ISSN 2676-9042

Vol 3, No 1, 2021.

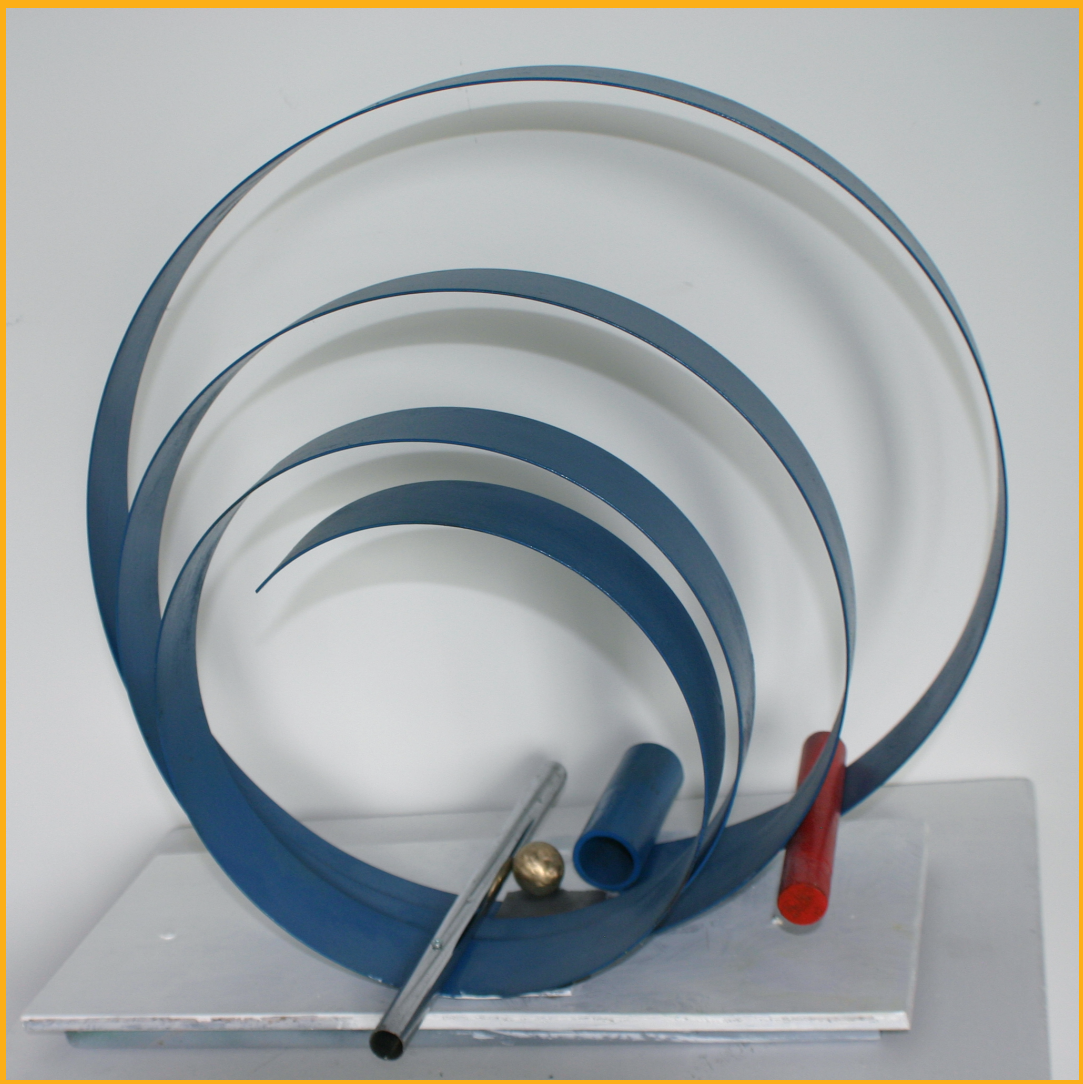
2021, III. évf. 1. szám

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
ÉZSIÁS István
sculptor/szobrászművész
Transversal statue | **Transzverzális** című szobra látható

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	Élelmiszerbiztonság
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
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, articles, book reviews of the broad discipline of security science for professionals working in or related fields of security science, thereby developing security awareness and security culture.	A **folyóirat célja** a biztonságtudomány területén, vagy ahhoz kapcsolódó területeken dolgozó szakemberek és a téma iránt érdeklődők számára a biztonságtudomány tágan értelmezett diszciplináris keretébe tartozó tanulmányok, kutatási jelentések, beszámolók, könyvismertetők megjelentetése, s ennek révén a biztonságtudatosság és a biztonsági kultúra fejlesztése.
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.	**Megjelenés** negyedévente, jellemzően magyar, eseti jelleggel idegen nyelven. Konferenciákhoz és témákhoz kapcsolódóan különszámok, tematikus számok alkalmi jelleggel magyar, vagy idegen nyelven jelennek meg.
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.	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.
Articles in the Safety and Security Sciences Review are archived in the Digital Archives of Óbuda University (ÓDA). 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 Biztonságtudományi Szemle folyóiratban megjelenő cikkek az Óbudai Egyetem Digitális Archívumában (ÓDA) archiválásra kerülnek. 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

ALSHAMAILEH, Lafee

lafee.alshamaileh@uni-obuda.hu

My Doctoral Study is focused on Aviation Security, biometrics and Transportation Security Administration Areas. My main Doctoral research interest is based about the effect of Risk Management on Biometric Systems in Aviation industry. I have a BSc degree in Aviation and Cosmonautics form State Flight Academy of Ukraine. My MSc degree was in Aircraft maintenance repair and Diagnostics from Kirovograd Flight Academy of the National Aviation University in Ukraine. I have worked for 4 years as maintenance Engineer in one Aviation company in Amman, Jordan.

A doktori tanulmányaim a repülésbiztonságra fókuszálnak, biometriára és a TSA-ra. A fő doktori kutatásaim a repülésiparban alkalmazott biometrikus rendszerek kockázatmenedzsment hatásaira épül. BSc diplomat szereztem Repülés és kozmoutazás területen az Ukrán Állami Repüléstudományi Akadémián. Az MSc diplomám Repülőgép karbantartás és diagnosztikából szereztem az Állami Kirovograd Repüléstudományi Akadémián. 4 évet dolgoztam mint karbantartó mérnök egy repüléstechnikai cégnél Ammanban, Jordánban.

BÁLINT Márton

balint.marton@phd.uni-obuda.hu

My name is Marton BALINT. I joined the PHD School of Obudai University at 40 years, following my studies of economics at the Foreign School of Economics in Budapest and at University of Montreal. At present I am working with the building of electrical networks. During my work I was involved in several cases when the security of a secure, reliable, and continuous electrical supply was at stake, and the level of danger that a breach is these securities needed to be assessed for the population, the institutions and our everyday life. At this point I felt the need to further study the question of security and to know its widespread details, and the Obudai University, along with the guidance of Mr Dr. Endre Szucs offers great opportunities in this field. Drones are the basis of my studies, the use of which are far more exceeding the hobby type of application and can be source of real danger in our lives.

Bálint Márton vagyok, 40 évesen iratkoztam be az Óbudai Egyetem Doktori Iskolába. Ezt megelőzően tanulmányaimat először a Külkereskedelmi Főiskola Közgazdasági Karán, majd a Montreali Közgazdasági Egyetemen folytattam. Jelenleg villamos hálózatok építésével foglalkozom. Ennek során találkoztam számos olyan esettel, melyek során a biztonságos, megbízható és folyamatos áramellátás biztosításának a veszélyét kellett megoldani, illetve átgondolni, hogy ezen veszélyek milyen kockázatokat jelentenek a lakosságra, intézmények működésére és a megszokott mindennapjainkra. Ekkor fogalmazódott bennem meg az igény arra, hogy mélyebben tanulmányozzam a biztonság kérdését, megismerni annak rendkívül sokrétű részleteit. Az Óbudai Egyetem doktori iskoláján, Dr. Szűcs Endre irányításával alkalmam nyílik mélyebb tudást szerezni ezen a téren. Munkám fókuszába a drónokat állítottam, melyek hobbi felhasználáson felül sokkal komolyabb szerepet is tudnak kapni, és ezáltal veszélyt jelenteni a mindennapjaink biztonságára is.

BELÁZ Annamária

belaz.annamaria@uni-obuda.hu

ANNAMÁRIA BELÁZ (1993) is an expert of public administration specialized in administrative science, and she obtained her bachelor's degree in 2015 and her master's degree in 2017 in the field of public administration at the National University of Public Administration. She won the "Information Security

BELÁZ ANNAMÁRIA (1993) okleveles közigazgatási szakértő, alapdiplomáját 2015-ben, mesterfokozatát 2017-ben szerezte közigazgatás-tudományi szakirányon a Nemzeti Közszolgálati Egyetemen. Elnyerte a Hétpecsét Információbiztonsági Egyesület által adományozott, „Az év információbiztonsági

Thesis of the Year 2017" award donated by the Seven Seal Information Security Association in the MA diploma category. She is currently a doctoral candidate at the Óbuda University Doctoral School on Safety and a law student at the Faculty of Law at Eötvös Loránd University. In 2017 and 2018, she was one of the main organizers of the "National Cyber Competition" higher education simulation competition. Since its launch in 2017, she has been the editor of the professional journal Banki Reports. She teaches courses related to the regulation of info-communication systems, information and cybersecurity, and project management. Her research field is the development of information security in public administration from a legal and technical point of view, regulating cybersecurity in Hungary, Europe, and at an international level, with particular regard to strategy development.

szak-és diplomadolgozata 2017" díjat diplomadolgozat kategóriában. Jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskola doktorandusza, az Eötvös Loránd Tudományegyetem Állam- és Jogtudományi Kar jogász szakos hallgatója. 2017-ben és 2018-ban a „Nemzeti Kiberverseny" felsőoktatási szimulációs verseny főszervezője volt. 2017 óta a Bánki Közlemények című szakmai folyóirat szerkesztője. Az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Karán az infokommunikációs rendszerek, az információbiztonság szabályozása mellett projektmenedzsment témájú tárgyakat oktat. Kutatási területe a közigazgatás információbiztonságának fejlesztése jogi és műszaki szempontokból, a kiberbiztonság hazai, európai- és nemzetközijogi szabályozása különös tekintettel a stratégiaalkotásra.

BESENYŐ János

besenyo.janos@uni-obuda.hu

János Besenyő holds PhD of Military Science and habilitated doctorate from History. He works full time as Associate professor for the Óbudai University, Doctoral School for Safety and Security Sciences, as the head of the Africa Research Center. Between 1987 - 2018 he was a professional soldier and served several times in Africa (Western Sahara, Darfur) and Afghanistan in various peacekeeping and military missions. His research interests include contemporary and re-cent history of Africa, migration and the Middle East, military conflicts, peacekeeping, military logistics, terrorism, and Christian-Muslim reletionship on the continent. He is teaching not only at Óbudai University, Doctoral School for Safety and Security Sciences, but ELTE Doctoral School of History, EKE Doctoral School of History, and National University of Public Service, Doctoral School of Military Sciences. He wrote several books and articles. His most recent publication is „Hungary and the crisis in Western Sahara" (Monarchia Ltd, 2020).

Besenyő János, a hadtudományok doktora, habilitált történész. Az Óbudai Egyetem Biztonságtudományi Doktori Iskolájának Afrika Kutatóintézetét vezeti. 1987 és 2018 között hivatásos katonaként szolgált, amely időszakban több afrikai és afganisztáni béketámogató műveletben vett részt. A kutatási tevékenységébe tartozik Afrika Új és legújabb kori történelme, migráció, Közel-Kelet, katonai konfliktusok, békeműveleti tevékenység, katonai logisztika, valamint az afrikai keresztény és muzulmán közösségek kapcsolata. Nem csak az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában, hanem az Eszterházy Károly Egyetem Történelemtudományi Doktori Iskolájában, az Eötvös Lóránt Tudományegyetem Történelemtudományi Doktori Iskolájában és a Nemzeti Közszolgálati Egyetem, Hadtudományi Doktori Iskolájában is oktat. Több könyv és tanulmány szerzője, legutóbbi könyve „Magyarország és a nyugat-szaharai krízis" amelyet a Monarchia Kiadónál jelentetett meg 2020-ban.

DOMJÁN András

andras.domjan@gmail.com

In terms of my qualifications, I am an electrical engineer, a certified safety engineer and a blasting engineer. I am using my knowledge in the field of counter-terrorism within the framework of the Police as the Head of Department of the Information Protection Department, and I am currently expanding my knowledge as a PhD student at the University of

Végzettségeimet tekintve villamos mérnök, okleveles biztonságtechnikai mérnök és robbantástechnikai szakmérnök vagyok. A megszerzett ismereteimet a Rendőrség keretein belül a terrorelhárítás területén, információvédelmi osztály vezetőjeként kamatoztatom, jelenleg az Óbudai Egyetem Biztonságtudomá-

Óbuda Doctoral School of Security Studies. My research area is to examine the possibilities offered by the radio spectrum monitoring system to be used as part of complex establishment protection. Within this - in particular - the detection of remotely controlled IED and eavesdropping equipment based on parasitic RF radiation.

nyi Doktori Iskola PhD hallgatójaként bővítem ismereteimet. A kutatási területem a komplex objektumvédelem részeként alkalmazásra kerülő rádióspektrum monitor rendszer nyújtotta lehetőségek vizsgálata. Ezen belül konkrétan a parazita RF-sugárzás alapján történő távvezérlésű IED-, és lehallgató berendezések detektálása.

FÁBIÁN Péter

fabianpeter@topcopgroup.com

The author is a police officer, lawyer, criminologist, national security analyst. For many years he worked as a criminal intelligence officer at various police departments. He has been working as a leader in the private security sector for more than 20 years. Private forensic security expert, security consultant for several large multinational corporations. Expert of the PTE Center for Defense Research. He is a doctoral candidate of the Doctoral School of Security Sciences of the University of Óbuda. His research topic is private security.

A szerző rendőrtiszt, jogász, kriminológus, nemzetbiztonsági elemző. Sok évig bűnügyi hírszerzőként dolgozott a Rendőrség különböző szerveinél. Több, mint 20 éve a magánbiztonsági szektorban dolgozik vezetőként. Igazságügyi magánbiztonsági szakértő, több multinacionális nagyvállalat biztonsági tanácsadója. A PTE Védelmi Kutatások Központ szakértője. Az Óbudai Egyetem Biztonságtudományi Doktori Iskola doktorjelöltje. Kutatási témája a magánbiztonság.

FARKAS Tibor

Farkas.Tibor@uni-nke.hu

Tibor Farkas is a military technology manager (MA), associate professor at the Department of CIS of the University of Public Service -Ludovica, Faculty of Military Sciences and Officer Training. In 2010 he earned PhD degree in the field of Military Sciences, and habilitation in Military Engineering Sciences in 2015. His major research areas are the infocommunication system management; the defence infocommunication system; and the infocommunication support for NATO multinational operations.

Farkas Tibor okleveles haditechnikai menedzser, a Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar, Híradó Tanszék egyetemi docense. 2010-ben szerzett Phd fokozatot Hadtudományok területen, illetve 2015-ben habiltált doktor címet Katonai Műszaki Tudományok területén. Fontosabb kutatási területei közé tartozik az infokommunikációs rendszerek tervezése és szervezése; a védelmi szféra infokommunikációs rendszerei; valamint a NATO többnemzeti műveletek infokommunikációs támogatása.

HETYEI Csaba

hetyei.csaba@uni-obuda.hu

I started my college studies at College of Dunaújváros, where I obtained a bachelor's degree in mechanical engineering in 2013. After the BSc, I attended quality control engineering and mechanical engineering master programs, which I had completed at the University of Dunaújváros. After obtaining my MSc degree, I continued my studies at the Doctoral School on Safety and Security Sciences of the Óbuda University, where with my college and university professor dr. habil. Ferenc Szlivka, who accepted me as his PhD student for the Modelling and optimization of the interaction of wind turbines PhD topic. After my BSc studies, I worked as an R&D engineer

Dunaújvárosi Főiskolán kezdtem el főiskolai tanulmányaimat, ahol 2013-ban gépészmérnöki alapdiplomát szereztem. Ezt követően minőségügyi szakmérnöki majd gépészmérnöki mester képzésre jártam, amit már a Dunaújvárosi Egyetemen fejeztem be. MSc-s diplomám megszerzése után tanulmányaimat az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában folytattam, ahol főiskolai és egyetemi tanárom dr. habil. Szlivka Ferenc témavezetésével Szélkerekek egymásra hatásának áramlástani modellezése, optimalizálása doktori témával és az ezt kiegészítő tudományterületek megismerésével foglal-

in an engineering office, then as a product support engineer for CAD and simulation (FEA, CFD) software.

kozom. BSc-s tanulmányaim után egy mérnökirodában K+F mérnökként dolgoztam, amit idővel a CAD és szimulációs (VEM, CFD) szoftverek terméktámogatása felváltott.

HORVÁTH Ádám Béla

kutatas@horvath-adam.hu

Ádám Horváth graduated in 2006 at the Faculty of Business and Economics of the University of Pécs. After that, he had worked as an IT consultant for a medium-sized company in Hungary for four years. During this period, he was involved in the projects aimed the implementation of SOA-based systems and in the management of EU-funded IT projects. He worked as a teaching assistant between 2010 and 2016 and was able to give lectures in Zagreb, Graz, Würzburg and Winnipeg, and in 2018 he graduated from the Doctoral School for Security Sciences at the University of Óbuda and in 2019 he obtained a qualification in Data Center Systems Engineering. His research interests include the measurement of the convergence (or divergence) of the IT infrastructure and information security maturity of small and medium-sized enterprises and its impact on business competitiveness, as well as the use of data mining methods in social science analyses. He is currently working at the Data Science and Engineering Department of Faculty of Informatics in ELTE-University.

Horváth Ádám 2006-ban diplomázott a Pécsi Tudományegyetem Közgazdaságtudományi Karán. Ezt követően négy évig IT-tanácsadóként dolgozott egy magyarországi középvállalkozásnál. Munkája során részt vett SOA-alapú rendszerek bevezetésében, valamint EU-támogatott IT-projektek menedzselésében. 2010 és 2016 tanársegédként dolgozott és vendégoktató tarthatott előadásokat Zágrábban, Grazban, Würzburgban és Winnipegben, és 2018-ban szereztett abszolutóriumot az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában, valamint 2019-ben Adatközponti Rendszermérnöki képesítést szerzett. Kutatási területe a kis- és középvállalatok informatikai infrastruktúrájának és az információbiztonsági érettsége konvergenciájának (illetve divergenciájának) valamit annak az üzleti versenyképességre gyakorolt hatásának mérése, valamint az adatbányászati módszerek felhasználása társadalom-tudományi célú elemzések során. Jelenleg az Eötvös Lóránd Tudományegyetem Informatikai Karának Adattudományi és Adattechnológiai tanszékén dolgozik.

HRONYECZ Erika

hronyecz.erika@gmail.com

In 2008, she obtained an MSc degree at the Zrínyi Miklós National Defense University as a graduate security and defense policy expert. She began her doctoral studies at the Doctoral School of Military Sciences at the University of Public Service. Her research field is the common foreign and security policy of the V4s, including the direction and process of armed forces modernization and development activities in the member states. She is currently student at the Doctoral School on Safety and Security Sciences.

2008-ban a Zrínyi Miklós Nemzetvédelmi Egyetemen szerzett MSc diplomát, mint okleveles biztonság- és védelempolitikai szakértő. A doktori képzést a Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskolájában kezdte el, ahol kutatási területe a V4-ek közös kül- és biztonságpolitikája, azon belül a tagállamok haderőfejlesztési tevékenységek iránya és folyamata. Jelenleg a Biztonságtudományi Doktori Iskola hallgatója.

KOLLÁR Csaba

kollar.csaba@uni-obuda.hu

Communications engineer, certified communications specialist, head of electronic information security, doctor of economics (PhD), 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,

Kommunikációtechnikai mérnök, okleveles kommunikációs szakember, elektronikus információbiztonsági vezető, a közgazdaságtudományok doktora (PhD), tanácsadó, coach, mediátor. Kutatási területe a digitális kor társadalmi vetületei és gazdasági hatá-

the development of information security awareness, human-robot interaction, smart city, artificial intelligence, and social credit system, domotics. He is an associate professor at the Óbuda University, lecturer and supervisor at the National University of Public Service Doctoral School of Military Engineering. He is a registered mediator of the Ministry of Justice, and 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.

sai, 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 egyetemi docense, a Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola oktatója, témavezetője. Az Igazságügyi Minisztérium regisztrált közvetítője (mediátora), elnök a szakmai képesítő vizsgákon (OKJ). 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.

KOVÁCS Éva

kovacs.eva1@uni-obuda.hu

Kovács Éva received her qualification at the Faculty of Humanities and Social Sciences of Károli Gáspár University of the Reformed Church in Hungary as English language and literature and History teacher. She has pursuited her career in education teaching General English and English for Specific Purposes of various levels at technical universities, language schools and companies. She has been an accredited oral language examiner at two different language examination centers (ECL, EUROexam). At her workplace, the Faculty of Law Enforcement, University of Public Service, she teaches English for law enforcement student, and is the co-author of the textbook 'Crime and Law Enforcement'. She leads courses at Donát Bánki Faculty of Mechanical and Safety Engineering, such as Advanced Technical English, and she also introduced Security Technology English as a new ESP subject into the university's training program. She has been conducting her doctoral studies at the Doctoral School on Safety and Security Sciences. Her specialized field of research pertains to teaching the language of security technology within the scope of ESP, gaining novel scientific results through its practical implementation.

Kovács Éva angol nyelv és irodalom, valamint történelem szakos bölcsészeti és pedagógiai végzettséget szerzett a Károli Gáspár Református Egyetem Bölcsészettudományi Karán. A különböző szintű általános és szakmai angol nyelv oktatását hazai műszaki egyetemeken, nyelviskolákban és vállalatoknál végezte. Két nyelvvizsgaközpont (ECL, EUROexam) akkreditált szóbeli vizsgáztatója. Munkahelyén, a Nemzeti Közszolgálati Egyetem Rendészettudományi Karán rendészeti szaknyelvet oktat, a „Crime and Law Enforcement" tankönyv társszerzője. Az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Karán felsőfokú angol műszaki szaknyelvet tanít, az angol biztonságtechnikai szaknyelv oktatását önálló tárgyként vezette be az egyetem képzési programjába. Az Óbudai Egyetem Biztonságtudományi Doktori Iskolájának doktorandusz hallgatója. Kutatási területe az angol biztonságtechnikai műszaki szaknyelv oktatása, valamint a tevékenység során kapott tapasztalatok és új tudományos eredmények rendszerbe állítása.

MIKLÓS Gellért

gellert.miklos@gmail.com

The author is a lawyer, infocommunication specialist. He is currently a doctoral student at the Doctoral School of Security Sciences of the University of Óbuda. His studies and research focus on domestic and international regulation of cyber security, data security and data protection. He is also a regulatory manager for an international telecommunications

A szerző jogász, infokommunikációs szakjogász. Jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskolájának doktorandusz hallgatója. Tanulmányai és kutatásai középpontjában a kiberbiztonság, adatbiztonság és adatvédelem hazai és nemzetközi szabályozása áll. Emellett egy nemzetközi távközlési vállalat jogszabályi megfeleléssel foglalkozó

company, specializing in the regulation of IoT devices and permanent roaming. On a daily basis, he deals with the evaluation of legislation and draft legislation relevant to the above topic, and with the examination of the legal compliance of various products and services.

munkatársa, szakterülete az IoT eszközök és az állandó barangolás (permanent roaming) szabályozása. Napi szinten foglalkozik a fenti témakörben releváns jogszabályok, jogszabály tervezetek értékelésével, a különböző termékek, szolgáltatások jogszabályi megfelelőségének vizsgálatával.

NAGY Barna

nagy.barna@blx.hu

Msc in Electrical Engineering (Budapest University of Technology and Economics) Engineer-Economist (Corvinus University) Legal studies for engineers (Eötvös Lóránt University) Information Security Engineer (Óbuda University). Certified Ethical Hacker (CEH). At the beginning of his professional career, he worked as a software engineer, software architect and maintenance engineer in the Hungarian telecommunication and financial sectors. He is currently working as a software architect and lead developer for Blumenthal Consulting Kft. He is responsible for the design and development of software products that support industrial safety and maintenance and automatic regulatory compliance. Areas of professional interest and research: implementing information security in the software development, information security issues in embedded systems, language processing (NLP) in legal documents.

Okleveles villamosmérnök (BME-VIK), mérnök-közgazdász (Corvinus Egyetem), jogi szakokleveles mérnök (ELTE-ÁJK), információbiztonsági szakmérnök (Óbudai Egyetem). Etikus hacker (CEH) és szoftvermérnök. Szakmai karrierének elején a magyar telekommunikációs és pénzügyi szektorban nagyvállalati információs rendszerek fejlesztésével, tervezésével és üzemeltetésével foglalkozott. Jelenleg a Blumenthal Consulting Kft szoftver architectje és vezető fejlesztőjeként dolgozik. Iparbiztonsági és karbantartási területeket támogató, illetve az automatikus jogszabályfigyelést megvalósító szoftverek tervezéséért és fejlesztéséért felelős. Szakmai érdeklődési és kutatási területei: információbiztonság megvalósítása a szoftverfejlesztésben, beágyazott rendszerek információbiztonsági kérdései, nyelvfeldolgozás (NLP) jogi környezetben.

ŐSZI Arnold

oszi.arnold@bgk.uni-obuda.hu

I started my studies in Bánki faculty at 2004. My field was Security and safety technology. Then I applied for teacher degree. I started to teach biometric identification. At the same time started to research biometrics. Later I finished my studies at ÓBUDAI UNIVERSITY Doctoral School on Safety and Security Sciences, where I get my PhD. Now I am a teacher in Óbuda University as an Assistant Professor.

2004-ben kezdtem meg a tanulmányaimat a Bánki karon. A területem a biztonságtechnika volt. Ezután jelentkeztem a tanárszakra. Biometrkus azonosítást kezdtem tanítani. Ugyanebben az időben kutatni kezdtem a biometriát. Később az ÓBUDAI EGYETEM Biztonságtudományi Doktori Iskolájában fejeztem be a tanulmányaimat, ahol PhD fokozatot szereztem. Jelenleg oktató vagyok az Óbudai Egyetemen adjunktusként.

RAJNAI Zoltán

rajnai.zoltan@bgk.uni-obuda.hu

Zoltán RAJNAI (1962) engineer colonel, dean of the Óbuda University, Donát Bánki Faculty of Mechanical and Security Engineering, operating manager of the Doctoral School of Security Sciences of the University, cyber coordinator of Hungary. He completed his military studies at the Máté Zalka Military Technical College and then at the Miklós Zrínyi Military Academy. From 1993 he worked as a university adjunct at the Miklós Zrínyi Military Academy and the

RAJNAI Zoltán (1962) mérnök ezredes, az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar dékánja, az Egyetem Biztonságtudományi Doktori Iskolája operatív vezetője, Magyarország kiberkoordinátora. Katonai tanulmányait a Zalka Máté Katonai Műszaki Főiskolán, majd a Zrínyi Miklós Katonai Akadémián végezte. 1993-tól a Zrínyi Miklós Katonai Akadémián, illetve a Zrínyi

Miklós Zrínyi National Defense University, the predecessor institutions of the University of Public Service. Under its leadership the Telecommunication Department at NKE was established in 2008 by merging the Faculties of Telecommunication of the János Bolyai Faculty of Military Engineering and the National Defense University. He received his doctorate in 2001 and his habilitation in 2006. He won a research scholarship named after János Bolyai of the Hungarian Academy of Sciences. Between 2007 and 2011 he was the Hungarian program director of the COMMIT French-Hungarian International Science (R & D & I) project, and at the same time a guest lecturer in France at the Military Technical College in Rennes. He is the president of the Puskás Tivadar Telecommunication Comrades Association since 2012. His research interests include security of communication networks in qualified periods, protection of critical infrastructure, information security.

Miklós Nemzetvédelmi Egyetemen, a Nemzeti Közszolgálati Egyetem jogelőd intézményeiben dolgozott egyetemi oktatóként. A vezetésével alakult meg 2008-ban a Bolyai János Katonai Műszaki Kar és a Nemzetvédelmi Egyetem Híradó tanszékeinek összevonásával az NKE-n ma is működő híradó tanszék. 2001-ben doktori fokozatot, 2006-ban habilitációt szerzett. Elnyerte a Magyar Tudományos Akadémia Bolyai Jánosról elnevezett kutatási ösztöndíját. 2007 és 2011 között a COMMIT francia-magyar nemzetközi tudományos (K+F+I) projekt magyarországi programigazgatója volt, ezzel párhuzamosan vendégoktató Franciaországban a Rennes-i Katonai Műszaki Főiskolán. 2012-től a Puskás Tivadar Híradó Bajtársi Egyesület elnöke. Kutatási területei: minősített időszakok kommunikációs hálózatainak biztonsága, kritikus infrastruktúra védelme, információbiztonság.

SZALÁNCZI-ORBÁN Virág

szalancziorban.virag@uni-obuda.hu

SZALÁNCZI-ORBÁN VIRÁG (1984) Logistics manager, economist, currently a PhD student at the Doctoral School for Safety and Security Sciences of the University of Óbuda. Research areas: logistics, network science, transport and transportation as critical infrastructure, information security. Title of the research topic: Increasing the logistics role of Hungary with the participation of systems logistics, security sciences and other interdisciplinary disciplines.

SZALÁNCZI-ORBÁN VIRÁG (1984) Logisztikai menedzser, közgazdász, jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában PhD hallgató. Kutatási terület: logisztika, hálózattudomány, közlekedés és szállítás mint kritikus infrastruktúra, információbiztonság. Kutatási téma címe: Rendszerlogisztikai, biztonságtudományi és más interdiszciplináris tudományágak közreműködésével Magyarország logisztikai szerepének növelése.

SZLIVKA Ferenc

szlivka.ferenc@bgk.uni-obuda.hu

I graduated in mechanical engineering with fluid dynamic specialization, and I worked within the same discipline during my doctoral studies. Since graduating, I have been researching in the fields of mechanical and agricultural sciences. Currently, I am a PhD supervisor at the Doctoral School on Safety and Security Sciences in Óbuda University, and I am a professor at the University of Dunaújváros and the Donát Bánki Faculty of Mechanical and Safety Engineering at Óbuda University. In addition to education and research, I was involved in founding the Kéményjobbítók Országos Szövetsége (National Association of Chimney Improvers), and the Országos Szélenergia Bizottság (National Wind Energy Commission), and I have been a member of COST MC since 2013.

Gépészmérnök képzést áramlástan szakirányon végeztem el, és ugyanezen a tudományágon belül tevékenykedtem doktori tanulmányaim alatt. Fokozatszerzésem óta a gépészeti és az agrárműszaki tudományokterületeken kutatok. Jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában vagyok témavezető, a Dunaújvárosi Egyetemen és az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki karon egyetemi tanárként oktatok. Oktatás és kutatás mellett részt vettem a Kéményjobbítók Országos Szövetsége és az Országos Szélenergia Bizottság megalapításában, illetve 2013-óta COST MC tagja vagyok.

SZŰCS Endre

szucs.endre@bgk.uni-obuda.hu

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

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

VÉGH Attila

vvscadaa.ph@gmail.com

Attila VÉGH (1974) has a bachelor's degree in Information Technology and a master's degree in Security Engineering. He works in the telecommunication industry and has more than 20 years experience in wireless technologies. He is a PhD student in Doctoral School of Safety and Security Sciences in the Óbuda University. As a technical scientific researcher he is currently conducting research on safety and security, especially issues of intelligent systems for public safety.

VÉGH Attila (1974) mérnök-informatikus, okleveles biztonságtechnikai mérnök. A telekommunikációs szektorban több mint húsz éves tapasztalatra tett szert a vezeték nélküli kommunikációs eszközök terén. Az Óbudai Egyetem Biztonságtudományi Doktori Iskolájának PhD hallgatója. Kutatási területe a közbiztonságban alkalmazott intelligens rendszerek alkalmazásának a vizsgálata

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 3, No 1, 2021. | 2021. III. évf. 1. szám

CONTENT | TARTALOM

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

Industrial and Operational Safety column | Ipar- és üzembiztonság rovat

Private Security column | Magánbiztonság rovat

Artificial Intelligence column | Mesterséges intelligencia rovat

Book Review column | Könyvismertetés rovat

DEVELOPMENT STRATEGIES OF THE VISEGRAD GROUP MEMBER STATES AND THEIR IMPACT ON THE SECURITY OF THE REGION

A VISEGRÁDI EGYÜTTMŰKÖDÉS TAGORSZÁGAINAK HADERŐFEJLESZTÉSI STRATÉGIÁI ÉS HATÁSA A RÉGIÓ BIZTONSÁGÁRA

FARKAS Tibor [1] – HRONYECZ Erika[2]

Abstract

There have been several events in Europe and the Central European region over the last decade, many of which have had a significant impact on the lives of both the region and the countries in the region. Since the mid-2010s, the security environment in Europe, including Central Europe, has undergone a dynamic and far-reaching change and this process continues today. In the countries of the Visegrad Group, a change of direction has also begun in the field of national defence, with the unified goal of implementing radical force development. The main efforts of the V4's defence policy at the international level continue to be to involve member countries' armed forces in international crisis management operations, in line with their membership obligations in NATO, the EU and the UN.

Keywords

Visegrad Group, force development, international cooperation, defence policy, security strategies

Absztrakt

Európában, illetve a közép-európai régióban számos olyan esemény történt az elmúlt évtizedben, melyek közül már sok egymagában is komoly hatással volt a térségre és országainak életére. A 2010-es évek közepétől az európai, ezen belül is a közép-európai biztonsági környezet dinamikus és nagymértékű változáson ment keresztül és ez a folyamat napjainkban is zajlik. Ismét előtérbe került a kollektív védelem, az európai országok megkezdték képességeik és erőik fejlesztését. A Visegrádi Csoport országaiban is megindult az irányváltás a honvédelem területén, egységesen célul tűzték ki a radikális haderőfejlesztés végrehajtását. Az V4-ek védelmi politikájának főbb erőfeszítései nemzetközi szinten továbbra is arra irányulnak, hogy a tagországok fegyveres erői részt vegyenek a nemzetközi válságkezelési műveletekben, összhangban a NATO-ban, az EU-ban és az ENSZ-ben való tagság kötelezettségeikkel.

Kulcsszavak

Visegrádi Együttműködés, haderőfejlesztés, nemzetközi együttműködés, védelempolitika, biztonsági stratégiák

[1] farkas.tibor@uni-nke.hu | ORCID: 0000-0002-8868-9628 | egyetemi docens/ associate professor | Nemzeti Közszolgálati Egyetem

[2] hronyecz.erika@gmail.com | ORCID: 0000-0003-2002-8521 | doktorjelölt/ PhD candidate | Nemzeti Közszolgálati Egyetem

BEVEZETÉS

A Visegrádi Négyek 1991-es alapításától kezdve számos perióduson ment keresztül a működés, együttműködés tekintetében. Az elmúlt három évtizedeben a tagállamokban, illetve a közép-európai térségben végbement változásoktól függően módosultak a célok és a prioritások, és ebből adódóan értelemszerűen mindig az adott nemzeti, nemzetközi szituációknak megfelelően változott a kooperáció dinamikája is. A 90-es években a V4 országok legfontosabb célkitűzése az volt, hogy megszabaduljanak a varsói szerződés örökségétől és csatlakozhassanak az euroatlanti térséghez, az EU és a NATO tagállamai lehessenek. Miután 2004-re minden részes állam tagjává vált mind az Észak-atlanti Szövetségnek, mind pedig az Európai Uniónak teljesítve ezáltal a korábban elérni kívánt eredményeket, a további együttműködés mellett döntve új célokat és feladatokat határoztak meg, melyek az uniós kül- és biztonságpolitikára, illetve a NATO-n belüli szerepvállalás megerősítésre irányultak, támogatva azt egy saját védelempolitika kidolgozásával.

A VISEGRÁDI ORSZÁGOK VÉDELMI EGYÜTTMŰKÖDÉSE

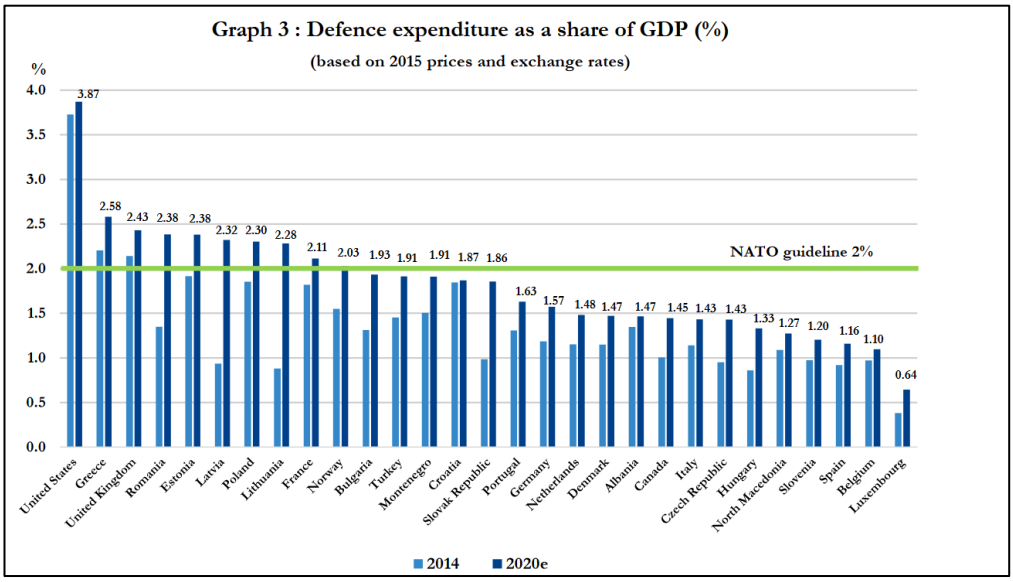
2014-ben a Visegrádi Együttműködés a szorosabb védelmi integráció mellett döntött. A V4-ek védelmi miniszterei ezen elhatározás megerősítéseként az alábbi két stratégiai dokumentumot írták alá: „Long Term Vision of the Visegrad Countries on Deepening their Defence Cooperation" és „Framework for Enhanced Visegrad Defence Planning Cooperation". Míg az előbbi a tagországok hosszú távú elképzelését fogalmazza meg a védelmi együttműködés fokozásáról a közös képességek és a védelmi ipar fejlesztése, többnemzeti alakulatok létrehozás, közös képzés, oktatás és gyakorlatok által, addig a másik dokumentum azokat irányokat és tevékenységeket foglalja össze, melyek területén megvalósulhatnak a közös védelmi célokat szolgáló beszerzések és fejlesztések. [1] A Visegrádi Együttműködés további mérföldkövének számított a védelemi együttműködés területén 2016-ban a V4 EU Harccsoport felállítása, illetve a NATO védelmi képességeinek szükséges kiegészítése céljából a V4 Közös Logisztikai Támogató Csoport (V4 JLSG HQ) megalakítása, melyet a NATO védelmi minisztereinek 2018. júniusában tartott találkozóján Brüsszelben jelentettek be. A fent nevezett védelmi együttműködést megerősítő legfontosabb intézkedések meghozatalához a 2010-es években bekövetkezett, a tagállamokat, illetve a térséget érintő biztonsági kockázattal járó események is hozzájárultak.

Az Észak-atlanti Szerződés Szervezetének és az Európai Uniónak a tagjaiként a Visegrádi Négyek országai az elmúlt két évtizedben a hagyományos katonai fenyegetést illetően példátlan biztonságot élvezhettek, de Európa szomszédságában a biztonsági környezet törékenyebbé vált, új típusú biztonsági kihívások jelentek meg, illetve már ismert, de korábban nem jelentős aktivitást mutató fenyegetések erősödtek meg, melyek már nem maradhattak, maradhatnak periférián az ellenük való hatékony felkészültséget és választ illetően. A V4-ek biztonságpolitikájának főbb céljai közé tartozik a terrorizmus elleni küzdelem - különös tekintettel a kibertérben történő támadásokra-, illetve az energiabiztonság szavatolása. Ez a két elem mind a négy országban elsőszámú biztonsági tényezőnek számít. Viszont a tagországokban egyéb területeket illetően már eltolódni látszanak a fontosság szintjei a biztonsági faktorok tekintetében. V4-es országok ugyanolyan tudatában vannak a fenyegetéseknek, de eltérő álláspontjuk van a kockázatok jellegét és mértékét tekintve. Míg Lengyelország az aktív orosz jelenlétet tartja fenyegető tényezőnek, addig az ellenőrizetlen

migráció növekedésével Budapest, Pozsony és Prága a kontinens déli részéből fakadó fenyegetést sokkal súlyosabbnak érzékeli, mint a keletről – Oroszországból - származó fenyegetést. [2]

A Krím-félsziget Oroszország által történt annektálása komoly hatással volt nemcsak a környező országok biztonságpolitikai helyzetére, hanem az egész euro-atlanti térség biztonságára és stabilitására. Az ukrán válság bekövetkeztével a NATO képességfejlesztési törekvései új értelemzést kaptak. Ráirányította a figyelmet a hosszútávú haderőfejlesztés fontosságára, emellett az azonnali bevethető erők nélkülözhetetlenségét is bizonyította, emellett világossá vált, hogy szükség van a valós katonai képességek meglétre. [3, p. 11] A 2014. tavaszán bekövetkezett esemény komoly, gyors és hatékony döntések meghozatalára kényszerítette a NATO-t. Szükségszerűvé vált a katonai képességek gyorsütemű és radikális megerősítése, kiemelkedő szereppel bírt ezen a területen a szövetségen belül is a NATO keleti tagállamainak nagyobb léptékű fejlesztése.

A 2014. szeptember elején megrendezett walesi csúcstalálkozón a tagállamok megerősítették elkötelezettségüket a kollektív védelem, a válságkezelés és a kooperatív biztonság mellett, és megállapodtak abban, hogy egységesen törekednek arra, hogy egy évtizeden belül elérjék a 2% -os GDP arányos védelmi kiadási szintet (lásd 1. sz. ábra), továbbá célul tűzték ki, hogy a védelmi kiadásokon belül a modernizációra fordított arány elérje a legalább 20% -ot. Ez a vállalás a V4-ek tagállamainak esetében hosszú távon is komoly kihívást jelent, legfőképp a három kisebb ország, Szlovákia, Csehország és Magyarország vonatkozásában, de az elmúlt 4 évet tekintve mind a négy tagállamban látható az érdemben tett erőfeszítés ezen a téren. A V4 országok haderőfejlesztési folyamatainak, programjainak már látható és számos területen látványos eredményei vannak.



1. Ábra: A tagállamok védelmi kiadásainak GDP-hez viszonyított aránya [4, p. 3]

CSEHORSZÁG VÉDELMI STRATÉGIÁJA ÉS HADERŐFEJLESZTÉSI TEVÉKENYSÉGE

Csehország, mint más egyéb országok biztonsági helyzetét számos tényező befolyásolja, határozza meg – nemzeti, regionális (európai) és globális–, amelyek jelentős kihívás elé állítják az országot. A Cseh Köztársaság jelenlegi helyzete szilárd, a különböző szövetségesi tagságai, együttműködései mindezt tovább erősítik. Az ország védelmének és biztonságának alapvető, meghatározó eleme a NATO kollektív védelmi rendszerében történő részvétel, az EU válságkezelési képességeinek fejlesztésében történő együttműködés és a partnerállamokkal történő kölcsönös összefogás. Az ország alapvető, létfontosságú érdeke a szuverenitásának védelme, a területi integritás, valamint az EU értékeinek megőrzése valamennyi területen a jogállamiságot és a lakosság jogait és szabadságát figyelembe véve. Az állam és a lakosság létfontosságú érdekeinek védelme alapvető kötelezettség, amelyek biztosítása alapjaiban teremtik meg az állam biztonságát. Az elemi, létfontosságú érdekek védelmét biztosítják mindazon stratégiai tervek és érdekek megőrzése is, amelyeket szem előtt tartva valósítható meg az ország komplex biztonsága. Ilyen stratégiai célok és érdekek: a biztonság és stabilitás, a helyi és regionális konfliktusok megelőzése és kezelése; az esetleges konfliktusok hatásainak enyhítése, valamint azok hatásainak enyhítése; a fegyverzet-ellenőrzés támogatása; a demokrácia, az alapvető szabadságjogok és a jogállamiság elveinek támogatása; gazdasági biztonság megteremtése és megóvása; a létfontosságú rendszerek megóvása és védelme; a kiberbiztonság megteremtése, valamint számos egyéb stratégiai terület. Az ország, mint nemzetközi szervezetek tagja mindazon tevékenységeket, eseményeket biztonsági fenyegetések közé sorolja, amelyeknek nincs közvetlen hatása a saját biztonságára, de a szövetségeseire igen.

Biztonsági érdekeinek védelme érdekében a Cseh Köztársaság átfogó, hierarchikus felépítésű biztonsági rendszert fejleszt ki, amely egyesíti a nemzeti és nemzetközi politikai, katonai biztonságot, lakosságvédelmet, gazdasági, pénzügyi, jogi és társadalmi szinten. A biztonsági rendszer működése, alrendszerei képességeinek kiépítése és fejlesztése, valamint a szükséges gazdasági és pénzügyi források biztosítása hosszú távú folyamat, amely során szem előtt kell tartani, hogy a rendszernek rugalmasan kell reagálnia a változó körülményekre, a biztonsági környezet változásaira és az új fenyegetésekre. [4, p. 26] [5]

A Cseh Köztársaság Védelmi Minisztérium - Hadtörténeti Intézet 2019-ben kiadta a Hosszú Távú Védelmi Stratégiáját (továbbiakban: stratégia), amely 2035-ig határozza meg az alapvető irányokat a katonai képességek fejlesztésére, valamint útmutatást nyújt a „Cseh fegyveres erők fejlesztési koncepciójának" és egyéb kapcsolódó dokumentumok, stratégiák időszakos felülvizsgálatához. A stratégia behatárolja a 2035-ig folyamatosan változó biztonsági környezetet, amelyre az országnak és a szövetségnek fel kell készülnie. Ennek elemei például az információs és kommunikációs technológia (IKT) intenzív és magas fokú fejlődése által kiterjesztett és megnövelt sebességű internet, amelynek egyes alkalmazásai (pl. közösségi média) az információs és pszichológiai műveletek színterei lettek. A NATO és az EU mellett a tagországoknak is meg kell tennie mindent annak érdekében, hogy a romló biztonsági környezet negatív hatásait a lehető legjobban lecsökkentsék.

A stratégia meghatározza továbbá a jövő biztonsági környezetének és erejének jellemzőit, amelyek közül a legfontosabbak az alábbiak [6, p. 12]:

- az állami- és nem állami szereplők elleni sikeres fellépes (aszimmetrikus);

- a teljes spektrumú katonai képességek megvalósítása, amely lehetővé teszi a sikeres fellépést a hagyományos hadszíntéren, az információs környezetben, a kibertérben;
- a stratégiai- és műveleti vezetés és irányítás részeként hatékony művelettervezés és (katonai) döntéshozatali folyamatok;
- rugalmasan reagáló, bevethető, expedíciós képességekkel rendelkező, korszerű haditechnikai eszközökkel felszerelt haderő;
- nemzetközi együttműködésben, többnemzeti műveletekben alkalmazható fegyveres erők hadtest szinten.

A napjaink és a jövőbeli biztonsági kihívásokra történő hatásos reagálás érdekében a Cseh Fegyveres Erő fejlesztése nélkülözhetetlen, a feladatainak meghatározása alapján a képességek és követelmények hozzárendelésre kerültek, amely behatárolja a haderőfejlesztés irányvonalait, legfontosabb elemeit. Ennek megfelelően a kormány biztosítja modernizációhoz szükséges anyagi támogatást. A Védelmi Minisztérium költségvetése az elmúlt néhány évben növekedett, amellyel biztosítani kívánják a fejlesztéseket és a szükséges egyéb költségek fedezetét. A minisztérium közel húsz éves kiadásának GDP-hez viszonyított arányát az 2. sz. ábra mutatja.

2. Ábra: A védelmi kiadások GDP-hez viszonyított aránya (szerkesztette a szerző a [7] [8] alapján)

A jelenlegi biztonsági fenyegetések és kockázatok alapján a Cseh Fegyveres Erők felépítésének átalakítása, és haderejének megerősítése nélkülözhetetlen hosszútávú feladat, amelynek elsődleges iránya a szárazföldi erők (harci) képességeinek bővítése, amelynek része a létszám növelése is. A technológia folyamatos fejlődésének köszönhetően a katonai fejlesztések elengedhetetlen elem lett a hagyományos fegyverek és haditechnikai eszközök mellett a speciális vezetés és irányítási rendszerek, a robotika által nyújtott speciális támogató rendszerek, a mesterséges intelligencia a nanotechnológia és a biotechnológia számos részterülete. A stratégia meghatározza azokat a területeket, amelyek fejlesztése nélkülözhetetlen a kitűzött célok elérése érdekében. Ezeknek megfelelően a fejlesztés területei a következők [6, pp. 18-24]:

- *hírszerzés és információs támogatás*, elsősorban a fegyveres erők vezetés és irányításának támogatására;

- *vezetés és irányítás, parancsnoki struktúra,* amely biztosítja a NATO FMN (Kapcsolt Műveleti Hálózat)koncepciót;
- *szárazföldi erők*, amely fejlesztés NATO követelményeknek és képességeknek megfelel (elsődleges cél két gépesített dandár fenntartása békeidőben), valamint C4ISTAR[3] rendszer integrációja;
- *légierő,* az ország és a szövetség légterének biztosítása 3D radarok, passzív megfigyelő rendszerek mellett földi légvédelmi rendszerek és repülőgépek
- *kibervédelem*, a kiberműveletek teljes spektrumához szükséges eszköz és képességfejlesztés;
- *különleges műveleti képesség*;
- *logisztika,* amely kiterjed az állandó és telepíthető logisztikai támogatásra a logisztikai infrastruktúra információs rendszerrel történő fejlesztésére;
- *infokommunikáció*, IKT alkalmazása a teljes spektrumú műveletek kiszolgálására és a katonai döntéshozatali folyamatok támogatására;
- *egészségügyi szolgálat,* a telepíthető egészségügyi létesítményekre és azok kiszolgálására, valamint a szakállomány és a nem egészségügyállomány felkészítésre összpontosítva;
- *katonai rendész;*
- *személyi fejlesztések*, toborzás, felkészítés, (ki)képzés, oktatás;
- *hadifelszerelés korszerűsítése*;
- *kutatás és fejlesztés, védelmi ipar*, a védelmi képességek biztosítása nemzeti fejlesztésekkel és technológiai/technikai eszközök gyártásával.

A megváltozott nemzetközi biztonsági helyzetre reagálva, a régió más szövetségesi tagállamaihoz hasonlóan a Cseh Köztársaság is felülvizsgálta védelmi stratégiáját, védelmi képességeit. Ennek megfelelően meghatározta azokat a nemzeti és szövetséges képességeket és követelményeket, amelyek elengedhetetlenül szükségesek a biztonság hatékony fenntartásához. Ennek érdekében megkezdte a Cseh Fegyveres Erők modernizációját, amely a személyi, technikai és felkészítési részterületeket is magába foglal.

MAGYARORSZÁG VÉDELMI STRATÉGIÁJA ÉS HADERŐFEJLESZTÉSI TEVÉKENYSÉGE

A globális biztonsági környezet változásaira történő reagálás, valamint a megújuló fenyegetések kezelésére irányuló törekvései folyamatos változásokat követelt meg a NATO tagállamoktól. A NATO az elmúlt húsz évben jelentős változáson ment keresztül mind szervezeti felépítését, mind képességét tekintve. A megújuló fenyegetésekre kizárólag innovatív reagálással lehet válaszolni, amely képes garantálni a Szövetség tagállamainak biztonságát. Ennek megfelelően az államok, így a régió országaihoz hasonlóan Magyarország is megkezdte ennek a folyamatnak a végrehajtását. A NATO válasza a jelenlegi fenyegetésekre (tömegpusztító fegyverek jelenléte, a világméretű terrorizmus okozta veszélyek, az energiaellátást fenyegető veszélyek, környezeti kihívások, a különböző kibertámadások, a hibrid

[3] C4ISTAR: Command, Control, Communications, Computers, Information/Intelligence, Surveillance, Targeting Acquisition and Reconnaissance (Vezetés, Irányítás, Kommunikáció, Számítógépek, Információ/Hírszerzés, Megfigyelés, Célzás, Felderítés)

hadviselés komplex alkalmazása, és a mindezekből következő komplex biztonsági következmények) a kollektív védelem, a vezetési struktúra folyamatos fejlesztése és formálása, a védelmi kiadások növelése, a haderőfejlesztés gyorsítása, a képességek megosztása valamint a közös gyakorlatok és kiképzések végrehajtása. [9]

A Kormány 1163/2020. (IV. 21.) Korm. határozata Magyarország Nemzeti Biztonsági Stratégiájáról (továbbiakban: stratégia) 2020. április 21-én jelent meg a Magyar Közlönyben, amely kiemelt jelentőségű az előzőekben leírt folyamatok sikeres végrehajtásában, mintegy keretet meghatározva a szükséges előrelépéseknek. A stratégia megfogalmazza, hogy ennek megvalósítása érdekében közös nemzeti erőfeszítéseket kell tenni, de a szövetségesi és európai uniós tagállami státusunk nagymértékben erősíti biztonsági helyzetünket. A nemzeti- és nemzetközi biztonság megvalósításának alapja a korszerű haditechnikai eszközökkel felszerelt magyar haderő, amely képes Magyarország függetlenségének, területi épségének és a lakosság védelmének biztosítására, és a szövetségesi védelmi feladatok ellátására.

A 179 pontból álló dokumentumnak már az első tíz pontján belül megfogalmazásra kerül, hogy „*2030-ra hazánk Európa öt, illetve a világ tíz legbiztonságosabb országának egyike kell legyen, egyfelől az ország magas szintű közbiztonságának fenntartása, másfelől egy regionális szinten is az egyik meghatározó, korszerű haderő felépítése révén, amely az exportképes hazai védelmi iparra támaszkodik. A haderő ütemes fejlesztése tovább bővíti annak lehetőségeit, hogy megvédjük alapvető értékeinket és érdekeinket valamint az euroatlanti biztonság aktív és hiteles hozzájárulói maradjunk a jövőben is. A sikeres Magyarország alapköveit a jelenben rakjuk le, de a jövőben is fontos a fenntartható fejlődés feltételeinek biztosítása, amelynek gazdasági alapját hazánk nemzetközi versenyképességének fokozása, a védelmi szektorban az ipari kapacitások kiépítése és fejlesztése, társadalmi pillérét pedig hazánk demográfiai helyzetének javítása képezi* [10, pp. 2101-2102].

A stratégia fontos dokumentum többek között abból a szempontból is, hogy nyomatékot ad a korszerű haderő szükségességének, de természetesen már a stratégia megjelenését megelőzően is történtek előrelépések haderőfejlesztési és beszerzési programok tekintetében. A Zrínyi 2026 Honvédelmi és Haderőfejlesztési Programot (Zrínyi 2026) 2016-ban indították útjára, mely programot 2017 januárjában hozta nyilvánosságra a Honvédelmi Minisztérium. Az átfogó katonai modernizációs program célja a haderőfejlesztés megvalósulása Magyarország hadiiparának felélesztésének segítségével. A stratégia 27. pontja is rögzíti, hogy válsághelyzet esetén hatékony védelmet és segítségnyújtást kifejteni képes haderő alapjai a Zrínyi 2026 kerülnek megteremtésre. A fent említett pont kimondja továbbá, „*hogy a NATO vonatkozó irányelvével összhangban – 2024-től – a bruttó hazai össztermék évi legalább 2%-ának felhasználása nyomán kialakításra kerül a hazánk nemzetközi kötelezettségei és nemzeti feladatai érdekében szükséges, regionális szinten is meghatározó haderőképesség”*. [10, p. 2103]

A nemzeti haderőfejlesztés célja, hogy az új kihívásokra történő új műveleti képességek és alkalmazási elvek megteremtésre kerüljenek, kiegészítve a küldetés alapú vezetéssel, és az ezek megvalósítását biztosító korszerű haditechnikai eszközök beszerzése megvalósuljon. Ennek a komplex és átfogó tevékenységnek biztosítania kell a haderő teljes technikai, szervezeti, személyi és vezetési rendszerének átalakítását.

A stratégia által meghatározottak biztosítását[4] a Zrínyi 2026 program összetett rendszere szavatolja a Magyar Honvédség számára, amelynek területei a következőkből tevődik össze.

A személyi állomány (hivatásos és szerződéses) feltöltöttségének növelése, amely mellett az Önkéntes Tartalékos Rendszer megerősítése is kiemelt fontosságú. A civil lakosság meggyőzése a honvédelem ügyének összetett és megújult módszereket követel meg, melynek egyik eleme a Honvédelmi Sportszövetség megújítása. A honvédelmi életpályamodell kialakítása biztosítja a fiatalok beáramlásának növelését akár szerződéses, akár hivatásos pályára. Az idei évben került fókuszba a nemzeti tisztképzés rendszerének átalakítása, amely ezen célokat szintén jelentős mértékben támogatja és az elkövetkező néhány évben megerősíti a felkészítését a fiatal tiszteknek.

A korszerű fegyverzeti és haditechnikai eszközök üzemeltetésének, valamint az új műveleti alkalmazáshoz szükséges vezetői képességek elsajátításának nélkülözhetetlen eleme a *kiképzés és felkészítés rendszerének átalakítása*, korszerűsítése.

A *fegyverzet és a haditechnikai eszközpark* korszerűsítése a szárazföldi és a légierő haderőnem valamennyi területén megjelenik. A gyalogsági harcjárművektől kezdve a tüzér- és páncéltörő tüzér képességek fejlesztését biztosító eszközökön át, a légvédelem fejlesztését és a különleges műveleti képességek továbbfejlesztését is tartalmazza a program. Az elmúlt években megkezdődtek ezen fegyverek, fegyverrendszerek beszerzése. A légierő képességének fejlesztése magába foglalja továbbá a szállító kapacitás növelését és harci képességek emelését.

A fegyverrendszerek mellet a *katonák egyéni harcászati felszerelésének* modernizációját is magába foglalja a program.

A korszerű haditechnikai eszközök megjelenése a honvédség harci kiszolgáló-támogató, *logisztikai rendszerének korszerűsítését* is magába foglalja a modernizáció, valamint a teljes logisztikai ellátó rendszer átalakítását, fejlesztését.

A NATO 2016-ban a kiberteret elfogadta ötödik műveleti dimenziónak a szárazföldi, légi, tengeri és az űr mellett, és nélkülözhetetlen elemeként ismerik el a szövetségi műveleteknek. Ennek megfelelően a hibrid hadviselés elleni fellépés elemeként megalakult és folyamatosan fejlődik a *kibervédelmi képesség* a Magyar Honvédségben

A meghatározott eszközök és képességek fejlesztése mellett átalakításra került a *Magyar Honvédség szervezete, vezetési struktúrája*, megalakult a Magyar Honvédség Parancsnoksága, valamint új hadrendi elemek alakultak. A folyamatosan változó stratégiai környezetben történő megfelelésnek ez az egyik alapvető eleme

Az új szervezetek és képességek kiszolgálása érdekében jelentős *infrastrukturális fejlesztésre* is sor kerül a program keretében, amely teljesen új létesítmények megépítésével, vagy meglévő infrastruktúra korszerűsítésével valósul meg.

[4] „A Magyar Honvédségnek jól felszerelt és jól kiképzett erőkkel, valamint rugalmas, hatékonyan alkalmazható, telepíthető és fenntartható, a szükséges mértékben interoperábilis képességekkel kell rendelkeznie, a mennyiségi mellett a minőségi mutatók javítására törekedve. Hagyományos országvédelmi és nemzetközi válságkezelési feladatai mellett egyaránt alkalmasnak kell lennie a tömeges bevándorlás okozta válsághelyzet, vagy a terrorveszély-helyzet kezeléséhez történő hozzájárulásra, a hibrid támadások elhárításában való szerepvállalásra, valamint a természeti vagy ipari katasztrófák következményeinek felszámolásában való közreműködésre. A haderőt úgy kell fejleszteni, hogy képes legyen hatásokat kiváltani a hazánk szempontjából releváns összes műveleti térben: a szárazföldön, a levegőben és a kibertérben egyaránt.” [10, p. 2115]

Az elmúlt évtizedekben nem volt ilyen mértékű haderőátalakítás és haderőfejlesztés, amely hozzájárult volna a feladatok maradéktalan és sikeres ellátásához, és az ország biztonságának szavatolásához. A haderőfejlesztési és modernizációs program minden részterületre kiterjedő fejlesztést takar, amelynek személyi, szervezeti és technikai komplexitása a siker elengedhetetlen feltétele. A hadsereg képességfejlesztése tehát a nemzetek összetett feladata, amelyet tovább nehezít, hogy az elmúlt évtizedekben lecsökkentetésre került a hadsereg létszáma, a technikai eszközök egy része pedig elavulttá vált.

