ISSN 2676-9042

Vol 4, No 3, 2022.

2022, IV. évf. 3. szám

Safety and Security Sciences Review

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

Biztonságtudományi Szemle

a biztonságtudomány nemzetközi, lektorált, szakmai és tudományos folyóirata

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

On the cover can be seen | A borítón
BORS Györgyi
painter/festőművész
Emotional state | **Érzelmi állapot**
painting | című festménye 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
Facility Security	Létesítménybiztonság
Private Security	Magánbiztonság
Artificial Intelligence	Mesterséges intelligencia
Safety and Security in General	Munkabiztonság
Technical Security	Műszaki biztonság

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

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

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

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

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

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

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

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 4, No 3, 2022. | **2022. IV. évf. 3. szám**

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

BÁLINT Márton

hubalmar@gmail.com

My name is Márton BÁLINT. 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 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.

GULYÁS Attila

agulyas66@gmail.com

Attila GULYÁS ret. LTC graduated from the Kossuth Lajos Military College as an infantry officer in 1988. After serving a four-year period of time as a troop officer he was transferred to the Military Security Office, where he served in different positions. He retired from the service as a head of department and in the rank of Lieutenant Colonel in 2010. He has been interested in IT for a quarter century. His hobby is computer programming (Visual C++, and Python), as well as computer forensic on personal computers on MS Windows, and Ubuntu operating systems. He is a PhD aspirant at the Óbuda University Doctoral School on Safety and Security Sciences, where he is researching the connection between the terrorism and the Dark Web.

GULYÁS Attila nyugállományú alezredes 1988-ban végzett a Kossuth Lajos Katonai Főiskola gépesített lövész szakán 1988-ban. Négyéves csapatszolgálatot követően a Katonai Biztonsági Hivatal állományában szolgált tovább, ahonnan osztályvezetőként vonult szolgálati nyugállományba 2010-ben. Több mint 25 éve foglalkozik informatikával, ezen belül programozással (Visual C++, Python), a személyi számítógépeken hátrahagyott nyomok tanulmányozásával MS Windows és Ubuntu operációs rendszereken. Jelenleg doktoandusz hallgató az Óbudai Egyetem Biztonságtudományi Doktori iskoláján, ahol kutatási témája a „Terrorszervezetek tevékenysége a kibertérben: a közösségi médiától a Dark Webig”.

KRASNYÁNSZKI Brúnó

brunokrasnyanszki@gmail.com

He is a first-year student of the János Von Neumann Faculty of Informatics at Óbuda University, major-

Az Óbudai Egyetem Neumann János Informatika Kar mérnökinformatika szakos elsőéves hallgatója.

ing in Computer Science Engineering. His areas of interest are safety and security sciences and information technology, but he is most interested in cyber security. He started researching in 2021, where he researched the human risk factor of cyber security and had the opportunity to present the results of his research at Student Circles XXII. in the Technical and Real Science section of the Carpathian Basin Conference. Since July 2022, he has been the Deputy Head of the Technical and Real Sciences Department of the National Association of Research Students.

Érdeklődési területe a biztonságtudomány és az informatika, de a kiberbiztonság foglalkoztatja legjobban. 2021-ben kezdett kutatni, ahol akiberbiztonság humán kockázati tényezőjét kutatta és kutatásának eredményeit lehetősége volt előadni Tudományos Diákkörök XXII. Kárpát-medencei Konferenciájának Műszaki és Reáltudományi szekciójában. 2022 júliusa óta Kutató Diákok Országos Szövetségének Műszaki- és Reáltudományi Tagozat Tagozatvezető-helyettese.

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 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.

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

NAGY Attila

oktotorp@fastmail.com

My name is NAGY Attila. I completed my studies at the Technical College in Subotica, Serbia, as an electrical and computer engineering engineer. I completed a specialization there as a mechatronics engineer. I obtained my first master's degree at the János Neumann Faculty of Informatics of the University of Óbuda as a certified engineering teacher (computer science engineer). I hold my second master's degree from the Donát Bánki Faculty of Mechanical and Security Engineering at the University of Óbuda as a graduate mechatronics engineer. I am currently a doctoral student at the Doctoral School of Security Sciences of the University of Óbuda. My research topic is the detection of network anomalies using machine learning procedures.

NAGY Attilának hívnak. A Műszaki Szakfőiskolán fejeztem be a tanulmányaimat Szabadkán, Szerbiában, mint villamosságtan és számítástechnika mérnök. Ugyanitt befejeztem egy specializációt, mint mechatronikai szakmérnök. Az első mester fokozatomat az Óbudai Egyetem Neumann János Informatikai karán szereztem meg, mint okleveles mérnöktanár (mérnök informatikus). Második mester fokozatomat az Óbudai Egyetem Bánki Donát Gépész és Biztonságtecnikai Mérnöki Karán, mint okleveles mechatronikai mérnök. Jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskola doktorandusz hallgatója vagyok. A kutatási témám a hálózati anomáliák detektálása gépi tanulási eljárásokkal.

NAGY Sarolta

nagy.sarolta@nnk.gov.hu

NAGY Sarolta is an occupational health specialist, she has been working in field of occupational health since 1996. She completed the “Training of trainers

NAGY Sarolta foglalkozás-egészségügyi szakorvos, 1996 óta dolgozik a foglalkozás-egészségügy területén. 2013-ban elvégezte az FSZK szervezésében a

– Preparation for the teaching of training programs on accessibility in healthcare", organized by Ltd. for Equal Opportunities for Persons with Disabilities (FSZK) in 2013, and she completed the post-graduate training in employment rehabilitation human and technical consultatnt at the Budapest University of Technology and Economy in 2017. Her research topics are the factors influencing the disabled persons' employment, especially the aspects of occupational health and safety. Since 2011 she has conducted research with employees belonging to three disability groups (hearing-impaired, visually-impaired, mobility-impaired), mainly on their employment difficulties and about the assistive technologies they use, and the possible discrimination they experienced in the world of work. She participates in specialist training and also teaches at the Pedagogy and Rehabilitation of Hearing Impaired Persons Cours at the Eötvös Lorand University BGGYK Institute of Therapeutic Pedagogy and Rehabilitation.

„Képzők képzése – Felkészítés akadálymentesítés témájú képzési programok oktatására az egészségügyben" képzést, 2017-ben pedig a Budapesti Műszaki Egyetemen a foglalkoztatási rehabilitációs humán és műszaki szaktanácsadó posztgraduális képzést. Kutatási témái a megváltozott munkaképességű, fogyatékos személyek foglalkoztatását befolyásoló tényezők, különös tekintettel a munkavédelemre. 2011-től három fogyatékossági csoportba tartozó (hallássérült, látássérült, mozgáskorlátozott) munkavállalókkal végzett kutatásokat, elsősorban a munkavállalási nehézségeikről, az általuk használt segítőtechnológiákról és az esetlegesen megélt hátrányos megkülönböztetésről a munkavilágában. Részt vesz a szakorvos képzésben és az ELTE BGGYK Gyógypedagógiai Módszertani és Rehabilitációs Intézet Hallássérült személyek pedagógiája és rehabilitációja szakon óraadóként oktat.

PÁL Anita Brigitta

pal.anita@hm.gov.hu

In the past 15 years, I represented law firms, economic companies and commercial companies as an English and German Consecutive Interpreter in various projects. In terms of my studies, I started with law, but since my goal was to find a position in the diplomatic environment, I rather obtained my first diploma as a Specialist in Foreign Affairs and International Relations. After that, I completed my master's degree at the Faculty of Military Science and Defense Officer Training of the National Public Service University as an Expert in International Security and Defense Policy. I would like to deepen my knowledge in the strategic planning of security and defense systems and the effective operation of their organizations as well as in optimizing the possibilities between the defense organizations and institutions, that play a role in central and local defense administration, Currently I am serving with my knowledge the International Directorate of the Defense Economics Bureoau of the Ministry of National Defense as a volunteer operational reserve lieutenant. I trust that in the future I will have the opportunity to represent Hungary with appropriate expertise as a consecutive interpreter or expert in the field of diplomacy, in foreign representation, in the security and defense policy of the EU, and in the NATO.

Az elmúlt 15 évben ügyvédi irodák, gazdasági cégek és kereskedelmi vállalatok angol és német nyelvű képviseletét láttam el különböző projekteken belül. Tanulmányaimat tekintve először jogot tanultam, majd diplomát szereztem nemzetközi tanulmányokon, lévén hogy célom a diplomáciai környezetben való elhelyezkedés volt. Ezt követően a Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Karának mesterképzésen végeztem nemzetközi biztonság- és védelempolitikai szakértőként. Tudásomat szeretném elmélyíteni a védelmi szervezetek, a központi és a helyi védelmi közigazgatásban szerepet játszó intézmények optimalizálásának lehetőségében, illetve a biztonsági és védelmi rendszerek stratégiai tervezésében és szervezeteinek hatékony működtetésében. Tudásommal jelenleg a Honvédelmi Minisztérium Védelemgazdasági Hivatal Nemzetközi Igazgatóságát szolgálom önkéntes műveleti tartalékos hadnagyként. Bízom abban, hogy a későbbiek folyamán lehetőségem nyílik megfelelő szaktudással képviselni Magyarországot konszekutív tolmácsként vagy szakértőként diplomáciai területén, külképviseletben, az EU biztonság- és védelempolitikájában, illetve a NATO-ban.

VALOCIKOVÁ, Cyntia

valocikova.cyntia@uni-obuda.hu

VALOCIKOVÁ, Cyntia graduated with a master's degree in business development at Keleti Faculty of Business and Management of Obuda University (2018) and is currently a PhD student at the Doctoral School on Safety and Security Sciences. During her master's degree, her research moved in the direction of social sciences, and her research experience elaborated. She improved her skills through several domestic and foreign conferences, academics trips and TDKs, and then at the OTDK in 2019 she took second place in the Sociology of Economics section. During her doctoral studies, her field of research changed; however, she continued her work in social sciences and economics. Research focuses on altruism and the dangers of selflessness. The current direction of research is the exploitation of selfless behavior on the Internet, through fraud and deception. However, the research deal with the traditional turnout of altruism, with its development, and incorporation into online interfaces.

VALOCIKOVÁ, Cyntia okleveles közgazdászként végzett vállalkozásfejlesztés mesterszakon az Óbudai Egyetem Keleti Károly Gazdasági Karán (2018), jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskola doktorandusza. A mesterképzés alatt kutatása a társadalomtudományok irányába mozdult, kutatási tapasztalatát széles körben hasznosította. Számos hazai és külföldi konferencián, tanulmányúton, TDK-n részt vett, majd 2019-ben az OTDK-n tanulmányával második helyezést ért el a Gazdaságszociológia szekcióban. A doktori képzés alatt kutatási területe változott, azonban továbbra is a társadalom és gazdaságtudományokra épül. A kutatás középpontjában az altruizmus és az önzetlenséggel járó veszélyek állnak. A kutatás jelenlegi iránya az önzetlen viselkedés internetes kihasználása, csalások, megtévesztések révén. A kutatás azonban foglalkozik az altruizmus hagyományos megjelenésével, fejlődésével és beépülésével az online felületekbe.

Creator of the cover image | **A borítón látható kép alkotója**

BORS Györgyi

borsgyorgyi77@gmail.com

She was born in 1977 in Tapolca, Hungary. The tragic early death of his mother was decisive in her life because she was then raised in state care until she was 18 years old. During her years there, she realized that she found the greatest pleasure in art. She studied graphic art for several years at the Railway School of Music and Fine Arts in Budapest with the painter and sculptor György BENEDEK, and later with Árpád "Pika" NAGY and Zoltán SEBESTYÉN. In 2007 she graduated from the King Zsigmond College with a degree in Cultural Management. From 2017, her master is Kálmán GASZTONYI, from whom she learned the different techniques of oil painting. She is narrative painter. It is important for her to be creative about something, a feeling, an idea, an impression, or even a human quality. She creates using the tools of abstract painting. With her innovative style, she brings experiences, feelings and thoughts with the tools of painting to a universal level that we have all known or experienced in some form. Her work has been successfully featured in various domestic and international competitions and exhibitions (Budapest, London, New Jersey, Hong Kong) and has

Magyarországon, Tapolcán született 1977-ben. Édesanyja tragikus korai halála meghatározó volt az életében, mert ezt követően 18 éves koráig állami gondozásban nevelkedett. Az ott töltött évek alatt jött rá, hogy a művészetben leli a legnagyobb örömet. Grafikai tanulmányokat folytatott több évig Budapesten a Vasutas Zene- és Képzőművészeti Iskolában BENEDEK György festő és szobrászművésznél, majd később NAGY Árpád „Pika"-nál és SEBESTYÉN Zoltánnál is tanult. 2007-ben diplomázott a Zsigmond Király Főiskola Művelődésszervező szakán. 2017-től Mestere GASZTONYI Kálmán, akitől elsajátította az olajfestés különböző technikáit. Narratív festő. Fontos számára, hogy alkotási szóljanak valamiről, egy érzésről, egy gondolatról, egy benyomásról, vagy akár egy emberi tulajdonságról. Az absztrakt festészet eszközeit felhasználva alkot. Innovatív stílusával olyan tapasztalatokat, érzéseket és gondolatokat emel a festészet eszközeivel egyetemes szintre, melyeket mindnyájan ismerünk vagy megéltünk már valamilyen formában. Munkái sikeresen szerepeltek különféle hazai és nemzetközi versenyeken és kiállításokon. (Budapest, London, New

appeared in several contemporary art albums and art magazines. One of her works can also be found in the public collection of the Hungarian Museum of Circus Art. Her expression is geometric and lyrical abstract, which are side by side yet reinforce her art organically intertwined.

Jersey, Hong Kong) Több kortárs művészeti albumban, art magazinban jelentek meg munkái. Egyik alkotása a Magyar Cirkuszművészeti Múzeum közgyűjteményében is megtalálható. Kifejezésmódja a geometriai- és lírai absztrakt, melyek egymás mellett, de mégis szervesen összefonódva erősítik művészetét.

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

Vol 4, No 3, 2022. | **2022. IV. évf. 3. szám**

CONTENT | TARTALOM

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

Security Policy column | Biztonságpolitika rovat

Information Security column | Információbiztonság rovat

Safety and Security in General column | Munkabiztonság rovat

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

Book Review column | Könyvismertetés rovat

GULYÁS Attila

Review about the book Amy B. Zegart: Spies, Lies, and Algorithms: The History and Future of American Intelligence	Recenzió Amy B. Zegart: Spies, Lies, and Algorithms: The History and Future of American Intelligence című könyvéről

83-87

HISTORY, TYPES, APPLICATION AND CONTROL OF DRONES

DRÓNOK FEJLŐDÉSE, CSOPORTOSÍTÁSA, FELHASZNÁLÁSA ÉS ELLENŐRZÉSE

BÁLINT Márton[1]

Abstract

Nowadays thanks to the technical innovations drones plays a very important role in many of the main areas, in public service, in agriculture, in international and domestic business as well as for the military and law enforcement units. Drones raised new legal questions that the old regulations could no longer answer. The presence of drones is now unavoidable, but this technology affects many areas of law, such as rights of personality, the right and conditions of drone usage. But drones also have a significant impact on national security and some public administration procedures. Drones mean a huge potential, but it is necessary to develop an appropriate regulatory safety framework. The technology of pilot-free aerial vehicles will definitely result in major changes and the legislation must react to these changes by creating a flexible legal framework. In this paper I would like to present the basic features of the drone technology and the drone development, and I also aim to analyze the legal environment of the usage of the drones. Our main purpose with this study is to identify and highlight the main emphasis of drone regulations.

Keywords

drone, development, application, technology, legislation

Absztrakt

A drónok műszaki fejlődéséből következően fontos szerepet játszanak életünk több területén is, úgy mint a közigazgatás, mezőgazdaság, nemzetközi és hazai kereskedelem valamint a honvédelem és rendvédelmi szervek életében. A drónok azonban új jogi kérdéseket is felvetettek, melyeket a régi szabályozások nem tudnak megfelelően megválaszolni. A drónok jelenléte már elkerülhetetlen, ez a technológia azonban több jogi területet is érint, például személyiségi jogokat és használati engedélyezési jogokat. Azonban a drónok jelentős szerepet játszanak a nemzetbiztonság és több állami közigazgatási szerv működésében is. A drónok jelentős felhasználási potenciált rejtenek magukban, mindemellett a biztonságos használatához elengedhetetlen a megfelelő szabályozási keretek felállítása. Az pilóta nélküli légi járművek technológiája jelentős változásokat von maga után, és a jogalkotóknak ezeket a változásokat megfelelő flexibilis jogi keretek kialakításával szükséges lekövetni. Jelen cikkünkben bemutatjuk a drón technológia és drón fejlesztések alapvető elemeit, valamint elemezzük a drón használat jogi környezetét, fő célunk a drónszabályozás legfontosabb aspektusainak azonosítása és kiemelése.

Kulcsszavak

drónok, fejlődés, felhasználás, technológia, szabályozás

[1] hubalmar@gmail.com | ORCID: 0000-0002-5703-5584 | PhD Student, Óbuda University Doctoral School for Safety and Security Sciences | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

INTRODUCTION

By preparing this paper I used different types of secondary data collection methods. In addition to the scientific articles available on the Internet, as well as authentic reports, published studies, and published interviews, the published literature and the published results of previous scientific research were also useful. In addition, the information leaflets and guiding advice published on the websites of the official bodies greatly contributed to the processing of the topic, and I was able to study the legal background of the examined topic firsthand through the published legislation, international treaties and other legal documents.

The paper is based on the material of various monographs, collections and articles in scientific journals. I would like to outline the legal background of the research area of the dissertation, relying on the relevant legislation in force and some sources in the legal literature.

HISTORICAL BACKGROUND

One would think that drones are the result of the technical developments of modern times. In reality, as many developments, it has a history of several decades. Moreover, its development is far from being finished, it is still ongoing in order to propose always better and more modern drones on the market, easily accessible to private consumers.

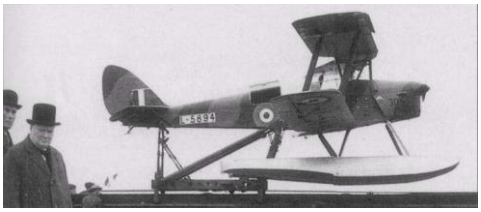
As for most of the technical findings, the drones are originating from the military industry. Back to the end of the 19th century, the need to developing a flying vehicle without pilot sitting in it has been risen. The first written note about it dates from 1849, but of course at that time it was about a very rudimentary version and changes in wind and weather conditions mostly deviated them from their original destination. In 1849, Austrian armies deployed against Venice unmanned aerial vehicles that are considered as predecessors of the drones. The vehicles were hot air balloons and were filled with explosives that were detonated by a timer. Following calibration settings based on preparatory calculations, the device was sent over the target are by wind force. These vehicles are not considered as UAV, because they did not meet the requirements of the modern drones, since although they were unmanned aircrafts, nobody could control them. [1]

The next important tool was called the Kettering Bug, a development during World War I, but it was not actually deployed in the war. It looked like a two-deck plane, but it didn't have a wheel, it got off a four-wheeled car running on rails.

1. Picture: Kettering Bug.: https://www.daviddarling.info/encyclopedia/K/Kettering_Bug.html

He was unable to land, but was not needed as planned, as soon as he reached the designated target, the engine stopped, the wings detached from his fuselage, and the explosive-packed fuselage crashed into the ground like a torpedo. It was also impossible to control, but it contained important components that formed the basis of the structure of remotely controlled machines still in use today. The heading was controlled by a gyroscope, and the altitude was controlled by a barometer. [2]

The first real drone dates from 1935, was called DH 82B Queen Bee, and was used by the British Royal Navy for practice, target shooting. It was remotely controllable, able to land and take off, and was a reusable device as long as it was not damaged excessively during exercise. Moreover, the name drone used today is also related to this device: when Delmer Fahrney, commander of the U.S. Navy, was commissioned to develop a device similar to the British Queen Bee. Fahrney - out of respect for the name of the original device – named his own development as "drone", meaning male bee, which has remained in popular use ever since. [3]



2. Picture: DH 82B Queen Bee. https://hushkit.net/2013/10/01/ka-boom-a-gallery-of-target-drones/de-havilland-dh82b-queen-bee/

Unmanned aerial vehicles were used for military purposes as early as the 20th century. They have been used since the beginning of the 20th century, in the 80s and 90s, although thousands of such devices were already in the possession of the army, with which they carried out reconnaissance and espionage tasks or mounted bombs and firearms on them for attacking purposes. [4]

The technology of unmanned aerial vehicles became essentially widespread in the 1950s, which in those times in the field of military aviation were primarily intended to help train air defense forces by using drones as moving targets. In order for the drones to be used for both direct tactical purposes and reconnaissance tasks, it was necessary to innovate in a direction that took place in the first decades of the millennium. For the first time in the US, the possibility of mass tactical use of drones has been on a more serious agenda under the Obama administration, and the development of automation, robotics, and machine-to-machine communication has greatly contributed to this new role of drones. By analyzing the development patterns of unmanned aerial vehicles so far, it can be concluded that the military and defense application of drones was fundamentally based on the following three goals.

- The drone as a mean of transport: That is, the drone is a device that can be used for transporting and deploying various weapons, thus paralyzing or destroying designated targets, forces, critical infrastructures of the enemy forces.

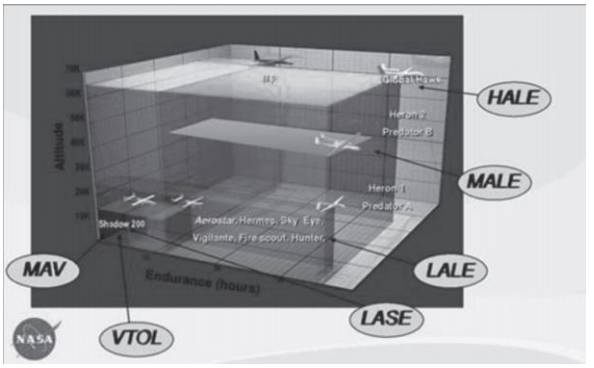
- Acquisition of Information: In order to properly prepare for military deployments, drones can also provide important information that can be used during training of air defense forces, in training simulations as well as directly on battlefields.
- Decision Support: An important military function of drones is that they can be equipped with a variety of sensors that enable drones to obtain information from the air and transmit it immediately, making information decision-makers in charge of the operation more informed. The decision support function of the defense application of drones allows for real and similar to on-field information to be used for by different decision-making levels. [5]

The commercial use of the unmanned vehicles had to wait until the early 2000s years, when the professionals and manufacturers began to discover that these devices could be used for multiple purposes. The breakthrough came in 2013 with the DJI Phantom series, as it already had the parameters and technology to be able to fly without any special training. The development of drones has continued at a steady pace ever since, with areas of use far beyond military applications, such as peaceful use for industrial purposes and more and more for hobby users as well.

