized alatt a puha robotruhák kiemelkedő eredményeket értek el az emberi motoros mozgások koordinálásában és segítésében. Ez a cikk áttekintést nyújt az exoskeletonok kialakulásának és technológiai fejlődésének menetéről és a jelenlegi fejlesztési irányokról, illetve bemutatásra kerülnek az exoskeletonokhoz kapcsolódó szabványok és nemzetközi kezdeményezések, melyek a technológia széleskörű és biztonságos elterjedését hivatottak szolgálni.

Kulcsszavak

Exoskeleton, Exomuscles, Exosuits, AMST, FEA, Szabvány

[1] m-attila@mk.u-szeged.hu | ORCID: 0000-0002-3084-0321| Assistant lecturer, University of Szeged Faculty of Engineering, Department of Mechatronics and Automation| Tanársegéd, Szegedi Tudományegyetem Mérnöki Kar, Mechatronikai és Automatizálási Intézet

[2] koczid@mk.u-szeged.hu | ORCID: 0000-0002-5090-3270 | Assistant lecturer, University of Szeged Faculty of Engineering, Department of Mechatronics and Automation| Tanársegéd, Szegedi Tudományegyetem Mérnöki Kar, Mechatronikai és Automatizálási Intézet

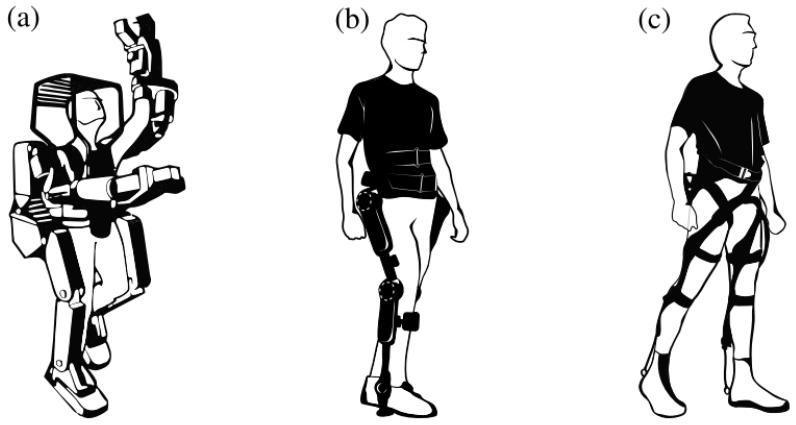
[3] sarosi@mk.u-szeged.hu| ORCID: 0000-0002-6303-5011 | Full professor, University of Szeged Faculty of Engineering, Department of Mechatronics and Automation| Egyetemi tanár, Szegedi Tudományegyetem Mérnöki Kar, Mechatronikai és Automatizálási Intézet

BEVEZETÉS

Régóta ismeretes, hogy a munka és a munkakörnyezet összefügg a munkavállalók rossz egészségi állapotával. A váz- és izomrendszeri betegségek (MSD-k), amelyek az izmokat és az ízületeket érintik, a munkahelyi betegszabadságok és korengedményes nyugdíjba vonulások fő oka, ugyanis a dolgozók nem képesek a szokásos napi munkafeladatok ellátására [1]. A rendellenességek száma évről évre növekszik, és világszerte minden munkavállalót érintenek. Következésképpen ezek a folyamatok az érintett személyeknek, munkaadóiknak és a gazdaságnak jelentős anyagi terhet jelentenek [2]. A rendellenességek kialakulásához kapcsolódó kockázati tényezők közé tartozik a kézi tehermozgatás, különösen a nehezebb rakományok esetén, illetve a kézi mozgatás időtartama, az ismétlődő mozgások és az extrém vagy kényelmetlen testhelyzetek, mint pl. hajlítás, nyújtás vagy csavarás [3].

Az automatizálására kifejlesztett gépek ihlették annak az ötletét, hogy olyan gépeket alkossanak, melyek képes levenni bizonyos mértékben az emberi testet érő erőhatások egy részét. A viselhető robotok első koncepciói osztoztak egy nem meglepő közös tulajdonságon: az eszköz váz szerkezete, tükrözte a pilóta csontvázát, merev anyagból készültek, illetve mechanikus csuklópontokkal voltak ellátva a mozgás biztosítása érdekében. A General Electric 1967-ben megvalósította ezt a koncepciót Ralph Mosher vezetésével és megépítette a Hardimant [4]. A Hardimant (1. ábra a) kialakításában sajnos korlátozta korának technológiája, a robotot soha nem tesztelték emberi pilótával. Ennek ellenére a projektnek megvolt az érdeme, ugyanis felkeltette az érdeklődést a robotok iránt, amelyek fokozhatják vagy segíthetik az emberi teljesítményt az emberi résztvevő anatómiájához illeszkedő szerkezet segítségével. Ez volt az exoskeletonok születése.

Közel ötven évvel később az exoskeletonok rohamosan fejlődtek az új technológiai, elektronikai, vezérlési, gyártási és energiatároló megoldásoknak köszönhetően [5]. Az exoskeletonok sikeresen növelték az emberi erőt a mozgás során [6], csökkentették a járás terhelését [7], képesek voltak helyreállítani a paraplégiás betegek mozgási képességeit [8] (a hozzá használt exoskeleton az 1.b) ábrán látható) segítette a stroke betegek rehabilitációját [9], képes volt az emberi mozgásokból energiát nyerni [10], és segítettek az emberi motoros mozgások alapelveinek tanulmányozásában [11].



1. Ábra: Különböző exoskeleton kialakítások. a) Hardimant, az első exoskeleton koncepció, b) alsó végtag exoskeleton (Cybernyde), c) Harvard exosuit [17]

A hordható technológia fejlődéséről szóló közelmúltbeli betekintésben J. L. Pons elegánsan rámutatott, hogy a hordható robotok esetén a kevésbé korlátozó és inkább biomimetikus architektúrák felé való elmozdulás lenne célszerű, előnyben részesítve azokat az anyagokat, amelyek jobban megfelelnek az emberi test anatómiai összetettségéhez [12]. Pons elképzelését az elmúlt évtizedben kifejlesztett viselhető robotok jellemzői igazolják. Kihasználva a lágy anyagok előnyös tulajdonságait, illetve a megfelelő szabályozási és a nemlineáris modellezési technikákat [13], egyre több tudományos és ipari kutatócsoport textilekből és elasztomerekből tervez hordozható robotokat. Ez lehetővé teszi az eszközök könnyebb hordozhatóságát és a mozgás elősegítését az emberi biomechanika korlátozása nélkül. Ezekre az új eszközökre különböző kifejezésekkel hivatkoztak, mint: „exomuscles" [14], „soft exoskeletons" [15] és „exosuits" [16] (1. ábra c).

FELSŐ VÉGTAGRA ILLESZTHETŐ EXOSKELETONOK TÍPUSAI

Az első soft-jellegű exoskeletonok a 2000-es évek elején készültek az úgynevezett McKibben féle mesterséges műizmok (PAM) segítségével. 2004 elején Kobayashi et al. Elkészítették az úgynevezett „muscle suit"-ot [18] (2. ábra), amely McKibben féle félmerev PAM-ok, hálózatából állt. A nyomás szabályozásával Kobayashi bizonyította, hogy a koncepciójával megvalósítható a váll ellenőrzött mozgatása. Ez a típusú exoskeleton a McKibben féle mesterséges műizmok miatt jelentősen korlátozza az emberi mozgást, szinte csak az előre tervezett mozdulatsorok hatjhatóak végre.

2. Ábra: McKibben féle PAM-ok hálózatából álló exoskeleton [18]

2014-ben Koo és munkatársai egy softrobotruhát mutattak be, melyet úgy terveztek, hogy segítse az étel szájba juttatásának mozdulatsorait [19]. Az eszköz (3. ábra), kifejezetten olyan embereket céloz meg akik poliomyositis okozta izomgyengeségben szenvednek. Az eszköz egy elektromos motorral hajtott ín egység és egy felfújt kamra ötvözete. A készülék később passzív mechanizmussal lett kiegészítve, amely párhuzamosan működik a motorral, a rendszer energiafogyasztásának csökkentése érdekében. Későbbi kutatások kimutatták, hogy egészséges résztvevők esetén a passzív komponens önmagában elegendő az izomfáradtság kialakulásának késleltetéséhez [20].

3. Ábra: Étel szájba juttatásának mozdulatsorait segítő hibrid exoskeleton [19]

Az újabb kutatások a pneumatikus kontraktilis hálózat ötletével foglalkoznak, melyek az emberi izmokkal párhuzamosan működő elemeket valósítanak meg. [21]. Ezeket miniatűr McKibben aktuátorok hálózatával érik el, melyek párhuzamos elrendezése nagyobb erők elérése szolgál, sorba kapcsolva pedig hosszabb löketet tudnak megvalósítani (4. ábra). Ezzel a megoldással, már jóval nagyobb szabadságfokot lehet biztosítani a mozgatni kívánt végtagnak, így bonyolultabb mozdulatsorok is korlátozottan kivitelezhetővé válnak.