LENGYELORSZÁG VÉDELMI STRATÉGIÁJA ÉS HADERŐFEJLESZTÉSI TEVÉKENYSÉGE

A Lengyel Köztársaság területi, népességi, gazdasági adottságait és adatait tekintve a V4-ek legnagyobb országa. Lengyelország az EU és a NATO határállamaként és a közvetlen orosz szomszédság tekintetében stratégiailag kiemelt jelentőséggel bír, területi adottságaiból kifolyólag meghatározó geopolitikai gondolkodással rendelkező állam. A Visegrádi Együttműködés közül a lefejlettebb és legnagyobb katonai erővel rendelkező Lengyelország a NATO-hoz és az EU-hoz történt sikeres csatlakozása után a V4-ek másik három tagországától eltérően nem építette le radikálisan haderejét. Földrajzi adottságai és történelmi tapasztalatai alapján ezt nem engedhette meg magának, csökkentette ugyan a védelmi kiadásokra, a haderőfejlesztésekre szánt összegeket, de a honvédelmi rendszer drasztikus amortizációját elutasította, mi több, már 2008-ban a védelmi szférát érintően egy precízen megtervezett, átfogó modernizációs programot indított el. Új parancsnoki struktúra került bevezetésre, és a hidegháború befejezése óta a legnagyobb beszerzési programot vezényleték le a szárazföldi erők és a légierők korszerűsítése terén. [11] Mindezek következtében viszonylag gyors ütemben sikerült a hadseregben az idáig zajló modernizációs folyamatokat véghez vinni. Lengyelország arra törekszik, hogy 2026-ig a GDP 2,4% -át fordítsa védelemre, ez a célkitűzés a legújabb nemzetbiztonsági stratégiában is megerősítésre került, de elképzelhetőnek tartják, hogy ez a 2,4%-os érték 2030-ra akár 2,5% -ra is nőhet. A legfrissebb NATO-adatok szerint Lengyelország jelenleg a GDP 2,05% -át költi védelemre, ez a kiemelkedő teljesítménynek számít nemcsak a V4-ek államaihoz viszonyítva, de a NATO tagországai között is. [12]

Ez elmúlt évek történéseit figyelembe véve megállapítható, hogy egy újabb nagyhatalmi verseny időszakába léptünk, mely szituáció a Kelet és Nyugat határvonalán elhelyezkedő Lengyelországtól fokozottabb felkészültséget és készenlétet követel meg. A Lengyel Köztársaság Nemzeti Biztonsági Stratégiája, mely reagál többek között Lengyelország régióban betöltött szerepére és az azzal járó esetleges kockázatokra, 2020. májusában került jóváhagyásra, felváltva ezzel a korábbi, 2014-ben elfogadott verziót. A biztonság és a védelem vonatkozásában alapvető állami dokumentum átfogó elképzelést kínál a Lengyel Köztársaság nemzetbiztonságának alakításáról annak minden dimenziójában. A dokumentumban Lengyelország a legsúlyosabb fenyegetésként Oroszország új birodalmi politikáját jelöli meg. A Grúzia elleni agresszió, a Krím illegális annektálása és a kelet-ukrajnai tevékenység megsértette a nemzetközi jog alapelveit, és aláaknázta az európai biztonsági rendszer pilléreit. A stratégiai dokumentum alapján Lengyelország biztonságát alapvetően meghatározó tényező továbbra is a transzatlanti és európai struktúrába történő beágyazódás, a NATO és az EU szövetségi rendszereken belüli aktív részvétel határozza meg. Kiemelkedő szerepet kap többek között a dokumentumban az energiabiztonság. Lengyelország ezenen

a területen a diverzifikációt szükségszerűnek tartja, mivel a lengyel, a közép-európai és a balkáni olaj- és gázpiacot továbbra is az orosz szállítások uralják, meg kell erősíteni a régió ellenálló képességét a gázellátás politikai nyomás eszközeként történő felhasználásának kockázatával szemben. A kiberbiztonságot illetően kiemelten jegyzi a dokumentum, hogy Oroszország a háború küszöbértéke alatti (hibrid jellegű) tevékenységeket végez, sokoldalú és átfogó akciókat hajt végre nem katonai eszközökkel ideértve többek között a kibertámadásokat is. Ezen a területen lényeges célkitűzés és egyben megoldandó feladat a stratégiai dokumentum szerint:

- növelni a köz- és magánszféra, valamint a katonai és polgári információs rendszerek ellenálló képeségét, hogy el tudják érni a kiberfenyegetések hatékony megelőzésének, leküzdésének és az azokra való reagálás képességét;
- az állam védelmi képességeinek megerősítése a nemzeti kiberbiztonsági rendszer folyamatos fejlesztésének biztosításával;
- képességek elérése a katonai műveletek teljes spektrumának lebonyolításához a kibertérben;
- nemzeti képességek fejlesztése a kiberbiztonsági megoldások és szolgáltatások tesztelése, kutatása, értékelése és tanúsítása terén;
- fejleszteni kell a kompetenciákat, a fenyegetésekkel és kihívásokkal kapcsolatos ismereteket és tudatosságot a közigazgatás alkalmazottainak és a társadalomnak a kiberbiztonság területén. [13]

Lengyelországban a kiberbiztonság katonai és civil téren történő fejlesztése magas szinten állt már a legújabb stratégiai dokumentum elfogadás előtt, 2019. februárjában kihirdették és elindították a CYBER.MIL.PL programot, amelynek célja, hogy átfogóan fejlessze Lengyelország azon képességeit, melyek segítségével le tudja küzdeni a kibertérben megjelenő fenyegetéseket. A program erejét és volumenét többek között a benne részt vevő intézmények is mutatják: Nemzeti Kiberbiztonsági Központ, Operációs Kiberbiztonsági Központ, Katonai Elhárítás, Katonai Infokommunikációs Intézet, Haditengerészeti Akadémia, Katonai Műszaki Akadémia, Területvédelmi Erők [14].

A stratégia alapján a fejlesztés fő területei a következők:

- *Kibervédelemi erők felállítása, kapacitásépítés;*
- *A2/AD-kapacitások, nagy hatótávolságú, precíziós csapásmérő képességek, légvédelmi és harckocsi-elhárító képességek fejlesztése;*
- *a lengyel különleges erők, illetve a Területvédelmi Erők megerősítése;*
- *a lengyel haditengerészet fejlesztése.*

SZLOVÁKIA VÉDELMI STRATÉGIÁJA ÉS HADERŐFEJLESZTÉSI TEVÉKENYSÉGE

A Szlovák Köztársaság a V4 országok legkisebb tagállama, az EU, a schengeni övezet és a NATO határállama. A 2000-es évektől kezdve Szlovákiában – hasonlóan mint Magyarországon és Csehországban - jellemző volt a haderő alulfinanszírozása, fokozott leépítése mind a humán, mind az eszközállományra vonatkozóan. Ennek kiszámítható következménye lett, hogy a legtöbb katonai felszerelés - mint például a sugárhajtású vadászgépek, a páncélos harcjárművek és a katonai radarok - elavult és rossz állapotban lévő eszköz korszerűsítésre, illetve komplett cserére szorul. A szlovák fegyveres erők fejlesztésének

szükségszerűsége megkérdőjelezhetetlen, hiszen az idejét múlt, túlnyomó részt szovjet felszerelések és technológiák már erősen korlátolták az utóbbi években a szlovák haderőt mind az országon belüli, mind pedig a szövetségesi szinten vállalt feladatok minőségi és hatékony ellátásában. Mindez értelemszerűen negatív hatással van a kiképzés színvonalára és a hadsereg felkészültségére. Az új eszközök és fejlesztések beszerzése ugyan már elkezdődött, de Magyarországhoz és Csehországhoz hasonlóan igen elhúzódó folyamatra kell Szlovákia esetében is számítani. Az új gépparkok és technikák túlnyomó része külföldi - amerikai, olasz - forrásokból kerül beszerzésre, de természetesen a többi V4 tagországhoz hasonlóan a hazai védelmi ipar maximális bevonását szem előtt tartva.

Egy radikális haderőfejlesztéshez nem elegendő pusztán az ezzel kapcsolatos célokat és feladatokat megfogalmazó programok kidolgozása és útnak indítása, alapvető fontosságú ezek mellett, hogy az adott ország stratégiai dokumentumai is tartalmazzák a hosszútávú fejlesztési reformokat, az ehhez vezető főbb irányvonalakat. A szlovák stratégiai dokumentumok frissítése jelentős elmaradást mutatott az elmúlt évtizedet tekintve, a 2005 óta érvényben lévő Szlovák Biztonsági Stratégiát is csak 2017-re sikerült megreformálni. Szlovákia közvetlen szomszédságában, illetve a régióban történt események hatására jelentős változások mentek végbe a közép-európai térségben, melyekre szükségszerű volt reagálni. A biztonsági és védelmi stratégiai dokumentumok aktualizálása kiemelkedően fontos feladat a V4-ek tagállamait illetően, hiszen az elmúlt évek során mind országos, mind nemzetközi szinten katonai, politikai, gazdasági téren történt változások ezt már megkövetelik. A Szlovák Biztonsági Stratégia frissítése során Csehország és Lengyelország stratégiai dokumentumait vették alapul, ennek oka, hogy a 3 ország biztonsági környezete sok szempontból nézve is hasonlóságot mutat. A stratégia a Szlovák Köztársaság alkotmányán, az EU-ban, a NATO-ban, az ENSZ-ben és más nemzetközi szervezetekben való tagságból eredő kötelezettségeken alapul. Jellemzi a biztonsági környezetet és meghatározza a biztonsági érdekeket. Alapvető célkitűzésként természetesen az állampolgárok és az állam biztonságának megóvását határozza meg. A 2005-ös stratégia és a 2017-es dokumentum tervezetét összehasonlítva megállapítható, hogy nem történt jelentős elmozdulás a biztonsági érdekek azonosításában, szövegüket és rendjüket tekintve szinte azonosak maradtak. Főbb célok továbbra is:

- *az állami lét, a szuverenitás és az integritás megőrzése*;
- *a demokratikus rendszer és a jogállamiság fejlesztése*;
- *és a biztonság fenntartható fejlesztése*.

A 2005-ben kiadott dokumentumhoz képest a 2017-es tervezet már a kulturális fejlődéssel és a biztonságos kibertérrel kapcsolatos elvárásokkal és megállapításokkal bővült. Megfigyelhető továbbá, hogy a tömegpusztító fegyverek használatának veszélye még mindig kiemelt szereppel bír, de alacsonyabb lett az erre vonatkozó készültség prioritása, és nagyobb hangsúlyt kap a dokumentumban a szélsőségesség, a kiberbiztonság, a hibrid tevékenység, a terrorizmus és a migrációs válság. A 2017-es dokumentum kimondja, hogy a biztonsági környezet jelentősen romlott, mely jelenség az alábbi formában mutatkozik meg:

- növekvő terrortámadások;
- a nemzetközi jog gyakoribb megsértése;
- más ország területi integritásának veszélyeztetése katonai erő alkalmazásával;
- bukott államok növekedése az EU szomszédos régióiban. [15]

A stratégiai dokumentumban megjelenik, hogy a Szlovák Köztársaság nem tartja valószínűnek egy országot ért támadás bekövetkezését, viszont a migrációs jelenség és az energiabiztonság szavatolása komoly feladatot és kihívást jelent számára, hiszen Szlovákia tapasztalhatta, hogy az ő esetében a kelet-ukrajnai konfliktus elsősorban az ország energiabiztonságát veszélyeztette az országba irányuló gázszállítások tranzitját illetően. [16] A Szlovák Köztársaság NATO-hoz való hozzáállását, az azon belül vállalt szerepét és feladatait a dokumentum 56. bekezdése tisztán és egyértelműen tartalmazza, miszerint az ország mindent megtesz a kollektív védelem megerősítéséért, támogatja annak átalakítását és alkalmazkodását az új típusú fegyverekhez és kihívásokhoz. Vállalja, hogy megreformálja és kiépíti biztonsági rendszerét annak érdekében, hogy hozzá tudjon járulni a NATO képességeinek fejlesztéséhez, a NATO-tagországok és a partnerországok területi védelméhez, a szövetség misszióihoz és műveleteihez. A vállalt kötelezettségeknek megfelelően fokozatosan növeli védelmi kiadásait, a megfelelő arányban finanszírozva a szlovák fegyveres erők fegyverzetének és technológiájának fejlesztését, illetve a kapcsolódó kutatásokat, beruházásokat. Előzetes kalkulációk alapján 2030-ig a védelemre körülbelül 30 milliárd eurót terveznek fordítani. A Szlovák Biztonsági Stratégia 78. bekezdésében megfogalmazásra is kerül, hogy a Szlovák Köztársaság biztosítja az állam védelméhez szükséges forrásokat, elkötelezi magát a védelmi kiadások növelése és a fegyveres erők modernizálása mellett, és Szlovákia 2020-ig a GDP 1,6 százalékára, 2024-re 2 százalékra növeli védelmi kiadásait. [17]

KONKLÚZIÓ

A Visegrádi Csoport mind a négy tagállama egységesen detektálta, hogy európai szomszédságában a biztonsági helyzet sokat romlott az elmúlt évtizedben. A V4-ek továbbra is a NATO és az EU tagságában látják biztonságuk garanciáját, az európai biztonság és stabilitás szempontjából megkérdőjelezhetetlen mind a négy tagállam esetében ezen szervezetekben való aktív részvételük. Biztonságpolitikai szempontból nézve mind a négy ország elkötelezett partner és szövetséges, és hajlandók hozzájárulni a nemzetközi békéhez és biztonsághoz. Egységesen mindannyian érdekeltek az államok szuverenitásának és területi integritásának megőrzésében. Bár az elmúlt években a négy tagállam biztonsága közvetlen veszélynek nem volt kitéve, azonban közvetett módon érintve voltak, hiszen a szomszédos országokban, régiókban történt események hatással voltak a védelmi folyamatokra és tevékenységekre mind a négy ország esetében. Az új típusú biztonsági kihívások új szemléletet, új hozzáállást, új módszereket és új megoldásokat követelnek meg a tagállamok részéről, melyek hatékony alkalmazására megerősített együttműködésre van szükség. A tagállamok stratégiai dokumentumaiban és az adott haderőfejlesztési programjaikban megfogalmazott értékrendek, célok és prioritások alapján, illetve a NATO-ban vállalt kötelezettségeiket figyelembe véve megállapítható, hogy a haderő- és képességfejlesztés egységesen kiemelt szereppel bír a V4-ek védelempolitikájában, emellett pedig a védelmi együttműködések megerősítése mind a négy tagállamban elsődlegesnek számít. Hogy milyen intenzitással, ütemben és intervallumban fogják véghez vinni a V4-országok az átlagosan 2030-ig tervezett komplex fejlesztési folyamat befejezését, azt jelentősen befolyásolni fogják az elkövetkezendő években az adott tagállamok politikai és gazdasági helyzetében megjelenő változások. Az tény, hogy a közép-európai térséget érintő fenyegetések eltérő felfogása időnként megnehezíti a hatékony kooperációt, a V4-ek az elmúlt évtizedekben végzett tevékenységét

és annak hatékonyságát tekintve jól működik, mint biztonsági és védelmi szövetség. Az eltérő nemzeti érdekek, belpolitikai történések természetszerűleg visszavethetik és időnként vissza is vetik a együttműködés intenzitását stagnálásra ítélve hosszabb-rövidebb időszakra a szövetség aktivitását és produktivitását, mégis V4-ek elmúlt három évtizedének eredményeit és a tagállamok hozzáállását tekintve valószínűsíthető, hogy erős stratégiai érdekek által motiválva a Visegrádi Csoport az elkövetkezendő években is funkcionáló társulás marad, erősítve ezáltal az közép-európai térség biztonsági környezetét.

„AZ INNOVÁCIÓS ÉS TECHNOLÓGIAI MINISZTÉRIUM ÚNKP-19-3-III-NKE-47 KÓDSZÁMÚ ÚJ NEMZETI KIVÁLÓSÁG PROGRAMJÁNAK SZAKMAI TÁMOGATÁSÁVAL KÉSZÜLT.”

FELHASZNÁLT FORRÁSOK

[1] „Visegrad Group Defence Cooperation”, [Online]. Available: http://www.visegradgroup.eu/about/cooperation/defence. [Hozzáférés dátuma: 3. március 2020.].

[2] T. A. Nagy, „V4 Defence Cooperation: Great Ambitions But Limited Achievements,” *RUSI Newsbrief,* 1. kötet 36., pp. 3-5., 2016.

[3] Z. Szenes, „Előre a múltba? A NATO Wales után,” *Külügyi Szemle,* 1. kötet3, pp. 3-26, 2014.

[4] Ministry of Foreign Affairs of the Czech Republic, „Security Strategy of the Czech Republic,” Government of the Czech Republic, Prága, 2015.

[5] Ministry of Defence of the Czech Republic, „The Defence Strategy of the Czech Republic,” MHI Prague, the Presentation and Production Department, Prága, 2017.

[6] Ministry of Defence of the Czech Republic, „The Long Term Perspective for Defence 2035,” Ministry of Defence of the Czech Republic, Prága, 2019.

[7] „Ministry of Defence & Armed Forcesof the Czech Republic,” Ministry of Defence & Armed Forces, [Online]. Available: https://www.army.cz/en/facts-file/defence-budget/defence-budget-130198/. [Hozzáférés dátuma: 12 10 2020].

[8] NATO, „Defence Expenditure of NATO Countries (2013-2020),” Bruxelles, 2020.

[9] T. Farkas, „Communication and information services – NATO requirements Part I.,” *Land Forces Academi Review,* 2020.

[10] *A Kormány 1163/2020. (IV. 21.) Korm. határozata Magyarország Nemzeti Biztonsági Stratégiájáról,* 2020.04.21..

[11] B. Németh és A. Kránicz, „Új hidegháborúra készülve?Eltérő biztonságpercepciókés haderőfejlesztési modellek a NATO keleti szárnyán,” *Külügyi Szemle,* 1. kötet19, 1. szám2, pp. 43-77., 2019.

[12] „Global Defence Technology,” [Online]. Available: https://defence.nridigital.com/global_defence_technology_jun19/from_russia_to

_nato_the_logic_behind_poland_s_military_modernisation. [Hozzáférés dátuma: 1. október 2020.].

[13] „National Security Strategy of the Republic of Poland," [Online]. Available: https://www.bbn.gov.pl/ftp/dokumenty/National_Security_Strategy_of_the_Republic_of_Poland_2020.pdf. [Hozzáférés dátuma: 3. október 2020.].

[14] „Website of the Republic of Poland," [Online]. Available: https://www.gov.pl/web/national-defence/cybermilpl-we-develop-polands-abilities-to-fight-threats-in-cyberspace. [Hozzáférés dátuma: 23. szeptember 2020.].

[15] [Online]. Available: https://stratpol.sk/wp-content/uploads/2017/08/fSSSR-2017-ENG-v-final-OND-final.pdf. [Hozzáférés dátuma: 01 10 2020].

[16] I. Majchút, „Security aspects of the Slovak republic in the second decade of 21st Century," in *Selected Economic Issues of Central and Eastern Europe*, 2016, pp. 15-23.

[17] [Online]. Available: http://mepoforum.sk/wp-content/uploads/2017/09/N%C3%A1vrh-Bezpe%C4%8Dnostnej-strat%C3%A9gie-SR.pdf. [Hozzáférés dátuma: 03 09 2020].

IoT AND THE REGULATION OF CYBERCRIMES

IoT ÉS A KIBERBŰNCSELEKMÉNYEK SZABÁLYOZÁSA

MIKLÓS Gellért[1]

Abstract

The aim of this paper is to present the Hungarian regulation of cybercrime related to the information system, as well as the closely related international legal documents. The actuality of the topic is provided by the explosive growth of IoT devices and, in parallel, the number of cybercrimes. Given the cross-border nature of these offenses, it seems unavoidable to regulate minimum security standards for IoT devices in addition to criminal offenses. Recommendations, guidelines and standards have already been drawn up, but there are currently no such binding regulations.

Keywords

IoT, cybercrime, EU law, criminal law, information system

Absztrakt

Jelen írás célja bemutatni az információs rendszerrel kapcsolatos kiberbűncselekmények magyar szabályozását, valamit az azzal szorosan összefüggő nemzetközi jogi dokumentumokat. A téma aktualitását az IoT eszközök elterjedésének és ezzel párhuzamosan a kiberbűncselekmények számának robbanásszerű növekedése szolgáltatja. Tekintettel ezen bűncselekmények határokon átívelő jellegére, megkerülhetetlennek tűnik a bűncselekmények mellett az IoT eszközökre vonatkozó minimum biztonsági előírások nemzetközi szabályozása is. Ajánlások, iránymutatások, valamint szabványok már készültek, de jelenleg nincs érvényben ilyen jellegű kötelező érvényű szabályozás.

Kulcsszavak

IoT, kiberbűnözés, EU jog, büntetőjog, információs rendszer

[1] gellert.miklos@gmail.com | ORCID: 0000-0002-3757-6834 | doctoral candidate / doktorandusz hallgató | Óbudai Egyetem Biztonságtudományi Doktori Iskola

BEVEZETÉS

A számítástechnika megállíthatatlan fejlődésével napjainkra már szinte majdnem minden jogi és természetes személy kapcsolódik valamilyen módon a globális hálózathoz. Magyarországon 2019-ben a háztartások 86%-a rendelkezett internet hozzáféréssel. [1] Napjaink egyik meghatározó globális megatrendje a digitalizáció, amelynek egyik velejárója, hogy olyan eszközök is intelligenssé váltak, amelyeket korábban nem érintett a számítástechnikai fejlődés. Az IoT felhasználási köre nem korlátozódik az iparra, mezőgazdaságra vagy a közlekedésre, hanem jelen van a háztartásokban is. Egy okostelefonról vezérelhető mosógép, vagy egy vízforraló tulajdonosának időt és energiát takaríthat meg az által, hogy lehetővé teszi a távoli irányítást, azonban legalább ekkora biztonsági kockázatot is jelent a felhasználójára nézve. Több, különböző meghatározás is született a tudományos világ és a gazdasági élet szereplőitől a dolgok internetének meghatározására. Ebben a cikkben a Nemzetközi Távközlési Egyesület (angolul International Telecommunication Union, ITU) által közzétett meghatározást fogom alkalmazni, amely alapján az IoT az információs társadalom globális infrastruktúrája, amely lehetővé teszi a fejlett szolgáltatásokat a (fizikai és virtuális) dolgok összekapcsolásával a meglévő és fejlődő interoperábilis információs és kommunikációs technológiák alapján. [2]

Jelen publikáció be kívánja mutatni a kiberbűncselekmények és azon belül is kifejezetten az információs rendszerek ellen elkövetett bűncselekményre vonatkozó főbb nemzetközi jogforrásokat, valamint a magyarországi büntetőjogi szabályozást, valamint rámutatni egy egységes szabványosítási és tanúsítási rendszer szükségességére.

A KIBERBŰNCSELEKMÉNYEK JOGI SZABÁLYOZÁSÁNAK FŐBB NEMZETKÖZI ÉS HAZAI FORRÁSAI

A kiberbűnözés a számítástechnika fejlődésével egyidejű, napjainkra pedig már magányos hackerek és szervezett bűnözői csoportok sora specializálódott az informatikai bűncselekmények elkövetésére. Megjelentek olyan, új bűncselekmények, amelyek csak információs rendszerekkel követhetők el, amelyeknek tárgya maga az információs rendszer. A digitalizáció azonban számos olyan hétköznapi bűncselekményt is befolyásolt, amelyek korábban is léteztek ugyan, de az információs rendszerek segítségével is elkövethetők, erre jó példa a csalás. Ezeknél a bűncselekményeknél az információs rendszerek az elkövetés eszközéül szolgálnak. [3] A technológia fejlődésével sem a jogi szabályozás, sem a felhasználók tudatossága nem tudja tartani a lépést.

A kiberbűncselekményeknek több olyan jellemzője is van, amelyek megnehezítik az érintettek és sokszor a hatóságok számára is a kiberbűncselekmények felismerését és azok elkövetőinek felkutatását, azonosítását. Ennek oka többrétű, amely szorosan összefügg a virtuális tér sajátosságaival, ezáltal pedig jellemzi IoT-t is. Egyrészt a technológia lehetővé teszi a bűnözők számára, hogy identitásukat elrejtsék és a bűncselekményeket anonim módon hajtsák végre. Ma már könnyedén megoldható, hogy az elkövetők titkosított csatornán keresztül tartsanak kapcsolatot egymással, saját azonosítóikat, nyomaikat pedig elrejtsék, megváltoztassák a hatóság fürkésző tekintete elől. A darkneten az illegális termékek és szolgáltatások széles köre érhető el magas fokú titkosítás mellett. Másrészt meghatározó ezen bűncselekmények vonatkozásában a nemzetközi jelleg. A hálózathoz csatlakozó rendszerek

és felhasználók előtt nincsenek fizikai határok, az információ a kibertérben szabadon áramolhat a felek között. Éppen ezért az IoT eszközök és felhasználóik ki vannak téve földrajzilag akár több ezer kilométerre, más kontinensen tartózkodó bűnözők támadásainak is. A kiberbűncselekmények ráadásul általában rendkívül gyorsan zajlanak le. Egy információs rendszerbe történő jogosulatlan belépés előkészítése ugyan az alkalmazott védelmi intézkedésektől és annak megkerülésének módszerétől (phising, social engineering, brute force jellegű támadások stb.) függően különböző ideig tarthat, azonban magába a rendszerbe történő belépés már csak pillanatok kérdése. Ezzel magyarázható a kiberbűncselekmények körében a magas fokú felderítetlenség, hogy az esetek nagy részében a hatóságok soha nem szereznek tudomást ezekről bűncselekményekről. Ez összefüggésben állhat azzal, hogy a sértettek gyakran nem észlelik a sérelmükre elkövetett kiberbűncselekményt, és elképzelhető az is, hogy bizonyos sértetteknek nem fűződik érdekük a bűncselekmény bejelentéséhez, ugyanis az incidens bejelentése hátrányosan befolyásolná az ügyfelek bizalmát és a sértett hírnevét, márkanevét. [4]

Az IoT eszközökre egyelőre nem vonatkozik olyan kötelező jogi követelményrendszer, amely meghatározná a védelem minimálisan kötelező szintjét. Vannak ugyan a védelmi intézkedésekre vonatkozó ajánlások, iránymutatások és szabványok, ezek alkalmazása azonban jelenleg önkéntes. A gyártók a költséghatékonyság és az eszközök korlátozott életciklusa miatt nem látják el az IoT eszközöket megfelelő védelemmel. Az IoT eszközök széleskörű alkalmazása ezért korábban nem ismert támadási lehetőségeket kínál a támadók, kiberbűnözők számára. Egy hálózatra kapcsolódó jármű felett menet a támadók akár menet közben is átvehetik az irányítást, teljesen kiszolgáltatva annak utasait. Az Európai Uniós Hálózat- és Információbiztonsági Ügynökség (angolul European Union Agency for Cybersecurity ENISA) ajánlásában több, az intelligens gépjárművekre vonatkozó lehetséges támadási forgatókönyvet is ismertet. [5] Nem csak az intelligens gépjárművek, de az egyszerű háztartási eszközök is veszélyt jelenthetnek a felhasználóikra. Kutatások igazolták, hogy a legtöbb IoT zár feltörhető, annak ellenére, hogy a gyártók robosztus védelmet ígérnek a felhasználók számára. Egy ilyen hibát a bűnözők egyaránt használhatnak az ingatlanba történő bejutásra, de akár az ingatlanban tartózkodó személyek foglyul ejtésére is az ajtó bezárásával. A felsorolás szinte vég nélkül folytatható lenne, naponta jelennek meg híradások az IoT eszközök sérülékenységét feltáró tesztekről, incidensekről.

A kiberbűnözéssel kapcsolatos szabályozás egyik első és mindmáig meghatározó egyezménye az Európa Tanács által 2001. november 23-án elfogadott Számítástechnikai Bűnözésről szóló Egyezmény (angolul Convention on Cybercrime, a továbbiakban: Budapesti Egyezmény). [6] A Budapesti Egyezmény egyrészt definíciókat alkot és rögzíti a számítástechnikai rendszer, a számítástechnikai adat, a szolgáltató és a forgalmi adat fogalmát, másrészt négy címbe sorolva csoportosítja azokat a büntető anyagi jogi tényállásokat, amelyekre nézve az aláíró tagállamok kötelesek arányos, hatékony és visszatartó erejű büntetéseket alkalmazni, ideértve a szabadságelvonó büntetéseket is.

A Budapesti Egyezmény az alábbi bűncselekménykategóriákat különbözteti meg:

- I. Cím Számítástechnikai rendszer és számítástechnikai adat hozzáférhetősége, sértetlensége és titkossága elleni bűncselekmények
- II. cím Számítógéppel kapcsolatos bűncselekmények
- III. cím Számítástechnikai adatok tartalmával kapcsolatos bűncselekmények

- IV. Cím Szerzői vagy szomszédos jogok megsértésével kapcsolatos bűncselekmények

Az Európai Unió Tanácsa 2005. február 24.-én fogadta el a 2005/222/IB Kerethatározatát a tagállamok büntető jogszabályainak az információs rendszerek elleni támadások terén történő közelítése érdekében. A kerethatározat érdeme, hogy abban a számítástechnikai rendszer helyett már az információs rendszer fogalma kerül meghatározásra. A Kerethatározatot a szorosabb integráció és a jogközelítés érdekében felváltotta az Európai Parlament és Tanács 2013/40/EU irányelve (a továbbiakban: Irányelv).[7] Az irányelvek az Európai Unió olyan jogalkotási aktusai, amelyek a tagállamok számára rögzítik elérendő célkitűzéseket, azokat azonban a tagállamok saját jogalkotásuk keretében elfogadott aktusokkal valósítják meg. Az Irányelv deklarált célja volt a tagállamok büntetőjogának harmonizációja, valamint az illetékes hatóságai közötti együttműködés erősítése. Az Irányelv Preambulumában hivatkozik továbbá a Budapesti Egyezményre, mint a számítástechnikai bűnözés, többek között az információs rendszerek elleni támadásokkal szembeni küzdelem irányadó jogi keretére, amelyre maga az Irányelv is épül.

Az irányelv az alábbi bűncselekményeket szabályozza:

- Információs rendszerekhez való jogellenes hozzáférés
- Rendszert érintő jogellenes beavatkozás
- Adatot érintő jogellenes beavatkozás
- Jogellenes adatszerzés

Az irányelv alapján jogellenes a hozzáférés valamely információs rendszerhez vagy annak egy részéhez, ha azt szándékosan és jogosulatlanul, valamely biztonsági intézkedés megsértésével követték el. Az Irányelv a bűncselekmények meghatározásán túlmenően minimum büntetési tételeket is meghatároz a tagállamok számára, amelyekhez képest azonban a tagállamok szigorúbb büntetési tételeket is kiszabhatnak [2]

Az irányelvnek való megfelelés érdekében Magyarországon a 2014. évi LXXII. Törvény módosította a Büntető Törvénykönyvről szóló 2012. évi C. törvény (a továbbiakban: Btk.) 423. §-át. [8] A Btk. meghatározása alapján információs rendszer az adatok automatikus feldolgozását, kezelését, tárolását, továbbítását biztosító berendezés, vagy az egymással kapcsolatban lévő ilyen berendezések összessége3, amely meghatározás megfelel az Irányelvben foglaltaknak és magába foglalja számítógépeken túlmenően az IoT eszközöket, a hírközlési és telekommunikációs hálózatokat, rendszereket és a SIM kártyákat is. A meghatározás nem tesz különbséget a jelek továbbítása között, így egyaránt magába foglalja az elektronikus, az optikai, a rádióhullámok, az infravörös vagy rövidhullámok, valamint műholdas sugárzás útján létrejövő információs rendszereket. [9] Az Irányelvnek megfelelően átültetésre kerül az adat fogalma is, amely magába foglalja a programot is, mint olyan adatot, amely valamely funkciónak az információs rendszer által való végrehajtását biztosítja.

[2] Irányelv 9. cikk
[3] Btk. 459. (1) 15. pontja

Az Információs rendszer vagy adat megsértése bűncselekmény alapesetét[4] az információs rendszerbe az információs rendszer védelmét biztosító technikai intézkedés megsértésével vagy kijátszásával történő jogosulatlan belépés, vagy az elkövető belépési jogosultsága kereteit túllépve vagy azt megsértve bent maradása valósítja meg. Az alapesetben foglalt bűncselekmény tehát már a védelmi intézkedés megsértésével vagy kijátszásával megvalósított jogosulatlan belépés, valamint a jogsértő bennmaradás ténye önmagában megvalósítja. A bűncselekmény elkövetési tárgya maga az információs rendszer, elkövetése pedig két évig terjedő szabadságvesztésbüntetéssel büntetendő. A fenti megfogalmazásból több fontos megállapítás is levezethető. Egyrészt amennyiben az információs rendszer védelmét technikai intézkedés nem biztosítja, úgy az elkövető információs rendszerbe történő jogosulatlan belépése nem valósítja meg a bűncselekményt. Az IoT eszközökre nézve jelenleg nincs kötelezően alkalmazandó magyar, vagy egységes európai vagy nemzetközi szabvány, amely kötelező jelleggel írná elő védelmi intézkedések, például jelszó vagy tűzfal alkalmazását ezen eszközökben. A forgalomban lévő és felhasználók számára elérhető legtöbb okoseszköz semmilyen fajta védelemmel nincs ellátva, az adattovábbítás pedig nem titkosított. A bűncselekmény alaki (immateriális) bűncselekmény, amely magával az elkövetési magatartás tanúsításával befejezetté válik. A kísérlet megállapítható amennyiben az elkövető megkísérli a védelmi intézkedés kijátszását, azonban az információs rendszerbe nem sikerült még belépnie. Ma már számos rendszer vezet nyilvántartást a sikertelen belépési kísérletekről is, amelyek bizonyítékul szolgálhatnak egy nyomozás során.

A bűncselekmény második alapesete akkor valósul meg, ha az elkövető az információs rendszer működését jogosulatlanul vagy jogosultsága kereteit megsértve akadályozza. Az akadályoztatás mibenlétéről a Btk. hallgat, azonban az értelmezés segíti mind a Budapesti Egyezményben[5], mind az Irányelvben[6] található akadályozás cselekményeket tartalmazó példálózó felsorolása, amely szerint adatok bevitele, továbbítása, megrongálása, törlése, minőségi rontása, megváltoztatása, elrejtése vagy hozzáférhetetlenné tétele az információs rendszert akadályozó cselekménynek minősül. Az akadályozásnak itt az információs rendszer rendeltetésszerű használatát kell megakadályoznia. Ebben az esetben is a kísérlet már az elkövetési magatartás – tehát az akadályozásra irányuló cselekmény – megkezdésével megvalósul. A bűncselekmény harmadik fordulata az adat jogosulatlan megváltoztatását, törlését vagy hozzáférhetetlenné tételét szankcionálja[7] az elkövetési tárgy pedig maga a számítógépes adat, beleértve a programot is. Az okos szenzorok, mérőegységek például a hálózathoz kapcsolódva továbbítanak adatokat a felhasználó fogyasztásáról, vagy különböző folyamatok állásáról. Támadók az IoT eszközbe belépve megváltoztathatják az érzékelő vagy mérőegység által továbbított jeleket, ezáltal jelentősen magasabb fogyasztási adatokat továbbíthatnak, vagy a magasabb mérési adatokkal (például hőmérséklet), kiválthatnak rendszerspecifikus válaszintézkedéseket, mindkét esetben kárt okozva a felhasználónak. Természetesen amennyire az IoT eszközök és felhasználásuk sokféle, úgy képtelenség számba venni és felsorolni az összes lehetséges károkozást. A törvény szövegéből egy-

[4] Btk. 423. § (1)
[5] Budapesti Egyezmény 5. cikk
[6] Irányelv 3. cikk
[7] Btk. 423. § (2) b)

értelmű, hogy már egyetlen adat megváltoztatása, törlése, hozzáférhetetlenné tétele megvalósítja a bűncselekményt, nem szükséges azonban, hogy a felsorolt cselekmények az adatfeldolgozást eredményét ténylegesen befolyásolják is. Az akadályozás és a megváltoztatás bűntette legfeljebb három évig terjedő szabadságvesztéssel büntetendő.

A törvény alapján a fentebb ismertetett bűncselekmény második és harmadik fordulata súlyosabban büntetendő, amennyiben az jelentős számú információs rendszert érint. A jelentős szám értelmezésére sem a törvény, sem a Budapesti Egyezmény, sem az Irányelv nem ad útmutatást, így annak kimunkálása a jogalkalmazói gyakorlatra hárul. Tekintettel arra, hogy a minősített eset megvalósulása az érintett információs rendszerek számától függ, ezért valószínűsíthető, hogy az érintett rendszerek számának a százas nagyságrendet el kell érnie. [9] A büntetés ebben az esetben egy évtől öt évig terjedő szabadságvesztés lehet. Az IoT eszközök sokfélesége miatt számtalan olyan felhasználási mód képzelhető el, ahol ezek az eszközök százas, ezres nagyságrendben kerülnek alkalmazásra akár egy létesítményen belül is. Ilyen esetekben a létesítmény elleni támadás már önmagában megvalósíthatja a minősített esetet. Megvalósulhat a minősített eset továbbá információs rendszer botnet hálózatba történő szervezésével is. A botnet, vagy más néven robothálózat egy fertőzött informatikai eszközökből – köztük IoT eszközökből - is álló hálózat, amelyet a botnet gazdája többféle károkozásra is alkalmazhat. [10] 2016-ban például egy kizárólag biztonsági kamerákból álló botnethálózattal hajtottak végre szolgáltatás megtagadást okozó támadást (Denial-of-Service ─ DoS) egy vállalkozás szerverei ellen. [11] A kamerák azért is bizonyultak a támadás szempontjából kézenfekvő választásnak, mert a felvételek továbbításához rendelkeztek szélessávú internet hozzáféréssel, azonban sem az eszközök, sem pedig hálózati szinten nem rendelkeztek semmiféle védelemmel.

Még súlyosabban büntetendő a bűncselekmény, ha azt közérdekű üzem ellen követik el. Közérdekű üzem alatt a törvény a közművet, a közösségi közlekedési üzemet, az elektronikus hírközlő hálózatot, az egyetemes postai szolgáltató közérdekű feladatainak teljesítése érdekében üzemeltetett logisztikai, pénzforgalmi és informatikai központok és üzemek, valamint a hadianyagot, haditechnikai eszközt termelőüzemet, energiát vagy üzemi felhasználásra szánt alapanyagot termelőüzemet érti. A törvény érthető okokból ezt a minősített esetet bünteti a legsúlyosabban, a büntetés két évtől nyolc évig terjedő szabadságvesztés. Amint arra tanulmányában Mezei Kitti is rámutat, a Btk. fogalomhasználata indokolatlanul szűkíti az Irányelv által meghatározott tényállást, ugyanis a közérdekű üzem és az irányelv által alkalmazott kritikus infrastruktúra fogalma eltér egymástól. [3] Ez különösen annak tükrében érdekes, hogy az európai kritikus infrastruktúrák azonosításáról és kijelöléséről, valamint védelmük javítása szükségességének értékeléséről szóló 2008/114/EK irányelvet implementáló hazai jogszabály [12] pedig létfontosságú rendszerelemként jelöli a kritikus infrastruktúrákat. Így fordulhat elő, hogy a magyar szabályozásban két külön fogalom, eltérő jelentéstartalommal jelöli ugyan azt az uniós jogban meghatározott fogalmat. A minősített esetben foglalt cselekmény azonban nagyon is valós veszélyt jelent a társadalomra. Nagyszámú IoT eszköz egyidejű aktiválásával (például légkondicionáló berendezések, vízforralók és egyéb nagy áramfogyasztású háztartási elektronikai eszközök) ugyanis a támadók komoly terhelésnek tehetik ki az elektromos rendszert, amely szélsőséges esetben áramkimaradáshoz, áramszünethez is vezethet.

Tekintettel a kiberbűnözés természetére, valamint arra, hogy manapság az információs rendszer vagy adat megsértéséhez szükséges programok, tudás, felhasználói azonosítók

ellenérték fejében vagy akár ingyen is hozzáférhetőek az interneten, szükséges már az előkészítő cselekmény kriminalizálása is. A tagállamok kriminalizációs kötelezettségét az Irányelv is rögzíti.[8] A törvény alapján információs rendszer védelmét biztosító technikai intézkedés kijátszásának vétségét követi el aki az információs az információs adat vagy rendszer megsértéséhez szükséges jelszót vagy számítástechnikai programot készít, átad, hozzáférhetővé tesz, megszerez, vagy forgalomba hoz, illetve jelszó vagy számítástechnikai program készítésére vonatkozó gazdasági, műszaki, szervezési ismereteit más rendelkezésére bocsátja. A vétség két évig terjedő szabadságvesztéssel büntetendő.

ELJÁRÁSI KÉRDÉSEK

A kiberbűnözés fentebb már ismertetett sajátosságai miatt nem egyszerű annak a kérdésnek megválaszolása, hogy a bűncselekmény elkövetését követően ki jogosult eljárni, mely szervek rendelkeznek hatáskörrel és illetékességgel. Elsősorban a joghatóságot kell megvizsgálni, azaz, hogy az adott bűncselekmény vonatkozásában mely állam jogosult megindítani a nyomozást és lefolytatni a büntetőeljárást. Erre vonatkozóan az Irányelv előírja, hogy a tagállamok megállapítják joghatóságukat az alábbi esetekben:

- az információs rendszer elleni bűncselekményt egészben vagy részben a területükön követték el, vagy
- egy állampolgáruk követte el, legalább azokban az esetekben, ha a cselekmény az elkövetés helyén bűncselekménynek minősül.

Egy bűncselekmény akkor minősül a fenti i) pont szerint az adott tagállam területén elkövetettnek, amennyiben az elkövető a bűncselekmény elkövetésekor fizikailag jelen van a területükön, függetlenül attól, hogy a bűncselekmény a területükön található információs rendszer ellen irányul-e; vagy a bűncselekmény a területükön található információs rendszer ellen irányul, függetlenül attól, hogy az elkövető a bűncselekmény elkövetésekor fizikailag jelen van-e a területükön. Az Irányelv alapján a tagállamok megállapíthatják joghatóságukat abban az esetben is, ha az elkövető szokásos tartózkodási helye a tagállam területén van, vagy a bűncselekményt a területükön letelepedett jogi személy javára követték el.[9] A Btk. területi és személyi hatályára vonatkozó rendelkezései alapján a magyar büntető törvényt kell alkalmazni a belföldön elkövetett bűncselekményre, a magyar állampolgár által külföldön elkövetett olyan cselekményre, amely a magyar törvény szerint bűncselekmény, valamint a magyar állampolgár, magyar jog alapján létrejött jogi személy és jogi személyiséggel nem rendelkező egyéb jogalany sérelmére nem magyar állampolgár által külföldön elkövetett olyan cselekményre is, amely a magyar törvény szerint büntetendő. A magyar hatóságok joghatósága tehát mind abban az esetben biztosított, amikor magyar állampolgárságú személyek belföldön vagy külföldön követik el az információs rendszerek elleni bűncselekményt, mind abban az esetben, amennyiben külföldi személyek magyar állampolgárok terhére külföldön követik el a bűncselekményt. Tekintettel a kiberbűnözés nemzetközi jellegére, a joghatóság megállapítása nem mindig olyan egyszerű, mint azt a fenti szabályok alapján gondolni lehetne. Ezek a bűncselekmények ugyanis gyakran több országban valósulnak meg, az áldozatok között több ország állampolgára is van (például egy nulladik napi

[8] Irányelv 7. cikk
[9] Irányelv 12. cikk

támadás érint egy IoT termék összes eszközét) vagy pedig maguk az elkövetők szerveződnek több országból.

A fent ismertetett információs rendszerrel kapcsolatos bűncselekményekre a rendőrség hatásköréről és illetékességéről szóló jogszabály [13] a Készenléti Rendőrséget jelöli ki [10], mint a nyomozásra hatáskörrel rendelkező szerv. A nyomozás során a nyomozó hatóság felkutatja, megismeri és rögzíti a bűncselekmény alapjául szolgáló adatállományt, az információs rendszerben megtalálható elektronikus nyomokat és bizonyítékokat. [14] Beszerzi továbbá a naplófájlokat és a regisztrált adatokat. Ezek a naplózott adatok kiemelt szerephez juthatnak a fentebb ismertetett bűncselekmények kísérletének bizonyítása során.

KÖVETKEZTETÉSEK

Amint arra a bevezetőben már utalás történt, a számítástechnika fejlődése és a mindent átszövő digitalizáció napjainkra már az élet minden részén érezteti hatását. Ennek a fejlődésnek azonban árnyoldalai is vannak, a kiberbűncselekmények és a kibertámadások száma ugyanis évről évre nő. Ez egyrészt összefügg azzal a ténnyel, hogy egyre több a felhasználó és egyre több a támadási felületként szolgáló információs rendszer, másrészt pedig azzal, hogy ezen cselekmények elkövetéséhez szükséges tudás, hardware és szoftverek átlagember számára is könnyedén hozzáférhetőek. A hackerek és a szervezett bűnözői csoportok jellemzően több országból szerveződve hajtanak végre bűncselekményeket nagy számú, különböző országban élő áldozattal szemben. Ebben a környezetben a rendkívül dinamikusan növekvő számú IoT eszköz jelentős információbiztonsági kihívást jelent. Amint az fentebb ismertetésre került, az Irányelv és az alapján a Btk. csak a védett eszközökbe történő jogosulatlan belépést szankcionálja. A büntetőszabályozás mindenképpen szükséges, de nem elégséges megoldása ennek az egyre növekvő problémának.

Az IoT eszközök egy jelentős részénél semmilyen védelmi mechanizmus nincs beépítve, az eszközökön futó szoftverek nem kerülnek frissítésre és az adatok továbbítása sem titkosított. Ebből adódóan a kiszivárgott, napvilágot látott hibák, sérülékenységek sem kerülnek sokszor javításra, kiszolgáltatva ezeket az eszközöket és felhasználóikat. Nem véletlen, hogy a különböző szakmai szervezetek által kidolgozott ajánlások, iránymutatások és szabványok mind tartalmazzák ezeket az alapvető védelmi intézkedéseket. Jelenleg az Európai Unióban egyedül Nagy-Britanniában van nyilvános konzultáció és kidolgozás alatt egy tervezet a fogyasztóknak szánt (angolul B2C vagy business to consumer) IoT eszközökre vonatkozó kötelezően alkalmazandó biztonsági követelményekről [15] Amennyiben ez a trend folytatódik és a nemzeti kormányok saját IoT keretrendszert fogadnak el eltérő módon szabályozva a védelmi intézkedésekkel szemben támasztott minimum követelményeket, akkor az az Európai Unió digitális belső piacának felaprózódásához vezethet. Ez a folyamat egyúttal jelentősen megnövelné a gyártók számára a piacra lépéssel és a jogszabályi megfeleléssel kapcsolatos költségeit. Erre megoldást jelenthetne egy egységes európai követelményrendszer, ilyen azonban jelenleg még nem került elfogadásra. Az Európai Távközlési Szabványosítási Intézet (angolul European Telecommunications Standards Institute vagy ETSI) 2020. június 30-án jelentette be az ETSI EN 303 645 szabványát, amely a fogyasztói IoT eszközök számára alapvető követelményeket határoz meg. [16] Ez az európai szabvány, amennyiben Európai Uniós jogforrás előírná alapul szolgálhatna egy egységes

[10] 2. Melléklet 22. k

európai tanúsítási mechanizmusnak, a védelem egységes minimumszintjét garantálva a belső piacon forgalomba bocsájtott IoT termékek esetén.

FELHASZNÁLT FORRÁSOK

[1] A digitális gazdaságra és társadalomra vonatkozó statisztikák – háztartások és magánszemélyek [Online] Elérhető: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Digital_economy_and_society_statistics_-_households_and_individuals
[2] Recommendation ITU-T Y.2060, 2012. [Online] Elérhető: http://handle.itu.int/11.1002/1000/11559
[3] Mezei, Kitti (2018) A kiberbűncselekmények hazai szabályozásának aktuális kérdései. In: Magyar Jogászegyleti Értekezések. Magyar Közlöny Lap- és Könyvkiadó; Magyar Jogász Egylet, BUDAPEST, pp. 157-173.
[4] Gyaraki Réka (2018) A számítógépes nyomozás problémái, PhD értekezés, PÉCS
[5] Cyber Security and Resilience of smart cars - Good practices and recommendations. 201. [Online] Elérhető: https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars
[6] 2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről
[7] AZ EURÓPAI PARLAMENT ÉS A TANÁCS 2013/40/EU IRÁNYELVE (2013. augusztus 12.) az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról
[8] Büntető Törvénykönyvről szóló 2012. évi C. törvény
[9] Akácz József; Belegi József; Katona Sándor; Kónya István; Márki Zoltán; Mészár Róza; Molnár Gábor Miklós; Soós László (2020) Magyar Büntetőjog I-III. - új Btk. - Kommentár a gyakorlat számára, HVG-ORAC Lap- és Könyvkiadó, Budapest
[10] Robothálózat (Botnet) [Online] Elérhető: https://nki.gov.hu/it-biztonsag/tudastar/robothalozat-botnet-2/
[11] IoT botnets might be the cybersecurity industry's next big worry [Online] Elérhető: https://bdtechtalks.com/2016/07/12/iot-botnets-might-be-the-cybersecurity-industrys-next-big-worry/
[12] 2012. évi CLXVI. Törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről
[13] 25/2013. (VI. 24.) BM rendelet a Rendőrség nyomozó hatóságainak hatásköréről és illetékességéről
[14] Kiss, Tibor, ed. (2020) Kibervédelem a bűnügyi tudományokban. Dialóg Campus Kiadó, Budapest. ISBN 9789635310302, p. 59.
[15] Mandating security requirements for consumer 'IoT' products [Online] Elérhető: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/798722/Secure_by_Design_Consultation_Stage_Regulatory_Impact_Assessment.pdf
[16] ETSI EN 303 645 V2.1.1 (2020-06) szabvány [Online] Elérhető: https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

BIOMETRIC SYSTEM IN AVIATION INDUSTRY (SECOND PART)

A REPÜLÉSIPAR BIOMETRIKUS RENDSZEREI (MÁSODIK RÉSZ)

ALSHAMAILEH Lafee[1] – ŐSZI Arnold[2]

Abstract

This review aims to summarize all applied and hypothesized alternatives of improving the Risk-Based Security (RBS) which are applied by the Transportation Security Administration in order to optimize the unique way for passenger screening and to inspect the present RBS passengers screening platform. It also aims to review current biometric technologies and highlighst current incorporation of biometrics into RBS initiative programs. Several governmental programs, which have combined biometrics into their measures to develop the proficiency and consistency by using biometrically enriched security measures, were investigated. This review will give a insight into how to include biometrics into the current Risk-Based Security Aviation Passenger Screening Program.

Keywords

Aviation Security, biometrics, Transportation Security Administration, Risk Based Security (RBS)

Absztrakt

Ez az áttekintő cikk a gyakorlati és a feltételezett alternatívák összefoglalását célozza meg, amelyek segítik a Veszély Alapú Biztonság (Risk-Based Security, RBS) növelését. Ezt a Transportation Security Administration alkalmazza, páratlan utas vizsgálattal és a jelenlegi RBS utasvizsgáló plattformmal. A cikk áttekinti a jelenlegi biometrikus technológiákat és kiemeli az RBS induló programokba bevont biometriát. Számos kormányzati programot vizsgáltunk, amely a biometriát használja a méréseihez, hogy növelje a hatékonyságot és a következetességet. Ez a review cikk egy jó rátekintést ad arra, hogy hogyan vonjuk be a biometriát a jelenegi kockázat alapú repülés biztonsági utas átvizsgáló programba.

Kulcsszavak

Repülés biztonság, biometria, Transportation Security Administration, Kockázat Alapú Biztonság (Risk Based Security, RBS)

[1] lafee.alshamaileh@uni-obuda.hu| ORCID: 0000-0002-5141-4786 | PhD student/doktorandusz | Óbudai Egyetem Biztonságtudományi Doktori Iskola

[2] oszi.arnold@bgk.uni-obuda.hu | ORCID: 0000-0001-5988-0143 | adjunct professor/egyetemi adjunktus | Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

ABBREVIATION

US-VISIT: unveiled United States Visitor and Immigrant Status Indicator Technology
DHS: Department of Homeland Security
TSA: Transportation Security Administration
RBS: Risk-Based Security
CAPPS I, II: Computer Assisted Passenger Pre-Screening
IATA: The International Air Transport Association

INTRODUCTION

Biometric technologies play a vital role in the simplification of more appropriate and protected passengers processing systems. Though, these growths are disintegrated. There is a must for information sharing on optimized practices and lessons learned in order to have the augmented configuration.

In recent years, different technologies and applications in biometric technologies have become increasingly widespread, and parallel to this, the subject is also attracted by academicians. The different evaluation of the developed methods depending on their areas of use causes the number of biometric methods to increase. However, these methods' common point is that risks are minimized, and the safest system is established. Another critical issue, which is the main reason for these security concerns, is the operation of these technologies and ensuring their cybersecurity that does not harm people's information security and constitutional freedom. This issue, which every biometric method developed pays attention to, has been frequently questioned in recent years, but the legislative arrangements have not been fully completed yet.

In USA, Transportation Security Administration (TSA) integrates unpredictable security measures, both seen and unseen for high quality service. Combining biometric systems is one of TSA services. TSA is an agency of the U.S. Department of Homeland Security that was created in 2001 to be responsible for passenger security in American air.

Incorporating biometric technology that validates an individual's identification will mend the competence and efficiency of the screening system since biometrics offers more superior security and accessibility than traditional approaches of personal recognition. Biometrics can replace or enhance the existing technologies.

The idea of the biometric system is that once a passenger match between facial characteristics and the passport is created, the passenger will be able to proceed through all of the terminal checkpoints from the curb to the cabin. In addition, biometric systems will allow the TSA to re-concentrate on high risk or unknown risk travelers thus increasing security effectiveness.

This review will give visions on how biometrics can elevate key features of the passengers processing at airports and it will discuss many new opportunities arising from improved biometric technologies and methods, intelligent use of networked data and sophisticated public/private partnerships.

Biometric innovation is rising as the best arrangement for aircraft and aeroplane terminals to mechanize character checks amid rising traveller numbers. Concurring to Biometrics for Way better Travel: An ID Administration Transformation, a report distributed nowadays by SITA. It traces how utilizing biometrics to check passenger's character will

control quicker and more secure self-service forms at aeroplane terminals as traveller numbers are set to nearly twofold to 7.8 billion by 2036.

Airlines and air terminals are as of now contributing to different shapes of biometric innovation, and SITA's report investigates inventive ID administration programs that are changing the travel encounter nowadays. Within the future, these will be more commonplace around the world as 63% of aeroplane terminals and 43% of carriers arrange to contribute to biometric ID administration arrangements within the following three a long time.

BIOMETRIC SYSTEM AND AIRPORT SECURITY

Air travel has become a standard not only in international travel between countries but even in domestic flights between cities. Reducing air travel costs close to the costs of land travel made air travel preferable to land travel in terms of costs and reducing travel time, which causes airports to become more crowded. Not only citizens but even diplomatic visitors, government officials, foreign and domestic tourists, and immigrants pass through airports to travel from one city to another. This makes airports vulnerable to provocation attempts and terrorist acts and creates security vulnerabilities in them.

Given that terrorism has become a global threat, security weakness cannot be tolerated. However, it is impossible to fill this security gap by increasing the number of security personnel or resources allocated to security. Because of the congestion of airports, security personnel cannot over-pay attention to more than one problem or verify more than one topic simultaneously. There are inevitable gaps and blind spots in such an environment, so airport security must be handed over to flexible and scalable technology and systems.

The People's Republic of China is one of the leading states in this field. China can follow its citizens very closely within the social credit system framework, which was first announced in 2018. This practice, which is considered Orwellian-style social engineering, is also criticized seriously for the violation of private life privacy. The information screens at Chengdu Shuangliu Airport add a different dimension to the use of biometric data. The system provides this information by scanning the face of the passenger and matching it in the database. The most interesting aspect of this practice at Chengdu Shuangliu Airport is that the passenger does not need to have his / her face scanned at any point in the airport as per their request. To put it more clearly, even if the passenger made the check-in process using known methods (check-in counter, kiosk, mobile, internet, etc.), but at the airport but somewhere in the city, the face of the passenger in question was scanned and entered the database of the relevant system. As a result, although there are opponents, it seems that the use of personal data in the electronic environment will become increasingly common. Thus, it seems that the "good" citizens will have a lot easier on their travels.

Several biometric systems were used at different facilities at airports. The following scheme (Figure 9) shows a representation for the possibilities to place a biometric system.

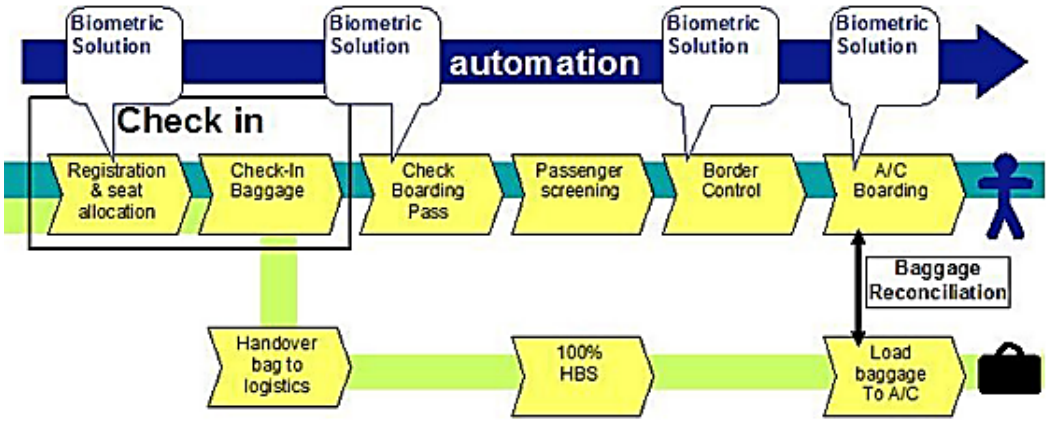


Figure 9: Diagram courtesy of Fraport; based on Simplifying Passenger Travel (SPT) Programme's Ideal Process Flow

The integration of many biometric solutions during passenger processing will smooth the passenger flow through the airport. When practicable, airports and their investors in one location should work with airports and the stakeholders in other locations, to develop interoperable systems that will let a traveler move from one location to another using the same travel token.

Some examples for biometric systems are represented in next section.

CASE STUDIES IN THE USA

In this section some case studies will be discussed showing their system engineering design of biometric systems and decision-making support in complex biometric-based systems.

Ross and Coworker reported in his work the process of a digital biometric measurement, primarily data is collected then it is transformed to set of numbers or codes and then stored in a database. As soon as the database is gathered, it is matched to other measurements previously stored in the database to see if there is a match. [18]

Ever since September 11, 2001, the Department of Homeland Security (DHS) and, within it, the Transportation Security Administration (TSA) has been established by the American federal government, which is responsible for passenger security at the nation's many airports.

A. US-VISIT

As per the unveiled United States Visitor and Immigrant Status Indicator Technology (US-VISIT) and according to the Department of Homeland Security (DHS), new techniques were executed for all the visitors from nominated countries that pass in the United States at different ports of entry to be photographed and fingerprinted by customs officials. [19] As stated by DHS, using the biometric identifiers will provide higher security than the

use of name databases alone, particularly since persons will not be able to claim another's identity or fake travel documents. All the stored data will be safely stored, and it is just available only for the authorized and official usage, that international travelers are who they say they are and do not pose a threat to the United States. [19]

Figure 10: US-VISIT's innovative biometric technology enables officers to efficiently verify

B. CAPPS

The Computer-Assisted Passenger Pre-screening System (often abbreviated as CAPPS) is a counter-terrorism system in place in the United States' air travel industry. The United States Transportation Security Administration (TSA) preserves a watch list of individuals known to pose, or suspected of posing, a risk of air piracy or terrorism or a threat to airline or passenger safety." The list is used to preventively recognize terrorists trying to buy airline tickets or board aircraft traveling in the United States, and to alleviate apparent threats.

There are two versions in the USA of the program called CAPPS. The first version of CAAPS was managed by the FBI and FAA in the late1990s, at that time CAPPS I was implemented in response to the supposed threat of U.S. domestic and international terrorism.

The principle of CAPPS is to screen the selected passengers for additional screening of their checked baggage for explosives. CAPPS selectees did not undergo any additional screening at passenger security checkpoints. [20]

The Office of National Risk Assessment (ONRA) proposed a second version of CAPPS (CAPPS II), with a list of necessities for a replacement to CAPPS I. Some of those requirements were:

- The government, not the airlines, would control and administer the system
- Every ticketed passenger would be screened, not just those who check bags
- Every airline and every airport would be covered by the system

In the summer of 2004, CAPPS II was cancelled by the TSA as the new version of CAPPS II is all dressed up in the language of privacy and concern for freedom, but it fails to address the core problems with the concept and continues to pose an enormous threat to American freedom and privacy.

Shortly thereafter, the TSA announced a successor program, called Secure Flight that would work much the same way as CAPPS II. Secure Flight was implemented in August 2009.

C. Secure Flight

This program matches passenger information against watch lists maintained by the federal government. The initial implementation phase of Secure Flight resulted in the complete transfer of responsibility for passenger watch list matching to TSA from aircraft operators whose flights operate within the United States. The second phase of Secure Flight will result in the transfer of responsibility for passenger watch list matching to TSA for flights into, out of, and over the United States.