The drone, also known as UAV (unmanned aerial vehicle) is a flying device that has no crew on board but can be remotely controlled by its pilot. It can also be equipped with a system of automated or pre-programmed control that can operate part or all of the route without a pilot.

Types of drones can also be grouped according to flight range as well as flight altitude. English designations, based on the above parameters and widely accepted in international practice, are used as follows:

HALE - the designation is used for high altitude, long endurance drones,
MALE - medium altitude, long endurance is used for medium-height but long-range drones,
LALE - used for low altitude but long range unmanned aerial vehicles (low altitude, long endurance),
LASE - the mark typifies low altitude and short endurance drones,
VTOL - designation according to flight functions, refers to drones used for vertical takeoff and landing machines,
MAV - Denotes very low weight (micro air vehicle) aircraft. [6]



3. Picture: Drawing showing the categories of pilot free aircrafts.
http://www.kozszov.org.hu/dokumentumok/UMK_2017/3/05_Dronok_a_kozszolgalatban.pdf

Types of drones can be distinguished according to their use, which can basically be either civil or military. Within the civil category it can be divided according to industrial or hobby use, within the military category reconnaissance or strike categorization is a possible division. In addition to these groups, of course, they can be diverse, can be differentiated according to control (autonomous, remote control, use of several remote controls), drive (electric, explosive motor) equipment level, number of sensors.

However, drones can be classified according to the design solutions as follows.

- **Rigid-wing drones**: The main feature of this type is that the position of the wings to the axles of the aircraft does not actually change. It is important to point out that this construction alone cannot take off from ground. The advantage of these types of drones is that they are capable of higher top speeds and relatively high peaks in height and high impact.
- **Multi-rotor drones**: The rotors are responsible for buoyancy and suspension during horizontal flight. With a classic ground takeoff construction, such drones are also differentiated from the pilot-operated aircrafts in number of rotors. Contrary to pilot-operated aircrafts having one or two rotors, Rotary-wing drones have mostly more than two rotors. Disadvantages are: high power consumption, reduced range and flight time. Although the number of rotors can be arbitrary, it is important to use an even number of rotors (rotating in opposite directions per pair) due to torque compensation. The four (quadro), six (hexa) and eight (octo) rotor versions are also common.
- **Lighter than air drones:** This class includes in effect airships where the buoyancy is provided by a gas lighter than a certain air.
- **Experimental and other drones:** This class usually includes solutions that do not spread more widely, such as flapping wings. [7]

APPLICATION OF THE DRONES

Drones can be used in many situations for a variety of reasons: cost reduction, no need to send people to hard-to-reach or dangerous places, faster and more efficient work.

Civil application

- **Transportation -** Unmanned aerial vehicles have many options for transporting small packages, but for the time being this industry is still quite young, many legal and technological barriers exist. We can use them only in connection to online consuming. However, it is worth working on this type of automation, since not only they allow a faster delivery service, but with a well-chosen central drone base the amount of greenhouse gases from transportation can be reduced, thus contributing to environment protection. [8]
- **Security service -** The use of drones can also be of great benefit in terms of surveillance and patrol. It is able to fly a pre-programmed route and repeat it many times a day, sensors can detect movements and send an alarm to the control center. Moreover, the recordings can be further analyzed to help identify intruders. They can be efficiently used for border surveillance or surveillance of large areas such as highway sections or railroad tracks.

- **Damage management -** Following natural disasters, damages usually occur over a large area the details inside which are difficult to approach quickly. For recovery teams UAV are useful since they can guide them from above, critical areas can be more easily identified without having to send people into unknown conditions. But a disaster doesn't necessarily have to happen to require an area survey. They make high-resolution images of drones or the topographic models they create, which can be used, for example, to survey plots for construction, for map design or for foresters for vegetation observation. [9]
- **Agriculture -** One of the largest and increasingly popular applications of drones is agriculture. The trend may be due to the fact that - similarly to the area survey - it is necessary to survey large, open plots in agriculture, which can often be very cumbersome on foot and not least time consuming. These activities can be performed easily and quickly from the air. Furthermore, there are a number of agricultural activities that can be done with drones, for which practicality and speed are also what advocates for unmanned aerial vehicles. For example, spray drones can be used to quickly and easily treat plants with nutrients and pesticides, and even preventive surveys can be carried out with drones, and based on the analysis of the data obtained, the development status of the plants and the level of infection can be determined that is used as a base for treatment and intervention. Assessing the current condition of plants is also important because it allows the programmed drone to emit extra material in areas where it is needed, so not only will plant care and plant protection be effective, but this method can also guarantee a uniform quality crop in the given cultivation period. [10]
- **Alpinism -** Climbers have to climb to dangerous places or hang from the sides of buildings for avoiding the construction of scaffolding, thus saving costs. However, in several cases, a flying device may be able to replace the role of climbers, further reducing costs and avoiding unnecessary risks. Such a situation could be inspections where human labor is avoidable, such as inspecting radio towers after a storm, inspecting roof tiles, inspecting lightning rods, chimneys, inspecting high-voltage wires.
- **Hobby -** In the last few years, drones for hobby use have started to explode. More and more models appeared in the lower price ranges, and this impressively complex technology has reached a wider range of users. Moreover, thanks to their efficient development, the tools are becoming safer and easier to use year after year. Operation is not more complicated today, than the use of a smartphone or a computer game; most machines are so intuitive that your operator can control them almost immediately after taking the remote unit in hand, no training course is required. In addition, they are equipped with various optical and ultrasonic sensors, using which the device can avoid collisions and accidents.

  The knowledge of hobby drones is catching up with the knowledge of their industrial counterparts, and the technological leap between them is diminishing. More and more tasks can be performed by factory made hobby drones, which previously could only be done with a specially built device.

Public application

The increasing spread of drones may also have an impact on the performance of certain public service tasks and may be helpful for data collection and the rapid and efficient mapping of certain sites, thus contributing with high quality information in decision-making processes.

- **Municipals -** Local municipalities perform a wide range of tasks serving the local public interest and organizing public services. Many municipal tasks could be made simpler and more cost-effective using of the opportunities offered by drones. In this context it is enough to think about how much the local governments have been helped by the introduction of the various GIS systems, which are now used regularly with tangible results. The situation could be similar in the case of drones. Drones could be used in connection with essentially all tasks where some kind of imaging and long-term observation is required. In connection with the tasks of the municipality and the applicability of the overhead line electrical distribution the settlement planning should be emphasized, in the planning and implementation phase of which the drones could serve a huge service.

  Through the drones, local municipals could also create databases that would lay the foundations for positive development in almost all public services affecting the population. Based on the accurate and objective information that municipalities can obtain through drone technology, public services could be improved, municipal asset management could be made more efficient, and public utility services and health programs could be optimized. Municipalities currently use drone technology only on a case-by-case basis but exploring the endless array of possibilities and developing methods will certainly receive increasing emphasis in the future. [11]

- **Environment Protection -** Drones may play an important role in organizing efficient environmental protection and monitoring in the near future. In the field of environmental protection, it is also key to assess a realistic picture of a given problem, which can be worked out either by personal experience, by means, by consistent use, or by a combination of these. There are often situations where environmental authorities and government organizations cannot access some delicate areas - because they are very difficult to reach, or precisely because it is dangerous to human life - thus it is difficult to assess the actual damages and determine the necessary recovery measures. In such cases, drones can provide a very useful service, as they can access areas whose condition can only be estimated by estimation or inference.

- **Military, police, disaster protection/management -** The work of the police can also be greatly aided by various drones. By monitoring an area with a higher crime rate, the number of cases that can occur can be greatly reduced, and it can also improve the sense of security of the civilian population in the area.

  Drones are also a great help in assessing forest fires and various natural disasters. For example, we can get a picture of the area affected by a flood. We can track changes on a minute-by-minute basis, so we can react much faster to events and minimize additional losses and damages. UAVs make it easier to control various

wildlife damages, inland waters and other damage, following possibly a fully automated process.

The use of drones is also of great importance in the field of national security, especially in preventing attacks against individual states and in preparation for defense actions. Terrorism as an asymmetric warfare, and there seems to be a paradigm shift in defense views about the war, brought the use of drones in national security and defense. This is because it is one of the most widely used weapons by terrorist organizations, and in case of attacks by bombing with the hell machine, the drones can perform a special and grateful service in finding and neutralizing them. Considering that the decontamination and detection of explosives requires special expertise, and that the recordings made by drones can be transmitted even over long geographical distances, it is also feasible to be able to make an expert analysis of a hell machine in a different location in physical space. [12]

In general, drones can be used successfully in many areas of the public service, and essentially almost all tasks previously performed with a pilot-controlled aircraft will likely be able to be performed with drones in the near future.

THE REGULATION OF THE UAV

At first glance, drones may seem like harmless toys, but with the development of technology, more and more complicated tasks can be performed with them in many cases, already completely automatically, without human intervention. With the help of the image and sound recording devices that can be mounted on them, it is easy to collect data almost unnoticed, or in case of improper use, the device can be extremely dangerous.

Another problem is the restriction of airspace. It is not obvious to many people, but you can't fly a drone just anywhere. Also a few years ago, a drone strayed into the White House area, causing the entire building to be locked down for several hours until it was ascertained that the device in not a cause for alarm.

In addition to the incidents listed above, there are a number of other problems that can arise during the flight of a drone, so in order to avoid accidents and prevent illegal data collection, it is necessary to introduce regulations, bind flying to permit and registration, and inform pilots about the dangers of drones. Up to the last regulation, there was no uniform EU legislation on the use of unmanned aerial vehicles, so legislation varies from country to country.

The European Aviation Safety Agency (EASA) has a special role to play in developing the rules on drones, with the task of drawing up rules and drafting legislation on aviation safety.

The Agency has made the following recommendations:

- The drone should always be in our field of vision
- Check the device and plan the flight before each flight
- Always read the information about the device carefully
- Do not fly near airports or helicopter landings
- Do not fly while endangering others
- Do not fly over people, vehicles or private property
- Do not fly closer than 50m to people or private property

- Do not fly higher than 150m

In September 2015, the agency issued a framework of 27 actual proposals for drones. This was the first single draft regulation to divide the instruments into three categories: "open" (low risk), "specific" (medium risk) and "certified" (high risk). [13]

EASA has created the following categories:

- **"Open" category -** No prior permits are required to fly, and compliance with the rules is ensured by industry standards, some bylaws, and technological constraints. In case of violation, the police can intervene. This category includes devices with a maximum weight of 25 kg, such as civilian drones, which must always be kept in our field of vision during flight, must not fly above 150 m, or have a so-called "geofencing" mode, which prevents to fly to a restricted area with the device. [14]
- **"Specific" category -** A risk analysis issued by the operator or the competent authority is required. To facilitate the analysis, standards have been developed that include flights under certain conditions, such as farm work or infrastructure monitoring. This group includes devices that, due to their parameters, no longer fall into the "open" category.
- **"Certified" category -** Because drones in this group are already very similar to piloted aircraft due to their size and technical parameters, the requirements are similarly stringent. Many permits and trainings are required for use, and the operator has many responsibilities. This category includes, for example, drones used by the military. [15]

In developing the regulatory framework for drones, the U-SPACE framework is still worth describing. The recommendation was issued by an organization called SESAR in 2017, which aims to make EU regulation as appropriate as possible. U-space aims to create a framework that supports, on the one hand, routine drone flying and, on the other hand can provide an interface with the relevant authorities as well as with other aviation actors and stakeholders.

At the same time, it is important to clarify that U-space is not an airspace specifically dedicated to drones, not an airspace with pre-designed rigid boundaries, but a cohesive system that is connected at many points and compatible with other airspace users in aviation. with other actors involved.

The regulation demarcates the following three different areas of operation in connection with the operation of drones:

- Urban
- Suburban
- Rural

The U-Space framework was based on the following principles.

- The primary purpose of the regulation must be to ensure that the operation of the drones can be carried out without accident. The requirement for safe and accident-free operation must also cover the protection of persons and objects.
- The principle of equal access to airspace for all users should apply to the use of airspace.

- The framework should also include the necessary mechanisms to support the development of drone-related businesses through competitive and cost-effective service standards.
- During the creation of the framework, the aspect that the regulation must be adaptive and flexibly adaptable in order to meet the emerging needs has been given an important role. This principle is also particularly important because, as a dynamically evolving sector, there is a need for a framework that is appropriate for both technological innovation and business model innovation, that is able to react in a timely manner and that is flexible enough to handle change.
- It is important from the outset for the regulation that, in addition to emphasizing adaptive capabilities, the investment and operation of the system and the maintenance of the system associated costs should be kept to a minimum in order to make the system economically sustainable in the long term.
- A further principle is that, if possible, the new drone regulation can be properly integrated into the system of the already established and successfully functioning aviation and telecommunications networks,
- Carry out complex operations at high frequencies using automated drones under fleet supervision.
- In addition to the above, the regulation of drones must in all cases prioritize the highest possible level of safety and security requirements, which includes cyber protection, the protection of personal data and data protection in general. The protection of the environment is important, and the regulation must protect private property and the inviolability of privacy. [16]

THE HUNGARIAN REGULATION

In this section, I outline the main points of the Hungarian regulations on drones. In Hungary, in order to buy a drone or keep a drone, a separate permit is not required, however, the use of drones is already indirectly subject to a permit. More specifically, the above statement is intended that anyone wishing to enter the airspace with their drone needs an ad hoc airspace use permit. The permit itself is issued by the Ministry of Defense and applies only to the occasional use of airspace by drones. [17]

The current rules have abolished the previous rule that the drone users were required to report their activity, but the new rules do not require the use of drones for sports and private purposes to be reported separately, but occasional use of airspace is an activity subject to licensing.

The decree 392/2016 of the military aviation authority on the ad hoc airspace use license and the conditions for its issuance. (XII. 5.) of the Government defines the following criteria in connection with the permit application: [18]

- The applicant must submit an application for a permit at least thirty days before the drone is flown
- The applicant must indicate in his / her application the planned date and duration of the drone flying.
- The application for a permit must state the planned route of the flight, indicating its exact coordinates and the flight altitude.

- The application must also be accompanied by the permit of the operator of the overlapping airports.
- It is also a condition for accepting the application that the applicant has valid liability insurance.
- The result of the safety assessment related to the planned flight must also be attached to the permit application.
- Finally, the applicant must prove that he has duly paid the procedure fee, and a document certifying this must also be attached to the application. The fee for occasional airspace use according to the current rules is currently 3,000 HUF.

Pursuant to the ad hoc airspace use permit, the authority shall activate the airspace before the drone flight, based on the applicant's telephone call at least thirty minutes before the flight, a notification by telephone of flight ending is also required. The contact telephone number shall be recorded by the authority in the decision granting the permit. [19]

VIOLATIONS

The Cases of the violation of the rules of drones can be divided into several groups. In the following section I present these groups, which highlight the nature of drone regulation violation. The drone usage violation can involve civil or penal responsibilities. According to the rules of the civil law, the damage caused need to be compensated by the blameful. If the drone user during the flying caused a material damage in someone property, it will be refund. The most contentious civil law question is connected to the recordings by drones which is injury to various civil interests, first of all to the right for picture and voice recording.

Violation of the flight rules

The easiest way to violate the drone regulation is the breaching the rules of flight. The rules of the flight are the set of rules related to the use of airspace, for example the requirement of maximum flight altitude, the obligation to register, the training requirements. [20]

Picture and voice recording without authorization

To take a photo or video of someone, you need the verbal, written, or implied consent of that person. This is no different for images taken with a drone camera: we need to seek approval from the party concerned to take, use, and publish photographs. Although it is “only” an offense to take a picture of a person or their apartment in a recognizable way without permission, if the purpose of the observation is proven, for example, the activity is repeated regularly, a crime is already committed that can result in a much more severe punishment.

The authorization of the data subject is not required for the recording and use of the recording in the case of mass recordings and recordings of public performances.

The sanctions of the violations

According to the Hungarian drone regulation in the case the breach of the flight regulation will be fined by the law enforcement authority. The amount of the financial penalty depends on several circumstances. For example:

- The size of the range of the aggrieved parties
- The gravity of the injuring
- The mark of the caused danger and effects
- The duration of the injuring
- The repetition of the injuring conduct
- The extent of the damage
- The possibility of the recoverability
- In view of the extent of the undue advantage obtained by the violator

In all cases the real amount of the fine will be determined by the authority. According to the regulation the amount of the financial penalty reaches 20.000 to 100.000 HUF. [21]

SUMMARY

In this paper I clarified what does unmanned vehicles means and took a brief overview of the history and technical background of the drones. Also, I have briefly reviewed the grouping methods of drones and the main possibilities of the applications, explored the most important EU rules for drones and analyzed the domestic regulations too and analyzed the question of violations and sanctions to them. But, as in other fields of sanctions, one can say that a regulation is only as good as the respect of it is consequently observed. This is all the more difficult since the drone technology is in constant and rapid change, and the adaptation to them is a real challenge for the law making and law enforcement authorities. It seems that a flexible frame legal environment is the right answer to such challenges, and to make them respect is a perpetual task.

REFERENCES

[1] Holman, B.: The first air bomb: Venice, 15 July 18. https://air-minded.org/2009/08/22/the-firstair-bomb-venice-15-july-1849/ Downloaded: 8 January 2021

[2] Hunt, D.: World War 1 History: The Kettering Bug—World's First Drone. https://owlcation.com/humanities/World-War-1-History-The-Kettering-Bug-WorldsFirst-Flying-Bomb, Downloaded: 12. January 2021

[3] Kaag, J. – Kreps, S. Drones and Democratic Peace. Brown Journal of WorldAffairs, 2013 pages 97-109.

[4] Zimmer, Ben: The Flight of 'Drone' From Bees to Planes. lhttps://www.wsj.com/articles/SB10001424127887324110404578625803736954968, Downloaded: 12. January 2021

[5] Kovács L., Ványa L., Haig Zs.: Főbb műszaki elvárások és követelmények a pilóta nélküli repülőgépekkel szemben Magyarországon. pages12-14

[6] Restás, Ágoston: A drónok közszolgálati alkalmazásának lehetőségei. http://www.kozszov.org.hu/dokumentumok/UMK_2017/3/05_Dronok_a_kozszolgalatban.pdf, Downloaded: 14. January 2021

[7] Dobi, Sándor Gábor – Fekete, Róbert Tamás – Rohács, Dániel: Az európai UTM helyzete és jövője. http://www.repulestudomany.hu/folyoirat/2018_2/2018-2-17-0467_Dobi_Sandor_Gabor_et_al.pdf, Downloaded: 14. January 2021
[8] Cargo drones: the future of parcel delivery https://www.rolandberger.com/en/Insights/Publications/Cargo-drones-The-future-of-parcel-delivery.html, Downloaded: 15. January 2021
[9] Restás, Ágoston: A drónok közszolgálati alkalmazásának lehetőségei. http://www.kozszov.org.hu/dokumentumok/UMK_2017/3/05_Dronok_a_kozszolgalatban.pdf, Downloaded: 14. January 2021
[10] Digital Transformation Monitor Drones in agriculture. https://ec.europa.eu/growth/tools-databases/dem/monitor/sites/default/files/Drones_vf.pdf, published: January 2018
[11] Restás, Ágoston: A drónok közszolgálati alkalmazásának lehetőségei. http://www.kozszov.org.hu/dokumentumok/UMK_2017/3/05_Dronok_a_kozszolgalatban.pdf, Downloaded: 14. January 2021
[12] Kovács L., Ványa L., Haig Zs.:Főbb műszaki elvárások és követelmények a pilóta nélküli repülőgépekkel szemben Magyarországon. pages12-14
[13] EASA homepage: https://www.easa.europa.eu/regulations, Downloaded: 3. January 2021
[14] EASA webpage: https://www.easa.europa.eu/domains/civil-drones-rpas/open-category-civil-drones, Downloaded: 3. January 2021
[15] EASA homepage: https://www.easa.europa.eu/regulations, Downloaded: 3. January 2021
[16] SESAR hompage: U-Spase Owerview. https://www.sesarju.eu/U-space, Downloaded: 4. January 2021
[17] Rottler, Violetta: A drónhasználat jogi szabályozásának nemzetközi trendjei és hazai helyzete. Magyar Rendészet 2018/4. pages 157—171
[18] Az eseti légtérhasználati engedélyről, valamint a kiadásának a feltételeiről a katonai légügyi hatóság kijelöléséről szóló 392/2016. (XII. 5.) Korm. rendelet. https://net.jogtar.hu/jogszabaly?docid=a1600392.kor. Downloaded: 4. January 2021
[19] Rottler, Violetta: A drónhasználat jogi szabályozásának nemzetközi trendjei és hazai helyzete. Magyar Rendészet 2018/4. pages 157—171
[20] DOE – Drónpilóták Országos Egyesület official website: https://doe.hu/dron-es-modell-repules-jogi-szabalyozas, Downloaded: 14. January 2021
[21] Dróninfo: https://droninfo.blog.hu/2018/05/03/kideritettuk_miert_es_mennyire_birsagoljak_a_dronozast, Downloaded: 14. January 2021

THE PRESENCE OF ALTRUISTIC BEHAVIOR IN TRUST GAME

AZ ALTRUISTA MAGATARTÁS MEGJELENÉSE A BIZALOMJÁTÉKBAN

VALOCIKOVÁ, Cyntia[1]

Abstract

Altruism spans many fields of science, however, different motivations and also different mechanisms can cause altruistic behavior depending on the situation,. However, most researchers agree that trust and reciprocity are both important components of altruism. With altruism, we give up our own selfish interests for the benefit of others, which can increase the well-being not only of the individual, but of the entire society. In my study, I provide an overview of the appearance of altruism in various disciplines, however, due to its complexity, I do not see it as an action limited to a concept, but rather as a hierarchically structured, developing and changing behavior in the environment. The study then deals with a type of game theory, the trust game. The trust game is a two-step, situational game in which both trust and reciprocity presume altruistic behavior. Therefore, it provides an exciting research basis for a more thorough understanding of altruistic behavior.