4. Ábra: Miniatűr McKibben aktuátorok hálózatával megvalósított exoskeleton [21]

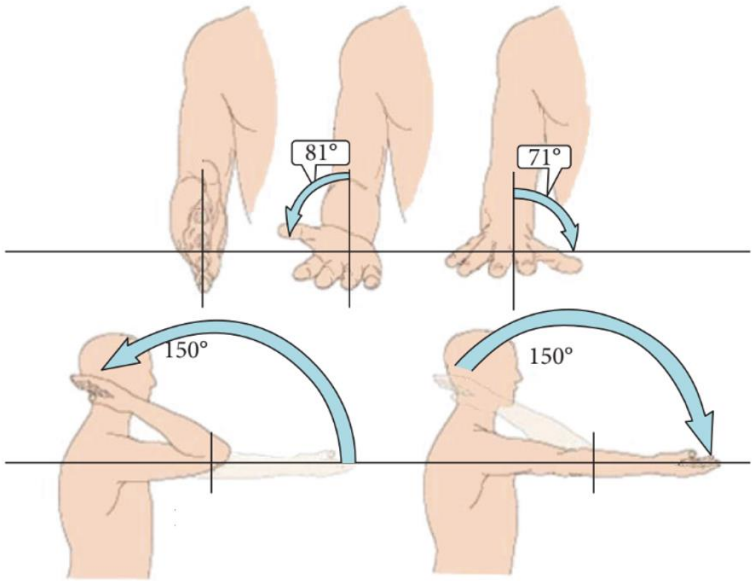
Park és munkatársai egy másik megközelítést alkalmaztak [22]. A szerzők egy puha robotruhát írnak le amely a könyök izület hajlítását teszi lehetővé memóriaötvözet alapú izom segítségével. Az izom nikkel-titán (NiTi) huzalból készült tekercsrugókból áll, amelyek párhuzamosan vannak elrendezve a maximális 120 N erő létrehozásához és mindössze 24 g tömeggel rendelkeznek.

A hajlítónyomatékot pneumatikus működtetésű kamrák hálózatával is létrehozhatjuk. Ezeket az eszközöket nevezzük Fluid Elastomer Actuator-nak (FEA). Thalman és társai lágy hengeres működtetőket használnak, amelyek egy tömbben vannak elrendezve [23]. A rugalmas felső rész és a rugalmatlan alapnak köszönhetően létrejön egy kiszámítható mértékű hajlítás és egy lineáris nyomaték-nyomás karakterisztika. Felfújt állapotban az egyes működtetők kölcsönhatásba lépnek egymással, így hajlító mozgást hozva létre a könyökízület körül (5. ábra).

5. Ábra: FEA alapú könyök mozgatására alkalmas exoskeleton [23]

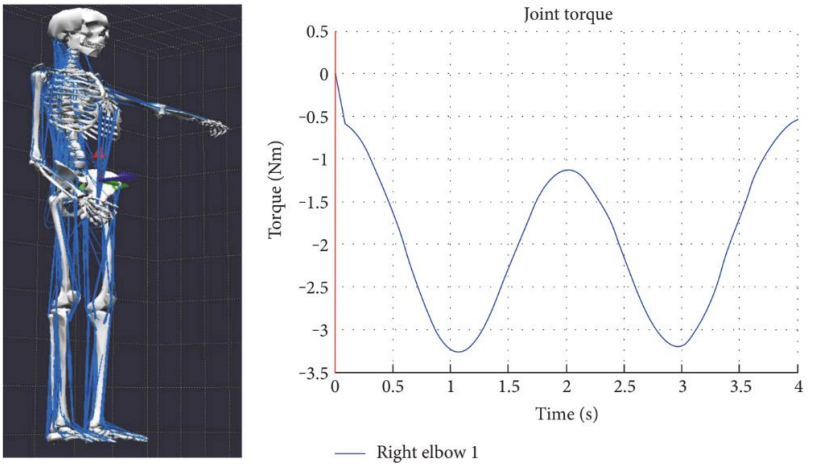
FELSŐ VÉGTAGRA ILLESZTHETŐ EXOSKELETON TERVEZÉSI IRÁNYELVEI

Copaci at al. mérései alapján a könyök rehabilitációs eszközöket úgy kell megtervezi, hogy illeszkedjenek a kéz elmozdulásnak tartományába (6. ábra), ami a könyököt tekintve 0° és 150° közé tehető nyújtott végtag esetén, a tenyér befelé fordítás esetén 71°-ot képes csavarodni, kifelé mozgás esetén pedig 81°-ot [24].



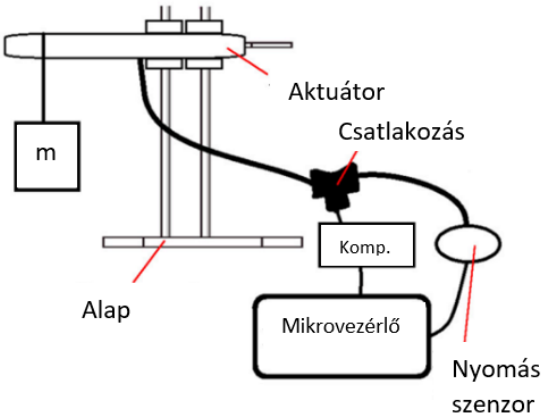
6. Ábra: Kar mozgási tartománya [24]

Ezen mozgástartományokat figyelembe véve szimulációs paraméterként súly 80kg, magasság 1,8m, könyök 0° és 150° közötti elmozdulást végezve 0,25 Hz frekvenciával , a könyök mozgástartományának nyomaték szükséglete idő függvényében 0 és 3,5 Nm közé tehető annak biztosítása érdekében, hogy a motoros funkciók teljes hiányában a könyök megfelelően mozgatható legyen [24] (7. ábra).



7. Ábra: Könyök mozgás nyomaték szükséglete [24]

A felsővégtagra illeszthető rehabilitációs eszközök közül a könyök rehabilitációra használt exoskeletonok, melyet Kohn at al. is bemutat értekezésében, alapvetően áll egy aktuátorból egy nyomás érzékelőből, egy mikrovezérlőből és egy kompresszorból. Az aktuátor rögzítési pontokat úgy kell kialakítani, hogy a felső bicepsztől az alkar közepéig terjedjen a két pneumatikus aktuátor rögzítése [25] (8. ábra).



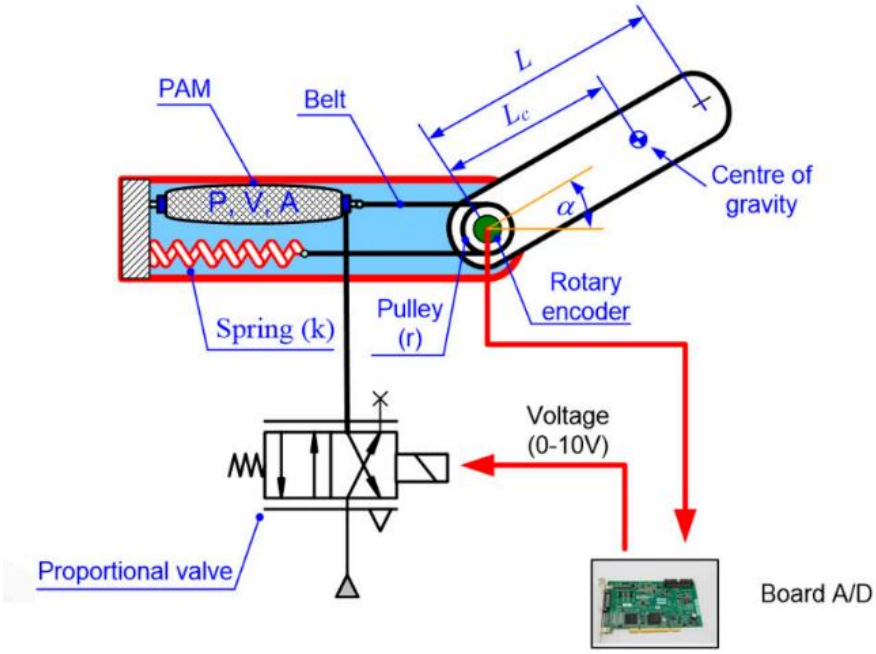
8. Ábra: FEA alapú könyök mozgatására alkalmas exoskeleton elvi mérési elrendezése [25]

Működtetését tekintve elmondható, hogy az aktuátor kamráiban a nyomásszabályozás mikrokontroller segítségével PID szabályozással valósul meg, az alábbi egyszerű összefüggés alapján:

$$u(t) = K_p e(t) + K_i \int_0^t e(t)dt + K_d \frac{de(t)}{dt} \quad (1)$$

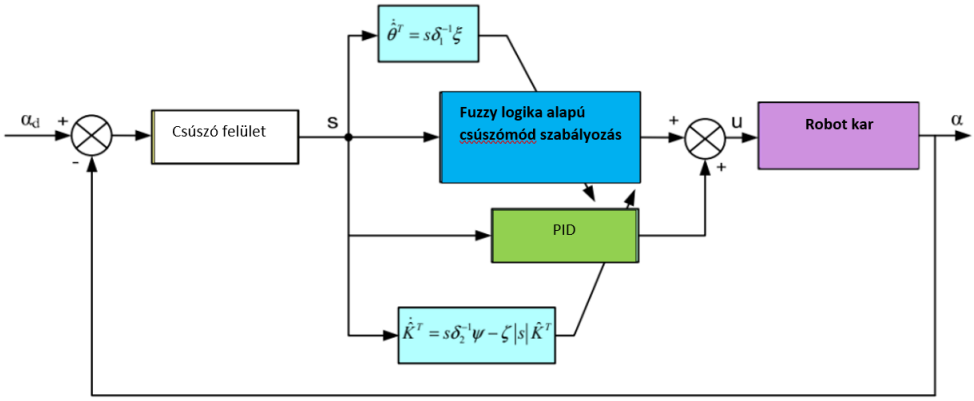
A függvény bemenete u(t) a beállított nyomásérték a visszacsatolás pedig a nyomásszenzor által biztosított jel valamint opcionálisan EMG szenzor is lehet, e(t) a hiba értéke, K_p, K_i, K_d pedig az arányos, integráló és deriváló tagok erősítése, t pedig az idő [25].