The primary differences between Secure Flight and CAPPS II are summarized in Table 1. Unlike CAPPS II, the new system will not seek to identify anyone other than known or suspected terrorists.

Secure Flight Compared to CAPPS II		
Program elements	CAPPS II	Secure Flight
Provides no protection against terrorists with fake IDs	√	√
Provides no meaningful way for individuals to challenge their security designation	√	√
Centers around reliance on secret, inaccurate government terrorrist watch lists		√
Checks personal information against private databases	√	√
Requires collection of personal information from travelers making reservations	√	√
Expands program beyond terrorists	√	
Uses computer algorithms to rate individuals' "threat to aviation"	√	

Table 1: Comparison between CAPPSII and Secure Flight (ACLU Conference) [21]

NEW MODELS FOR AIRPORT SECURITY AND BIOMETRICS

Br¨omme in his article stated that biometric innovation ought to be accessible, for instance with institutionalized information positions for biometric interchanging information, correspondence conventions. Also, it should bring together programming interfaces for empowering the interoperability of various biometric frameworks and parts in existing information and communication technology (ICT) infrastructures. [12]

Improving airport security and immigration pain points with a risk-based approach is a new challenging trend. Smart security does not mean having to wait a long time in a

queue, as many companies integrate devices and programs to enhance the airport layout to further improve ambience and passenger flows, e.g IATA/ACI Smart Security program believed to be a catalyst for an important shift in the way certain passengers are screened. [22]

Antoine Rostworowski, Director of Montréal Trudeau International Airport stated that the industry is moving towards this approach where a single token process is feasible, and that could make a difference. IATA, ACI, ICAO and others are having a lot of discussions around this, and biometrics is what many believe is the way forward. [23]

On March 2018, British Airways brough its biometric identification gates to three more US airports. Biometric identification gates were expanded to New York (JFK), Miami (MIA), and Orlando (MCO) airports. These "biometric e-Gates," which have been in trial at Los Angeles International Airport (LAX) since November 2017, use facial recognition to match flyers with their passport, visa, or immigration photos and can remove the need to show a boarding pass or identification when getting on a plane. Lufthansa has started using facial scans to permit passenger self-boarding at Los Angeles International. [24]

Figure 11: Biometrics boom at the airport: Using fingerprints, facial scans to enter clubs, get on planes

CONCLUSION

Any new system must be in line with ACI recommendations, and biometric systems deployed at airports must be compatible with and capable of forwarding data to multiple systems. Systems applicable at airports ought to be fast, efficient, secure, reliable, scalable, certified according to ICAO and ISO standards and conscious of environmental requirements of each location.

Several research and studies must be conducted in cooperation between governments and research centers to optimize the suitable biometric configuration for high level of security which would improve aviation safety in various ways.

REFERENCES

[1] Transportation Security Administration: "49 U.S. Code § 114 - Transportation Security Administration | US Law | LII / Legal Information Institute". Law.cornell.edu. Retrieved 2016-08-08..
[2] Poole, Jr., Robert W. "Airport Security: Time For a New Model." Policy Study 340. Los Angeles, CA: Reason Foundation, January 2006..
[3] Ross, Prabhakar & Jain, An Introduction to Biometric Recognition, IEEE TRANSACTIONS ON CIRCUITS AND SYSTEMS FOR VIDEO TECHNOLOGY, VOL. 14, NO. 1, JANUARY 2004, supra note 125.
[4] US-VISIT FACT SHEET, findBiometrics.com, at http://www.findbiometrics.com/Pages/feature%20articles/usvisit.html, 2004.
[5] 2. US-VISIT Data Sheet www.dhs.gov/us-visit.
[6] The Aviation Security System and the 9/11 Attacks - Staff Statement No. 3": "The Aviation Security System and the 9/11 Attacks - Staff Statement No. 3" . 9-11commission.gov. Retrieved 2016-08-08..
[7] ACLU conference, https://www.aclu.org/other/secure-flight-compared-capps-ii.
[8] Eric P. Haas, Back to the Future - The Use of Biometrics, Its Impact of Airport Security, and How This Technology Should Be Governed , Journal of Air Law and Commerce Volume 69 2004..
[9] BIOMETRICS | SECURITY // JUL 2014, Improving airport security and immigration pain points with a risk-based approach, automation and more choice, http://www.futuretravelexperience.com/2014/07/improving-airport-security-immigration-pain-points-risk-based-a.
[10] ACI Media Releases, 2015, http://www.aci.aero/News/Releases/Most-Recent/2015/02/09/Antoine-Rostworowski-joins-ACI-World-as-Director-of-Facilitation-and-IT..
[11] Chris McGinnis, Biometrics boom at the airport,2018, https://www.sfgate.com/chris-mcginnis/article/Delta-other-airlines-bring-biometrics-to-more-12782175.php, Published 11:20 am, Monday, March 26, 2018.
[12] Őszi Arnold, Kovács Tibor: „Theory of the Biometric-based Technology in the field of e-commerce" Óbuda University – CINTI 2011 – 12th IEEE International Symposium on Computational Intelligence and Informatics, 2011. nov. 21-22. ISBN: 978-1-4577.
[13] ACI World Headquarters • Geneva • Switzerland, The Application of Biometrics at Airports, http://www.aci.aero/media/aci/file/free%20docs/aci%20biometric%20position%20final.pdf.
[14] Schneier, "Attack trees," Dr. Dobb's Journ. of Softw. Tools, vol. 24, no. 12, 1999..
[15] US-VISIT Program, Increment Privacy Impact Assessment, Dec. 18, 2003.
[16] Bartlow, Nick and Zekster, Gregory. "Holistic Evaluation of Multi-Biometric Systems." BRTRC, October 2009..
[17] N. G. Leveson, Safeware - System Safety and Computers, Addison-Wesley, 1995.
[18] B. a. I. M. N. S. a. T. C. W. N. 2. National Science and Technology Council. Biometrics in Government Post 9/11. Report.
[19] Svetlana N. Yanushkevich and Anna V. Shmerko ,Fundamentals of Biometric System Design: New Course for Electrical, Computer, and Software Engineering Students, 2009, ISBN: 978-0-7695-3754-2 doi>10.1109/BLISS.2009.27.

[20] Press Release, ACLU, supra note 180..
[21] Center for Army Lessons Learned (CALL). Commander's Guide to Biometrics in Afghanistan. Vols. 11–25. For Leavenworth, KS: CALL, 2011..
[22] Bundesamt f¨ur Sicherheit in der Informationstechnik (BSI): Vergleichende Untersuchung biometrischer Identifikationssysteme - BioIS, Bonn, Germany, 2000.
[23] Accenture, "Insights into Automated Border Clearance." Accenture: High performance. Delivered. Chicago, IL: Accenture, 2010.
[24] L. Hong and A. K. Jain, Multimodal Biometrics, in: Jain, Bolle, and Pankanti (eds.), Biometrics: Personal Identification in Networked Society, Kluwer Academic Press, 1999..
[25] National Research Council of the National Academies. Biometric Recognition Challenges and Opportunities. Research Report, Engineering and Physical Sciences, National Academy of Sciences, Washington: National Academy of Sciences, 2010..

Other sources:
https://www.theverge.com/2018/3/9/17100314/british-airways-facial-recognition-boarding-airports
International Journal of Network Security, Vol.2, No.1, PP.52–63, Jan. 2006 (http://isrc.nchu.edu.tw/ijns/)

USE OF DRONES FOR CIVIL PURPOSES

DRÓNOK FELHASZNÁLÁSA CIVIL CÉLOKRA

BÁLINT Márton[1] – SZŰCS Endre[2]

Abstract

One would think that non-military use of drones is only leisure type picture and video recording. Indeed, this type of use is very widespread and is continuously increasing, however the non-military use of drones is already at present time much more widespread. The proliferation and technical development of such devices result in the need for an analyze about possible future useful goals the technical advantages of drones could serve, how could they be placed in the service of humanity, to scientific development, to the security of our en-vironment, what could be their new applications making our life easier and to what commercial activity could be the base for. In our article we will analyze the alternative and non-military applications of drones. Based on several existing fields of application we will analyze all those new possibilities that drones offer or could offer, including electrical networks, observation of nature, security techniques, railway systems, municipalities and environment protection.

Keywords

drone, application, alternative application, non-military application, civil service, science, research, security, business

Absztrakt

A nem-katonai célú drónok használata esetén a kedvtelési fénykép- és videó készítésre gondolunk. Jelenleg az ilyen jellegű felhasználás valóban jelentős és folyamatosan fejlődik, azonban a drónok nem-katonai felhasználása már jelenleg is ennél jóval széleskörűbb. Az ilyen szerkezetek elterjedése és műszaki fejlődése felveti azonban egy olyan elemzés szükségességét, hogy a jövőben milyen további egyéb hasznos célokra lehetne fordítani a drónok adta technikai előnyöket, hogyan tudnák segíteni az emberiséget, a tudomány fejlődését, a környezetünk biztonságát szolgálni, hogyan tudnának új, az életünk könnyítését szolgáló felhasználást elérni és milyen új kereskedelmi tevékenységeknek szolgáltathatnak alapot. Cikkünkben a drónok használatának alternatív, nem-katonai lehetőségeit elemezzük. Több jelenlegi felhasználási területet vizsgálva elemezzük azokat az új lehetőségeket, melyek a drónok magukban rejtenek vagy rejthetnek, érintve a villamos hálózatok, természeti megfigyelések, biztonságtechnika, vasúthálózat, önkormányzati, valamint környezetvédelmi témaköröket.

Kulcsszavak

drón, felhasználás, alternatív felhasználás, nem-katonai felhasználás, közszolgálat, tudomány, kutatás, biztonság, kereskedelem

[1] balint.marton@phd.uni-obuda.hu | ORCID: 0000-0002-5703-5584 | PhD Student/doktorandusz | Óbuda University Doctoral School of Safety and Security Sciences / Óbudai Egyetem Biztonságtudományi Doktori Iskola

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

ELŐSZÓ

Drón. A szó hallatán sokunknak eszünkbe jutnak azok a pici, apró repülő szerkezetek melyeket fiatalok vagy fiatalos apukák használnak strandokon, mezők fölött, jellemzően gyakorlásnak tűnő mozdulatokkal. Valóban, az elmúlt években az ilyen jellegű drónok jelenléte hatalmas növekedést mutat. Pedig néhány évvel ezelőtt, az első drónnal kapcsolatos hír sokak számára egy osztrák politikus, Jörg Haider halálos közúti balesetével kapcsolatban merült föl. Akkoriban az egyik elmélet hátterének a dróntámadást jelöltek meg, mint egy lehetséges elmélet. Sokak számára akkoriban ez egy megfoghatatlan fogalom volt. Azóta természetesen a katonai célú drónokról szóló hírek is eljutnak a civil lakossághoz, legutóbb egy orosz felderítő lopakodó drónról lehetett olvasni cikkeket.

A továbbiakban a drón meghatározására az általánosan elfogadott meghatározást használjuk, mely szerint a drón egy pilóta nélküli légi jármű, vagy járműrendszer.

DRÓNOK FELHASZNÁLÁSI LEHETŐSÉGEI

A cikk a drónok civil felhasználását taglalja, így érdemes megvizsgálni, hogy milyen területeken alkalmazzák ezeket az eszközöket. Ennek a felosztását az 1. ábra szemlélteti.

1. ábra: A drónok alkalmazásának lehetőségei [1]

A fenti ábra alapján, tehát a drónokat összesen 4 csoportba sorolhatjuk: katonai, közszolgálati, kutatási, illetve kereskedelmi.

A továbbiakban több terület vizsgálatával foglalkozunk, mert jelen cikk célja nem a katonai célú felhasználás vizsgálata.

A drónok nem-katonai felhasználása a korábbi években, több irányban is felmerült, ennek egyik fő mozgatója az energiaszektor, ezen belül is a villamosipar, pontosabban az villamos áram szállítói- és elosztási szegmensek.

VILLAMOS HÁLÓZATOK

Ezeket az alkalmazásokat közszolgálati csoportba sorolhatjuk. Ez első próbálkozások és fejlesztések a magasan levő, feszültség alatt levő hálózatokon történő beavatkozások lehetőségeinek irányába mutattak. A próbálkozások elsődleges célja az emberi beavatkozás kiváltása, hiszen a hálózatok kezelése és karbantartása, főleg feszültség alatt levő vezetékek esetében, nagy kihívást és egyben veszélyt is jelent a villamos ipari munkavállalók biztonságra. Annak ellenére, hogy egy részletes szabályozás, valamint modern és szakszerű felszerelések állnak rendelkezésre, a munkavégzés ilyen vezetékek környezetében továbbra is folyamatos veszélyforrást jelent, és sajnálatos módon rendszeresen fordulnak elő munkabalesetek is.

A drónok által történő munkavégzés kihívásai még nem kerültek megoldásra. A kihívások közé számítanak a szélnek kitett vezetékek és szigetelők mozgásainak, kilengéseinek kompenzálása. Igen nehéz precíz munkát végezni a széllökések hatására folyamatosan mozgó tárgyon. További nehézséget okoz a munkavégzés teljes ideje. Néhány gyors munka kivételével, mint amilyen például bizonyos madáreltérítő eszközök felhelyezése, a villamos hálózatokon történő beavatkozás időigényes, amit a drónok jelenlegi energiaellátási lehetőségei nem tudnak biztosítani. Felmerült ebben az esetben a helyszíni töltés is, azonban több, ebben a tárgyban született tanulmány is arra következtetésre jutott, hogy ennek a műszaki megvalósítása – egyelőre legalábbis – nem megoldható.

Azonban érdemes tanulmányozni a drónok egyelőre nem alkalmazott felhasználási lehetőségeit is, érdemes túllépni a jelenlegi gondolkodásmódon, és olyan, egyszerűbb feladatok elvégzését elemezni, melyek jelenlegi módjához képest hatékonyabban, gyorsabban lehet megoldani drónok felhasználásával, illetve segítségükkel esetlegesen új típusú információszerzésre is lehetőség nyílik. [3] [5]

A villamos hálózatok területén maradva egyre nagyobb hangsúlyt kap a hálózati veszteségek kérdése. Ez, azon felül, hogy energiapazarlás, komoly költségeket jelent az áramszolgáltatók számára, amennyiben az áramtermelés és elosztás közös tulajdonban van, akkor az bevételkiesést is jelent. A hálózati veszteségeket jelen tanulmányban kizárólag műszaki szempontból elemezzük, és figyelmen kívül hagyjuk a fogyasztói fizetések elmaradását.

A hálózati veszteségek fő forrása az elektromos áram vezetésnek fizikai megvalósításából ered. Minden olyan anyag, amin áthalad az áram, bizonyos mértékű ellenállással bír. Miközben az elektromos áram áthalad ezeken, elkerülhetetlen, hogy az ellenállás leküzdése során bizonyos mennyiségű veszteséget kell elszámolni. Bár bizonyos veszteség elkerülhetetlen, de, nagyon sokat számít annak a mértéke. Nagyságrendekkel nagyobb veszteséget termel egy rossz minőségű vagy anyagában elöregedett szerelvény. A nagy ellenállással, így a nagy veszteséggel együtt jár a magas hőmérsékleten történő üzemelés is, amelyeket a hőkamerák egyértelműen ki tudnak mutatni. Több olyan hőkamera is elérhető, amelyeket drónra is fel lehet szerelni. Egy hőkamerával felszerelt drónnal lehetőség nyílik hosszabb szakaszok vagy bonyolultabb szerelvények diagnosztikai jellegű körberepülésére, a szerelvények hő képének rögzítésére és a felvételek utólagosan, irodai körülmények között történő elemzésére, valamint az eredmények alapján egy karbantartási és beavatkozási terv elkészítésére. [5]. A drón és a villamos irányító központ közötti valós idejű kapcsolat kialakítását is vizsgálni célszerű. A valós idejű kapcsolat esetén a hőkamera

által mutatott a megengedett értékek feletti érték esetén azonnali beavatkozásra nyílhat lehetőség. Az azonnali beavatkozás eredménye is valós időben ellenőrizhető lehet a drónon lévő hőkamerával. A villamos hálózatokat azonban nem csak veszteség szempontól érdemes elemezni, hanem különböző egyéb műszaki szempontok is felmerülnek. Ilyenek a vezetékek szálszakadásai is, ami fontos karbantartási tervek alapjait jelenti. Ezt, megfelelő fénykörülmények között, akár gyorsabb sebességgel végzett felvétellel is el lehet érni, és amennyiben megfelelő minőségű a felvétel, a drón rendelkezésre álló repülési ideje alatt jelentős szakaszt is fel lehet deríteni, és a felvételeket lassított üzemmódban visszanézve elemezni a hálózat állapotát.

Ugyanígy az oszlopok tetején, több méteres magasságban elhelyezkedő szigetelők és túlfeszültség korlátozók állapotát is lehet 360 fokos szögből ellenőrizni, ráadásul olyan perspektívából, amilyenre a hálózat karbantartó személyzetnek hálózat-bejárás során nincs lehetősége. A hálózat karbantartó személyzet csak a földről tudja a tárgyi eszközöket ellenőrizni, és még optikai nagyító eszköz használata mellett is maradnak fedett helyek, mit például a kúszóáramút biztosítását szolgáló ernyők tövében található pontok. Ezeket a drón, mivel egy magasságba tud helyezkedni ezekkel az eszközökkel, mind látja.

Gondoljunk csak bele, mennyi idő, mire például egy kb. 100 méterenként elhelyezkedő oszlopsort ellenőrizni tud egy karbantartó személyzet, főleg, ha az adott oszlopsor gyalogos vagy autós közvetlen elérésére alkalmatlan vagy nagyon nehéz – például árkok, mezőgazdasági művelt területek, patakok esetében – szemben egy drónnal történő felmérésre. Megállapítható, hogy hatékonyabb és biztonságosabb a drón használat. Ez igaz a rendszeres karbantartási feladatokon felül olyan esetekben is, amikor fakidőlések okozta oszloptörések vagy vezetékszakadások helyét kell azonosítani, főleg vihar utáni és téli (nagy mennyiségű hó) környezeti körülmények következményeképpen.

A villamos hálózatokon sok üzemzavart okoz a növényzet. Bár mindegyik áramszolgáltató rendelkezik megfelelő gallyazási munkákat végző csoporttal, a természet sokszor felülírja a tervezett gallyazási munkák ritmusát, és a tervezettől eltérően növekedő növényzet többször is zárlatokat, tehát üzemzavart eredményez a villamos hálózaton. Biztonságtechnikai szempontból nagyon fontos információkhoz tudunk jutni, ha a kritikus területeken, mint például erdősávok fölött rendszeresen végig repítünk egy drónt, és a felvételeket elemezve, valamint a korábbi felvételekkel összehasonlítva megállapítjuk a gallyazási munkák prioritását és sorrendjét. [3]

TERMÉSZETI MEGFIGYELÉSÉRE ALKALMAS FELHASZNÁLÁSOK

Az akkumulátorral üzemelő drónok jelenlegi műszaki jellemzőit vizsgálva a következő években az drónok új felhasználási lehetőségei túlnyomórészt inkább az utólagos elemzéseknek háttéranyagot biztosító feladatok irányába mutatnak majd, ezzel nagymértékben elősegítve kutatási feladatokat is. Ehhez ráadásul elégséges, ha a képrögzítés a drón készülékben történik, a kezelőnek csupán egy vizuális irányítói szerepre van szüksége, ami egy sokkal jobb minőségű felvételre ad lehetőséget.

A fenti, leginkább elemzési háttéranyagot biztosító felderítési munkákra koncentrálva, felmerül annak a lehetősége, hogy a vízrendészeti és vízbiztonsági szempontból rendkívül fontos gátak állapotának rövid idő alatt, hosszú szakaszok elemzésére is lehetőséget adnak a drónok, szintén nagy felbontású kamerák drónokra történő felszerelésével.

Ugyanígy a folyók állapotát normál állapotban is, de alacsony- illetve magas vízállásnál is gyors és hatékony elemzési megoldást kínál egy vagy több drónnal való berepülés és utólagos elemzés. „A drón repülésekkel légi megfigyelés útján rövid idő alatt nagy területek, hosszú folyószakaszok ellenőrizhetők”

BIZTONSÁGTECHNIKA

További biztonságtechnikai megoldást kínálnak a drónok tömegrendezvények esetében, ahol – a közterületi kamerákhoz hasonlóan – a drónok felvételeit arcfelismerő rendszerrel kombinálva eddig elérhetetlen információkhoz tudunk jutni. Ilyen esetekben több drón egyidejű felhasználásával, és a labdarúgó stadionokból ismert, kereskedelmi célú, többkamerás adatfeldolgozó rendszer használatával különböző, biztonságtechnikailag veszélyes személyt és csoportot lesz lehetőségünk azonosítani, mozgásukat követni. [6], mint például az illegális határátlépő esetében [7]. Hasonlóképpen szabálytalan gépjármű manőverek azonosítására is használja már most is a magyar rendőrség, például a nyári zsúfolt autópályákon a leállósávot szabálytalanul használó - és ezzel veszély esetén a veszélyelhárító járművek mozgását akadályozó – gépjárművezetők kiszűrésére [8].

VASÚTHÁLÓZAT

Egy fontos és kritikus infrastrukturális elem a vasúthálózat. Ebben az esetben mind a sínek, mint az áramellátást biztosító villamos hálózat, mind a vasúti átkelők biztonságos állapotának elemzésére kitűnő megoldást kínálnak a drónfelvételek. Ezek könnyű tárolhatóságának köszönhetően az összehasonlító elemzésből nyert információkat is kaphatunk, amire korábban nem volt lehetőség, valamint a drónok segítségével elkerülhetőek lehetnek az olyan veszélyes helyzetek, amikor valamilyen nagyobb tárgyat helyeznek vasúti sínekre az ütközés megfigyelésének reményében. [9]

ÖNKORMÁNYZATI LEHETŐSÉGEK

Tulajdonképpen a drónok minden olyan feladatra bevethetők, amit az önkormányzat légi fotózással oldana meg. Alapvetően az önkormányzat működését térinformatikai rendszerek már erőteljesen támogatják. A drónok alkalmazhatóak település és terület tervezésnél, lakás, ingatlan és vagyon gazdálkodásnál, logisztikánál és sok egyéb területen is.

Azt már az eddigiekből is megállapítottuk, hogy a drónok felhasználásának, alkalmazásának széles körű lehetősége van. Közvetlenül vagy közvetve, de a mindennapjainkban valamilyen módon megtalálhatóak. A településrendezés tervezés hatása vagy a pontos korrekcióknak a felismerése is támogathatók drón felhasználásával. Egy-egy önkormányzati befektetésnél a település hosszú távú fejlesztési lehetőségeit határozzák meg, hogy ezek a tervek, így ennek ráhatása van a közlekedésre, illetve a további fejlesztési lehetőségekre. Ezeket a terveket drónok segítségével könnyen és egyszerű módon el lehet készíteni, amiből később látványtervet lehet készíteni. Ezekkel a tervekkel a lakosságot tudja az önkormányzat tájékoztatni és így be tudja mutatni az adott fejlesztés terveit, amivel a könnyebb és átláthatóbb megértést, illetve ezáltal a nyíltabb véleménynyilvánítást készíti elő. A településrendezés tervezése az önkormányzatnak fontos feladata, hiszen a település mindennapjait széles körben befolyásolja. Egy-egy nagyobb volumenű beruházás komoly

terhelés mind a környezetnek mind a város\falu lakosainak is. Viszont fontos megjegyezni, hogy ezzel a település munkahelyeket is teremt, így a lakosságnak biztos anyagi környezetet biztosít. A fentiekkel együtt a drónokat rengeteg célra tudja használni az önkormányzat, ide tartoznak az utólagos hatások felmérése, az önkormányzat által vállalt felelősségek teljesítésében, illetve a jogkövetés nyomon követésében is, például építkezések során. [6]

Ezeknél a tervezéseknél nagy hangsúlyt kell fektetni az előkészítő és utólagos munkákra is. Magyarországi példaként erre mindenképp fontos megemlíteni a Balaton partvonalának illegális nádvágásait, melyet az alábbi ábra szemléltet, és partfeltöltését, illetve ezeknek a partszakaszoknak a feltérképezését. Ezeket a feladatokat az önkormányzatok által igénybe vett eszközökkel könnyen, egyszerűen, rövid idő alatt megoldhatók. Így pontosan és hatékonyan feltudják térképezni, illetve le lehet ellenőrizni, és eleinte még megelőzni is tudják a Balaton partszakaszán végzett illegális tevékenységeket.

2. ábra: Nádirtás a Balatonon

KÖRNYEZETVÉDELMI LEHETŐSÉGEK

Úgy gondoljuk, hogy a környezetvédelmi célú lehetőségek a drónok alkalmazásának egyik legfontosabb lehetősége. Gondoljunk csak bele a vízi élőhelyek felmérése milyen nehéz és komplikált feladat. A roppant nehéz megközelítés, a természetvédők, illetve a nemzeti parkok munkavállalóinak is komoly kihívásokat okoz, azonban ezeknek a területeknek a magasból történő megfigyelésével, illetve feltérképezésével könnyen kivitelezhető. A hagyományos megoldások (pilóta által vezetett légi-járművek) sokszor egyszerűbb megoldásnak tűnhetnek, viszont ne feledjük ezeknek a megoldásoknak a hátrányos jellemzőit. Hiszen a rendkívül magas hangok, a repülő, helikopter robosztus termete, vagy ezeknek a mozgása könnyen megzavarhatja a terület élőközösségnek a mindennapjait, így egy esetleges felmérés során nem kapunk pontos képet, adatokat az adott terület megfigyeléséről. [4]

A légi megfigyelés kezdeményezését számos tényező befolyásolja és ezáltal indokolttá teheti. Egy-egy kiemelten védett terület, annak dús élettel teli lelőhelye és élővilága sajnos az embereket törvénytelen tettekre késztetheti. Ezeknek a csoportoknak a felderítése, illetve a védett természet és élővilág megőrzése céljából a természetvédők gyakran vetnek be drónokat. Ilyen esetekben a repüléseket mindenképp hang és zajmentesen kell végrehajtani. Így a külvilág számára szinte láthatatlan lesz a megfigyelés, így a törvénytelen tettek végrehajtásától az elkövetőket elidegeníti. Ilyenkor a természetvédők kétféle képen tudják

a természetet megóvni és megvédeni: egyrészt az adott terület konkrét megfigyelésével, illetve az adott területen élő állatok megszámlálásával tudják ezt biztosítani. Mindenképp meg kell említeni, hogy bár korábban az állatszámlálások gyakoriak voltak, manapság már a magas költségek miatt csak ritkábban vagy korlátozottan alkalmazzák. A drónok alkalmazása viszont ezt a kritériumot is könnyen kiválthatja, hiszen ezek az eszközök manapság már jóval alacsonyabb áron beszerezhetők.

Sajnos a természetvédőknek nem csak az illegális tevékenységet tervező csoportoktól kell tartania. Egyes területek csoda szép látványa, illetve ezeknek a helyeknek a nem mindennapi élővilága gyakran nagyszámú turista tömegeket vonz az adott élőhelyre. Ilyenkor gyakori a turisták kíváncsiskodása, ami sokszor zavarhatja, vagy kifejezetten rossz hatással lehet az adott élővilág környezetére. Ez a megállapítás különös tekintettel igaz fokozottan védett területek esetében A nem engedélyezett látogatások ellenőrzésére, illetve ezeknek az embereknek a távoltartására a természetvédők gyakran alkalmaznak drónokat. [6]

A vadkempingezés felderítése és megállítása komoly kihívások elé állítja a természetvédőket. Véleményünk szerint is kiemelten fontos feladat, hiszen fontosnak tartom, hogy ezek a csodás élőhelyek megőrizzék a természet szépségét. Ezeket a területeket drónok használatával könnyen lehet felügyelni. A természetvédelmi szakemberek a parkok területei felett alkalmazzák a kisméretű viszont könnyű kezelhetőségű drónokat. Ezek az eszközök korlátozott képeségekkel bírnak, ami alatt a repülési időt és megtehető távolságot értjük. Bár ezeknél drónoknál a megtehető táv korlátozott, mindenképp fontos megemlíteni, hogy a könnyű kezelésből adódóan egyszerűen és gyorsan bevethetők. Ezek az eszközök nem nehezek, néhány kilogrammot nyomnak, ezáltal könnyen mozgathatók, így nagy flexibilitást biztosítanak a felhasználójuknak. Nem bocsájtanak ki nagy hangot (hajtásuk villanymotorral történik), rájuk leggyakrabban valamilyen hőkamera kerül. Ezeknek a lehetőségeknek a felhasználási köre szinte korlátlan, ennek tényleg csak a fantáziánk szabhat határokat. Természetesen a környezetvédelmi célok között nem csak a területek megóvását, megőrzését értjük, hanem ide tartozik a területek környezetszennyezésének a visszaszorítása. A közeljövőben a drónok, különösen az akkumulátor kapacitás várható fejlődése tovább szélesíti az ilyen jellegű felhasználási lehetőségek körét.

ÖSSZEFOGLALÁS

A nem katonai drónok felhasználási potenciálja jóval túlmutat a mostani felhasználásokon, több területen is be lehet vetni a drónokat különösebb fejlesztések igénye nélkül, főleg felderítő jelleggel, álló- és mozgóképrögzítésre és azok későbbi szakmai elemzésére. Meggondolandó a drónok és irányító, felügyeletet ellátó központok közötti valós idejű kapcsolat biztosítása.

Ennek köszönhetően több olyan infrastrukturális biztonságtechnikai beavatkozásra is fel lehet használni őket, mint a villamoshálózatok, gát hálózatok, vasúti hálózatok állapotának gyors és átfogó elemzésére, amik egy hatékonyabb preventív és karbantartási jellegű munkák alapjait biztosítják, vagy tömegrendezvények során veszélyes személyek vagy csoportok azonosítására.

Amennyiben a fenti lehetőségek valóban elterjednek, felmerül a kérdés, hogy drónok jószándékú felhasználásán felül, a drónok adta információszerzési lehetőségek rosszhi-

szemű felhasználása ellen is védekezés szükségessége, az ezzel kapcsolatos biztonsági előírásokat, szabályozásokat és műszaki követelményeket és technikai eszközöket érdemes kidolgozni annak érdekében, hogy az ilyen szerkezetek használata során eleget tudjunk tenni az ebből eredő, új típusú biztonságtechnikai kihívásoknak. [2]

Megállapítottuk, hogy a drónokat az önkormányzatok is számos célra tudják alkalmazni, például a településrendezés tervezésnél. Ennek segítségével a település területi könnyen felderíthetők, aminek segítségével olyan látványtervek készíthetők, amikkel az adott település lakosait könnyen lehet véleménynyilvánításra sarkalni.

Rámutattunk, hogy a környezetvédelmi feladatok ellátása is segíthető a drónok alkalmazásával. Ezekkel az eszközökkel a természetvédők az adott védett területeket könnyen ellenőrizhetik és megóvhatják.

FELHASZNÁLT FORRÁSOK

[1] Drónok a közszolgálatban.
http://www.kozszov.org.hu/dokumentumok/UMK_2017/3/05_Dronok_a_kozszolgalatban.pdf
letöltve: 2020.09.05
[2] A drónok használatának legújabb szabályozása
https://arsboni.hu/a-dronok-hasznalatanak-legujabb-szabalyozasa/
letöltve:2020.09.05.
[3] Drónok energia- és közüzemi alkalmazása
http://www.jovogyara.hu/dronok-energia-es-kozuzemi-alkalmazasa.html
letöltve: 2020.09.11
[4] Színfelismerés alkalmazásának lehetőségei szántóföldi növénytermesztésben
https://www.researchgate.net/publication/333966396_Szinfelismeres_alkalmazasanak_lehetosegei_szantofoldi_novenytermesztesben
letöltve 2020.09.11
[5] Drónok ipari alkalmazásai
ftp://www.energia.bme.hu/pub/Energetika%20a%20mindennapokban/2016-17-02/04/dronok.pdf
letöltve: 2020.09.15
[6] UAV-k alkalmazása a közfeladatok ellátása során
http://real.mtak.hu/87038/1/183_06_nemeth.pdf
letöltve: 2020.09.17
[7] Robotszemek vigyázzák majd a magyar határt
https://magyarnemzet.hu/belfold/robotszemek-vigyazzak-majd-a-magyar-hatart-7253216/
letöltve: 2020.10.15
[8] Hosszú hétvége: százezres bírságot kap az, aki pofátlanul közlekedik az M7-esen
https://www.napi.hu/magyar_vallalatok/m7-autopalya-hosszu-hetvege-augusztus-20-rendorseg-ellenorzes-leallosav.712000.html
letöltve: 2020.10.15
[9] Bevásárlókocsit és kukát tettek a sínekre – a rákosmenti rendőrök elfogták őket
http://www.police.hu/hu/hirek-es-informaciok/legfrissebb-hireink/bunugyek/bevasarlokocsit-es-kukat-tettek-a-sinekre-a#3
letöltve: 2020.10.15

SIGNIFICANCE OF SPECTRUM MONITORING SYSTEMS IN THE FIELD OF ESTABLISHMENT PROTECTION

A SPEKTRUM MONITOR RENDSZEREK JELENTŐSÉGE AZ OBJEKTUMVÉDELEM TERÜLETÉN

DOMJÁN András [1]

Abstract

Wireless data connection has been built due to recent technological developments including either infocommunicational applications or any electronic devices surrounding us. We use radio connections in many cases because it's comfortable only, in other cases it would be too complicated to build it or not possible physically at all. Radio spectrum inspecting system mentioned in the title should be the strategic element of the modern building protection because the mechanical and technical devices used in our everyday life are based on electronic mechanism. Due to the mentioned reasons the detection of electro-magnetic force field could be the base during the realization of a complex security system. I'm going to describe the advantages of a spectrum-monitor function that was built as a part a complex building protection system and the tasks to be solved in connection with detection. I will show you how an RF-monitor application could detect a remote controlled listener or improvised explosive structure within a building during switching on.

Keywords

Electormagnetic field, Radiospectrum-monitor system, principle of detecton, selectivity

Absztrakt

Napjaink technológiai fejlesztéseinek köszönhetően szinte kivétel nélkül minden területen vezeték nélküli átvitel került kialakításra az infokommunikációs alkalmazásoktól kezdve a közvetlen környezetünkben található egyéb berendezések működtetéséig. A mindennapi életünk során alkalmazott műszaki-technikai eszközeink mindegyike elektromos működésen alapul, ezért az elektromágneses erőtér jelenléte a detektálás alapját képezi egy komplex biztonsági rendszer megvalósítása során. A következőkben ismertetem a rendszer részeként kiépítésre kerülő spektrum monitor funkció nyújtotta előnyöket, és a detektálással összefüggő megoldandó feladatokat. Bemutatom hogyan képes az RF[2] monitor alkalmazás épületen belül detektálni egy előre definiált védett területen megjelenő (pl.: a bekapcsolás folyamata során), távvezérelt lehallgató vagy improvizált robbanó szerkezetet.

Kulcsszavak

elektromágneses sugárzás, RF monitor rendszer, detektálás alapelve, szelektivitás

[1] andras.domjan@gmail.com | ORCID: 0000-0002-0178-5263 | Head of Information Protection Department/Információvédelmi Osztályvezető | Counter Terrorism Centre/Terrorelhárítási Központ

[2] Rádiófrekvenciás

A VÉDELMI RENDSZER TERVEZÉSE

Egy komplex objektumvédelmi rendszer megtervezése során a teljes kockázatanalízis elvégzésével tudjuk feltárni, hogy valójában milyen veszélyekkel kell számolnunk az épület majdani működtetése folyamán.

A fenyegetettséget figyelembe véve, alapvetően két fő csoportba sorolhatjuk a kiemelten védett objektumok védelme során jelentkező veszélyeket. Ezen területek közül az egyik kategóriába az épület elleni közvetlen támadásokat, a másikba az épületek funkciójához, továbbá az ott dolgozók munkájához fűződő bizalmas információk jogosulatlan megszerzésére irányuló tevékenységeket sorolhatjuk. [1] A terjedelemre való tekintettel, cikkemben csak a robbantás elleni védelem és az információvédelem egy-egy speciális -távirányításos lehallgató berendezések- szempontjából közelítem a komplex védelem megvalósításának egy lehetséges változatát, amelynek kiépítésében meghatározó szerep jut a rádió spektrum ellenőrzésére. A nyílt sajtóban is közzétettek több olyan esetet, amikor a világ különböző részein megtalálható kormányzati épületeket értek támadások. Köztük nagy számban szerepelnek robbantásos merényletek, valamint titkos lehallgatáson alapuló információszerzési cselekmények. A két kategória detektálhatósága tekintetében a működtetésük alapját jelentő rádiótávirányítású eszközök jelentik a közös pontot. A távolról vezérelhető vagy indítható robbanó-, és lehallgató szerkezetek esetében - a felhasználásukat megelőzően - lehet esélyünk a védekezésre, valamint a komolyabb károk bekövetkezésének a megakadályozására. Ennek a feladatnak a megoldására szükség van egy, a védendő épületben történő állandó és valós idejű rádió spektrum figyelő rendszer kiépítésére.

A rádióspektrum (hatósági) ellenőrzése

A frekvenciagazdálkodás a nemzetközi és a nemzeti jogszabályokban rögzített módon, minden államnak komoly gazdasági hatással bíró feladatköre. Nemzetközi szinten az ITU-R[3] által rögzített alapelvek határozzák meg a frekvencia kiosztással és a használt spektrum ellenőrzésével kapcsolatos eljárási rendeket és módszereket. A frekvenciakészlet védelmén túl a nemzeti szabályozás célja a rádiós átvitel zavartalanságának biztosítása is. Hazánkban az elektronikus hírközlésről szóló 2003. évi C. törvény (a továbbiakban Eht.) írja elő tételesen a kijelölt állami szerv részére a tevékenység megkezdésétől a hatósági ellenőrzési kötelezettségig a frekvenciagazdálkodással összefüggő feladatokat. Az Eht. 11.§ (3)(4) -es bekezdése a következőket tartalmazza:

„(3) A Hivatal köteles a frekvenciahasználattal kapcsolatos nemzeti, illetve nemzetközi megállapodásokon alapuló nemzetközi rádiómegfigyelést, ellenőrzést, felderítést, zavarvizsgálati és zavarelhárítási tevékenységet végezni, amelynek során jogosult a rádióadások műszaki-forgalmi megfigyelésére és azok rögzítésére, jogszabályban meghatározott feltételek szerint.

(4) A hírközlés védelme, a frekvenciahasználat hatékonysága és káros zavaroktól való mentessége, valamint az elektromágneses összeférhetőség (EMC[4]) biztosítása céljából a Hivatal rádióméről és rádió-zavarelhárító szolgálatot tart fenn."[5] [2] A jogszabályból is egyértelműen látható, hogy a rádióspektrummal összefüggésben rögzített feladatkörként a

[3] International Telecommunication Union Radiocommunication Sector - Nemzetközi Távközlési Unió Rádiós tagozata

[4] Electromagnetic Compatibility - elektromágneses kompatibilitás vizsgálatok (az elektromágneses sugárzás okozta zavarok mérése)

[5] 2003. évi C. törvény - az elektronikus hírközlésről 10. oldal (Netjogtár - Letöltés ideje: 2020. december 10.)

mérési tevékenység kiemelt helyen szerepel. Ennek érdekében a Nemzeti Média- és Hírközlési Hatóság (a továbbiakban a Hatóság) a SIMON[6] projekt részeként egy országos mérő-iránymeghatározó rendszert hozott létre. A rádiómegfigyelés segítségével folyamatosan detektálja az éterbe kisugárzott elektromágneses hullámok jelenlétét, a rádióállomások jeleinek jellemzőit. A rádióellenőrzés során az engedéllyel rendelkező rádióadók műszaki paramétereit mérik, hogy azok mennyiben felelnek meg a nyilvántartásban szereplő értékekkel. A rádiófelderítési feladatkör hivatott az ismeretlen rádiófrekvenciás sugárzások helyének a megállapítására, amely fixen telepített, gépjárműbe szerelt vagy kézi iránymérő műszerek segítségével történik. [3]

A hatósági ellenőrzési feladatkörökből egyértelműen látszik, hogy a hírközlés szabályainak betartása és betartatása meglehetősen összetett tevékenység, amelynek kivitelezéséhez komoly műszaki - elsősorban rádiótechnikai - ismeretekre és műszerezettségre van szükség.

A detektálás alapelve

A törvény szövege is megemlíti az elektromágneses összeférhetőség (EMC) szempontjából való ellenőrzés szükségességét. Az érzékelés alapját képezi a parazita elektromágneses hullámok berendezések általi sugárzása, amelyek a vezeték nélküli összeköttetéseken felül megjelennek az éterben, és megfelelően paraméterezett mérő-ellenőrző rendszer segítségével felfedhetők a rendelkezésre álló rádió spektrumból.

Ezt az elvet kezdték vizsgálni, majd alkalmazni 2007 körül IED[7]-k felderítésére az amerikai hadseregnél, a háborús övezetekben. A kísérletek során drónokra telepített RF vevőkkel próbálták felkutatni a nyílt terepen rejtett vezeték nélküli improvizált robbanószerkezeteket (RCIED[8]). Az egységeik ellen elkövetett robbantásos merényletek számának markáns növekedése rávilágított a védelmük ezen területének hiányosságára, és arra, hogy leghatékonyabban a megelőzéssel lehet harcolni az ilyen jellegű tevékenységgel szemben. [4]

Az épületeinket behálózzák a különböző információ és villamos energia továbbítására kiépített vezetékrendszerek. Az objektumvédelem szempontjából egy további detektálási lehetőségként jelentkezik ezen vezetékes hálózatok - mint antennák - által „összegyűjtött" úgynevezett vezetett jelek vizsgálata. Itt ugyanúgy az RF spektrumanalízis kerül szóba a gyenge-, és erősáramú vezeték rendszerek esetében is.

A mérés szempontjából nagyon lényeges jellemző a mérőműszer és a vizsgálandó eszköz közötti távolság, ugyanis az elektromágneses hullámok esetében - a sugárforrástól távolodva - a jelszint hatványozottan csökken. Ezt a kiindulási értéket figyelembe véve meglehetősen alacsony jelszintet képvisel a vevő bemenetén.

A detektálási szint határának vizsgálata során meg kell említeni a Johnson - Nyquist tétel néven ismert termikus zaj fogalmát, amely alapján a sávszélességtől függően becsülhető az adott abszolút „zajszint". [5]

[6] Spektrum és Interferencia Monitor rendszer
[7] Improvised Explosive Device - improvizált robbanóeszköz
[8] Radio Controlled Improvised Explosive Device - rádióvezérlésű improvizált robbanó szerkezet

A SPEKTRUM MONIOR RENDSZER AZ OBJEKTUMVÉDELEMBEN

A hatósági rádió felügyeleti rendszerhez és a harctéri RCIED felderítési metodikához hasonlóan a komplex objektumvédelem egyik fontos egységének kell tekinteni az információvédelem és a robbantás elleni védekezés részeként kiépített spektrum mérő-ellenőrző hálózatot. Az országosan kialakított mérőpontok analógiájára, a védendő területeken (irodák, tárgyalók, előadó termek) elhelyezett szondák segítségével tudjuk megfelelő hatékonysággal detektálni az épületbe bekerült távirányításos IED-k és lehallgató berendezések jelenlétét.

A hatékony felderítés érdekében a mérés és ellenőrzés menete folyamatosan kell történjen, továbbá egy komplex egységet kell alkotnia az épület behatolásjelző-, és videó megfigyelő rendszerével.

A rendszer alapvetően három fő részből tevődik össze:

- mérőmodulok (antennák);
- központi egység (jelfeldolgozás, adattárolás);
- felügyeleti (operátor).

Az RF monitor rendszer elvi felépítése

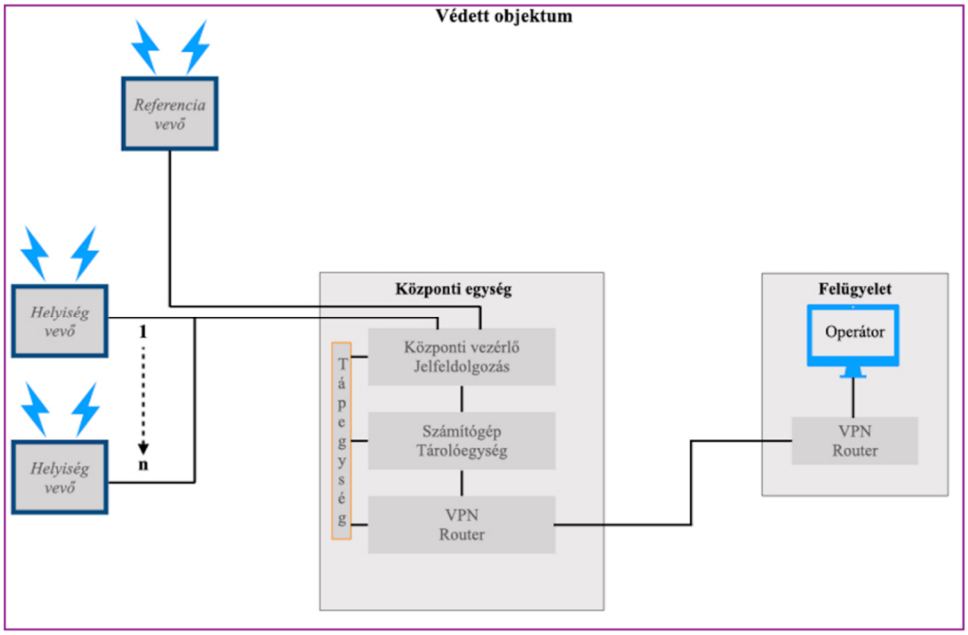
A helyiségekbe beépített mérő modulokhoz közvetlenül vannak csatlakoztatva a különböző tartományú és sávszélességű antennák. Az érzékelés teljesítményszintje döntő a hatékony működés szempontjából, ezért az antennák elhelyezése és vezetékezése kulcsfontosságú a rendszer kiépítése során.

A központi mérő-feldolgozó egység és az operátor munkaállomásának egymáshoz viszonyított elhelyezkedése - a hálózati összeköttetés miatt - kevésbé lényeges szempont, mivel annak menedzselése akár távfelügyelet formájában is megoldható.

A mérési eredmények feldolgozása valós időben kell, hogy történjen különös tekintettel a rendszer védelmi jellegére és az esetleges szükséges intézkedések megtétele miatt.

A védendő objektum területén elhelyezett mérőegységek hálózaton keresztül vannak összeköttetésben a központi egységgel. Ennek az egyik fő feladata, hogy a mért jelek egy helyen legyenek kiértékelve, lehetőség szerint egymáshoz többféle szempontból is viszonyítva. Ez az értékelés történhet egymás utáni (időben) ún. soros módon vagy párhuzamos szervezésű jelfeldolgozással, amely lényegesen nagyobb hatékonysággal bír. Ezt a műveletet a központi számítógép végzi, amely egy adatbázist hoz létre a mérési eredményekből, melyet további vizsgálatokkal statisztikai elemzésekkel - különböző időtartományokra vonatkoztatva - tudunk szűrni, vizsgálni.

A keletkezett adatok lehetnek a kiindulópontjai egy későbbi alaposabb technikai átvizsgálás, ellenőrzés megtervezésének. Így különösen a még nem beazonosított spektrumösszetevők vagy meghatározott időben ismétlődő rádiófrekvenciás jelek pontos sugárzási helyének a felkutatásában.



1. ábra: RF monitor rendszer elvi rajza (Forrás: szerző által szerkesztett)

Mérési elvek, módszerek

A megfelelő hatékonyság elérése céljából folyamatos frekvencia figyelést kell végeznünk, melyet bizonyos időtartamig rögzítünk egy esetleges későbbi feldolgozás érdekében.

A detektálást követően az ellenőrzés alapját a spektrumanalízis jelenti, amelyet a digitális jelfeldolgozás segítségével akár valós időben is megtehetünk. Első lépésként a vizsgálandó jeleket szeparálnunk kell a keletkezésük szerint, szét kell választanunk az úgynevezett külső és belső forrásokra (mikró- és - makrókörnyezet). Ezt hívjuk térbeli elhatárolásnak. Ennek a megvalósítása érdekében a belső antennarendszeren felül alkalmazni kell egy külső (referencia) mérőpontot is. A szeparációt segítik az építmények szerkezetéből adódó tulajdonságok, mint a térelhatároló és térelválasztó falak, amelyek a szabadtéri terjedési viszonyokhoz képest jelentős csillapítással rendelkeznek. Az objektumoknak a rádióhullámokra gyakorolt hatásán felül meg kell említeni az elektromágneses sugárzás tekintetében meglehetősen zsúfoltnak számító környezetünket, amely jelentősen megnehezíti a veszélyt jelentő eszközök kiszűrését. Ehhez szükséges egy rendszeresen frissített adatbázis megléte, illetve a mérési eredmények feldolgozásához, adott esetben mesterséges intelligencia (AI[9]) alkalmazása. A jelanalízis segítségével a rádiójelek fizikai paraméterein túl (jelerősség, vivőfrekvencia, sávszélesség, moduláció), akár az alkalmazott csatorna-, és blokk kódok megállapítása is lehetséges. Ezek ismeretében van esélyünk az esetleges rejtett adattartalom kiszűrésére. Az információvédelem vagy akár az RCIED felderítés esetén, a monitor rendszer pozitív jelzése is elégséges lehet egy rejtett eszköz jelenlétének a felfedésében.

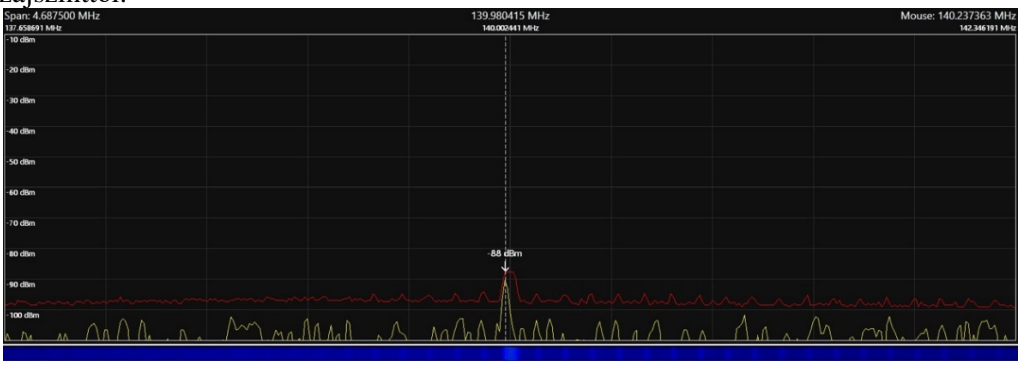
[9] Artificial Intelligence - mesterséges intelligencia

A 24/7 monitor rendszer jelentősége

A lehallgatás elleni védelem során a TSCM[10] tevékenység kiemelt részeként említik a szakértők a rádióspektrum folyamatos figyelését, a védendő objektumon belül. Az információvédelem alapját képező taktikai elem - spektrumanalízis - megszakítás nélküli végzése elengedhetetlen az illegális megfigyelés szembeni hatékony védekezés szempontjából. A mai technikai eszközök kínálta lehetőségek (SDR - szoftverrádió) képesek biztosítani számunkra a megfelelő paraméterű rendszer kiépítésének lehetőségét. A technikai elhárítást végzők körében sokszor alakul ki hamis biztonságérzet az átvizsgálás során, mégpedig a rádióspektrum ellenőrzése kapcsán. A kellő felkészültség hiányában a feladatot végrehajtók hajlamosak abban a tévhitben befejezni a munkájukat, hogy az átvizsgálás ideje alatt folytatott frekvencia ellenőrzés - aktív vezeték nélküli eszköz kutatására vonatkozólag - valós negatív eredményt jelentett. A spektrum monitor rendszerekre vonatkozólag létezik egy jelölő szám, amely százalékos arányként mutatja, hogy a frekvencia vizsgálat ideje alatt, milyen hatásfokkal képes felderíteni az ismert jelek közül a rejtett eszköz elektromágneses hullámait. Ez a POD[11]. A mérési tevékenységet statisztikai szempontból megközelítve egyértelművé válik mindenki számára, hogy az úgynevezett POD értéke a vizsgálat időtartamára levetítve, elenyésző százalékot jelent az éves viszonylathoz képest. Konkrétan vizsgálva a POD által meghatározott százalékot egy rendszeresen átvizsgált objektum esetén: a frekvencia ellenőrzési tevékenység heti 1 óra időtartamban, éves viszonylatban körülbelül 50 órát jelent, ez egy évre számítva 0,5%-os találati arányt képvisel. [6]

Egy komplex objektumvédelmi rendszer esetében az éter folyamatos minitorozásán felül, nem szabad figyelmen kívül hagyni a kapacitív-, induktív csatolásokon keresztül az erőátviteli hálózatokon (230VAC) megjelenő (vezetett) jelek ellenőrzését sem. A rejtett eszközök sok esetben közvetlen közelségbe kerülhetnek a vezetékes hálózathoz, amelynek folyamatos vizsgálata javíthatja a találati arányt. [7]

A következő ábrán bemutatásra kerül egy 140 MHz-es FM adónak a 230 V-os hálózaton megjelenő spektrumképe. A villanyvezetékek közelébe - teszt jelleggel elhelyezett - RF sugárzó (-30 dBm) jele, jól érzékelhető módon megjelenik vonali jelként az erőátviteli hálózaton (-88 dBm). A jelszintek közötti jelentős csillapítás ellenére, markánsan elkülönül a zajszinttől.



2. ábra: 140 MHz-es rádió adó vonali (230VAC) spektrumképe (forrás: szerző által mérés során rögzített (2020. 05. 21.))

[10] Technical Surveillance Countermeasures – rejtett lehallgató-, megfigyelő eszközök felkutatásának végrehajtása
[11] Probability of Detection – detektálás valószínűsége

A teszt eszköz frekvencia értékét szándékosan választottam a 140 MHz-körüli tartományba, mivel az adott vezeték hálózat (230VAC) viszonylag „csendes" volt, ezen a szakaszon.

Figyelembe véve a 24/7 monitor rendszer hatékonyságát - a statisztikai felderíthetőséget figyelembe véve - a következőkben bemutatott rejtett eszközökkel szemben az eseti jelleggel végrehajtott technikai átvizsgálás (TSCM) meglehetősen nagy hibaszázalékúnak tekinthető. Ez nem megengedett a megfelelő biztonsági szint elérése érdekében.

A távirányítású improvizált robbanószerkezet és a lehallgató berendezés

Alkalmazásuk szempontjából mindkét szerkezetet a célhelyre kell juttatni a kívánt „hatás" elérése érdekében. Taktikailag egy improvizált robbanószerkezet, valamint a távvezérelt lehallgató berendezés esetén is csak a tényleges műveleti helyszínen történik meg az „élesítés" - bekapcsolást követően, távolról indíthatóvá válik -, majd ezután a rejtett szerkezet úgynevezett „várakozó" állapotba kerül. A szerkezetek felderítésére a várakozástól a vezérlőjel kiadásáig van lehetőségünk, mivel a konkrét indítójel megjelenésével gyakorlatilag az elektronikai működés sebességétől függően (néhány század másodperc) bekövetkezik a nem kívánt hatás. Egy vezeték nélküli lehallgató berendezés a bekapcsolás után egy újabb rádiós csatornán - az adatátvitelhez szükséges sávszélességben - keresztül kezd sugározni, ami relatív könnyen felfedhető az RF-spektrum figyelésével.

A rádió spektrum tekintetében az ISM[12] sáv használata a legelterjedtebb, mivel az adott csatornákon működő rádióadóknak nem szükséges külön hatósági engedéllyel rendelkezniük. Az ISM csatornák közül Európában a 27 MHz, a **433 MHz**, a 868 MHz és a 2,4 GHz-eseket használják. Az utóbbi időben az 5 GHz-es tartomány is kezd forgalmasabbá válni. A 433 MHz-es sávot külön kiemelten kell kezelni, mivel háborús konfliktusok szempontjából érintett területeken is (Közel-Kelet, volt Szovjetunió, Perzsa-öböl, Afrika) engedélyezettnek számít.

Az RCIED konkrét felépítése meghatározza a felderíthetőségét a merénylet elkövetése előtt. Jelen esetben az egyik legfontosabb szempontot jelentik a működtetésében kulcsszerepet játszó rádiós modult alkotó speciális áramköri elemek, amelyek nagyban hozzájárulnak a spektrumfigyelés útján történő detektáláshoz.

Főbb szerkezeti elemei

Mindkét ábrán a rádiósugárzás ikonja szimbolizálja az adott berendezésből származó elektromágneses hullámokat, amelyek detektálására képes rendszert tervezünk a komplex objektumvédelmi részeként.

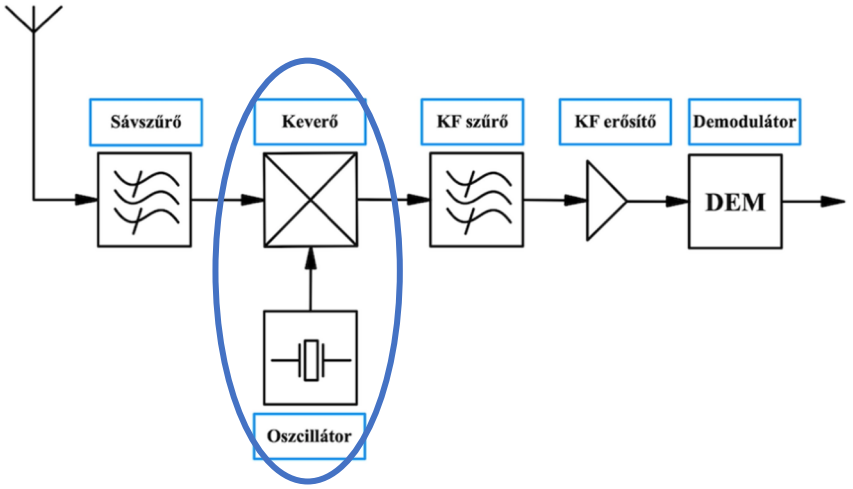
Az 1-es számú ábrán egy RCIED elvi rajza látható, amelyek közül a tervezett merénylet helyszínén maga a vevőegység - a robbanószerkezetbe szerelve - teszi lehetővé számunkra a pokolgép robbanása előtti felfedését. Jól érzékelhető, hogy a vezérlő (adó) térben elkülönül az improvizált eszköztől, és ez a távolság elsősorban az adó műszaki paramétereitől függ. Az üzemszerű működés tekintetében a két eszköz helyzete az adó RF sugárzási teljesítményétől, a terjedési paraméterektől és a vevő érzékenységétől függ. Az adó által kisugárzott jel szintje nagyságrenddel meghaladja a vevőegység által produkált teljesítmény szintet.

[12] Industrial, Scientific and Medical band - Ipari-, kutatási-, egészségügyi frekvencia sáv

A „*Vevőegység*” néven jelzett alkatrész többnyire a „távolkeleti” RF-alkatrészeket gyártó cégek kínálatából, akár nagyobb mennyiségben is elérhető az internetes piacon keresztül, a világ bármely pontjáról. Az áramköri kialakításuk egy-egy főbb vevőtípusra koncentrálódik, közöttük jellemzően a „szuperheterodin” - elv a legnagyobb számban előforduló.

A terjedelemre való tekintettel, a vevő elvét jelen dolgozatomban nem ismertetem, annak csak a témakörrel kapcsolatban érintett részével foglalkozom.

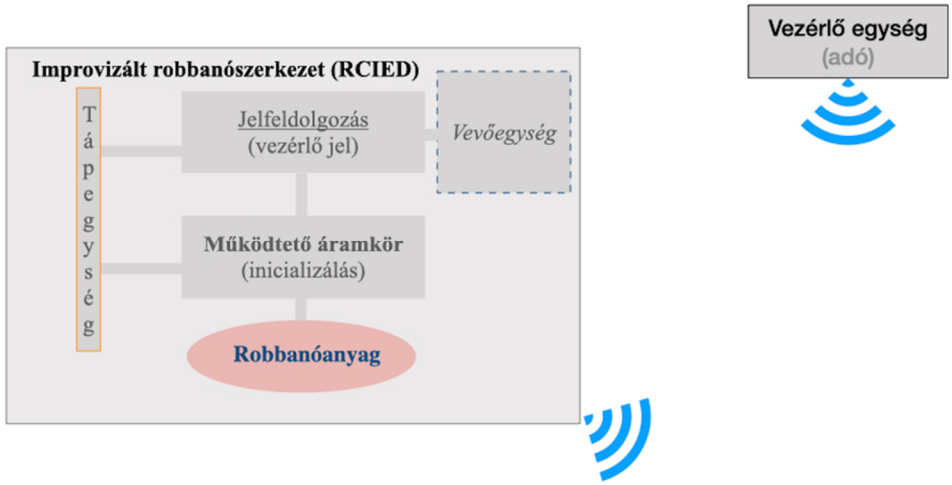
A következő ábrán a vevő elvi felépítése látható, amelyen a detektálás szempontjából a „legaktívabb” részegységként a mixert emelném ki a rezgéskeltő alkatrésszel együtt.