Keywords

trust, self-interest, trustgame, altruism, reciprocity

Absztrakt

Az altruizmus számos tudományterületet átölel, azonban más-más motivációk és ugyancsak, helyzettől függően eltérő mechanizmusok idézhetik elő az altruista viselkedést. Abban azonban a legtöbb kutató egyetért, hogy a bizalom és a reciprocitás egyaránt fontos összetevői az altruizmusnak. Az önzetlenséggel mások javára lemondunk saját önző érdekeinkről, mely nem csupán az egyén, hanem az egész társadalom jólétét növelheti. Tanulmányomban kitekintést teszek az altruizmus különböző tudományágakban való megjelenéséről, azonban összetettségénél fogva nem tekintem egy fogalom köré behatárolt cselekedetnek, inkább egy hierarchikusan felépített, fejlődő és környezetben változó magatartásnak. A tanulmányban ezt követően foglalkozom a játékelmélet egy típusával, a bizalomjátékkal. A bizalomjáték olyan kétszereplős, szituációs játék melyben a bizalom és a reciprocitás egyaránt feltételezi az altruista viselkedést. Ennél fogva izgalmas vizsgálati alapot biztosít az altruista magatartás alaposabb megismerésében.

Kulcsszavak

bizalom, önérdek, bizalomjáték, altruizmus, reciprocitás

[1] valocikova.cyntia@uni-obuda.hu | ORCID: 0000-0003-3541-4222 | PhD Student, Óbuda University Doctoral School for Safety and Security Sciences | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

BEVEZETÉS

Az altruizmus olyan önzetlen viselkedés, amely mások jólétével való törődést helyezi az egyén viselkedésének középpontjába. Ez egy elengedhetetlen magatartásforma az élőlények létezése és túlélése szempontjából. Az élet és a társadalmi kontroll fenntartása nagymértékben függ az egyének altruista viselkedésének különböző szintjétől. Ettől fogva, ez a terület széles körben elterjedt és megvitatásra alkalmas, az idők során pedig számos különböző elmélet foglalkozott az állatvilág és az emberek altruista evolúciójának magyarázatával, azonban máig számos korláttal rendelkezik. Az egyénekben lezajló önzetlenség evolúciója jobban megérthető három különböző nézőponton keresztül, mint az altruizmus evolúciója a fajok evolúciójának részeként, az altruizmus evolúciója az emberi civilizáció történetében, és az altruizmus evolúciója az egyén élettartama során. A tiszta altruizmus feltétlen önzetlenség, amely nem várja el a viszonzást, segítséget nyújt, és az elégedettség jóleső érzését éri el mások megsegítésével. A bizalom, mint az altruizmus egy fontos építőköve alapvető fontosságú az emberi társadalom stabilitásához. A kísérleteken alapuló szakirodalom nagy része a bizalom mérésére a bizalomjátékra támaszkodik, mint a bizalom és megbízhatóság egyéni különbségeinek mérésére. A közgazdaságtanban a bizalom mértékeként széles körben alkalmazott bizalomjáték lényege, hogy vajon a két játékos hogyan dönt a bizalom és a bizalomra méltóság dimenziói között [1] [2].

A tanulmányban az altruizmus fogalmát közelítem meg számos szakirodalmi és definíciós szemszögből annak érdekében, hogy közelebb kerüljek ennek a komplex magatartásformának a megértéséhez. Ezt követően a bizalomjáték vizsgálatával igyekszem kísérleti lehetőségek köré építeni az altruizmust. A tanulmány a szakirodalomra támaszkodik, azonban kitekintést enged az altruizmus vizsgálatának lehetőségeire.

AZ ALTRUIZMUS SZERTEÁGAZÓ FOGALMA

A híres filozófus, Thomas Nagel foglalkozott az elsők között az altruizmus definiálásával. A szerző szerint *„az altruizmus alatt nem az önfeláldozást értem, hanem pusztán azt a hajlandóságot, hogy mások érdekeit szem előtt tartva cselekedjünk, bármilyen rejtett szándék nélkül"* [3, p. 79]. Megfigyelhető, hogy a definíció két részre osztható. Az első, mely szerint a cselekménynek mások irányába kell mozdulnia. Ez magában foglalhatja az önfeláldozást, azonban biztosan megköveteli, hogy a következmények befolyásolják az egyén döntését. A második szempont, hogy az önzetlen viselkedést nem feltétlenül az önzésben gyökerező „rejtett szándék" motiválja. Ez nem azt jelenti, hogy önző motiváció nem állhat az altruista viselkedés mögött, azonban ez nem lehet az egyedüli indíték. Amennyiben ebből a definícióból indulunk ki, vajon honnan tudjuk, hogy valaki tényleg altruistán viselkedik? A tisztán, önzetlen célok motiválta altruista viselkedés akkor történik meg, ha nem látjuk. Az altruizmus olyan magatartás, amely nem keretezhető bizonyos rejtett szándékok felismerésével. Az altruizmus vizsgálatára irányuló kísérletek tehát az önzésben gyökerező esetleges rejtett szándékok kiküszöbölésére irányulnak. Az altruizmos alapvető motivációja az adakozásból és önzetlen cselekedetből származó jótett "jóleső" érzése, vagyis az a hasznosság, amelyet közvetlen ellenszolgáltatás igénye nélkül a törődésből nyerünk. Minél erősebb az önzetlen cselekvés iránti vágy, annál nagyobb a személyes elégedettség. Az altruista személyiség kirajzolódása szükségszerűen megelőzheti az altruista cselekedeteket, és így

az altruizmus ténylegesen a nagylelkűségből fakadhat. Azonban a kizárólag rejtett szándéktól mentes altruista viselkedés megjelenése a modern szakirodalomban mér kevésbé elterjedt, és az altruizmusnak számos megjelenési formája került a vizsgálatok középpontjába [4]. A konzekvencialista erkölcselméletek szerint, az altruizmus olyan viselkedést jelent, amely az egyik egyén számára költségekkel jár, a befogadó számára pedig hasznot hoz. A költségek és hasznok számításának módja eltér a kutatási vizsgálatok között, leginkább gazdasági (azaz erőforrás-orientált) és evolúciós megközelítésben. Közgazdasági megközelítésben az altruista viselkedés költséges tevékenység, amely gazdasági előnyöket biztosít a fogadó egyén számára. A költségeket és hasznokat gyakran pénzadományként értelmezik (például a társadalmi értékorientációs szakirodalomban), de néha más erőforrásokat is magukban foglalnak, mint idő vagy energia. Az evolúciós megközelítésben az altruizmus olyan viselkedést tükröz, amely költséges a cselekvő számára és előnyös a befogadó számára. A költségeket és hasznokat az élettartamra vetített közvetlen fitnesz (alkalmasság) alapján határozzák meg. A közgazdasági megközelítéstől eltérően a költségeket és hasznokat nem rövid időtartam alapján kalkulálják, inkább az egyén élete során különböző helyzetekben ismétlődő viselkedésként, mely csak akkor költséges, ha csökkenti az egyén felnőttkoráig tartó saját alkalmasságát az utódlásra. Az áttekintett szempontokon túl azonban úgy tűnik, hogy az altruizmus eredeti jelentéséhez a társadalmi megközelítés áll a legközelebb. Amikor Auguste Comte megalkotta a kifejezést, az altruizmus az egoizmus ellentéte, a kollektivisztikus elvre utalt, mely szerint az egyén valaki más(ok)ért éli az életét. Hasonlóképpen, Bykov az altruizmust erkölcsi normaként határozza meg, amely bizonyos társadalmi elvárásokat támaszt a mások megsegítésére különböző társadalmi kontextusok alapján. Eszerint a meghatározás szerint az altruizmus a társadalmi elvárásokat és a társadalomban való viselkedés vezérelvét tükrözi, mely szerint az egyén elzárkózik a személyes haszontól a csoport javára. Így, míg a proszociális viselkedés társadalmi szempontból a társadalom által elvárt viselkedésre utal, az altruizmus specifikusabb abban a tekintetben, hogy mit várnak el a közösség jólétének elősegítése érdekében. A szociológusok szerint az altruista viselkedés mások jólétének fenntartásában játszik nagy szerepet, így az altruizmus a szociális kompetencia kiemelkedő formája [5].

Az altruizmus egy meghatározó viselkedésforma, melynek fogalmával számos kutató, közgazdász és szociológus foglalkozott már – Piliavin & Charng (1990), Samuelson (1993), Monroe (1994), Michalski (2003) – így nehezen keretezhető be egyetlen definícióval. Az idők során a kutatókban időről időre több kérdés merült fel. Létezik-e tiszta, önzetlen segítségnyújtás? Vannak-e az altruizmusnak különböző típusai? Az evolúcióelmélet hívei a viselkedésgenetikával kötik össze, Richard Dawkins szerint: *„A biológus abban az esetben mond egy viselkedést altruistának, ha az más egyedek számára előnyökkel, az altruista számára viszont hátrányokkal jár”* (Dawkins, 1989, pp. 80-81). A közgazdasági megközelítésben, Hámori Balázs szerint: „*az altruizmust úgy határozhatjuk meg, mint mások jólétének a bevonását az egyén jóléti függvényébe*” (Hámori, 2003, p. 59). Hámori egy másik tanulmányában rámutat arra, hogy *„[…] a közgazdaságtan utóbbi két-három évtizedben tapasztalható fejlődésének megfelelően az önérdeken túli motivációkat, a jó- és rosszindulat eseteit vizsgálja. A gazdaság szereplőire különösen a fejletlen és az átmeneti gazdaságokban oly jellemző irigység és káröröm megváltoztatja az egyéni hasznossági függvényeket, és kapcsolatot teremt az egyéni hasznosságok között. Ugyanígy az altruista és részvétet ta-*

núsító gazdasági szereplők, akiknek sokáig még hosszú távú fennmaradását is kétségbe vonták, nemcsak hogy léteznek, de magatartásukkal átmágnesezik a velük kapcsolatba kerülő önző szereplők viselkedését. Az önző aktorok ezen együttműködése nyomán úgy viselkednek, mintha önzetlenek lennének" (Hámori, 1994, p. 510). Ezek a megfogalmazások sem fedik le teljesen az altruizmust, mivel láthatóan akár tudományágakon belül is eltérőek lehetnek, attól függően, hogy az altruizmus mely megjelenési formáit veszik alapul [6].

Vannak azonban különböző külső és belső aspektusotól függő megjelenési formái is. A legnyilvánvalóbb, hogy az altruista vágy először előidézhető egy egyén veleszületett mechanizmusával, majd pedig kondicionálással megerősíthető. Alkalmazható szemlélet a vágy, mint motiváló mechanizmus etológiai megközelítése a segítő döntés problémájának megoldására. A pszichológiai egoizmus esetén, az egyén önző érdekek alapján választja a cselekvést. Nem szükséges a segítő magatartást tanúsítania, azonban megteheti. Amennyiben megteszi, önző elvekből kiindulva indokolhatja meg a segítő magatartás célszerűségét. A klasszikus altruista viselkedést a tiszta önzetlenség, a nem klasszikus altruizmust pedig önző és önzetlen érdekek egyaránt hajtják. Ezesetben az egyén másokon való segítését nem kell sikernek kísérnie, de mégis vágyakozik a segítő magatartás bemutatására. Az altruista tartalmú vágyak fő forrása a jutalomalapú tanulás. Ez a fajta tanulás egy korábban fellépő vágy megismétlődéséhez vezet azáltal, hogy jutalmazza annak jelenlétét vagy bünteti a hiányát [5].

Batson (2011) az empátia elméletéből kiindulva összpontosított az altruizmus jellemzőinek magyarázatára, mely szerint az egyének ezt a viselkedést azon képességük alapján határozzák meg, mennyire képesek együtt érezni másokkal. Azok az egyének, akik jobban megértik a rászorulók helyzetét, és együtt éreznek velük, nagyobb valószínűséggel tanúsítanak altruista viselkedést. Az empátiát úgy határozhatjuk meg, mint egy olyan belsőleg generált érzelmi állapotot, melyet egy másik személy érzelmi állapota vált ki a jóindulat érzésével kombinálva [7] [8]. Egy más megközelítésben, a pszichoanalitikus felfogás szerint altruista viselkedés két formában jöhet létre. Egyrészt létrejöhet egy altruista figurával való azonosulás során, másrészt a lelkiismeretfurdalás és szorongás leküzdésekor [9]. Az altruista büntetés és jutalmazás fogalmai is két felé ágaznak, míg az altruista bűntetés jelentése egy nyereséges, de méltánytalan helyzet visszautasítása a szociális normák lehetséges megszegésének büntetésére, addig az altruista jutalmazás a bizalom megelőlegezését jelenti a csalás válaszának fennállása esetében is [10].

Az altruizmusnak számos "típusa" ismert, egyike pedig a reciprok altruizmus, mely az "ajándékcsere" egy fajtája, amikor az egyén önzetlenségéért cserébe viszonzást vár a jövőben. Az altruista cserekapcsolatok kockázatközösségnek is tekinthető, ennél fogva a reciprok altruizmus a kockázat megosztásaként működik. Az altruizmus nagyon szoros kapcsolatban áll a bizalommal, azonban a kockázat szempontjának figyelembe vételéve a reciprok altruizmusban megjelenik a kockázat alapú bizalom, mely Das & Teng (2004) megfogalmazásában, Nagy & Schubert (2007) fordításában pedig azt jelenti, *"a bizalom pozitív vélekedés a másik fél magatartásáról akképpen, hogy a körülmények bármiféle változása esetén az nem cselekszik opportunista módon. A bizalom tehát azt jelenti, hogy önkéntesen kockázatot vállalunk abból fakadóan, hogy sebezhetővé válunk a másik fél által"* [11] [12, p. 5]. A megfogalmazásból kiindulva elmondható, hogy a bizalom és a kockázat egymás fordított tükörképe. A bizalom és a kockázat lehet ugyanazon együttműködésen alapuló esemény két teljesen különböző végkifejlete, a kockázat az elkerülendő eredményt hozza,

míg a bizalom a kívánt eredményt. Minél nagyobb a bizalom a két fél között annál kisebb a kockázat, és fordítva. A felek együttműködése során pedig a bizalom mértéke hatással van az egyén kockázatvállalási hajlandóságára, mely szerint minél erősebb a bizalom a két fél között, annál nagyobb mértékben hajlandóak kockázatot vállalni. A megelőlegezett bizalom sikeres vagy sikertelen eredményt hozhat, mivel a bizalmat adó egyén nem irányíthatja, vagy ellenőrizheti a másik fél viselkedését, a döntése és magatartása ennél fogva bizonytalan [13] [11].

Az altruizmus szintjei a biológiai, hierarchikus rendről szóló általános elképzeléseken alapulnak. Ez a séma a sokrétű tudást egy olyan koherens képpé rendezi, amely a lehetséges társadalmi kihívásokból kiindulva motivátorként szerepelnek az altruista viselkedésben. Az első, alapvető szintje az önérdek, mely evolúciós késztetés a cselekvésre. A következő szintje a rokoni altruizmus, mely során a rokonszelekció váltja ki az altruista viselkedést. A rokoni kapcsolatok irányából az altruizmus szintje tovább mozdul az altruistával közvetlen interakcióban lépő egyének irányába, azaz a társas kapcsolat alapú altruizmushoz, majd nem csak az egyén, hanem egy csoport érdekeit is előtérbe helyezve lép a hierarchia magasabb szintjére. Mindezen szintek tartoznak az altruizmus biológiai természetéhez, azonban a csoport érdek már átfedést jelent az altruizmus társadalmi-kulturális természetéhez. Az egyetemes etika faji alapú altruizmust ösztönöz, mely szerint az egyénnek a „szomszédját" azonosnak kell tekintenie önmagával. Ezt követően jelenik meg az empátia, amely más előlény lelkiállapotával való azonosulásának a képessége. Az empátia kiterjesztése pedig nem csupán az előlényekre, hanem a bioszférára, mint az élet biztosításának felelőssége is. Ebben a felfogásban így teljesedik ki az altruizmus, az alsó tartomány mechanizmusai egymásra épülve egészülnek ki, azonban a rendszerben feljebb haladva a genetikai tényezőket nagyrészt felváltják a pszichológiai tényezők [14]. Az altruizmus kiterjesztett modellezési formája a Levine (1998) által létrehozott lineáris függvény:

$$v_i = u_i + \sum_{j \neq 1} \frac{a_i + \lambda a_j}{1 + \lambda} u_j \quad (1)$$

ahol

$$i \neq j$$

$$-1 \leq a \leq 1$$

$$0 \leq \lambda \leq 1$$

A kifizetés monoton függvénye jelenti a hasznosságot, ahol i egyén egy u_i nagyságú közvetlen haszonra tesz szert. A teljes hasznosság (v_i) pedig figyelembe veszi a másik személy hasznosságát is (u_j), az a értékek pedig az önzőség és önzetlenség mértékét adják meg negatív vagy pozitív tartományban. Az altruista viselkedés függővé teszi, hogy az egyik egyén (i) viselkedését, milyen mértékben befolyásolja a másik egyén (j) viselkedése. Az λ érték egyfajta reciprocitásként jelenik meg, hiszen ha értéke nagyobb a nullánál, azt jelenti, hogy a másik játékos kész viszonozni az altruista viselkedést [15] [16]. Az altruizmus modellezése lehetőséget nyújt a közgazdasági problémák megoldására kínált játékelméleti megközelítésre, amelyeknek habár középpontjában nem áll az altruista viselkedés, mégis fontos következtetések vonhatók le.

AZ ALTRUISTA VISELKEDÉS EGY JÁTÉKELMÉLETBEN

A játékelméleti modellek (diktátor-, ultimátum-, bizalomjáték, közlegelők tragédiája) gazdasági szituációk elemzésére szolgáló matematikai összefüggéseket alkalmaznak. Az altruista viselkedés domináns motivációjaként a bizalom kerül középpontba, tanulmányomban így a bizalomjáték gyakorlatát vizsgálom. A bizalomjáték a magatartás mércéjévé vált a bizalom társadalomtudományi vizsgálataiban. Ezt a mércét gyakran használják az egyének és kultúrák közötti bizalom szintjének összehasonlítására, még akkor is, ha ezeket a szinteket befolyásolhatja az egyének kockázathoz való hozzáállása. A bizalom melletti döntés olyan környezetben történik, ahol stratégiai bizonytalanság van, abban az értelemben, hogy az eredményt egy másik fél előre nem determinálható cselekedete határozza meg. A kockázatos döntések ezzel szemben a bizonytalanság állapotában születnek, ahol az eredményt a véletlenek is megszabják. A kockázat az egyik lehetséges viselkedést befolyásoló tényező a bizalom játékban. Amennyiben a bizalom előre jelezhető a kockázat alapú magatartás szerint, a bizalom építésére irányuló magatartásnak szabályokat kell felállítania, mint átláthatóság vagy a bizalom megszegésére irányuló büntetés. Ezzel szemben, ha a bizalom nem a kockázatról szól, akkor az ilyen irányelvek nem hatékonyak a cserekapcsolatok előmozdításában. Azonban a bizalom alapú döntések nem feltétlenül kapcsolódnak szorosan a kockázathoz, mivel az árulástól való félelem is fontos szerepet játszhat a bizalmi döntésben. A kockázat és a bizalom kapcsolata jóval bonyolultabb, az egyén kockázati attitűdje nem jósolja meg a bizalom alapú döntéseket, azonban ez nem jelenti azt, hogy nem befolyásolnák azokat [17]. Fairley et. al (2016) választ kerestek arra, hogy vajon a bizalomjáték során a bizalom magyarázható-e egy egyén kockázatészlelésével. Eredményképp arra a megállapításra jutottak, hogy abban az esetben befolyásolható, ha a kockázatészlelés mértékét (az egyén kockázatkerülő, kockázatsemleges vagy kockázatszerető) a bizalmi döntés során érzékelt bizonytalansághoz igazítjuk [18]. Habár a tanulmány fókuszában nem a kockázat és a bizalom kapcsolata áll, kitekintésként segíthet megérteni a bizalomjátékban mérhető faktorok sokrétűségét.

Berg et al. (1995) bizalomjátéka a bizalom mérésének standard kísérletévé vált. A bizalomjátékban az első szereplőt véletlenszerűen és anonim párosítják egy második szereplővel. A játék során mindkét szereplő pénzbeli juttatást kap. Az első szereplő átruházhatja pénzének egy részét vagy egészét a második szereplőnek. Az összeget a kísérlet vezetője megtöbbszörözve (általában megháromszorozódva) átadja a második szereplőnek, aki végül dönthet úgy, hogy megtartja a teljes összeget, egy részét, vagy akár a kapott összegtől is nagyobb összeget visszaadja az első szereplőnek. Az első szereplő döntését a bizalom megnyilvánulásaként értelmezik, a második szereplő döntését pedig a megbízhatóság mércéjeként. Az első szereplő döntése a bizalom (átadja az összeget) vagy bizalmatlanság (nem adja át az összeget), a bizalmatlanság döntésénél a játék nulla kifizetéssel zárul [19] [20].

A bizalomjátékba fektetett összegek nem feltétlenül azonosítják a bizalmat, csak azt mutatják meg, hogy a tisztán önző szereplő mennyire bízik meg a másikban. Azaz a bizalom mérése a klasszikus bizalomjátékkal azt feltételezi, hogy semmilyen más motiváció nem magyarázza a cselekvést. Feltételezhetjük azonban, hogy az önzőség és a reciprocitás aszimmetrikusan működik. A szereplők visszaadhatják az összeget méltányosságból, ugyanúgy odaadhatja az első szereplő a másik szereplőnek az összeget altruista viselkedésből.