Nguyen at al. álltal bemutatott könyökrehabilitációs eszközben, a PAM szabályozás megoldására a csúszómód szabályozás egy változatát alkalmazza, ami szintén alkalmas lehet a precíz működtetésre [26] (9. ábra).



9. Ábra: PAM alapú könyök mozgatására alkalmas exoskeleton elvi elrendezése [26]

Szabályozási köre alapvetően úgy épül fel, hogy a Fuzzy szabályozást és a PID szabályozás kombinációját alkalmazza előbbit bemenetként szolgáltatva a csúszómód szabályozásnak majd a PID szabályozást kompenzátorként alkalmazza a csúszómód szabályozás kimenetén [26] (10. ábra).



10. Ábra: Rehabilitációs eszköz szabályozási blokkdiagramja [25]

FELSŐ VÉGTAGRA ILLESZTHETŐ EXOSKELETONOK ÖSSZEHASONLÍTÁSA

A végtagok elmozdítását külső egységek segítségével különböző módszerekkel valósíthatjuk meg. Az exoskeleton kialakítások 3 főbb trendet követnek:

- A legelterjedtebb változat a szilárd komponensekből és motorokból álló elektromechanikus variánsok.
- Ezt követi a PAM (Pneumatic Artifical Muscle) aktuátorokkal szerelt megoldások.
- Végül a FEA (Fluidic Elastomer Actuator) egységekkel ellátott eszközök

Az exoskeleton variánsok közötti fő különbséget az azokat működtető aktuátorok kialakítása adja. Ez alapjában különbözteti meg az eszközöket, ugyanis mindegyik más-más megoldást használ az ízületek rotációs mozgásának előidézésére. Azonban mindegyik megoldásban közös pont az, hogy az aktuátorokat a mozgatni kívánt testrészhez kell rögzíteni oly módon, hogy az a mozgást ne korlátozza vagy befolyásolja. A különböző kialakításoknak természetesen megvannak a maga előnyei és hátrányai, melyeket a felhasználás módjánál figyelembe kell venni. A következő táblázat (1. táblázat) ezeket az exoskeleton megoldásokat hasonítja össze különböző elvek és szempontrendszer alapján.

	Elektro-mechanikus	***PAM***	***FEA***
Az eszköz mozgási tartománya a végtagra vonatkoztatva.	A végtagok teljes tartományban mozgathatók, azonban a szilárd részegységek miatt bizonyos mellék mozdulatok, rotációk korlátozva vannak működés közben.	A végtagok mozgása korlátozott mértékű, mellékmozdulatok, rotációk kevésbe korlátozottak.	A végtagok teljes tartományban mozgathatóak, a mellékmozgások és rotációk kevésbé korlátozottak.
Erőkifejtés a mozgástartományban.	Állandó.	Állandó.	Változó.

	Elektro-mechanikus	***PAM***	***FEA***
Kialakításból, illetve túlvezérlésből adódó sérülésveszély.	A szilárd részegységek miatt, illetve az elektormos motorok maximális nyomatéka miatt a sérülésveszély közepes.	A magas működési nyomás miatt magas.	A nagy rugalmasságú részegységek miatt és a kis működtető nyomás miatt alacsony.
Exoskeletonként való viselhetőség.	A szilárd részegységek és a mozgató motorok speciális elhelyezése miatt nehézkes.	A nagy helyigényű kialakítás miatt, illetve az átalakító részegységek miatt nehézkes.	Aktuátorok méretei és testhez való alkalmazkodási képességei miatt kevésbé megterhelő.
Adaptálhatóság, variálhatóság.	A rotációs pontokon elhelyezett motoroknak köszönhetően a rögzítési pontok nagy szabadsággal állíthatóak.	Kialakításuk miatt korlátozottan állíthatóak.	Kialakításuk miatt korlátozottan állíthatóak.
Energiaellátás hordható eszközök esetén.	Az akkumulátortechnológia adta lehetőségek miatt hosszabb távon is működtethető az eszköz kis helyigényű energiaforrás segítségével.	A működéshez szükséges nagyobb nyomás miatt a működtetés hordható eszközök esetén erősen korlátozott.	A működéshez szükséges kis nyomások miatt, kis helyigényű energiaforrás segítségével mérsékelten korlátozott.
Eszköz bekerülési költsége.	A mozgató motorok és az azokat vezérlő egységek miatt magas bekerülési költség.	Az egyszerű aktuátor kialakítás, és a mozgásátalakító részegségek miatt közepes a bekerülési költség.	Az egyszerű aktuátor kialakítás, illetve az előállításhoz szükséges anyagok miatt alacsony bekerülési költség.
Az eszközök tömeg/teljesítmény aránya.	A motorok által kifejtett nyomaték nagy, míg a szilárd mozgató mechanizmusok tömege magas.	Az aktuátorok nagy erők kifejtésére képesek, az átalakító mechanizmusok tömege nagy.	Az aktuátorok közepes erőkifejtésre képesek, a rögzítő részegségek tömege alacsony.

1. Táblázat: Különböző kialakítású exoskeletonok összehasonlítása

A fenti ábra jól szemlélteti, hogy a FEA típusú aktuátorok sok esetben előnyösebb tulajdonságokkal bírnak, mint az elektro-mechanikus vagy a PAM kialakítású társaik. Ezen típusú aktuátoroknak nagy előnye, hogy a rugalmas anyaghasználat miatt a viselőnek igen

nagy mozgásszabadságot biztosít akár működtetett, akár alap állapotban. Az aktuátorok testhez idomuló kialakítása miatt, illetve a különböző mechanikai átalakítók nélkül a hordozó számára kevésbé megterhelő ezeknek az aktuátoroknak a viselése akár hosszabb távon is. Szemléletes az a tulajdonságuk is, hogy az esetleges meghibásodásból vagy túlvezérlésből adódó sérülések előfordulása ennél a típusnál alacsony. Ugyanis a rugalmas aktuátorok képesek a hirtelen fellépő, váratlan erőhatásokat saját deformációjukra fordítani, így kímélve a mozgatni kívánt ízületet. A felhasznált anyagok tekintetében is jelentős előnnyel bírnak a FEA soft-exoskeletonok. Előállításukhoz nincs szükség drága nyersanyagokra, illetve bonyolult megmunkálási folyamatokra, melyek által a költségek jelentősen csökkennek. Ezek a tulajdonságok mind azt vetítik elő, hogy az exoskeletonok körében egyre jobban elterjedő soft megoldások lehetnek a technológia jövőjének kulcsa. Ezen a területen a kutatások jelenleg is a softaktuátorok erősebbé, ellenállóbbá és kompaktabbá tételére fókuszálnak annak érdekében, hogy a jelenlegi szilárd mechanikai megoldásokat felváltsák.

EXOSKELETONOKRA VONATKOZÓ ISO SZABVÁNYOK

A Nemzetközi Szabványügyi Szervezet (ISO) 13482:2014 foglalkozik a személyes gondoskodást nyújtó robotok biztonsági követelményeivel, amelyek közül néhányat exoskeletonnak tekintenek. Az ISO 13482 szabványok az exoskeletonok egy részhalmazára alkalmazhatók, de az exoskeleton fogalom nagy része kívül esik ennek hatókörén. Azonban az ISO 13482 nem alkalmazható robotokra, mint orvosi eszközökre, sem katonai erő alkalmazására szolgáló robotokra, ami egy hatalmas hiányosság. További emberi tevékenységgel együtt működő robotok követelményeit az ISO 10218, valamint az ISO/TS15066 rögzíti ipari vonatkozásban [26,27,28,29,30] (2. táblázat).

Szabvány	Alkalmazása
ISO 13482:2014 Robotok és robotszerkezetek. Személysegítő robotok biztonsági követelményei (ISO 13482:2014)	Specifikus elvárások és útmutatók a biztonságos tervezéséhez, biztonsági mérésekhez, és információk a személysegítő robotokhoz. Ez az egyetlen szabvány, amely tartalmaz exoskeletonokra vonatkozó részeket.
ISO 10218-1:2011 Robotok és robotszerkezetek. Ipari robotok biztonsági követelményei. 1. rész: Robotok	Specifikus elvárások és útmutatók a biztonságos tervezéshez, biztonsági mérésekhez, és információk az ipari robotokhoz.
ISO 10218-2:2011 Robotok és robotszerkezetek. Ipari robotok biztonsági követelményei. 2. rész: Robotrendszerek és összehangolásuk	Specifikus elvárások és útmutatók a biztonságos tervezéshez, biztonsági mérésekhez, és információk a ipari robotok és robotrendszerek integrátori számára.
ISO/TS15066 Robotok és robot szerkezetek. Kollaboratív robotok	Specifikus elvárások és útmutatók a biztonságos tervezéshez, biztonsági mérésekhez, és információk a kollaboratív robotokhoz.