3. ábra: A szuperheterodin vevő elvi rajza (forrás: szerző által szerkesztett)

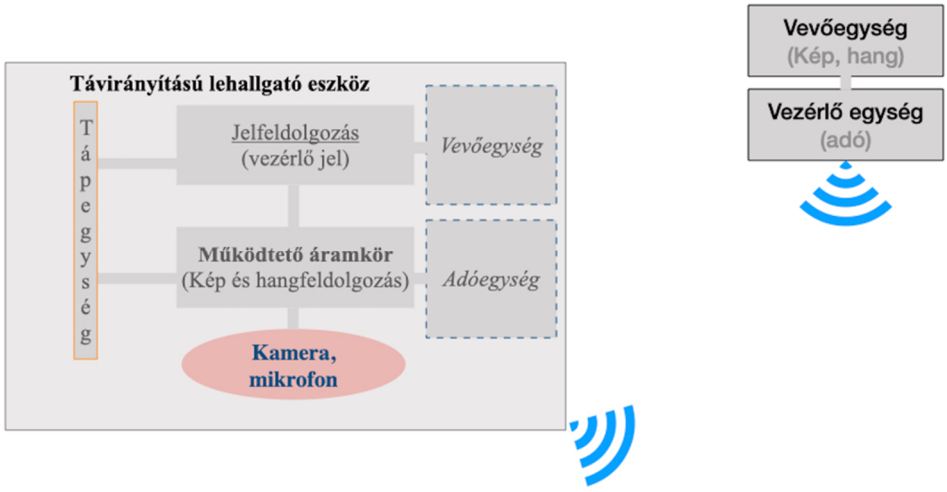
A mixerben a vivő-, és az oszcillátor frekvenciája kerül összeszorzásra, ez által megjelenik a kettő különbsége is, ami általában a soron következő részegység - középfrekvencia - tartományába eső érték. Ebből adódik, hogy a helyi oszcillátor a venni kívánt frekvencia közeli értékén rezeg (sugároz).

A gyakorlati tapasztalat szerint a gyártók törekednek a nemkívánatos, úgynevezett parazita RF összetevők sugárzásának a csökkentésére, de a legnagyobb igyekezetük ellenére mindig mérhető valamilyen szintű jel a távolság függvényében.



4. ábra: RCIED elvi felépítése (Forrás: szerző által szerkesztett)

A következő ábrán egy távolról vezérelhető lehallgató berendezés elvi felépítése kerül bemutatásra. Rögtön szembetűnik a két szerkezet közötti hasonlóság a rádiós kapcsolat kialakítása alapján. Mindkét eszköz tartalmaz egy vevőegységet, amely meghatározó a működése szempontjából. Az RCIED-től eltérően a távirányítású lehallgató eszköz szerkezeti elemei között megfigyelhetünk egy külön adóegységet is, ami a megszerzett információ vezeték nélküli továbbítására szolgál.



5. ábra: Távirányítású lehallgató berendezés elvi felépítése (Forrás: szerző által szerkesztett)

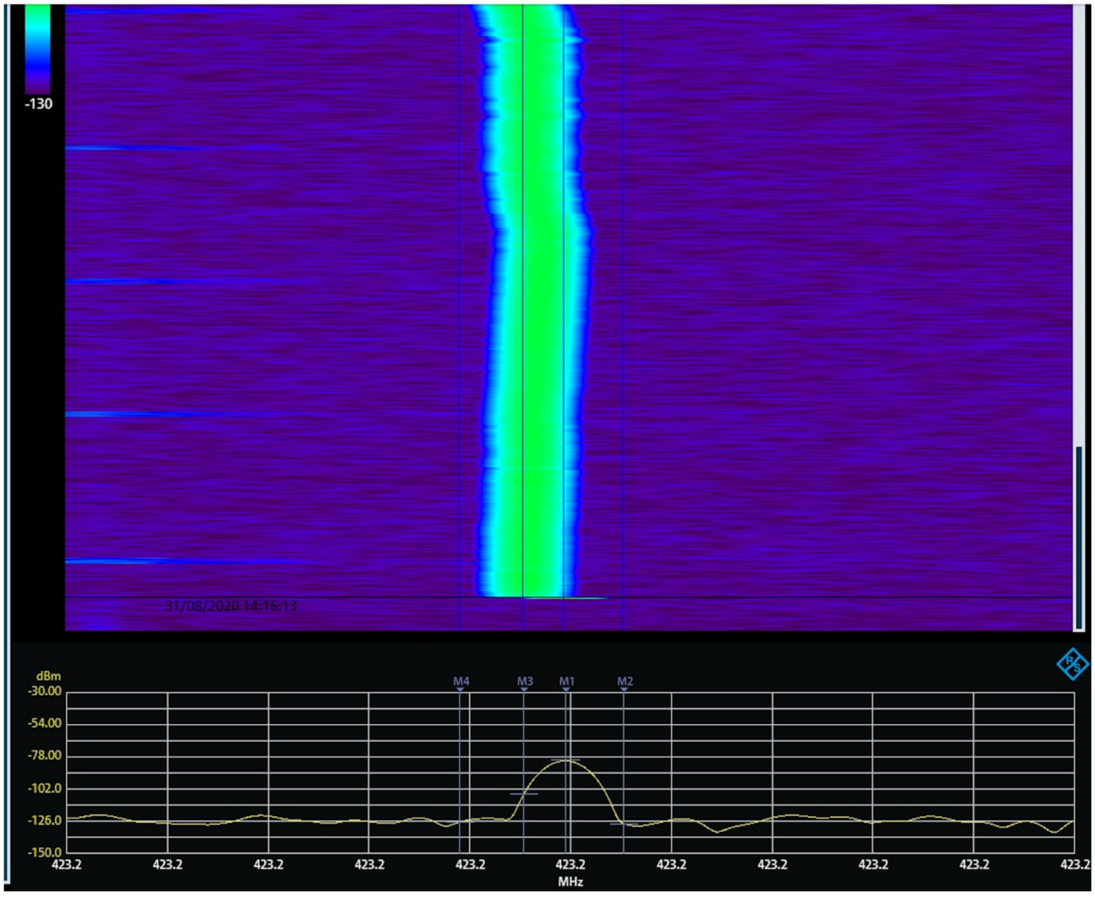
A bemutatott két rádióvezérelt eszköz közös jellemzője, hogy egy távolról leadott jellel indítható, de míg egy rejtett lehallgató „csak" információszivárgási csatornát jelent számunkra (közvetett hatás), addig egy távvezértelt improvizált robbanószerkezet súlyos sérüléseket, illetve jelentős anyagi károkat okozhat a detonáció hatására.

A két ismertetett berendezés közös eleme (vevőegység) kapcsán van lehetőségünk a védendő objektumon belül felfedni a rejtett eszközöket, amennyiben rendelkezünk a kellő érzékenységű és természetesen időben folyamatosan működő detektáló rendszerrel.

A bűnös célú - fentebb bemutatott - elkövetésekből adódóan, a monitor rendszernek képesnek kell lennie az időbeni spektrumváltozások pontos érzékelésére, és adott esetben egymástól való megkülönböztetésére is. Alkalmas kell legyen egy rádióvezérlésű improvizált robbanóeszköz vagy egy lehallgató berendezés védett épületrészen történő bekapcsolásának felismerésére.

A következő spektogramon (6. ábra) egy RXB8 jelű rádiós modul bekapcsolási folyamata figyelhető meg egy spektrumanalizátor segítségével.

A kép felső része mutatja a frekvencia időbeni változását (alulról felfelé haladva), a jelszinteket a színek szimbolizálják (kb. -80 dBm a zöld sáv). A kezdő pillanatból és a „kanyargásból" következik, hogy a frekvenciamenet - ami leginkább hőmérsékletfüggő a vizsgált típusú modulok esetében - időben változó, esetenként alkatrészfüggő is.



6. ábra: 433 MHz-es vevő modul bekapcsolási frekvencia változása az időtartományban (szerző által mérés során rögzített (2020.06.10.))

Az ábra alsó felére esik az amplitúdó-frekvencia érték megjelenítése, amely közvetlenül a bekapcsolásról nyújt értékes információkat. Leolvasható a kezdő frekvencia, a sávszélesség, a jelszint, majd az állandósult csúcsérték is.

A monitor rendszernek ezt a folyamatot kell tudni rögzítenie, - megfelelő felbontással - hogy az a későbbi feldolgozás során összehasonlítható és természetesen adott esetben megkülönböztethető is legyen más jelektől, a vizsgálatok alkalmával.

ÖSSZEGZÉS

A bemutatott spektrum monitor rendszer védelmi képességeként ismertetett RCIED és lehallgató szerkezetek detektálására való alkalmasságának az egyik leglényegesebb feltétele az érzékenységén túlmenően, a szelektálási tulajdonsága. A mai világunkban az éter „zsúfoltsága" nem elhanyagolandó jellemző sem a városi, sem a közvetlen környezetünkben sem.

A komplex objektumvédelmi rendszer egyik fő összetevőjeként bemutatott spektrum monitor tevékenység hatékony végrehajtásához - a referencia szint mérés kiegészítéseként - szükséges lehet a Hatóság által üzemeltetett rádiómegfigyelő hálózathoz való kapcsolódás, hogy a makrókörnyezetről mindig valós adatokkal rendelkezzünk.

A meglehetősen alacsony jelszintek érzékeléséhez megfelelő karakterisztikájú antennákat kell illeszteni a vevőmodulokhoz, a lehető legrövidebb csatlakozóvezetékek használatával.

A bevezetőben ismertetett, elsősorban kényelmi szempontok miatt zsúfolttá váló rádió spektrum elemzése során, a speciális tulajdonságokat is figyelembe vevő analizátor szoftver nélkülözhetetlen a releváns eszközök felismerése és megkülönböztetése céljából. A megfelelő részletességgel rögzített mérési adatok teszik lehetővé a feldolgozó program számára, hogy a rádióspektrumban nagyon rövid idő alatt, alacsony jelszinten lezajló folyamatokat is a legkisebb reakcióidővel tudja kellő biztonsággal veszélyesnek vagy veszélytelennek nyilvánítani. Ennek végrehajtására bonyolult algoritmusok és részletes adatbázisok szükségesek a nagy és gyors számítási kapacitás mellett.

FELHASZNÁLT FORRÁSOK

[1] Domján András, „A KIEMELTEN VÉDETT OBJEKTUMOK BIZTONSÁGA A FENYEGETETTSÉG TÜKRÉBEN," *Hadmérnök,* XII/3 szám, pp. 26-36, 2017.

[2] 2003. évi C. törvény - az elektronikus hírközlésről, „Netjogtár," Letöltés helye: https://net.jogtar.hu/jogszabaly?docid=a0300100.tv. Letöltés ideje: 10. 12. 2020.

[3] Tomka Péter, „hiradastechnika.hu," július 2004. Letöltés helye: https://www.hiradastechnika.hu/data/upload/file/2004/2004_07/HT0407-7.pdf. Letöltés ideje: 01. 10. 2010.

[4] Cristopher M. Griffith, *Unnamed Aerial Vehicle-Mounted High Sensitivity RF Receiver to Detect Impovised Explosive Devices,* Montery, California: Naval Postgraduate School, 2007. 09.

[5] Horváth Zsolt, „mti.kvk.uni-obuda.hu," 2014. Letöltés helye: http://mti.kvk.uni-obuda.hu/adat/tananyag/passziv/Passziv8Zajok2014.pdf. Letöltés ideje: 15. 10. 2020.

[6] Paul. D. Turner, „intersecmag.co.uk," jan. 2017. Letöltés helye: http://www.intersecmag.co.uk/wp-content/uploads/2017/01/int-jan-feature-34-36.pdf. Letöltés ideje: 10. 2018.

[7] Paul. D. Turner, „intersecmag.co.uk," 20. 02. 2020. Letöltés helye: http://www.intersecmag.co.uk/remote-control/. Letöltés ideje: 10. 06. 2020.

EVOLUTION AND THE CURRENT STATE OF THE VOICE COMMUNICATION EQUIPMENTS INTEGRATED INTO OPERATIONS MANAGEMENT SYSTEMS

A BEVETÉSIRÁNYÍTÁSI RENDSZEREKBE INTEGRÁLT BESZÉDCÉLÚ ESZKÖZÖK FEJLŐDÉSE, JELENE

RAJNAI Zoltán[1] – VÉGH Attila[2]

Abstract

Voice communication equipment are basic accessories of the today's operations management systems. Due to the nature of the activity, wireless devices and systems are integrated into these systems. The wireless devices in the past decade have undergone huge development, due to the convergence of information and telecommunication systems. Our study focuses on point-to-multipoint communication technologies, review the development of these eqipments, basic features. Analog systems that are still in use today, the circuit-switched digital technologies, and technologies that work as applications on packet-switched systems released a few years ago are disclosed. We refer the dispatcher softwares that can be interpreted as an integration interface of these systems, in addition, standards are mentioned that assures compatibility in the technical development of technologies

Keywords

operations management, TETRA, EDR, MCPTT over LTE, PoC

Absztrakt

A mai bevetésirányítási rendszerekben alapvető tartozékok a beszédcélú eszközök. A tevékenység jellegéből adódóan ezekbe a rendszerekbe vezeték nélküli eszközök, rendszerek kerülnek integrálásra. A vezeték nélküli eszközök az elmúlt évtizedben óriási fejlődésen mentek keresztül, köszönhetően többek között az informatikai és távközlési rendszerek konvergenciájának. Tanulmányunkban hangsúlyt a pont-multipont közötti kommunikációs technológiák kapnak, áttekintjük ezeknek az eszközöknek a fejlődését, továbbá az alapvető tulajdonságait. Bemutatásra kerülnek a még jelenleg is forgalomban lévő analóg rendszerek, az áramkörkapcsolt digitális technológiák, illetve a pár éve megjelent csomagkapcsolt rendszereken alkalmazásként működő technológiák. Érintjük a rendszerek integrációs felületeként értelmezhető diszpécseri szoftvereket, továbbá a technológiák műszaki fejlődésében a kompatibilitást biztosító szabványok is említésre kerülnek.

Kulcsszavak

bevetésirányítás, TETRA, EDR, MCPTT over LTE, PoC

[1] rajnai.zoltan@bgk.uni-obuda.hu | ORCID: 0000-0002-9139-736X | dean/dékán | Óbuda University Donát Bánki Faculty of Mechanical and Safety Engineering / Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar
[2] vvscadaa.ph@gmail.com | ORCID: 0000-0002-4187-3997 | PhD student / doktorandusz | Obuda University Doctoral School of Safety and Security Sciences / Óbudai Egyetem Biztonságtudományi Doktori Iskola

BEVEZETÉS

A beszédcélú, vezeték nélküli kommunikációs rendszereket gyakorlati felhasználás szempontjából két kategóriába soroljuk:

- pont-multipont rendszerek
- pont-pont közötti rendszerek

A gyakorlatban megvalósult rendszerek az általános emberi kommunikációs formák modellezésén alapulnak.

A pont-multipont közötti kommunikáció a csoportba szerveződött emberek között folyik, ez a legalapvetőbb kommunikációs formánk. Ennél a modellnél a csoport egy ember beszédét hallgatja. A beszédet közlő személye folyamatosan változhat, kulturált keretek között azonban mindig csak egy ember beszél. Munkaszervezés szempontjából a pont-multipont kommunikációs modell a leghatékonyabb, mivel a csoport minden szereplője részese a kommunikációnak, ezáltal értesülnek a feladat minden részletéről, tisztában vannak a munkafolyamatok állapotával [1].

A pont-pont közötti kommunikáció a csoportból elkülönülő két szereplő között alakul ki, akik azért válnak ki a csoportból, hogy magánbeszélgetést folytassanak. Ebben a kommunikációs módban lehet hatékonyan a feladatok részleteit a két embernek átbeszélnie, nem kell versenyezniük a többi csoporttag figyelméért. Többek között a bizalmas információk is ebben a formában kerülnek megbeszélésre a két fél között.

VEZETÉK NÉLKÜLI BESZÉDCÉLÚ PONT-MULTIPONT RENDSZEREK

Az egymástól nagyobb távolságokban lévő csoporttagok kommunikációjának elősegítésére megjelentek az adó-vevő készülékek. Alapvető tulajdonságuk, hogy az eszköz üzemmódjának váltásával kell kezdeményezni a kommunikációt. Az adás kezdeményezéséhez minden adó-vevő készülék rendelkezik adásváltó nyomógombbal, melynek megnyomásával ő lesz az aktív, kezdeményező szereplője a csoportnak, ezzel együtt az ő beszédét hallja minden (ellátottsági területen belül lévő) csoporttag. Ezt a nyomógombot PTT (Push to Talk)-nak is nevezzük az angol nyelvű rövidítéséből adódóan. A szakirodalom összefoglaló néven PTT alapú kommunikációs rendszereknek is nevezi [1].

Az adó-vevő készülékek többnyire előre kiépített infrastruktúra nélkül is képesek működni. A lefedettségi terület kiterjesztése aktív átjátszó, átemelő berendezések telepítésével lehetséges. A kiterjesztés értelmezhető földrajzilag egy magaslati pozícióba telepített átjátszóberendezéssel, de a műtárgyak okozta többletcsillapítás leküzdését is jelentheti amennyiben az épületen belüli, föld alatti, zárt terekben kell biztosítani a rendszer ellátottságát. Az infrastruktúra esetleges kiesésével azonban a felhasználó nem tudja a megszokott ellátottsági területen használni a végkészülékét. Ennek a hátránynak a kiküszöböléséhez - ha az alkalmazott technológia engedi és a kieső szolgáltatások hiánya részben kezelhető – az érintett csoporttagoknak át kell térniük az infrastruktúra nélküli használatra [2].

TRÖNKÖLT RÁDIÓRENDSZEREK

Azonos ellátottsági területen több beszédcsoport kiszolgálásának az igénye is felmerülhet. Ennek a megoldására a legegyszerűbb lehetőség, hogy minden beszédcsoport számára létesítünk egy-egy különálló infrastruktúrát.

Kis felhasználói csoportszám esetében - a rendelkezésreállás fenntartása végett – ez megfelelő megoldás. Nagyszámú felhasználói csoport esetében viszont ez eléggé gazdaságtalan megoldás, ugyanis a végberendezéseket – ebből következően a kiszolgáló rendszert - nem mindenki és mindenkor használja. Statisztikailag kimutatható, hogy a rendszerben egyidejűleg maximálisan felhasznált erőforrások száma kisebb, mint a felhasználói csoportok száma.

A hatékony rendszerszervezés érdekében a szabad erőforrások (jelen esetben a szabad beszédcsatornák) összevonásra kerülnek, majd a felhasználói igényeknek megfelelően a PTT megnyomását követően a kezdeményező beszédcsoporthoz hozzárendelésre kerül.

A módszernek – azaz a trönkölésnek – a hátránya, hogy a szabad erőforrások elfogyása előfordulhat. A trönkölt rendszerekben az erőforrások szélsőséges használata esetén prioritási szinteket határoznak meg – azaz amennyiben két csoport versenyez az utolsó csatornáért, azt a magasabb prioritású csoport kapja meg. Szélsőséges esetben egy, már felépült kapcsolat kerül eldobásra egy magasabb prioritású igény kiszolgálására. Komolyabb rendszerek operátori beavatkozásra előre meghatározott forgatókönyvnek megfelelően a beszédcsoportok újraszervezésére is képesek. Erre példa, hogy egy lakatos, egy biztonsági őr illetve egy munkavédelmi előadó is lehet létesítményi tűzoltó, akit vészhelyzet esetén a saját beszédcsoportjukból kiragadva a katasztrófavédelmi csoportba kell átsorolni.

A szabad erőforrások közös felhasználásával – azaz trönköléssel - kialakított rendszerek képezik a modern távközlési technológiák alapjait [3].

ANALÓG RENDSZEREK

Az analóg PMR (Private Mobile Radio) rádiórendszerek a végkészülékek közötti direkt kommunikációtól a komoly, több bázisállomás hálózatba kötéséből alkotott cellás trönkölt rádiórendszerig kínálnak megbízható műszaki megoldást. Ezek a rendszerek mind a mai napig üzemelnek, alkotóelemeik kereskedelmi forgalomban vannak. Az analóg rendszerek esetében egy vivőfrekvencián egy csoport képes egyidőben kommunikálni. A technológiák fejlődésével, új műszaki megoldások megjelenésével az utóbbi években a középpontba került a spektrumhatékonyság kérdése. Továbbá a felhasználók részéről is jelentkezett az igény a digitális rendszerekben látott szolgáltatások iránt (pl. egyszerű adatátviteli megoldások, szöveges üzenetek kezelése stb.). Ezért a vezető gyártók a tisztán analóg képességű rádiós rendszerelemek gyártását többségében már kifuttatták [3, 4].

DIGITÁLIS MOBIL RÁDIÓRENDSZEREK

A DMR (Digital Mobile Radio) rendszerek áramkörkapcsolt digitális rendszerek, melyek a mai modern követelményeket kielégítik. Alapvetően a civil felhasználói kört célozták meg a szabvány lefektetésével, azonban számos olyan szolgáltatással rendelkeznek, melyek a később bemutatásra kerülő, készenléti szervek számára tervezett rendszerek szolgáltatásai között is szerepelnek. Ezeket a szolgáltatásokat részleteiben ebben a fejezetben tárgyalom [5].

A DMR szabványban – melyet az ETSI (European Telecommunications Standards Institute - Európai Távközlési Szabványügyi Intézet) 2005-ben jelentetett meg - az analóg PMR rendszerelemek a spektrumhatékonyság és a többletszolgáltatások igényének megfelelően lettek átgondolva úgy, hogy az analóg rendszerek kiváltása kompatibilitási gondok

nélkül legyen megoldva. Az analóg-digitális átállás folytonossága végett gyártók által készített digitális DMR berendezések nagy többsége analóg módon is képes kommunikálni, így a meglévő analóg infrastruktúrán is lehet őket használni. A rendszerelemek folyamatában történő cseréjével kisebb, többszöri befektetéssel valósítható meg az átállás.

A szabvány három szinten különbözteti meg a rendszerösszetevőket:

1. DMR Tier I. – Rádióengedély nélkül, szabadfelhasználású csatornákon üzemeltethető végkészülékek, 446 MHz frekvenciatartományban, limitált csatornaszámban, maximum 0,5 Watt ERP rádiós teljesítménnyel. Egyéb rendszerelem (átjátszó, fix telepítés külső antennáával stb.) itt nem üzemeltethető.
2. DMR Tier II. – Rádióengedéllyel, bérelhető frekvenciákon használható, hagyományos felépítésű hálózatokat vannak meghatározva. A felhasználás elsődleges célja a professzionális, spektrumhatékony digitális hang-és adatkommunikáció.
3. DMR Tier III. – Nagyobb mennyiségű felhasználói csoportok professzionális kiszolgálását célzó trönkölt működési módot határoz meg, spektrumhatékony digitális hang-és adatkommunikációval.

A DMR rendszerek - melyek hazánkban is nagy népszerűségnek örvendenek a professzionális felhasználók körében a kibővített szolgáltatásaikkal mindamellett, hogy az analóg készülékekhez képest kétszeres spektrumhatékonysággal rendelkeznek. A használt vivőfrekvenciát időosztásos (TDMA) technológiával két időrésre osztja fel, így egy 12,5 kHz széles rádiós csatornán két, azonos időben működő logikai beszéd vagy adatcsatornát hoz létre. A csomagokra tördelt információk keretei egyéb, hasznos információkat, jelzéseket is tartalmazhatnak. Ezek az információk tartalmazzák a hívás azonosítókat, jelzéseket és a hívás típusát (egyedi, csoport, mindenki hívása). [6]

A DMR rendszerek hangátviteli szolgáltatásai:

- privát hívás
- csoporthívás
- mindenki hívása
- vészhívás

A kommunikáció során az információk bizalmasságának megőrzése céljából a DMR rendszerek többféle titkosítási szintet valósítanak meg. Az átjátszóállomások elérését azonosításhoz lehet kötni, továbbá a végkészülékek igény szerint az adat illetve beszédkommunikációt 8, 40, illetve 256 bites titkosítással tudják megvalósítani. A szabványtól eltérően, gyártóspecifikusan többnyire az AES256 titkosítási algoritmus is implementálásra került.

A prioritások kezelése a DMR Tier I és II rendszerek esetében a központi vezérlőelem hiányából adódóan nem tökéletes. A hívások megszakításának engedélyezésével, tiltásával két prioritási szint valósítható meg. A DMR Tier III, trönkölt kiépítésben megjelenik a központi vezérlőegység. Ezzel a vezérlőegységgel a rádiókészülékek egy dedikált vezérlőcsatornán folyamatos kapcsolatban vannak. Az így központosított vezérlés teszi lehetővé a prioritások többszintű kezelését.

Hívásjelzések segítségével minden esetben azonosításra kerül a hívó fél illetve az éppen használt beszédcsoport. Az eltulajdonított, idegen kézbe került készüléket lehetőség van kitiltani illetve az eszköz előkerülése esetén újra aktiválni. Lehetőség nyílik továbbá a

készülékeket távolról adásra kényszeríteni, ezzel a közvetlen környezetükbe távolról bel e lehet hallgatni. További szolgáltatás, hogy az egyes készülékek üzemkészségét (azaz be van-e kapcsolva, nincs lemerülve az akkumulátor illetve a lefedettségi területen belül van-e), illetve jelzést lehet nekik küldeni, azaz hangjelzéssel jelzik a készülékek, hogy keresték őket.

A DMR rendszer adatátviteli szolgáltatásai

- IP alapú adatátvitel
- Rövid szöveges üzenetküldési lehetőségek
- GPS alapú helymeghatározási szolgáltatások
- telemetriás szolgáltatások

DMR rendszerek felépítése

A DMR rendszer alap kiépítettségében egy átjátszóállomásból és a hozzá tartozó végkészülékekből áll.

Az átjátszóállomások IP hálózatokon is képesek kommunikálni. Ezáltal lehetőség nyílik az ellátott terület növelésére, a rendszerelemek felügyeletére, de a felhasználást elősegítő diszpécseri alkalmazások is ezen a felületen kapcsolódhatnak a rendszerhez.

Ha nem a lefedettségi területet, hanem a kapacitás hatékony növelése a cél, lehetőség nyílik több átjátszóállomás közös erőforráskezelésére, trönkölésére.

Ha a nagyobb kapacitású rendszert nagyobb területen kívánjuk használni, a lokális trönkölt rendszereket IP hálózat segítségével össze lehet kapcsolni, ezzel kiterjesztve az ellátott területet.

Diszpécseri rendszerek [7]

Az előzőekben felsorol topológiák mindegyikében a DMR rendszer kiegészíthető diszpécseri és rendszerfelügyeleti alkalmazással, mely szintén IP hálózaton keresztül csatlakoztatható. Az alkalmazások grafikus felületen keresztül elősegítik, hogy kezelhető legyen a rendszerhez fűződő, illetve a rendszerrel kapcsolatos összes szolgáltatás, melyek közül a legfontosabbakat kiemelve:

- előzőekben felsorolt hívásfajták kezelése
- AVL/APL rendszer (automatic vehicle location / automatic person location), GPS és / vagy beacon alapú helymeghatározó, pozíció megjelenítő, ellenőrző rendszer
- szöveges üzenetek
- hang-és eseményrögzítés

TERRESTRIAL TRUNKED RADIO (TETRA)

A TErrestrial Trunked RAdio (TETRA) - digitális trönkölt rádiós szabvány, melyet az ETSI a TETRA and Critical Communications Association (TCCA) közreműködésével hozott létre az 1990-es években. A szabvány megalkotásával egy rugalmasan skálázható trönkölt rádiórendszer alapjait hoztak létre a nagyfelhasználók részére. A TETRA esetében ez 25 kHz széles rádiós csatornán 4 logikai csatorna létrehozásával valósul meg – ezzel a spektrumhatékonyság igényét is kielégítették. A TETRA rendszerelemekkel egy telephe-

lyes, több telephelyes, illetve akár nemzeti v. nemzetközi szintű lefedettség is megvalósítható. Példaként meg kell említenünk a készenléti szervezetek számára felépített TETRA rendszert, melynek hazai neve az EDR (Egységes Digitális Rádiórendszer) [6].

A rendszer előtérbe a Schengeni határok védelmi együttműködésének meghatározásakor került, melyben az együttműködő szervezetek közötti, határokon túli kommunikációs rendszer megléte alapfeltétel volt. Nemzetközi szervezetek, azaz a szabványalkotók, a gyártók, és a felhasználók közötti együttműködés eredménye TETRA szabvány.

Elsődleges felhasználói, az európai készenléti szervek mellett a rendszerek felhasználói között megjelentek a honvédség, közlekedési vállalatok és a közművek üzemeltetői is.

Néhány funkció, melyre kizárólag a TETRA rendszerben kerültek megvalósításra:

- nagy kiterjedésű hálózatokon is gyors hívásfelépülés
- a készenléti szervek igényeinek megfelelő szintű titkosítás
- vészhívás kezelés – a rendszer foglaltsága esetén is biztosítja a hívás megérkezését
- a belső telefonhálózatokkal összekötött hívások kezelésére duplex kommunikáció

TETRA technológia beszédcsoport és adatkommunikáció kiszolgálására lett optimalizálva nagykapacitású, sűrűn telepített cellás felépítésű bázisállomásokkal. Következésképp a végkészülékek rádiófrekvenciás teljesítménye - azaz mérete csökkent.

A hang –és alapszintű adatátviteli funkciók a DMR rendszereknél említettekkel lényegében megegyeznek.

A készenléti szervezetek által használt technológiák fejlődésével megfogalmazódott az igény az egyre nagyobb mennyiségű adat átvitele. Természetesen az operatív egységek számára mindezt vezeték nélkül kell megvalósítani. A TETRA Release 2, avagy a TEDS (TETRA Enhanced Datat Service) szabvány nagyobb adatátviteli sebességet (max. 473 kbit/s) képes megvalósítani az eredetileg 25 kHz széles rádiós csatorna felhasználása helyett több csatorna összenyalábolásával, illetve fejlettebb modulációs módok felhasználásával. Ez az adatátviteli képesség már lehetőséget nyújt akár mozgó képi információk korlátozott átvitelére is.

Az adatátviteli felhasználásra azonban jelenleg a 4G – LTE (Long Term Evolution) tűnik sikeresebbnek a készenléti felhasználók között. A közeljövőben bevezetésre kerülő 5G technológia már teljesen elhomályosítja a létjogosultságát a TETRA adatátviteli képességeinek a fejlesztésére. A végberendezések gyártói is felismerték ezt a tendenciát, mára már megjelentek a beszédcélra TETRA, adatátviteli célra LTE rendszert használó terminálokkal [8].

MCPTT OVER LTE

Azok a pont-multipont kommunikációs rendszereket, melyek megfelelnek a közbiztonság szempontjából kritikus hangkommunikációs elvárásoknak, azaz

- a rendszer magas rendelkezésreállású
- a rendszer magas megbízhatóságú
- gyors a hívásfelépülés, alacsony a késleltetés
- csoporthívás lehetőséget biztosít
- privát hívás lehetőséget biztosít

- a hívó fél/csoport azonosítható
- végkészülékek az infrastruktúra kiesése esetén egymás között is képesek kommunikálni
- vészhívás lehetőséget biztosít
- stb.

Mission Critical PTT, avagy az MCPTT rendszereknek.

A 3GPP szervezet 2016 márciusában megjelentetett LTE (Release 13) szabványa már lehetőséget ad Mission Critical Push to Talk alkalmazások fejlesztésére közös adatátviteli platformon.

A szabvány 2017-es és 2018-as (Release 14 és 15) kiadásai által a Mission Critical Data, illetve a Mission Critical Video alkalmazások számára is lehetőséget nyújt [9].

A Mission Critical over LTE előnye, hogy egy technológia biztosítja a hang és az adatcélú szolgáltatást, (nem kell külön integrált rádió a két külön szolgáltatáshoz – ebből adódóan kisebb a fogyasztás, illetve a technológiák közötti váltás nem okoz kiesést az elérésben, készülék antennája könnyebben optimalizálható, stb. [10].

A rendszer rugalmassága, könnyebb integrálhatósága végett a szervezet megjelentetett egy nyílt forráskódú szoftverfejlesztői csomagot MCOP - Mission Critical Open Platform néven. Ennek megjelentetése 2018-ra kelteződik. Ezek a csomagok a 3GPP vonatkozó szabványainak legújabb megjelenéseit implementálják, továbbá tesztelési céllal kapcsolódási lehetőséget is nyújtanak [11].

PUSH TO TALK OVER CELLULAR

A Push To Talk over cellular (avagy a PoC) technológia egy vezeték nélküli beszédcélú szolgáltatás, mely platformon pont-multipont közötti kommunikációs kapcsolat teremthető. A mobil terminálok a celluláris hálózatok adatátviteli platformján, azaz GPRS illetve LTE összeköttetést használva VoIP (Voice Over Internet Protocol - Voice Over Internet Protocol) segítségével valósítják meg az összeköttetést. Ebből következik, hogy kapcsolat felépítése csomagkapcsolt, nem pedig áramkör-kapcsolt. Ezáltal a platform – bár az alapelképzelés szerint a GSM hálózatok adatátviteli szolgáltatásait használják – minden további fejlesztés nélkül alkalmas a terminálokba integrált egyéb adatátviteli módok kihasználására, gondolva itt elsősorban az egyénileg kiépített WIFI hálózatokra. Az amerikai piacon ez a megoldás már bizonyított, olcsó csoportkommunikációs technológiát biztosítva a felhasználóknak [12].

A technológia fejlődése arra vezethető vissza, hogy a mobilszolgáltatók az alap GSM, CDMA technológiát biztosító hálózatain a nem pont-pont kommunikációra használható szolgáltatásokat nem támogatták, ezzel szemben az adatátviteli hálózatot folyamatosan fejlesztették. A csomagkapcsolt adatátvitelnek köszönhetően a hálózat erőforrásainak felhasználása kismértékű, a technológia jó hatékonysággal üzemel, a szolgáltatók immáron nem zárkóznak el a szolgáltatás elől.

Az amerikai szolgáltatók saját technológiákba fektettek, ezzel szemben az európai szolgáltatók vártak a befektetéssel egy széles körben elfogadott, több technológiát magába foglaló szabványra. A távközlési ipar olyan lépcsőzetes megközelítést követett, amely egy ilyen szabványhoz kapcsolódik. Az első lépés a hangátvitel, vezérlés és jelzésátvitel szab-

ványosítása. Ezt az első szabványt „NEMS" -nek nevezték el (NOKIA, ERICSSON, MOTOROLA, SIEMENS). A következő lépés a szabvány finomítása, illetve pár funkcióval történő kiterjesztése volt. A második szabvány az OMA (Open Mobile Alliance) konzorciumban készült. Ezzel együtt a szabvány implementálásaként elkészült az első SDK, melynek segítségével könnyedél elkészíthető a szolgáltatáshoz szükséges számítógépes alkalmazás [13].

A rendszer működéséhez, mint ahogy az MCPTT over LTE esetében is - mindenképp szükség van egy szerver alkalmazásra, amely szervezi a csoporton belüli és a csoportok közötti adatforgalmat. Ezek a szerveralkalmazások hatékonyan üzemeltethetők felhő szolgáltatásként [14].

A VEZETÉK NÉLKÜLI KOMMUNIKÁCIÓ JÖVŐJE

A kritikus infrastruktúrák szemszögéből

A kritikus infrastruktúrák üzemeltetéséhez, rendelkezésre állásuk folyamatosságának biztosításához, rendkívüli események kezeléséhez a célnak megfelelő kommunikációs rendszerek léte elengedhetetlen követelmény.

Ezek a rendszerek ritkán, speciális esetben kapcsolódnak, kapcsolódhatnak független szolgáltatói háttérhez, azaz többnyire szükséges a szigetüzem biztosítása. Jelenleg hazánkban még a legjobb megoldás erre digitális (DMR, TETRA) rendszerek alkalmazása. Ezeknél az üzemeknél nem megengedhető, hogy szabad sávon (WIFI) üzemelő berendezéseket alkalmazzanak, a kormányzati LTE megoldás pedig jelen kiépítettségében az MCPTT szolgáltatásra még nem alkalmas.

Szigetüzem tekintetében ígéretesnek tűnik a jelenleg hazánkban még nem elérhető Motorola Nitro készülékeinek a megjelenése, melyek támogatják az amerikai kontinensen használható egyénileg telepíthető LTE bázisállomások használatát. Gyakorlatilag ez a rendszer egy mobil eszközök számára kiépített vezeték nélküli hálózat, ami alkalmas az azt kezelni képes eszközök közötti adatátvitelre ezzel együtt természetesen az azon keresztüli beszédkommunikációra is. Ezekkel az eszközökkel kiépíti a szervezet a saját LTE szolgáltatását, egyedi működési frekvenciákon. Tervezhető teljesítménnyel, területi ellátottsággal – sajátkézben lévő központi menedzsmenttel, jobban skálázhatóan áll majd rendelkezésre mint a szolgáltatói LTE rendszerek – azaz a létesítésük komolyabb tervezési, szervezési, mérnöki munkát igényel.

Európában azonban jelenleg ilyen eszközök üzemeltetésére - használatára nincs meg a jogi háttér. Az LTE mint technológia a felhasznált sávszélességével és frekvenciatartományával együtt csak és kizárólag szolgáltatói célokra vehető igénybe – azaz pályázat útján elnyerhető frekvenciatartományokban telepíthetők ezek a berendezések.

Ennek a jogi akadálynak a megszűnésére jelenleg a hatóság nem lát lehetőséget.

Az általános kereskedelmi felhasználók szemszögéből

A kevésbé kritikus alkalmazások tekintetében a PoC technológia versenyképessége a jelenlegi DMR rendszerekkel szemben megkérdőjelezhetetlen. Műszaki, üzemeltetési szempontból a tervezési, hatósági ügyintézési költségek megszűnnek, sok esetben az egyéb-

ként is kiépített WIFI hálózatokat használhatja a rendszer, illetve kültéren a 3-4G hálózatokat (minimális adatfelhasználással). Saját szervert üzemeltetve, az adatkártyákat külön APN-be szervezve, esetleg VPN-t használva a biztonság is hatékonyan megoldható.

Problémát egyelőre a saját szerver témakörében látok. A PoC szerver szoftverek fejlesztői többnyire felhőben lévő szolgáltatásként kínálják a rendszereket, igénytől, felhasználástól függő díjcsomagokkal. Ebben az esetben a felhasználóknak tisztázniuk kell, hogy belső szabályozásuk szerint a rendszeren történő kommunikációk, beszélgetések kezelhetők, tárolhatók-e harmadik fél által.

A hardverrel együtt árusított szerver szoftver jó megoldásnak tűnik, azonban komolyabb cégeknél felmerül az informatikai rendszerbe integrálás alkalmával, hogy komoly biztonsági vizsgálaton szeretnék keresztülvinni az eszközöket. A friss név a piacon és a gyártók nem éppen rugalmas hozzáállása a kérdések megválaszolásához komoly akadályokat gördít a rendszer elterjedése elé.

Ezekben az esetekben a informatikai - szoftveres megoldásokat mellőző DMR rendszerek nyújthatnak megoldást. Várhatóan még jó pár évig.

ÖSSZEFOGLALÁS

A tanulmányban szereplő rendszerek vizsgálata után egyértelműen kimutatható hogy ezen a területen is jellemző az a technológiai konvergencia az informatikai technológiák irányában, mely az elektronikai műszaki területek minden ágazatát érintik.

Megjelentek a már digitálisan működő rádiórendszerek (DMR, TETRA, P25 stb.), ezeket követte a rendszerek összeköttetését biztosító hálózatok átültetése IP alapú hálózatra. A legújabb technológiákban már a csoportkommunikáció megvalósítása nem más, mint egy applikáció egy IP hálózatokon működni képes terminálon. Ennek professzionális és olcsó kereskedelmi megoldásai – melyek műszaki alapjai azonosak – lényegében abban különböznek, hogy a professzionális megoldásban az applikáció a készülék szoros része, míg a kereskedelmi kategóriájú készülékeknél egy általános operációs rendszerrel rendelkező (android, iOS, Windows mobile) mobil készülékre letölthető alkalmazás [15].

FELHASZNÁLT FORRÁSOK

[1] Dárdai Á.: „Mobil Távközlés, Mobil Internet”, Budapest: Mobil Ismeret Kiadó, 2003.
[2] Farkas T, Hronyecz E.: „The infocommunication system requirements and analysis of the communication of the deployable rapid diagnostic laboratory support „sampling group”” II. Academic and applied research in public management science XIV:(1) pp. 53-61, 2015.
[3] Mobile and Private Mobile Radio https://www.etsi.org/technologies-clusters/technologies/mobile-radio (Letöltve: 2020.09.10.)
[4] Baldini G., Karanasios S., Allen D., Vergari F.: „Survey of wireless communication technologies for public safety” IEEE Communications Surveys and Tutorials, 16 (2) ,art. no. 6599064 , pp. 619-641, 2014.

[5] ITU-R Radio Regulations, Section IV. Radio Stations and Systems – Article 1.25, p9 http://search.itu.int/history/HistoryDigitalCollectionDocLibrary/1.43.48.en.101.pdf (Letöltve: 2020.09.10.)
[6] Tetra and DMR Tier III: Which open standard digital trunking is right for me? Whitepaper http://www.criticalcommunicationsreview.com/ccr/document/download/95885/%7B:any?%7D (Letöltve: 2020.09.22.)
[7] Digital Mobile Radio Association https://www.dmrassociation.org/ (Letöltve: 2020.10.12.)
[8] ETSI TETRA – Introduction https://www.etsi.org/technologies-clusters/technologies/tetra (Letöltve: 2020.10.12.)
[9] Mission Critical Services in 3GPP http://www.3gpp.org/NEWS-EVENTS/3GPP-NEWS/1875-MC_SERVICES (Letöltve: 2020.11.04.)
[10] Broadband Push To Talk (PTT) Services https://www.motorolasolutions.com/en_us/products/command-center-software/broadband-ptt-and-lmr-interoperability.html (Letöltve: 2020.11.05.)
[11] MCOP releases the source code for MCPTT apps and SDK http://www.criticalcomms.com/news/mcop-source-code-mcptt-sdk (Letöltve: 2020.11.08.)
[12] ProPTT2 - World First PTT App without PTT button, ProPTT2 Embedded https://www.proptt2.com/en/index.html (Letöltve: 2020.12.01.)
[13] Peak PTT Platform Solutions – Everest PTT system https://www.peakptt.com/collections/all?page=1 (Letöltve: 2020.12.01.)
[14] A. Albini, D. Tokody, Z. Rajnai.: „Theoretical Study of Cloud Technologies" Interdisciplinary description of complex systems 17: 3A pp. 511-519. , 9 p, 2019.
[15] Broadband Push-to –X https://urgentcomm.com/2019/03/21/motorola-solutions-michael-doerk-highlights-new-poc-interop-offering-features-on-roadmap-to-mcptt/ (Letöltve: 2020.12.01.)

THE EXPERIENCES OF RUNNING "ADVANCED TECHNICAL ENGLISH" COURSES FOR ENGINEERING STUDENTS AT DONÁT BÁNKI FACULTY OF MECHANICAL AND SAFETY ENGINEERING, ÓBUDA UNIVERSITY

A MÉRNÖK HALLGATÓK „FELSŐFOKÚ MŰSZAKI ANGOL" TANTÁRGYÁNAK OKTATÁSI TAPASZTALATAI AZ ÓBUDAI EGYETEM BÁNKI DONÁT GÉPÉSZ ÉS BIZTONSÁGTECHNIKAI MÉRNÖKI KARÁN

KOVÁCS Éva[1]

Abstract

This article aims to elaborate on the process of course design, material development, course implementation, student feedback and evaluation to provide recommendations for the planning of future ESP[2] courses dedicated to engineering and technical students with a high command of English in tertiary education. Courses bearing the name *'Advanced Technical English*' were run between 2015 and 2016 over two consecutive academic years at Donát Bánki Faculty of Mechanical and Safety Engineering. For the purpose of further future development, both theoretical and practical, it also lays down the fundamental elements of Mission-Oriented Preparation (MOP).

Keywords

course design, ESP, language examination preparation, Technical English, impact

Absztrakt

Jelen cikk megírásával az a célom, hogy részletesen bemutassam a kurzustervezés, tananyagfejlesztés, tantárgy végrehajtás, hallgatói visszajelzés és értékelés folyamatát. Ez ahhoz szükséges, hogy javaslatokat fogalmazzak meg az angol nyelvet magas szinten bíró műszaki- és mérnökhallgatók számára a jövőben kidolgozandó angol nyelvű műszaki szaknyelvi képzés tervezéséhez a felsőoktatásban. A "Felsőfokú műszaki angol" nevet viselő tantárgy oktatása az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Karán két egymást követő tanévben, 2015-ben és 2016-ban zajlott. A jövőbeli továbbfejlesztés, elméleti és gyakorlati kidolgozás érdekében lefektetem a Feladatorientált Felkészítés koncepciójának néhány meghatározó alappillérét, amelyet elsőként itt teszek meg.

Kulcsszavak

kurzustervezés, szaknyelv, nyelvvizsgafelkészítés, műszaki angol, visszahatás

[1] kovacs.eva1@uni-obuda.hu | ORCID: 0000-0003-3295-9243 | ESP teacher/angol szaknyelv oktató | Nemzeti Közszolgálati Egyetem, Rendészettudományi Kar, Idegennyelvi és Szaknyelvi Lektorátus

[2] English for Special Purposes

INTRODUCTION

Óbuda University is a "dynamic and thriving institution" [1] with its focus on training students primarily in technical, engineering and business studies. 140 years old in 2019, the integrated university consists of six faculties, one central and three doctoral schools, offering training in all three cycles of EHEA[3], thus covering the full spectrum of higher education at bachelor, master and doctoral level, training both domestic and international students. (Students from the European Union come through the Erasmus Programme, while the state-financed Stipendium Hungaricum brings students mainly from Asia, South America and the Middle East.) Since the official terminology and technical language skills have been tested within a framework of accredited technical language examinations for decades in Hungary, the need to provide students with a suitable language examination preparatory to training naturally arose.

Having looked into the two available accredited Technical English language examinations [2], [3] and the current curriculum at Óbuda University and other engineer training institutions, it was clear that an existing gap occurred between the option to attain a certificate for Technical English language skills and the overall absence of a tailor-made language examination course at university level. This design began in the spring semester of 2016, and after working through the official forums of the university's relevant decision-making boards, a course under the name "Advanced Technical English" was introduced into the curriculum of the University. The significance of this is not just relevant for the provision of a high-level language learning option. The application of the acquired new language skills is more and more apparent in the changing industrial environment. [4]

GENERAL LEGAL REQUIREMENTS OF LANGUAGE EXAMINATIONS TODAY IN TERTIARY EDUCATION

Firstly, let me elaborate on the legislation regulating secondary school leavers' university admission. According to a government decree passed in December 2014, as of the beginning of the 2020/21 academic year, only applicants having obtained a level B2 complex language examination may submit their applications for any university major at bachelor level, in any training form (regular, correspondence, distance learning) [5]. Therefore, the law provided a six-year long 'breathing space' for students, secondary schools and teachers before the introduction of this measure.

Before the regulation became effective, pressure from student government organizations, professional language teaching associations and parents had mounted on the educational department and the government. [6] In fear of losing approximately half of potential university students from September 2020, the government issued a new decree which annulled the B2 level language examination prerequisite as an admission criterion for any tertiary educational institution. [7].

Secondly, regulations on the attainment of diplomas and degrees in tertiary education needed to be discussed. Previously, output requirements to obtain any bachelor or master's qualifications had been tied to the attainment of a level B2 complex language exami-

[3] European Higher Education Area

nation. [8] Controversies in Hungarian society have since lined the path of language learning and examination preparation, leaving thousands of graduates without a recognised diploma at the end of their studies in higher education. [9]

Although government funding was provided for programs to redeem unawarded degrees due to the lack of language examinations, figures demonstrate that they have only scratched the surface of the problem. Only a small portion of the previously unawarded degrees could be redeemed with a successful B2 examination result after the completion of the state-financed language learning course. [10] The sheer presence of an official prerequisite for the attainment of a degree in higher education has been looked into with a broader international overview, bringing about further discussions in relevant professional and social forums, where the conclusion often points to prior insufficient language teaching conditions. [11] It is also important to note that certain majors, in Hungary, create extra output requirements for qualification. Some of them (e.g. technical military training) demand specialized professional language examinations, others bind the attainment of a degree to general language tests in more than one language. [12]

The Hungarian government recently issued a new decree concerning unawarded degrees and output level B2 language examination requirements. This was done within the framework of emergency legislation amid COVID-19 protection as part of a series of measures. The decree was published on 10 April 2020. In a two-line paragraph, all students having passed their final state examination before 31 August 2020 must be exempt from the requirement to obtain a complex language examination pass. [13]

Having demonstrated the inadequacy of legislation governing input and output requirements with regard to obtaining a language examination certificate, it becomes clear how it all exemplifies the effects of testing at various levels. Compulsory nation-wide testing falls under the category of *impact*, as described by Shohamy. [14] Both their enormous *educational* and *social impact* may be observed. Because of their mandatory nature, these tests are highly important, which causes all test candidates, students and teachers alike to alter their attitude towards the learning and teaching process. As well as modifying the participants' behaviour, the arbitrary alternation between retaining and abolishing language test-bound admission and graduation preconditions on the government's part seem to exert a disproportional influence on a social scale. The number of applicants to tertiary education institutions hit an alarmingly low level in 2020, with only 91460 candidates having filed applications. [15] Further extended studies into its many potential causes must be conducted, yet the obvious link between these issues have been voiced by the representatives of the language teaching profession and the press. [16], [17]

Taking all the legal steps and this controversy into consideration, it is obvious that terminating the examination-bound obligation that kept higher education students studying languages even after leaving formal tertiary education will, sadly, discourage students from acquiring General English skills. Retaining the mandatory requirement after the said date will maintain the interest in and need for continuous provision of language teaching at university level. This must be strengthened to offer sufficient language learning options for the large number of high-school leavers who will continue to begin their further tuition lacking a proper high level examination in any major language.

THE REASONS FOR PREFERRING ESP TO GENERAL ENGLISH

Generally speaking, nearly half of the candidates admitted to universities in Hungary obtained a level B2 complex examination acceptable as a requirement for finishing their studies with a suitable certificate in recent years. [18] To investigate the specific situation at Donát Bánki Faculty of Mechanical and Safety Engineering, I have gathered data from the Registrar's Office.

	Number of students				Proportion of students [%]			
Year	**N1**	**N2**	**N3**	**N4**	**P1**	**P2**	**P3**	**P4**
2019	381	313	54	14	100	82,15	14,17	3,67
2018	419	339	66	14	100	80,91	15,75	3,34
2017	371	288	59	24	100	77,63	15,90	6,47

1. Table: Students with a final examination at BSc level (self-editing)

N1: Number of all students taking their final examination
N2: Number of students immediately receiving their diplomas holding a language certificate
N3: Number of students redeeming their diplomas with a delay filing their language examination certificates at a later date
N4: Number of students not having received their diplomas with a language certificate, though diplomas are to be granted after the government decree on language examinations
P1: Proportion of all students taking their final examination
P2: Proportion of students immediately receiving their diplomas holding a language certificate
P3: Proportion of students redeeming their diplomas with a delay filing their language examination certificates at a later date
P4: Proportion of students not having received their diplomas with a language certificate, though diplomas are to be granted after the government decree without a language examination

	Number of students		Proportion of students [%]
Year	**N1**	**N2**	**P**
2019	533	326	61,16
2018	643	432	67,19

2. Table: All students admitted and enrolled for BSc program (self-editing)

N1: Number of students admitted and enrolled for BSc programs
N2: Number of students holding a B2 English or German language examination at the time of admission
P: Proportion of students admitted and enrolled for BSc programs holding a B2 English or German language examination at the time of admission

General language teaching at tertiary level must not ignore but should target the considerable proportion (38-33%) of students not holding a B2 certificate at the threshold

of university entry. As in many other institutions, Óbuda University addresses the problem of language learning during formal tertiary studies in many different forms.

As part of the Ágoston Trefort Centre for Engineering Education, general language learning is provided in the curriculum in three languages: English, German and Russian. To cater for the basic needs, that is, students without a B2 examination, the Centre offers courses for beginners, pre-intermediate and intermediate learners with the ultimate aim, at the end of their courses, for students to have an examination pass. A lack of applicants may prevent a course from starting.[19] As I have explained above, general purpose language learning needs are addressed and student expectations are fulfilled through the courses run at Óbuda University.

The success of language learning at tertiary level does not only depend on officially provided in-house tuition. Extra-institutional, private and autonomous learning must also contribute to the final tangible requirement. With all these efforts, roughly 80 per cent of students are able to graduate and obtain their degrees by the end of the seven semester-long BSc program, as the figures cited above demonstrate, along with a year-on-year improvement in numbers. This means, that the 33-38 per cent gap at the entrance point is reduced to approximately 20 per cent at the exit. The judgement on this, whether it is a failure or success may be looked at later and in detail at all possible levels – institutional and national. However, the numerous and particularly the most recent governmental interventions through the law and regulations described earlier suggest that it is a situation which is far from being acceptable at a national level.

In my view, professional language teaching capacity at tertiary educational level must not be overwhelmed trying to tackle the problem of unattained intermediate language examinations. On the contrary, courses and professional teachers must focus on specific language teaching pertaining to the profile of the faculty and subsequent job needs. This was the reason why my attention has been focussed towards offering ESP courses at this institution.

THE MISSION OF ADVANCED TECHNICAL ENGLISH

To provide a meaningful and content-laden course for engineering students at Óbuda University, I had to take into consideration the various faculties and majors the institution offers. Mechanical engineering, safety engineering, economics, business and management studies are available in the two faculties on the premises on Népszínház Street, where I expected most students to enrol, however, as later occurred, information technology and electric engineering students also participated in the course from more distant campuses. All students completing either their bachelor or master training had to be accommodated. This meant that the course needed to be attractive to virtually the whole student population.

Administrative incentives were assigned to the completion of the subject, which in practice meant 3 credit values. After its second semester it was also made one of the criterion subjects, an English-language elective course, making it even more worth taking.

Since the elective course targeted the training of any engineering student, irrespective of their faculty, whether they were in their bachelor’s or master’s training stage, there

was a minimum entry criterion for the course. The decisive factor, to draw the line of admission, was the holding of a level B2 complex English language examination or its equivalent knowledge. This ensured the target level C1 - advanced language skills could be attained even from an intermediate or upper-intermediate plateau. 'In addition to this core vocabulary, there are another 1,000 or so words common to academic disciplines, sometimes referred to as the basis for an academic vocabulary. However, once learners reach the intermediate level, they often fail to make sufficient gains in their knowledge of vocabulary'. [20] The course took on the mission to overcome this barrier with this purpose in mind. Enriching the scope of academic terms with 1,000 or so relevant engineering vocabulary items may make a significant difference in language skills, enabling them to attempt and successfully pass an advanced complex language test.

THE PROCESS OF COURSE DESIGN

Attaining advanced language skills in a specific academic field presumes general higher-level thinking skills. In Bloom's taxonomy the latter are summarized in *analysing, evaluating* and *creating* stages in the order of thinking skills, which are further refined in sub-categories. [21] In a most recently revised new taxonomy, Marzano and Kendall set up and named the last three stages as *knowledge-utilization, metacognition,* and *self-system thinking.* [22] For learners to activate these high level thinking skills in the target language, they need to be exposed to a construct that is of high complexity regarding both its lexical and grammatical content and a methodology of instruction that is both challenging and varied.

With that in mind, when developing the course curriculum, I was forced to take into consideration the level of knowledge and skills description of the Common European Framework of Reference (CERF) for C1 level. Hungary as a European Union member state applies the CERF levels and criteria in its language testing. Even though high-stakes language testing has been widely reflected on and is constantly a subject of criticism by renowned academics of the field, [23] we have to be conscious of the backwash effect that Hungarian language examinations based on CERF descriptions exert on classroom procedures and learning and teaching processes. In the case of *Advanced Technical English,* the pressing compulsory nature of test taking has been diminished. One reason is that the course was chosen to be elective. Another is that, despite the availability of the two technical ESP examinations, Óbuda University does not compel their students to take advanced level examinations, neither at GE, nor at an ESP type as an output requirement. The course may not do that either, however, giving encouragement, ample preparation and recommendation, the option to enrol and pass a C1 test was realistic upon finishing the semester. The course objective, which was the first element of course design, was worded so that students see this opportunity as a potential benefit in the job market:

'The course objective is the preparation in fulfilling the requirements of both oral and written Technical English examination at level C1 that is accredited in Hungary. By improving their receptive, productive and mediation skills, not only will the course enable students to successfully pass a specified technical language examination at an advanced level, but it will also provide them with a competitive advantage in the labour market, since the course will be enriched with business and technical vocabulary based on students' needs.'

My assumption that this was sufficient to appeal to students such that they would enrol on the course was confirmed by the influx of applicants. The number of students immediately filling the available places, through online registration, within hours of enrolment opening.

The next step in course design was the in-depth study and analysis of the program, topics, tasks and officially provided online and paper-based test material by the two language examination centres offering the advanced technical language test. As for *BMEnyelvvizsga* (Language Centre at Budapest University of Technology and Economics), at the time of the course design, ESP language tests both in technology and economics were offered in a bilingual version. Hungarian used to be involved in testing. As in the case of many other language tests, oral and writing skills may be examined separately or in a complex way, but only in the written part was mediation as a separate skill embraced. At the oral part at *BMEnyelvvizsga*, there was an active performance test in front of a two-member committee with one candidate at a time as a form of oral interview with three task types: a personal and professional introduction, discussion of a topic prompted by a visual input and finally an argumentative presentation with a 5-minute preparation time allotted. At the listening test, two audio texts of various genres are provided coupled with note-taking and true/false statement task types. The written test included two reading tasks to measure global comprehension and elicit specific data in the task format of paragraph and paragraph heading matching. The other reading task was an integrated one with mediation, since it required a summary of an English text on a technical topic of approximately 1000 words in Hungarian. Two tasks to test and measure writing skills incorporated the format of formal letter writing on a technical or business problem, and a guided argumentative written essay based on a given title to be debated. Last but not least, three Use of English tasks completed the written part with the tasks of sentence transformation, cloze test and text completion with four content-word multiple-choice options. It must be noted here that since the running of the course, the language centre for *BMEnyelvvizsga* has transformed all of its ESP tests from bilingual to mono-lingual, which means that mediation as a skill to be tested formerly has been removed in favour of more monolingual tasks.

As far as the other domestically available technical language examination is concerned, *Zöld Út Nyelvvizsga* (Green Path Language Examination), operated by Szent István University, also used to include testing mediation skills in its earlier available form. The task assigned to the skill was placed in the written part, candidates had to summarize a one-page long text in Hungarian into English on a technical topic. With later modifications to the test, this part has also been eliminated, thus transforming the examination into a monolingual type. Reading skills are tested through two lengthy texts with two tasks assigned to each text, with various reading task types, such as information-gap filling, note-taking, matching paragraph headings. Writing skills are examined through two tasks, mandating candidates to compose a written analysis of a table or chart provided. The other task is a guided composition in the genre of a reader’s letter to the editor of a professional newspaper on a given technical topic. As part of the oral test, listening comprehension is tested by audio news samples with true/false statements and a lengthier and more complex spoken explanation of a technical problem, with an information-gap exercise attached. The speaking part, in form of a two-member committee involves two dialogues and one monologue.

The first dialogue is an introductory one related to a technical topic, a list being given on the official website. [24] What is very special about the speaking test routine is the presentation task and its preparation. Three weeks prior to the date of the speaking test, candidates are asked to submit an official form, in which they must send the draft and three reliable sources of three different presentations on a certain technical topic. At the examination, they are made to draw one title out of the three, after which they must deliver an 8-minute talk. Following this, candidates are asked questions and debate with the examiner.

While *Advanced Technical English* courses were running, the two language centres made their ESP tests in English available in their May and November examination periods. This meant that both in the spring and autumn semesters there was one available technical examination to take for those students who were interested. In my preliminary inquiries at the outset of each course, together with needs analysis in writing, I asked students for the reasons they took the elective course and their expectations from it, in an informal, open classroom discussion. Amongst these general reasons were foreign language improvement and an interest in the technical topics in the syllabus. There were typically three students of the maximum 15 allowed per course that showed interest in applying for the C1 examination. After the in-depth study, the task types and skills testing, I needed to design the course in such a way that it would grant sufficient time for in-class development and home practice of all the tested skills and task types at the examination detailed above. This is represented in the course syllabus as follows:

'Syllabus: Discussion of the most typical technical language examination topics on a weekly basis in the form of individual topic preparation, presentations, situational and simulation tasks and debates. Revision of grammatical structures combined with a refined vocabulary and set of idiomatic expressions incorporated into and active in oral and written productive tasks. Task-based approach to examinations: the introduction and practice in at least one oral or written task-type on a weekly basis.'

In practice, the two weekly contact lessons with three 45-minute sessions at a time gave ample opportunity to introduce and practice C1 examination task types in parallel with continuous skills development. Optional extra oral and written exercises were provided for students committed to applying for the technical language test. This also meant individual tutoring and consultation for the instructor and the student.