Az első játékos tisztán önző döntése a bizalomjátékban a következő módon modellezhető:

$$\max_{x_s x_o} \int_0^1 u(x_s + r x_o) f(r|v) dr \quad (2)$$

azzal a feltétellel, hogy

$$x_s + p x_o \leq B^t$$

$$p \leq 1$$

Az első szereplő maximalizálja a hasznosságot azáltal, hogy elosztja a rendelkezésre álló pénzeszközöket maga és partnere között. Az x_s érték az első szereplő által megtartott összeg, az x_o érték pedig az a pénzösszeg, amelyet az első szereplő átad a második szereplőnek. Egy egység pénzösszeg megtartásának a költsége 1, egy egység pénz átadásának a költsége a második szereplőnek pedig p. Nincs azonban arra garancia, hogy ha az első szereplő kifizetést is alkalmaz, abból bármennyit is visszakap a második szereplőtől. Legyen r a megtérülés, mint a második szereplő által viszonzott pénzösszeg százalékos aránya, az $f(r|v)$ pedig az a valószínűségi függvény, amely leírja a második szereplő meggyőződését a megtérülésről (r), a v pedig ennek a tranzakciónak a paramétereit jelöli. Az altruizmus lehetőségének figyelembe vétele érdekében a probléma az alábbiak szerint módosítható, mely lehetővé teszi, hogy a haszon függ a kifizetésektől:

$$\max_{x_o} \int_0^1 u(B^t - \tilde{p} x_o, x_o(1 - r)) f(r|v) dr \quad (3)$$

Ebben az általánosabb ábrázolásban egy altruista első szereplő, aki törődik a második szereplővel is választhatja az $x_o > 0$ értéket, ha nem vár semmi viszonzást cserébe a második szereplőtől [21]. Továbbfejlesztett és módosított változata a fenti modellezésnek megtalálható a szakirodalomban — Berg et al. (1995), Bolton (2000) — mely foglalkozik a bizalomjáték szereplőinek döntésmechanizmusával, azonban a bizalom, az altruizmus és a reciprocitás kísérleti módszerekkel való méréséhez elsősorban ismerni kell azt is, hogy az egyének lényegében mennyire törődnek másokkal [19] [22].

ÖSSZEFOGLALÁS

Az altruizmus egy olyan viselkedésforma, melynek pontos definiálása és keretbe foglalása eltér a különböző szakirodalmak között. A viselkedés motivációinak megértése ugyancsak szerteágazó így egyetlen egységes megfogalmazás nem létezik, mely teljes körűen lefedi az altruizmust. A bizalom, reputáció, reciprocitás, génszelekció, kockázat és társadalmi-kulturális elvárások befolyásolják az egyén altruista döntését, mely megmutatkozik a játékelméletek gyakorlatán keresztül is. Habár jelen tanulmányban kizárólag a bizalomjátékra tértem ki, ebben az esetben is nehéz egyetlen modellel lefedni a viselkedést, viszont kiváló útmutatást és kísérleti lehetőségeket nyújtanak. Ha az altruizmust beemeljük a bizalomjátékba, megváltozik az eredeti modell felépítése azáltal, hogy módosul a második szereplő kifizetése. Ha a második szereplő altruista viselkedést mutat, növekedik a kifizetés összege az első szereplőtől, így a második szereplőnek nem éri meg önzően viselkedni, létrejön a társadalom számára is optimális Nash-egyensúly [19] [23] [16].

FELHASZNÁLT FORRÁSOK

[1] D. Cesarini, C. T. Dawes és J. H. Fowler, „Heritability of cooperative behavior in the trust game," PNAS, %1. kötet105, %1. szám10, pp. 3721-3726, 2008.

[2] C. Alós-Ferrer és F. Farolfi, „Trust Games and Beyond," Frontiers in Neuroscience, %1. kötet13, %1. szám887, pp. 1-14, 2019.

[3] T. Nagel, The Possibility of Altruism, %1. kötet2, Michigan: Clarendon, 1970, pp. 391-402.

[4] P. DeScioli és S. Krishna, „Giving to whom? Altruism in different types of relationships," Journal of Economic Psychology, %1. kötet34, pp. 218-228, 2013.

[5] S. Pfattheicher, Y. A. Nielsen és I. Thielmann, „Prosocial behavior and altruism: A review of concepts and definitions," Current Opinion in Psychology, %1. kötet44, pp. 124-129, 2022.

[6] C. Valociková és J. Velencei, „How Did Reciprocity Evolve in Online Communication? Turnout of Reciprocal Altruism," Theory Methodology Practice, %1. kötet16, %1. szám2, pp. 103-113, 2020.

[7] D. C. Batson, Altruism in humans, New York: Oxford University Press, 2011.

[8] R. M. Ali és Z. D. Bozorgi, „The Relationship of Altruistic Behavior, Empathetic Sense, and Social Responsibility with Happiness among University Students," Practice in Clinical Psychology, %1. kötet4, %1. szám1, pp. 51-56, 2016.

[9] E. Molnár, „Az empátia, a szorongás és a személyiség szerepe a reklámok által kiváltott vásárlási döntésekben," Acta Carolus Robertus, %1. kötet10, %1. szám1, pp. 95-109, 2020.

[10] R. Teodorescu és K. Demeter, „Az asszertivitás, empátia és altruizmus kapcsolatának összehasonlító vizsgálata egyházi és állami iskolában tanuló fiataloknál," Erdélyi Pszichológiai Szemle, %1. kötet10, %1. szám1, pp. 58-81, 2009.

[11] T. Das and B. Teng, "The risk-based view of trust: a conceptual framework," Journal of Business and Psychology, vol. 19, no. 1, pp. 85-119, 2004.

[12] A. Schubert és J. Nagy, „A bizalom szerepe az üzleti kapcsolatokban," Budapesti Corvinus Egyetem Vállalatgazdaságtan Intézet, Budapest, 2007.

[13] A. Gelei and I. Dobos , "Bizalom és kockázat a kapcsolatokban – egy kísérlet eredményei," BCE Versenyképesség Kutató Központ, Budapest, 2012.

[14] M. Zwick, „Some Analogies of Hierarchical Order in Biology and Linguistics," in Applied General Systems Research: Recent Developments and Trends, G. Klir, Szerk., New York, Plenum Press, 1978, pp. 521-529.

[15] D. K. Levine, „Modeling Altruism and Spitefulness in Experiments," Review of Economic Dynamics, %1. kötet1, %1. szám3, pp. 593-622, 1998.

[16] S. Karajz, „Az altruista viselkedés modellezési lehetőségei," Észak-magyarországi Stratégiai Füzetek, %1. kötet15, pp. 82-91, 2018.

[17] D. Houser, D. Schunk és J. Winter, „Distinguishing trust from risk: An anatomy of the investment game," Journal of Economic Behavior & Organization, %1. kötet74, %1. szám1-2, pp. 72-81, 2010.

[18] K. Fairley, A. Sanfey, J. Vyrastekova és U. Weitzel, „Trust and risk revisited," Journal of Economic Psychology, %1. kötet57, pp. 74-85, 2016.

[19] J. Berg, J. Dickhaut és K. McCabe, „Trust, reciprocity and social history," Games and Economic Behavior, %1. kötet10, pp. 122-142, 1995.

[20] M. Brülhart és J.-C. Usunier, „Does the trust game measure trust?,” Economics Letters, %1. kötet115, pp. 20-23, 2012.
[21] M. R. Carter és M. Castillo, „The Economic Impacts of Trust and Altruism: An Experimental Approach to Social Capital,” Staff Papers, University of Wisconsin-Madison, Department of Agricultural and Applied Economics, 2002.
[22] G. Bolton és A. Ockenfelds, „“ERC: A Theory of Equity, Reciprocity, and Competition,” American Economic Review, %1. kötetXC, pp. 166-193, 2000.
[23] B. Hámori, Érzelemgazdaságtan, Budapest: Kossuth Kiadó, 2003.

THE ART OF DETERRENCE THE ROLE OF THE MILITARY INDUSTRY IN THE ARMS COMPETITION

AZ ELRETTENTÉS MŰVÉSZETE A HADIIPAR SZEREPE A FEGYVERKEZÉSI VERSENYBEN

PÁL Anita Brigitta[1]

Abstract

Since the end of the Cold War, a thorough restructuring of the armed forces has taken place. What we are witnessing is not the contraction of military forces, but rather the reorganization and increased diversity of the types of military forces. A strong parallel can be shown with the pre-modern period, which is characterized by the diversity of military forces and warfare (feudal levies, civil militias, mercenaries, pirates) and the corresponding diversity of the new dynamics. In my opinion, two interconnected developments played a critical role in bringing about these changes: one was the destructive nature of modern warfare, while the other development was the process known as globalization, which created the ever-increasing interdependence and interdependence of economies and societies. In this article, I want to examine how the art of deterrence and the central perception of the concept of security have been transformed by globalization.

Keywords

globalization, proliferation, transnationalization, defense industry

Absztrakt

A hidegháború vége óta a fegyveres erők alapos szerkezetátalakítása ment végbe. Aminek tanúi vagyunk, az nem a katonai erők összehúzódása, hanem sokkal inkább a katonai erők típusainak átszervezése és megnövekedett sokfélesége. Erős párhuzam mutatható ki a modern kor előtti időszakkal, amelyet a katonai erők és a hadviselés sokfélesége (feudális illetékek, polgári milíciák, zsoldosok, kalózok) az új dinamikához való viszonyulása és megfelelő változatossága jellemez. Véleményem szerint két egymással összefüggő fejlemény hatott kritikusan ezen változások előidézésében: az egyik a modern hadviselés pusztító mivolta, míg a másik fejlemény a globalizáció néven ismert folyamat, ami a gazdaságok és társadalmak egyre növekvő kölcsönös függőségét és interdependenciáját hozta létre. Ebben a cikkben azt kívánom megvizsgálni, hogy az elrettentés művészete és a biztonság fogalmának központi percepciója hogyan alakult át a globalizáció hatására.

Kulcsszavak

globalizáció, proliferáció, transznacionalizáció, védelempar

[1] pal.anita@hm.gov.hu | ORCID: 0000-0003-4750-193X | volunteer operational reserve lieutenant, international relations expert, international security and defense policy expert, Ministry of Defence Defence Economic Bureau International Directorate Customs, Excise and Bordercrossing Branch | önkéntes műveleti tartalékos hadnagy, nemzetközi kapcsolatok szakreferens, nemzetközi biztonság- és védelempolitikai szakértő, nemzetközi kapcsolatok szakreferens, nemzetközi biztonság- és védelempolitikai szakértő, HM Védelemgazdasági Hivatal Nemzetközi Igazgatóság Vám, Jövedék és Határforgalmi Osztály

GLOBALIZÁCIÓ ÉS NEMZETBIZTONSÁG

A globalizáció hatása az egyes államok biztonságára már az 1970-es évek olajválságai kapcsán érzékelhetővé vált, amely kezdte megingatni a katonai és nemzeti biztonság primátusát. A hidegháború végével és a globalizálódás felgyorsulásával a nemzetközi szervezetek és transznacionális vállalatok is a rendszer teljes jogú szereplőivé váltak, az államközpontú gondolkodásmód pedig háttérbe szorult. A nemzetközi rendszerben egyre meghatározóbbá vált – és válik mai is – a szereplők közötti kölcsönös függőség, az interdependencia. Az aktorok egyre nagyobb egymásrautaltsága és az egymásba kapcsolódó érdekhálózatok révén az államok nemzeti biztonságra alapozott felfogásának helyét átvette a nemzetközi biztonság megközelítése. A tömegpusztító fegyverek proliferációját szintén előmozdította a globalizálódás. A nukleáris fegyverkezés és elrettentés, tehát a leginkább katonai kihívások helyét pedig átvették a biztonságpolitikában új típusú biztonsági kihívásokként emlegetett fenyegetések.

Az állami szuverenitás

A globalizáció hatással van a szuverenitásra, amely a biztonsági perspektívához viszonyul. Míg az egymásrautaltság bonyolítja a külső szuverenitást az államok közötti tudatos és ratifikált alkalmazkodás érdekében, addig a globalizáció a termelésre, a pénzügyre, az iparra és más kiterjedések térbeli átrendeződésére fejti ki hatását, amelynek eredményeként a helyi döntések globális következményekkel járnak, és a rutin életet a globális események mozgatják. Így a szuverenitás, a nemzetbiztonság hagyományos megközelítésének alappillére, és amelyet „egy adott területen belül az állampolgárok feletti legitim hatalom monopóliumaként" értelmeznek, mind belül, mind kívül érintett. Egy másik hatás a kollektivizmus iránti növekvő hajlandóság az együttműködésre. A különböző államok más-más biztonsági és gazdasági eszközt kerestek, így abszolút szuverenitásukkal kereskednek egy viszonylag nagyobb biztonsági és gazdasági térért, ezért a nemzetállamok egyre inkább több egymást átfedő szervezet tagjaivá válnak. Előreláthatólag ugyan a globalizációnak egy homogénebb világot kellett volna eredményeznie, de a „hidegháború" vége ellenére egyre nagyobb különbségek mutatkoznak a terrorizmus elleni küzdelem megközelítései között, amely ma az egész földkerekséget érinti. Ebből arra lehet következtetni, hogy a globalizáció hatása a szuverenitásra hibrid.

Gazdasági biztonság

A nemzetközi kereskedelem mai sokrétű szerkezetében, amelyet többnemzetiségű megállapodások, egymásrautaltság és erőforrás-hozzáférhetőség stb. kategorizálnak, a gazdasági biztonság garantálja a nemzetbiztonság legfontosabb elemét. A globalizáció azonban a hagyományos határok érzékelhető gyengüléséhez vezetett, és a közgazdaságtan vált a nemzetbiztonság új pénznemévé. A gazdaság szegénységhez és sivársághoz vezet a lakosság számára. A mai világban az országok célja nem a földek meghódítása, hanem a piacok uralása és ellenőrzése. Arra a következtetésre jutunk, hogy a globalizáció vegyes hatást gyakorol az országokra nemzeti hatalmuktól, elhelyezkedésüktől és nemzetközi helyzetüktől függően. [1]

Társadalmi biztonság

1993-ban a kutatók egy csoportja, a Koppenhágai Iskola, úgy fogalmazta meg a társadalmi biztonság fogalmát, mint a társadalom azon képességét, hogy a változó feltételek és lehetséges vagy tényleges fenyegetések mellett megmaradjon alapvető karakterében. A társadalmi biztonság kiemelt kérdéssé válhat, mivel a közösségi identitás és kultúra mintáit érintő fenyegetésekkel és sebezhető pontokkal kapcsolatos. A migráció fontos oka a demográfiai minták változásának, ezért egy bizonyos számon túl a migráció társadalmi feszültségeket szül. [2]

Katonai biztonság

A haderők új fenyegetései között éles párhuzam vonható a globalizáció által elmosott szektorok és a hatalmi rendszert jellemző polarizáció között, amely felerősítette a terrorizmus jelenségét a hidegháború óta. Az uralkodó környezetben látható átalakulás tapasztalható a háborúk következtében a „clausewitzi államközi háborúktól a harmadik típusú etnikai polgárháborúkon keresztül a kis államok közötti háborúkig". [3] Az átfogó nemzetbiztonság ma már mindenre kiterjed, mint ahogy az emberi biztonságot érintő tágabb témákra is, például az ökológiára, az egészségügyre, az oktatásre és a kereskedelemre, csak hogy néhányat említsek, mivel a veszélyek gazdasági, környezeti és betegségekkel kapcsolatos területeken nyilvánulnak meg. [4]

Környezetbiztonság

A környezetbiztonság az életfenntartás képessége három jelentős elemmel, például a környezetben okozott katonai károk megelőzése vagy helyreállítása, a környezeti eredetű konfliktusok megelőzése vagy az azokra való reagálásnak a képessége, valamint a környezet védelme annak eredendő erkölcsi értékéből fakadóan.

Terrorizmus

Az elmúlt évtizedekben lezajló információs forradalom leginkább a csúcstechnológia szektort érintette, azaz a számítógépek technológiai világának „infokommunikációs" szektorát. Egyik példája a pilóta nélküli repülőeszközök, azaz a dróntechnológia gyors fejlődése, amely komoly kérdéseket vet fel a nemzetbiztonság által viselt kockázatainak szempontjából és azok legitim felhasználásáról. A terroristák általában támadásra, megzavarásra, megfigyelésre vagy propaganda videók készítésére használják fel a dróntechnológia fejlődését. Azonosítható drónprogrammal jelenleg 4 terrorszervezet rendelkezik: a Hezbollah, a Hamász, az Iszlám állam, és a Jabhat Fateh al-Sham. [5]

Hangsúlyozni szeretném, hogy a terrorizmus elterjedése a globalizációval és a technika fejlődésével kéz a kézben járnak. Ahogy összefonódtak, azonnal felgyorsították a pénzügyi átutalások rendszerét és egy eléggé radikális módon újra strukturálták a pénzügyi szektor tevékenységét, mely kihatott a társadalmi tevékenységekre is. Az új vívmányok széles körű elterjedésének köszönhetően az 1990-es évek posztindusztriális társadalmaiból létrejöttek az első információs társadalmak.

A technológiai forradalom másik hozadéka, hogy a nemzetközi gazdaságtan (international economics) és a világgazdaságtan (world economics) az elmúlt másfél évtizedben

jelentős átalakuláson mentek keresztül és kialakították az egyenlőtlenségek különböző dimenzióit. Számos társadalmi-gazdasági tényező kapcsolódik a terrorizmushoz, amelyek szinte minden országban közösek. A gazdaságilag fejlett és a fejlődő országok között azonban jelentős különbségek is megtalálhatóak, amelyek a terrorizmussal összefüggő társadalmi-gazdasági tényezők közé tartoznak:

- A csoportos panaszok magas szintje és a gyenge jogállamiság minden országban összefügg a terrorizmussal.
- A gazdaságilag fejlettebb országokban a társadalmi jogfosztás és kirekesztés fontos szerepet játszik a terrorizmusban.
- A gazdaságilag kevésbé fejlett országokban a vallási vagy etnikai szakadások és a korrupció erősebben kapcsolódnak a magas szintű terrorizmushoz. [6]

A globalizáció egyik legjelentősebb hozadéka, az államok közötti kölcsönös függőségek kialakulása. Az technológia fejlődése és az internet megjelenése megszüntette a tér és az idő korlátokat, így a válságok rendkívül gyorsan át tudnak terjedni egyéb régiókra. Az államok közötti hagyományos hadviselést felváltották a nehezen besorolható konfliktusok, amelyekben kiemelt helyen szerepel az aszimmetrikus és hibrid hadviselés. Az információs technológia által létrehozott újfajta hadviselési módszerek, elmosták a háborúról alkotott eddigi elképzeléseinket és egyfajta "szürkezónás" átmeneti állapotot alakítottak ki a hadviselésben. Az államok és a társadalmak funkciója szempontjából egy olyan világ jött létre, amelyben a digitalizációra épülő elektronikus információs rendszerek biztonsági kockázatot jelentenek.

A globális biztonsági helyzet összességében romló tendenciát mutat. Lévén a regionális és globális hatalmi centrumok közötti versengés mellett, megnőtt az állami és nemállami szereplők lehetősége is hogy érvényt szerezzen saját érdekeinek és gyengítse a nemzetközi rendet.

Az elrettentés központi elemét a 21. század ingatag nemzetközi biztonsági környezetében, a nukleáris és egyéb tömegpusztító fegyverek elterjedésével, valamint a ballisztikus rakéták elleni védelemmel lehet jellemezni. A 21. századi nemzeti és nemzetközi biztonságot fenyegető aszimmetrikus vagy hibrid fenyegetéseket, amelyeket a fejlett technológia lehetővé tesz, rendkívül ingatag geopolitikai környezet kíséri.

AZ ELRETTENTÉS MŰVÉSZETE

Az Egyesült Államok elrettentésének céljai

Az elrettentés alapvető célja továbbra is az, ami a hidegháború alatti elrettentésnek a stratégiai koncepciójának a megszületése óta volt: befolyásolni a nemzetek viselkedését, úgy, hogy ne vállaljanak agressziót az Egyesült Államok globális érdekeivel ellentétben. A hidegháború idején az elrettentési stratégia főként az ellenséges kommunista erőközpontok – a Szovjetunió és szövetségesei, a kommunista Kína és Észak-Korea – agressziójának a megakadályozására irányultak. A stratégiát alapvetően a Szovjetunió és Kína nukleáris támadásainak megakadályozására dolgozták ki.

A nemzetek és más csoportok köre, valamint az amerikaiak által elrettenteni kívánt viselkedéstípusok a hidegháború óta óriási mértékben bővültek. Az Egyesült Államok je

lenlegi biztonsági aggályainak továbbra is magában kell foglalniuk az Egyesült Államok szülőföldjének és azon szövetségeseinek védelmét, akikkel szerződéses kötelezettségeik vannak, és amelyek garantálják a kölcsönös biztonságot. De kiterjednek a nemzetbiztonságukat közvetlenül és közvetve befolyásoló érdekek széles körének védelmére is. Bár ezek a szélesebb körű problémák mindig is nyilvánvalóak voltak, ma már egyértelműbben megfogalmazódnak azon igényük részeként, amelyben a nemzetbiztonságukra ártalmas cselekedeteket elrettenthetik. A probléma kiterjed a tengerekre, a légutakra és a nemzetközi kereskedelemmel és a biztonsággal kapcsolatos tevékenységekre, a szabad felhasználásától a kulcsfontosságú erőforrásokig és az azokat irányító és biztosító nemzetek védelmére, a demokratikus nemzetek közösségének növekedésének ösztönzésére egy békésen fejlődő világban, amelyen keresztül saját biztonságukat is erősítik.

Az agresszió természete, amellyel most az Egyesült Államok foglalkozik, magába foglal számos, a katonai támadástól eltérő tevékenységet is. A nukleáris és más tömegpusztító fegyverek elterjedése ma már a nemzetbiztonsági prioritások egyik legfontosabb szempontja. A gazdasági hadviselés, a politikai felfogás, sőt a humanitárius aggodalmak, amelyeket az etnikai konfliktusokkal együtt járó kiterjedt emberi szenvedés, a nemzetek belső rendjének felbomlása és a regionális konfliktusok váltottak ki, mind-mind előtérbe kerültek, mint közvetlenül vagy közvetve, sokféle módon érintve az Egyesült Államok biztonságát.