2. Táblázat: Exoskeletonokra és egyéb robotrendszerkere vonatkozó ISO szabványok [26]

Az ISO 13482:2014 azonban kiterjed a munkahelyen használható, hordható fizikai asszisztens robotokra. Ezek a technológiák lehetővé tehetik a munkaképesség növelését és csökkenthetik a biomechanikai terhelést és a dolgozók fáradtságát, illetve csökkenti túlerőltetés kockázatát. Az ISO 13482 elismeri, hogy bár a fizikai asszisztens robotok bizonyos emberi képességeket növelhetnek, használatuk potenciális új veszélyeket rejt magában. E veszélyek egy része a roboteszköz rögzítéséből és a felhasználóval való közvetlen érintkezéséből fakad. Az ISO szabvány hangsúlyozza a kockázatértékelés és a veszély azonosítás elemzésének szükségességét e technológiák biztonságos tervezése és üzemeltetése érdekében. Az ISO Technikai Bizottság (TC) 299 munkacsoportjai két vizsgálati módszert fejlesztenek ki [27]:

- egy bőrterhelési vizsgálati módszert exoskeletonokra, amely egy szimulációs eszköz segítségével vizsgálja a felhasználó bőrének lehetséges maximális terhelését,
- egy vizsgálati módszert a látható törésekre, deformációkra, az alkatrészek szétválására és a robot funkcionális károsodására, beleértve azokat is, amelyeket egy személy visel

Az ISO 13482:2014 a Személysegítő robotok esetén a vizsgálati módszert alkalmazva a következő releváns kockázati kategóriákat kell mérlegelni (3. táblázat), exoskeleton tervezése esetén is:

Kockázati kategória	Leírás
Akkumulátor töltés	Túltöltés, mélymerülés, szigetelési problémák, rövidzárlat
Energiatárolás és energiaellátás	Szigetelési probléma, Laza mechanikus kapcsolat, Csatlakozási problémák: Pneumatika, Hidraulika, Szélsőséges hőmérséklet, Túlterhelés
Robot/Eszköz indítása	Nem várt működés, Nem várt újra indulás
Robot/Eszköz kialakítása	Éles szélek, Furatok és terek a mozgó részek között, Geometriai kialakítás
Zaj	Akusztikus zaj, Ultrahang,
Megbízhatóság	Pl.: Ütközés következtében nem várt működés
Vibráció	Káros rezgések, érintkezési problémák
Káros anyagok vagy folyadék	Káros anyagokkal/folyadékokkal való érintkezés
Káros környezeti kondíciók	Por, Pára, Robbanásveszély, Tűz, Víz, Jég…
Extrém hőmérséklet	Felforrósodó felület, Hideg felület, Kijelző rossz láthatósága
Nem ionizált és ionizált sugárzás	Káros optikai sugárzás, Káros lézer sugárzás

Kockázati kategória	Leírás
EMC	Sugárzott és vezetett zavartűrés és zajkibocsátás
Feszültség, pozíció és használat	Használat közben feszítő pozíció, fizikai diszkomfort, test méretre nem illeszkedő, kezelőszervek nem láthatók nem használhatóak
Robot/Eszköz mozgása	Mechanikai instabilitás, Mozgás közbeni instabilitás, Terhelés közbeni instabilitás, Elválik a testtől ütközés hatására…
Robot/Eszköz Ütközése	Ütközés hatására biztonsági megállás, Ütközés mozgó tárgyakkal, állatokkal, robotokkal
Veszélyes ember-robot fizikai kontaktus	Rosszul érzékelt biztonsági megállítás, Túlzott biztonsági megállítás reakció
Alul méretezés / tartósság	Váratlan tönkremenetel
Váratlan automata működés	Program hiba
Pozicionálási, navigációs kockázatok	Gyenge visszacsatolás, felhasználó korlátozott irányíthatósága.

3. Táblázat: Az ISO 13482:2014 által figyelemebe vehető kockázatok [27]

ASTM F48 BIZOTTSÁG

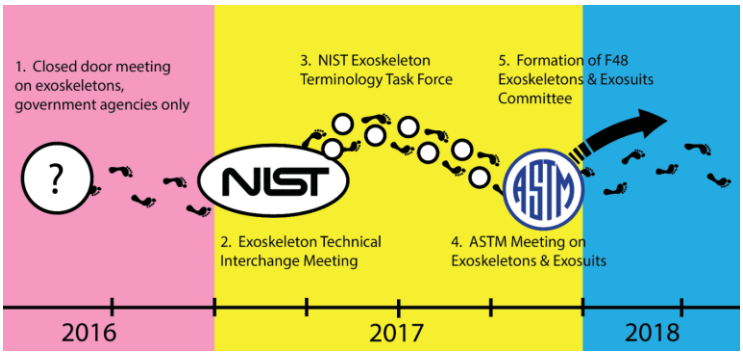
A termékszabványok és tanúsítványok hiánya az exoskeleton technológiák ipari gyakorlatban való alkalmazásának hatalmas akadálya. Bár az exoskeletonokat nem tekintik hagyományosan vett védőeszközöknek, azonban hasonlóan viselhetők, és az ipari/munkahelyi alkalmazásuk iránti érdeklődés nagy részét a sérülések megelőzése generálja. Az ASTM International Techni-cal Committee on Exoskeletons and Exosuits (ASTM F48) úgy véli, hogy az exoskeletonokra vonatkozó szabványok és tanúsítványok nagyban hozzájárulna a gyártásuk, telepítésük és felhasználásuk megkönnyítéséhez, illetve azok munkahelyi alkalmazásához.

2016 augusztusában a NIST (National Institute of Standards and Technology) előzetes találkozót rendezett, hogy megvitassák a jelenlegi helyzetet az exoskeletonok és a viselhető robotika területén belüli szabványokra vonatkozóan, valamint, hogy beazonosítsák azokat a hiányosságokat, amelyek a biztonság, a teljesítmény, az ergonómia és a kiberbiztonság tekintetében. Ezt követően 2017 januárjában nyílt nyilvános technikai találkozót tartottak, amely széles körben magában foglalta a katonai, egészségügyi és ipari területek érdekelt feleit. A találkozón a következő témák kerültek napirendre:

- Hiányosságok azonosítása az exoskeletonokra vonatkozó szabványok tekintetében, beleértve a terminológiát, a vizsgálati módszereket és a teljesítménymutatókat a ipari, katonai és egészségügyi ágazatokban
- elősegíteni az összes érdekelt fél bevonását ezekbe a fejlesztésekbe és szabályalkotási procedúrákba

- elősegíteni a technológiai fejlődést a kulcsfontosságú érdekelt felek közötti kapcsolatépítés révén

A folyamat időrendbeli lefolyását a 11. ábra mutatja.



11. ábra: Az ASTM F48 létrejöttének folymata [31]

2017 szeptemberében mintegy 40 terület képviselői beleértve a katonai, szövetségi ügynökségeket, exoskeleton gyártókat, alkatrészgyártókat, tudományos körök tagjait, illetve a felhasználói csoportokat, az ASTM összehívott egy új exoskeleton szabvány megszervezésére irányuló bizottságot, ami a ASTM F48 nevet kapta. Az F48 ma már széles körben foglalkozik az aktív, passzív exoskeletonokkal, és általános felhasználási eseteiket a következők szerint osztályozza [32]:

- Orvosi: Az amputált, sérült és/vagy fizikailag fogyatékkal élő, exoskeletont viselő betegeknek fokozott mobilitást és stabilitást biztosít az eszköz. Ez felgyorsíthatja a munkába való visszatérést és a felépülést, ami a betegek, az egészségügyi szolgáltatók és a biztosítótársaságok javát szolgálja.
- Ipari: A logisztikában, raktárban és gyári környezetben dolgozó alkalmazottak használhatják az exoskeletonokat fej feletti, teherhordási, szerszámhasználati, mobilitási és guggolásos tevékenységekhez, lehetővé téve számukra, hogy hosszabb ideig nagyobb teljesítményt érjenek el, és kevésbé terheljék a testüket, ezáltal csökkentsék a sérülésveszélyt is.
- Katonai: A katonák számára az exoskeletonok lehetővé teszik, hogy kevésbé fáradtan vonuljanak messzebbre, könnyebben és biztonságosabban mozgassák a logisztikai terheket és több készletet vagy fegyvert vihessenek magukkal, amelyek egyébként túl nehéznek vagy megterhelőnek bizonyulnának.
- Közbiztonság: Az elsősegélynyújtók számára előnyösek lehetnek az exoskeletonok, amelyek lehetővé teszik számukra, hogy nagyobb tárgyakat mozgassanak, amikor áldozatokat keresnek az összeomlott építmények között, és több felszerelést szállíthatnak, például extra légpalackokat a tűzoltóknak és nehéz bombaruhákat a robbanóanyagártalmatlanító technikusok számára.
- Fogyasztói/rekreációs: A fogyasztók számára előnyösek lehetnek az exoskeletonok személyes használatra, szabadidős sportokhoz (pl. síelés), otthoni és udvari munkához és más fizikailag megterhelő feladatokhoz.