We should not overlook the evident backwash effect which preparation for a language test in itself entails. [25] On the one hand, by labelling the course 'exam-preparatory' in the academic registration system, I intended to capitalize on the obvious high prestige of language examinations both in the Hungarian educational system and in society. It was evident that the opportunity and potential output of the course in test-taking would draw students, since they felt that they might receive an official certificate, even if it was not a compulsory requirement. In our document-centred society, it is something which is not to be neglected, even though the majority of students are interested in gaining presently applicable and real-life knowledge. In case of other technolects, such as English for law enforcement, the practical application of this has also been highlighted. [26] Explicitly described by academics as '*impact'* [27], high-stakes language tests exert such an influence in society that it may be detrimental to minorities and impaired social groups. Unless high-stakes language tests are continually supervised and classroom procedures adopt the most advanced

learning and teaching methods, the teaching and learning activities may easily decline to a mere 'teaching to the test' and 'learning to the test'. [28]

Evidence to demonstrate the adverse and unintended effects of such preparation is amply provided by scholars. [29] To avoid this, in classroom activities, examination material should be used in way that it should create no pressure on the student. One visual 'trick' was the eradication of the official reference to examination centres on paper-based and online material. Therefore, students did not have the sense that what they were dealing with was preparatory material coming directly from the language centres. Another method was the leisurely pace and the lack of time constraints during in-class tasks. The aim was meticulous discussion and an indulgence in detail, therefore, only when students gained more practice and confidence with task types and their applicable learning and solution strategies could procedures be accelerated. Precise time based task solutions on both test parts were measured in case the students needed to apply to take the examination.

MATERIAL DEVELOPMENT AND TEACHING STRATEGIES

Regarding the technical ESP nature of the preparatory course, high student expectations were expressed for cutting-edge content at the beginning of the semesters, manifested in written needs analyses and informal conversations with the tutors. The material that comprised 'trait', [30] that is *what* to teach, had to fulfil several requirements. First and foremost, it reflected the majority of the oral topics listed online on the websites of the language centres. By touching upon the topics at C1 level oral examination, it was guaranteed that during the 14-week long semester, students gained an overall insight of the most relevant technical issues. The weekly plan of the syllabus with its theme deployment was as follows:

- automation
- ergonomics, environmental issues
- energy
- virtual reality
- communication, computers
- space research
- quality or quantity
- safety technology
- transportation
- from wheels to space shuttles
- auto industry
- recycling

Recognizing students' interests and the end-of-the-course feedback, one or two topics were replaced per semester taking into consideration students' wishes, thus allowing classroom time for special individual and group interests. These included artificial intelligence or welding technologies for instance.

Secondly, as regards the availability of the course material, various sources had to be incorporated. I obtained all the official paper-based and Internet-based publications issued by the language examination centres themselves. [31] Limited resources allowed only

a test sample on both of the websites and a practice booklet issued by *BMEnyelvvizsga*. The lack of such material urged me to seek other technical or engineering textbooks designed for ESP classrooms and learning. [32] Only after thorough content-revision did I select units or sub-topics that could be incorporated as material for the lessons, naturally, with necessary modifications, additionally designed exercises or omissions. Besides engineering ESP textbooks, I also revisited advanced level course books and language examination preparatory test booklets in General English, searching for special technical themes that would incidentally be featured in them, with exercises ready for classroom use. [33]

Finally, the most important material to be used was always the up-to-date topics sourced from recent online publications. This meant the application of at least one topical issue per weekly theme. Any online material featured in the lessons went through a process of material design, where the length of texts, video or audio were cut, edited and received individually tailored exercises to fulfil the purposes of advanced skills practice that included mediation, reading, writing, listening and speaking. [34], [35] Skills practice was in accordance with the task format of the model exercises provided by the test centres. Undoubtedly, the latter part of the process of course material development, which fundamentally requires a rigorous and systematic approach, [36] is the most challenging and responsible aspect for any ESP teacher.

Along with vocabulary and skills improvement, the course took on the important mission to elevate students' structural awareness and level of understanding in the target language. Therefore, lessons embraced grammatical revision as well. The selection of structures to be included had previously been carried out. Looking through a number of advanced level General English course books, [37] the preferred grammatical topics were those that are complex and sufficiently refined for that level, thus receiving less attention in teaching English at lower levels. Also, these are the structures that are more frequently used in academic environment. Advanced structures featured in class were

- passive forms,
- reduced relative clauses,
- noun clauses,
- gradable and non-gradable adjectives,
- modals with perfect infinitives,
- conditional base and mixed types with alternatives to *'if'*,
- past tenses for hypothetical meaning,
- patterns after reporting verbs,
- gerunds and infinitives as verb compliment,
- using fronting for emphasis.

As for teaching structures, the challenge of linking the vocabulary to the topical technical content was unavoidable. Besides turning to readily available high-level English grammar exercises, teachers also had to compose structural drills and exercises of their own to suit the actual learning needs and the ESP content. Additional drills were provided at the students' request and for those who had some weakness in the field. Correction and feedback were offered individually in form of a tutorial.

During the implementation of subsequent courses, several teaching strategies were adopted. As a result of its popularity, the number of participants necessitated that two

courses be operated simultaneously. Inviting more colleagues to teach *Advanced Technical English* was done with the emphasis on an ESP teaching background. Sharing the *trait* ensured mutual compliance with the syllabus. Naturally, all four colleagues taking part in teaching *Advanced Technical Englis*h enjoyed the liberty in utilizing various teaching approaches, strategies and methodology. With a maximum number of 15 participants, students were allowed to work in various groupings during the lessons: with chosen or randomly assigned pairs for special tasks or for the whole duration of a lesson. Group work was facilitated by more complex and time-consuming exercises. There were lesson-length projects assigned to teams of students, when they had to come up with a common project product, for instance, designing a trade fair stall. Preparing for and giving a presentation was a major part of oral language test training. Therefore, students took on the task individually or working in pairs, making a final oral contribution enhanced with visual aids. They received feedback from both fellow students and the teacher with suggestions for further improvement. Classroom teaching procedures influenced student behaviour outside the classroom, where they prepared in cooperation with others, shared common knowledge through informal online channels and applied forms of autonomous learning, demonstrating their abilities to organize their studies independently. [38]

To conclude, the material development for this specially designed course was a momentous piece of work prior to and during its operation. Although the syllabus and structure remained, its content was constantly updated and renewed. This was crucial for several reasons. On the one hand, the technical nature of the ESP course calls for maintaining the pace alongside rapid technological development, affecting the content to be put on the table. On the other hand, students had ample opportunity to satisfy their own interests and needs, which also prompted greater resilience on the teachers' part. Finally, examination preparation was decisive in both task selection and the application of the various teaching and learning strategies.

STUDENTS' FEEDBACK AND CONCLUSION

The experience of running *Advanced Technical English,* an examination-preparatory course of ESP at Óbuda University, has highlighted considerable implications for the future of ESP teaching. Students were asked to give anonymous written feedback at the end of each course. They were requested to name both favourable and unfavourable elements and experiences they had over their semester-long involvement in the course. Unlike the generalized course feedback available in the online university registration questionnaire, students were asked to compose their own ideas, therefore, the answers I received were far less cliché ridden. On the contrary, the course feedback sheets mirrored the most important and urgent ideas students had to reflect about their complex experience of the classroom procedure, teaching and learning process they underwent. Among the positive things they mentioned were the colourful material and general devoted teaching attitude, the possibility to prepare for a level C1 technical examination and the opportunity to upgrade their overall language skill to match their requirements. However, a number of students expressed their wish to learn more specialist vocabulary and topics pertaining to their studies, the major that they have chosen and the future profession they are about to pursue after graduation. Such expectations point beyond the original purpose of *Advanced Technical English*. Even

so, the ideas students worded expressed their immediate need for the kind of English they would most willingly learn at university level and that undoubtedly points towards more field-specific language use.

RECOMMENDATIONS FOR FUTURE ESP COURSES: MISSION-ORIENTED PREPARATION

Capitalizing on students' calls for more field-specific language knowledge, I have devised the foundations of a teaching concept that I wish to elaborate in more detail in its theory and practice. I named it '*Mission-Oriented Preparation' (MOP)*. It comprises common knowledge and experience in ESP teaching, ushering in more innovative changes in classroom procedures, teaching and learning processes.

Mission-Oriented Preparation commences with defining a mission for a learner that will govern the whole learning process. Students must articulate and proclaim their immediate short-term and mid-term goals of their language learning. To achieve these goals, the teaching and learning processes must be conducted in close cooperation with the teachers, tutors in the field the student studies, including future job market representatives and potential employers in the area. Cooperative course design and implementation is an essential element of MOP, where the participants of certain domains collaborate in order to map and develop students' general professional abilities and English language synchronically. (The use of similar methods of needs analysis for ESP course design, involving non-linguist domain experts is on the increase in a number of professional fields [39], [40].) With regard to diverse student ambitions, MOP intends to focus both on English for Academic Purposes (EAP) and English for Vocational Purposes (EVP). However, especially in the case of EVP, courses may operate to embrace students with a wider scale of language proficiency, including lower level speakers to motivate learning professional English and a prompt application of the language. MOP is also characterised by taking advantage of various modern teaching and learning approaches, such as using the Café method, [41] portfolio assessment, dynamic assessment, cognitive assessment or autonomous learning, since the experts of such methods generally call for more empirical gain. [42] In future course designs and implementations, *Mission-Oriented Preparation* will be further refined in both theory and practise.

REFERENCES

[1] http://uni-obuda.hu/en/university, accessed: 8 August 2020
[2] http://www.bmenyelvvizsga.bme.hu/hu/muszaki_egynyelvu/nyelvvizsgak, accessed: 20 May 2019
[3] https://zoldut.szie.hu/nyelvvizsgarol, accessed: 8 August 2020
[4] FREGAN, B; KOCSIS, I; RAJNAI, Z: Risks of Industry 4.0 and Digitization, MŰSZAKI TUDOMÁNYOS KÖZLEMÉNYEK (EN) 9 : 1 pp. 87-90. , 4 p. (2018)
[5] A Kormány 335/2014. (XII. 18.) Korm. rendelete a felsőoktatási felvételi eljárásról szóló 423/2012. (XII. 29.) Korm. rendelet módosításáról, 10. § (2) b)
[6] https://eduline.hu/erettsegi_felveteli/20191105_kotelezo_nyelvvizsga, accessed: 20 May 2020

[7] A Kormány 261/2019. (XI. 14.) Korm. rendelete a felsőoktatási felvételi eljárással összefüggésben egyes kormányrendeletek módosításáról, 1/1. §
[8] Az alap- és mesterképzési szakok képzési és kimeneti követelményeiről szóló 15/2006. (IV. 3.) OM rendelet. 2. sz melléklet
[9] http://eduline.hu/nyelvtanulas/nyelvvizsga_nelkul_diploma_0TEAGV, accessed: 8 August 2020
[10] http://eduline.hu/nyelvtanulas/Diplomamento_program_eredmenyek_LEAB03, accessed: 8 August 2020
[11] https://www.nyest.hu/hirek/kell-e-nyelvvizsga-a-diplomahoz, accessed: 8 August 2020
[12] FREGÁN, B: Un établissement européen au service de la défense In: Fregan, Beatrix (szerk.) Success and Challenges in Foreign Language Teaching : International Conference for Language Instructors, Budapest, Magyarország : Nemzeti Közszolgálati Egyetem, (2014) pp. 83-87. , 5 p.
[13] A Kormány 101/2020. (IV. 10.) Korm. rendelete a veszélyhelyzet során teendő egyes, a felsőoktatási intézményeket és a hallgatókat érintő intézkedésekről, 6. §
[14] SHOHAMY, E.: Critical Language Testing In: Shohamy, E, Iair G. Or; May, S (ed.) Language Testing and Assessment, Encyclopedia of Language and Education, Springer, 2017, p. 445.
[15] https://www.felvi.hu/felveteli/ponthatarok_statisztikak/friss_statisztikak/!FrissStatisztikak/index.php/friss_statisztikak/, accessed: 11 June 2020
[16] https://24.hu/belfold/2018/09/01/nyelvvizsga-felsooktatas/, accessed: 10 June 2020
[17] https://magyarhang.org/belfold/2019/07/13/kotelezo-nyelvvizsga-2020-ban-oszeomolhat-a-felsooktatas/, accessed: 11 June 2020
[18] https://nyak.oh.gov.hu/doc/statisztika.asp?strId=_491, accessed: 10 June 2020
[19] http://tmpk.uni-obuda.hu/letoltes/nyelvi-kepzes-az-obudai-egyetemen-2018-tol-2018-01-16.pdf, accessed: 11 June 2020
[20] RICHARDS, J. C.: Moving Beyond the Plateau From Intermediate to Advanced Levels in Language Learning, Cambridge English Research and Methodology, New York, 2008
[21] BLOOM, B.: Taxonomy of Educational Objectives: The Classification of Educational Goals, Longmans, Green and Co, New York, 1956
[22] MARZANO, R. J., KENDALL, J.C.: The New Taxonomy of Educational Objectives, Corwin Press, Thousand Oaks, 2007
[23] MENKEN, K.: High-Stakes Tests as De Facto Language Education Policies In: Shohamy, E, Iair G. Or; May, S (ed.) Language Testing and Assessment, Encyclopedia of Language and Education, Springer, 2017, pp. 385-397
[24] https://zoldut.szie.hu/temakorok, accessed: 16 July, 2020
[25] TSAGARI, D., CHENG, L.: Washback, Impact and Consequences Revisited In: Shohamy, E, Iair G. Or; May, S (ed.) Language Testing and Assessment, Encyclopedia of Language and Education, Springer, 2017, pp. 359-372
[26] ÜRMÖSNÉ SIMON, G., BARNUCZ,N.: Az Idegennyelvi és Szaknyelvi Lektorátus múltbeli, és jelenlegi tevékenységei, valamint a jövő perspektívája In: Porta Lingua. 2020
[27] WALL, D.: The Impact of High-Stakes Examinations on Classroom Teaching: A

case study using insights from testing and innovation theory (Studies in Language Testing), Cambridge University Press, 2006
[28] MENKEN, K.: High-Stakes Tests as De Facto Language Education Policies In: Shohamy, E, Iair G. Or; May, S (ed.) Language Testing and Assessment, Encyclopedia of Language and Education, Springer, 2017, p. 389.
[29] ELDER, C.: Language Assessment in Higher Education In: Shohamy, E, Iair G. Or; May, S (ed.) Language Testing and Assessment, Encyclopedia of Language and Education, Springer, 2017, p. 276.
[30] SHOHAMY, E., OR, I. G.: Volume Editors' Introduction to "Language Testing and Assessment" In: Shohamy, E, Iair G. Or; May, S (ed.) Language Testing and Assessment, Encyclopedia of Language and Education, Springer, 2017, p.x.
[31] Műszaki Mintafeladatsor Angol Felsőfok, BME Nyelvvizsgaközpont, 2010.
[32] IBBOTSON, M.: Cambridge English for Engineering, Cambridge University Press, 2008
[33]HORVÁTH, M., ZSIGMOND I., Nagy Origo Nyelvvizsgakönyv Angol Felsőfok, Lexika Kiadó, Székesfehérvár, 2018.
[34] BARNUCZ, N.: IKT eszközök szerepe az angol nyelv oktatásában. Educatio, Vol. 28. No. 2. pp. 403–414.
[35] BARNUCZ, N.: IKT-eszközökkel Támogatott (Rendészeti) Nyelvoktatás. Magyar Rendészet, Vol. 19. No. 4. pp. 15–31.
[36] Nagy, G. Towards intercultural competence: a model-based framework for improving ESOL learners' cultural content knowledge. In F. Mishan (Ed.), ESOL Provision in the UK and Ireland, 2019. pp. 341-360.
[37] BELL, J., GOWER, R., HYDE, D.: Advanced Expert CAE Coursebook, Pearson Longman, 2008
[38] ASZTALOS, R., SZÉNICH, A., CSIZÉR, K.: Foreign language teaching and autonomous language learning: an overview and innovative practices in Hungary In: Ludwig, Christian; Tassinari, Giovanna; Mynard, Jo (ed.) Navigating foreign language learner autonomy, Hong Kong, Kína : Candlin & Mynard ePublishing, 2020 pp. 280-297. ,
[39] Judit Borszéki: The Definition of Specific-Purpose English Language Competences Needed in Border Control and Their Development Potentials, II. English for Border and Coast Guards: Specific-Purpose English Language Skills and the FRONTEX Tools Designed for their Development – Level A2/B1. Magyar Rendészet, 2018/5
[40] Judit Borszéki: Az English for Border and Coast Guards című nemzetközi szaknyelvi oktatóanyag fejlesztésének folyamata – a nem-nyelvész szakemberek szerepe. In: PORTA LINGUA 2020: Szaknyelvoktatás és –kutatás nemzetközi kontextusban Budapest, SZOKOE 2020
[41] MOLNÁR, K., URICSKA, E.: A Café módszer alkalmazásának tapasztalatai a rendészeti felsőoktatásban, Budapest, 2019, Magyar Rendészet. 19/4, pp. 69–80.
[42] Fox, J.: Using Portfolios for Assessment/Alternative Assessment In: Shohamy, E, Iair G. Or; May, S (ed.) Language Testing and Assessment, Encyclopedia of Language and Education, Springer, 2017, pp. 135-144.

EMPIRICAL ANALYSIS OF THE INFORMATION SECURITY CHARACTERISTICS IN THE HUNGARIAN BUSINESS ORGANIZATIONS

A MAGYARORSZÁGI GAZDÁLKODÓ SZERVEZETEK INFORMÁCIÓBIZTONSÁGI JELLEMZŐINEK EMPIRIKUS ELEMZÉSE

HORVÁTH Ádám Béla[1]

Abstract

This publication is based on a questionnaire survey conducted in 2019-2020 among Hungarian for-profit organizations. 498 respondents participated in this research, 99% of them can be considered small or medium-sized enterprises. The sub-research examines the question of whether information security incidents are indeed discrete events, or whether the (Bayesian) stochastic relationship can be between them statistically confirmed. One sub-question of this research, if the compliance issues can be perceived as a security incident. The research also confirms the fact that systemic and non-systematic risks can be identified among IT risks, similarly to the financial world, thus sophisticate the previous picture of operational risks. One of the unexpected results of the research is that countermeasures against certain risks may indeed reduce the probability of a given risk occurring, but in the case of other risks it has the exact opposite effect: it increases the chances of the risk realisation.

Keywords

Empirical analysis, modelling, small and medium enterprises, information security, security incidents, compliance

Absztrakt

Jelen publikációm alapjául egy 2019-2020-ban, a magyarországi gazdálkodó szervezetek körében végzett kérdőíves felmérés szolgál. Ebben a lekérdezésben 498 válaszadó adott választ, amelyeknek 99%-a kis- vagy középvállalkozásnak tekinthető. Az itt bemutatott részkutatása azt a kérdéskört vizsgálja, hogy az információbiztonsági incidensesek valóban diszkért események-e, vagy ezek közötti (bayesi) sztochasztikus kapcsolat statisztikailag igazolható-e? Ennek egyik alkérdése, hogy a compliance problémák felfoghatóak-e biztonsági incidensként? A kutatás igazolja továbbá azt a tényt, hogy informatikai kockázatok között azonosítható – a pénzügyi világhoz hasonlóan – szisztematikus és nem szisztematikus kockázatok, így árnyalva a működési kockázatokról alkotott korábbi képet. A kutatás egyik váratlan eredménye, hogy bizonyos kockázatok ellen meghozott ellenintézkedés valóban csökkentheti az adott kockázat bekövetkezési valószínűségét, viszont más kockázatok esetében pont ellentétes hatással jár: megnöveli a kockázat realizálódásának esélyét.

Kulcsszavak

Empirikus elemzés, modellezés, kis- és középvállalatok, információ biztonság, biztonsági incidensek, compliance

[1] kutatas@horvath-adam.hu | ORCID: 0000-0001-5136-9316 | PhD-hallgató / PhD Student | Óbudai Egyetem Biztonságtudományi Doktori Iskola

BEVEZETÉS

Asta Tarutė és szerzőtársa 2014-es tanulmányában [1] tanulmányában bemutatta, hogy egy „hagyományos" ellátási láncban elhelyezkedő gazdálkodó szervezet életében milyen előnyökkel járhat az IT-megoldások minél szélesebb körű integrálása: a szerzőpáros által azonosított előnyök operatív jellegű hatékonyságnöveléstől kezdve egészen a stratégiai előnyökig terjed. Ugyanebben a tanulmány az Egyesült Királyságban működő kisvállalkozások elemzésén keresztül bemutatták, hogy IT-megoldások egyre szélesebb spektrumát nem az egyszeri implementáció révén integrálják, hanem egy fejlődési út vezet az első üzelti alkalmazásokról az első átfogóbb rendszer alkalmazásáig. Neirotti Paolo [2] és szerzőtársai 284 vállalat fejlődését elemezve mutatta ki, hogy kifejezetten a korai fejlődési szakaszukban marginálisan ruháznak az IT-infrastruktúrájukban. Részben ez lehet az oka, hogy egy ausztrál felmérés [3] szerint a 100 főnél kevesebb munkavállaló vállalatok egyharmada semmilyen megelőző óvintézkedést nem tesz az kiber-bűncselekmények megelőzése ellen, és a vállalatok 87%-a elegendőnek tartja mindössze az végponti biztonság (antivírus programok) telepítését.

Az elégtelen információ-biztonsági intézkedésekre (is) visszavezethető információbiztonsági incidenseknek számos több következménye lehet: a legkézenfekvőbb következménye az operatív kár, amely az esemény bekövetkeztéből ered. Ehhez kapcsolódnak olyan stratégiai károk, mint a piaci image és pozíció romlása, és ennek gyakran van egy vállalaton belüli következménye: gátként hat a jövőben meghozandó infokommunikációs megoldásokhoz kapcsolódó innovációs döntések során. Ez pedig hosszabb távon gátolhatja a gazdálkodó szervezetek fejlődését. [4]

A KUTATÁS ELMÉLETI HÁTTERE

A különböző kockázat-értékelési és kezelési eljárásokat többféleképpen csoportosíthatjuk (kvalitatív vs. kvantitatív [5], szakértői becslésen [6] vs. veszteség-adatbázison alapuló, mint amilyet a Bázel-II AMA eljárása is ajánl [7].). Amennyiben sikerül megbecsülni vagy explicit módon meghatározni az egyes kockázatok bekövetkezési valószínűségét és várható kárérték mértét / mértékeit (a kárértéket gyakran az információbiztonsági dimenziók mentén határozzák meg, tehát egy kockázat teljes kárértéke az egyes dimenziók szerinti körtékék összege), akkor a kockázatokat el lehet helyezni egy kockázati-mátrixban, és mindezek alapján megfelelő ellenintézkedéseket lehet foganatosítani. Ez a megközelítés implicit módon a következő feltételezésekkel él:

- Az egyes kockázatok bekövetkezési valószínűsége és a lehetséges kárértéke egymástól független, tehát nincs szinergia hatás
- A kockázatokkal szemben meghozott ellenintézkedések csak az adott kockázatra hatnak, tehát a kereszthatás nem mutatható ki.

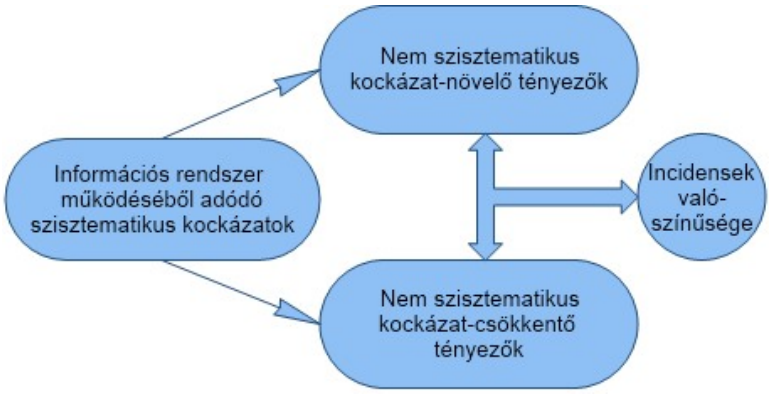
Ezzel szemben több szerző (angol nyelven [8], magyar nyelven: [9]) azzal a feltételezéssel él, hogy ezek a premisszák nem igazak, és felállítottak olyan elméleti modelleket, amelyekben az egyes kockázatok között mégiscsak léteznek kapcsolatok. Ez a feltételezés azzal a következménnyel jár, hogy ha egy hipotetikus „A" kockázat realizálódása sztochasztikus módon indukálja „B" kockázat bekövetkeztét, akkor az „A" kockázat kárértéke már nemcsak a saját kárértéke, hanem ehhez hozzáadódik „B" kockázat feltételes valószínűség-

gel korrigált kárértéke. Egy bayes-i feltételes valószínűségen alapuló kockázatkezelés azonban azzal a nehézséggel jár, hogy amint számos kutatás igazolta, a feltételes valószínűség mértéken kvantitatív módon, szakértői becsléssel csak nagyon pontatlanul határozható meg [10] [11], pontos becsléshez kvalitatív veszteség-adatbázisra van szükség. [A jelen publikációban bemutatott rész-kutatás a következő kérdésekre keresi a választ:

- Kimutathatóak-e a kérdőívet kitöltők körében az egyes realizálódott kockázatok (biztonsági incidensek) között sztochasztikus kapcsolat?
- Amennyiben kimutatható sztochasztikus kapcsolat, elkülöníthetőek-e
- Kimutathatóak-e a kockázatokkal szemben foganatosított ellenintézkedések körében „másodlagos", nem szándékolt hatás?
- A jogszabályoknak való megfeleltségre (compliance) tekinthető e a hatodik információ-biztonsági dimenzióként.

A KUTATÁS ÉS AZ EREDMÉNYEK

A gazdálkodó szervezetek informatikai infrastruktúrája és információbiztonsági érettsége között nyugvó összefüggéseket feltárni célzó kvantitatív kutatás, illetve annak a jelen publikációban bemutatásra kerülő részkutatás alapjául szolgáló adatbázis egy kérdőíves lekérdezés útján jött létre, illetve az egyes gazdálkodó szervezetektől beérkezett válaszok mellett a válaszadók pénzügyi beszámolóiból származó adatokkal kerültek kiegészítésre. A most bemutatott részkutatás elméleti modelljét a következő ábra segítségével foglalom össze.



1. Ábra: A részkutatás elméleti modellje (forrás: saját szerkesztés).

A részkutatás abból a feltételezésből indul ki, hogy az informatikai rendszereknek – átvéve a terminológiát a pénzügyi világból - vannak szisztematikus kockázatai, amely egy adott informatikai megoldásokat használók között minden felhasználóra – használat mértékétől függően – azonos módon, de eltérő mértékben hatnak: ide értendőek többek között azokat a hibák, amelyeket hibajavításokkal (patch) vagy frissítésekkel (update) szokott a gyártó javítani; ezzel szemben állnak azok a felhasználás egyedi módjából nem szisztematikus tényezők (például: erős jelszókövetelmény, biztonsági másolat megszervezése), amelyek egyedi módon növelik vagy csökkentik az információ-biztonsági incidensek realizálódásának valószínűségét. (Nem ebben a kutatásban használják fel a szisztematikus kockázat és nem szisztematikus kockázat fogalmát nem pénzügyi kontextusban [12].)

A kvalitatív kutatás alapjául egy online kérdőív-rendszer segítségével lebonyolított adatfelvétel révén előállít adatbázis szolgál. A kérdőív eredeti koncepciója – első változata – szerint a fent bemutatott modell mindhárom elemét (szisztematikus kockázatok, nem szisztematikus kockázat-növelő és csökkentő tényezők) az információ-biztonsági dimenziók (bizalmasság, integritás, rendelkezésre állás, letagadhatatlanság, reprodukálhatatlanság) szemszögéből kerülnek felmérésre, de a kérdőív első változatával lebonyolított próbakiötöltetések során kapott visszajelzések alapján több, a jelen publikáció szempontjából releváns kérdést törölni kellett, és így alakult ki a kérdőív végleges változata, amelyben a válaszdóknak mindösszesen 75 kérdésre kell választ adniuk. A kutatásba legalább kettő éve létező, nem digitális termékeket és / vagy szolgáltatásokat gyártó, illetve forgalomba hozó gazdálkodó szervezetek kerültek bevonásra. A kutatásba bevont gazdálkodó szervezetekkel e-mailen történt a kapcsolatfelvétel, és a kutatást támogatta több szakmai vagy területei alapon szerveződő kamara, illetve érdekvédelmi szervezet is. A kérdőív felépítésébe során szempont volt, hogy lehetőleg egyetlen vezető beosztású személy is ki tudja tölteni. A lekérdezéshez használt LimeSurvey nevű rendszer a beállításaival lehetővé teszi, hogy minden kérdést ne meg kelljen válaszolni, így biztosítható volt, hogy a kérdőívben ne maradjon megválaszolatlan kérdés. Ennek az is lett következménye, hogy nagyon sok félbehagyott kitöltésre került sor, 1 teljesen kitöltött kérdőívre nagyságrendileg 3-4 félbehagyott kérdőív jutott. A kutatásba közel 22.000 vállalat került bevonásra, és mindösszesen 498 értékelhető válasz érkezett. Az online kérdőív-rendszer lehetővé teszi a válaszok széles körben elterjedt fájlformátumban történő exportálását, egy táblázatkezelő szoftverrel készítettem elő statisztikai elemzéshez az adatokat és generáltam az ábrákat, valamint kereszttáblás lekérdezéseket, és az R keretrendszerét és annak több modulját használtam a statisztikai elemzésekhez. A nem szisztematikus kockázat-növelő és tényezők kérdéseit és az arra kapott válaszokat, a következő, táblázatban foglaltam össze:

Kérdés azonosítója	Kérdés szövege	Nem jellemző	Részben jellemző	Jellemző
C1/4	A GDPR hatályba lépését megelőző négy évben történt jelentős mértékű informatikai eredetű üzemzavar.	330		40
C1/5	A GDPR hatályba lépését megelőző négy évben volt a cégünkben több gépet érintő vírustámadás/-fertőzés.	294		76
C1/7	A GDPR hatályba lépését megelőző négy évben történt a vállalat életében jelentős mértékű meghibásodásból származó adatvesztés.	331		39
C1/9	Nehézséget jelentett a következő események valamelyike: GDPR bevezetése, online pénztárgépek bevezetése, NAV- hoz bekötött számlázó alkalmazás használata	262		108
C1/3	Problémát jelent, hogy különböző alkalmazások között adatokat kell manuálisan át/feltölteni.	186	142	42

Kérdés azonosítója	Kérdés szövege	Nem jellemző	Részben jellemző	Jellemző
C1/13	Fenn kell tartani valamilyen elavult informatikai rendszert, mert a rajta futó alkalmazást nem tudjuk frissíteni / helyettesíteni.	226	105	39
C1/19	Elegendőnek érezzük, hogy csak megvásárolható biztonsági alkalmazásokat (antivírus + tűzfal) telepítjük.	84	149	137
C1/2	Több évre visszamenőleg minden adat biztonsági mentés formájában a rendelkezésünkre áll, bármikor el tudjuk érni.	13	83	274
C1/6	A számítógépes hálózatunkat (LAN, WIFI) legalább egy haladó szintű védelemmel biztosítjuk	24	50	296
C1/8	Nyomon tudjuk követni a bejelentkezett felhasználók tevékenységét: ellenőrizzük napló-állományokat vagy behatolás-figyelő rendszert telepítünk.	106	129	135
C1/10	Képesek vagyunk az üzleti szempontból fontos állományokat titkosítva tárolni.	60	113	197
C1/14	Lemondunk valamelyik kényelmi szolgáltatásról a nagy biztonság érdekében: nem használunk laptopokat / USB- adathordozókat stb.	298	58	14
C1/15	Telepítettünk a legfontosabb informatikai eszközökhöz szünet-mentes tápegységet.	46	50	274
C1/16	Gondoskodunk arról, hogy szoftverek frissítései minél gyorsabban telepítésre kerüljenek.	21	97	252
C1/17	A legfontosabb eszközökből vannak tartalékaink meghibásodás esetére.	58	149	163
C1/20	Inkább használunk komplex biztonsági alkalmazásokat (antivírus + tűzfal), mint egyesével külön telepített megoldásokat.	54	118	198

1. táblázat: A biztonsági incidensek korrelációs mátrixa (forrás saját szerkesztés)

A kérdőívben lehetőség volt a „Nem tudom / nincs válasz" megjelölésére is. A kitöltések kiértékeléséből kitűnik, hogy erre megoldásra szükség volt, hiszen csak 370 olyan kitöltésre került sor (az összes kitöltés bő háromnegyede, pontosabban: a 74,30%-a), ahol egyetlenegy esetben sem adott „Nem tudom / nincs válasz"-t. Tekintettel arra, hogy a kérdőív további kérdései nem tették lehetővé, hogy következtetni lehessen, hogy mi motiválta a „Nem tudom / nincs válasz" megjelölését, ezért ebben a részkutatásban csak azt a 380 kitöltések vonom be az elemzésbe, ahol a válaszadó nem adott ilyen választ. Az 1. ábrán logikát követve:

- Nem szisztematikus kockázat-növelő tényezőkre a C1/2, C1/6, C1/8, C1/10, C1/14, C1/15, C1/16, C1/17 és a C1/20 jellegű kérdések vonatkoztak. Az adatfeldolgozás

során a „nem jellemző” válasz 0-as értéket kapott, a „részben jellemző” érték 0,5-ös értéket kapott és a jellemző érték 1-es értéket kapott.;

- nem szisztematikus kockázat-csökkentő tényezőkre a C1/3, C1/13 és a C1/19 jelű kérdések vonatkoztak. Az válaszok elemzésbe történő bevonása az előbbiekhez hasonlóan történt.
- információbiztonsági incidensekre a C1/4, a C1/5, C1/7 és a C1/9 jellegű kérdések vonatkoztak. A részkutatásba bevont 370 válaszadóból 191 (51,62%) nem számolt be információ-biztonsági incidensről, 120 válaszadó (32,43%) jelölt be 1 incidenst, 39-en (10,53%) jelöltek be 2, 15-en (4,05%) 3, és 5-en (1,35%) számoltak be mind a négy incidens bekövetkeztéről. Tekintettel arra, hogy eredmény-változóként azt vizsgáltam, hogy következett-e be bármilyen mértékű incidens, ennél a válasznál 0-as értéket kapott a „nem jellemző” válasz, és mind a „részben jellemző” és „jellemző” válasz 1-es értéket kapott.

Az elemzés első lépésében megvizsgálom az egyes kategóriákon belüli korrelációk alakulását. A biztonsági incidensek közötti korrelációs mátrixot a 2. táblában foglaltam össze (mindhárom mátrix esetében a cellák felső sorában a számított korreláció, az alsó sorban a számított p-érték került feltűntetésre).

	C1/4	C1/5	C1/7	C1/9
C1/4	1,00	0,25 (0,0000)	0,39 (0,0000)	0,14 (0,0069)
C1/5	0,25 (0,0000)	1,00	0,20 (0,0002)	0,06 (0,2813)
C1/7	0,39 (0,0000)	0,20 (0,0002)	1,00	0,05 (0,3313)
C1/9	0,14 (0,0069)	0,06 (0,2813)	0,05 (0,3313)	1,00

2. táblázat: A biztonsági incidensek korrelációs mátrixa (forrás saját szerkesztés)

Ahogy a korrelációs mátrixból leolvasható, a lehetséges 6 változó-párból kettő esetében nem mutatható ki szignifikáns korrelációs. Mindkét nem szignifikáns korreláció egyik tagja a C1/9 kérdés, amely nem klasszikus információ-biztonsággal kapcsolatos incidensekre kérdez rá, hanem a törvényi előírásoknak való megfeleltséggel (compliance) kapcsolatos problémákra kérdez rá. A szignifikáns korrelációk megerősítik azt a feltételezést, hogy a biztonsági incidensek nem diszkért események, hanem ezek a káresemények bekövetkezte egymásra hatással vannak.

A nem-szisztematikus kockázatnövelő-tényezők közötti kapcsolatot az alábbi mátrix mutatja meg:

	C1/3	C1/13	C1/19
C1/3	1,00	0,16 (0,0022)	0,01 (0,8707)
C1/13	0,16 (0,0022)	1,00	-0,06 (0,2593)
C1/19	0,01 (0,8707)	-0,06 (0,2593)	1,00

3. táblázat: A biztonsági incidensek korrelációs mátrixa (forrás saját szerkesztés)

Ahogy a korábbiakban bemutattam, a kutatás sikere érdekében jelentős körültekintéssel kellett eljárnom az információbiztonsági incidensekre vonatkozó kérdés feltételekor. A három kérdőívben maradt kérdés mindegyike olyan kockázatnövelő-tényezőre kérdez rá, amelyhez kapcsolódó incidensek bekövetkeztének esetében valószínűsíthetőek a vis maior jellegű esemény, azaz nem kell a jogellenes magatartást feltételezni. Az egyetlen szignifikáns korrelációt eredményező kérdéspár (C1/3 és C1/13) mindkét párja a „rendelkezésre állás" biztonsági dimenzióját érintő kockázat-növelő tényező. Sajnálatosan nagyon nagy kockázattal járt volna, a kockázat-növelő tényezők szélesebb körű felmérésének kísérlete. Abból a tényből, hogy a tényezők között vagy egyáltalán nincs szignifikáns korreláció, vagy a szignifikáns korreláció is gyenge kapcsolatot mutat, arra lehet következtetni, hogy a válaszadók kockázati térképe egymástól jelentős mértékben eltér.

Az információ-biztonsági-incidensek és a nem-szisztematikus kockázatnövelő-tényezők analógiájára megvizsgáltam a nem-szisztematikus kockázatcsökkentő-tényezők tényezők korrelációs kapcsolatát. Olvashatósági okokból kifolyólag a 9×9 dimenziójú korrelációs mátrix nem kerül itt bemutatásra, a 36 lehetséges változó párból csak azok változópárok nem mutattak szignifikáns korrelációt, ahol az egyik változó-pár egyik tagja a C1/14 jelű kérdés. A szignifikáns korrelációt mutató kérdések-párok körében a korreláció mértéke 0,16 és 0,35 közötti értékeket vett fel.

Bármely két kérdésre kapott választ reprezentáló változó között kimutatott korrelációs kapcsolat, pusztán a köztük fennálló lineáris kapcsolat erősségének mérésére szolgál. [14] Az előbbiekben bemutatott korreláción alapuló elemzések eredményéből azt valószínűsítik, hogy lehetséges olyan szignifikáns regressziós modell felállítása, amelynek általános képlete az 1. ábra alapján:

$SZR + NSZR^{+} - NSZR^{-}$ = Incidensek bekövetkezési valószínűsége
ahol:
SZR: a szisztematikus kockázatok összesége
$NSZR^{+}$:a nem szisztematikus kockázatnövelő tényezők összessége
$NSZR^{-}$: a nem szisztematikus kockázatcsökkentő tényezők összessége

a modell igazolására az konstruktív ökonometriai iskola [13] eljárás-mintáját követve az un. stepwise regressziós modell felállításával kerül sor. Az így felállított négy regressziós modell mindegyike szignifikánsak bizonyult, amint azt alábbiakban bemutatott ANOVA-táblázatokról is leolvasható (a táblázatban csak a szignifikáns változók kerülnek feltüntetésre):

R^2:		0,2188				
Korrigált R^2:		0,2037				
F-próba		14,49				
Szabadságfok:		7 és 362				
p-érték:		2,2e-16				
Változó neve		Becsült érték	St. hiba	t-érték	Pr(>|t|)	szig.
Tengelymetszet	(β_0)	0,1951	0,0665	2.936	0,0035	**
C1/2	(β_1)	-0,1447	0,0574	2,519	0,0122	*
C1/4	(β_2)	0,3650	0,0476	7,667	1,64e-13	***
C1/5	(β_3)	0,0634	0,0368	1,721	0,0860	.
C1/6	(β_4)	-0,2089	0,0551	-3,791	0,0001	***

Változó neve		Becsült érték	St. hiba	t-érték	Pr(>|t|)	szig.
C1/16	(β_5)	0,1024	0,0518	1,978	0,0487	*
Szignifikancia kódok:		”***”: 0,001	”**”: 0,01	”*”: 0,05	”.”: 0,1	” ”: 1

4. táblázat: Regressziós-model (eredmény-változó: C1/7) ANOVA-táblázata (forrás: saját szerkesztés)

Ebben a regressziós modellben azt vizsgáltam, hogy milyen tényezők csökkentik, illetve növelik a válaszadók körében az adatvesztés bekövetkeztetét. Fel kell hívni a figyelmet arra, hogy a tengelymetszet és szignifikáns alkotóeleme a regressziós-modellnek, amely azért fontos, mert így a vállalati IT-környezet szisztematikus kockázata reprezentáltnak tekinthető. A modell verifikációjaként tekinthetünk arra körülményre, hogy kettő, nem szisztematikus kockázat-csökkentő tényező, a biztonsági másolatok megléte (C1/2), és hálózati infrastruktúra emelt szintű védelme is szignifikáns változó (C1/6 jelű kérdés), és mindkettő előjele negatív, így ezek az intézkedések valóban be tudják tölteni szerepüket. A hálózati infrastruktúra szignifikáns szerepe modellben azért két szempontból is jelentős eredmény: egyrészről ezzel sikerült bebizonyítani, hogy az egyes biztonsági intézkedéseknek nemcsak azokon a területeken jut jelentős szerephez, amelyre területen „magától értetődően” el kell látnia a feladatát, hanem kimutatható egyfajta „kereszt-hatás” is; másrészről, ha olyan hálózati adattárolási megoldásokra gondolunk, mint a NAS- és SAN-eszközök, akkor visszaköszönni látszik az a körülmény, hogy a helyi hálózati- és adattárolási megoldások egy komolyabb IT-környezetben egymástól nem választhatóak el [15].

Szintén a kutatás eredményének kell értékelni, hogy megjelent a magyarázó változókban megjelentek – bár eltérő súllyal és szignifikancia-szinttel - más információ-biztonsági incidensek (ebben az esetben az informatikai üzemzavarokra vonatkozó C1/4 jelű, és a vírustámadásokra vonatkozó C1/5 jelű kérdések). és ezzel sikerült igazolni, hogy a kutatás alapgondolata helyes, azaz egyes káresemények bekövetkezte nem függetlenek egymástól.

A kutatás érdekes eredménye, hogy egy olyan intézkedés (a frissítések telepítésére vonatkozó C1/16 jelű kérdés, amelyről eredetileg azt feltételeztem, hogy növeli az adott szervezetben az információ-biztonság szintjét (ha rendszeresen végrehajtott intézkedés), a regressziós modell eredménye alapján inkább a kockázati kitettséget növelő tényező.) Ennek sajnos létezik gyakorlati válasza is (például a Windows 10 frissítésével fellépő problémák 2020. októberében.), és ezt tudományos alapon vizsgálja Tudor Dumitras és szerzőtársa [16]

R^2:		0,2067				
Korrigált R^2:		0,1980				
F-próba		23,77				
Szabadságfok:		4 és 365				
p-érték:		2,2e-16				
Változó neve		Becsült érték	St. hiba	t-érték	Pr(>|t|)	szig.
Tengelymetszet	(β_0)	-0,0723	0,0498	-1,453	0,1471	
C1/5	(β_1)	0,1386	0,0366	3,789	0,0002	***
C1/6	(β_2)	0,1033	0,0515	2,006	0,0456	*
C1/7	(β_3)	0,3676	0,0486	7,564	3,2e-13	***
C1/9	(β_4)	0,0806	0,0320	2,521	0,0121	*
Szignifikancia kódok:		”***”: 0,001	”**”: 0,01	”*”: 0,05	”.”: 0,1	” ”: 1

5. táblázat: Regressziós-model (eredmény-változó: C1/4) ANOVA-táblázata (forrás: saját szerkesztés)

Ebben a regressziós modellben azt vizsgáltam, hogy milyen tényezők vezetnek az informatikai üzemzavarok bekövetkeztéhez (C1/4 jelű kérdés.) Ebben a modellben a konstans változó nem szignifikáns, így ebben az esetben a szisztematikus kockázat szignifikáns voltanem mutatható ki. a négy szignifikáns változóból három biztonsági kockázat – így ebben modellben ugyanígy érvényes az előző modell esetében tett megállapítás, miszerint a kutatás alapgondolata helyes, azaz egyes káresemények bekövetkezte nem függetlenek egymástól, azaz statisztikailag igazolható egy negatív irányú szinergia-hatás kialakulásának valószínűsége. Az előző modellhez hasonlóan kockázat-növelő tényezőként jelenik meg egy olyan elem, amely elméletileg kockázat-csökkentő hatással kellene bírnia (C1/6 kérdés):

R^2:		0,1143				
Korrigált R^2:		0,0996				
F-próba		7,805				
Szabadságfok:		6 és 363				
p-érték:		6,491e-08				
Változó neve		Becsült érték	St. hiba	t-érték	Pr(>|t|)	szig.
Tengelymetszet	(β_0)	0,0982	0,0626	1,568	0,1178	
C1/4	(β_1)	0,2584	0,0700	3,692	0,0002	***
C1/7	(β_2)	0,1535	0,0708	2,169	0,0308	*
C1/10	(β_3)	-0,1435	0,0564	-2,546	0,0113	*
C1/14	(β_4)	-0,1582	0,0794	-1,993	0,0470	*
C1/15	(β_5)	0,1134	0,0598	1,895	0,0589	.
C1/20	(β_6)	0,6270	0,0570	2,227	0,0266	*
Szignifikancia kódok:		”***”: 0,001	”**”: 0,01	”*”: 0,05	”.”: 0,1	” ”: 1

6. táblázat: Regressziós-model (eredmény-változó: C1/5) ANOVA-táblázata (forrás: saját szerkesztés)

A jelen publikációban bemutatásra kerülő harmadik modell azt vizsgálja egy számítógép-vírus fertőzés elterjedését. Itt is találkozhatunk kettő olyan jelenséggel, amellyel a korábbi kettő modell esetében, azaz, ebben a modellben sem mutatható ki a szisztematikus kockázat (azaz a tengelymetszet) szignifikáns volta, és itt is kimutatható statisztikailag a többi incidens bekövetkeztének kockázat-növelő hatása. Szintén találkozunk azzal jelenséggel, hogy két olyan elem tölt be kockázat-növelő hatást, amelynek az információ-biztonság szintjét kellene elméletileg növelnie: a jelen kérdőívek nem ad rá választ, hogy miért mutatható ki – alacsony szignifikancia-szintű és együtthatójú, de ettől független figyelembe veendő – kapcsolat a szünetmentes-tápegységek és a vírusfertőzések között. Lehetséges okként merül, hogy mindkét tényező egy, a kérdőívben nem vizsgált harmadik tényezővel áll szignifikáns kapcsolatban. Az eredetileg kockázat-csökkentő tényezőnek C1/20-as kérdés kockázat-növelő hatásában sajnos vissza-igazolódik az jelenség, hogy tisztán a végpontokre telepített biztonsági alkalmazások nem jelentenek valós megoldásokat – erről a jelenségről írtam a cikkem bevezetőjében is.

R^2:	0,0967
Korrigált R^2:	0,0893
F-próba	23,77
Szabadságfok:	3 és 366
p-érték:	4,069-08

Változó neve		Becsült érték	St. hiba	t-érték	Pr(>|t|)	szig.
Tengelymetszet	(β_0)	0,1443	0,0336	4,292	2,27e-05	***
C1/3	(β_1)	0,1851	0,0673	2,750	0,0063	**
C1/4	(β_2)	0,1667	0,0731	2,280	0,0232	*
C1/13	(β_3)	0,2956	0,0675	4,378	1,56e-05	***
Szignifikancia kódok:		”***”: 0,001	”**”: 0,01	”*”: 0,05	”.”: 0,1	” ”: 1

7. táblázat: Regressziós-model (eredmény-változó: C1/9) ANOVA-táblázata (forrás: saját szerkesztés)

A negyedik regressziós modellben ismét szignifikáns lett a tengely-metszet, amely a szisztematikus kockázatokat hivatott reprezentálni, és ebben az egye modellben kockázatnövelő tényezőként megjelenik egy olyan tényező, amely önmagában nem biztonsági incidens. Ezzel a modellel sikerült igazolni a biztonsági incidensek és compliance-jellegű vállalati nehézségek közötti kapcsolatot.

A KUTATÁS ÉS AZ EREDMÉNYEK

A kutatásomban négy regressziós modellt állítottam fel, amelyek igazolták a kutatási kérdéseket. Meglátásom szerint sikerült elkülöníteni a „szisztematikus” és „nem szisztematikus” IT-kockázatokat – ezért tartom jó körülménynek, hogy a négy modellből kettő esetben szignifikáns volt, és kettő esetben nem volt szignifikáns a tengelymetszet. Sikerült továbbá bebizonyítani, hogy bizonyos intézkedések vannak kockázat-növelő hatása, és egy biztonsági incidens katalizálható hatással járhat egy másik biztonsági incidens tekintetében.

A kutatás járt nem várt eredménnyel is: egyik ilyen nem várt eredmény, hogy bizonyos biztonsági intézkedés, részben vagy egészben pont a szándékolttal ellentétes hatást idézhet elő.

Kényszerűségből a kutatás alapjául szolgáló kérdőív nem foglalhatta magában mind az öt biztonsági dimenziót felmérni tudó kérdéseket. Meglátásom szerint a jelen részkutatás eredményei, illetve a további még publikálásra váró eredmények kiértékelése alapján szükséges lenne Magyarországon megvalósítani egy olyan, nagyobb legitimációval (tehát nem ismeretlen megkeresésre alapuló) bíró kutatást, amely mélységében méri fel az informatikai infrastuktúra és az információ-biztonság szinte közötti összefüggést. Azért lenne lényeges egy ilyen megismételt kutatás, mert tudatosító erővel bírni, hogy informatikai beruházások mérlegelésekor ne csak a várható előnyöket vegyék figyelembe, hanem jobban tudatosuljon a leendő informatikai infrastruktúra magában hordozott kockázata, azaz, amikor ár / érték arányról gondolkodunk, akkor kiegyensúlyozottabb viszonyba kerüljön a várható hasznosság (benefit) és kockázat.

KÖSZÖNETNYILVÁNÍTÁS

A jelen kutatás létrejöttét a 2017-1.3.1-VKE-2017-00031 azonosítószámú, „Nagy pontosságú burkolat vizsgáló mérési technológia alapjainak kutatási programja” pályázat támogatta. Külön köszönöm a Budapesti Kereskedelemi- és Iparkamara erkölcsi és operatív támogatását!

FELHASZNÁLT FORRÁSOK

[1] Asta Tarutė and Rimantas Gatautis, „ICT Impact on SMEs Performance" in Contemporary Issues in Business, Management and Education 2013 in Procedia - Social and Behavioral Sciences Volume 110, January 2014, pp. 1218-1225, DOI: 10.1016/j.sbspro.2013.12.968

[2] Neirotti, Paolo, Elisabetta Raguseo, and Emilio Paolucci, How SMEs develop ICT-based capabilities in response to their environment: past evidence and implications for the uptake of the new ICT paradigm, Journal of Enterprise Information Management, Vol. 31 No. 1, pp. 10-37., 2018.

[3] Office of the Australian Small Business and Family Enterprise Ombudsman, „Cyber Security: The Small Business Best Practice Guide", Commonwealth of Australia 2017

[4] Ponemon Institute LLC, „THE IMPACT OF DATA BREACHES ON REPUTATION & SHARE VALUE", USA, May 2017.

[5] Wangen, G., Hallstensen, C. & Snekkenes, E, „A framework for estimating information security risk assessment method completeness" Int. J. Inf. Secur. 17, 681–699 (2018). https://doi.org/10.1007/s10207-017-0382-0

[6] Fumika Ouchi, „A Literature Review on the Use of Expert Opinion in Probabilistic Risk Analysis", World Bank Policy Research Working Paper 3201, February 2004

[7] Shevchenko, Pavel V. and Peters, Gareth, Loss Distribution Approach for Operational Risk Capital Modelling Under Basel II: Combining Different Data Sources for Risk Estimation (2013). Available at SSRN: https://ssrn.com/abstract=2980464 or http://dx.doi.org/10.2139/ssrn.2980464

[8] Figini, Silvia and Gao, Lijun and Giudici, Paolo, „Bayesian operational risk models". Journal of Operational Risk. Vol 10. pp. 45-60. (2015) 10.21314/JOP.2015.155.

[9] Horváth Ádám, „ Gondolatok az informatikai kockázatok kapcsán" in: Prof. Dr. Rajnai Zoltán (ed), Rajnai, Zoltán (szerk.) Kiberbiztonság - Cyber Security : Tanulmánykötet a Biztonságtudományi Doktori Iskola kutatásaiból. pp. 109-120. ISBN: 978-963-449-131-6 2018)

[10] Alexander Pollatsek and Arnold D Well and Clifford Konold and Pamela Hardiman, George Cobb, „Understanding conditional probabilities", Organizational Behavior and Human Decision Processes vol. 40 No.2., pp. 255-269. DOI: 10.1016/0749-5978(87)90015-X

[11] André C. R. Martins, „Probability biases as Bayesian inference", Judgment and Decision Making, Vol. 1, No. 2, November 2006, pp. 108–117

[12] Yang-Byung Park and:Hyung-Seok Kim, „Simulation-based evolutionary algorithm approach for deriving the operational planning of global supply chains from the systematic risk management", Computers in Industry Volume 83, pp. 68-77. DOI: 10.1016/j.compind.2016.09.003.

[13] ÁCS Pongrác: SPORT ÉS GAZDASÁG. Pécs, 2015. ISBN 978-963-642-372-8

[14] Alireza Dorestani and Sara Aliabad, „Academy of Accounting and Financial Studies Journal" Vol. 21, No 3, pp 1-13 (2017).

[15] Roland Döllinger and Reinhard Legler and Duc Thanh Bui: Praxishandbuch Speicherlösungen. dpunkt.verlag, 2010. ISBN: 978-3-89864-588-1

[16] Tudor Dumitras and and Priya Narasimhan: „Why Do Upgrades Fail and What Can We Do about It? - Toward Dependable, Online Upgrades in Enterprise System” in: J.M. Bacon and B.F. Cooper (Eds.): Middleware 2009, LNCS 5896, pp. 349–372, 2009

REVIEW OF THE AERODYNAMICAL LOAD ON A DUAL-ROTOR WIND TURBINE'S BLADE

IKERSZÉLTURBINA LAPÁTJAIN ÉBREDŐ AERODINAMIKAI TERHELÉSEK VIZSGÁLATA

HETYEI Csaba[1] – SZLIVKA Ferenc[2]

Abstract

In our article, we review the traditional wind turbines and non-traditional wind turbines. Then we described the turbine design process based on the available literature, highlighting the mechanical design criteria with the structural loads. Subsequently, a horizontal axis counter-rotating dual-rotor turbine (CO-DRWT) and a horizontal axis single-rotor wind turbine (HAWT) were compared by computational fluid dynamics simulation (CFD).

Based on our simulation, we were examining the forces on the blades of the two-rotor turbine and their components, we found that the residual force on the blades is higher and more complex, therefore, the possibility of fatigue is more likely. A dual-rotor wind turbine has a life and it requires more frequent condition diagnostics and maintenance.

Keywords

CFD, Fatigue, FEM, Fluid dynamics, Operational safety, Simulation, Solid mechanics, Wind turbine

Absztrakt

Cikkünkben áttekintettük a tradícionális szélturbinákat és a nemtradícionális szélturbinákat. Ezt követően ismertettük a rendelkezésünkre állós irodalom alapján a turbinatervezés folyamatát, kiemelve a gépészeti tervezést és az ott ébredő szerkezeti terheket. Ezt követően numerikus áramlástani szimulációval (CFD) összehasonlítottunk egy vízszintes tengelyű ikerturbinát (CO-DRWT) és egwy vízszintes tengelyű egyrotors turbinával (HAWT).

Szimulációnk alapján a kétrotoros turbina lapátjain ébredő erőket és azok komponenseit vizsgálva megállapítottuk, hogy a lapátokon ébredő erők eredője nagyobb, erőrendszere komplexebb, így a kifáradás lehetősége valószínűbb, mely rövidebb élettartamot és gyakoribb állapotdiagnosztikát és karbantartást igényel.

Kulcsszavak

CFD, Folyadékok mechanika, Kifáradás, Szilárdtest mechanika, Szélturbina, Szimuláció, Üzembiztonság, VEM

[1] hetyei.csaba@phd.uni-obuda.hu | ORCID: 0000-0003-2915-4540 | PhD student/doktorandusz | Óbudai Egyetem Biztonságtudományi Doktori Iskola

[2] szlivka.ferenc@bgk.uni-obuda.hu | ORCID: 0000-0002-3298-4142 | Professor/egyetemi tanár | Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

INTRODUCTION

Nowadays fear from the nuclear accident and the environmental damage, renewable energy sources become more and more into the focus. One of these energy sources the wind energy which was used until the beginning of the civilization for sailing and milling. The first example of a windmill which was used for flour grinding was the Nastifan. This ancient engineering machine was built in the 9th century, three centuries earlier than the first known windmills appear in north-western Europe [1]. The Nastifan Windmill was a vertical axis windmill, its reconstructed version is shown in Figure 1.

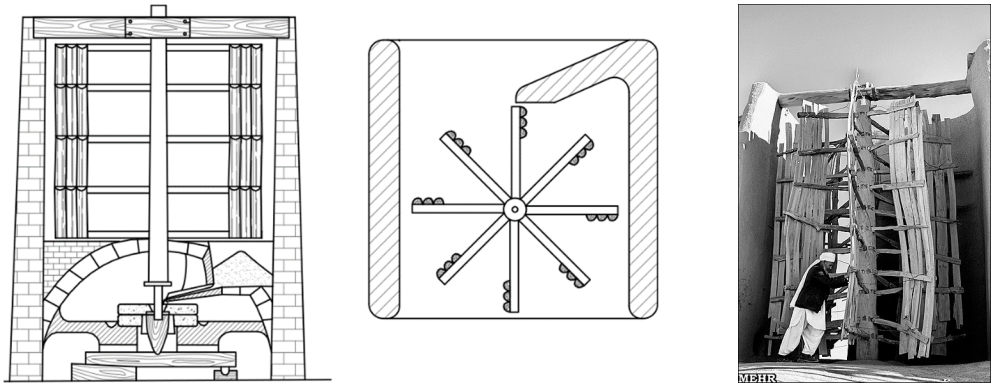


Figure 1.: Conceptual outline and reconstructed version of Nashtifan Windmill [2]

The European windmill which we know as the "Dutch Windmill" was a horizontal axis windmill, which has a long history until the American Windmill, the first modern windmill was invented by Daniel Halladay in the middle of the 19th century.

Using the existing design and knowledge after three decades of the invention of the American Windmill, the first vertical axis wind turbine (VAWT) was invented in 1887 by James Blyth and the first horizontal axis wind turbine (HAWT) was invented in 1888 by Charles Brush. This two turbine is shown in Figure 2.

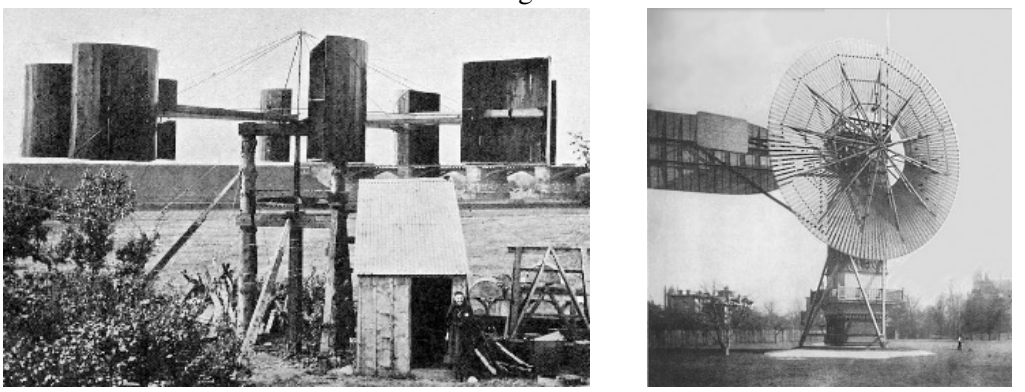


Figure 2.: James Blyth's VAWT (left) and Charles F. Brush's HAWT (right) [3, 4]

After the first VAWT and HAWT, the development of the wind turbines is increased and the turbines start to spread on the globe. The 70's and 80's oil crisis push in the developments and the number of the installation. Nowadays, fear from the nuclear accident and the environmental damage, the wind turbine (WT) installation progressively starts growing. This process can be seen in the global statistics, for example in BP's 2019 report [5], which can see in the next figure.

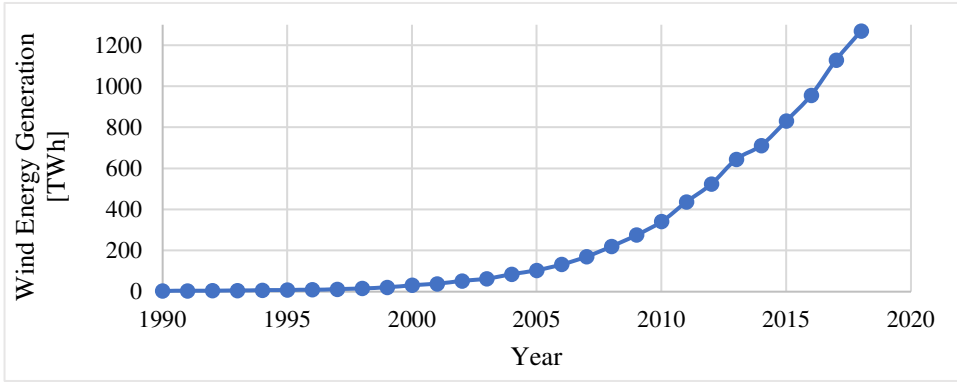


Figure 3.: Wind energy generation globally by year in Terawatt-hour [5]

The growing use of WTs has produced a new variety of appearance, which category is the unconventional wind turbines. This kind of turbines is any new type which has a parameter or property which alters from the 90's or the early 2000's design. One of them is the Archimedes Screw Wind Turbine, which can operate with low noise as a result of its relatively low rotational speed. This Archimedes Screw WT is shown in Figure 4.