Az elrettentés stratégiájának most a nemzetközi színtéren zajló fenyegető vagy erőszakos tevékenység nagy részével kell foglalkozni, amely érintheti az Egyesült Államokat, és az ilyen tevékenység elrettentése az Egyesült Államok szinte minden külpolitikai lépésére kiterjedhet. Nyilvánvaló azonban, hogy a hatékony katonai erő potenciális vagy tényleges alkalmazása lesz minden elrettentő erőfeszítés alapja, talán azoké is, amelyek olyan gazdasági vagy politikai akciókra reagálnak, amelyek kellően veszélyeztetik biztonságunkat. A katonai erő „használata" annyit jelenthet, mint az erők helyzetbe hozása a gyors cselekvéshez, vagy fegyveres konfliktusokat magában foglaló kiválasztott katonai akciók. Ezenkívül az elrettentés kudarcot vallhat, különösen olyan esetekben, amikor a kommunikáció félreérthető, vagy amikor – mint a terrorizmus esetében – az agresszor úgy gondolja, hogy olyan stratégiát dolgoztak ki, amely megtagadhatja a megtorlás lehetőségét. [7]

A fent említett átfogó nemzetbiztonsági megfontolások alapján az Egyesült Államok katonai erőinek képesnek kell lenniük a következő elrettentési célok teljesítésére:

- az Egyesült Államok és szövetségesei elleni külső erők támadásainak elrettentése, az ellenséges nemzetek fegyveres erőitől a nemzeti vagy multinacionális terrorista csoportokig;
- elrettenteni a hasonló támadásokat azon szövetségesek ellen, akikkel kölcsönös biztonsági szerződéseket kötöttek;
- a nukleáris fegyverek és más tömegpusztító fegyverek elterjedésének megakadályozása; és
- elrettenteni a nukleáris fegyverek és más tömegpusztító fegyverek alkalmazását katonai konfliktusokon belül, különösen, ha saját és szövetségeseinek a nemzetbiztonsági érdekei forognak kockán. [7]

Nukleáris fegyverkezési verseny

Noha az Egyesült Államok és a Szovjetunió szövetségesek voltak a második világháború idején, szövetségük a náci Németország 1945 májusi megadását követően megromlott. Az Egyesült Államok, miközben kiterjesztette a hatalmát és befolyását Kelet-Európa felett, gyanakvó szemmel nézte a Szovjetunió világuralmi törekvéseit, míg a Szovjetunió nehezményezte az az Egyesült Államok geopolitikai beavatkozását és saját fegyverkezését. Tovább szította a bizalmatlanságot, az Egyesült Államok közlékenységének hiánya a Szovjetunióval szemben, hogy 1945. augusztus 6-án atombombát terveztek ledobni Hirosimára, bár azt beismerték, hogy a bombát ők készítették. A szovjet kommunista terjeszkedés visszaszorítása érdekében az Egyesült Államok több atomfegyvert épített. De 1949-ben a szovjetek kipróbálták saját atombombájukat, és elkezdődött a hidegháborús nukleáris fegyverkezési verseny. Az Egyesült Államok 1952-ben a rendkívül pusztító hidrogén „szuperbomba" tesztelésével válaszolt, a Szovjetunió pedig 1953-ban követte a példát. Négy évvel később mindkét ország tesztelte első interkontinentális ballisztikus rakétáját, és a fegyverkezési verseny rémisztően új szintre emelkedett. [7]

A nemzetközi színtéren a kormányok alapvető kihívással néznek szembe államuk fennmaradásának biztosításában. Ezt a kihívást „biztonsági dilemmának" nevezik, amely növeli a fegyverkezési versenyt. Ez a nemzetközi rendszer szerkezetéből és a benne rejlő bizonytalanságokból adódik. A biztonsági dilemma megértéséhez látnunk kell, hogy a nemzetközi politikában nincs mindent átható felsőbbrendű világkormány, ahogy rendfenntartó rendőrség sincs. Ráadásul az államok soha nem lehetnek biztosak más államok természetében. Ez a bizonytalanság és az államok döntései ezen kockázatok kezelésére, merítik ki a biztonsági dilemma fogalmát. Dióhéjban ez annyit jelent, hogy bármit tesz egy állam biztonságának fenntartása érdekében, az elromolhat. Ha egy szomszédos államot barátságosnak tekint, és ennek következtében tartózkodik a fegyverkezéstől, miközben a szomszéd valójában ragadozó, akkor az agresszió áldozatává válhat, és megszűnhet létezni. Ha ellenségnek tekinti a szomszédos államot, és ezért tömeges fegyverkezésbe kezd, miközben a szomszédos államnak nincsenek valójában ellenséges szándékai, akkor az ellenfél fenyegetve érzi magát, és elkezdődik a felfegyverkezés ördögi spirálja, melynek eredménye, egy költséges és instabil fegyverkezési verseny lesz, amely háborúvá fajulhat. Minden válságjelenség, előrevetíti annak a lehetőségét, hogy a közösségen belül kialakított konszenzuális normák sérülnek. Tehát bármilyen választási lehetőség adódik is egy állam számára, az mindig magába foglalhat súlyos és kellemetlen következményeket. A hidegháború időszakában az volt a legfőbb kérdés, hogy hogyan lehetne megakadályozni a globális megsemmisítés háborúját. A dilemma enyhítésére a fegyverekkel kapcsolatban, az államok 3 kooperatív biztonsági intézkedés közül választhatnak: fegyverzetellenőrzés, non-proliferáció és leszerelés.

A hidegháborús fegyverkezési verseny: az űrprogram

Az első Szputnyiknak nevezett szovjet műhold fellövése 1957. október 4-én megdöbbentette az Egyesült Államokat és aggodalommal töltötte el a világ többi részét, mivel a hidegháborús fegyverkezési verseny hirtelen űrversennyé változott. [8] Dwight D. Eisenhower elnök megpróbálta tompítani a kilövés sikerével kapcsolatos retorikát, miközben szövetségi forrásokat juttatott az Egyesült Államok űrprogramjába, hogy megelőzze a lemara-

dást. Számos szerencsétlenség és kudarc után az Egyesült Államok 1958. január 31-én sikeresen felbocsátotta első műholdját az űrbe, és az űrverseny folytatódott, miközben mindkét ország új technológiát kutatott, hogy erősebb fegyvereket hozzanak létre.

Kubai Rakétaválság és a fegyverzetszabályozás

A fegyverzet ellenőrzési rendszerek alapvetően biztonságépítő hatással voltak a biztonsági rend átalakításában. A hidegháborús konfrontáció idején a Szovjetunió által vezetett Varsói Szerződés országai és az Egyesült Államok vezette NATO közötti konfliktus potenciális csataterének tekintették az egész földterületet. Több millió katonát és több százezer fegyvert vetettek be minden oldalon, közvetve vagy közvetlenül. Az európai államok területén több ezer robbanófejet állomásoztattak az úgynevezett taktikai nukleáris fegyverekhez. A fegyverzetellenőrzési rendszereket azért fejlesztették ki, hogy megelőzzenek egy nagyobb háborút és különösen, hogy gátat szabjanak a meglepetésszerű támadásoknak. Az is célja volt, hogy fokozatosan kiépítse a bizalmat a két egymással versengő katonai blokk: a NATO és a Varsói Szerződés között. A hidegháború idején bevezetett fegyverzet ellenőrzési intézkedések biztosították, a 1989 utáni biztonsági rend nagyrészt békés átalakítását.

A hidegháborús fegyverkezési verseny 1962-ben fordulóponthoz érkezett, miután a John F. Kennedy-adminisztráció kudarcot vallott Kuba miniszterelnökének, Fidel Castronak a megdöntésére, és Nyikita Hruscsov szovjet miniszterelnök titkos megállapodást hajtott végre a szovjet robbanófejek Kubában való elhelyezéséről, hogy elrettentse a jövőbeni puccskísérleteket.

Miután az amerikai hírszerzés megfigyelte Kubában épülő rakétabázisokat, ostromzárat kényszerítettek az országra, és követelték, hogy a Szovjetunió bontsa le a bázisait és távolítsa el az atomfegyvereket. John F. Kennedy elnök tengeri blokádot hirdetett a szigeten, és két hétig az Egyesült Államokkal és a Szovjetunióval együtt az egész világ felfokozott feszültségben élt. Az Egyesült Államok ígéretével, hogy nem dönti meg Fidel Castro kubai kormányát, a szovjetek lemondták a rakéták telepítésének tervét. A válság után Kennedy ezt írta Hruscsovnak: *„Egyetértek Önnel abban, hogy sürgősen figyelmet kell fordítanunk a leszerelés problémájára. Talán… együtt tudunk valódi előrelépést elérni ezen a létfontosságú területen.”*

A válság békésen ért véget; mindazonáltal mindkét fél és az amerikai közvélemény rettegve készült az atomháborúra, és elkezdték megkérdőjelezni a „kölcsönösen biztosított megsemmisítést” garantáló fegyverek szükségességét. [9]

Az 1962-es kubai rakétaválság küszöbén nem sokon múlott, hogy a világ elkerülte azt a nukleáris háborút, amely az egykori Szovjetunió és az Egyesült Államok között zajlott volna. Azóta pár ország felépítette nukleáris arzenálját, különösen azok, amelyek vitában állnak egymással (pl.: Pakisztán és India). A helyénvaló kérdés azonban a következő: Noha hivatalosan kilenc ország rendelkezik atomfegyverrel, miért volt képes a világ elkerülni az atomháborút? A választ a „nukleáris elrettentés elve” jelenti, amelyet olyan akadémikusok terjesztetek el a hidegháború idején, mint Thomas Schelling és B.D. Berkowitz. Azonban ez a logika még mindig releváns a nukleáris konfliktusok magyarázatában a hidegháború utáni világrendben?

A második világháborút követően a fegyverzetellenőrzés, mint a nemzetek közötti ellenségeskedés korlátozásának új megközelítésének hívei hangsúlyozták, hogy a katonai

fegyverek és a hatalom továbbra is a modern élet része marad. Szerintük irreális, sőt veszélyes, ha egy ország a fegyverek teljes felszámolására törekszik, és ez nem feltétlenül csökkenti a háború valószínűségét. Míg korábban a leszerelést a katonai erő alternatívájának tekintették, most a fegyverzetellenőrzést annak szerves részének tekintik. A fegyverzetellenőrzés hívei egy olyan stabil hatalmi egyensúly megteremtésére törekedtek, amelyben az államokat háborúba bocsátó erők ellenőrizhetők és szabályozhatók. A fegyverzetellenőrzésben tehát a hangsúly az általános stabilitáson van, nem pedig a fegyverek megszüntetésén, és a támogatók elismerik, hogy az erőegyensúly megőrzéséhez néha a fegyverzet növelésére van szükség. [10]

A fegyverzetellenőrzés fejlődése nagyban köszönhető az atomfegyverek létezésének is. Az 1950-es évekre, amikor az Egyesült Államok és a Szovjetunió is rendelkezett nukleáris fegyverekkel, a szuperhatalmak meg voltak győződve arról, hogy nem tudják biztonságosan leszerelni ezeket a fegyvereket. Garantált ellenőrzés hiányában – az a folyamat, amelynek során a szerződés résztvevői ellenőrzik egymás betartását a megállapodáshoz – egyik fél sem tud leszerelést végrehajtani anélkül, hogy sebezhetővé válna a másik fél csalásával szemben. A szuperhatalmak és más, atomfegyverrel rendelkező nemzetek célja tehát nem ezeknek a fegyvereknek a teljes felszámolása, hanem azok ellenőrzése lett, hogy a stabil nukleáris elrettentő erő fennmaradjon. A nukleáris elrettentés elképzelése szerint a nukleáris fegyverekkel rendelkező államot a megtorlás veszélye miatt elriasztják, vagy megakadályozzák attól, hogy azokat egy másik atomhatalommal szemben alkalmazza. Egyetlen állam sem hajlandó megkísérelni az első csapást, mert nem tudja megakadályozni, hogy a másik oldal visszacsapjon. A nukleáris elrettentés tehát az atomfegyverek pusztító erejével szembeni kölcsönös irtózáson alapul. Ezt az elképzelést kölcsönösen biztosított megsemmisítésnek (MAD) hívják. Sok szakértő az elrettentést tekinti a nukleáris fegyverek ellenőrzésének végső céljának. [11]

Mivel sok civil általában azt feltételezi, hogy a fegyverzetellenőrzés és a leszerelés ugyanaz, a köztudat gyakran csalódást okozott, amikor a szerződések a fegyverek számának vagy erejének növekedését eredményezték. A fegyverzetellenőrzés előnye azonban a leszereléssel szemben, hogy még az egymással szemben erősen gyanakvó vagy ellenséges államok is tárgyalhatnak megállapodásokról. A leszerelési egyezmények viszont nagyfokú bizalmat igényelnek, és nem valószínű, hogy ellenséges nemzetek között létrejöjjenek.

A fegyverzetellenőrzést gyakran használják a fegyverkezési verseny elkerülésére – két vagy több hatalom közötti versengő fegyvergyarapodásra. Egy ilyen verseny mindkét fél számára költséges lehet, és a fegyverzet-ellenőrzési szerződések azt a hasznos célt szolgálják, hogy a fegyverkészleteket olyan szintre korlátozzák, amely megőrzi az elrettentést, miközben megőrzi az állam gazdasági és társadalmi erőforrásait más célokra.

A huszonegyedik században a nemzetközi béke és biztonság megőrzésére tett egyik fő erőfeszítés a fegyverek számának és a fegyverek felhasználási módjának ellenőrzése vagy korlátozása volt. E cél elérésének két különböző módja a leszerelés és a fegyverzetellenőrzés. A leszerelés az állam által fenntartott fegyverek és csapatok számának csökkentése. A fegyverzetellenőrzés a lehetséges ellenfelek között kötött szerződésekre vonatkozik, amelyek csökkentik a háború valószínűségét és terjedelmét, általában korlátozva a katonai képességeket. Bár a leszerelés mindig magában foglalja a katonai erők vagy fegyverek csökkentését, a fegyverzetellenőrzés nem. Valójában a fegyverzet-ellenőrzési megállapodások

néha lehetővé teszik a fegyverek növelését egy szerződés egy vagy a többi részes fél számára. [11]

A fegyverzetellenőrzést tekintették a megelőzés egyik legfontosabb módszerének, mint az erőegyensúly felfogásának stabilizálásának módját. A valódi erőegyensúly olyan háború, amelyet valójában egyetlen fél sem nyerhet meg. A fegyverzet-ellenőrzési szerződések által kodifikálhatóvá váltak a helyettesítő erőegyensúly mennyiségi becslései. Erre a helyettesítő erőegyensúlyra pedig úgy tekintettek, mint az egyensúlytalanság észlelésének megelőzésére, amely az egyik vagy másik felet háború indítására késztethette.

Jelentős változásokat hozott a katonai erőre épülő bipoláris világ felbomlása. Ehhez hozzátartozik, hogy a hidegháború évei alatt katonai erővel elfojtott ellentétek, felszínre törtek. A nukleáris háború fenyegetése ugyan megszűnt, de ettől a világ még nem lett egységesebb vagy biztonságosabb. A globalizáció által kialakult stabilitások hiánya miatt kialakult egyenlőtlenségek hatására, megváltozott a biztonsági környezetünk is. Ideológiai, vallási, etnikai, nemzetiségi, területi viták jellemzik a 21. századot. A transznacionalizálódások megváltoztatták a piaci struktúrák láncolatát is, a nemzetközi áru-, technológia- és tőkeáramlás és a fölös globális beruházási tőke sodrásában.

A fegyverkezési verseny folytatódik

A hidegháború 1991-ben ért véget; 1987-ben azonban az Egyesült Államok és a Szovjetunió aláírta a közepes hatótávolságú nukleáris erőkről szóló szerződést (INF), hogy korlátozza minden típusú rakéta hatókörét. Más egyezmények, mint például az 1991-es START 1 szerződés és a 2011-es Új START szerződés, mindkét nemzet ballisztikus fegyverkezési képességének további csökkentését célozták.

Az Egyesült Államok azonban 2019-ben kilépett az INF-szerződésből, mivel úgy vélte, hogy Oroszország nem teljesíti az előírásokat. Bár az Egyesült Államok és Oroszország közötti hidegháború véget ért, sokan azt állítják, hogy a fegyverkezési verseny nem. Más országok megerősítették katonai erejüket, és a modern kori fegyverkezési versenyben vannak, vagy készen állnak arra, hogy belépjenek, ideértve Indiát és Pakisztánt, Észak-Koreát és Dél-Koreát, Iránt és Kínát. [12]

A nukleáris elrettentés logikájának megértése

Ennek a logikának az alapelve, hogy az egyik szereplő megakadályozza a másikat abban, hogy valamilyen cselekvést tegyen azáltal, hogy felkelti az utóbbi félelmét az ebből következő következményektől. Így egy atomháborúban mindkét fél olyan súlyosan megsérül, hogy lehetetlen lesz az egyik vagy a másik felet győztesnek nyilvánítani. Még ha egyikük meg is próbálná megtámadni és hatástalanítani riválisa nukleáris fegyvereit, a másik félnek akkor is maradna elegendő nukleáris fegyvere ahhoz, hogy teljes pusztítást tudjon végezni. [13] Annak ellenére, hogy a Szovjetuniónak 40.000 atomfegyverből álló nukleáris készlete volt, az USA-nak pedig 30.000 nukleáris fegyver, nem vettek részt atomháborúban. A kubai rakétaválság elemzése azt szemlélteti, hogy a csúcson szinte elkerülhetetlennek tűnt a szuperhatalmak közötti nukleáris háború. A vezetők azonban határozottan kitartottak amellett, hogy ne vegyenek részt nukleáris háborúban, mert az mindkét szuperhatalomnak pusztítást okozna. Ez az, ami arra késztette az USA-t, hogy elfogja a szovjet hadihajókat, ahelyett, hogy közvetlenül harcolna, Moszkvát pedig passzív kivonulásra. Az elrettentés a szuperhatalmak közötti tárgyalásokhoz vezetett, mivel a Szovjetunió beleegyezett a rakéták

Kubából való eltávolításába, míg az USA megígérte, hogy nem támadja meg Kubát, Kennedy elnök pedig még az amerikai rakéták Törökországból való eltávolítását is vállalta.

Ennek ellenére sok tudós szkepticizmusát fejezte ki az elrettentés logikájával kapcsolatban, azzal érvelve, hogy pusztán azért, mert elkerülte a Szovjetunió és az USA közötti nukleáris összecsapást, még nem jelenti azt, hogy ez „bizonyított tény". A nukleáris stratégák óvatosságra intették a vezetőket, amikor biztonsági stratégiájukat erre a logikára alapozzák. Például az, hogy Észak-Korea atomháborúval fenyegetőzik az Egyesült Államok ellen, sok tanácsadóban és akadémikusban kételyeket ébresztett.

A nukleáris elrettentés azon a feltételezésen alapul, hogy egy ország saját biztonságának védelme érdekében kerüli a nukleáris háború elindítását.

Aztán ott van ennek a gondolatmenetnek a hitelességének kérdése: vajon az országoknak logikára kell-e alapozniuk biztonsági stratégiájukat? Sokan azzal érveltek, hogy a nukleáris elrettentés logikája nem bevett norma, hanem „hipotézis", így egy nemzet biztonsági stratégiájának erre alapozása szerencsejáték.

Ennek a logikának egy másik nagy hibája a sok ellenőrizhetetlen változó jelenléte, mint például a nukleáris fegyverekkel való visszaélés, ha az irányítás nem megfelelő emberek kezébe kerül, vagy ha egy katona szándékosan nukleáris háborút indít, hogy rossz hírt keltsen. [14]

Miért nem felesleges a nukleáris elrettentés logikája a hidegháború utáni társadalomban?

Vitathatatlan, hogy a világ forgatókönyve megváltozott a Szovjetunió összeomlása és a bipolaritás megszűnése óta. Ahogy a hatalomért folytatott küzdelem fokozódik Kína és az Egyesült Államok között, egyre nagyobb aggodalomra adnak okot a Kína birtokában lévő nukleáris fegyverek, valamint annak lehetősége, hogy ezeket a fegyvereket az Egyesült Államok és India ellen is felhasználja. Aztán ott van Észak-Korea, amely folyamatosan elutasította Washington atommentesítési javaslatát, és továbbra is nukleáris fegyvereket gyárt. Ebben a dolgozatban azzal érvelek, hogy a rivalizálás ellenére a világ el tudta kerülni a nukleáris háborút, és a nukleáris elrettentés logikájának némi elismerést kell adni ebben.

Tekintettel az országok közötti feszült kapcsolatokra, úgy tűnhet, hogy a világ egy időzített bombán ül. Ennek ellenére azonban a nukleáris elrettentés logikája megnyugvást hoz. Először is ott van egy nukleáris háború költség-haszon elemzése. Magától értetődő, hogy a nukleáris fegyverek akkora pusztítást tudnak hozni, hogy a háború költségei meghaladják a hasznot, és ez „elriasztaná" a vezetőket a nukleáris hadviseléstől. Megújult a „második csapásmérő képesség" veszélye, amely visszatartja az országokat attól, hogy nukleáris hadviselésben vegyenek részt.

Másodszor, a személyes érdekek által vezérelt vezetők tisztában vannak azzal a ténnyel, hogy egy atomháborúból senki nem kerülhet ki győztesen. Figyelembe véve Kim Dzsongun-nak az Egyesült Államokkal szembeni nukleáris fenyegetéseit, úgy tűnhet, hogy fennáll az észak-koreai nukleáris támadások lehetősége. Azonban Phenjan nem lépett fel ezekre a fenyegetésekre. Ennek fő oka az, hogy Kim Dzsongun megérthette, hogy egy nukleáris háború „kölcsönös pusztulást" eredményezne, és ez visszatartotta őt egy nukleáris támadástól.

Ennek a logikának egy másik jó példája Dél-Ázsia – egy ingatag régió, három atomhatalommal, amelyek vitában állnak egymással. Annak ellenére, hogy Kínának, Indiának és

Pakisztánnak vannak nukleáris fegyverei, a régió el tudta kerülni a nukleáris összecsapást. Pakisztán és India a második világháború után nukleáris államokká váltak, és azóta egy háborút vívtak. Az 1999-ben vívott Kargil-háborúban azonban nem használtak atomfegyvert. Shamshad Ahmed pakisztáni külügyminiszter-helyettes egy pakisztáni újságnak azt mondta, hogy Pakisztán hajlandó „arzenáljának bármely fegyverét bevetni területi integritásának védelme érdekében". Erre George Fernandez, India akkori védelmi minisztere szerint, ezzel a kijelentéssel Pakisztán „likvidálja" a saját országát. Ez megmutatja, hogyan működik a nukleáris elrettentés, ha mindkét oldalról közvetett fenyegetést tesznek. A kínai-indiai kapcsolatokat elemezve, különös tekintettel a 2020-as ladakh-i helyzetre, nyilvánvaló, hogy mindkét ország ügyelt arra, hogy még a fenyegetésként se használjon atomfegyvert. Mindkét ország kijelentette, hogy a fegyver szerepe szűken a nukleáris zsarolás és kényszer elleni védelemre korlátozódik.