Valamennyi albizottság olyan nemzetközi szabványokat dolgoz ki és tart fenn, amelyek többek között a biztonságra, minőségre és hatékonyságra vonatkozó szabványokat foglalnak magukban. Ezen túlmenően az egyes albizottságok célja, hogy szabványokat dolgozzanak ki az exoskeleton technológiák alkalmazására az ipari, orvosi, katonai, fogyasztói és katasztrófaelhárítási szektorban. Ezen túlmenően minden albizottság arra törekszik, hogy megértse és hivatkozzon más meglévő és fejlődő szabványokra, és együttműködik más ASTM International bizottságokkal, valamint más, kölcsönösen érdekelt szervezetekkel.

ÖSSZEFOGLALÁS

Egyszerűségük és hordozhatóságuk révén a soft-exoskeletonok egy lépéssel közelebb hozták mindennapi életünkhöz a hordozható robotokat. A soft-aktuátorkat tartalmazó exoskeletonok előnye a többi megoldáshoz képes a rendkívüli rugalmasságukban rejlik. Ezeknél a megoldásoknál a végtagok elmozdulása korán sincs annyira lekorlátozva mint a többi variánsnál. Az egyszerű működési mechanizmus és a testhez alkalmazkodni képes kialakítás kényelmesebbé és funkcionálisabbá teszi az exoskeletonokat. A jelenlegi kutatások egyik fő kérdése, hogy a soft-aktuátorok hogyan válhatnak erősebbé, ellenállóbbá és könnyebben gyárthatóvá. Az egyik meghatározó trend a kompozit anyagok felhasználása, illetve a szálerősítéses anyagok alkalmazása az aktuátor testen belül. Ezek a kutatások már most kecsegtető eredményekkel szolgálnak, ami azt mutatja, hogy a softaktuátorok a jövőben képesek lesznek olyan tulajdonságokra szert tenni, amelyek segítségével megvalósulhatnak olyan exoskeletonok melyek kényelmesen hordhatók, nem korlátozzák a végtagok mozgását és emellett megfelelő nagyságú erőt képesek kifejteni ahhoz, hogy fizikai munkát segítő vagy rehabilitációs jellegű mozgás kivitelezésében tudjanak segíteni a viselőjének. Azonban mielőtt ezt megtennénk, létre kell hozni azt a szabályrendszert, amely keretet ad a fejlesztéseknek. Ezen az új technológiai piacon az elsődleges kihívás a biztonság és a bizalom megteremtése. Mind az ISO 13482 mind az ASTM F48 konszenzusos szabványok kialakításán dolgozik, hogy a kutatók, fejlesztők és az exoskeletonok vásárlói bízhassanak abban, hogy a berendezések biztonságára és teljesítményére vonatkozó állításokat hitelesítették. A szabványos vizsgálati módszerek kialakítása lehetővé teszik a tanúsítási folyamatokat, így a felhasználók jobban bíznak az általuk megvásárolt és telepített exoskeletonokban.

FELHASZNÁLT IRODALOM

[1] B.R. da Costa and E.R. Vieira, Risk factors for work-related musculoskeletal disorders: a systematic review of recent longitudinal studies, American Journal of Industrial Medicine. (2010). 53(3): pp. 285-323.

[2] Indecon, Economic Impact of the Safety Health and Welfare at Work Legislation, Department of Enterprise, Trade, and Employment: Dublin, (2006).

[3] M. Stattin and B. Järvholm, Occupation, work environment, and disability pension: A pros-pective study of construction workers. Scandinavian Journal of Public Health, (2005), 33(2): pp. 84-90.

[4] R. S. Mosher, "Handyman to Hardiman," SAE Transactions, vol. 76, no. 1, pp. 588–597, 1967.

[5] E. Guizzo and H. Goldstein, "The rise of the body bots," IEEE Spectrum, vol. 42, no. 10, pp. 42–48, 2005.
[6] H. Kazerooni, "Exoskeletons for human power augmentation," 2005 IEEE/RSJ International Conference on Intelligent Robots and Systems, IROS, pp. 3120–3125, 2005.
[7] L. M. Mooney, E. J. Rouse, and H. Herr, "Autonomous exoskeleton reduces metabolic cost of human walking during load carriage," Journal of NeuroEngineering and Rehabilitation, vol. 11, no. 1, p. 80, 2014.
[8]] H. Kawamoto and Y. Sankai, "Power assist system HAL-3 for gait disorder person," in Lecture Notes in Computer Science, vol. 2398. Springer, Berlin, Heidelberg, 2002, pp. 196–203.
[9] V. Klamroth-Marganska, J. Blanco, K. Campen, A. Curt, V. Dietz, T. Ettlin, M. Felder, B. Fellinghauer, M. Guidali, A. Kollmar, A. Luft, T. Nef, C. Schuster-Amft, W. Stahel, and R. Ri-ener, "Threedimensional, task-specific robot therapy of the arm after stroke: A multicentre, parallel-group randomised trial," The Lancet Neurology, vol. 13, no. 2, pp. 159–166, 2014.
[10] J. M. Donelan, Q. Li, V. Naing, J. A. Hoffer, D. J. Weber, and A. D. Kuo, "Biomechanical energy harvesting: Generating electricity during walking with minimal user effort," Science, 2008.
[11] T. Lam, "Contribution of Feedback and Feedforward Strategies to Locomotor Adaptations," Journal of Neurophysiology, vol. 95, no. 2, pp. 766–773, 2005.
[12] J. L. Pons, "Witnessing a wearables transition," Science, vol. 365, no. 6454, pp. 636–637, 2019.
[13] V. Sanchez, C. J. Walsh, and R. J. Wood, "Textile Technology for Soft Robotic and Autono-mous Garments," Advanced Functional Materials, vol. 31, no. 6, 2021.
[14] C. Simpson, B. Heurta, S. Sketch, M. Lansberg, E. Hawkes, and A. Okamura, "Upper extremity exomuscle for shoulder abduction support," bioRxiv, pp. 1–11, 2020.
[15] H. K. Yap, J. H. Lim, F. Nasrallah, J. C. H. Goh, and R. C. H. Yeow, "A soft exoskeleton for hand assistive and rehabilitation application using pneumatic actuators with variable stiffness," in Proceedings – IEEE International Conference on Robotics and Automation, vol. 2015-June, no. June, 2015, pp. 4967–4972.
[16] A. T. Asbeck, S. M. De Rossi, I. Galiana, Y. Ding, and C. J. Walsh, "Stronger, smarter, softer: Next-generation wearable robots," IEEE Robotics and Automation Magazine, vol. 21, no. 4, pp. 22–33, 2014.
[17] K. Kusek, "The $3 million suit," 2014. [Online]. Availab-le:https://news.harvard.edu/gazette/story/2014/09/the-3-million-suit/
[18] H. Kobayashi and K. Hiramatsu, "Development of muscle suit for upper limb," in IEEE Interna-tional Conference on Robotics and Automation, 2004. Proceedings. ICRA '04. 2004, vol. 3, no. April. IEEE, 2004, pp. 2480–2485 Vol.3
[19] I. Koo, C. Yun, M. V. Costa, J. V. Scognamiglio, T. A. Yangali, D. Park, and K.-J. Cho, "Deve-lopment of a meal assistive exoskeleton made of soft materials for polymyositis patients," in IEEE International Conference on Intelligent Robots and Systems, 2014, pp. 542–547
[20] D. Park, I. Koo, and K.-J. Cho, "Evaluation of an improved soft meal assistive exoskeleton with an adjustable weight-bearing system for people with disability," in Rehabilitation Robotics (ICORR), 2015, 2015.

[21] D. Chiaradia, M. Xiloyannis, C. W. W. Antuvan, A. Frisoli, and L. Masia, “Design and embed-ded control of a soft elbow exosuit,” in 2018 IEEE International Conference on Soft Robotics (RoboSoft). Livorno, Italy: IEEE, apr 2018, pp. 565–571.
[22] S. J. Park and C. H. Park, “Suit-type Wearable Robot Powered by Shape-memory-alloy-based Fabric Muscle,” Scientific Reports, vol. 9, no. 1, 2019.
[23] C. M. Thalman, Q. P. Lam, P. H. Nguyen, S. Sridar, and P. Polygerinos, “A Novel Soft Elbow Exosuit to Supplement Bicep Lifting Capacity,” in IEEE International Conference on Intelli-gent Robots and Systems. IEEE, 2018, pp. 6965–6971.
[24] D. Copaci, E. Cano, L. Moreno, and D. Blanco, New Design of a Soft Robotics Wearable Elbow Exoskeleton Based on Shape Memory Alloy Wire Actuators; Hindawi Applied Bionics and Biomechanics 2017. https://doi.org/10.1155/2017/1605101
[25] Koh TH, Cheng N, Yap HK and Yeow C-H (2017) Design of a Soft Robotic Elbow Sleeve with Passive and Intent-Controlled Actuation. Front. Neurosci. 11:597. doi:10.3389/fnins.2017.00597
[26] T. Nguyen, C. Trinh, T. Danh Le „An Adaptive Fast Terminal Sliding Mode Controller of Exer-cise-Assisted Robotic Arm for Elbow Joint Rehabilitation Featuring Pneumatic Artificial Muscle Actuator” Actuators. 2022; doi:10.3390/act9040118
[27] ISO 13482:2014 Robotok és robotszerkezetek. Személysegítő robotok biztonsági követelményei (ISO 13482:2014)
[28] ISO 10218-1:2011 - Robotok és robotszerkezetek. Ipari robotok biztonsági követelményei. 1. rész: Robotok (ISO 10218-1:2011)
[29] ISO 10218-2:2011 - Robotok és robotszerkezetek. Ipari robotok biztonsági követelményei. 2. rész: Robotrendszerek és összehangolásuk (ISO 10218-2:2011)
[30] ISO/TS 15066 Robotok és robot szerkezetek. Kollaboratív robotok
[31] Bostelman R and Hong T (2018). Test methods for exoskeletons—lessons learned from indust-rial andresponse robotics In Wearable Exoskeleton Systems: Design, Control and Applications. S. Bai, G.SVirk, and T Sugar (Eds.) Institution of Engineering Technology, 335–361.
[32] Lowe, Brian & Billotte, William & Peterson, Donald. (2019). ASTM F48 Formation and Stan-dards for Industrial Exoskeletons and Exosuits. IISE Transactions on Occupational Ergonomics and Human Factors. 7. 1-8. 10.1080/24725838.2019.1579769.