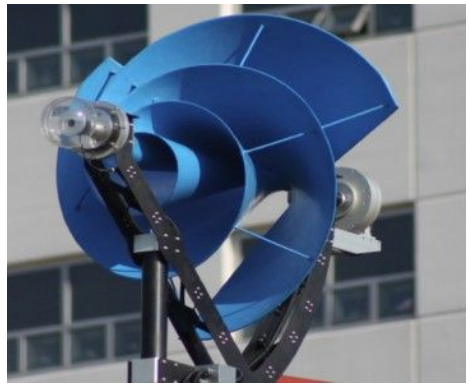


Figure 4.: Unconventional WT: Archimedes Screw Wind Turbine [6]

Other examples for the unconventional WTs are the dual rotor wind turbines, which has two rotors. This type of WTs has two subcategories according to the direction of rotation, these are the co and counter-rotating dual-rotor wind turbines. When the geometry of the turbine are mirrored and the rotors are rotating in the opposite direction they are the counter-rotating dual-rotor wind turbines (CO-DRWT). When the geometry is the same and

the rotors rotate in the same direction, they are the co-rotating dual-rotor wind turbines (CR-DRWT).

Figure 5.: Unconventional WTs: Dual-Rotor Wind Turbine

The first theory about the single rotating wind turbines (SRWT) efficiency was made by Betz in 1919. The Betz's model predicts the power coefficient (c_p), which is the efficiency to 16/27 (59.259%) in an idealized world, where there is no any kind of loss factor, and the turbine is independent of the geometry and it has an infinite number of blades. By the GGS model [8] from 2001, which is a curvilinear model against the rectilinear Betz model, the c_p's maximum value is 30.113%. By measurements, the WTs' power coefficient usually between these two limits.

Theoretically, with the known maximum performance the SRWT's maximum load can be calculated. In the next two chapters, we will review the foundation of the wind turbine's design and the basics of the fatigue failure, then with the use of a CFD (computational fluid dynamics) software, we will determine the aerodynamical load of a CO-DRWT, which can be used for an FEA (finite element analysis) software to establish the stress and the durability.

THE BASICS OF WIND TURBINE'S DESIGN

The wind turbines are complex electro-mechanical systems which have multiple design conditions in the mechanical side as well in the electrical side and IT side. In this paper, we will focus just the structural loads, the internal loads of the working mechanical and electrical component will not be detailed.

The mechanical design usually starts with the structural design of the rotor and tower, then it is followed by the aerodynamic design, where the aerodynamic loads are derived. The structural design seeks the optimum of strength, weight, and cost, the aerodynamic design main goals are the optimum of efficiency, noise reduction (if it's needed, e.g. for onshore turbines or for small WTs that can be installed on buildings), and cost [9]. The requirements of a WT design shown in Figure 6.

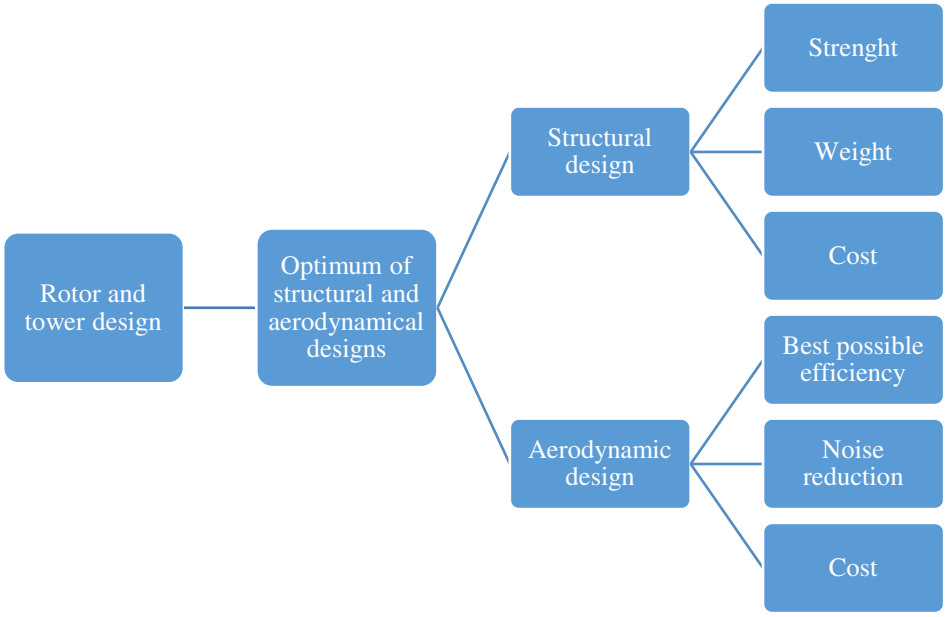


Figure 6.: Design requirements for a wind turbine [9]

The wind turbines failure can occur for four reasons, 1. Extreme wind; 2. Inadequate control system; 3. Collision with birds, UAVs, and other flying objects; and 4. Cyclic-load fatigue which may lead to material fatigue.

The first three reasons will not be explained in this article. The fatigue is an important topic since wind turbines are designed to operate at least 20 years, within the rotor rotates more than 10^9 revolutions. In every rotation, the loads are repeated, which lead to material changing example strain hardening or brittle fracture.

For the HAWT the most relevant loads are the 1. aerodynamic loads; 2. control loads; 3. dynamic loads; and 4. gravitational loads.

The aerodynamic loads are the lift and drag forces, and the momentum which can be predicted with the blade element momentum (BEM) theory. The control loads origins are the blade pitch angle control which is why the torque is used to continuously change for the optimal tip-speed ratio. The dynamic loads are related to the blade's motion, for example, the centrifugal force or the gyroscopic loads. The gravitational loads are associated with the weight of the blade, example the self-weight which is altering by the rotational angle or the eccentricity which due to the deformation in wind load, or due to the manufacture and assembly… [9]

The listed forces also load the tower as well as the blades. The tower is usually a cylinder with decreasing cross-section, in contrast, the blades are multi-component parts. The parts are the 1. airfoil skin; 2. spam flange; 3. shear web, and 4. adhesive. The structural function of the airfoil skin is to provide edge-wise torsional stiffness, the spare flange has to support the flap-wise bending stiffness and the buckling resistance, the shear web or webs have to handle the shear stiffness, and the adhesive must ensure structural integrity. By the

number of shear webs, the blade structures are divided into chambers, a three-chamber airfoil structure shown in Figure 7.

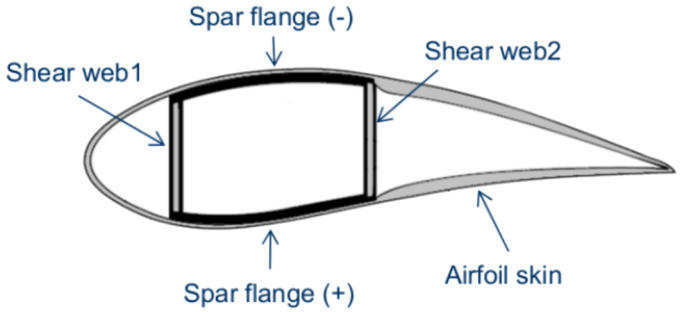


Figure 7.: Cross-section of a 3 cell airfoil structure [12]

For the sections structure design, the two main requirements are to be stiff and lightweight. Lin *et al.* [13] was creating a mathematical model for calculating the cross-section of a multiple composite layer airfoil with one to three-chamber. Heo *et al.* [14] analysed with FSI (fluid-structure interaction) a three cell airfoil structure with chiral, regular and re-entrant hexagonal honeycombs cellular cores under a static load through the deformation. They airfoil cross-sections are shown in the next figure.

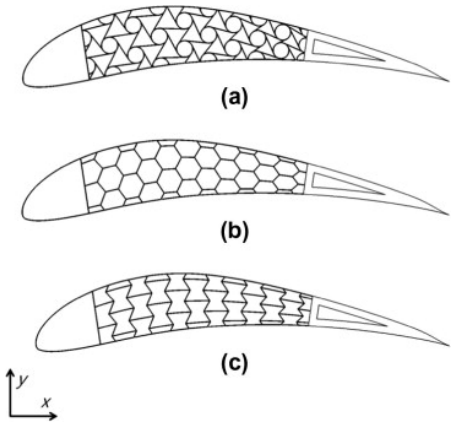


Figure 8.: Analysed airfoil sections of Heo et al.*:*
(a) chiral honeycomb, (b) regular and (c) re-entrant honeycombs [14]

The rotor's blade can be modelled as a cantilever beam, where for each section the BEM theory provide the loads for the segment as it is shown for a *dx* segment on Figure 9.

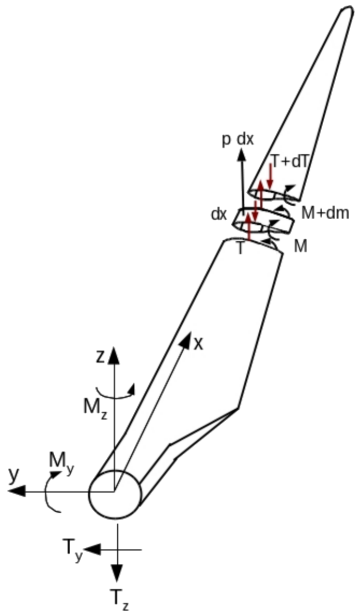


Figure 9.: Shear forces and moments on the root of the blade and a dx long segment [9]

In the previous figure, T_i and dT are the shear forces, M_i and dM are the moments in the x-y-z coordinate system, and p is the residual force on the segment.

The deformation which occurs on the blade can be calculated analytically as we mentioned previously and numerically like Cox presented [12] in his study. On the other hand, laboratory testing with small scale model can predict the deformation and the forces on the 1:1 scale turbine, and the on-site measurement can clarify the simulated and predicted loads and deformation. Example Ovenden *et al.* [15] had a strain gauge and a laser displacement measurement to detect the blade faults. The laboratory experiment showed the strain gauge measurement was more precise, and the laser displacement sensor was able to detect misalignment and bolt loosening. This built-in system can extend the currently running SCADA (supervisory control and data acquisition) system of the WTs. Small and medium-sized wind turbines, where a complex SCADA system and its sensors are not required by economic reasons and by internal space requirements, or for old large-scale turbines which control and data acquisition systems are insufficient and the upgrade is not possible Nagy and Ingo [16] designed an unmanned flying platform (UAV) with a data acquisition system (DAQ). This system was able to measure ambient temperature, humidity, pressure, wind speed and direction, spatial position with high accuracy, and distance with range sensor. If the UAV extended with a DAQ and an image acquisition system for measuring fluid dynamic parameters and analysing graphically the blades of the WTs a high speed and reliable communication system is required. Huszák [17] designed a GPS based automatic UAV antenna tracker system which can be used between a continuously moving UAVs and their ground control system.

BASICS OF FATIGUE FAILURE

With a better and more detailed analytical and numerical tool and with their validating measurements, loads of the components of a WT can be described more precisely. Knowing the generated forces and the component failure process a malfunction is more predictable. When the wind turbine blades have a failure, which is not a collision with an unattended fling object or it does not the cause of an overload or a malfunction of the control system, it is the fatigue failure.

The first stage of the fatigue failure progress, when cyclic-load damages the microstructure of the blade and it create new crack nucleations. On the second stage, the existing micro-crack (by the damages or by the manufacturing) start growing and a "short" discontinuity arises. On the third stage, a "large" crack growing until the fourth and final stage, when the ultimate failure occurs. These stages are shown with their theoretical cycle number in Figure 10.

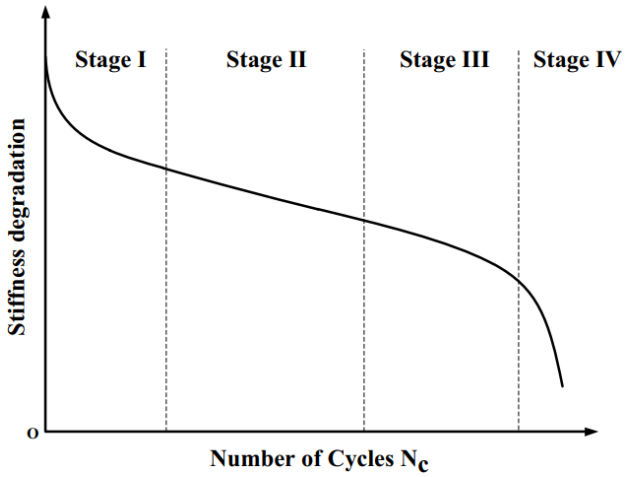


Figure 10.: Four stages of the fatigue failure process [18]

Depending on the material and the stress ratio, the critical number of cycles are changing. For some blade material an S-N curve (Wöhler curve), which is the alternating average stress against the number of load cycle shown in the next figure (Figure 11).

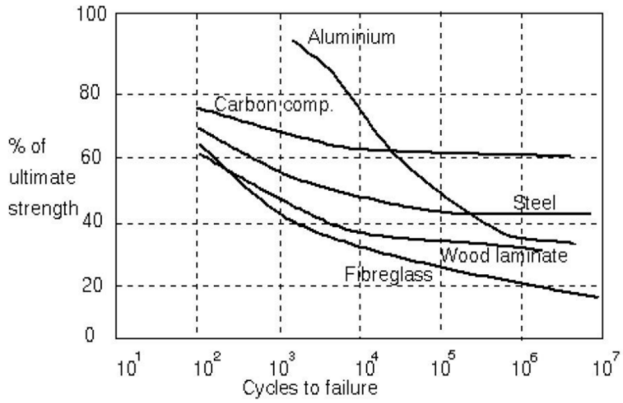


Figure 11.: S-N curves for blade materials [19]

In the previous figure, the ultimate strength was used as a failure parameter besides, other parameters can be used for stiffness degradation e.g. the dislocation density.

The blade structure has different material for a different purpose, the shear web usually made by aluminium or a highly alloyed lightweight steel. The airfoil skin is generally high-strength composite materials, such as fibres (glass-carbon, aramid-basalt, natural and hybrid composites) with thermosets (epoxies, polyesters, vinylesthers), thermoplastics or nanoengineered polymers matrix. Usually, adhesive bonding is carried out the connection between the shear web and the airfoil skin.

The fatigue of the wind turbine blades is a known failure process, Chen *et al.* [21] have a preliminary full-scale (52.3 m long) blade test, where they found during the physical tests the blade exhibited multiple failure modes e.g. laminate fracture, delamination, sandwich skin-core debonding, sandwich core failure, and shear web fracture. Lee *et al.* [22] presented an experiment and a finite element study in their paper, where they find a delamination failure at the end of the wind turbine blade root. Ghasemnejad *et al.* [23] was testing composite materials post-buckling failures.

Noda and Flay [24] were written a fatigue estimation program for HAWTs. Repetto and Torrielli [25] have a used simulation with a rainflow-counting algorithm for 50 years wind-induced fatigue loadings of a slender steel structure (lightning pole) which can be used for wind turbine tower. Repetto and Torielli's long-term simulation includes a mean wind speed combined with short-term wind fluctuation due to the turbulence. Jang *et al.* [26] presented a fatigue life prediction method, where Yang *et al.* developed a fatigue stress spectrum for fatigue critical locations and they have estimated the fatigue life of a blade.

CAD AND SIMULATION PARAMETERS

For having the aerodynamical loads, we had to create a 3D CAD model, where the first turbine rotor was mirrored and used for the second rotor and they rotated in opposite direction. The rotors were connected with a cylindrical nacelle. The diameter of the rotors was 1800 mm, for the root sections FFA-W3-211, to the middle sections S807 and for the tip section, NACA 63-215 airfoils were used. CAD geometry is shown in Figure 12. The

distance between the two rotors was 450 mm which is 0.25D distance (D denotes the rotor diameter).

The twist angle and the radius vs. chord length shown in Figure 13. For clarity, the cord length of the first section (at R = 0 mm) was 71.998 mm and the ratio is 0, which can see in the figure.

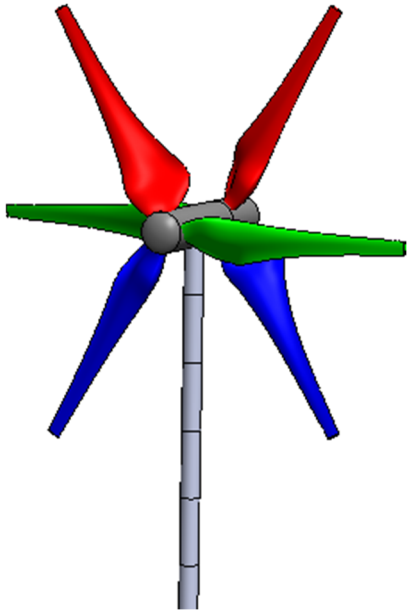


Figure 12.: CAD model of CO-DRWT (self-editing)

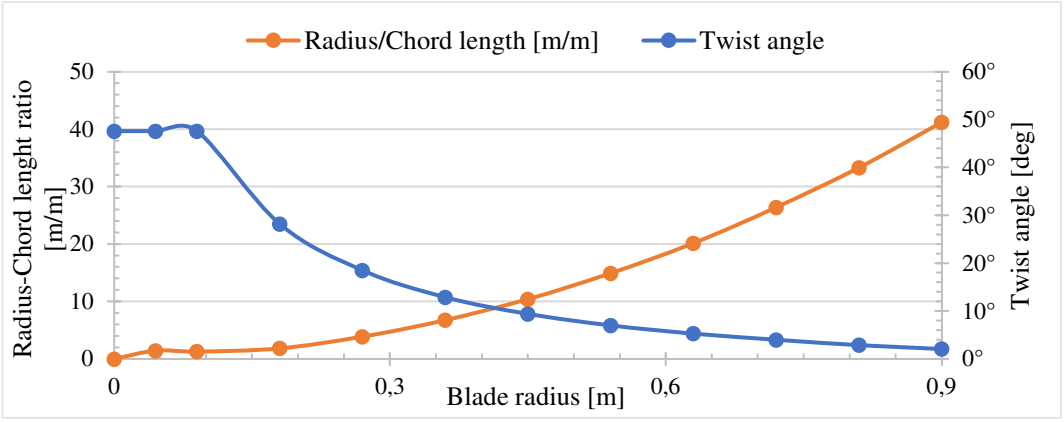


Figure 13.: Chord length and twist angle of the blade (self-editing)

The tower height was 2 000 mm with a constant 70 mm diameter. The external face of the tower was divided with 250 mm segments for evaluation purpose. The tower was halfway from each rotor.

For the simulation, Mentor Graphics' FLOEFD was employed with a rectangular computational domain, which is shown in Figure 14.

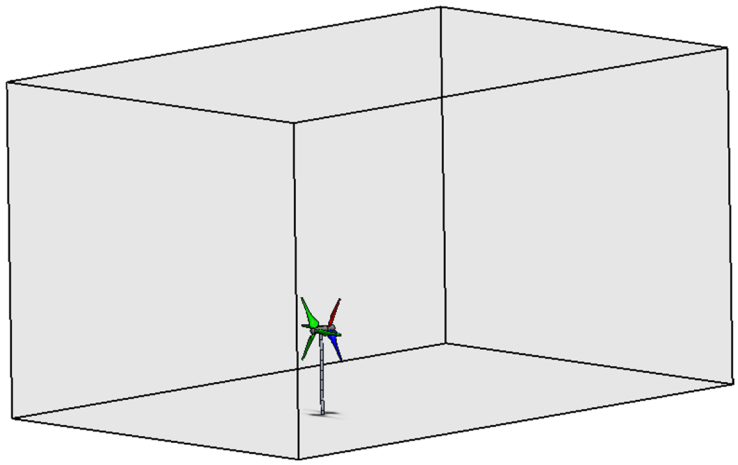


Figure 14.: Computational domain ()

The domain sizes were 5.5D x 4.65D x 8.35D. The domine started 3.225D before the centre of the tower and ended after the tower's centre with 5.125D. The bottom of the tower was aligned with the bottom of the computation domain. The centre of the tower was in the middle of the width of the domain.

The air entered at the beginning of the domain, the other five faces have an environment pressure boundary condition, where the air could enter and exit from the domain. The turbines rotational speed was 20 RPM.

K-ε turbulence model was used with a two-scale wall function based on the Van Driest model.

For computing resource efficiency, we started our simulation from steady-state as an initial condition, then we continued the study until 7.25 seconds. For meshing, we used a basic mesh for steady-state and the same for transient simulation until the 0.5 seconds, where the adaptive meshing finer automatically the initial grid till 1 500 000 elements.

For comparison purpose, we created an SRWT (single rotor wind turbine) model with the same simulation parameters.

RESULTS

After each simulation, we have a pressure distribution on the surfaces as well in the sections of the domain. The pressure distribution of the two configurations shown in Figure 15.

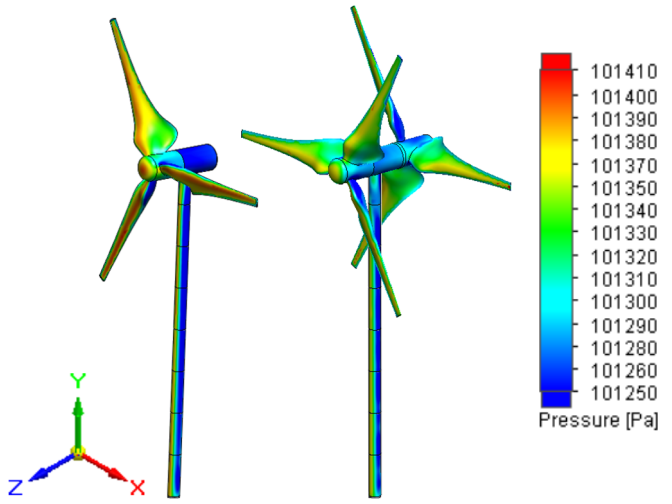


Figure 15.: Pressure distribution on the turbines (self-editing)

On the pressure distribution we can establish, the pressure on the front face where the flow reaches the body higher than on the back faces due to the dynamic pressure.

The velocity filed for steady-state cases shown in the next figures (Figure 16 and Figure 17). From both results we can establish, the wind velocities increase near the blades, and back to the wind turbines and the towers in the wake region, the velocities are slowed down. Also, we can state the CO-DRWT have a larger wake than the SRWT. In the transient simulations, the flow filed depend by the time, therefore the higher and lower velocities are fluctuating hence the turbulency and we can see the vortex shedding at the tip of the blades.

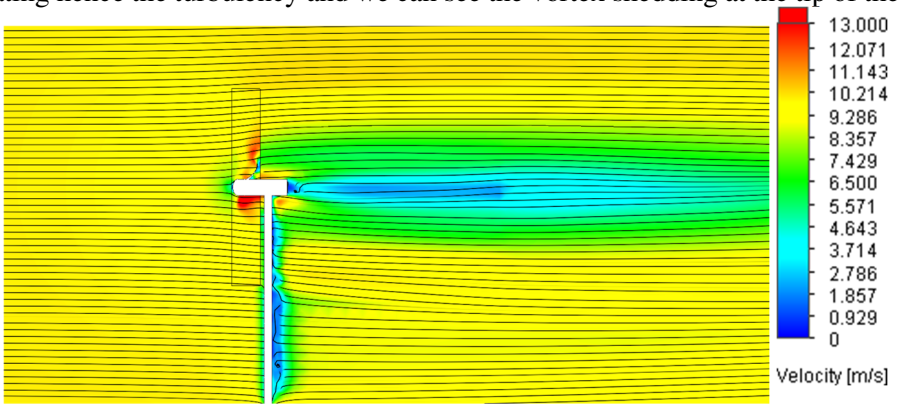


Figure 16.: Velocity distribution in the region of SRWT (from steady-state)

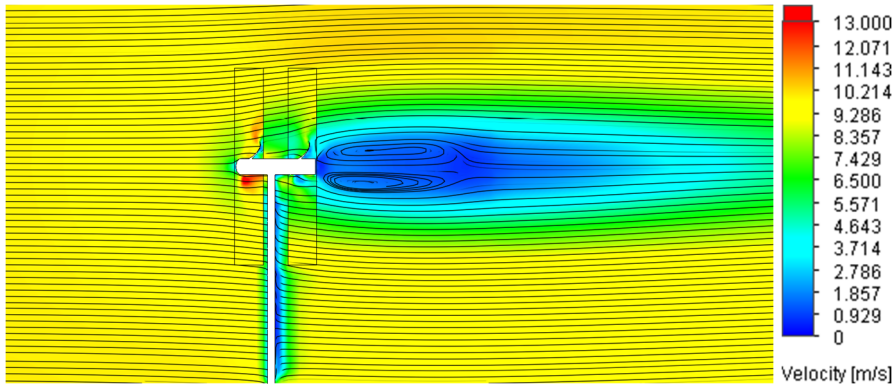


Figure 17.: Velocity distribution in the region of CO-DRWT (from steady-state)

The simulations started with an initial coarser mesh until 0.5 second where the adaptive mesher of the FLOEFD was finer the grid. After the adaptive re-meshing, the flow field should be relaxing for a couple of iterations, therefore we chose 1 second to start our evaluation.

For evaluation, we were numbering the blades and the tower's sections, which are shown in Figure 18. For evaluation, we choose the Blade 1 (marked with red colour) from each rotor and the tower's second and third section (marked with mustard yellow colour). The indications were likewise for SRWT.

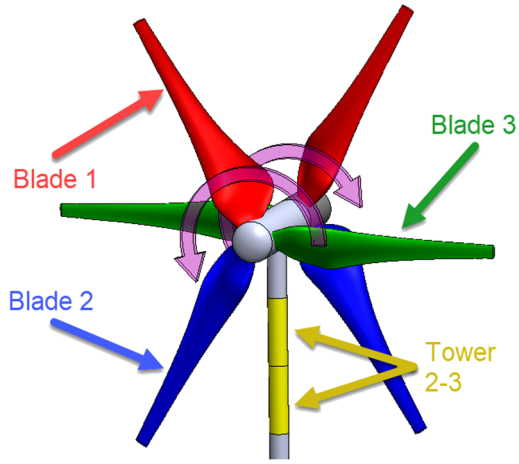


Figure 18.: The numbers of the blade and tower sections (self-editing)

In the next figure (Figure 19) the aerodynamical forces are shown on Blade 1.

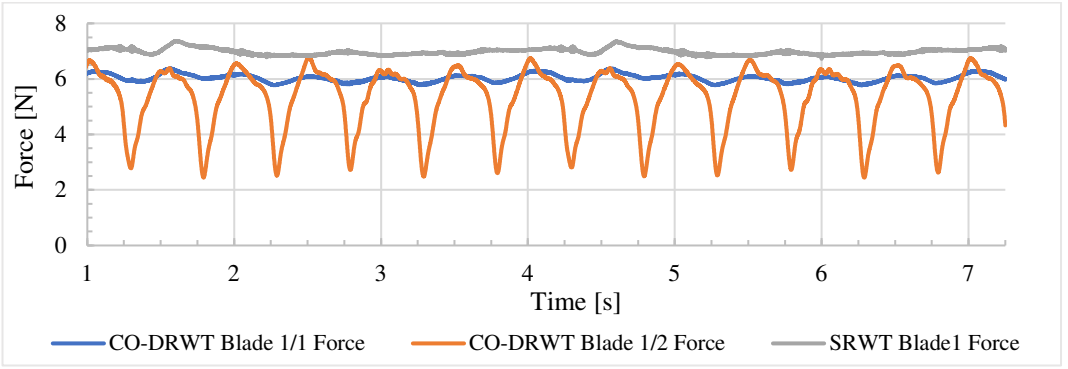


Figure 19.: Aerodynamical force on the surface of Blade 1 (self-editing)

Using the coordinate system of Figure 15, the X component of the aerodynamic forces on Blade 1 is shown in Figure 20.

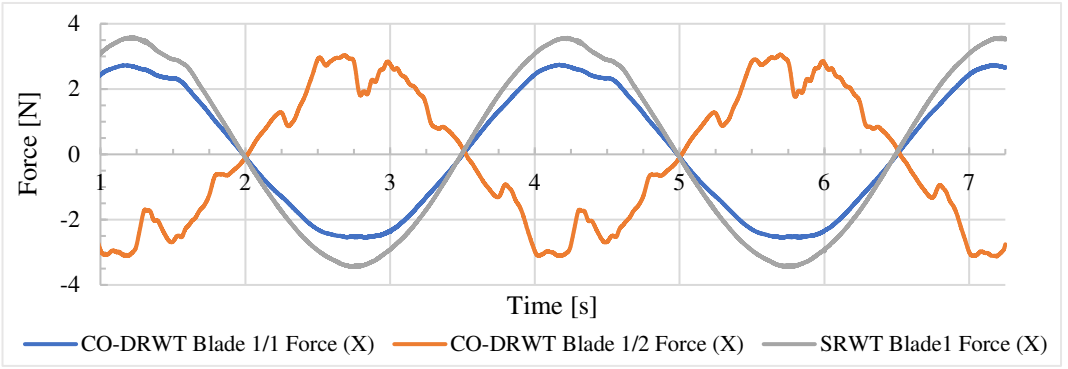


Figure 20.: X component of the aerodynamic force on the surface of Blade 1 (self-editing)

Using the coordinate system of Figure 15, the Y component of the aerodynamic forces on Blade 1 is shown in Figure 21.

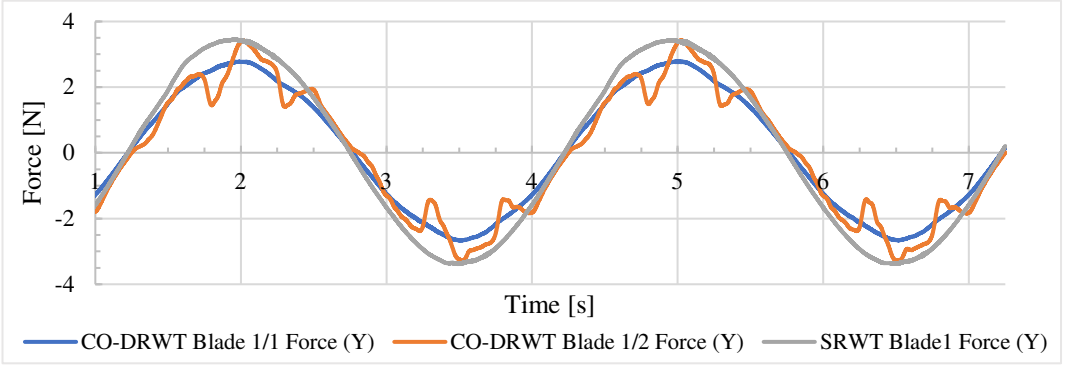


Figure 21.: Y component of the aerodynamic force on the surface of Blade 1 (self-editing)

Using the coordinate system of Figure 15, the Z component of the aerodynamic forces on Blade 1 is shown in Figure 22.

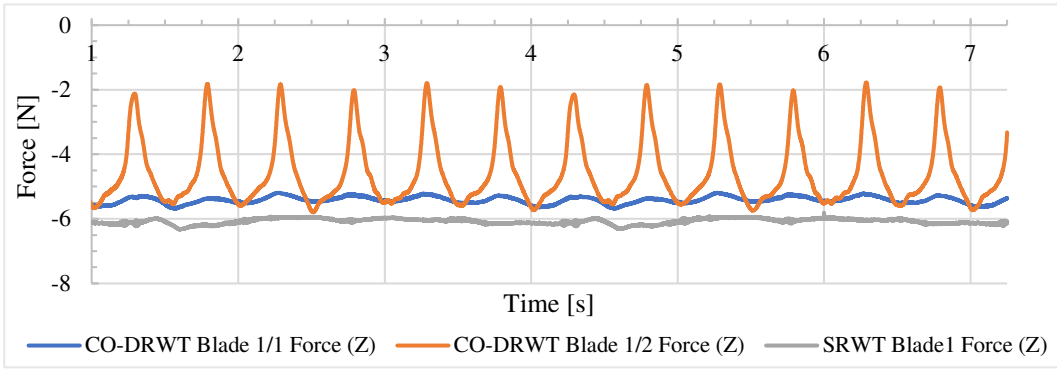


Figure 22.: Z component of the aerodynamic force on the surface of Blade 1 (self-editing)

The residual force on the tower's second and third sections shown on Blade 1 in Figure 23.

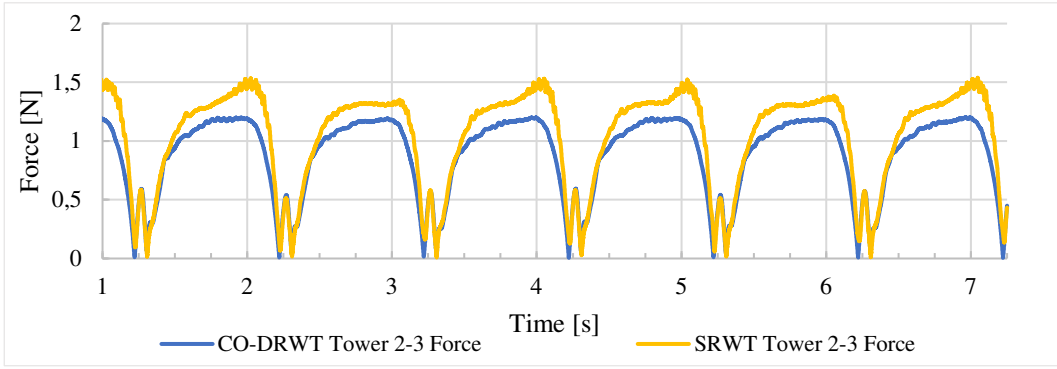


Figure 23.: The residual aerodynamical force on the tower's second and third sections (self-editing)

The component of the residual aerodynamical force on the tower's second and third sections is shown in Figure 24.

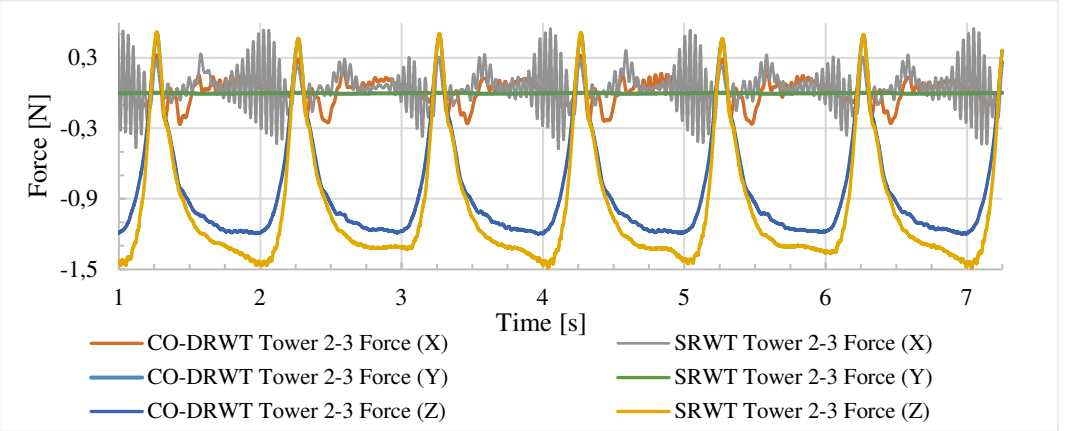


Figure 24.: The X, Y, and Z component of the aerodynamic force on the tower's second and third sections (self-editing)

Based on the results, the following can be stated:

1. On the blades of the SRWT's rotor, the aerodynamic force is higher, than on the blades of the CO-DRWT's first rotor (Blade 1/1), but it is less than the overall loads on the CO-DRWT's rotors (see Figure 19).
2. The tower's pass frequency is difficult to see but can be found on the parameters (e.g. aerodynamic force) of the SRTW's blades.
3. The rotational speed of the rotors was constant 20 RPM, the Blade 1 had to pass in front of the tower at 1.25 sec and further 3 sec later. The trace of the blade-tower interaction can be seen on the aerodynamical load diagrams 0.35 second later than as when it happened, due to the distance between the two surfaces. The Blade 1 of the CO-DRWT's blade has the trace of the blade-tower interaction, approximately in the same moment than the SRWT's first blade, but it is not noticeable, because the Z component of the aerodynamical load is sinusoidal and the minima of the sine are approx. in the same moment with the interaction of the two faces (see Figure 19 and Figure 22).
4. On the blades of the CO-DRWT's second rotor, the trace of the first rotor's blade can be found in every 0.5 seconds (see Figure 20, Figure 21 and Figure 22).
5. The X and Y components of the aerodynamical force on the blades are sinusoidal. The X component of the aerodynamical force on the CO-DRWT's second rotor is shifted with 90° than the first rotor's phase. The Y component of the aerodynamical force on the CO-DRWT's first and second rotor are in sync (see Figure 20, Figure 21).
6. The blade pass frequency can be seen in each second on the forces of the 2nd and 3rd sections of the tower (see Figure 23 and Figure 24).
7. The Z component of the aerodynamical load on the 2nd and 3rd sections of the tower resembled a trapezoid for SRWT and CO-DRWT. By the coordinate system (which

is shown in Figure 12) the Z component is negative in most of the time. When the blades pass in front of the tower the loads change their direction and it's peak value positive. The maximum value for each turbine approx. +0.45 N, the minimum values are near -1.1 N for the CO-DRWT and -1.4 N for the SRWT. The Y component of the aerodynamical load seems to be a random fluctuation, which changed its direction and its value increases near the blade-tower interaction. Contrary to our expectations, the frequency of the load fluctuation is faster to the SRWT, than for the CO-DRWT. The Y component peak values are between -0.042 and +0.5 N for the SRWT, and -0.027 and +0.03 N for the CO-DRWT. The X component of the aerodynamical load resembles a sawtooth wave for each turbine. The X components value for SRWT is between -0.0055 and +0.003 N, for CO-DRWT -0.0045 and +0.0035 N (see Figure 24).

8. For the SRWT the rotational frequency and the tower pass frequency are 1X, the blade pass frequency is 3X, where the X is the frequency of the rotational speed.
9. For the CO-DRWT, the first rotor's rotational frequency is 1X, the tower pass frequency is 3X, and the second rotor's rotational frequency is 6X.

Based on the statements, we reached the following conclusions:

a) As shown in the figures from Figure 19 to Figure 22, loads of the first rotors have the same characteristics just the magnitude is different. The Z component of the aerodynamical force on the first rotors' blade alternating around a non-zero mean force. The X and Y component of the aerodynamical force on the first rotors' blade is sinusoidal and it is alternating around a zero-mean force.
b) By Figure 22, the Z component of the aerodynamical force on the CO-DRWT's second rotor has a 6X frequency component, due to the first rotor's rotation as it was mentioned in Statement 9. The force is altering around a non-zero mean force and its minima are zero or a close zero values.
c) According to Statement 1, the aerodynamical loads of the SRWT are higher, therefore it will reach the fatigue limit earlier than the first rotor of the CO-DRWT.
d) As shown in Figure 20 and Figure 21, the blades of the CO-DRWT's second rotor have a primary load with 1X frequency, which is superimposed with a smaller 6X frequency load.
e) Due to the Conclusion b) and d), the blades of the CO-DRWT's second rotor are exposed to greater fatigue than the first rotor of CO-DRWT or the SRWT's rotor.

SUMMARY

In our study, we described the main loads of a wind turbine, then with a CFD software we were simulating a single rotor wind turbine (SRWT) and for a counter-rotating dual rotor wind turbine (CO-DRWT). Based on our results we were comparing the aerodynamical forces on the turbines and then we analysed the results in terms of the high-cycle fatigue.

In our results, we were able to detect the blade-tower interaction for the SRWT and the blade-blade interaction for the CO-DRWT. The second rotor of the dual rotor wind turbine has in the axial direction (Z component of the aerodynamical load) 6 additional load cycle during one rotation (see Figure 22) and in the two other directions (X and Y components of the aerodynamical load) have 6 smaller cycles which were alternating around the primary load (see Figure 20 and Figure 21). By the 6 additional load-cycle, the blades of the second rotor are exposed to have higher fatigue failure than the blades of the first rotor.

Based on the current and our previous studies [27, 28], a CO-DRWT has a shorter operating time due to fatigue, but at this time it is generating more electricity than an SRWT. The optimum between a shorter life with higher energy density and a longer life with lower energy harvesting capability could be one of the next study's subject.

REFERENCES

[1] Szlivka Ferenc, Molnár Ildikó, "*Víz- és szélenergia hasznosítás (Hydro and wind energy utilization)"*, Edutus Főiskola Kiadó, 2012, https://regi.tankonyvtar.hu/hu/tartalom/tamop412A/2010-0017_10_viz_es_szelenergia/index.html

[2] Nashtifan Windmills, http://historicaliran.blogspot.hu/2012/03/nashtifan-windmills.html (Access Date: 23. 09. 2019.)

[3] *"Blyth's Wind Turbine"*, https://upload.wikimedia.org/wikipedia/commons/1/13/James_Blyth%27s_1891_windmill.jpg

[4] *"Charles F. Brush Wind Turbine"*, https://media2.fdncms.com/clevescene/imager/tilting-at-windmills/u/zoom/2622441/cover-3.jpg

[5] BP, "*Statistical Review of World Energy"*, BP Statistical Review of World Energy, London (UK), p. 50, 2019, https://www.bp.com/content/dam/bp/business-sites/en/global/corporate/pdfs/energy-economics/statistical-review/bp-stats-review-2019-full-report.pdf

[6] *"Bizarre Wind Turbines",* https://cdn.trendhunterstatic.com/thumbs/urban-wind-turbine.jpeg

[7] Romańskia L., Bienieka J., Komarnickia P., Dębowskia M., and Detynab J., *"Estimation of operational parameters of the counter-rotating wind turbine with artificial neural networks",* Archives of Civil and Mechanical Engineering, **17**(4), pp. 1019-1028, 2017, https://doi.org/10.1016/j.acme.2017.04.010

[8] Gorban A. N., Gorlov A. M., and Silantyev V. M., "*Limits of the Turbine Efficiency for Free Fluid Flow",* Journal of Energy Resources Technology, **123**(4), pp. 311-317, 2001, https://doi.org/10.1115/1.1414137

[9] Corke T., Matlis E., *"Wind Turbine Performance, Control and Design - AME 40530 (lecture note)"*, University of Notre Dame, Notre Dame, Indiana, United States, 2018.

[10] Johnson D. A., Gu M., and Gaunt B., *"Wind Turbine Performance in Controlled Conditions: BEM Modeling and Comparison with Experimental Results"*, International Journal of Rotating Machinery, **2016**(3), pp. 1-11, 2016, https://doi.org/10.1155/2016/5460823

[11] Probst O., Martínez J., Elizondo J., and Monroy O., "*Wind turbines"*, *Chapter 5: Small Wind Turbine Technology,* IntechOpen, London, 2011, ISBN: 978-953-51-4506-6, https://doi.org/10.5772/643

[12] Cox K., *"Structural design and analysis of a 10 MW wind turbine blade"*, Deep Sea Offshore Wind R&D Seminar, Trondheim (Norway), 19. January 2012., https://www3.nd.edu/~tcorke/w.windturbinecourse/Watson-Ahumada.pdf

[13] Lin W., Xiongwei L., Lianggang G., Nathalie R., and Matthew S., *"A mathematical model for calculating cross-sectional properties of modern wind turbine composite blades"*, Renewable Energy, **64**, pp. 52-60, 2014, https://doi.org/10.1016/j.renene.2013.10.046

[14] Heo H., Ju J., and Kim D.M., *"Compliant cellular structures: Application to a passive morphing airfoil"*, Composite Structures, **106**, pp. 560-569, 2013, https://doi.org/10.1016/j.compstruct.2013.07.013

[15] Ovenden M., Wang Q., Huang S., Zhao W., and Wang S., *"Real-Time Monitoring of Wind Turbine Blade Alignment Using Laser Displacement and Strain Measurement"*, ASME J Nondestructive Evaluation, **2**(3), 2019, https://doi.org/10.1115/1.4043850

[16] Nagy A., Jahn I., *"Advanced Data Acquisition System for Wind Energy Applications",* Periodica Polytechnica Transportation Engineering, **47**(2), 2019, pp. 124-130, https://doi.org/10.3311/PPtr.11515

[17] Huszár P., *"UAV és földi szegmense közötti kommunikáció hatékonyságának javítása (Improving communication efficiency between UAV and its ground segment)"*, Repüléstudományi Közlemények, **31**(1), pp. 167–182., https://doi.org/10.32560/rk.2019.1.14

[18] Gao X., Koval G., and Chazallon C., *"A discrete element model for damage and fracture of geomaterials under fatigue loading"*, The European Physical Journal Conferences, **140**, 2017, https://doi.org/10.1051/epjconf/201714012018

[19] Ragheb M., *"Fatigue loading wind turbine"* https://mragheb.com/NPRE%20475%20Wind%20Power%20Systems/Fatigue%20Loading%20in%20Wind%20Turbines.pdf

[20] Mishnaevsky L., Branner K., Petersen N. H., Beauson J., McGugan M. and Sørensen, F. B.,, *"Materials for Wind Turbine Blades: An Overview"*, Materials, **10**(11), 2017, https://dx.doi.org/10.3390%2Fma10111285

[21] Chen X., Zhao W., Zhao X. L., and Xu J. Z., *"Preliminary failure investigation of a 52.3 m glass/epoxy composite wind turbine blade"*, Engineering Failure Analysis, **44**, pp. 345–350, 2014, http://dx.doi.org/10.1016/j.engfailanal.2014.05.024

[22] Lee H. G., Kang M. G., and Park J., "Fatigue failure of a composite wind turbine blade at its root end", Composite Structures, **133**, pp. 878-885, December 2015, https://doi.org/10.1016/j.compstruct.2015.08.010

[23] Ghasemnejad H., Occhineri L., and Swift-Hook D.T., *"Post-buckling failure in multi-delaminated composite wind turbine blade materials"*, **32**(10), pp. 5106-5112, 2011, https://doi.org/10.1016/j.matdes.2011.06.012

[24] Noda M., Flay R.G.J., *"A simulation model for wind turbine blade fatigue loads"*, Journal of Wind Engineering and Industrial Aerodynamics, **83**(1-3), pp. 527-540, 1999, https://doi.org/10.1016/S0167-6105(99)00099-9

[25] Repetto M. P., Torrielli A., *"Long term simulation of wind-induced fatigue loadings",* Engineering Structures, **132**, pp. 551-561, 2017, https://doi.org/10.1016/j.engstruct.2016.11.057

[26] Jang Y. J., Choi C. W., Lee J. H., and Kang K. W., *"Development of fatigue life prediction method and effect of 10-minute mean wind speed distribution on fatigue life of small wind turbine composite blade"*, Renewable Energy, **79**, pp. 187-198, 2015, https://doi.org/10.1016/j.renene.2014.10.006

[27] Hetyei Cs., Szlikva F., "*Axial Gap Optimisation of Half Diameter Shifted Counter Rotating Dual Rotor Wind Turbine*", Interdisciplinary Description of Complex Systems, **18**(3), pp. 389-399, 2020, https://doi.org/10.7906/indecs.18.3.9

[28] Hetyei Cs., Szlivka F., *"Rotor size optimisation of a counter-rotating dual-rotor wind turbine",* Biztonságtudományi Szemle, **2**(4), pp. 91-105, 2020. https://biztonsag-tudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/86/103

THE DEVELOPMENT AND BEGINNINGS OF THE HUNGARIAN LEGAL REGULATION OF PRIVATE SECURITY ACTIVITIES

A MAGÁNBIZTONSÁGI TEVÉKENYSÉG MAGYARORSZÁGI JOGI SZABÁLYOZÁSÁNAK KIALAKULÁSA ÉS KEZDETEI

FÁBIÁN Péter [1]

Abstract

A democratic market economy is inconceivable without the primacy of private property, without privately owned companies. The security and protection of private property and, in many cases, state property cannot be imagined without the existence of the private security sector. In Hungary, the change of regime in 1990 brought with it the market-based liberalization of the security sector, but in the following 8 years the sector was typically a "playground" of underworld interests without legal regulation. The law, passed in 1998, was outdated, worrying professionally and legally, and placed the legal regulations of a sector employing nearly 200,000 active workers on a misguided, misinterpreted legislative trail to this day. As a result, the sector still has the highest number of black jobs and financial crime to date. The current legislation is diverse, over-regulated, contradictory and without legal consequences on many issues.

Keywords

private property, private security, property protection law

Absztrakt

A demokratikus piacgazdaság elképzelhetetlen a magántulajdon primátusa, magántulajdonban lévő gazdasági társaságok nélkül. A magántulajdon és sok esetben az állami tulajdon biztonsága, védelme sem képzelhető el a magánbiztonsági ágazat megléte nélkül. Hazánkban az 1990-ben történt rendszerváltás magával hozta a biztonsági ágazat piaci alapú liberalizációját, azonban azt ezt követő 8 évben az ágazat törvényi szabályozás nélkül, jellemzően alvilági érdekkörök „játéktere" volt. Az 1998-ban elfogadott törvény már kihirdetésekor is idejét múlt volt, szakmailag és jogilag is aggályos, s a közel 200.000 aktív munkavállalót foglalkoztató ágazat jogi szabályozását a mai napig is tartó, téves, rosszul értelmezett jogalkotói nyomvonalra helyezte. Ennek következménye, hogy az ágazatban a mai napig a legmagasabb a fekete foglalkoztatás és pénzügyi bűncselekmények száma is szignifikáns. A hatályos szabályozás, sokrétű, túlszabályozott, ellentmondásos, számos kérdésben pedig jogi következmények nélküli.

Kulcsszavak

magántulajdon, magánbiztonság, vagyonvédelmi törvény

[1] fabianpeter@topcopgroup.com| ORCID: 0000-0003-0640-6557 | Founder / Alapító | Top Cop Group

BEVEZETÉS

A biztonság legáltalánosabb megközelítésben „egy háborítatlan, mindenféle támadó jellegű behatástól mentes állapot”. [1] Biztonság alatt hajlamosak vagyunk az „állam által biztosítandó fizikai biztonságot” érteni. [2] Ez a fajta biztonság azonban napjainkban egyre több veszélynek és fenyegetésnek van kitéve, és tényként kell elfogadnunk: az állam szervei egyedül már nem képesek e veszélyek és fenyegetések elhárítására. A magántulajdonra épülő piacgazdaság viszonyai között így megteremtődik az igény a magánbiztonsági tevékenységre. [3]

Közbiztonság és magánbiztonság, közrend és magánrend – nem ellentétes fogalmak, nem is vonható közöttük éles határvonal, és egyik a másik nélkül aligha létezhet. A 2005.évi CXXXIII. törvény is a közrend részeként határozza meg a magánrendet. Nemzetközi trend: az állam a hagyományosan közbiztonság körébe tartozó tevékenységek egyre szélesebb körét tekintve biztosít lehetőséget arra, hogy a polgárok és vállalkozások piaci alapon vásárolhassanak magánbiztonsági szolgáltatásokat. [4]

Magyarországon a szocialista viszonyok között – értelemszerűen – magánbiztonsági szolgáltatás nem létezett, és csak 1995-ben nyert polgárjogot a személy- és vagyonőri szakma. Jelen tanulmány annak áttekintésére vállalkozik, hogy miként alakult ki hazánkban a személy- és vagyonőri tevékenységre vonatkozó jogi szabályozás, továbbá bemutassa és értékelje az első törvényi szabályozást.

A SZEMÉLY ÉS VAGYONVÉDELEM MIBENLÉTE

A magánbiztonság – ilyenformán a személy- és vagyonőri tevékenység – alkotmányos alapjai az Alaptörvény V. cikkében találhatók. Eszerint „mindenkinek joga van törvényben meghatározottak szerint a személye, illetve a tulajdona ellen intézett vagy az ezeket közvetlenül fenyegető jogtalan támadás elhárításához”. [5] A jogos védelem intézménye a büntetőjogból ismert: „nem büntetendő az a cselekmény, amely a saját, illetve más vagy mások személye, javai vagy a közérdek ellen intézett, illetve ezeket közvetlenül fenyegető jogtalan támadás elhárításához szükséges”. [6] A védelemhez való jog a személy és a javak ellen intézett jogtalan támadás esetén is fennáll, és nemcsak a tulajdonost illeti meg. A normaszöveg ezáltal teremti meg a jogalapot a magánbiztonsági szolgáltatások igénybevételéhez. [7]

Az 1998. évi IV. törvény volt az, mely először lehetővé tette személy- és vagyonvédelmi vállalkozások alapítását. [8] Az Alkotmánybíróság a 3/2001. (I.31.) AB határozatában vizsgálta e törvény egyes rendelkezéseit, ennek kapcsán rámutatott arra, hogy „az állam, miközben megteremti az alkotmányos tulajdonjog védelme körében a tulajdon technikai értelemben vett védelmét, egyúttal arról is köteles gondoskodni, hogy ez más alapjog aránytalan sérelmét ne idézze elő”. [9] A magánszemélyek, gazdasági társaságok dönthetnek úgy, hogy megbízási szerződést kötnek biztonsági szolgáltatást nyújtó vállalkozásokkal. Ezek a vállalkozások azonban nem rendelkeznek sem az állami rendészet jogosítványaival, sem annak eszköztárával. Tevékenységüket a megbízóval kötött polgári jogi szerződés alapján, annak keretei között folytatják, és csak olyan és annyi jogosultsággal rendelkeznek, amilyen és amennyi jogosultsággal a megbízó rendelkezik. [10]

A személy-és vagyonvédelem célja a bűnmegelőzés, nem feladata a bűnüldözés. Tevékenysége alapvetően őrzésből és/vagy védelemből áll. Az őrzési tevékenység egy feltételezett jogellenes cselekmény bekövetkeztétől igyekszik megvédeni az őrzött személyt, vagyontárgyat, létesítményt, a védelmi tevékenység aktivitással jár, és a már megkezdett jogellenes cselekményt igyekszik megszakítani. Az őrzés-biztonsági tevékenység őrzési és védelmi tevékenységet is magában foglal, az élőerő mellett biztonságtechnikai eszközök igénybevételével. [11]

JOGTÖRTÉNETI ELŐZMÉNYEK 1998-IG

A rendszerváltást megelőzően személyvédelmi tevékenységről nem beszélhetünk, erre a magánszemélyek részéről – a rendőrség által biztosított védelmen túlmenően – igény sem volt. A pénz- és értékszállításról az állam gondoskodott, túlnyomórészt a Magyar Posta, kisebb részben a Magyar Nemzeti Bank révén. [12] A vagyonvédelemre – „a társadalmi tulajdon fokozottabb védelmére" – az üzemrendészeti tevékenység keretében nyílt lehetőség. [13]

Az üzemrendészet

A 14/1960. (III. 24.) Kormányrendelet előírta, hogy minden olyan vállalatnál, melynél a társadalmi tulajdon védelme érdekében szükséges, üzemrendészeti szervet kell felállítani. A szükségesség kérdésében a vállalat felett felügyeletet gyakorló miniszter, vagy pedig a fővárosi, megyei tanács végrehajtó bizottságának elnöke volt jogosult dönteni. Az üzemrendészeti szerv tevékenységét a vállalat igazgatójának irányítása alatt végezte. [14] Az üzemrendészeti szerv elsődleges feladata – a társadalmi tulajdon védelme – mellett gondoskodott a vállalat rendjének és biztonságának fenntartásáról, a munkafegyelem megszilárdításáról, és feladata volt annak megakadályozása, hogy bűncselekményt kövessenek el a dolgozók személyi tulajdona ellen. [15] Az üzemrendészeti szerv tagja csak nagykorú, büntetlen előéletű és feddhetetlen személy lehetett, aki a szolgálat ellátása során a hivatalos személlyel azonos büntetőjogi védelmet élvezett. [16]

Az üzemrendészeti szerv tagjának feladatait a 2027/1960. (III. 24.) Kormányhatározat szabályozta**.** Folyamatosan tájékoztatniuk kellett a vállalat igazgatóját, a felügyeletet gyakorló minisztérium illetékes szervét, valamint a rendőrséget. Az üzemrendészeti szerv vezetője irányította és felügyelte a polgári fegyveres őrség, a kapuszolgálat, az éjjeliőrök, valamint a tárgyőrzők, a motozók, a személyi kísérők munkáját. [17]

Azt, aki jogosulatlanul – például engedély nélkül, vagy a jogszabályban írt kötelezettségét megszegve – folytatott személy- és vagyonvédelmi tevékenységet, szabálysértés miatt vonták felelősségre. A rendőrség hatáskörébe tartozó szabálysértési eljárásban az elkövetővel szemben ötvenezer forintig terjedő pénzbírságot lehetett kiszabni. [18]

A közületi szervek rendészeti tevékenységét a 6/1988. (II. 12.) MT rendelet szabályozta, és az egészen 2000. január 31-ig hatályban is maradt. [19] A rendelet hatálya a költségvetési szervek és egyesületek mellett csak a gazdasági tevékenységet folytató jogi személyekre terjedt ki, így a betéti társaságokra és a közkereseti társaságokra nem. [19]

Üzemi rendészetet azoknál a közületi szerveknél lehetett felállítani, melyek védelmét a rendőrség jogszabályi rendelkezés hiányában nem volt köteles ellátni. [20]

A rendészeti szervet a közületi szerv vezetője irányította, közvetlenül vagy megbízott útján. A rendészek képzéséről a rendőrség gondoskodott. [21] Rendész munkakörben nagykorú, büntetlen előéletű, magyar állampolgárságú, a feladat ellátására egészségügyileg alkalmas személyt lehetett alkalmazni. Szakképesítésre vonatkozó követelményt csak a rendészeti vezető, illetve annál magasabb pozíció esetében írtak elő. A rendészeti dolgozó a közületi szerv tevékenységében nem vehetett részt, csak a rendészeti tevékenységgel nem összeférhetetlen munkavégzésre lehetett kötelezni (jellemzően leltárfelelős munkakört, tűzvédelmi, munkavédelmi feladatokat láttak el). Feladatköre rendkívül széles volt, a rendelet is csak példálózó jelleggel sorolt fel néhányat: például üzemek, raktárak, alapanyagok, termékek őrzése; sokszorosítógépek védelmére vonatkozó szabályok betartatása; rendkívüli esemény esetén azonnali intézkedés és a helyszín biztosítása; a dolgozók munkahelyre bevett személyes tárgyainak a védelme.

A rendész közfeladatot ellátó polgári őrnek minősült. Jogában állt – egyebek mellett – a munkahelyre belépők igazoltatása, az ittas személyek belépésének megakadályozása; alkoholszonda használata a gyaníthatóan ittas állapotban lévő egyénnél; járművek, csomagok, menetokmányok ellenőrzése. [22]

A személy- és vagyonvédelem kezdetei

Az 1980-as évek derekától egyre élénkült a gazdaság, sorra jöttek létre a különböző vállalkozások, köztük nagy számban olyanok is, melyekben külföldi polgárok is részt vettek. Megnövekedett az igény a vagyonvédelmi szolgáltatások iránt, ezeknek az igényeknek a rendőrség nem tudott eleget tenni, az üzemrendészet pedig nem biztosított megfelelő jogi kereteket. Ezt felismerve született meg a vagyonvédelmi tevékenység szabályait megállapító 24/1987. (VII.22) MT. számú rendelet, mely azonban a személyvédelmet és a magánnyomozói szolgáltatást kategorikusan megtiltotta. [23]

A magánbiztonsági tevékenység történetében a fordulatot a rendőrségről szóló 1994. évi XXXIV. törvény jelentette, mely 28. §-ában kimondta, hogy „a személy- és vagyonvédelmi tevékenység engedélyhez kötött szolgáltatás, amelynek során a vállalkozó a megrendelőt megillető jogok keretein belül, szerződés alapján létesítményt, telephelyet, területet, járművet, más dolgot őriz; rendezvényt biztosít; szállítmányt kísér, őriz, pénz- és értékszállítást végez; személyt véd; személy- és vagyonvédelmi szakképzési, tanácsadási, szakértői szolgáltatást nyújt; vagyonvédelmi műszaki rendszerek tervezését, telepítését, karbantartását végzi". [24]

Ezen túlmenően a rendőrségi törvény a 100. §-ának (1) bekezdése h) pontjában felhatalmazást adott a kormánynak, hogy alkossa meg a társas vállalkozás keretében folytatható személy- és vagyonvédelmi, valamint magánnyomozói tevékenységre vonatkozó átmeneti szabályokat. Ennek alapján született meg a 87/1995. (VII. 14.) Kormányrendelet. [25]

A kormányrendelet leszögezte, hogy a személy- és vagyonvédelmi szolgáltatás engedélyhez kötött szolgáltatás, melynek során a vállalkozó az alábbi tevékenységeket folytathatja „létesítményt, telephelyet, területet, járművet, más dolgot őriz; rendezvényt biztosít; szállítmányt kísér, őriz, illetve pénz- és értékszállítást végez; személyt véd; személy- és vagyonvédelmi szakképzési, tanácsadási, szakértői szolgáltatást nyújt; vagyonvédelmi műszaki rendszerek tervezését, telepítését, karbantartását végzi". [26]

Fontos kitétel, miszerint e tevékenységek folytatására csak a megbízót megillető jogok keretein belül, szerződés alapján volt lehetőség. Személy- és vagyonőri tevékenységet

csak a rendőrség által kiadott, személyre szóló igazolvány birtokában lehetett végezni. Igazolványt az a nagykorú, cselekvőképes, büntetlen előéletű magyar állampolgár kaphatott, aki belföldi lakóhellyel rendelkezett, valamint személy- és vagyonőri képesítést szerzett. [27] A rendelet kitért arra az esetre is, ha a rendőr a személy- és vagyonőrt a tevékenysége gyakorlása során szándékos bűncselekmény vagy a foglalkozása szabályainak megszegésével kapcsolatos szabálysértés elkövetésén éri tetten. Ekkor az igazolványt még ott, a helyszínen – átvételi elismervény ellenében – el kellett vennie, és köteles volt megküldeni az azt kiadó rendőrkapitányságnak, mely döntött az igazolvány visszaadásáról vagy bevonásáról. A rendelet leszögezte, hogy e döntésig az érintett nem folytathat személy- és vagyonőrzési tevékenységet. [28]

Azt, hogy a személyi és vagyonőri tevékenység folytatásához milyen szakképesítési követelményeknek kellett megfelelni, a 12/1995.(VIII. 18.) BM rendelet melléklete tartalmazta, a képzés és vizsgáztatás szabályait pedig elsőként a 38/1997. (VI. 27.) BM rendelet határozta meg. [29] Ez utóbbi szerint a személy- és vagyonőri oktatásra azt lehetett felvenni, aki tizennyolcadik életévét betöltötte, büntetlen előéletű, cselkevőképes és rendelkezik belföldi lakóhellyel. Az alapképzés időtartama háromszáz óra volt, ebből 180 óra elméleti és 120 óra gyakorlati foglalkozást kellett teljesíteni.