Így a nukleáris elrettentés nem csak egy hidegháborús kifejezés, hanem rendkívül érvényes a hidegháború utáni forgatókönyvben. Az országok megértették a nukleáris elrettentés fontosságát, és fontos szerepet játszik biztonsági stratégiáik kialakításában. Az országok tárgyalási alapként használják, hogy megakadályozzák más országok nukleáris megtorlását. Meg kell azonban jegyezni, hogy a nukleáris elrettentés nem az egyetlen válasz a biztonsági problémákra, és alkalmazása más stratégiák, például béketárgyalások és békeépítő intézkedések alkalmazásával is fokozható. Jóllehet nyilvánvaló, hogy az országok megértették a nukleáris elrettentés fontosságát, a világot a nem állami szereplők nukleáris támadása fenyegeti, mivel az elrettentés, mint stratégia ilyen esetekben valószínűleg kudarcot vallhat. [15]

A nemzetközi tapasztalatok azt mutatják, hogy a nukleáris elrettentés veszélyt jelent a stratégiai stabilitásra, hiszen az erőegyensúlyok helyzete gyorsan változhat egyaránt jóra és rosszra is a globalizáció által megteremtett változó biztonsági környezetben. A hatalmi elitnek fel kell ismernie, hogy a nukleáris fegyverzet-ellenőrzési rendszerek, az emberi civilizáció túlélésének biztosítékai. A világrend, a haditechnika és a stratégiai gondolkodás dinamikus változásai nem jelentik azt, hogy már nincs szükség rá.

FELHASZNÁLT FORRÁSOK

[1] Stephen J. Flanagan, Ellen L. Frost, Richard L. Kugler: Challenges of the Global Century: Report of the Project on Globalization and National Security, National Defense University, 2001.
[2] Fiona B. Adamson: Crossing Borders: International Migration and National Security, The MIT Press, 2006. 199. oldal
[3] Antulio Joseph Echevarria: Globalization and the nature of war, University of Michigan Library, 2003.
[4] Norrin M. Ripsman, T. V. Paul: Globalization and the National Security State: A Framework for Analysis, International Studies Review 2005. 199–227. oldal
[5] Kis-Benedek József: A NEMZETKÖZI TERRORIZMUS JELENLEGI TENDENCIÁI EURÓPÁBAN. KATONAI NEMZETBIZTONSÁGI SZOLGÁLAT FELDERÍTŐ SZEMLE: XVIII. évfolyam 3. szám https://www.knbsz.gov.hu/hu/letoltes/fsz/2019-3.pdf Letöltés ideje: 2021.06.26

[6] Global Terrorism Index 2020: A terrorizmus hatásának mérése. https://reliefweb.int/sites/reliefweb.int/files/resources/GTI-2020-web-2.pdf. Letöltés ideje 2021.09.26.
[7] Richard A. Paulsen: The role of US Nuclear Weapons in the Post-Cold War Era https://www.airuniversity.af.edu/Portals/10/AUPress/Books/b_0058_paulsen_role_nuclear_weapons.pdf (letöltés: 2022.04.04)
[8] The Space Race: https://www.history.com/topics/cold-war/space-race (letöltés: 2022.04.04)
[9] Key Moments in the Cuban Missile Crisis: https://www.history.com/news/cuban-missile-crisis-timeline-jfk-khrushchev (letöltés: 2022.04.11)
[10] THE COST OF DISARMAMENT: DISMANTLEMENT OF WEAPONS AND THE DISPOSAL OF MILITARY SURPLUS: https://www.nonproliferation.org/wp-content/uploads/npr/kopte32.pdf (letöltés: 2022.04.05)
[11] Michael A. Bellesiles: Firearms Regulation: A Historical Overview https://www.jstor.org/stable/1147674 (letöltés: 2022.03.18)
[12] US Leaves INF Treaty, Says Russia 'Solely Responsible': https://www.voanews.com/a/usa_us-leaves-inf-treaty-says-russia-solely-responsible/6173090.html (letöltés: 2022.04.10)
[13] Richard A. Paulsen: The role of US Nuclear Weapons in the Post-Cold War Era https://www.airuniversity.af.edu/Portals/10/AUPress/Books/b_0058_paulsen_role_nuclear_weapons.pdf (letöltés: 2022.04.04)
[14] David Krieger: TEN SERIOUS FLAWS IN NUCLEAR DETERRENCE THEORY https://www.wagingpeace.org/ten-serious-flaws-in-nuclear-deterrence-theory/ (letöltés: 2022.04.04)
[15] Richard A. Paulsen: The role of US Nuclear Weapons in the Post-Cold War Era https://www.airuniversity.af.edu/Portals/10/AUPress/Books/b_0058_paulsen_role_nuclear_weapons.pdf (letöltés: 2022.04.04)

How did Social Engineering change 21st century cybersecurity?

Hogyan változtatta meg a XXI-ik századi kibervédelmet a Social Engineering?[1]

KRASNYÁNSZKI Brúnó[2]

Abstract

My goal with this research is to find the non-informatic attack vectors with which the today's information security experts has the need to face. According to the hypothesis that established before the research, nowadays information security experts don't take appropriate actions to prevent non informatic threats. Due to this reason the non-informatic security infrastructures haven't been established. During my research my next goal was to inspect and compare the differences between the public sector and the market sector. On the top of that I would like to give good practices to SMEs for whom it has now become necessary to deal with cyber security. For my primer research I tried to fill out surveys with IT head of departments and after that I made deep interviews with IT leaders, auditors, cybersecurity researchers and university professors. As my secondary research, I had analysed the available literature!

Keywords

Social Engineering, Information Security, Cyber Security, Security Awareness

Absztrakt

Kutatásom célja, felmérni milyen nem csak informatikai támadásokkal kell szembenéznie napjaink információbiztonsági szakembereinek.

Kutatásom előtt felállított hipotéziseim szerint a jelenlegi informatikai biztonsági szakértők nem foglalkoznak megfelelően a nem informatikai irányultságú támadásokkal és ennek köszönhetően nem épültek ki megfelelő nem informatikai védelmi megoldások sem. Kutatásom során célom továbbá összehasonlítani az állami szektor intézményeit a piaci intézményekkel és jó gyakorlatokat javaslatként megfogalmazni az olyan KKV-k számára, akiknek most vált szükségessé a kiberbiztonsággal foglalkozni. Primer kutatásként kérdőíveket töltettem ki cégek informatikai osztályvezetőivel és ezek után mélyinterjúkat készítettem felső vezetőkkel, auditorokkal, kiberbiztonsági kutatókkal és egyetemi professzorokkal. Szekunder kutatásként pedig a fennálló szakirodalmat elemeztem!

Kulcsszavak

Social Engineering, információbiztonság, kiberbiztonság, biztonságtudatosság

[1] A tanulmány kutatási hátterének alapját a Kutató Dákok Mozgalmában végzett kutatásom adta, amivel 2022-ben a Tudományos Diákkörök XXII. Kárpát-medencei Konferenciáján Harmadik, a XX. KutDiák Tudományos Esszépályázaton második helyezést értem el Műszaki és reáltudományi szekcióban.

[2] brunokrasnyanszki@gmail.com | ORCID: 0000-0002-5672-4919 | university student, Óbuda University John Von Neumann Faculty of Informatics | egyetemi hallgató, Óbudai Egyetem Neumann János Informatika Kar

BEVEZETÉS

Motiváció és a kutatásom felépítése

Mindig is érdekeltek azok a területek, amivel kevesebben foglalkoznak. Nem volt ez másként a biztonsággal sem. Biztonságtudatos felhasználóként láttam magam körül, hogy minden második ismerősömet valamilyen kibertámadás érte. Tízből kettő vette észre ennek következményeit és csupán tízből 1 volt az, akinek az informatikai védelmi megoldásai megakadályozták ezt.

Testközelből láttam amikor 2 multinacionális céget, ahol barátaim gyakornokként dolgoznak teljesen működésképtelenné tett a WannaCry és a NOPetya és a családom majdnem minden tagját is érte már valamilyen támadás. Célom lenne felhívni a vállalatok, állami intézmények és felhasználók figyelmét arra, hogy a XXI-ik században már nem csak informatikai támadás érhet minket és ez ellen szükséges védekeznünk!

Célom továbbá bemutatni a védekezés lehetséges formáit melyben górcső alá veszem az informatikai és nem informatikai védelmi metódusokat összehasonlítva ezek hatékonyságát, integrálhatóságát és költségeit, bemutatva ezeket az opciókat az állami szférára és a piaci cégekre.

Célom továbbá bemutatni a közepesen reprezentatív kutatásomat, melyben azt vizsgáltam, hogy mennyire foglalkozik az állami szektor és a piaci cégek a biztonsági megoldásokkal és a kiberbiztonsági tudatosítással. Primer kutatásként kérdőíveket töltettem ki cégek informatikai osztályvezetőivel és ezek után mély interjúkat készítettem felső vezetőkkel, auditorokkal, kiberbiztonsági kutatókkal és egyetemi professzorokkal. Szekunder kutatásomként pedig a fenn álló szakirodalmat elemeztem.

Ez után szeretném megmutatni azt is, hogy a humán faktor sérülékenysége fuzzy logika segítségével matematikailag mérhető, de nem csak a humán faktor sérülékenysége, hanem a szervezeti biztonságtudatossági kultúra és a biztonságtudatossági oktatások hatékonysága is.

Végül javaslatokat fogalmazok meg arra vonatkozóan mikortól érdemes egy vállalatnál foglalkozni a kiberbiztonsággal és hogy a konvencionális informatikai megoldásokkal vagy inkább az un-konvencionális védelmi kontrollokkal foglalkozzon.

Hipotézis

A hipotézisem az volt, hogy a jelenlegi informatikai biztonsági szakértők nem foglalkoznak megfelelően a nem informatikai jellegű támadásokkal (például a Social Engineeringel) és mind az állami intézmények, mind a piaci cégek estében ez egy komoly probléma, aminek a leghatékonyabb kezelése az lenne, ha megpróbálnánk a dolgozóinkat tudatosítani és a védelmi kiadásokat a hagyományos vírusirtó[3] + tűzfal helyett biztonságtudato-

[3] Hagyományos vírusirtó alatt a reaktív védelmet nyújtó vírusírtókat értem, melyek vírusdefiníciós adatbázis alapján találják meg a kártékony kódokat rendszereinken. A mesterséges intelligencia alapú úgynevezett heurisztikus vírusvédelmet nyújtó szolgáltatást azért nem értem alatta, mivel ez általában nem a vírusírtó szoftver része, hanem egy komplex informatikai biztonsági megoldásnak amely általában a következő elemeket tartalmazza: Adatbázis alapú vírus védelem, viselkedés alapú vírusvédelem, valós idejű védelem (heurisztikus védelem ami az operációs rendszer kritikus részein történő változásokat kiséri figyelemmel), dinamikus tűzfal szolgáltatás, szolgáltatás/applikáció engedély kontroll.

sító képzésekbe, adminisztratív és logikai preventív védelmi kontrollokra próbálnánk fordítani a detektív védelmi mechanizmust tartalmazó vírusirtók helyett, mivel ezeket egy belső, zárt nagyvállalati környezetben nem gondolom hatékonynak a nem tisztán informatikai támadásokkal szemben. Ezen hipotézisemet arra alapozom, hogy a támadások nem csak informatikai eredetűek lehetnek. Ezáltal a vírusírtók egy fizikai térben vagy akár telefonhíváson keresztül történő támadáskor semmilyen védelmet nem tudnak nyújtani.

Ezzel szemben a biztonságtudatosító képzésekkel elérhető, hogy a dolgozók felkészültek legyenek a nem nulla kattintás-os sérülékenységekkel[4] szemben szinte passzív kivédésére és ezen felül a nem informatikai támadásokkal szemben is felkészültek lesznek. További fontos nemzeti kiberbiztonsági szempont az is, hogy a munkahelyen tanult tudást és tapasztalatot haza is vihetik. Ezáltal nem csak a munkahelyük lesz biztonságosabb, hanem a dolgozók családja is biztonságtudatosabb lesz!

MI IS A SOCIAL ENGINEERING?

A fő nem informatikai támadási lehetőség a Social Engineering[5]. „A Social Engineering a befolyásolás és rábeszélés eszközével megtéveszti az embereket, manipulálja vagy meggyőzi őket, hogy a Social Engineer tényleg az, akinek mondja magát. Ennek eredményeként a Social Engineer – technológia használatával vagy anélkül – képes az embereket információszerzés érdekében kihasználni” [2]. A Social Engineering (továbbiakban SE) a leggyakoribb nem informatikán alapuló támadási forma, ahol az emberen, a leggyengébb láncszemen van a hangsúly. Ez azért fontos, mert a legtöbb cég életében már evidensé vált, hogy amennyiben nem költ informatikai védelmi megoldásokra akkor a teljes internetet támadó automata bot net-ek könnyedén átveszik a cégük teljes informatikai irányítási rendszerét, mely nélkül a legtöbb cég nem, vagy akiknek van erre alkalmas BCP-je[6] csökkentett üzemmódban képes csak működni, termelni. De azokkal a támadásokkal, amiket a kiberbiztonsági szakemberek nem észlelnek, a cég vezetésnek pedig rövid távon fel sem tűnik nagyon nehéz foglalkozni. De hogyan is érzékelhetne az a biztonsági elemző egy támadást, aki csak a kibertérből[7] érkező támadásokat vizsgálja? A kérdés egyszerű ahogy a válasz is. Sehogy! Amire a cégek többségének sikerült 2022-re eljutnia az az, hogy megértsék a fizikai és az informatikai biztonság fogalmát (Informatikai biztonság alatt minden olyan védelmi megoldást értünk, ami informatikai eszközökön fut és a fizikai térbe semmilyen módon nem terjed ki. Pl.: vírusirtó és tűzfal informatikai biztonsági megoldás, míg a dolgozóink munkaidő monitorozása adminisztratív biztonsági kontroll), de az olyan veszélyek, amik nem tartoznak bele a fent említett kategóriákba sajnos nem kerülnek detektálásra sem. Sajnos, mivel ahány szakember, annyi definíció. Így a későbbiek folyamán én Krasznay Csaba definícióját fogom használni, mivel véleményem szerint az Ő összefoglalása nyújtja

[4] Nulla kattintás-os sérülékenység alatt minden olyan sérülékenységet értek melynek kihasználásához nem kell humán interakciót igénybe venni. Ezeket a sérülékenységeket nyilvános felfedezésükig nulladik napi sérülékenységnek is nevezzük.[1]

[5] A magyar szakzsargonban nem terjedt még el megfelelő fordítás. Ezért az angol kifejezést fogom használni.

[6] (Business Continuity Plan – üzletmenet folytonosság) [3]

[7] „A kibertér egy számítógépekkel és kommunikációs kapcsolatokkal kialakított, globális hálózatra alapozott, többdimenziós, mesterségesen létrehozott virtuális valóság.” [4]

a legszélesebb körű definíciót. „Az információbiztonság az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és kockázatokkal arányos”. [5]
Míg ezzel szemben „a kiberbiztonság a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez.” [5]
Miért fontos a humán tényező és miért kell vele foglalkoznunk?
Már akkor a humán tényező volt a leggyengébb tényező a kiberbiztonsági képletünkben amikor elkezdtünk jelszavakat használni. Ezeknek bonyolultnak kell lennie és az sem árt, ha az ember megjegyzi őket. Ma már viszont, ha felhívunk egy titkárnőt vagy egy középvezetőt a rendszergazda nevében, hogy behatolás történt és szükségünk lenne a jelszavára annak érdekében, hogy megakadályozzuk az egész céget érintő kibertámadást gondolkodás nélkül hangosan lediktálják!
Ezekre a szituációkra a dolgozókat fel lehet (és az Információ Biztonsági Törvény [továbbiakban IBTV] hatálya alá eső intézményeknek kötelező is!) készíteni biztonságtudatosító képzésekkel.

Ezen képzések elsődleges célja, hogy a dolgozók vegyék észre, ha valami nem stimmel az adott szituációban és amennyiben ezt észrevették kérdéseket tegyenek fel annak megállapítására, hogy ez jelenthet-e kockázatot vagy sem. Az ilyen képzések azért is fontosak, mert az olyan jellegű támadásokat, ahol a dolgozókat felhívják a saját telefonjukon és így próbálják rávenni őket különböző SE technikákkal hozzáférések vagy információk átadására jelenleg nem kivédhető semmilyen műszaki és informatikai megoldással! Ezért az egyetlen megoldás az, ha ilyen képzésekkel felkészítjük a dolgozóinkat, hogy gyanakodjanak, amikor olyat kérnek tőlük, amit a szervezet szabálya szerint tilos vagy valamilyen csalásra adhat okot.

A SOCIAL ENGINEERING TÁMADÁSOK FAJTÁI

Ebben a szekcióban szeretném röviden bemutatni milyen SE támadási formák léteznek, azért, hogy az olvasó jobban el tudja képzelni mi is ez valójában. Ehhez Tóth Tamás az egyes Social Engineering módszerek elhatárolása és rendszerezése című publikációját és Hadnagy Cristopher (2011): Social Engineering The Art of Human Hacking című könyvében leírt példákat fogom bemutatni a leggyakoribb SE támadások típusait és rendszerezéseit! A SE támadásokat két típusra oszthatjuk. A tisztán humán módszerrel elkövetett SE támadások, illetve az IT-alapú módszerek. Amennyiben a támadás hatékonyságát növelni szeretnénk, kombinálhatjuk is a két típust. A két típus alkalmazásának célja a támadó legendájának megerősítése, így az áldozat egy hamis biztonságérzetet kaphat, a „másik forrásból” ezáltál nőni fog a bizalom a támadó felé. [6, p. 87]

Humán alapú támadások típusai:

1. Idegen identitás felhasználása

Mint a nevéből is kiderül valaki másnak a személyazonosságát használja fel a támadó arra, hogy információhoz jusson egy természetes személy megtestesítésével. Nagy cégek esetében felső vezetőként mutatkozik be egy alkalmazottnak akkor nagy rá az esély, hogy az alkalmazott jóhiszeműen megteszi, amit a „felsővezetője" kér tőle. A személyazonosság lopás egy másik formája az úgynevezett „tombstone theft" – sírkőlopás amikor egy nemrég eltűnt vagy elhunyt ember személyazonosságát „felhasználva" rendelkezik az elhunyt jogosultságaival. Ezért használhatja a közösségi felületeit, a bankkártyáját, de akár még a munkahelyi belépőjét is! Amivel jogosulatlanul visszaélve nem csak egy cég üzletmenet folytonosságát veszélyezteti, hanem adott esetben egy kritikus infrastruktúrát is megbéníthat, mivel az adatait nem törlik a rendszerből közvetlen a halála után.
Az is előfordulhat, hogy egy fiktív személy legendáját („Előre kidolgozott, a valóság elemire épülő, nagyrészt ellenőrizhető, dokumentumokkal is alátámasztott fedőtörténet, magyarázat…") [7] alkalmazzák [6, p. 89] a támadásra, mely módszer jól alkalmazható eseti jelleggel amikor rögtönözni kell, de akár hosszú távon is, amikor tetszőleges karakterre van szüksége a támadónak. Ennek hatékony módja lehet, hogyha valaki auditornak adja ki magát, ezáltal beleláthat minden kényes adatba. További nagyon hatékony módszer amikor valaki rendőrtisztnek adja ki magát és egy folyamatban lévő nyomozásban kér segítséget, gyakran olyan emberektől, akik a célponttal rossz kapcsolatot ápolnak. A rendőri legendát erősítheti, ha rendelkezik hamis okmányokkal, egyenruhával, kényszerítő eszközökkel és akár többen is vannak. További kreatív módszer lehet az objektum feltérképezésére amikor karácsony tájékán valaki mikulásjelmezben csokoládét, cukrot osztogatva jelenik meg. Ennek alkalmával körbe „kell" mennie az egész épületben, mely során dokumentálhat és megfigyelhet mindent. [6, p. 88] Ugyanakkor egy egyszerű ételfutár vagy kézbesítő is elég lehet ahhoz, hogy valaki bejusson egy őrzött épületbe. De bármilyen formát is ölt a támadó a legfontosabb teendője az előzetes információgyűjtés, amit ma leggyakrabban nyílt forrású hírszerzéssel (továbbiakban: OSINT – Open Source Intelligence) [8]. Ennek segítségével minden nyilvánosan elérhető (közösségi oldalak [9], munkahely weboldala stb..) adatot összegyűjt annak érdekében, hogy az előzetes információt kihasználva előnyre tegyen szert bizonyos szituációkban.

2. A második gyakori módszer a segítség kérése. Ebben az esetben az emberek jóhiszeműségét és segítőkészségét használja ki a támadó. Ilyen támadási formák lehetnek az ügyfélszolgálat kihasználása. Általában vezetőt megszemélyesítve „felejtik el jelszavukat" amire nagyon gyorsan szükségük van egy határidős feladathoz, mivel ezen a cég pénzügyi helyzete múlik és az sem lenne jó, ha amiatt, hogy nem teljesíti a nagyon sürgős feladatát és a cégét rossz pénzügyi helyzetbe sodorja emiatt le kellene építeni az ügyfélszolgálatot. De működőképes forgatókönyv lehet az is amikor egy „rendszerhiba" miatt egy lehetetlen munkaidő utáni pillanatban hívják fel a dolgozót, hogy remek lenne, amennyiben be tudna fáradni és bejelentkezni egy adatmentésre, mert különben holnapra elvesznek az adatai. A dolgozó, aki nem tud bemenni megkéri, hogy találjanak ki valami megoldást erre, de a „rendszergazda" azt mondja, hogy ez csak akkor lenne lehetséges, ha megadná a jelszavát, ami pedig szigorúan tilos, de a dolgozó csak, hogy ne kelljen bemennie szívesen megadja a jelszavát, ezzel céges szabályzatot szegve [6, pp. 89-90]. Támadási forma lehet még az úgynevezett harmadik fél felhatalmazása, ahol vezetőre hivatkozva kikapcsoltatja a biztonságtechnikai eszközöket, hogy a „szerelők" hozzáférjenek a rendszerhez [6, p. 91].