ENGINEERS IN THE PRIVATE SECURITY SECTOR

MÉRNÖKÖK A MAGÁNBIZTONSÁGI SZFÉRÁBAN

STEIN Vera[1]

Abstract

The article deals with the successful incorporation of security engineering graduates into the labour market, the rules governing their activities, and the practices of private security employers. It sheds light onto that in higher education, as well as in public education, a major change of approach is needed to produce engineering students with the skills and competences who are able to develop themselves to meet the demands of the labour market.

Keywords

security engineer, security engineering, property protection, private security, law enforcement, education

Absztrakt

A tanulmány a biztonságtechnikai mérnöki diplomával rendelkezők munkaerőpiaci érvényesülésével, a tevékenységüket meghatározó szabályokkal, és magánbiztonsági alkalmazási gyakorlatukkal foglalkozik. Rávilágít, hogy a felsőoktatásban, csakúgy, mint a közoktatásban is, jelentős szemléletváltásra van szükség ahhoz, hogy a munkaerőpiaci elvárásoknak megfelelő képességekkel és készségekkel bíró, önfejlesztésre képes mérnökhallgatókat képezzünk.

Kulcsszavak

biztonságtechnikai mérnök, biztonságtechnika, vagyonvédelem, magánbiztonság, rendvédelem, oktatás

[1] stein.vera@bgk.uni-obuda.hu | ORCID: 0000-0002-8868-1677 | assistant lecturer, Óbuda University | tanársegéd, Óbudai Egyetem

BEVEZETÉS

A biztonság megteremtésében az állam, az önkormányzati- és rendészeti szervek, valamint a rendvédelmi tevékenységet végző társadalmi szervek mellett a magánbiztonsági szolgáltatási ágazat is komoly szerepet játszik. [1] A megfelelő közbiztonság fenntartásához összehangolt, egymást inkább támogató és kiegészítő működést kell megvalósítani, ezért lassan elmosódni látszik a magán- és a közbiztonság közti határ: „…nemzetközi tendencia a magánbiztonság térnyerése, expanziója, amelynek hátterében többek között a rendőrségek kapacitásainak megváltozott irányú eloszlása és a költséghatékonyság áll. Az államok, kormányok rájöttek, hogy a rendészeti monopólium szigorú fenntartása mellett, bizonyos feladatok, különösen egyes háttértevékenységek privatizálhatók, kiszervezhetők. Ezáltal egyre nagyobb igény jelentkezik a teljes körű vagyonvédelem kiépítésére, illetve a meglévő biztonságvédelmi rendszerek folyamatos fejlesztésére, bővítésére." [2]

Tanulmányunkban a biztonságtechnika szakokon végzett mérnökök piaci környezetben való érvényesülésének lehetőségeit, tevékenységüket meghatározó szabályokat, és a jelenleg érvényes szakmai gyakorlatot vesszük górcső alá.

Ehhez először a magánbiztonsági szolgáltatási területet kell megvizsgálni, hiszen egy szerteágazó, és részleteiben is nagyon komoly különbségekkel bíró, mégis egységes jegyeket képviselő területről beszélhetünk.

Itt kell azonban megjegyezni, hogy a biztonságtechnikai végzettséggel rendelkező diplomások számára lehetséges állások közé tartoznak a biztonsági vezetői pozíciók is a magánbiztonsági cégek potenciális megrendelőinél, de erre majd a későbbiekben fogunk kitérni.

Mint ahogyan az az élet minden területén tapasztalható, az online tér, és az informatikai szolgáltatások egyedi, semmivel össze nem téveszthető sajátosságokkal bírnak, így vizsgálatunkat most nem terjesztjük ki a kiberbiztonsággal foglalkozó szakterületekre. A magánnyomozói tevékenység pedig nem feltétlenül igényel biztonságtechnikai mérnöki közreműködést, ezért ezt a területet is kihagyjuk a vizsgálatból. A fent említett szolgáltatásokra nem, hanem csak a klasszikus magánbiztonsági szolgáltatókra, és a biztonságtechnikai gyártó-, és forgalmazó cégekre összpontosítunk.

Természetesen, az az evolúciós tendencia – amit a COVID19 járvány alatt bekövetkező törvényszerű változások csak méginkább felgyorsítottak – informatikai rendszerek használatát feltételezi, miszerint a – szakzsargonban csak élőerős tevékenységnek nevezett – emberi erőforrások alkalmazását egyre több területen veszi majd át a technológiai eszközök célirányos és komplex használata. [3] Azonban itt kell megemlíteni, hogy különösen a biztonságtechnika területén a jövőben sem fog teljesen kiszorulni az emberi tevékenység, csupán az egyre inkább képzettebb, rugalmasan alkalmazkodni képes humánerőforrás felé fog eltolódni a hangsúly.

A tanulmányban magánbiztonsági szolgáltató, valamint biztonságtechnikai eszközöket, rendszereket forgalmazó, és ezeket kivitelező cégek vezetőivel készített interjúk árnyalják azt a képet, mely a piaci és oktatási helyzetről kialakulhat az olvasóban a Biztonságpiac évkönyv 2013-2021. kiadványok áttekintésekor.

A vizsgálat időszerűségét indokolja, hogy a felsőoktatási intézmények működésük során mindinkább olyan nehézségekkel találják magukat szemben, melyeknek a megoldása nem megkerülhető, ha életben kívánnak maradni. Az oktatás a nonprofit jellegét elveszíteni látszik, legyen szó egyaránt állami, vagy alapítványi fenntartásról. A hallgatók bevonzása,

megtartása, valamint a munkaerőpiac számára releváns kompetenciákkal és tudással rendelkező diplomások kibocsátása mind-mind olyan szempontok, melyekre jóval komolyabb hangsúly került, mint az ezt megelőző évtizedekben. Bizonyos értelemben fontosabbá vált a képzés módszertana, mint maga a megszerezhető tudás. A munkáltatók körében egyre inkább uralkodó az a nézet, hogy egy leendő munkatárs esetében a cégprofil- és megbízásspecifikus ismeretek még megtaníthatóak, de a hibás szemlélet nehezen, vagy nem korrigálható, és ugyanígy a biztos alapok sem pótolhatóak. Pontosan a biztonságtechnikai szakma szerteágazó volta is ezt a hozzáállást látszik erősíteni.

Kezdetnek a magánbiztonság területén végzett mérnöki munka jogi szabályozását és a tevékenység felügyeletét tekintjük át. Ezt követően ismertetjük a céginterjúk alapján megismert szolgáltató, forgalmazó, és kivitelező vállalkozások működésében rejlő, a diplomás biztonságtechnikai mérnökök számára releváns foglalkoztatási és szakmagyakorlási lehetőségeket. Végül a vázolt helyzetből az oktatásra fókuszálva levonható tanulságok és konklúziók következnek majd.