A rendeletet meghatározták azt is, hogy milyen diplomát, illetve szakképesítést lehetett személy- és vagyonőri képzettségként elfogadni. Ilyen volt például a jogi egyetemi diploma, a Rendőrtiszti Főiskolán szerzett diploma, a Rendőrtiszti Szakközépiskolában szerzett bizonyítvány, vagy éppen a kutyavezetői szakképesítés. [30]

Láthatjuk, hogy a szakképesítésre vonatkozó szabályok egyfelől kedveztek az egykori rendvédelmi dolgozóknak, akik a már korábban megszerzett végzettségük, képzettségük birtokában – az összeférhetetlenségi szabályokban meghatározott időtartam leteltét követően – minden további tanulmányi kötelezettség nélkül elhelyezkedhettek a magánbiztonsági ágazatban. Ugyanakkor, a mindenki más számára meghatározott képesítési feltételek nem voltak különösebben szigorúak, azokat az alacsony képzettségűek is könnyen tudták teljesíteni. E két tényezőnek köszönhetően egyfelől nagyon sok leszerelt rendőr indított személy- és vagyonvédelmi vállalkozást (vagy csatlakozott ilyenhez), másfelől pedig a végrehajtói pozíciókat jellemzően nyolc általánost végzett munkanélküliekkel töltötték fel. [31]

1998. június 1-jén lépett hatályba az 1997. évi CLIX. törvény, mely a fegyveres biztonsági őrzésről rendelkezett [32], majd pedig az 1998. évi IV. törvény, mely immár átfogó jelleggel igyekezett szabályozni a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenységet. [8] Ez utóbbi törvény hatályon kívül helyezte az átmeneti szabályokat megállapító 87/1995. Kormányrendeletet és 6/1988. MT rendeletet. Ezzel megszűnt az üzemrendészet, és lehetővé vált a vállalkozások számára, hogy piaci alapon vegyenek igénybe magánbiztonsági szolgáltatást. [33]

AZ 1998. ÉVI IV.-ES TÖRVÉNY

1998. május 1-jén lépett hatályba a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenységről szóló törvény (a továbbiakban: VSzVMt.), mely egyúttal a Személy-, Vagyonvédelmi és Magánnyomozói Szakmai Kamarára (a továbbiakban: Kamara) vonatkozó szabályokat is tartalmazza. Habár már a megszületésekor sok kritika érte, az vitathatatlan, hogy e törvény által nyert létjogosultságot a személy- és vagyonőri, illetve a magánnyomozói vállalkozói szolgáltatás. A továbbiakban – tárgyalt témámhoz igazodóan

– csak a személy- és vagyonőri tevékenységre vonatkozóan ismertetem a törvény rendelkezéseit, azzal, hogy e rendelkezéseket a magánnyomozói tevékenységre is alkalmazni kellett.

A jogalkotó kettős célt tűzött ki, egyfelől a közrend és a közbiztonság javítását, ezzel összefüggésben a bűnmegelőzés hatékonyabbá tételét célozta azáltal, hogy megteremti a hatálya alá tartozó szolgáltatások törvényességét. Másfelől, a szolgáltatások igénybe vevői, valamint a szolgáltatások gyakorlása során érintetté válók számára igyekezett garanciát nyújtani „személyhez fűződő jogai, vagyoni érdekei sérthetetlenségére irányuló igényeinek érvényesítéséhez". [34]

A személy- és vagyonvédelmi tevékenység folytatásának feltételei

A törvény hatálya alá tartozó tevékenységeket egyéni vállalkozóként és bármilyen gazdasági társasági formában lehetett folytatni. A fegyveres erők és a rendvédelmi szervek hivatásos állományú tagjai szolgálati viszonyuk fennállása alatt nem lehettek sem tulajdonosai, sem vezető tisztségviselői, sem pedig tagjai ilyen vállalkozásnak. [35] A személy- és vagyonőri, valamint a magánnyomozói tevékenység egyidejűleg, egy vállalkozás keretében is folytatható volt, más, a személy- és vagyonvédelemmel közvetlen összefüggésben nem álló gazdasági tevékenység azonban nem. [36]

A személy- és vagyonvédelmi tevékenység folytatásának két alapvető feltételét határozta meg a törvény: az egyik volt a kamarai tagság, a másik pedig a rendőrség által kiadott működési engedély. A rendőrség a vállalkozás számára akkor adta ki a működési engedélyt, ha az igazolta, hogy a személy- és/vagy vagyonőri tevékenységet személyesen folytató tagja (alkalmazottja, segítő családtagja) rendelkezik az erre jogosító igazolvánnyal. A természetes személy csak akkor végezhetett a törvény hatálya alá tartozó tevékenységet, ha az igazolványon kívül kamarai tagsággal is rendelkezett, a vállalkozásnak pedig nyilvántartásba kellett magát vetetnie a kamaránál. A kamarai nyilvántartásba vételhez igazolni kellett, hogy a vállalkozás rendelkezik a tevékenység folytatásához szükséges technikai és anyagi eszközökkel. A törvény feltételként írta elő a szolgáltatási felelősségbiztosítás meglétét is. [37] Ez a biztosításforma azonban csak a szerződésen belül okozott károk megtérítését garantálta, a VSzVMt. nem írta elő a szerződésen kívül okozott károk megtérítését, enyhítését szolgáló biztosítás-forma meglétét.

A rendőrség abban az esetben tagadta meg a működési engedély kiadása iránti kérelmet, ha a kérelmező egyéni vállalkozó vagy a vállalkozás vezető tisztségviselője büntetett előéletű; a kérelmezőt a törvényben meghatározott bűncselekmény (személy elleni erőszakos bűncselekmény, nem erkölcs elleni erőszakos bűncselekmény, hivatali bűncselekmény, hivatalos személy elleni bűncselekmény, terrorcselekmény, vagyon elleni bűntett) miatt elítélték, a mentesülési idő leteltéig; vagy pedig a kérelmező a megelőző két évben nyomozóhatósági jogkörrel rendelkező szervezet állományának volt a tagja. [37]

A tevékenység végzésére jogosító, személyre szóló igazolvány kiadásának feltételei a következők voltak: a kérelmezőnek büntetlen előéletű, nagykorú, cselekvőképes magyar állampolgárnak kellett lennie, aki belföldi lakóhellyel, és a tevékenység folytatásához szükséges szakképesítéssel rendelkezik, és nem folyik ellene büntetőeljárás három évi vagy annál súlyosabb szabadságvesztéssel fenyegetett szándékos bűncselekmény miatt. [38] Ha a kérelmező ellen három évi vagy annál súlyosabb szabadságvesztéssel fenyegetett bűncselekmény miatt volt folyamatban büntetőeljárás, a kérelem kiadását nem utasították el automatikusan, hanem annak elbírálását az ügy befejezéséig felfüggesztették. El kellett azonban

a kérelmet utasítani abban az esetben, ha a kérelmező korábban már rendelkezett igazolvánnyal, de azt a kérelem benyújtását megelőző két éven belül a törvényben írt kötelezettségek megszegése miatt bevonták. [39]

A tevékenységet ideiglenes igazolvány birtokában is meg lehetett kezdeni. Az ideiglenes igazolványt, mely hat hónapra szólt, az engedéllyel rendelkező vállalkozás azon tagjának (alkalmazottjának, segítő családtagjának) lehetett kiadni, aki az igazolvány kiadására előírt feltételeknek a szakképzettség kivételével megfelelt, és a szakképzést folytató intézménnyel már megkötötte a képzési szerződést. [40] A kiadott ideiglenes igazolványt öt éven belül csak egy ízben lehetett kiadni, érvényességét pedig nem lehetett meghosszabbítani. Az ideiglenes igazolvánnyal rendelkező személy jogosítványai korlátozottak voltak (például nem tarthatott magánál gumibotot, lőfegyvert), tevékenységét csak igazolvánnyal rendelkező személy irányítása és felügyelete alatt végezhette. [41]

A rendőrség feladat-és hatásköre

A rendőrség a kiadott engedélyekről és igazolványokról, valamint az azokkal kapcsolatos releváns tényekről (így a kiadás alapjául szolgáló adatokról, az adatváltozásokról, a visszavont engedélyekről és a bevont igazolványokról) nyilvántartást vezetett. A tevékenység feletti hatósági ellenőrzés ugyancsak a rendőrség hatáskörébe tartozott. Ennek keretében a rendőrség a nyilvántartásban szereplő adatok valódiságát, a tevékenység gyakorlásának jogszerűségét, a vállalkozó által naplózott adatokat vizsgálta, de a szerződés tartalmát nem ismerhette meg. [42] A személy- és vagyonvédelmi tevékenységre vonatkozó szerződést írásba kellett foglalni, és a megbízó nevét és címét a vállalkozó által vezetett nyilvántartásban és naplóban rögzíteni kellett. A rendőrség a nyilvántartásba és a – szerződést ténylegesen teljesítő személyek nevét is tartalmazó – naplóba az ellenőrzés során betekinthetett. [43]

A törvény rendelkezett a működési engedély és az igazolvány visszavonásáról, bevonásáról, illetve elvételéről. A visszavonás végleges, például akkor kerülhetett rá sor, ha az igazolvány tulajdonosát a bíróság jogerősen eltiltotta a foglalkozása gyakorlásától.

A bevonás ideiglenes, és meghatározott idő elteltével a bevont engedélyt, illetve igazolványt a jogosult visszakapta. Például, az eljárás végéig vonta be a rendőrség az igazolványt, ha a jogosult ellen három év vagy annál súlyosabb szabadságvesztés miatt indult büntetőeljárás.

Az igazolvány elvételére akkor kerülhetett sor, amikor a rendőr a foglalkozása gyakorlásával összefüggő szándékos bűncselekmény vagy a tevékenység törvényben rögzített szabályainak megszegésével elkövetett szabálysértés elkövetésén érte tetten a személy- vagy vagyonőrt. [44]

A személy-és vagyonőr tevékenységére vonatkozó szabályok

A személy- és vagyonőr – mondta ki a VSzVMt. – hatósági jogkörrel nem rendelkezik, és nem kelthet ezzel ellentétes látszatot (például hatóságra utaló formaruha, jelzés használatával). [45]

A törvény részletesen szabályozta a személyőr, illetve a vagyonőr feladatkörét, jogosítványait. A személyőr a megbízó személyi biztonságát védi fizikai és technikai eszközökkel, ennek során azt, aki a védett személy biztonságát fenyegeti, felszólíthatja kilétének igazolására, a jogsértő magatartás abbahagyására. A vagyonőr a megbízó közterületnek nem

minősülő létesítményét védi. Ennek érdekében a területre belépő vagy ott tartózkodó személyt felszólíthatja kilétének igazolására, a belépés céljának közlésére; ellenőrizheti a belépő járművét, csomagját, szállítmányát, felszólíthatja a szállítási okmányok bemutatására. A felszólításnak eleget nem tévők belépését megtagadhatja, illetve távozásra szólíthatja fel őket, a jogsértést elkövetőket pedig a jogsértés abbahagyására hívhatja fel. Ha a személy- és vagyonőr rendezvény biztosítását végzi, a rendezvényt zavaró, annak biztonságát veszélyeztető személyeket felszólíthatja kilétük igazolására, végső esetben pedig a rendezvény elhagyására. [46]

Amennyiben a kilétének igazolására felszólított személy a felszólításnak nem tesz eleget, a személy- és vagyonőr az igazoltatásra arra jogosult hatósági személyt kérhet fel. Mind a személy-, mind a vagyonőr jogosult a bűncselekmény elkövetésén tetten ért személyt elfogni, és a támadásra alkalmas eszközöket tőle elvenni, azzal, hogy az elfogott személyt köteles haladéktalanul átadni a rendőrségnek vagy az ügyészségnek, ha pedig ez nem kivitelezhető, köteles e szervek valamelyikét értesíteni.

A személy- és vagyonőr a törvényben meghatározott esetekben alkalmazhat „arányos mérvű kényszerítő testi erőt", így – többek között – a védett személy, illetve a pénz- és értékszállítmány biztonságát fenyegető támadás elhárítására, a védett létesítménybe való jogosulatlan belépés megakadályozására, a rendezvényt zavaró személy rendezvényről való eltávolítására. [47] Használhat fegyver- és robbanóanyag-kutató eszközt, ha az a megbízó közterületnek nem minősülő területére, objektumába belépő személyek ellenőrzése érdekében szükséges. A feladata ellátása során őrkutyát, vegyi eszközt, gumibotot, a vonatkozó jogszabályok betartásával lőfegyvert, gáz- és riasztófegyvert tarthat magánál, ám ezeket csak jogos védelmi helyzetben vagy végszükség esetén használhatja. [48]

A kamara feladat- és hatásköre

A Kamarára vonatkozó szabályokat az 1998. évi IV. törvény III. fejezete tartalmazta. Eszerint a Kamara önkormányzattal rendelkező köztestület, mely egyszerre lát el közfeladatot és tölt be általános érdek-képviseleti szerepet. Kényszertársulás, mivel kizárólag kamarai tagok gyakorolhatják személyesen a törvény hatálya alá tartozó tevékenységet.

Tagjai természetes személyek, a vállalkozásokról nyilvántartást vezet: előbbiek esetében a tagság, utóbbiak esetében a regisztráció alapvető feltétele a tevékenység végzésére való jogosultságnak. A Kamara szervezeti rendszere kétszintű, az országos központ mellett területi (egy vagy több megyére kiterjedő illetékességű) szervezetekből áll. [49]

Feladatai közé tartoztak – egyebek mellett – a következők: kidolgozza a kamara alapszabályát, a személy- és vagyonvédelmi tevékenység szakmai irányelveit, etikai szabályait. Kidolgozza a szakképzés és továbbképzés követelményrendszerét, közreműködik a vizsgáztatásban. Részt vállal a tevékenységi engedély kiadása iránti eljárásban, amennyiben előzetes nyilvántartásba veszi a személy- és vagyonvédelmi tevékenységet folytatni kívánó vállalkozókat, megvizsgálja, hogy rendelkeznek-e az ehhez szükséges, jogszabályban meghatározott feltételekkel, és igazolást állít ki erről.

Véleményt nyilvánít a szakmát érintő jogszabályokról, kezdeményezi a biztosító egyesület létrehozását. Etikai eljárást folytat le az etikai szabályokat megszegő tagjaival szemben. [50] Etikai vétség miatt a Kamara csak figyelmeztetést vagy kizárást alkalmazhatott. [51]

A törvény végrehajtási rendelete

Az 1998. évi törvény végrehajtásáról a 24/1998. (VI. 9.) BM rendelet gondoskodott. [23] Eszerint a tevékenység folytatására jogosító engedély, illetve igazolvány kiadására a vállalkozás székhelye szerinti, illetve a kérelmező lakhelye szerinti városi rendőrkapitányság jogosult. [52] A rendelet meghatározta a kérelmező által fizetendő igazgatási díj összegét, ez az engedély iránti kérelem esetében – tevékenységenként – húszezer forint, az igazolvány kiadása iránti kérelemnél pedig hatezer forint volt. [53] A személy-, illetve vagyonvédelmi tevékenységet folytató személy köteles a munkavégzés ideje alatt az igazolványt magánál tartani, és köteles azt felmutatni a hatóság, valamint az intézkedéssel érintett személy felhívására. [54]

A személy- és vagyonőri képesítés szakmai vizsgáinak szervezésére a munkaerő-fejlesztő és – képző központok, valamint – a rendelet 2. számú mellékletében felsorolt – rendőrségi oktatási intézmények bírtak jogosultsággal. A rendelet egyúttal meghatározta azt is, hogy melyek azok a végzettségek, melyek egyenértékűek e szakmai képesítéssel. Így személy- és vagyonőri képesítésként kellett elfogadni – egyebek mellett – az egyetemek állam- és jogtudományi karán, a Rendőrtiszti Főiskolán szerzett, Zrínyi Miklós Katonai Akadémián szerzett diplomát, a rendőri szakközépiskolában szerzett bizonyítványt. [55] A rendelet ugyanakkor a tevékenység gyakorlásához szükséges szakképzés tartalmi követelményeit nem állapította meg.

ÖSSZEGZÉS

Az 1998. évi IV. törvényt a hatályba lépésétől kezdődően számos kritika érte, több ízben kezdeményezett vizsgálatot a legfőbb ügyész, de maga a Kamara is javaslatot tett a törvény módosítására. Az Alkotmánybíróság mulasztásban megnyilvánuló alkotmányellenességet állapított meg, és a 22/2004. (VI. 19.) AB határozattal megsemmisítette a csomagellenőrzésre vonatkozó rendelkezést. A határozat indokolása szerint a VSzVMt. a személy- és vagyonőrök esetében nem szabályozta az adatkezelés és a titoktartás miként jét, nem határozta meg, hogy a csomagellenőrzésre milyen esetekben kerülhet sor, miként kell a belépéskor elvett tárgyakat ellenőrizni, és minderről miként kell az érintett személyt tájékoztatni. [56]

Bár megvalósult az ágazat első törvényi szabályozása, (megszületett a "vagyonvédelmi törvény") azzal kapcsolatosan nem csak jogi, hanem számos szakmai hiányosság is felmerült. Álláspontom szerint a legnagyobb probléma inkább az volt, hogy maga a jogszabály megalkotása 8 évet váratott magára, és mire elfogadásra került, már olyan mértékben változott az ágazat, hogy a törvényi rendelkezések nem csak felületesek, vitathatóak, de idejét múltak is voltak.

A fentieken kívül jól látható volt egy mai napig egyre szilárdabb -álláspontom szerint rossz- jogalkotói szándék térnyerésének első mozzanata, mely szerint a magánbiztonságot valami szervezetidegen formában, a rendészet, rendvédelem részeként, azzal összefüggő szabályait és képzését tekintve összekapcsolódó értelmezhetetlen üzleti tevékenységnek képzelik el. Ezt támasztja alá, hogy a tevékenységet kezdetben a Rendőrségről szóló törvényben próbálták szabályozni. Sikertelenül. Dolgozatomban való áttekintés és értelmezés álláspontom szerint azért nagyon fontos, mert ebben az időszakban alakultak ki és szilárdultak meg azok az értelmezési, dogmatikai tévedések, amelyek a mai napig az ágazat

fundamentális problémáit eredményezik. Újabb 8 évre volt szükség, hogy megszülessen az új törvényi szabályozás, amely nem csak a korábbi hibáit volt hivatott orvosolni, hanem előkészíteni az Európai Unió-s jogharmonizációt is. Bár 2006-ra az ágazatból sikerült a erőszakos bűnözői köröket kiszorítani, ez nem az ágazati törvény érdeme. Ellenben a szektor és kapcsolódó szabályok hiányosságára vezethető vissza, hogy időközben az őrző-védő cégek váltak a feketefoglalkoztatás és a pénzmosás melegágyává. Olvasatomban az 1998. évi IV. törvény totális jogalkotói téveszme volt és olyan szabályozási deficitet kezdett el megtermelni, amely azóta is csak gyarapszik, vakvágányra terelve az egyik legnagyobb munkavállalói létszámot foglalkoztató, nélkülözhetetlen ágazatot.

FELHASZNÁLT FORRÁSOK

[1] Boi L., „Pécsi Határőr. Tudományos Közlemények. 15. köt. Tanulmányok a "Biztonsági kockázatok - rendészeti válaszok" című tudományos konferenciáról 77-81.,” 2014. [Online]. Available: http://jog.tk.mta.hu/uploads/files/Koenyvek/A_vilag_mi_magunk_vagyunk.pdf .
[2] Jakab A, „Jogállamiság és terrorfenyegetés. Az alkotmány normativitásának és az életmentő kínzás megengedhetőségének kérdése.,” in *A világ mi vagyunk: Liber Amicorum Imre Vörös.*, Budapest, HVG-Orac, 2014, pp. 240-262.
[3] Christián L, A magánbiztonság elméleti alapjai, Budapest: Nemzeti Közszolgálati Egyetem Rendészettudományi Kar, 2014, p. 10.
[4] Christián L, A magánbiztonság elméleti alapjai, Budapest: Nemzeti Közszolgálati Egyetem Rendészettudományi Kar, 2014, p. 16.
[5] *Magyarország Alaptörvénye (2011. április 25.).*
[6] *2012. évi C. törvény a Büntető Törvénykönyvről.*
[7] Christián L, A magánbiztonság elméleti alapjai, Budapest: Nemzeti Közszolgálati Egyetem Rendészettudományi Kar, 2014, p. 20.
[8] *1998. évi IV. törvény a vállalkozás keretében végzett személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól, a Személy-, Vagyonvédelmi és Magánnyomozói Szakmai Kamaráról.*
[9] *3/2001. (I.31.) AB határozat.*
[10] Christián L, A magánbiztonság elméleti alapjai, Budapest: Nemzeti Közszolgálati Egyetem Rendészettudományi Kar, 2014, p. 22.
[11] Szabó A, „Az élőerős objektumőrzés és a tekintélyelvű vezetési stílus kapcsolata.,” *Hadmérnök XII. évf. 2017/3.* pp. 279-294., 2017.
[12] Kántás P, A közrend elleni jogsértések természetéről. Doktori értekezés., Budapest: Eötvös Lóránd Tudományegyetem ÁJK, 2007.
[13] *14/1960. (III. 24.) Korm. rendelet üzemrendészeti szervek szervezéséről.*
[14] *14/1960. (III. 24.) Korm. rendelet 1. §.*
[15] *14/1960. (III. 24.) Korm. rendelet 2. §.*
[16] *14/1960. (III. 24.) Korm. rendelet 3–4. §.*
[17] Szabó L. - Szigeti L, „Magánbiztonság, rendészet, rendvédelem.,” *Pécsi Határőr. Tudományos közlemények. 12. köt. Tanulmányok a "Rendészeti kutatások - A rendvédelem fejlesztése" című tudományos konferenciáról.,* pp. 407-411., 2011. http://www.pecshor.hu/periodika/XII/szabszig.pdf
[18] *17/1968. (IV. 14.) Korm. rendelet az egyes szabálysértésekről..*
[19] *6/1988. (II. 12.) MT rendelet a közületi szervek rendészeti tevékenységéről..*

[20] Munkaadók Lapja, „Üzemi rendészet," *Munkaadók lapja,* 1998/4. (1998. április 15.) https://munkaugyilevelek.hu/1998/04/uzemi-rendeszet/
[21] *6/1988. (II. 12.) MT rendelet 5 – 6. §.*
[22] *6/1988. (II. 12.) MT rendelet 7 – 10. §.*
[23] *24/1998. (VI. 9.) BM rendelet a vállalkozás keretében végzett személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól, a Személy-, Vagyonvédelmi és Magánnyomozói Szakmai Kamaráról szóló törvény végrehajtásáról.*
[24] *1994. évi XXXIV. törvény 28. § (1) bekezdés (közlönyállapot).*
[25] *87/1995. (VII. 14.) Korm. rendelet a vállalkozás keretében végzett személyes vagyonvédelmi, valamint a magánnyomozói tevékenység átmeneti szabályairól.*
[26] *87/1995. (VII. 14.) Korm. rendelet 1. § (2) bekezdés.*
[27] *87/1995. (VII. 14.) Korm. rendelet 3. §.*
[28] *87/1995. (VII. 14.) Korm. rendelet 8. §.*
[29] *12/1995. (VIII. 18.) BM rendelet a vállalkozás keretében végzett személy- és vagyonőri, valamint a magánnyomozói tevékenység végzéséhez szükséges szakképesítésről.*
[30] Csege Gy, „Magyarországi vagyonvédelem oktatás fejlődése és kilátásai a robantásos cselekmények kezelésének tükrében.," *Műszaki Katonai Közlöny XXV. évf.,* pp. 173-182, 2 2015. http://hhk.archiv.uni-nke.hu/downloads/kiadvanyok/mkk.uni-
[31] Galántai B, „A polgári társadalomvédelem társadalmi integrációjának dilemmái - avagy - hol tart a magánbiztonsági szolgáltatás," *Pécsi Határőr.Tudományos közlemények. 11. köt. Tanulmányok a "Quo vadis rendvédelem? Szabadságjogok, társadalmi kötelezettségek és a biztonság" című tudományos konferenciáról.,* pp. 249-280, 2010. http://pecshor.hu/periodika/XI/galantai.pdf
[32] *1997. évi CLIX. törvény a fegyveres biztonsági őrségről, a természetvédelmi és a mezei őrszolgálatról..*
[33] L. Christián, A magánbiztonság elméleti alapjai, budapest: Nemzeti Közszolgálati Egyetem Rendészettudományi Kar, 2014, p. 13.
[34] *1998. évi IV. tv. Preambulum.*
[35] *1998. évi IV. tv. 1–3. §.*
[36] *1998. évi IV. tv. 4. § (1) – (2) bekezdések.*
[37] *1998. évi IV. tv. 4. § (3) – (4) bekezdések.*
[38] *1998. évi IV. tv. 5. § (1) – (3) bekezdések.*
[39] *1998. évi IV. tv. 5. § (5) – (6) bekezdések.*
[40] *1998. évi IV. tv. 5. § (2) bekezdés, 6. § (1) bekezdés.*
[41] *1998. évi IV. tv. 6. § (2) – (3) bekezdések.*
[42] *1998. évi IV. tv. 7. §.*
[43] *1998. évi IV. tv. 10 – 11. §.*
[44] *1998. évi IV. tv. 8 – 9. §.*
[45] *1998. évi IV. tv. 12. § (1) – (2) bekezdések.*
[46] *1998. évi IV. tv. 14. §.*
[47] *1998. évi IV. tv. 15. § (3) bekezdés.*
[48] *1998. évi IV. tv. 15. § (4) – (5) bekezdések.*
[49] *1998. évi IV. tv. 21. § (1) – (3) bekezdések.*
[50] *1998. évi IV. tv. 23. § (1) bekezdés.*
[51] *1998. évi IV. tv. 36. §.*
[52] *24/1998. (VI. 9.) BM rendelet 1–2. §.*
[53] *24/1998. (VI. 9.) BM rendelet 3. §.*
[54] *24/1998. (VI. 9.) BM rendelet 6. §.*

[55] *24/1998. (VI. 9.) BM rendelet 8–9. §.*
[56] *22/2004. (VI. 19.) AB határozat II. 1.3.*

Egyéb források:

[57] Berek L, T. Berek és L. Berek, Személy- és vagyonbiztonság, Budapest: Óbudai Egyetem, 2016, p. 174.
[58] G. Arany, „Megint Kötelező lesz a kamarai tagság?," 12 03 2017. [Online]. Available: https://www.zaol.hu/gazdasag/megint-kotelezo-lesz-1825044/.
[59] L. Christián, „A magánbiztonság aktuális nemzetközi trendjei, rövid hazai helyzetértékeléssel," *Pécsi határőr. Tudományos közlemények, 16. szám* 15, 2016.
[60] G. Finszter, „Magánvállalkozások a biztonságért," *Belügyi Szemle,* pp. 5-10, 12 1998.
[61] Gyulavári T, „A gazdaságileg függő munkavégzés szabályozása. Kényszer vagy lehetőség?," *Magyar Munkajog. E-folyóirat., 2014/1*, pp. 1-25.13., 2014. http://hllj.hu/letolt/2014_1/01.pdf
[62] Németh Z, „Az élőerős személy -és vagyonvédelem jellemzői szociológiai kutatás alapján.," *Pécsi Határőr. Tudományos Közlemények. 11. köt. Tanulmánok a "Quo vadis rendvédelem? Szabadságjogok, társadalmi kötelezettségek és a biztonság" című tudományos konferenciáról.,* pp. 295-299., 2010.
[63] Szövenyi G, „Jogszabály változások hatása a magánbiztonságra," *Pécsi határőr. Tudományos közlemények. 12. köt. Tanulmányok a "Rendészeti kutatások - A rendvédelem fejlesztése" című tudományos konferenciáról.,* pp. 369-377., 2011.
[64] *2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól.*
[65] *2011. évi XXIV. törvény az Európai Rendőrségi Hivatallal, a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenységgel, a lőfegyverrel és a pirotechnikával kapcsolatos törvények jogharmonizációs célú módosításáról.*
[66] *2015. évi CCXXVI. törvény a közbeszerzésekről szóló 2015. évi CXLIII. törvény, valamint az azzal összefüggő törvények módosításáról.*
[67] *218/1999. (XII. 28.) Korm. rendelet az egyes szabálysértésekről.*
[68] *116/2018. (VII. 2.) Korm. rendelet a minimális vagyonvédelmi szolgáltatási rezsióradíj 2018. évi mértékéről.*
[69] *24/1987. (VII. 22.) MT rendelet a vagyonvédelmi tevékenységről és a magánnyomozás tilalmáról.*
[70] *20/2013. (V. 28.) BM rendelet a belügyminiszter ágazatába tartozó szakképesítések szakmai és vizsgakövetelményeiről, valamint egyes, szakmai és vizsgakövetelmények kiadásáról szóló miniszteri rendeletek hatályon kívül helyezéséről.*
[71] *36/2005. (X. 5.) AB határozat.*
[72] *1998. évi IV. tv. 2. §.*

USING ARTIFICIAL INTELLIGENCE FOR OBJECT DETECTION (FIRST PART)

A MESTERSÉGES INTELLIGENCIA FELHASZNÁLÁSI LEHETŐSÉGEI AZ OBJEKTUMFELISMERÉSBEN (ELSŐ RÉSZ)

KOLLÁR Csaba[1] – NAGY Barna[2]

Abstract

The dominance of artificial intelligence is becoming more and more important in everyday life and in the field of scientific discourses, and security technology and security science are no exception. In the first – theoretical – part of our study we deal with machine vision, the history of technical and information science of machine vision, neural networks, and the teaching of networks. In a separate section we discuss the common types of tasks in computer vision (image classification, object localization, object detection), as well as the hardware and development environment (Intel Neural Compute Stick, OpenVINO Toolkit, Raspberry Pi), through which we were able to implement the developments and their results, will be published in the next part of our study. We conclude our theoretical study with an introduction to the concepts of artificial intelligence, machine learning, and deep learning.

Keywords

security systems, artificial intelligence, computer vision, Intel Neural Compute Stick, Raspberry Pi

Absztrakt

A mesterséges intelligencia dominanciája a mindennapi életben és a tudományos diskurzusok területén is egyre jelentősebb, s ez alól a biztonságtechnika és a biztonságtudomány sem kivétel. Tanulmányunk első – elméleti – részében a gépi látással, a gépi látás technika- és információtudományi történetével, a neurális hálózatokkal, a hálózatok tanításával foglalkozunk. Külön részben értekezünk a gépi látás gyakori feladattípusairól (képosztályozás, objektum lokalizáció, objektum detektálás), valamint bemutatjuk azt a hardver- és fejlesztőkörnyezetet is (Intel Neural Compute Stick, OpenVINO Toolkit, Raspberry Pi), amelyik révén a tanulmányunk következő részében ismertetésre kerülő fejlesztéseket és annak eredményeit tudtuk megvalósítani. Elméleti tanulmányunkat a mesterséges intelligencia, gépi tanulás, mélytanulás fogalmainak ismertetésével zárjuk.

Kulcsszavak

biztonságtechnika, mesterséges intelligencia, gépi látás, Intel Neural Compute Stick, Raspberry Pi

[1] kollar.csaba@phd.uni-obuda.hu | ORCID: 0000-0002-0981-2385 | associate professor/egyetemi docens | Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

[2] nagy.barna@blx.hu | ORCID: 0000-0002-8101-1080 | Software Architect/szoftver architect | Blumenthal Consulting Kft.

BEVEZETÉS

Egy szervezet információbiztonságának megteremtése és fenntartása egyszerre több területre is feladatot ró. Ennek része az objektum- és területvédelem is, melynek célja, hogy illetéktelenek ne tudjanak fizikailag hozzáférni a különféle információtároló, -továbbító, vagy -feldolgozó eszközökhöz. A megvalósítás során védjük a védendő terület határfelületét a bejutásról, a belépési pontokat az illetéktelen átjutástól, a területen belül pedig keressük az illetéktelen mozgást, vagy egyéb, nem kívánatos tevékenységeket.

Ezeknek a tevékenységeknek az eszköztárából manapság már nem hiányoznak a technikai ellenőrzésű beléptető és a mozgást ellenőrző rendszerek sem. Az ellenőrző rendszerek gyakran tartalmaznak videómegfigyelést, mely egyrészt csökkenti a szükséges élőmunka mennyiségét, másrészt megsokszorozza annak hatékonyságát. Ezek a rendszerek azonban egyre inkább túllépnek a hagyományos megfigyelő szerepükön és egyre komplexebb feladatok végzésére vállalkoznak.

A gépi látás használatával nemcsak az ember (például fáradékonyságból, figyelmetlenségből eredő) hibáit küszöbölhetjük ki, hanem a biztonságtechnika területéről kimutató, üzleti vagy társadalmi célú alkalmazásra is lehetőség nyílik.

Példaként említhető az okos városok és okos falvak koncepciója, ahol az okos jelzőt részben a mesterséges intelligencia, a gépi tanulás, a gépi látás újfajta hasznosítása igazolja. A gépi látás segítségével olyan információk birtokába kerülhetünk, mint például a településre érkező és kilépő gépjárműforgalom nagysága, a gépjárművek típusa, vagy a településen tartózkodók demográfiai adatai (nem, életkor). Egy olyan kor veheti kezdetét, amikor nemcsak régi, hónapokkal, évekkel ezelőtt gyűjtött adatokkal rendelkezhetünk a településről, hanem gyakorlatilag egy azonnali pillanatképünk van az éppen most történő folyamatokról. [1]

A látogatószámlálás, nem- és kormeghatározás inkább üzletileg hasznosítható információ, de az arcfelismerés, a rendszámfelismerés vagy az objektumkövetés már a terület fizikai védelmét is szolgálja. [2]

Ezeknek a gépi látást használó feladatoknak van egy komoly problémája. Folyamatos és jelentős számítási kapacitást igényelnek, ami a végponti eszközökben, például egy videokamerában jellemzően nem áll rendelkezésre. A végponti eszközök gyakran csak az adatok digitalizálására és IP hálózaton történő továbbítására képesek. A gépi látást segítő neurális hálózatok (kellő sebességű) futtatása már meghaladja a képességeiket, így az egy központi szerverre marad (amennyiben fel van erre készítve a rendszer). Az már a jelenlegi rendszereknél is megállapítható, hogy a rendszer bővíthetőségét rontja, ha a végpontok „buták” és minden számítás a központi szerverre marad. Például, ha egy videokamera nem tud tömörített videojelet küldeni, akkor néhány példány könnyen elfogyasztja az infrastruktúrában rendelkezésre álló sávszélességet.

Az egyik lehetséges fejlődési irány az, hogy a végponti eszközök válnak egyre „okosabbá”. Ezek az eszközök lesznek képesek olyan gépi látást igénylő feladatokra, amelynek csak a végeredményét, a kimenetét továbbítják a központ felé.

Ehhez viszont szükséges, hogy a végponti eszközök képesek legyenek a gépi látás számításigényes feladatainak elvégzésére. Az Intel Corporation erre a feladatra fejlesztett

egy feldolgozó egységet (processing unit), mely a felhasználási köre miatt Vision Processing Unit (VPU) nevet kapta.

Írásunkban az vizsgáljuk, hogy hogyan valósítható meg az Intel kis teljesítményű eszközökbe szánt Neural Compute Stick 2 képi feldolgozó segítségével a gépi látás (Computer Vision – CV) két gyakori feladata, az objektumfelismerés és -azonosítás. Több környezetben, gyakorlati példákon vizsgáltuk az eszközt. Feldolgozó teljesítményét összevetettük más, általános célú processzorokkal (Intel CPU), így könnyebben meg lehet ítélni, hogy mekkora számítási teljesítménnyel bír a gépi látás feladatainak körében.

Tanulmányunk első része – ahogy arról már az absztraktnál is írtunk – a téma elméleti keretét vázolja fel. Mivel a mesterséges intelligencia és a kapcsolódó fogalmak tartalmukban és tartalmuk értelmezésében is gyorsan és folyamatosan fejlődnek, ezért nem találkoztunk egységesen használt fogalmakkal. Különösen igaz ez a magyar nyelvű szakirodalomra, mely gyakran nem találja a megfelelő és elfogadható kifejezést egy-egy új fogalomra. Ennek ellenére igyekeztünk mindig a magyar kifejezéseket használni, megadva annak az angol megfelelőjét is. Ettől csak akkor tértünk el, ha a magyar változat mindenképpen rontotta volna az érthetőséget.

A GÉPI LÁTÁS

A gépi látás (Computer Vision) egy olyan interdiszciplináris tudományterület, mely a számítógépek számára teszi lehetővé álló- vagy mozgóképek olyan magasszintű értelmezését, „látását", mellyel eddig csak emberek rendelkeztek. Fontos hangsúlyozni a magas szintet, mert a használt technológiáktól a háromdimenziós világunk egyfajta megismerését, feltárását várjuk el, úgy, hogy a rendszer bemenete gyakran csak kétdimenziós képek, illetve képek sorozata.

A terület pontos megértéséhez érdemes tudni, hogy az idegennyelvű szakirodalom megkülönbözteti a Machine Vision és Computer Vision fogalmakat, de a magyar nyelvben ugyanazt a kifejezést, a gépi látást használjuk mindkettőre. A fogalmak meghatározását nehezíti, hogy értelmezésük nem letisztult, gyakran szükséges azok definiálása a használatuk előtt.

A Machine Vision (MV) technológiákat – azok használói – általában a Computer Vision részterületének tekintik és jellemzően ipari, szabályozási területen hasznosítják. Fontos tulajdonságuk, hogy általában kontrollált körülmények (előre beállított fényviszonyok, ismert objektumok, jól definiált optikai jellemzők) között végeznek velük ipari vagy ipart támogató tevékenységeket. Elterjedésük a 90-es évekre tehető, amikor a különféle gyártósorok minőségbiztosítási feladatait segítették velük. [3]

A Computer Vision tudomány művelői szerint a két terület között a legfőbb különbség, hogy míg a Machine Vision-t inkább mérésre, értékelésre és az ehhez kapcsolódó vezérlésre, szabályozásra használják, addig a Computer Vision-t értelmezésre, látásra, de mindenképpen valami összetettebb, magasabb szintű tevékenységre. [4]

Tipikus MV felhasználási területek: a mérések, méretezések, pozícionálás, robotok irányítása, kódok olvasása, egyszerűbb jelenségek (pl.: anyaghibák) felismerése, míg a CV-t az alábbi problémakörökben használják: objektumfelismerés, objektumazonosítás, számlálás, nyomkövetés, mechanikai elemzések. [5]

A jövőben, várhatóan, a két terület egyre jobban össze fog fonódni, ahogy a CV technológiái egyre inkább megjelennek ipari környezetben is.

A gépi látás rövid története

A Computer Vision múltja messzire tekint vissza, bár igazán nagy népszerűség csak mostanában övezi. Ennek több oka van. Egyrészt a felhasznált matematikai elmélet is sokat fejlődött. Sikerült olyan területek találni, ahol a gyakorlatban is jól teljesít, valamint az egységi áron rendelkezésre álló számítási kapacitás is hatalmasat nőt az elmúlt évtizedekben.

Az egyik legfontosabb kezdeti mérföldkő Lawrence Roberts PhD tézise volt: „Machine Perception of Three-Dimensional Solids" (Lawrence, 1963), melyben háromdimenziós „információt" próbált kinyerni kétdimenziós képekből. Ő a tézisében még vonalas ábrákkal dolgozott, ám pár évvel később Seymour Papert az MIT AI laboratórium professzora már valós fényképek segítségével szeretett volna áttörést elérni.

A híres „Summer Vision Project" azonban kudarcba fulladt, és egyben rávilágított a CV nehézségeire. (Zbigniew, 2018) A projekt ambiciózus célkitűzését valószínűleg az is fűtötte, hogy a 60-as években nagyon felkapott kutatási téma volt a mesterséges intelligencia. Akkoriban többen azt vízionálták, hogy 25 éven belül a számítógépek olyan intelligensek lesznek, mint az emberek. És ahhoz, hogy ez megtörténjen a gépi látásnak is fejlődnie kellett.

A következő nagy lépés a CV fejlődésében David Marr könyve volt: „Vision: A computational investigation into the human representation and processing of visual information". David Marr egy új módszert vezetett be, mely „bottom-up" megközelítésként terjedt el. Ennek lényege, hogy a képfeldolgozás egy hierarchikus lépéssorozat, mely alulról építkezik. Első lépésben alacsony szintű feldolgozás hajt végre. Ilyenek például az éldetektálás, sarok detektálás, majd a következő lépésben már komplexebb műveletek következnek, míg végül a háromdimenziós modell megalkotása. (Gomes, 2000) [6]

Ez a fajta „alulról történő építkezés" mind a mai napig meghatározó elv a CV-ben, a deep learning rendszerek is így működnek.

Bár Marr könyve mérföldkő volt, kevés gyakorlati információt tartalmazott. Ezzel szemben Kunihiko Fukushima japán számítógéptudós, egy olyan neurális hálót alkotott – ez volt a Neocognitron (Fukushima, 1980) – mely már képes volt minták felismerésére. A hálózat több (különböző feladatot ellátó) rétegből állt és működését tekintve a mai konvolúciós neurális hálózatok (Convolutional Neural Network – CNN) ősének tekinthető. (Demush, 2019) [7]

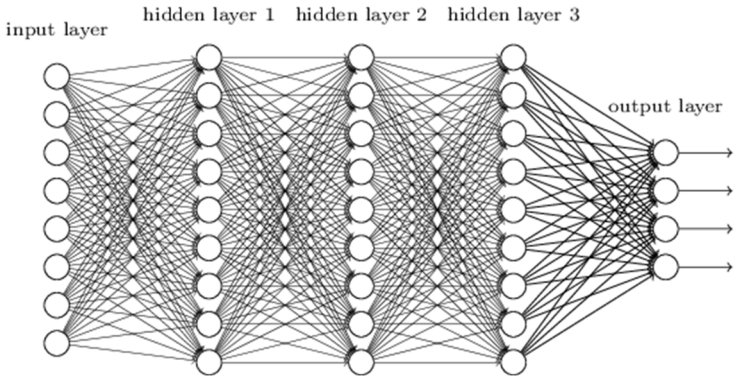
A 90-es évek végén a Computer Vision elfordult az objektumok háromdimenziós modellezése felől (ez volt a CV kutatások kezdeti célkitűzése) és az objektumok felismerése került a középpontba. 2006-ban született meg a Pascal VOC project, mely egyfelől standardizálta a képeket az objektum osztályozási feladatokhoz, másfelől egy workshop-okkal záruló versenysorozatot hirdetett (Visual Object Classes Challenge). A versenyben minden évben összemérték az induló objektumfelismerő metódusokat. (Demush, 2019) [7]

2010-ben indult a Pascal VOC-hez hasonló versenysorozat, az ImageNet Large Scale Visual Recognition Challenge (ILSVRC). A technológiai haladásnak köszönhetően a számok gyorsan nőni kezdtek. Amíg a Pascal VOC 2012-ben még csak 11.530 darab képpel és 20 osztállyal rendelkezett, addig az ImageNet több millió felcímkézett képpel és több

ezer osztállyal várta a jelentkezőket. A versenysorozat indulásakor még 26% körül volt az osztályozás hibaszázaléka, de ez gyorsan lecsökkent pár százalékra. Volt egy másik hozadéka is a versenynek: az objektumfelismerés témakörében egyeduralkodóvá tette a konvolúciós neurális hálózatokat (CNN).

A neurális hálózatok

A mesterséges neurális hálózat (Artificial Neural Network – ANN) egy olyan nagyszámú, hasonló típusú, önmagában egyszerű felépítésű, valamilyen gráfba szervezett műveleti elemekből (neuronok) álló hálózat, mely elosztott működésű információfeldolgozásra képes.



1. Ábra: A neurális hálózat egy lehetséges topológiája (forrás: neuralnetworksanddeeplearning.com)

A hálózatok lehetnek szoftveres és/vagy hardveres megvalósításúak. Közös bennük, hogy rendelkeznek tanulási fázissal (training phase), mely során eltároljuk bennük azokat a bemeneti adatokban rejtve meglévő információkat, melyeket a felhasználás során, később majd előhívunk (inference) belőlük. Ez a két fázis néha nem válik élesen szét, ilyenkor adaptív viselkedésű hálózatokról beszélünk, melyek az információ előhívása során is módosítják belső struktúrájukat, ilyenkor is tanulnak. [8]

Fontos hangsúlyozni, hogy a mesterséges neurális hálózatok tanítása során nem egyszerű adatrögzítés történik. Az előhívás során nem a megtanított adatokat kérjük vissza, és nem is a hálózat bemenetét várjuk vissza a kimeneten.

Ugyan a hálózatok tanítása felfogható egyfajta programozásként is, hiszen korábban nem létező információfeldolgozó képességgel ruházzuk fel a hálózatot, ez azonban nem azonos sem a procedurális programozással, hiszen nem egy algoritmust alkotunk. És nem azonos a deklaratív programozással sem, mert nem a problémát fogalmazzuk meg.

A neurális hálózatok tanítása során az ismert bemeneti (input data) és – felügyelt tanítás során – a kimeneti értékek (output data) alapján a hálózat belső változóit (súlyokat) változtatjuk annak érdekében, hogy majd az előhívás során, egy ismeretlen, de a korábbi bemenetekre a megfelelő módon hasonlító bemeneti mintára az elvárt, egyfajta generalizált választ adja a hálózat. [8] [9]

A hálózat bemenete és kimenete között általában valamilyen nemlineáris kapcsolat van. Ez a hálózati elemek nemlinearitásával magyarázható. A hálózatok képessége nagy

mértékben függ az elemek (neuronok) topológiájától, a neuronok tulajdonságától, a belső súlyok értékétől.

A hálózat ezen képessége egyébként meg is határozza, hogy milyen problémákra, feladatok használható a neurális háló. Azoknál a feladatoknál teljesíthet jól, aminek a megoldása nem, vagy csak nagyon nehezen, nagyon költségesen algoritmizálható. Továbbá azokban az esetekben, ahol a bemeneti adatok zajosak, zavarosan, nehezen specifikálhatók. Tipikusan ilyen feladatok a felismerési problémák és optimalizálási feladatok.

A hálózat ötlete a biológiai neurális hálózatokból ered. A terület úttörői úgy gondolták, hogy a természetes hálózatok mintájára létrehozhatók és működtethetők mesterséges neurális hálózatok is. Ennek eredményeképp a 40-es években jelentek meg az első tanulmányok és modellek, majd indult el a neurális számítástudomány a fejlődés útján.

1959-ben már gyakorlati alkalmazása volt a neurális hálóknak. A MADALINE egy több rétegű hálózat volt, melyet a telefonvonalak visszhangjainak kiküszöbölésére használtak. Később azonban elcsendesedtek a neurális hálók kutatásai. Ennek legfőbb oka az volt, hogy Marvin Minsky és Seymour Papert a Perceptrons című könyvükben (Minsky, 1969.) kimondták, hogy a perceptronok valójában csak nagyon kevés feladatban használhatók, mert csak lineárisan szeparálható osztályozási feladatok megoldására képesek. [8]

További oka a kutatások visszaszorulásának az volt, hogy a Neumann architektúrára épülő számítógépek népszerűsége és gyakorlati használhatósága nagyra nőtt, a neurális hálók általános alkalmazhatóságának ígérete azonban beteljesületlen maradt.

Újabb lendületet csak a 80-as években kapott a terület. Az 1982-ben tartott amerikai-japán közös neurális hálózat konferenciának köszönhetően az amerikaiak – attól félve, hogy lemaradnak a japánok mögött – jelentős erőforrást allokáltak erre a kutatási területre.

A Hopfield-háló (Hopfield, 1982.) [10] és a hálózatok tanításában jelentős backpropagation algoritmus publikálása visszafordította az érdeklődést a neurális hálózatok felé. Ennek eredményeképpen elterjedtek a többrétegű (multiple layered) hálózatok és megoldás született azok tanítására is. (Strachnyi, 2019.) [11]

A neurális hálózatok tanítása

A mesterséges neurális hálózatok egyik fontos jellemzője azok tanulási képessége. Ez alatt olyan adaptációs képességet értünk mellyel változtatni tudják viselkedésüket, működésüket. Természetesen – a tanítás során – ez a változtatás egy kívánt cél, egy elvárt működés irányába történik, amely, ha időben változik, akkor (további tanítással) tovább adaptálódhat a hálózat. A tanításoknak két fő típusa van (Horváth, 2006.) [8]:

- felügyelt tanítás (supervised learning) során a meghatározott bemeneti értékekhez az elvárt kimeneti értékek is rendelkezésre állnak. A tanítás során úgy módosítjuk a hálózat belső paramétereit (súlyokat), hogy a hálózat tényleges (aktuális) válasza minél inkább megegyezzen az elvárt válasszal. Ez a gyakorlatban nagy mennyiségű bemenet-kimenet páros (tanító mintapont) használatát jelenti, melyekkel iteratív módon, gyakran a tanítópontok ismételt felhasználásával közelítjük a kívánt eredményt.

- nem felügyelt tanítás (unsupervised learning) esetében csak bemeneti értékeink vannak, az elvárt kimeneti értékek nem állnak rendelkezésre. Nem tudjuk megmondani, hogy adott bemenetre mi a helyes válasz. Ebben az esetben nem előre meghatározott bemenet-kimenet párosok alapján várjuk el, hogy a hálózatunk valamiféle absztrakciós képességgel rendelkezzen, hanem csak a tanításban használt bemenetére tudunk olyan megkötéseket tenni, ami segítségével a hálózat működése kedvező irányba módosul. Például megkötések lehetnek, hogy a minták mennyire hasonlítanak egymásra, vannak-e a minták terében olyan tartományok, ahol sűrűsödnek, lehet-e a térben csoportokat találni. A nem felügyelt tanítású hálózatok által megoldott feladatokra gyakori példa a klaszterezés (csoportosítás).

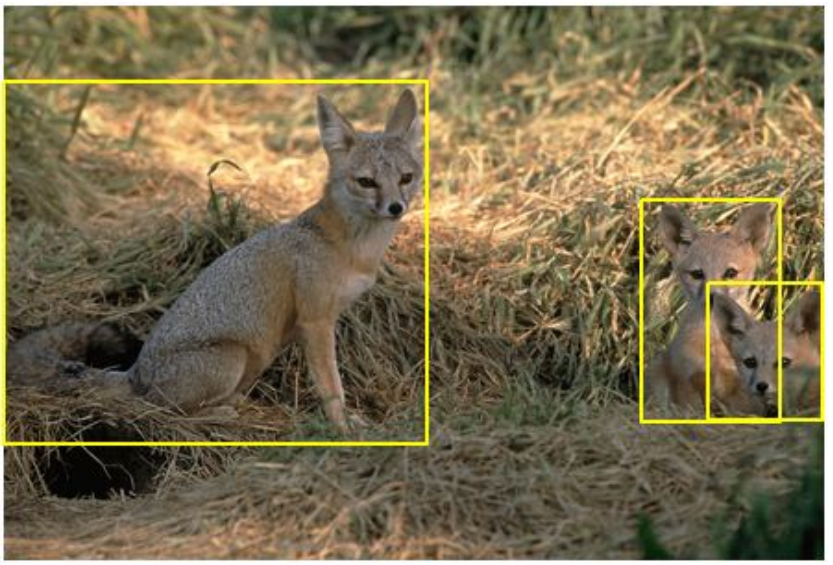
Megjegyezzük, hogy a felügyelt és nem felügyelt tanulás mellett egyes források megkülönböztetik még a megerősítő (visszacsatolásos) tanulást is, amelyiknek a lényege annak vizsgálata, hogy a kumulatív jutalom maximalizálása érdekében milyen cselekvési stratégiát kellene folytatnia az intelligens „ügynöknek", vagyis magának a gépi tanulónak az adott környezetben.

A gép látás gyakori feladattípusai

A gépi látás (Computer Vision) gyakorlati alkalmazásait jól definiálható feladatokra lehet osztani. Egy-egy összetett probléma megoldása gyakran bomlik ezekre a részfeladatokra, úgy, hogy a részfeladatokat láncba fűzik. Így egyik részfeladat megoldása (kimenete) egyben inputja (bemenete) a sorban utána következő feladatnak.

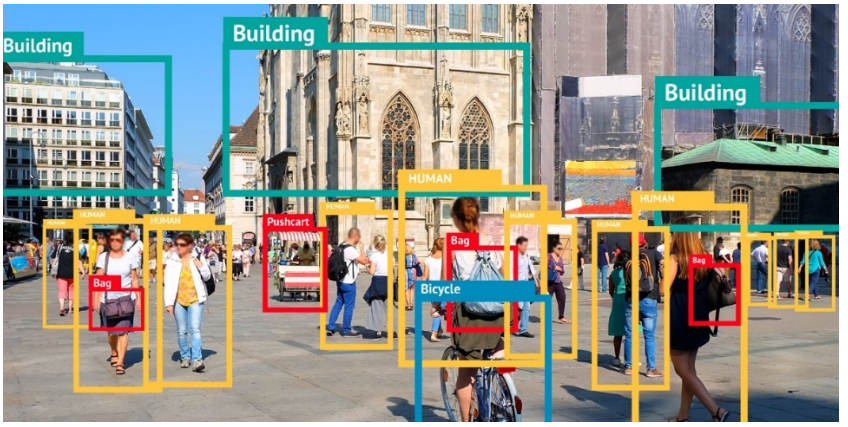
Képosztályozás. A képosztályozás (Image Classification, másképp Image Recognition) egy olyan eljárás, mely során egy osztályt vagy címkét rendelünk a bemenetként kapott képhez. Az eljárás a több előre meghatározott osztály közül megmondja, hogy mely, illetve melyek tartozhatnak a képhez. Ez a megvalósításokban általában azt jelenti, hogy kimenetként egy vektort kapunk vissza, melynek minden eleme egy osztályhoz tartozik, értéke pedig megadja, hogy milyen valószínűséggel tartozik a kép abba az osztályba. [12]

Objektum lokalizáció. Az objektum lokalizáció (Object Localization) az a művelet, mely során a hálózat megpróbálja az objektum (vagy objektumok) helyét meghatározni egy képen. A helymeghatározás során jellemzően az objektumot befoglaló téglalap paramétereit adja vissza a hálózat. [13]



2. Ábra: Object localization: a képen a megjelölt rókák (forrás: https://www.kaggle.com/c/imagenet-object-localization-challenge)

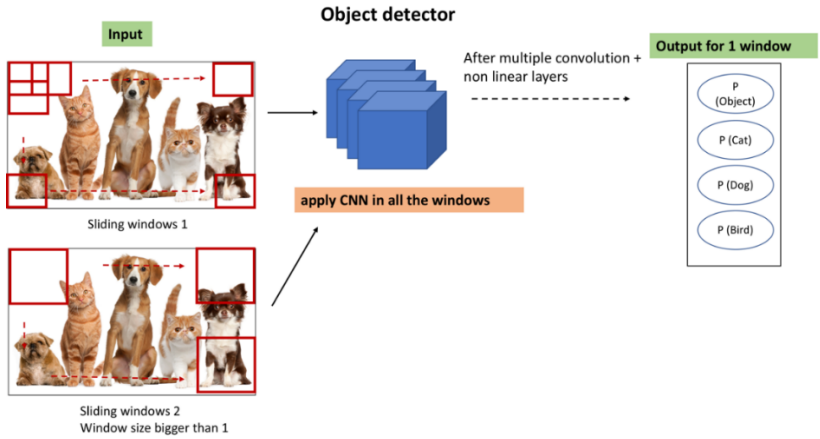
Objektum detektálás. Az objektum detektálás (Object Detection) egy összetett feladat, mely során a hálózat egyrészt lokalizálja (localization) az egyes objektumok helyét, másrészt azonosítja (image classification) azokat. Végeredményben a neurális hálózat a kimenete segítségével megmondja, hogy mely (jellemzően) téglalap által határolt területen mi található. Az azonosítás, jelen esetben image classification egy véges számú lista (label list) alapján történik, a hálózat a klasszikus image classification-höz hasonlóan csak azokat az objektumokat ismeri fel, amire tanítva lett. [12]



3. Ábra: Példa az objektum detektálás kimenetére. (forrás: https://bitmovin.com/object-detection)

Az object detection általában egyszerre több objektum lokalizációját és azonosítását végzi el. A hálózatokkal kapcsolatban az az elvárás, hogy egy többféle tárgyat tartalmazó képről (pl.: videómegfigyelő rendszer) mondja meg, hogy miket tartalmaz. [14]

A legelső megvalósítások az úgynevezett Sliding Window (**csúsztatott ablak**) megközelítést használták, mely során (alkalmazásfüggő módon) különböző alakú és méretű téglalapokkal pásztázták végig a képet, közben pedig vizsgálták az így kimetszett területet. Ez nagyon idő és erőforrásigényes megoldás volt, de megjelentek jobb megközelítések. [15]



4. Ábra: Csúsztatott ablak használata az objektumdetektálásban (forrás: https://towardsdatascience.com/evolution-of-object-detection-and-localization-algorithms-e241021d8bad)

A Region-CNN (R-CNN), majd később a Fast R-CNN módszerek nem pásztázták végig a képet, hanem generáltak számos potenciális régiót (region proposal) és azokon dolgoztak tovább. Ez gyorsabb volt, mint a sliding windows megközelítés, de még mindig túl lassú. Ezek a megvalósítások az úgynevezett két lépéses (two-step) megoldások voltak. Első lépésben történt a régió generálás, másodikban pedig az image classification.

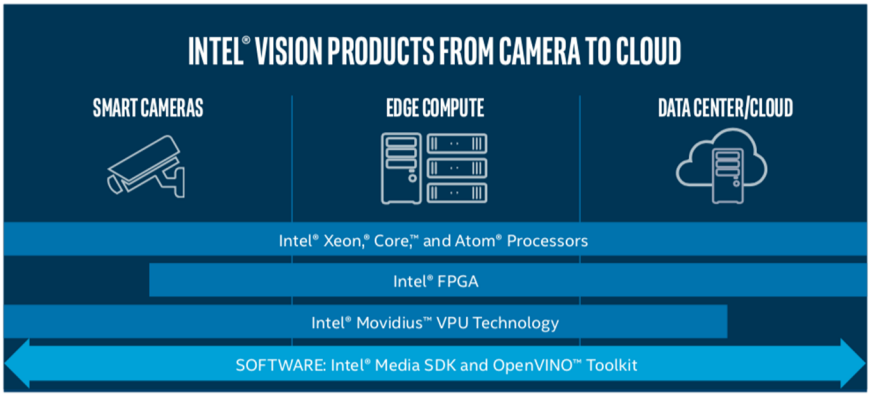
Jelenleg a leggyorsabb megoldást egylépéses (single-shot) objektum detektálás adja. Gyakran valós idejű képfeldolgozásra is alkalmasak, viszont sokkal pontatlanabbul. [16] Az egy lépéses hálózatra példa a YOLO (You Only Look Once) és az SSD (Single Shot Detection) hálózatok. Ezeket később részletezem.