További támadási módszer az úgynevezett piggybacking (más jogosultságának kihasználása), célja bejutni egy objektumba más személyazonosságának felhasználásával. Például otthon hagyta a belépőkártyáját ezért megkéri az őrszemélyzetet, hogy engedjék be őt [6, p. 91].
Ehhez hasonló módszer az úgynevezett „tailgating" [6, p. 92] – azaz magyarul a szoros követés. Biztonsági intézkedések hiányosak, mivel az alkalmazottak közlekedhetnek csoportosan, a támadó is „csatlakozhat egy csoporthoz". Az utolsó ezen kategóriába tartozó támadási forma a hamis bizalomkeltés. Hamis bizalomkeltés során nem feltétlenül kell más személyazonosságot felvenni. A cél az, hogy pozitív vélemény alakuljon ki róla. Remek technika lehet, ha egy ellenkező nemű dekoratívan öltözött nő vagy férfi leköti az ellenkező nemű őrt/alkalmazottat míg társai bejutnak az objektumba.

3. A következő nagyobb támadási kategória a segítség nyújtás [6, p. 92] módszere, melynek során egy mesterségesen előidézett szituációt alakít ki a támadó. Ez a szituáció úgy van kialakítva, hogy csak a támadó tudjon segíteni. Ez azért hatékony, mert legtöbbször az áldozat keresi fel támadót és ennek okán teljesen más függési lánc alakul ki, amit a támadó ki tud használni.

4. Egy érdekes módszer a fordított Social Engineering [6, p. 93] ahol el kell hitetni a célponttal, hogy egy áldozat. Erre egy tökéletes konspirált megoldás lehet egy telefonhívás, ahol a támadó egy banki alkalmazottnak kiadva magát felhívja, hogy gyanús pénzmozgást észleltek vagy túllépte a hitelkeretét és 2 napja van rendezni különben a bank zárolja a számláját. Ettől az áldozat megijed és bármit hajlandó lenne megtenni, hogy megoldódjon a probléma. A banki ügyintéző felajánlhatja, hogy újra ellenőrzi vagy visszaélést jelent be, amennyiben hitelt érdemlően igazolja magát. A támadó így megszerezhet minden adatot, amit személyazonosság lopáshoz. De akár nagy segítség lehet egy informatikai probléma a nem ismert jelszó beállításában is, mivel rengetegen adják meg vagy építik a születésnapjuk vagy tajszámuk köré a jelszavukat.

5. Ennek a technikának a fejlettebb hosszú távú módja a VALAMIT VALAMIÉRT MÓDSZER [6, p. 93], ahol egy hosszú bizalmas kapcsolatra alapoz a támadó a biztos siker érdekében. Ekkor a támadó küld egy kártékony kódot tartalmazó emailt [10] [11]. A támadást követően az áldozat rögtön a támadóhoz rohan „javításért". A támadó így nem csak a felhasználónév/jelszó párosokat szerezheti meg, hanem minden adatot a laptopról! Illetve viszonzást is várhat ezért cserébe, amit a későbbiekben ki fog tudni használni. Azzal a jócselekedettel, hogy megoldotta a számítógépes „problémáját" még tovább fokozza a legendáját, mint kiváló szakember képét.

6. Két nagyon hasonló támadás a shoulder surfing [6, p. 94] (váll fölött átnézés tükörfordítás szerint, viszont valójában a képernyő jogosulatlan megtekintését jelenti) és a dumpster diving [6, p. 94] (az információ felkutatása a hulladékban). Első esetben a célpont mögött, hogy rálássunk a képernyőjére (kamera is elhelyezhető). Míg a másik esetben elég átkutatni a céges szemetet, ami tartalmazhat kényes adatokat is, de abban az esetben sem jobb a hely-

zet amikor az audit előtt gyorsan kidobott jelszófecnit a kukába való kidobással „semmisítjük meg". Persze gondolhatnánk, hogy „kinek van kedve a szemetemben turkálni???", de „van az a pénz…" (jelen esetben információ)!

IT alapú támadások típusai

A másik nagy csoport az IT alapú támadások [6, p. 94], melynek előnye, hogy nem kell személyesen ellátogatni a helyszínre. Emiatt a támadó személyazonossága is rejtve marad. A kiberteret kihasználva csak annyit kell elhitetni a célponttal, hogy a rendszer, amivel kommunikál valós. Ennek köszönhetően nagyon kevésszer veszik észre azonnal, hogy támadás áldozativá váltak!
Egyik ilyen támadási forma az álweboldalak készítése [6, p.94], sokszor nem is az számít, hogy kik a célpontok, hanem hogy mennyien vannak. Ezek a weboldalak valamilyen szolgáltatást vagy terméket hirdetnek meg, ehhez viszont a felhasználónak regisztrálnia kell! Ezzel a regisztrációval viszont olyan adatokat kényszerül megadni, amivel a célpontunk sebezhetővé válik. Email cím és jelszó mindenhol kötelező, viszont abba kevesen gondolnak bele, hogy ma átlagosan 50-200 helyre vagyunk beregisztrálva ugyanazzal az email/jelszó párossal.

Az egyik, hanem a leghatékonyabb és legflexibilisebb módszer az adathalászat [6, p. 95]. Ennél lesarkítva nem kell mást csinálnunk csak lemásolni egy weboldalt, ahol található bejelentkező panel. Erre az álweboldalra kell eljuttatni a célpontot és megvárni ameddig jóhiszeműen bejelentkezik. Ezzel lényegében bármilyen adatot megszerezhetünk a felhasználótól. Leggyakoribb közösségi oldalak vagy email fiókok esetén mivel ezekbe gyakran kell belépnünk, de az általam végzett kísérletek alapján remekül hasznosítható az egyébként nehezen törhető WPA2[8] -es Wifi jelszavak megszerzésére is. Ennek a támadásnak az a sajátossága, hogy rá kell vennünk egy felhasználót, hogy újra beírja a wifi jelszavát, csak most a mi rogue access pointunk [9] által létrehozott hálózatba.

De nézzük is meg az általános támadás fajtáit:
1. Phising (email alapú adathalász módszer) [6, p. 95]
Ennek a módszernek a segítségével egy hamisított emailt küld a támadó az áldozatnak egy olyan indokkal, hogy sürgősen változtasson jelszót, mert a céget támadás érte, vagy egyszerűen csak tartozása van, amiben egy hivatkozás található egy olyan weboldalra (pl.: bankok, közösségi oldalak, kormányzat által kezelt létfontosságú oldalak például ügyfélkapu) ahol a bejelentkezési panel valójában a támadónak továbbítja az adatokat. Amennyiben nem „körlevélként" kiküldjük százezreknek, hanem csak egy vagy pár kiválasztott személyt támadunk, ahol fontos, hogy ki a célszemély úgy ez a támadási forma részletes felderítést igényel a célpontokról, amit általában OSINT segítségével valósítanak meg és így állítják össze az emailt is, ott ezt a támadási formát spear fishing-nek hívják, mivel csak konkrét célpontokat „akarunk kifogni".

[8] WPA2 (Wi-Fi Protected Access – Wi-Fi védett hozzáférés): A vezeték nélküli kapcsolat titkosítására szolgáló technológia és szabvány
[9] Gonosz hozzáférési pont – Gyakran használják az olyan eszközök elnevezésére, amelyeket a támadó úgy állít be, mint ha valódi hozzáférési pont lenne.

2. Whailing (vezető IT-eszközöket célzó támadás)
Ez a phising vagy spear phising egy olyan formája, ahol kifejezetten az IT vezetőket, magas állami tisztviselőket és egyéb magas rangú, befolyásos embereket céloz meg a támadó.

3. Smishing (SMS alapú adathalászat) [6, p. 98]
Az SMS alapó támadási módszerrel lehetőségünk van nagyobb bizalmat kialakítani, mivel nem közvetlen SMS-ben várunk el cselekedeteket az áldozattól, hanem hogy egy életszerű példát hozzak az áldozat kap egy SMS-t miszerint zárolták a bankszámláját gyanús pénzmozgás miatt. Leírják, hogy bemehet egy bankfiókba vagy felhívhatja az „ügyfélszolgálat" telefonszámát (péntek délután az utóbbit fogja választani). Ekkor az „ügyfélszolgálat" egy készséges adategyeztetés után sűrűn elnézést kér a probléma miatt és feloldja a célszemély számláját.

4. További SE támadás lehet még egy trójai program [6, p. 103] vagy dokumentum, ami ugyan egy hasznos és jóindulatú programnak adja ki magát, de valójában kártékony kódot tartalmaz. Nem kell akkor sem megnyugodni, hogyha „mi sosem töltünk le az internetről semmit", mert elég nagy valószínűséggel nyitottunk meg olyan Word dokumentumot vagy Excel táblát, amit a kollégánktól kaptunk és esetenként még makró is volt benne. Ez ugyan olyan kockázat, mint az internetről letöltött programok. Sosem tudhatjuk, hogy valójában ki küldte az az emailt, amit a főnökünk írt alá!

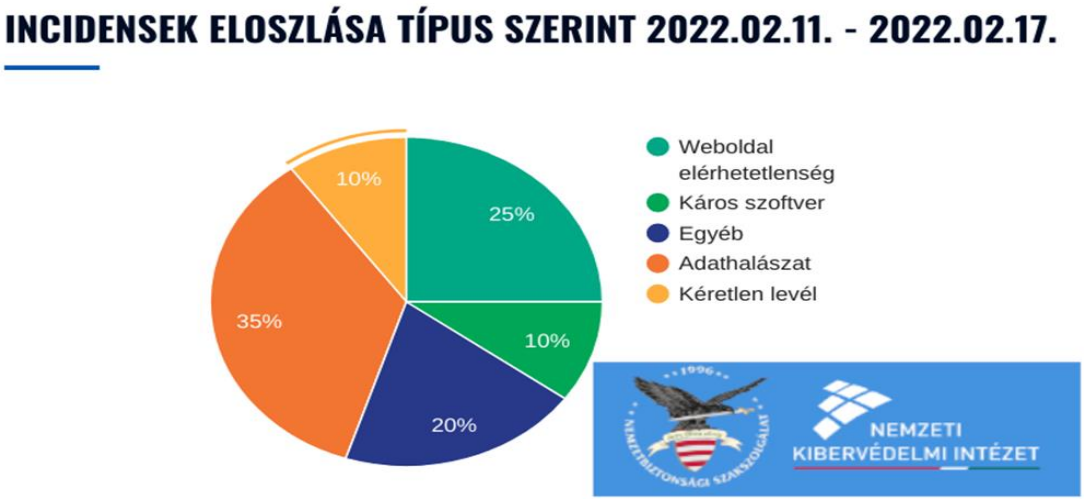
5. Baiting – adathordozó szétszórása [6, p. 104]
Az adathalászat után talán a legnagyobb hatékonysággal végrehajtható támadási forma a baiting során adathordozókat (régebben CD-t, ma már inkább pendrive-okat) hagyunk szándékosan a célobjektum közelében, vagy amennyiben fizikai biztonságot nem implementáltak a célobjektumban akár valamilyen ürügy folyamán be is mehetünk. Remek példa lehet erre amikor egy IT osztályvezetőt megkér egy kedves diák, hogy legyen a konzulense a tárgyévi Tudományos Diákköri Konferencián! Ennek okán könnyedén (és úgymond legálisan) bejut az épületbe, ahonnan, ha nem kísérik ki „szétnézhet", elhozhat iratokat (akár laptopokat is [10]), de elejthet 1-2 pendrive-ot is, amelyet más dolgozók megtalálnak és annak érdekében, hogy „kiderüljön kié" (vagy, hogy már rögtön használatba is vegyék) bedugják a munkahelyi számítógépükbe. Ekkor még nem tudják, de abban a pillanatban fertőzték meg a teljes céges hálózatot!

VIZSGÁLATOK ÉS EREDMÉNYEK

Az informatika fejlődésével együtt fejlődött a hacker kultúra és az államok érdeke is ezen a téren. Míg a kor mérnökeinek leginkább a CD-n terjedő vírusokkal kellett megbirkózniuk, a jelen kor biztonsági szakembereinek már egészen más helyzetük van. Nem elég pusztán jó informatikai vagy műszaki szakembernek lenniük. A kiberbiztonság ma már 95%-ban stratégia (soft defense) és csak 5%-ban technikai védelem (hard defense). [5, s. 4] Minden szakembernek, aki ma foglalkozik védelmi (vagy támadó) megoldásokkal

[10] Konzultáción elhangzott mondat: „Úgy a legkönnyebb laptopot lopni egy cégtől, hogy ebédidőben egy üres laptoptáskával besétálunk az épületbe, majd, amikor már mindenki elment enni csak „megkeressük a sajátunkat" és kisétálunk az épületből!"

el kell gondolkoznia miért alakult ez így? Az információ biztonság sosem volt még ennyire fontos, mint napjainkban, de nem védhetünk mindent technikával [13], mert a támadások sem csak informatikai jellegűek! A támadások 2022-ben akár 75%-ban11 is tartalmazhatnak olyan támadási vektort, ami nem informatikán, hanem pszichológián alapszik.



1. ábra: Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet Incidensek eloszlása 2022.02.11-17 Szerző által módosított diagram

Ennek oka az, hogy az ember nem tudatos, amikor információbiztonságról van szó, mivel a kibertér még csak pár éve létezik és nem alakultak ki azok a védekezési mechanizmusok, amik a fizikai dimenzióban már kialakultak [14] (pl.: Őseink megtanulták, hogy az éhes oroszlán elől el kell futni, de az adathalász e-mailekre való kattintás ellen még nem alakult az üss vagy fuss reakcióhoz hasonló védekezési mechanizmus). Erre rájöttek a támadók (támadók alatt innentől olyan szakembereket értek, akik vagy törvényi felhatalmazással [állam által támogatott hackerek pl.: Kiber katonák, kiber hírszerzők (CYBINT[12]), kiber nyomozók vagy egyéb az ország törvényei alapján felhatalmazott és jogos bűnüldözési vagy nemzetbiztonsági cél érdekében cselekvő személyek], vagy törvényi felhatalmazás nélküli kiberbűnözők[13] , köznapi értelemben vett szürke vagy fekete kalapos hackerek [16], kiber terroristák[14] [15] és ipari kémek [17] is) is. Ezen felül az informatika rohamos fejlődésével az informatikai biztonság is fejlődött, ennek okán bonyolultabbá és erőforrás igényesebbé váltak ezen támadási vektorok. Ennek köszönhetően csökkentek a technológiai sérülékenységek és emiatt a támadások is [6, p. 87]. Ez egészen pontosan azt jelenti, hogy

[11] 1. ábra adatai alapján
[12] Cyber Intelligence – Kiberhírszerzés [18]
[13] „A kiberbűnözés (…) az informatikai eszközök segítségével olyan illegális cselekmények elkövetése, amely a támadóknak anyagi haszonnal kecsegtet.” [15]
[14] Olyan terroristák, akik nem a fizikai dimenzióban, hanem a kibertérben akarnak kárt okozni. pl.: Kritikus infrastruktúrákat elérhetetlenné tenni
[15] A témával, mint terrorizmus elleni védekezés lásd: [19]

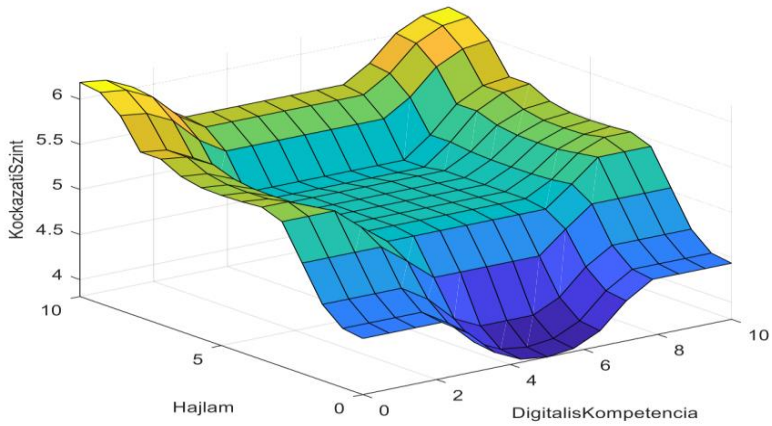
hatékonyabbnak találták, ha nem kattintás nélküli sérülékenységeket[16] keresnek, hanem csak a kártékony kódot juttatják el a célpont rendszerére és azt a felhasználó saját elgondolásból (igaz pszichológiai manipuláció hatására) fogja futtatni! Vagy kártékony kód helyett csupán nemes egyszerűséggel megkérik a felhasználót, hogy jelentkezzenek be a felhasználói profiljukba (ezt leggyakrabban egy úgynevezett phising-gel[17] vagy Smishingel[18] hajtják végre). Csak, hogy ebben az esetben nem a profiljukba jelentkeznek be (amennyiben profi támadóval van dolgunk a fiókunkba is bejelentkezünk és észre sem fogjuk venni, hogy bármi is történt), hanem a támadóknak adták meg az adataikat.
A SE típusú támadások különösen veszélyesek olyan célpontok ellen, akik nem tudatosan (itt csak a hagyományos tudatosságot értem, nem a biztonságtudatosságot) használják az informatikai eszközöket, például kisgyermekek vagy nyugdíjasok. A támadók gyakran ezen csoportokat célozzák meg botnetek építése céljából, mivel szinte garantált a siker! A botneteket pedig a támadó típusától függően pénzért a Dark Net-en eladásra bocsájthatják, vagy az adott állam kiberhadseregébe [21] [22] integrálódva indíthatnak kiberműveleteket ellenérdekelt országok infrastruktúrája ellen. [23] Az ilyen jellegű támadások közül a leggyakoribb a DDOS[19] támadás, melynek hatására az interneten keresztül elérhető szolgáltatások nem lesznek elérhetőek. Ezzel nagymértékű anyagi kárt okoz a cégeknek, mindazonáltal a civil lakosság körében kitörő pánik is hatalmas tud lenni, ami eseteként nagyobb kárt okoz. [24] [25]A SE támadásoknak az erőfölénye abban rejlik, hogy nem csak informatikai támadási vektorokat alkalmaznak, hanem pszichológiákat is, aminek kezelésére a cégek alapvetően informatikai biztonsággal foglalkozó szakemberei nem állnak készen! [20] Az informatikai támadások is mindig egy lépéssel a védelmi megoldások előtt járnak ebben a macska – egér játékban, de az emberi sérülékenységgel egy olyan tényezőt viszünk be az egyenletbe, ami konvencionális védelmi megoldásokkal nem, vagy csak részlegesen detektálható, kivédése pedig csak alacsony %-os arányban történik meg. Az egyedüli védelmi megoldás, amit kutatásom alatt találtam és képes érzékelni a már megtörtént SE támadásokat az a mesterséges intelligencia alapú felhasználói viselkedés elemzés (AI assisted User Behavior Analytics).[26] Ezen megoldások viszont jelenleg csak kezdeti fázisban vannak. Idő kell ameddig „megtanulják" a felhasználói szokásokat és védelmet nem nyújt a támadások ellen, csupán detektálja azokat.

Amennyiben az emberi tényező által okozott kockázatot matematikailag szeretnénk modellezni és mérni, már erre is megvan a lehetőségünk. Váczi Dániel egy cikke az Óbudai Egyetem Biztonságtudományi Doktori Iskolájának Kiberbiztonsági tanulmány kötetében (ISBN: 978-963-449-131-6) jelent meg „A kiberbiztonsági kockázatelemzés lehetséges új iránya. Az emberi tényező kockázatainak valós modellezésének lehetősége Fuzzy logikával a vasútnál, mint kritikus infrastruktúrában" címmel, amelyben felvázolta miért érdemes

[16] Olyan sérülékenység, ami nem igényel semmilyen humán interakciót ahhoz, hogy le tudjon futni a céleszközön
[17] A támadó egy legitimnek tűnő e-mailt küld a célpontnak, amely egy olyan felületre irányítja őt, ami megszólalásig hasonlít az eredeti bejelentkezési oldalra (Ennek az az oka, hogy a nyilvánosan elérhető, a böngészőnkbe letöltött úgy nevezett „Front End" részt másolja le a támadó. Ezáltal az oldal 100%-ban ugyan úgy fog kinézni). Magyar fordítása: „Adathalászat". Az adathalászat kifejezést fogom a későbbiekben használni. [20]
[18] SMS phising
[19] Distributed Denial Of Service attack – Elosztott Szolgáltatásmegtagadással járó támadás
[20] Konzultációk eredményei alapján

mérni a humán faktort, mint biztonsági tényezőt. Miért nem alkalmas ennek felmérésére a BOOLE algebra és miért lehet jobb megoldás a fuzzy logika? Ezen cikke szerint a következő szempontok az alapvetőek amennyiben meg akarjuk állapítani, hogy a dolgozóink jelenthetnek-e veszélyt cégünk kiberbiztonságára:

1. Életkor
2. Generációs jellemzők
3. Alaptermészet
4. Szociális helyzet
5. Családi helyzet
6. Anyagi helyzet[21]
7. Saját, egyéni érdek
8. Vallási háttér és etnikai háttér
9. Függőségek (itt nem csak az illegális kábítószerre kell gondolni, ugyanúgy veszélyes lehet a szerencsejáték függőség vagy egyéb káros hóbort)
10. Zsarolhatóság
11. Céges pozíció
12. A társadalomban betöltött hely
13. A szociális hálóban betöltött hely
14. Technológiai kompetenciák
15. Biztonságtudatosság
16. A dolgozót körülvevő informatikai eszközök és ezek használata
17. Online jelenlét és annak minősége (minél több szabadon elérhető információ érhető el valakiről annál könnyebb lesz zsarolási alapot találni)
18. A privát-magánszféra közötti helyzete



A Hajlam és a Digitális Kompetencia hatása a kimenetre

2. ábra [30]

[21] 2-es diagram egyszerű szemléltető példaként szolgál, hogy miért lehet a fuzzy-val ábrázolt érték pontosabban ábrázolható.