A TEVÉKENYSÉG KERETEI

A vagyonvédelemi törvény, valamint a végrehajtásáról szóló BM rendelet értelmében vagyonvédelmi rendszert tervező, szerelő tevékenység végzéséhez biztonságtechnikai, híradástechnikai, távközlési, mechanikai, illetve villamosmérnöki szakterületen szerzett BSc, vagy MSc diploma az előírás. A törvény szövege értelmében tervezésnek, szerelésnek minősül az „elektronikai vagy mechanikai vagyonvédelmi rendszerek tervezése, telepítése, szerelése, üzemeltetése, felügyelete, karbantartása, javítása”, mely a rendőrség által kiállított igazolvány és érvényes felelősségbiztosítás birtokában végezhető.[4] [5]

Jogi szabályozás és tevékenységfelügyelet

„A 2012-ben hatályba léptetett, átalakított vagyonvédelmi törvény nehéz helyzetbe hozta a magánbiztonsági ágazatot. Ennek a változtatásnak estek áldozatul a biztonságtechnikai tervezők is, akiknek a helyzete meglehetősen bizonytalanná vált. A megváltozott jogszabályi környezetben a Személy-, Vagyonvédelmi és Magánnyomozói Szakmai Kamara nem tarthatja nyilván a biztonságtechnikai tervezőket, nem felügyelheti szakmai tevékenységüket. A korábban szabályozott szakmagyakorlási jogosultsági rendszer, a jól működő továbbképzési, vizsgáztatási rendszer, a részletes nyilvántartási rendszer (névjegyzék) jelenleg nem működik.” [6]

Az ellenőrzés átkerült a Magyar Mérnöki Kamarához (MMK). Kormányrendelet határozza meg az engedélyhez kötött szakmagyakorlási tevékenységek körét, ennek értelmében az elektronikus vagyonvédelmi rendszerek tervezése már az építményvillamossági tervezési szakterülethez tartozik. [7]

Fent idézett cikkében [6] Tóth Attila arról is említést tesz, hogy komoly ellentmondás áll fenn az MMK tervezőkre vonatkozó kötelező kredit előírásai, és az egyetemi képzések számára irányadó jogszabályi képzési és kimeneti követelmények által meghatározott kreditértékek között. Így a szakképzettség megfelelőség megállapításakor a kamara nem veszi figyelembe a területspecifikus képzéseken megszerezhető kreditszámokat, és azoktól eltérő követelményeket támaszt a tervezői jogosultságot kérvényezőkkel szemben.

Ehhez kapcsolódva azt is taglalja, hogy fontos lenne a szakterületen biztosítani a folyamatos szakmai ellenőrzést és a tudásbázist megújító továbbképzések lehetőségét, mivel a biztonságtechnikai rendszerek „tervezésénél nem csupán az elektronikai, elektrotechnikai fogalmakkal, illetve a vonatkozó szabványokkal kell tisztában lennie a tervezőnek, hanem jóval szélesebb látókörrel kell rendelkeznie. A biztonságtechnikai tervezőnek ismernie kell a különféle építészeti, gépészeti megoldásokat, ismernie kell a védendő objektum minden részletét, megközelíthetőségét, a környezetének bűnügyi fertőzöttségét, ezek alapján pedig kockázatelemzést kell végeznie." [6] Nem tesz említést azonban arról, hogy egy mérnök a tervezéskor semmiképpen nem hagyhatja figyelmen kívül az általa tervezett rendszer telepítésében, üzemeltetésében résztvevő emberi erőforrás sajátosságait, és ezeknek a biztonságtechnikai rendszerek esetében talán még komolyabb figyelmet kell szentelni, mint más mérnöki szakterületek esetében, hiszen az üzemeltetők már nem feltétlenül rendelkeznek szakirányú képzettséggel.

A magánbiztonsági cégek működési gyakorlata

Kezdetnek tekintsük át azon potenciális megrendelők körét, ahol a vagyonvédelemből fakadóan a leggyakoribb az igény biztonsági eszközök igénybevételére, illetve biztonsági rendszerek telepítésére.

A legkézenfekvőbb elhatárolás, hogy a megbízó magánszemély, vagy jogi személy.

Ha csak a háztartásokat tekintjük, ma már sokkal gyakoribb, hogy a gépjárművünk, de főleg a lakóingatlanunk legalább mechanikus, vagy még inkább elektronikus védelmébe beruházunk. A legegyszerűbb biztonsági záraktól a legösszetettebb, komplex védelmi rendszerekig széles a paletta. A spektrum egyik végén a lakosság számára az üzleti forgalomban elérhető eszközök állnak, melynek beüzemeléséhez és működtetéséhez sem feltétlenül szükséges szakember. Ide sorolhatók a legkézenfekvőbb megoldásokon – a ma már akár mobiltelefonnal is vezérelhető, és felügyelhető biztonsági kamerákon – túl például a szénmonoxid- és füstérzékelő eszközök is, hiszen ezek is szerepet játszanak az emberi élet védelmében, és a vagyon biztonságának megőrzésében. A kínálat másik végén a komplex távfelügyeleti rendszereket találjuk, melyek valamelyik magánbiztonsági szolgáltató cég felügyelete alatt állnak és kerültek kiépítésre.

Ha a megbízó nem magánszemély, megkülönböztethető a szolgáltatás aszerint, hogy fixen telepített, vagy időszakosan alkalmazott, illetve mobil biztonságtechnikai eszközöket kell-e a szolgáltatás során igénybevenni. Ha egy bevásárlóközpont, vagy kereskedelmi létesítmény biztonsági felügyeletét kell ellátni, nyilván egész másfajta tervezői és kivitelezői gondolkodást igényel, mint ha egy fesztivált, koncertet, konferenciát vagy sportesemény kell biztosítani. Utóbbiak esetében kombinálódhat a fixen telepített eszközök, és a rendezvény sajátosságai miatt szükséges mobil eszközök használata, mely a tervezést, telepítést és üzemeltetést változékonyságánál, és a különböző technikai rendszerek illesztési igényénél fogva jelentősen megnehezítheti.

Más megközelítésben érdemes a magánbiztonsági szolgáltatásokat a megbízók céljai szerint is megkülönböztetni. Pontosan az informatikai fejlődés által megvalósuló „rendkívül dinamikus evolúciós folyamat" [8] teszi lehetővé a mind komplexebb biztonságtechnikai rendszerek telepíthetőségét, melyek már nem kizárólag az objektumok védelmében játszanak szerepet, de munkavédelmi szempontból is jelentőséggel bírnak, és más egyéb, például munkaügyi vagy belső ellenőrzési információk kinyerésére is alkalmasak lehetnek.

Említhetnénk itt példának az egyre korszerűbb és népszerűbb beléptető rendszereket. Bankok, irodaházak, gyárak, egyes oktatási intézmények, követségek, közigazgatási épületek stb. ma már szinte elképzelhetetlenek ezek nélkül. Termelő vállalatoknál telepített biztonságtechnikai rendszerek esetében sokszor nem is lehet megállapítani, hogy az objektumvédelmi funkció, és a folyamatok nyomonkövethetőségét célzó belső ellenőrzési funkció közül melyik a megbízó számára a lényegesebb.

Akár biztonsági vezetői státuszban, akár biztonsági rendszert tervező mérnökként kerül a biztonságtechnikai mérnök a folyamatba, már a háttérben zajló folyamatokhoz is valamennyire értenie kell, és a biztonságtudatosság növelését is célul kell kitűznie. „Nem elégséges, ha a biztonság a munkavállalók, a gazdasági vezetők szemében az marad, ami volt: szükséges rossz. A biztonság leggyengébb láncszeme leggyakrabban maga az ember. Aki nem tudja, hogy a biztonság érte, és a munkájáért, annak zavartalanságáért fenntartandó állapot, az maga is mulaszt, nem gondolva arra, hogy ezzel a saját és munkáltatója anyagi érdekei ellen is vét.” [9]

Bár a törvény kimondja, hogy a hatálya alá eső tervező-szerelő tevékenységre irányuló megállapodást írásba kell foglalni, szerződést kell kötni, de nincs nevesítve, hogy a biztonsági rendszer telepítésének kötelező feltétele lenne tervdokumentáció készítése, és ellenőrző hatóság sincs megjelölve, ami ennek meglétét, vagy minőségét lenne hivatott vizsgálni, mint például építkezéseknél az építési engedély esetében. Ez a tény kiszolgáltatottabbá teszi a biztonságtechnikai végzettséggel rendelkező mérnököket, hisz csupán a magánbiztonsági cég vezetésének hozzáállásán múlik, hogy igényli-e egyáltalán a tervező mérnökök alkalmazását, vagy megoldja a rendszerek telepítését, és üzemeltetését más módon. Gyakori ebben a viszonylatban, hogy egy több évtizedes tapasztalattal rendelkező biztonságtechnikai szerelő a biztonságtechnikai mérnöknek konkurenciája lehet.

Nehezíti a helyzetet az a gyakorlat is, hogy a fogyasztói társadalomban az eszközök-, illetve rendszerek meghibásodásának kezelésekor kevésbé a javítás, sokkal inkább a csere a bevett szokás, így a szakértelem látszólag háttérbe szorul. Látszólag, mert egy esetleges meghibásodás során sokkal eredményesebben tud működni a mérnök, ha rendszerében látja a feladatot, és tisztában van az általa használt eszközök alapvető felépítésével, és működésével.

További elhelyezkedési lehetőségként tekinthetünk a biztonságtechnikai képzettségű diplomások számára a biztonságtechnikai eszközöket gyártó, fejlesztő illetve forgalmazó cégekre, itt viszont gyakran előfordul, hogy szívesebben alkalmaznak informatikust, és villamosmérnököt a biztonságtechnikai mérnök helyett.

Bár a statisztikai adatok más képet mutatnak, mégis egyértelműen megállapítható, hogy a magyarországi magánbiztonsági piac nem túl nagy, a valódi munkát végző cégek munkaerőpiaci kereslete a diplomások tekintetében alacsony, ami a szűken vett szakmában való elhelyezkedést megnehezíti. [10] Így alakulhat ki ebben a szegmensben az a munkaadói nézet, hogy biztonságtechnikai mérnökökből túlképzés és túlkínálat van.