AZ INTEL COMPUTER VISION MEGOLDÁSAI

Az 1968-ban alapított Intel Corporation nagy múltú hardvergyártó, amely követi (és lehetőségeihez képest alakítja is) az aktuális trendeket. Ezért látva a Computer Vision alkalmazások gyorsuló terjedését, a saját termékpalettáját is az ehhez kapcsolódó igényekhez igazította. Az Intel felismerte, hogy mind a mesterséges intelligencia (MI), mind az erre épülő gépi látás egyre kevésbé az adat- és számítóközpontok (felhők) kiváltsága. A fajlagos számítási kapacitás és a MI technológiák fejlődésével a végponti eszközökben (edge computers) is megjelennek. Ma már nem elképzelhetetlen, hogy egy okoskamera, drón, kisebb robotok vagy más IoT eszközök komolyabb gépi látást igénylő feladatokat is megoldjanak,

bár ez gyakran célhardverek segítségével történik. Az Intel ezekre a (részben hardveres) kihívásokra az alábbi termék csoportokkal válaszol:

1. Intel Xeon, Core és Atom processzorok
2. Intel FPGA
3. Intel Movidius VPU



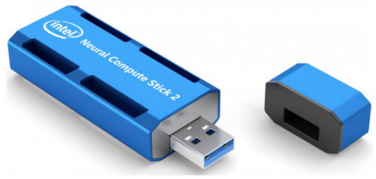
5. Ábra: az Intel termékcsaládjai Computer Vision feladatokra (forrás: intel.com)

Intel Movidius Vision Processing Unit (VPU)

Az Intel 2016-ban vásárolta fel a kaliforniai Movidius céget, mely speciális célprocesszorairól volt ismert. A vállalat Myriad nevű processzorai olyan kisfogyasztású célhardverek, melyek mesterséges intelligencia gyorsítóval (AI accelerator) rendelkeznek, és ezzel támogatják a gépi látást igénylő feladatokat. Ezt a processzor osztályt – hogy megkülönböztessék a többi célprocesszortól – VPU-nak, Visual Processing Unit-nak nevezték el.

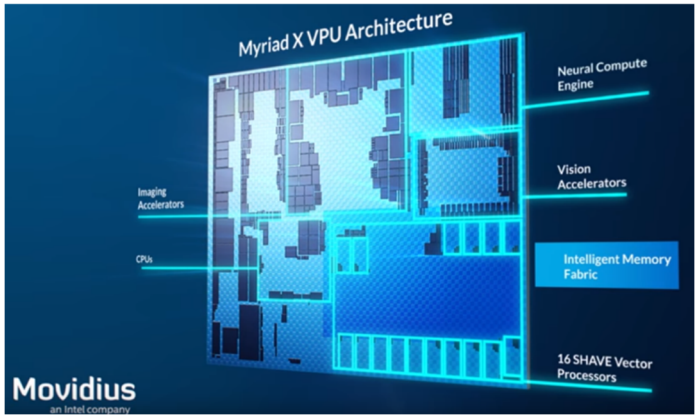
A hardverfejlesztő vállalatok érdekeltek abban, hogy termékeik kipróbálását, tesztelését és a velük való fejlesztést minél inkább támogassák. Ez a támogatás processzorok, mikrokontrollerek esetében általában fejlesztőlapot (development board) és fejlesztő környezetet (development environment) is jelent. Az Intel a Movidius VPU esetében több eszközzel is megjelent.

Az Intel Neural Compute Stick 2 eszköz. Az Intel vállalat Movidius VPU-t használó saját készítésű eszköze az Intel Neural Compute Stick 2 (NCS2), mely egy USB csatolókba illeszthető - ezen keresztül történik a kommunikáló és tápellátás – mesterséges intelligencia feladatokat támogató modul.



6. Ábra: Az Intel Neural Compute Stick 2 (forrás: intel.com)

Az NCS2 a Movidius™ Myriad™ X harmadik generációs VPU-t tartalmazza, mely akár 4 TOPS (Trillion Operations Per Second) teljesítményre is képes, csupán 1,5 W fogyasztás mellett. A VPU valójában nem egy darab processzor, hanem egy komplett SoC (System-On-Chip). [17]



7. Ábra: Myriad X VPU architektúra (forrás: tomshardware.com)

Az OpenVINO Toolkit

Az Intel a Computer Vision-t támogató eszközeinek (CPU-k, GPU-k, VPU-k, FPGA-k) szoftveres támogatását két szoftvercsomaggal segíti:

- Intel Media SDK
- OpenVINO Toolkit (Open Visual Inference and Neural network Optimization)

Az OpenVINO egy ingyenes csomag, mely közösségi támogatással és az Intel támogatásával rendelkező verzióban is elérhető. Az Apache Licence 2.0 licenccel letölthető Windows, Linux és macOS platformokra is. A csomag az alábbi főbb komponenseket tartalmazza [18]:

- Model Optimizer: egy parancssori modell konvertáló eszköz, mellyel ismert modellező eszközök modelljeit lehet olyan köztes formátumra (Intermediate Representation - IR) hozni, hogy azt az Intel eszköze is megértse
- Inference Engine: egy API, mely segítségével egy alkalmazásból is meghívható a neural stick.
- OpenCV könyvtár: az OpenCV közösségi verziója, újrafordítva az Intel eszközeire
- Model Downloader: parancssori eszköz, mellyel előre tanított modellek tölthetők le az eszközre.

Az Intel az OpenVINO szoftverfejlesztői csomaggal több hardvertípust is támogat, azonban ez a támogatás korlátos, azaz csak bizonyos generációk, bizonyos technológiákkal rendelkezők vannak a támogatottak listáján. Ennek az az oka, hogy az egyes hardvertípusokhoz külön-külön készült plugin, melyek csak bizonyos, elsősorban újabb utasításkészleteket vagy technológiákat használnak a neurális hálózatok futtatására.

(1) A processzorai közül az alábbiakat támogatja:
   a. Intel Xeon család: AVX és AVX512 utasításkészlettel
   b. Intel Core család: AVX2 utasításkészlettel
   c. Intel Atom család: SSE utasításkészlettel
(2) A grafikus gyorsítói közül:
   a. Intel HD Graphics
   b. Intel Iris Graphics
(3) FPGA kártyái közül:
   a. Intel Arria 10 FPGA 10
(4) VPU moduljai közül:
   a. Intel Movidis Myriad 2 lapkával szereltek
   b. Intel Movidis Myriad X lapkával szereltek

Ezzel a technológiai megkötések a processzorok fiatalabb generációkra szűkíti a támogatottak listáját. A támogatás hiánya azonban nem azt jelenti, hogy biztosan nem lehet futtatni hálózatokat. Csupán annyit jelent, hogy nem garantált, hogy a Model Optimizer eszköz olyan hálózatmodellre fog fordítani, aminek minden rétege megfelelően implementált a használt processzor utasításkészleteivel. [19]

Az általunk elérhető és a vizsgálatokban használt processzorok nem mindegyike van a támogatottak között, de a kiválasztott neurális hálózatok mégis futtathatók voltak rajtuk.

Számítógép	Processzor	Utasításkészlet kiegészítés	Hiányzó utasításkészlet
Mac mini "Core i5" 2.3 (Mid-2011)	Core i5 (I5-2415M) (2nd generation)	Intel® AVX	AVX2
MacBook Pro 13-Inch "Core i5" 2.6 Mid-2014	Core i5 (I5-4278U) (4th generation)	Intel® SSE4.1, Intel® SSE4.2, Intel® AVX2	

1. Táblázat: a használt Intel processzorok és utasításkészleteik (forrás: intel.com)

AZ EDGE COMPUTING

Az elosztott információs rendszerek architektúrájának egyik paradigmája, hogy a számítási és a tárolási kapacitás egy részét, közelebb hozzuk a végpontokhoz, melyek forrásai és/vagy fogyasztói lehetnek az adatoknak. Ezek a végpontok a rendszer alkalmazásától függően lehetnek személyi számítógépek, mobil eszközök, beágyazott eszközök, lokális szerverek, de az IoT világ erősödésével jelenthetnek szenzorokat (érzékelők), beavatkozókat (aktuátorok) vagy csak egyszerű felhasználói interfészeket.

A cél minden esetben az, hogy csökkenjen a rendszerek válaszideje, csökkenjen a szükséges sávszélesség, a szükséges adatkommunikáció mennyisége, vagy épp a központi szerverek erőforrásigénye. [20]

Megoszlanak a vélemények, hogy az edge computing körébe tartozik-e az az alkalmazási területe, mikor csupán a tárolási kapacitást hozzuk közelebb a felhasználás helyéhez.

Erre példa a 90-es évek vége felé megjelenő CDN-ek (Content Delivery Network), melyek az egyre növekvő mennyiségű és üzletileg egyre fontosabb adatok globális kiszolgálását végezték, illetve végzik most is. Ezek az adatok jellemzően statikus média tartalmak voltak: képek, videók, egyéb statikus webes tartalmak. Az alapelgondolás az volt, hogy a felhasználók által fogyasztandó ritkán változó, de nagy sávszélességet igénylő tartalmat, nem egy távoli központi szerverről szolgálják ki, hanem a felhasználó infrastuktúrájához közel létesített CDN szerverről. Ezek a szerverek egyfajta cache-ként működtek, főleg azokat a tartalmakat tárolták, melyek a hozzá tartozó felhasználók számára szükségesek voltak. Ezzel nemcsak az adatkommunikációt gyorsították, hanem az olykor jelentős távközlési költségeken is faragtak. [21]

A 2000-es évek elejére a webes alkalmazásokkal kapcsolatos elvárások megváltoztak. A weboldalak sokkal inkább dinamikus felépítésűek lettek. A felhasználói interakciók száma, melyeket már nem lehetett statikus tartalommal kiszolgálni megnőtt. Ez azt eredményezte, hogy az edge computing fejlődésével nem csak a statikus tartalmat tárolták közel a felhasználóhoz, hanem a dinamikus tartalomért felelős üzleti logikát is. Az így létrejövő distributed application service-ek, már a számítási kapacitást is közelebb vitték a felhasználás helyéhez. (Davis, 2004)

Az edge computing-nak a következő nagy lökést az IoT megjelenése adta. Az egyes végponti eszközökben lévő szenzorok, aktuátorok, vagy maguk a processzorok folyamatosan kommunikálnak a külvilággal. Ez a kommunikáció jelenthet nagyon kevés adatot pl. egy hőmérsékletmérő szenzor esetében, és igényelhet jelentős sávszélességet pl. egy videokamera esetén. [22]

Ez az adatfolyam általában valamilyen feldolgozást igényel, mielőtt tárolásra kerül vagy egyéb üzleti logika fut le a hatására. Ez a feldolgozás lehet egyszerű adattömörítés, szűrés vagy más komplexebb feladat.

A hálózatba kötött IoT eszközök száma egyre nő, az adatcenterek, illetve egyéb szerverek felé irányuló adatfolyam mind nagyobb sávszélességet igényel, ráadásul a feldolgozásuk is (a növekvő üzleti elvárások miatt) egyre erőforrásigényesebb. Ez már kisebb hálózatok esetén is könnyen kapacitásproblémákhoz vezethet, de az edge computing megoldást kínál erre a problémára.

A fajlagos számítási kapacitás egyre olcsóbb, így nemcsak a nagy szerverközpontok teljesítménye nőhet, hanem a végpontok is egyre intelligensebbek lehetnek. Az intelligens végpontok sok olyan előfeldolgozást el tudnak végezni, mellyel mind a hálózati infrastruktúrát, mind a központi gépeket tehermentesíteni tudják. Itt a hangsúly gyakran a hálózati kapcsolaton van. Egy videókamera például a nyers videó stream helyett tömörített streamet is küldhet, sőt megoldható, hogy csak akkor küldjön képet, ha mozgást is érzékelt. Ezzel már jelentős adatmennyiséget tud megtakarítani, de még tovább fejleszthető, hogy csak akkor küldjön képi információt, ha nem ismerte fel a látószögébe került személyt vagy tárgyat. Ez utóbbi már komolyabb computer vision (gépi látás) feladat, melyet a mai eszközök mesterséges neurális hálózattal végeznek. [20]

Az Intel Corporation hardver tervező és gyártó vállalat természetesen látja az edge computing kihívásait és saját termékpalettáját is ehhez igazította. Ennek egyik eleme a

Computer Vision területére fejlesztett Movidius VPU egysége, mely a gépi látást igénylő feladatokat segíti edge eszközökben.

AZ INTEL NEURAL COMPUTE STICK 2 HASZNÁLATA EGY EDGE COMPUTING DEVICE ESZKÖZBEN

A Movidius VPU működésének vizsgálatához egy népszerű egykártyás számítógépet a Raspberry Pi-t választottunk. A miniszámítógép teljesítményét, hardveres interfészeit és fogyasztását tekintve megfelel egy IoT eszköznek.

Környezet, számítógép	USB feszültség	Energiafogyasztás	Áram	USB feszültség	Energiafogyasztás	Áram
	idle[3]			peak[4]		
Raspberry Pi3	5,040V	0,594W	118mA	4,943V	3,041W	615mA
MacMini 2011	5,073V	0,613W	121mA	4,917V	3,136W	637mA

2. Táblázat: A fejlesztés során használt eszközök fontosabb paraméterei

Az egykártyás számítógép (single-board computer – SBC) modelljei közül a Raspberry Pi 3B vett részt a vizsgálatunkban, amely az alábbi főbb paraméterekkel rendelkezik:

Modell	Raspberry Pi 3B
Main chip	Broadcom BCM2837 - ARM core (64 bit) - VideoCore IV (32 bit)
Memória	1024MB SDRAM (shared with GPU)
USB interfészek	4x USB 2.0
Wifi (internal)	b/g/n single band 2.4 GHz
Háttértár	Micro SD csatlakozó
Tápellátás	5V DC power input
Operációs rendszer	Raspbian GNU/Linux 10 (buster) (release date: 2020-02-13)

3. Táblázat: A Raspberry Pi 3B főbb paraméterei (forrás: https://www.raspberrypi.org/products/raspberry-pi-3-model-b)

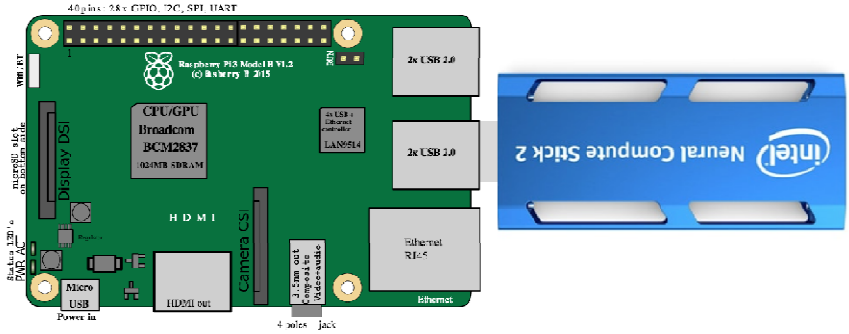
A Movidius VPU-t tartalmazó kártyák közül az Intel saját termékét választottuk, az Intel Neural Compute Stick 2-t (NCS2), mely az alábbi főbb paraméterekkel rendelkezik:

Modell	Intel Neural Compute Stick 2
VPU	Intel® Movidius™ Myriad™ X

[3] Nyugalmi (alap)állapot
[4] Performancia teszteknél mérték értékek

VPU nums	1x
Processor number	MA2485
Memory	4Gbit DDR3 (1600 MHz)
USB interfész	USB 3.1
Model data type	half-precision floating point (FP16)

4. Táblázat: Az Intel Neural Compute Stick 2 főbb paraméterei (forrás: intel.com)



8. Ábra: A Raspberry Pi[5] és az Intel Neural Compute Stick 2[6] konfigurációja

Az NCS2 kipróbálásához összerakott infrastruktúrám kevés elemből állt. A Raspberry Pi-hez csak az NCS2 csatlakozott USB interfész segítségével, valamint egy 2500 mA-es tápegység az erre a célra kialakított mikro USB csatlakozón keresztül. Beviteli eszközöket, illetve monitort külön nem csatlakoztattunk, minden adatforgalom a beépített WiFi csatolón keresztül történt. A Linux konzolt SSH kapcsolaton, a grafikus felületet pedig VNC[7]-n keresztül értük el. A mintaalkalmazások fejlesztéséhez és kipróbálásához az OpenVINO Toolkit fejlesztőeszköz 2020.1[8] -es verzióját használtuk. Ez a kísérleti/fejlesztési időszakban elérhető legfrissebb verzió volt.

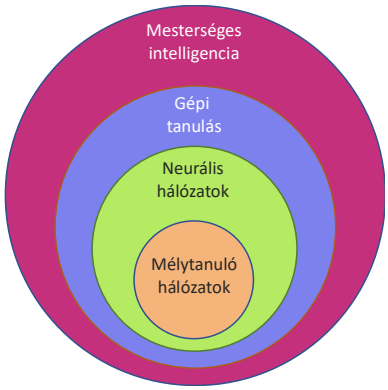
MESTERSÉGES INTELLIGENCIA, GÉPI TANULÁS, MÉLYTANULÁS

Az utóbbi években a mesterséges intelligencia (MI), különösen annak bizonyos részterületei sok új alkalmazásban, valamint korábban szinte elképzelhetetlen eszközökben (lásd: Edge Computing) jelentek meg. Célszerű pontosítani az ezzel kapcsolatos fogalmakat, hogy segítsük a téma megértését akkor is, mikor a kifejezéseket (gyakran hibásan) egymás helyettesítésére használják. A fogalmak definiáláskor feltüntettük azok angol elnevezését is, mert jellemzően még a magyar szakirodalomban is az angol terminológiával találkozhatunk.

[5] A kép forrása: https://upload.wikimedia.org/wikipedia/commons/e/e4/RaspberryPi_3B.svg
[6] A kép forrása: https://www.engadget.com/2018-11-14-intel-neural-compute-stick-2.html
[7] Virtual Network Computing (VNC) – egy grafikus képernyőmegosztó rendszer, mely hálózati kapcsolaton keresztül továbbítja a kliens felől érkező egér és billentyűzet eseményeket, valamint a szerver felől küldött grafikus képernyőmódosításokat.
[8] Telepítési utasítás elérhetősége: https://docs.openvinotoolkit.org/2020.1/_docs_install_guides_installing_openvino_raspbian.html

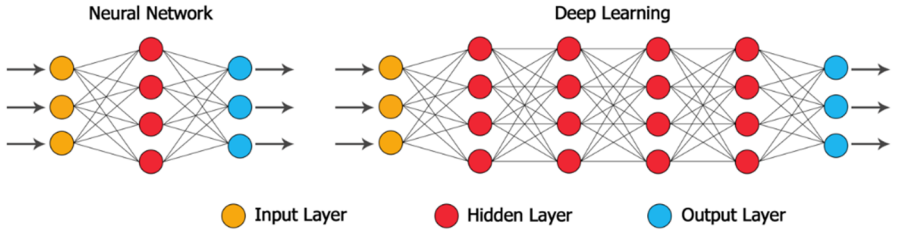
A mesterséges intelligencia (artificial intelligence/AI) fogalmának egy lehetséges definíciója szerint, a mesterséges intelligencia egy számítógép vagy számítógép vezérlésű rendszer, mely olyan feladatokat hajt végre, ami korábban csak humán intelligenciával volt lehetséges. (Copeland, 2020) Egy másik értelmezés szerint ez annak a tudománya, ami azt kutatja, hogyan lehet olyan intelligens gépeket vagy programokat készíteni, melyek eddig az embernek tulajdonított módon oldanak meg problémákat. [23]

A gépi tanulás (machine learning/ML) a mesterséges intelligencia egy részterülete, ami olyan rendszerek fejlesztésével foglalkozik, melyek automatikusan, tapasztalatokból tudnak tudást felhalmozni.



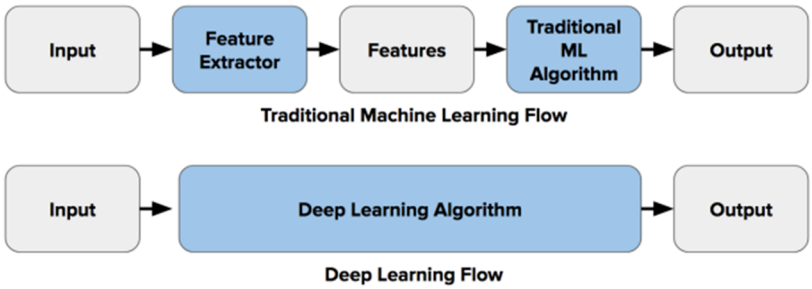
9. Ábra: Az egyes fogalmak kapcsolódása (saját szerkesztés)

A neurális hálózatok (neural networks/NN) olyan nagy számú, hasonló működésű mesterséges neuronokból álló hálózatok, amelyek egyfajta elosztott működésű információ-feldolgozást végeznek.



10. Ábra: Különbség a neurális hálózat és a mélytanuló neurális hálózat között (forrás: https://alphabold.com/neural-networks-and-deep-learning-an-overview/)

A mély tanuló hálózatok (deep neural networks/DNN) olyan mesterséges neurális hálózatok, melyek egyrészt több rejtett réteggel (hidden layers) rendelkeznek, mint a hagyományos neurális hálózatok. Másrészt nincs szükségük „manuális" feature extraction-re, mert ezt a munkát elvégzik a rétegeik (hidden layers). Egyik legismertebb mélytanuló hálózat a konvolúciós neurális hálózat (Convolutional Neural Networks/CNN). [24]



11. Ábra: Különbség a mélytanulás és a hagyományos gépi tanulás között (forrás: Haritha Thilakarathne[9])

ZÁRÓ GONDOLATOK

Tanulmányunk első – elméleti – részében a téma fogalmi keretét tekintettük át, valamint bemutattuk azokat az eszközöket, amelyek segítségével a konkrét – tanulmányunk következő részében ismertetésre kerülő – gyakorlati feladatot végeztük el. Ebben a második részében írunk továbbá a gépi látás neurális hálózatokkal történő támogatásáról is, illetve bemutatjuk a fontosabb keretrendszereket is.

FELHASZNÁLT FORRÁSOK

[1] Cs. Kollár, *„Az okos város és az okos vidék szimbiózisa: Utópia, fikció, vagy realitás?,”* Kecskemét, 2019.

[2] L. Gábor, „Intelligencia az IP-alapú videorendszerekben,” Detektor Plusz, pp. 26-27, vol. 4., 2013.

[3] *„Computer Vision vs. Machine Vision – What’s the Difference?,”* Appen.com, [Online]. https://appen.com/blog/computer-vision-vs-machine-vision/. [Hozzáférés dátuma: 2020.04.28.].

[4] *„MACHINE VISION VS. COMPUTER VISION,”* Intec Automation Inc., 2019. [Online]. https://www.intecautomation.com/blog/machine-vs-computer-vision/. [Hozzáférés dátuma: 2020.04.25.].

[5] *„Computer Vision vs. Machine Vision,”* AIA Weboldal, [Online]. https://www.visiononline.org/vision-resources-details.cfm/vision-resources/Computer-Vision-vs-Machine-Vision/content_id/4585. [Hozzáférés dátuma: 2002.04.28.].

[6] H. Gomes, *„Marr's Theory: From primal sketch to 3-D models,”* 2000. [Online]. http://homepages.inf.ed.ac.uk/rbf/CVonline/LOCAL_COPIES/GOMES1/marr.html. [Hozzáférés dátuma: 2020.04.29.].

[7] R. Demush, *„A Brief History of Computer Vision (and Convolutional Neural Networks,”* [Online]. https://hackernoon.com/a-brief-history-of-computer-vision-and-convolutional-neural-networks-8fe8aacc79f3. [Hozzáférés dátuma: 2020.05.01.].

[8] G. Horváth, *„Neurális hálózatok”*, Budapest: Panem Könyvkiadó Kft., 2006.

[9] G. Horváth, *„Neurális hálózatok és műszaki alkalmazásaik”*, Budapest, 1998.

[9] Webes elérhetőség: https://naadispeaks.wordpress.com/2018/08/12/deep-learning-vs-traditional-computer-vision

[10] J. J. Hopfield, *„Neural Networks and Physical Systems with Emergent Collective Computational Abilities,”* 1982. [Online]. https://www.researchgate.net/publication/16246447_Neural_Networks_and_Physical_Systems_with_Emergent_Collective_Computational_Abilities. [Hozzáférés dátuma: 2020.04.14.]
[11] K. Strachnyi, *„Brief History of Neural Networks,”* 2019. [Online]. https://medium.com/analytics-vidhya/brief-history-of-neural-networks-44c2bf72eec. [Hozzáférés dátuma: 2020.04.12.].
[12] Z. Luo, 10 szeptember 2017. [Online]. https://luozm.github.io/cv-tasks.
[13] H. Gao, 27 augusztus 2017. [Online]. https://towardsdatascience.com/object-localization-in-overfeat-5bb2f7328b62.
[14] P. Ganesh, 12 augusztus 2019. [Online]. https://towardsdatascience.com/object-detection-simplified-e07aa3830954.
[15] A. Rohan, *„Convolutional implementation of the sliding window algorithm,”* 2020. [Online]. https://medium.com/ai-quest/convolutional-implementation-of-the-sliding-window-algorithm-db93a49f99a0. [Hozzáférés dátuma: 2020.05.30.].
[16] J. Browniee, *„Machine Learning Mastery,”* 5 július 2019. [Online]. https://machinelearningmastery.com/object-recognition-with-deep-learning/.
[17] P. Alcorn, *„Intel Unveils Movidius Myriad X Vision Processing Unit,”* 2017. [Online]. https://www.tomshardware.com/news/intel-movidius-vpu-ai-inference,35327.html. [Hozzáférés dátuma: 2020.04.25.].
[18] *„Release Notes for Intel® Distribution of OpenVINO™ toolkit,”* Intel Corporation, [Online]. https://software.intel.com/content/www/us/en/develop/articles/openvino-relnotes.html. [Hozzáférés dátuma: 2020.04.15.].
[19] *„Supported Devices webpage,”* Intel Corporation, [Online]. https://docs.openvino-toolkit.org/2020.1/_docs_IE_DG_supported_plugins_Supported_Devices.html. [Hozzáférés dátuma: 2020.05.27.].
[20] K. Shaw, *„What is edge computing and why it matters,”* 2019. [Online]. https://www.networkworld.com/article/3224893/what-is-edge-computing-and-how-it-s-changing-the-network.html. [Hozzáférés dátuma: 2020.05.05.].
[21] *„The Debate in a Nutshell: CDN vs Edge Computing,”* BelugaCDN, [Online]. https://www.belugacdn.com/cdn-vs-edge-computing. [Hozzáférés dátuma: 2020.05.05.].
[22] L. Moné, *„IoT Devices, Sensors, and Actuators Explained,”* 2020. [Online]. https://www.leanix.net/en/blog/iot-devices-sensors-and-actuators-explained. [Hozzáférés dátuma: 2020.05.08.].
[23] *„Artificial Intelligence vs. Machine Learning vs. Deep Learning: What’s the Difference, Medium online magazin,”* Serokell, 2020. [Online]. https://medium.com/ai-in-plain-english/artificial-intelligence-vs-machine-learning-vs-deep-learning-whats-the-difference-dccce18efe7f. [Hozzáférés dátuma: 2020.05.25.].
[24] H. Thilakarathne, *„Deep Learning Vs. Traditional Computer Vision,”* 2018. [Online]. https://naadispeaks.wordpress.com/2018/08/12/deep-learning-vs-traditional-computer-vision/. [Hozzáférés dátuma: 2020.05.14.].

HÁNY ARCA LEHET A MIGRÁCIÓNAK? RECENZIÓ GLIED VIKTOR „AZ EURÓPAI MIGRÁCIÓ KÉT ARCA" CÍMŰ KÖNYVÉRŐL

BESENYŐ János[1]

Az európai migráció két arca című könyv az Ad Librum kiadó gondozásában nemrég került a könyvesboltok polcaira. A szerző, Glied Viktor [2] már a címválasztással is igyekszik kifejezni, hogy a migrációt nem fekete-fehérben látja, hanem többféle szemszöget mutat be. Ez akár azt is jelentheti, hogy a könyv nem fog hatalmas bevételt generálni a szerzőnek, de az olvasása közben egyértelművé vált számomra, hogy Glied Viktort nem az eladott példányszámok száma izgatja, hanem hogy az, hogy a migráció kérdését minél jobban körbejárja. Erre az átlagolvasó akár legyinthetne is, hiszen az elmúlt néhány években annyi cikket, tanulmányt, sőt könyvet írtak a témával kapcsolatosan, hogy azokkal Dunát lehetne rekeszteni. Az sem segíti a téma megértését, hogy a kérdés jelentősen túlpolitizált, így a migrációról írók jelentős része bizonyos okokból vagy a migrációt támogató tábor, míg más részük a migrációt elutasító tábor érveit ismétli, és meg sem próbálnak a kérdésről szakmai vitát folytatni. Úgy tűnik a szerző szakított ezzel a „kényelmes, jól bevált álláspontal" és 200 oldalon keresztül különböző állításokat, érveket és ellenérveket sorakoztat fel és kérdéseket tesz fel, amelyekkel kapcsolatosan az olvasót gondolkozásra, majd reagálásra készteti. Recenzensként már csak ezért is javaslom a könyv elolvasását, mindazoknak, akik bármilyen módon is érdeklődnek a migráció és az azt követő jelenségek (terrorizmus, szervezett bűnözés, külföldiek munkavállalása, integrációs kérdések, együttélési kihívások stb.) iránt.

A kötet egyébként egy tizenöt éves intenzív kutatási időszakot zár le, amely időszakban Glied többekkel együtt hazai és nemzetközi programok keretében foglalkozott a migráció különböző aspektusaival, amelyekkel kapcsolatosan több, szakmai szempontból is jelentősnek ítélt publikációt jelentetett meg, amelyek közül több is a magyar migrációs szakirodalom alapműveivé vált [3]. Ezalatt a szerző az elméleti kutatások mellett rengeteg személyes tapasztalatot gyűjtött össze a migrációban érintettektől, akik különböző inputokkal segítették a téma jobb megértését. Ekkor még csak alig néhányan (kutatók, egyetemi oktatók, bevándorlási szakemberek, civil szervezetek dolgozói) foglalkoztak Magyarországon ezzel a kérdéssel, ami aztán a 2015-ös „nagy migrációs válság" után megváltozott. Népszerűvé vált és mára már szinte mindenki szakértője lett a témának. Egy kedves külföldi ismerősöm szerint, aki sokat tartózkodik Magyarországon, a magyar ember két dologban tartja magát szakértőnek: a futballban és a migráció kérdésében, amelyekről órákig képesek beszélni. Már csak ezért is tiszteletre méltó a szerző azon törekvése, hogy egy mindenki számára érthető és használható könyvet tegyen le a migrációval kapcsolatosan. A kötet lektora Dövényi Zoltán professzor, aki maga is foglalkozott a migráció kérdéskörével és kiegyensúlyozott véleményével hozzájárult a könyv objektív látásmódjához.

[1] besenyo.janos@gmail.com | 0000-0001-7198-9328 | assistant professor,lecturer/egyetemi oktató | Óbudai Egyetem

A kötet három fejezetből áll, amelyekből az első a „***Migrációs kihívások az Európai Unióban***” címet viseli. Ebben a fejezetben megismerhetjük a nyugat-európai közösség migrációs történetét, a bevándorlás jellegét, a kibocsátó térségeket és az európai válaszokat. Ez rendkívül lényeges abból a szempontból, hogy megérthessük, hogy az EU vezetői és az átlag állampolgárai nagy része is mért gondolkodik úgy a migráció kérdéséről, ahogy gondolkodik. Ez már csak ezért is fontos, mivel az Unióhoz 2004-ben csatlakozott közép és kelet-európai államok többsége történelmi és más okokból is teljesen másképp tekint a migrációra, mint a nyugat-európai országok. Különösen Magyarország, amely több száz éves, tudatosan kialakított „migrációs politikát” működtetett [4]. Ráadásul az újonnan csatlakozó országok nem rendelkeztek gyarmatosító múlttal, amely szintén hatással van a nyugat-európai országokba érkező migránsok összetételére. Ezt a szerző igen szemléletesen ismerteti, valamint azt is, hogy ezek az államok hogyan építették újra a II. világháború után az országaikat balkáni, közel-keleti, valamint észak-afrikai országokból származó vendégmunkások segítségével, akiket egyáltalán nem kívántak befogadni. Azonban az eltervezett „üzleti modell” nem az elvártaknak megfelelően működött, így a vendégmunkások nem tértek vissza az őket kibocsátó államokba, hanem Európában maradtak, sőt a családtagjaik is követték őket. Erre pedig az európai országok egyáltalán nem voltak felkészülve. A migránsokkal kapcsolatos együttélési nehézségeket, problémákat igyekeztek elbagatellizálni, bíztak a multikulturalizmus vélt pozitív hatásaiban és az integrációjukat szinte csak a 24. órában kezdték meg, amikor újabb hatalmas, majd másfél milliós tömeg érkezett a kontinensre. Erre pedig még kevésbé volt az Unió felkészülve, így a migrációs hullám kezelését inkább „kommunikációs csaták” és nem tényleges, az európai közösség által elfogadott szakpolitikai tevékenység jellemezte [5]. Mindez annak ellenére történt így, hogy a kontinens országai öregedő tendenciát mutat, a szociális és nyugdíjrendszerek fenntartása egyre kevésbé megoldható, valamint nagyobb és nagyobb nehézséget jelent a gazdasági versenyképesség fenntartása, amihez nagy szükség lenne egy tudatosan irányított és működtetett migrációs politikára. A szerző szerint a migrációs kihívásokra adott választ egy egységesebb európai bevándorláspolitika képes lenne biztosítani, ezzel azonban több európai ország sem ért egyet, akik továbbra is külön, nemzeti hatáskörben kívánják tartani a migrációs szabályozás nagy részét [5, pp. 26–27]. Ezek az ellentétek jól láthatóak a 2014-2016-os menekültválság kezelésénél is, ahol a határvédelmi rendszerek egyértelműen csődöt mondtak. Ez pedig rákényszerítette az európai államok egy részét, hogy az addigi menekültpolitikájukat felülvizsgálják és szigorításokat vezessenek be a migránsok befogadásával kapcsolatosan. Így a korábbi „menekültbarát” attitűd megfordult, ami az Európai Unió vezetőit arra késztette, hogy visszaállítsák az EU külső határainak védelmét, valamint megállapodást kössenek Törökországgal az illegális migráció kezelésével kapcsolatosan [5, pp. 34–40]. Glied még 2015-ben írt cikket Behódolás címmel [6], amelyben a mostani könyvben részletesen és mélyebben elemzett konfliktusokat vizsgálta közvetlenül a migrációs válság tükrében. Érezhetően hatással voltak rá olyan gondolatok, mint az azonos című Houellebecq könyv [7], vagy Douglas Murray sötét fellegei [8]. A szerző ‘Az európai migráció két arcában’ úgy árnyalja a pesszimista forgatókönyveket, hogy melléjük rak egyéb tényezőket, amelyek újra fogalmazzák a migrációs folyamatok egydimenziós megközelítéseit. Ugyancsak ebben a fejezetben ismerhetjük meg az Európai Unióban élő bevándorlókat. Kik és milyen háttérrel érkeztek, hogyan illeszkedtek be, vagy éppen hogyan hoztak létre párhuzamos társadalma-

kat, amelyek komoly biztonsági kihívásokat jelentenek az őket befogadó országoknak. Elismerésre méltó, hogy Glied nem a sikertörténeteket igyekszik bemutatni, hanem a befogadó és a befogadottak közötti törésvonalakat, kihívásokat is [5, pp. 45-57]. Itt ismerhetjük meg a migrációt érintő politikai dokumentumokat, valamint az Európai Bizottság új megállapításait is a migráció lehetséges kezelésével kapcsolatosan is, amelyek azonban „*bár felmutatnak visszatérő, politika- és szabályzásformáló elemeket, de kevés olyan kimunkált tartalmat, amely valóban leköveti a történéseket és konkrét jogalkotási aktus kiindulópontját jelenthetné*." [5, p. 56]. Sajnálatosan ez is hozzájárul ahhoz, hogy a migráció kezelésével kapcsolatosan továbbra sincs egységes európai álláspont.

A második fejezet „***az európai migráció két arca***" azokkal a mély társadalmi, politikai, gazdasági kérdésekkel és vitákkal foglalkozik, amelyek a bevándorlás kapcsán az elmúlt évtizedekben felmerültek. Először a biztonsági kihívásokat veszi számba, amelyet igyekszik árnyaltan, kissé távolságtartóan ismertetni. A fejezet első felében inkább a migráció lehetséges előnyeit (demográfia, ellátórendszerek fenntartása, gazdasági fejlődés, stb.) mintsem kockázatait hangsúlyozza, de végül teljes mértékben egyetért Tálas Péterrel abban, hogy „*a migráció olyan jelenség, amely egyszerre jelent lehetőséget és kihívást, amelynek előnyei és hátrányai egyaránt vannak.*" [9]. A szerző itt arra a következtetésre jut, hogy az EU már nem képes a migránsok és a vendégmunkások nélkül boldogulni – amit a 2020-as koronavírus járvány is jól mutat – amikor a mezőgazdaság bizonyos területein hatalmas gondot okozott a munkáskéz hiánya [5, pp. 65–66]. Emellett körbejárja a kockázatokat is, ahol elismeri a nyelvi problémákat, az egyre súlyosabb etnikai, vallási és kulturális feszültségeket, a közbiztonság romlását és a terroristatámadásokat is, amelyek jelentős részét migráns háttérrel követik el. Itt hívja fel a figyelmet egy olyan szempontra is, amelyet már a politikai erők észrevettek és ki is használnak [5, p. 71], viszont a kutatók nem fektetnek megfelelő hangsúlyt, mégpedig a társadalmi percepcióra és szubjektív biztonságérzetre [10 és 11]. Ugyancsak problémaként említi, hogy az egyébként leterhelt határőrizeti szervek nem képesek különbséget tenni a politikai menekültek, a menedékkérők és a gazdasági menekültek között, ami emberi jogi szempontból aggályokat vet fel [5, p. 68]. Itt foglalkozik a korábban már ismertetett multikulturalizmus illetve a „Willkommenskultur" bukásával, annak okaival és hátterével, valamint azzal a kérdéssel, hogy helyette milyen integrációs stratégiákat lehetne alkalmazni. Ebben a fejezetben követhető nyomon az is, hogy a menekültek, mint áldozatok konnotációját felváltotta a migránsok, mint elkövetők formula; hogyan változott meg a nyugati társadalmak hozzáállása a migrációhoz és a korábbi elfogadó attitűdöt, hogy váltotta fel a mérlegelés, majd a távolságtartás, sőt elutasítás [5, pp. 80–83]. Olyan, a társadalmat korábban kevésbé érdeklő, főként a bevándorlókhoz kapcsolódó témák kerültek előtérbe, mint a mecsetépítések, a muzulmán nők viselete (fejkendő vita), Európa iszlamizációja, a keresztény-zsidó és az iszlám hátterű népesség közötti konfliktusok felerősödése. Ezekkel kapcsolatosan Glied szinte minden érvet bemutat pro és kontra, majd végül arra a megállapításra jut, hogy az európai országok többsége nem volt képes a főként muzulmánokból álló migráns tömegeket integrálni, amelyek párhuzamos társadalmakat hoztak létre, illetve működtetnek [5, p. 143]. Ez pedig szerinte Európa hanyatlásához, a liberális demokrácia válságához, valamint az iszlám fundamentalizmus és a szélsőjobb megerősödéséhez vezet [5, pp. 145–163].

A harmadik fejezet „***a migrációs válság a magyar kormányzat politikájában és kommunikációjában***" címet viseli. Ebben Magyarország példáján keresztül vizsgálja a

migrációs válságot és az arra épülő kommunikációs kampány kérdéskörét. A szerző itt is igyekszik objektívan bemutatni a migrációs időszakot és a magyar kormány arra adott válaszait. Bár a kormány több döntését is elfogadja és ésszerűnek nevezi, a kormányzati kommunikációt azonban sokszor leegyszerűsítettnek és megosztónak tartja [5, pp. 166–168]. A kormányzati kommunikáció egyes elemeit, például a „Ha Magyarországra jössz, tiszteletben kell tartanod…" feliratú óriásplakátokat és televíziós hirdetéseket elhibázottnak tartotta, már csak azért is, mert a magyar lakosságnak a jelenséggel kapcsolatosan személyes tapasztalata nem volt, nem is lehetett [5, p. 170]. Azonban ez az állítás csak részben fedi a valóságot, hiszen – mint említettem – a Honvéd Vezérkar Tudományos Kutatóhely szakemberei már a migránsválság kezdetén a határövezetben tartózkodtak, ahol egyedüliként végeztek kérdőíves és interjús kutatást a migránshullám által elsődlegesen érintett lakosok között Ásotthalom, Mórahalom és Röszke településeken. A kutatás publikálásra is került [11, pp. 83-95 és 10, pp. 335–363]. Ugyancsak ebben a fejezetben olvashatunk a déli határon felállított ideiglenes biztonsági kerítésről, amely sikeresen elterelte más országok irányába a migránshullámot, majd a Honvédség aktív bekapcsolódásával és további jelentős fejlesztések megvalósításával tényleges határvédelmi feladatot is ellátott. A szerző itt foglalkozik a menekültkvóta kérdésével is, valamint a kormányzatnak azzal a javaslatával – ezt nemcsak a V4 országok, de több európai állam is támogatja – hogy a migránsok problémáit a szülőföldjükön kellene orvosolni, ott kellene számukra élhető, biztonságos környezetet teremteni, nem pedig százezrével beengedni őket Európába, ahol egyelőre képtelenek vagyunk őket hatékonyan integrálni [5, pp. 178–180]. A szerző bemutatja a magyar kormányzat lépései által kiváltott nemzetközi reakciókat és a migránskérdéssel kapcsolatos európai vitákat, amelyek a mai napig sem zárultak le.

A jól megszerkesztett kötet igen sok és hasznos információt tartalmaz, amiket a szerző igyekezett a legobjektívebb módon ismertetni az olvasókkal. Azonban apróbb hiányosságok fellelhetőek a könyvben. A szerző, hol a szövegben, hol pedig lábjegyzetekben hivatkozza le a felhasznált irodalmat, amelyek egy részét a felhasznált irodalomjegyzék nem tartalmazza, illetve a képek alatt nem minden esetben találhatóak meg a források pontos helyei. Ezek azonban nem csökkentik a könyv értékét, amelynek elolvasása után egyértelművé válik, hogy a migrációnak nem kettő, de sok millió arca van. Éppen ezért egyáltalán nem lehet a migráció kérdését egységesen kezelni, hiszen minden ember, eset vagy szituáció, más és más megközelítést igényel. Ha erre a felismerésre eljut az olvasó, akkor a könyv már elérte a célját.

FELHASZNÁLT FORRÁSOK

[2] Glied Viktor a Pécsi Tudományegyetem, Politikatudományi és Nemzetközi Tanulmányok Tanszék adjunktusa, aki 2003-ban szerzett Történész és középiskolai tanár egyetemi diplomát, majd 2005-ben Politológus egyetemi diplomát a Pécsi Tudományegyetemen. 2013-ban szerezte meg a PhD fokozatát a politikatudományok területén. Fő kutatási területei: Migráció, vízkonfliktusok, környezeti konfliktusok, fenntartható fejlődés, ökopolitika, fejlesztéspolitika valamint terület- és településfejlesztés.

[3] Ezek közül az egyik legismertebb a 2016-ban megjelent, Tarrósy Istvánnal és Vörös Zoltánnal közösen jegyzett *Migráció a 21. században* című kötet, amely már a 2015-ös migrációs válság tapasztalatait is feldolgozta. Ugyancsak velük szerkesztette 2014-ben a *Migrációs tendenciák napjainkban* című kötetet, amelyben több ismert és kevésbé ismert

kutató fejtette ki az álláspontját a migráció különböző aspektusairól. A szerző egyébként a másik kutatási területét, a vízbiztonságot is gyakran összekapcsolja a migrációval, amely témában szintén több publikációja jelent meg.

[4] Bővebben erről a kérdésről: Miletics Péter és Stohl Róbert, „A magyar államtér helye, szerepe a történelmi migrációs folyamatokban," in *Európa és a migráció*, Besenyő János, Miletics Péter és Orbán Balázs, Eds, Budapest, Magyarország: Zrínyi Kiadó, 2019, pp. 230–301.

[5] Glied Viktor, *Az Európai migráció két arca*. Pécs, Magyarország: Ad Librum, 2020, pp. 14–21.

[6] Glied Viktor, „Behódolás? Európai szélsőséges pártok és a bevándorlás – helyzetkép," in *Változó Európa? Kérdések, kétségek, válaszok*, Tuka Ágnes, Ed., Pécs, Magyarország: Publikon Kiadó, 2015, pp. 179–196.

[7] Michel Houellebecq, *Behódolás*. Budapest, Magyarország: Magvető Kiadó, 2020.

[8] Douglas Murray, *Európa furcsa halála*. Pécs, Magyarország: Alexandra Kiadó, 2019.

[9] Tálas Péter, „A migráció mint biztonságpolitikai probléma," *Magyar Tudomány*, vol. 180, no 1, p. 68, Január 2019, doi: 10.1556/2065.180.2019.1.6.

[10] Ezzel kapcsolatosan megjegyezném, hogy az általam 2014-2018 között vezetett Honvéd Vezérkar Tudományos Kutatóhely volt, az egyetlen olyan tudományos szervezet, amelynek a munkatársai egy kérdőíves/interjús kutatást hajtottak végre azokban a határmenti településeken, ahol 2015-ben a migránsok több tízezer fős tömegben haladtak át. A kutatás kiemelten foglalkozott a társadalmi percepció és szubjektív biztonságérzet kérdéseivel. A kutatás nyilvános része pedig publikálásra is került. Rácz Attila és Balogh Péter, „A migrációs válságon innen és túl. Együttérzés, elutasítás, bizalom és szolidaritás (egy szociális kutatás eredménye)," in *Európa és a migráció*, Besenyő János, Miletics Péter és Orbán, Balázs, Eds., Budapest, Magyarország: Zrínyi Kiadó, 2019, pp. 335-363. valamint

[11] Rácz Attila, „The effects of Hungarian Defence Forces (HDF) border security deployment on the civilian population's subjective sense of security," *Belvedere Meridionale*, vol. 30, no. 4, pp. 83-95, Április 2018, doi: 10.14232/belv.2018.4.5.

A KÖTET KÖNYVÉSZETI ADATAI

Glied Viktor (1978-) Az európai migráció két arca. – Budapest: Ad Librum, 2020. - 201 p. : ill. Bibliogr.: p. 193-201. ISBN 978-615-5758-62-1 (nyomtatott)

1. Ábra: Glied Viktor „Az európai migráció két arca” című könyvének borítója

RECENZIÓ KRAJNC ZOLTÁN (FŐSZERK.) „HADTUDOMÁNYI LEXIKON (ÚJ KÖTET)" CÍMŰ KÖNYVÉRŐL

BELÁZ Annamária[1] – SZALÁNCZI-ORBÁN Virág[2]

A Biztonságtudományi Szemle ezen könyvismertetője részben rendhagyó, mivel a most ismertetett könyv egy összefoglaló mű: a Hadtudományi lexikon. Az új kötet elnevezés alapján tudhatjuk, hogy az új kiadást megelőzően már létezett egy korábbi Hadtudományi lexikon. Ahhoz, hogy bemutathassuk az új kiadást és annak kapcsolódását az Óbudai Egyetemhez és a Biztonságtudományi Szemléhez nézzük meg milyen is a korábbi kiadás és miért volt szükség egy új kötet megalkotásához.

A Magyar Hadtudományi Társaság gondozásában készült el 1995-ra a hadtudomány egészét átfogó Hadtudományi lexikon. Az 1995-ös kiadás két kötetet foglal magában, közel 1600 oldallal és összesen mintegy 4000 szócikkel, melyben feldolgozza a releváns hadtudományi ismeretanyagot. A kiadott lexikon adatai: Hadtudományi lexikon A-Zs I-II., kiadó: Magyar Hadtudományi Társaság, oldalak száma:1584, kötés: műbőr, sötétkék, ISBN:0469000676354, kiadás éve:1995. A lexikon a tágan értelmezett hadtudomány és a kapcsolódó határterületek (például belügy) fogalomkészletét öleli át. Szabó József vezérőrnagy, a Társaság akkori alelnöke vezetésével alakult meg a szerkesztőbizottság, amelyben mintegy 130 szakember dolgozott. Az alapvetően szárazabb műfajnak tartott lexikon olvasmányosságát javítja, hogy több ábra, 640 kép és sok életrajzi adat színesíti.

Dr. habil Berek Tamás (B.T.) és Dr. habil Besenyő János (B.J.), a Biztonságtudományi Szemle szerkesztőbizottságának a tagjai aktív szerepet vállaltak a lexikon elkészítésében. Egy interjú keretében meséltek a munkáról, valamint a kihívásokról melyekkel szembe néztek. Jogosan merül fel a kérdés, hogy mi volt a lexikon szerkesztőbizottságának motivációja a kötet elkészítéséhez? „Olyan méltó új kiadványt szerettünk volna készíteni, ami a közösen a korábbi Hadtudományi lexikonnal, valamint más korábban publikált kézikönyvvel, kiadvánnyal és adatbázissal (pl.: Katonai Terminológiai Értelmező Szótár (Zrínyi Kiadó 2015), Katonai Lexikon (Zrínyi Kiadó 1985), Magyar Honvédség Terminológiai Adatbázisa) a része legyen egy olyan alap ismeretbázisnak amit bárki fel tud használni az érdeklődésének megfelelően." (B.T.)

A Hadtudományi lexikon Új kötete a korábbi kiadás örököse kíván lenni. Az 1995-ös megjelenés óta eltelt több mint 20 év. Ezalatt az idő alatt a globális hadtechnikai fejlődés, politikai és geostratégiai átrendeződés történt, mely alapjaiban változtatta meg a hadviseléssel kapcsolatos gondolkodásmódot és dokumentumokat. „Gondoljunk egyszerűen csak arra, hogy a korábbi lexikon kiadása óta Magyarország NATO tag lett, új kifejezéseket kezdtünk el használni. Sőt, a terminológia folyamatosan változik ezért előfordult az, hogy

[1] belaz.annamaria@uni-obuda.hu | ORCID: 0000-0002-8222-5283 | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

[2] szalanczior ban.virag@phd.uni-obuda.hu | ORCID: 0000-0002-1073-2788 | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

különböző kifejezéseket használtunk ugyanarra a jelenségre. Ezeket az eltérő asszociációkat kellett egy közös mederbe hozni." (B. J.)

Az új kötet célja, hogy a hadtudomány korszerű ismereteit is magába foglalja, összefoglalja azt. A Magyar Tudományos Akadémia Hadtudományi Bizottsága, a Magyar Hadtudományi Társaság, a Honvéd Vezérkar Tudományos Kutatóhelye, valamint a Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar több mint 80 munkatársának összefogásával készült el és került kiadásra 2019-ben. A fejlesztő- és kutatómunka kereteit a Nemzeti Közszolgálati Egyetem-KÖFOP–2.1.2– VEKOP–15–2016–00001 jelű „A jó kormányzást megalapozó köz-szolgálat-fejlesztés" című projektje biztosította. A kötet alfabetikus sorrendben mintegy 4000 szócikket tartalmaz, 11 tematikus egységben.

Fsz.	*Főcsoport*	*Súlyozási érték*	*Címszó (db)*
1.	*Hadtudomány általános elmélete*	1	190
2.	*Katonai biztonság*	1,32	250
3.	*Hadművészet*	1,42	270
4.	*A hadtudomány műveleti területei (katonai műveletek)*	4	760
5.	*A hadtudomány műveleti támogató területei*	4	760
6.	*A hadtudomány műveleti kiszolgáló támogató területei*	4	760
7.	*Hadtörténet – hadművészet története*	1,5	~290
8.	*Védelmi (katonai) igazgatás – hadijog*	1	190
9.	*Humánpolitika – személyügy*	0,75	~150
10.	*Katonai képzés – kiképzés – felkészítés*	1	190
11.	*Katonai szociológia, pszichológia, pedagógia*	1	190
12.	**Összesen**	**–**	**4000**

1.ábra: A Hadtudományi lexikon új kötete főcsoportonkénti súlyozott címszó mennyiségei és főcsoportok

A SZERKESZTÉSI MUNKA ÉS A LEXIKON KÜLÖNLEGESSÉGEI

Hogyan zajlott a munka és milyen kihívásokkal találkozott a szerkesztőbizottság? A munka tervezése 2016 őszén indult, első feladatként a lexikon terjedelemi határait kellett meghúzni: eldöntötték mely szócikkek kerüljenek felfrissítésre, melyek kerülnek teljes átdolgozásra, valamint melyeket szükséges az új területek megjelenése miatt újonnan kidolgozni. A szerkesztőbizottság ezek után részletes útmutatást készített a szócikk szerzőknek. 2017 tavaszától indult a szócikkek kidolgozása, s egy igen rövid 1,5 éves időtartamban kellett a szerzőknek elvégezni a rájuk bízott feladatot. „Az idő nagy kihívást jelentett mindannyiunk számára. A szerzők egyéb feladataik mellett a szaktudásuk legjavát adták, hogy

egy megbízható és páratlan lexikont hozzanak létre." (B. J.) „Számomra az volt a legnagyobb kihívás, hogy 1-1 csupán féloldalas szócikkbe úgy sűrítsek bele tudásanyagot (mely témákkal teljes kötetek foglalkoznak), hogy az releváns és informatív legyen, egy érdeklődő kérdésre egyértelmű választ tudjon adni, anélkül, hogy további lexikonok, szakcikkek felkutatását tenné szükségessé. Kihívás volt az is, hogy úgy tudjam felújítani a szakcikkeket, hogy azok tartalmukban megújuljanak, rövidebbek és modernebbek legyenek." (B. T.)

Milyen különlegességei vannak az új Hadtudományi Lexikonnak? Ahogyan az 1. ábra is bemutatja a Lexikon tematikáját tekintve szerteágazó, több, mint 11 témakörben találunk szakkifejezéseket. A természet-, műszaki és társadalomtudományok iránt érdeklődőknek egyaránt hasznos információt nyújthat, nem csak azoknak, akik a hadtudományok iránt érdeklődnek. „Hatalmas tudásbázis gyűlt össze gyakorlatilag dióhéjban. Olyan egyedülálló tartalom, ami sehol máshol nem található meg, semmilyen más irodalmi formában publikációban." (B. T.) „Egyetlen hasonlóan nagyszabású munka van: az előző hadtudományi lexikon." (B. J.)

Igazán kiemelkedő a lexikon tudományos háttere, hiszen nem értelmező vagy szótárjellegű munka készült, hanem elsősorban tudományos. Minden megnyilvánulásában, szócikkében, magyarázatában releváns bizonyítékok állnak. „Minden szócikk szerzője a saját területéről írt. Éppen ezért nem szabad elfelejtenünk, hogy minden szócikk hátterében hosszú évtizedek tudományos munkái állnak. Végre egy terminológiájában egységes, előrevivő és modern lexikonnal rendelkezünk" (B. J.) A tudományos igény mellett a szerzők igyekeztek olyan megfogalmazást használni, amely minden korosztályú és hátterű olvasó számára közérthető.

A kötet további különlegessége, hogy elérhető elektronikus formában. Nincsen szükség számítógépre, CD-romra vagy arra, hogy a táskánkba helyezzünk egy súlyos könyvet, hiszen pdf formában könnyedén elfér egy telefonon is. „Az elektronikus forma praktikus, mobilis, könnyen kereshetünk benne és nem utolsó sorban ingyenesen hozzáférhető, letölthető." (B. T.)

Napjainkban amikor az interneten szintem bármi elérhető egy kattintásra talán elgondolkodik a kedves olvasó is azon, hogy miért van szükség egy lexikonra. Az interneten egy kulcsszó beírásával sok, témájában és megbízhatóságában változatos rekordot találhatunk, ezek esetében meg kell vizsgálni, mi az, ami szavahihető és mi az, amit figyelmen kívül lehet hagyni. Sokak számára ez egy nehéz és mindenekelőtt időigényes feladat. A lexikon használatával időt és energiát spórolhatunk, hiszen gyorsan tudományosan megalapozott és releváns információt nyújt. Éppen ezért érdeklődő személyek, Bsc/Msc szakos hallgatók és kutatók egyaránt origót találnak a lexikonban. „A tudományos munka megkezdése szinte kivétel nélkül a kulcsfogalmak meghatározásával indul. Úgy vélem, hogy a kutatók számára érdekes lesz áttekinteni a régi és az új lexikon fogalmainak változását ezáltal új összefüggésekre bukkanhatnak." (B.T.)

A szerkesztőbizottság, valamint a lexikon megalkotására összeállt konzorciumi tagok nem tekintik befejezettnek a munkát, a hadtudomány folyamatos fejlődése, a hadviselés változó természete megköveteli a szünet nélküli fejlesztést és az időszakonkénti felülvizsgálatot.

A könyvismertetést szeretnénk a munkában aktívan szerepet vállaló kollégáink szavaival zárni:

„Hihetetlen nagy megtiszteltetés, hogy Honvéd Vezérkar képviseletében részt vehettem ebben az előrevivő, nagyszerű tudományos munkában.” (B.J.)

„Roppant nagy megtiszteltetés és kihívás volt ez a feladat. Az előző lexikonnak a szerzői között volt édesapám Berek Lajos, hálás feladat, hogy részt vehettem ebben a munkában mert így – bár eltérő területen – folytathatom azt amit édesapám elkezdett.” (B.T.)

PUBLIKÁCIÓK

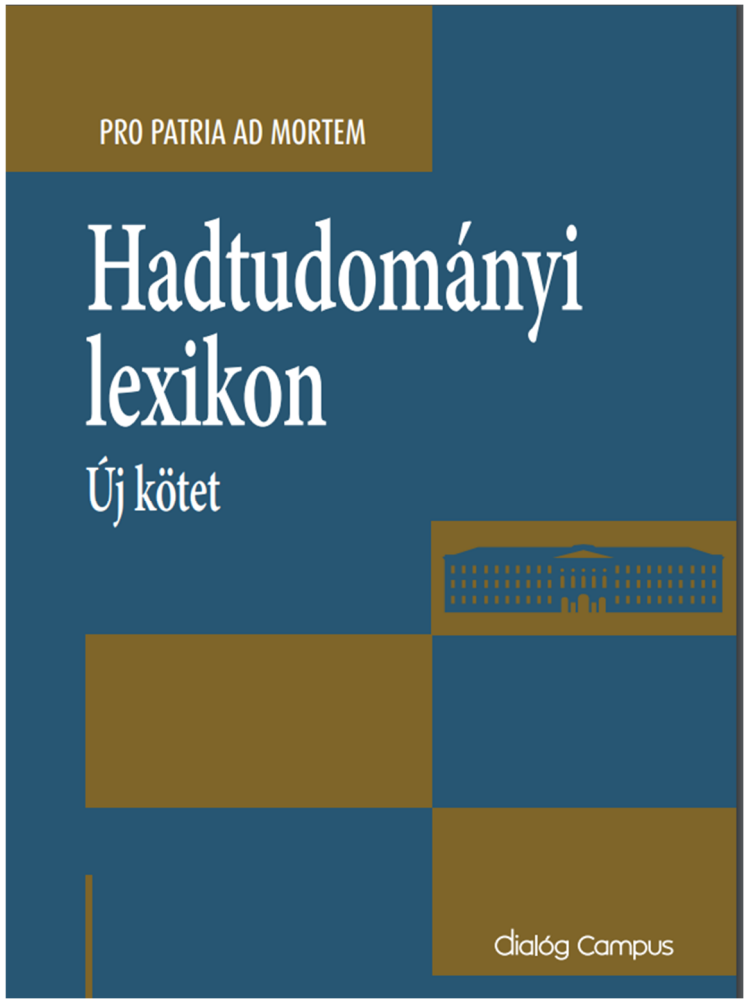
1. Hadtudományi lexikon A-Zs I-II., kiadó: Magyar Hadtudományi Társaság, oldalak száma:1584, kötés: műbőr, súly:5000 gr, ISBN:0469000676354, kiadás éve:1995.
2. Gőcze, István és Krajnc, Zoltán és Padányi, József (2020) A Hadtudományi Lexikon új kötetéről. HADTUDOMÁNY: A MAGYAR HADTUDOMÁNYI TÁRSASÁG FOLYÓIRATA, 30 (1). pp. 148-156. ISSN 1215-4121
3. Munk Sándor: Hadtudományi kutatók és kutatási területeik. 1. rész: A hadtudomány részterületeinek empirikus vizsgálata. Hadtudomány, 2015. 1–2. szám, pp. 4–16.
4. Gőcze István: A hadtudomány részterületeinek empirikus vizsgálata. 2. rész: A mértékadó hadtudományi folyóiratok elemzése és értékelése. Hadtudomány, 2015. 3–4. szám, pp. 21–35.
5. Gőcze István: A hadtudomány részterületeinek empirikus vizsgálata. 3. rész: A hadtudományi (tudományos) szervezetek elemzése és értékelése. Hadtudomány, 2017. 1–2. szám, pp. 3–31.

A KÖNYV KÖNYVÉSZETI ADATAI

Krajnc Zoltán (főszerk.) Hadtudományi lexikon : Új kötet. = Pro Patria Ad Mortem. - Budapest : Dialóg Campus, 2019. - 1199 p. ISBN 978-963-531-101-9 (nyomtatott), ISBN 978-963-531-095-1 (elektronikus PDF) , ISBN 978-963-531-094-4 (elektronikus ePUB)

A KÖTET ELÉRHETŐSÉGE

A Hadtudományi lexikon új kötetének elektronikus változata (PDF és ePUB) ingyenesen hozzáférhető és letölthető az NKE Közszolgálati Tudásportálon
https://tudasportal.uni-nke.hu/tudastar-reszletek?id=123456789/14688



2. Ábra: Hadtudományi lexikon – Új kötet című könyv borítója

Follow, like, post, publish! | Kövess, lájkolj, posztolj, publikálj!

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

https://www.linkedin.com/company/safety-and-security-sciences-review

https://www.facebook.com/biztonsagtudomanyi.szemle