Azoknál a cégeknél, ahol a biztonságtechnikai mérnök tervezőként kerül alkalmazásba, alapvetően kétféle foglalkoztatási, munkaszervezési stratégia figyelhető meg. Az egyik – a horizontális munkaszervezés szerint működő – vállalkozásfajta kettéválasztja a tervezői, és a kivitelezői funkciókat. A tervezői felelősség már nem terjed ki a telepítés és beüzemelés során bekövetkező esetleges kényszerű változtatásokra. Gondoljunk csak arra

a helyzetre, amikor a biztonsági rendszer telepítése az adott objektum építésével párhuzamosan zajlik, és olyan, előre nem látható problémák merülnek fel a kiépítése során, amelyek szükségessé teszik az eredeti tervektől való eltérést. Ilyenkor problémássá válik a felelősség kérdése, kinek, meddig terjed, hol a kivitelezést irányító mérnök, és hol a tervező felelősségének a határa. A vertikális megközelítés szerint egy tervező a terven szereplő első vonaltól az utolsó beüzemelt eszközig végigköveti a folyamatot, tervezőként, és kivitelezőként is egyaránt gondolkozik. Ez a hozzáállás lényegesen kevesebb hibalehetőséget rejt magában, bár tény, hogy foglalkoztatási szempontból bonyolultabb helyzetet eredményez.

Itt kell azonban megjegyezni, hogy amennyiben csak egy találomra kiragadott példát, a bankokat tekintjük, azt is látnunk kell, hogy bank és bank elvárásai között is olyan különbségek lehetnek, amiért bizonyos szolgáltatóknak megéri szakosodni adott cégekre. Ezért említettük a tanulmány bevezetőjében, hogy a cégspecifikus ismeretek gyakran nem szerezhetők meg a felsőoktatásban, csak a szakma gyakorlása során.

KONKLÚZIÓ

A biztonságtechnika területén komoly hátrány, hogy a szakmaspecifikus középfokú képzés hiányzik az oktatási struktúrából. Amíg a gépészetben, építőiparban, mechatronikában, villamossági területen stb. a megfelelő szakirányú középiskolából kikerülő diákok felsőfokú tanulmányaik során a már megszerzett szakmai tudást és affinitást tudják tovább kamatoztatni, addig ugyanez a biztonságtechnika területén nem működik. Legkorábban a felsőoktatásban találkoznak a hallgatók ilyen irányú ismeretekkel, mely a szakmaiság elmélyítésére nincs jó hatással.

Ha nem bocsátkozunk bővebb elemzésbe, csak egy kiragadott példa kapcsán nézzük a biztonságtechnikai mérnökök szakterületén zajló fejlődési folyamatokat, és megvizsgáljuk – az egyre inkább elterjedőben lévő – okosotthonokkal kapcsolatos teendőket, látszik, hogy a komplex rendszerek tervezése, telepítése, üzemeltetése, valamint karbantartása több műszaki szakterület összehangolt működését kívánná meg. Ez ma még gyerekcipőben jár, és nemhogy nem kiforrott, de sokszor még alig üzemképes is. Hiszen egy ingatlan biztonsági rendszere, mely integrálva van a gépészeti és villamos rendszerrel is, mindhárom szakterület tekintetében hozzáértést követel meg a telepítőtől, ahol jobb esetben a megrendelővel szemben csak egy informatikust találunk, akinek a szakmai támogatás tekintetében a villanyszerelő, és a gépész segítségére kell hagyatkoznia, biztonságtechnikai szakember meg aztán végképp sehol nincs a történetben. Így sem a rendszerekben rejlő lehetőségek nem használhatók ki, sem optimális megoldásról nem beszélhetünk, de gyakran komoly és hosszan megoldatlan műszaki hibák okozója ez a gyakorlat.

A magánbiztonsági szférában új trend lép az insource helyébe, az outsourcing. „Azok a cégek, amelyeknek a járvány miatti korlátozások következtében visszaesett a bevételük, és emiatt szigorítani kellett a költségvetésükön, az információbiztonsági és a kiberbiztonsági feladatokat már úgy oldják meg, hogy a biztonsági szolgáltatásokat is szolgáltatásként veszik igénybe. Ez egyébként szorosan összefügg az Európai Unió Ipar 4.0 koncepciójában megfogalmazott, a digitalizáció és a felhőalapú megoldások erősítését célként kitűzött fejlesztésekkel, amelyekhez nem csak új szemlélet, hanem új feladatok is kapcsolódnak.” [11]

Ugyanilyen jellegű, a biztonságtechnikát célzó trend lenne célszerű a munkaerőpiac több területén is, így a biztonságtechnikai végzettséggel rendelkező mérnökök szaktudása

sokkal jobban kiaknázhatóvá válna, és nem csupán a magánbiztonság területén tevékenykedő cégek jelentenének számukra potenciális álláslehetőséget.

A fiatal mérnöki tudományok, mint a mechatronika és ugyanígy a biztonságtechnika területén is érvényes az a megállapítás, hogy – hiszen pontosan ez az igény hozta létre őket önálló tudományterületként – az egyre komplexebbé váló műszaki feladatok megoldására egyre sokrétűbb, és más alaptudományokat is integrálni képes mérnöki tudást állíthassunk a megrendelők szolgálatába. Olyannyira összetett gondolkodást igénylő területekről van szó, hogy adott feladat megoldásánál sokszor éppen annyira fontossá válhat a jogi- és gazdasági környezet ismerete, figyelembevétele, mint maga a műszaki feladat. A rendszerben gondolkodás az igazi segítség a problémamegközelítésben.

Időszerű példa erre a 2023-ban szigorodó kamerás megfigyelési szabályok témája, melyek a jelentősen módosuló európai GDPR (General Data Protection Regulation – egységes adatvédelmi szabályozás) szabályok miatt lépnek életbe. A változások kifejtését mellőzve megállapítható, hogy amennyiben a tervező, és/vagy üzemeltető nem tartja be a kamerahasználatra vonatkozó új adatkezelési szabályokat, komoly GDPR-bírság kiszabására számíthat. Még abban az esetben is, amikor a biztonságtechnikai mérnök feladata már nem terjed ki az üzemeltetésre, a szolgáltatási szerződés jogkövetkezményeként a bírság megfizetését az üzemeltető visszaterhelheti a rendszer tervezőjére, annak munkáltatójára, hiszen a helytelenül, a szabályozást figyelmen kívül hagyó tervezésből is eredhetnek olyan nem megfelelések, melyek a bírság kiszabásához vezethetnek. [12]

Mindezek tükrében egyértelműen látszik, hogy az egyetemi mérnökképzés során nem célszerű azt a régebbi gyakorlatot követni, hogy a leendő diplomások minden munkáltató számára releváns ismeretanyagot, lexikális tudást kapjanak a képzésük során, sokkal inkább olyan képességek, készségek, és szemléletmód átadása kell legyen a cél, melyek segítségével a mérnök képessé válik – bármelyik speciális szakterület esetén – az önképzésre, a rendelkezésre álló ismeretanyag összegyűjtésére, értelmezésére valamint helyes használatára.

Továbbiakban a szerző – az Óbudai Egyetem Biztonságtudományi Doktori Iskolájának PhD hallgatójaként – oktatásmódszertani kutatásai során a biztonságtechnikai mérnökök fent bemutatott helyzetelemzését felhasználva kívánja tovább vizsgálni a prjektalapú oktatást támogató módszereket az egyetemi mérnökképzésben.

FELHASZNÁLT IRODALOM

[1] Körkérdés, Biztonságpiac Évkönyv 2013., Biztonságpiac.hu Kft., ISSN 2061-6082, pp. 89-90.

[2] Lippai Zsolt: Könyvismertetés a Biztonsági vezetői kézikönyvről, Magyar Rendészet 2020/4. pp. 249—253. DOI: 10.32577/mr.2020.4.17

[3] A magánbiztonság határai, Biztonságpiac Évkönyv 2015., Biztonságpiac.hu Kft., ISSN 2061-6082, pp. 11-13.

[4] 2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól I./1.§.(4)

[5] 22/2006. (IV.25.) BM rendelet a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól szóló 2005. évi CXXXIII. törvény végrehajtásáról

[6] Tóth Attila: A biztonságtechnikai tervezők helyzete, Bolyai Szemle 2018/01., NKE, ISSN 1416-1443, pp. 45-53.

[7] 266/2013. (VII.11.) Korm. rendelet az építésügyi és az építésüggyel összefüggő szakmagyakorlási tevékenységekről
[8] A biztonságtechnikai rendszerek evolúciója, Biztonságpiac Évkönyv 2015., Biztonságpiac.hu Kft., ISSN 2061-6082, pp. 193-194.
[9] A gazdasági vezetők és a biztonságtudatosság, Biztonságpiac Évkönyv 2015., Biztonságpiac.hu Kft., ISSN 2061-6082, pp. 86-87.
[10] Amikor Justitia istennő kezében megremeg a mérleg, Biztonságpiac Évkönyv 2021., Biztonságpiac.hu Kft., ISSN 2061-6082, pp.129-131.
[11] Mádi-Nátor: A maradék illúziómat is elvesztettem, Biztonságpiac Évkönyv 2021., Biztonságpiac.hu Kft., ISSN 2061-6082, pp.112-115.
[12] Officina.hu Gazdaság és adózás rovat: GDPR kamerás megfigyelés 2023: ezek az új szabályok léptek életbe, https://officina.hu/gazdasag/191-gdpr-kameras-megfigyeles-szabalyai, letöltve: 2023.02.22.

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