Állami intézmények esetében gyakran nincs szükség a fent említett módszertanra, mivel bizonyos pozíciók betöltéséhez nemzetbiztonsági ellenőrzés szükséges. A piaci cégek viszont nagyban profitálhatnának abból hogyha valamilyen módon ellenőrizhetnék a humán faktort, hasonlóan az állami szférához. A konzultációk és az interjúk tapasztalata alapján megérné a területtel foglalkozni, ezért a kutatásom jövője ebbe az irányba fog menni. Egy olyan automatizált keretrendszert szeretnék készíteni, mellyel mérhető lenne a humán faktor kockázata, mindazonáltal kitöltése nem eredményezhetne munkahelyi diszkriminációt a felhasznált kényes adatok jellege miatt.
Amennyiben már úgy gondoljuk, hogy megfelelő a biztonságtudatosság szervezetünkben érdemes lehet ezt is matematikailag mérni. Ennek alapjait Tarján Gábor fektette le „AZ INFORMÁCIÓBIZTONSÁGI TUDATOSSÁG ÉRETTSÉGI SZINTJÉNEK MÉRÉSE SZERVEZETEKBEN" című PhD dolgozatában melyben olyan minden szervezet számára hasznosítható következtetésre jutott, amit ma minden információbiztonsággal foglalkozó szakembernek érdemes fontolóra vennie. Többek között érdemes lehet ezeket a méréseket Magyarországon is a Spitzner, L. (2012): „Security Awareness Maturity Model" (SANS Institute) modellje alapján végezni, mivel ez jól adaptálható a magyar környezetbe is. Ezen felül remekül használható az ITIL érettségi modellje mely 6 szintet különböztet meg:
0. Szint – Káosz/Teljes hiány szintje
1. Szint – Kezdeti/reaktív folyamatok
2. Szint – Megismételhető és vagy aktív folyamatok
3. Szint – Meghatározott és proaktív tevékenységek
4. Szint – A folyamatok szilárdak és általában jól teljesítenek
5. Szint – Minden tevékenység jól kontrollált, menedzselt, irányított és optimalizált

A fent említett PhD dolgozat statisztikai adataiból, 2 cég Információbiztonsági menedzsment belső eljárásainak dokumentációjából, konklúziókból, továbbá a szakirodalomban mások által gyűjtött információból megállapítottam, hogy hatékonyabbá tehetőek a biztonsági irányú céges fejlődések amennyiben a modelleket és szabványokat követve folyamatosan monitorozva van cégünk biztonsági felkészültsége! Továbbá növelhető a képzések hatékonysága, hogyha először az érdeklődést teremtjük meg gyakorlati példákkal! [27]

Az oktatásnál viszont az is fontos szempont, hogy ne csak a munkahelyen legyünk tudatosak, hanem a közösségi médián is! [28] Ugyanis OSINT segítségével nagyon sok kritikus információ gyűjthető valakiről csak a nyílt források felhasználásával, amiket a támadó minden esetben ki fog használni. De ugyanolyan fontos, hogy a marketinges szakember megértsék, hogy a kiberbiztonságot is biztonságosan kell reklámozni. Erre az egyik példa a sok közül a Gloster Infokommunikációs Nyrt. esettanulmánya az Óbudai Egyetemről [29] amelyben pontosan megnevezik, hogy 2 darab Cisco Firepower 2130-as tűzfalat üzemeltek be az egyetemen. Ez első sorban azért lehet problémás mert olyan oldalakon mint például az exploit-db.com könnyen lehet eszköz típus alapján sérülékenységeket találni. [22,23]

[22] 3-as számú melléklet
[23] 4-es számú melléklet

Közintézményként az Óbudai Egyetem arra kötelezett, hogy a Digitális Kormányzati Ügynökség portálján keresztül bonyolítsa le a kiemelt beszerzéseit. Az IT eszközök megvásárlása is annak bizonyul. Az egyetemen hagyománya van a Cisco eszközök használatának, így az intézmény eleve Cisco megoldásban gondolkodott.

Az intézmény a legjobb ár-érték arányt képviselő megoldást kereste, ahol a termék árazása mellett fontos volt az is, hogy a kiválasztott vállalat milyen minőségű technikai támogatást nyújt. A Digitális Kormányzati Ügynökség portálon a Gloster ajánlata volt a legjobb ár-érték arányú.

Az egyetemnek a Cisco Magyarország képviselőivel is van közvetlen kapcsolatuk. A gyártó képviselői is kiemelten ajánlották a Gloster, megerősítették, hogy mint szállító, alkalmas feladatai ellátására. Erről tanúskodnak a **Gloster Cisco tanúsítványai is**: a cég a **Cisco Premier Partnere**, 2020 decemberében megkapta negyedik Advanced minősítését, data center területen, de security, collaboration és enterprise területeken is Advanced Partner.

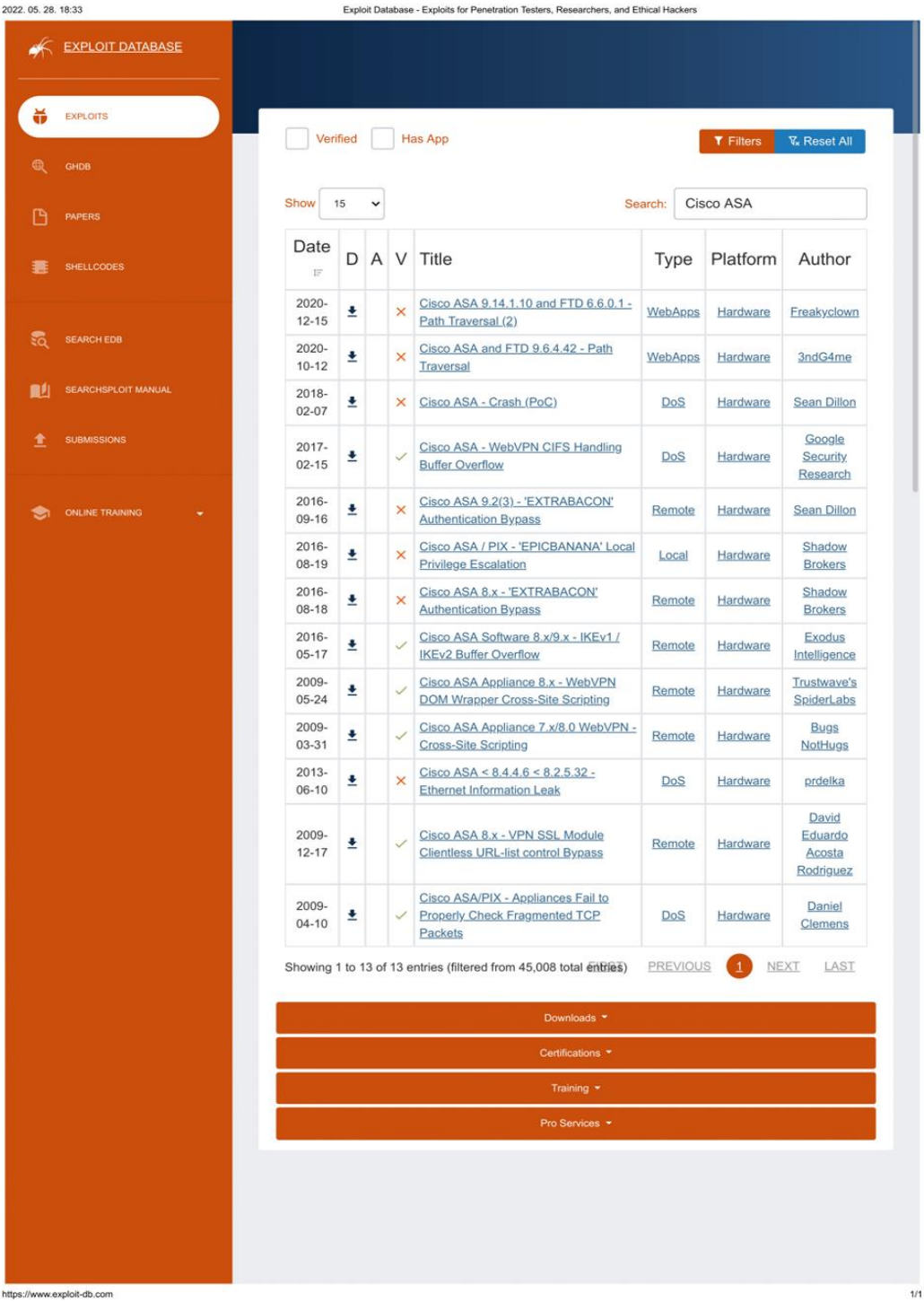
Korábbi közös IT projektek kapcsán az Óbudai Egyetem és a Gloster között már megvolt a kapcsolat, így már egy kipróbált vállalatra bízták a feladat megoldását.

A választás 2 darab redundáns, központi **Cisco Firepower 2130-as tűzfalra** esett.

A Gloster és az Óbudai Egyetem szakemberei első körben közösen beszélték meg, hogy pontosan milyen megoldás lenne ideális az intézmény számára. A tervezés, műszaki egyeztetés és beszerzés tekintetében egyaránt részt vettek a megbeszélésen és segítettek az egyetemnek a megfelelő eszközt kiválasztani. A műszaki paraméterezés során figyeltek a maximális terhelésre és a jövőbeli tervezett fejlesztésekre egyaránt.

A megoldás előnyei

3. számú melléklet



4. számú melléklet

Oroszi Eszter Diána előadásait hallgatva [30] és kutatásait olvasva elkezdett az foglalkoztatni, hogyan lehetne ezeket a biztonságtudatosító képzéseket hatékonyabbá tenni. Az auditorokkal folytatott konzultációim során megállapíthatóvá vált, hogy a képzések színvonala általában a management motivációját tükrözi a téma iránt. Amennyiben követelmény miatt (pl.: egy pályázat elnyeréséhez a cégnek rendelkeznie kell ISO 27001-es szabvánnyal) kell tartani ilyen képzéseket a színvonala a mindig rendkívül érdekes munka, baleset és tűzvédelmi előadásokhoz fogható. Vagyis a poroltó helyét vissza tudja mondani a dolgozó és valószínűleg ez után azt is, hogy hogyan néz ki egy erős jelszó, viszont amennyiben „éles helyzet állna elő" ezzel a tudással sajnos nem menne sokra. A management számára fontos szempont, hogy a dolgozók kevés időre vagy ne essenek ki a termelékeny munkafolyamatokból egy ilyen képzés miatt. Ezért ezeknek a képzéseknek az időpontját úgy kell megválasztani, hogy vagy az összes ilyen képzést egy napra kell időzíteni, ami eddigi tapasztalatok alapján kevésbé hatékony! Vagy céges ünnepségekhez, rendezvényekhez. Egy céges születésnap első programja vagy a karácsonyi vacsorát megelőző „biztonságtudatossági verseny" a dolgozók között motivációt adhat azoknak, akik fogékonyak lennének a téma iránt és jó élményekkel is összeköthetik az amúgy unalmas képzéseket!

KONKLÚZIÓ

- A humán faktor sérülékenysége matematikailag mérhető. Fuzzy logika alapú rendszerrel a pár fős cégektől a multinacionális vállalatokig korlátlanul skálázható.
- A dolgozók nem biztonságtudatos magatartása a rendszerünk legsérülékenyebb pontja.
- Biztonságtudatosító képzésekkel hatékonyan fel lehet készíteni a dolgozókat a Social Engineering támadásokra.
- Jelenleg (2022.05) nincs olyan informatikai védelmi megoldás, ami megakadályozná a Social Engineering támadásokat!
- Mesterséges intelligencia alapú valós idejű felhasználói viselkedés elemzéssel érzékelhető, ha a dolgozó digitális adatot juttat ki a cégből.
- Zero Trust módszer bevezetésével nagyban csökkenthetőek a károk egy támadás esetén
- Állami intézményeknek megalapításuktól, piaci cégeknek az első kockázat elemzésüktől érdemes információ biztonsággal foglalkozni.
- A vállalatok védekezését megkönnyítheti az ISO 27000-es szabványcsalád implementálása.
- A támadások döntő többsége már tartalmaz Social Engineeringet a hatékonysága miatt.
- Az állami szektor 2013 óta foglalkozik biztonságtudatosító képzésekkel!
- Érdemesebb a drága konvencionális védelmi megoldások előtt bevezetni azokat az adminisztratív és logikai biztonsági kontrollokat, amik nem kerülnek dologi kiadásba a cég számára.

JAVASLATOK

- Az IBTV hatálya alá tartozó intézményeknek megalakulásuktól törekedniük kell a számukra szükséges és elégséges információbiztonság megvalósítására

- A piaci szereplőknek az első kockázatelemzésüktől érdemes az információbiztonsággal foglalkozni, az abban megállapított kockázatokat kezelni, de alternatíva lehet a kockázat a biztosító felé történő áthárítása is.
- Nem célszerű nagyobb összeget költeni a védelemi megoldásokra, mint amekkora összeget vesztenénk a kockázat bekövetkeztével.
- Nem minden esetben célszerű a kockázatokat teljesen eliminálni költségességüknél fogva, mindazonáltal a menedzsmentnek törekednie kell arra, hogy számukra vállalható szinten mozogjanak!
- Amennyiben érzékeny adatokkal dolgozunk vagy olyan adatokkal (például szellemi termékkel) amiket ellopva anyagi ellentételezésben részesülne az adatok eltulajdonítója érdemes nem csak az üzletmenet folytonosságot védeni, hanem a cég belső információit, értékeit!
- Amennyiben a fent említett adatokat meg kell védenünk, érdemes nem csak a konvencionális védelmi megoldásokat beszereznünk, mivel ezek drágák és csak az informatikai kockázatok ellen nyújtanak bizonyos fokú védelmet. Emellett célszerű lenne biztonságtudatosító képzéseket tartani és a fizikai, logikai és adminisztratív védelmi kontrollokat erősíteni. Ezek preventív védelmi intézkedések, ezzel megelőzhetővé vállnak a támadások, míg a konvencionális védelmi megoldások (pl.: reaktív vírusírtók) detektív és korrektív védelmi kontrollokat nyújtanak. Próbáljuk meg megelőzni a támadásokat!
- Érdemes lehet vállalatirányítási szabványokat bevezetni (ISO 9001 és 27001).

FELHASZNÁLT IRODALOM

[1] Krasznay Csaba és Bányász Péter: Kiberbiztonsági incidensek a magyar közigazgatásba (https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/13172/A_Jo_Allam_merhetos-ege_III_2019.pdf?sequence=1#page=250 Hozzáférés ideje: 2022.05.21 21:05:13) p. 264

[2] Christopher Hadnagy „The Art of Human Hacking” ISBN: 978-1-118-02801-8 Wiley Publishing, Inc. (2011) p.23 szerző által fordított

[3] Katonai Nemzetbiztonsági Szolgálat Felderítő Szemle XIV. évfolyam 4. szám 2015. november HU ISSN 1588-242X Az Informatikai Üzemeltetés Általános Kérdései Holtai András, Magyar Sándor, Puskás Béla p. 91

[4] Haig Zsolt Információs Műveletek A Kibertérben Dialóg Campus Kiadó, 2018 p.220 4.1.1

[5] Információbiztonság vs. kiberbiztonság – az okos város szempontjából Krasznay Csaba NKE Kiberbiztonsági Akadémia https://www.hte.hu/documents/10180/4588545/2.4-Krasznay_Csaba.pdf hozzáférés ideje: 2022.05.21 21:05:13)

[6] Katonai Nemzetbiztonsági Szolgálat Szakmai Szemle XVIII. évfolyam 1. szám 2020. március HU ISSN 1785-1181 Tóth Tamás Az Egyes Social Engeneering Módszerek Elhatárolása És Rendszerezése

[7] Dezső András Fedősztori 2021 ISBN: 978 963 568 115 0 – p. 423

[8] Bányász Péter – Bóta Bettina – Csaba Zágon: A social engineering jelentette veszélyek napjainkban (https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/14723/01_Banyasz_Bota_Csaba_A_social_engineering.pdf?sequence=22 utolsó elérés ideje: 2022.05.21 21:05:13) p. 16
[9] . Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola Bányász Péter Doktori (PhD) Értekezés A közösségi média lehetőségei és kihívásai a védelmi szférában Budapest, 2018p. 84
[10] Katonai Nemzetbiztonsági Szolgálat XV. évfolyam 3. szám 2017. november Szakmai Szemle HU ISSN 1785-1181 60-76 Deák Veronika Biztonságtudatosság Az Információs Környezetben p. 64
[11] Dunakavics 2015. III. évfolyam VIII. szám Oroszi Eszter Diána: Kártékony programok terjedése social engineer szemmel p. 14
[12] ISO Consulting Kuwait https://isoconsultantkuwait.com/2019/12/08/iso-270012013-a-7-human-resource-security/ hozzáférés: 2022.05.21 21:05:13)
[13] Ludovika Szabadegyetem 2022. április 19. 18.00 Krasznay Csaba: A kiberbűnözés fajtái, kiberbűncselekmények és a dark web
[14] Nemzetbiztonsági Szemle HU ISSN 2064-3756 VI. évfolyam, 1. szám, 2018. Social engineering and social media 1 Bányász Péter p. 60
[15] Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet: Az információbiztonság lélektana (Psychology of Information Security) KÖFOP-2.2.2-VEKOP-16-2016-00001 pp. 6-7
[16] Zrínyi Miklós Nemzetvédelmi Egyetem Hadtudományi Kar
Katonai Műszaki Doktori Iskola Krasznay Csaba PhD Értekezés A Magyar Elektronikus Közigazgatási Alkalmazások Információbiztonsági Megoldásai Budapest, 2011 p. 119
[17] Katonai Nemzetbiztonsági Szolgálat Felderítő Szemle XIV. évfolyam 2. szám 2015. június HU ISSN 1588-242X Vida Csaba p. 197
[18] Zrínyi Miklós Nemzetvédelmi Egyetem Hadtudományi Doktori Iskola Pix Gábor Alezredes A Lélektani Műveletek Jellemzőinek Vizsgálata Doktori (Phd-) Értekezés Budapest, 2005 3.1.1 A terrorizmus kezelésének lehetősége – A lélektani műveletek szemszögéből pp. 77 – 80
[19] Cisco Networking Academy CCNA: Enterprise Networking, Security, and Automation (v7.02) 3. szemeszter online tananyag - 3-as fejezet Network Security Concepts - 3.5.6 alfejezet Social Engineering Attacks – szerző fordítása | elérhető: https://www.netacad.com/courses/networking/ccna-enterprise-networking-security-automation
[20] Haig Zsolt - Várhegyi István A cybertér és a cyberhadviselés értelmezése p. 6
[21] Ludovika Szabadegyetem Kovács László dandártábornok: Kiberbiztonság és kiberhadviselés 2022-. 03. 8 18:00
[22] Nemzet És Biztonság 2010. február Kovács László dandártábornok – Krasznay Csaba: Digitális Mohács Egy kibertámadási forgatókönyv Magyarország ellen p. 2
[23] Nemzet És Biztonság 2010. február Kovács László dandártábornok – Krasznay Csaba: Digitális Mohács Egy kibertámadási forgatókönyv Magyarország ellen p. 6

[24] Óbudai Egyetem Biztonságtudományi Doktori Iskola Váczi Dániel PhD értekezés Kiberbiztonsági humán kockázati matematikai modell szenzitív digitális információszivárgás potenciáljának mérésére Budapest, 2021. 09. hónap 27. nap p. 31
[25] https://www.splunk.com/en_us/data-insider/user-behavior-analytics-ueba.html utolsó hozzáférés: 2022. május 22. 00:08:01
[26] Dub Máté: A social engineering támadások megelőzésének lehetőségei (https://folyoirat.ludovika.hu/index.php/hadmernok/article/view/5476/4721 : 2022.05.21 21:05:13)
[27] Deák Veronika A Social Engineering humán alapú támadási technikái p. 8
[28] https://www.gloster.hu/eroforrasok/esettanulmany/obudai-egyetem-esettanulmany-cisco-tuzfal-vedi-az-online-egyetemi-oktatast hozzáférés: 2022. május 27. 20:48:27
[29] CodingClub - Oroszi Eszter: Social Engineering (https://www.youtube.com/watch?v=ikcuLV4HUvY&t=489s 2022.05.21 21:05:13)
[30] Bánki Közlemények 4.Évfolyam 1.Szám
Az emberi tényező fuzzy alapú kiberbiztonsági kockázatelemzése a minősített információszivárgás szempontjából Váczi Dániel, Tóth-Laufer Edit, Szádeczky Tamás 10. ábra: A pénzügyi helyzetet leíró tagsági függvény
[31] Konzultációk:
- Hack Zoltán (ISO 27001 auditor és oktató) – állandó konzulensem
- Krasznay Csaba (Nemzeti Közszolgálati Egyetem Eötvös József Kutatóközpont-Kiberbiztonsági Kutatóközpont vezető) 2022.03.23
- Kollár Csaba (Óbudai Egyetem Mesterséges Intelligencia Műhely vezető) 2022.04.05

AN OVERVIEW ON THE DIFFERENT APPROACHES TO REGULATE IOT PERMANENT ROAMING

AZ IOT TARTÓS BARANGOLÁS SZABÁLYOZÁSÁNAK ELTÉRŐ MEGKÖZELÍTÉSEINEK ÁTTEKINTÉSE

MIKLÓS Gellért [1]

Abstract

The aim of this paper is to present the different approaches to regulate the permanent roaming of IoT devices and the data security and economic aspects of such regulations. The topicality of the subject is provided by the increasing proliferation of IoT devices, the progress made in the field of connectivity, the deployment of next-generation mobile networks (5G) and the emergence of new applications based on them. IoT devices are able to connect to networks and communicate with other IoT devices using a variety of technologies. One way to do this is to connect to a mobile network. In the event that an IoT device is connected to a public mobile network in another state other than its public home network for a specified period of time, it is considered to be permanent roaming. The regulation of this phenomenon is evolving dynamically in the world along different concepts. Some states allow, while others prohibit or restrict permanent roaming, while there are states where the issue is currently completely unregulated. With the proliferation of IoT devices and the emergence of differing regulatory regimes, it is expected that more and more countries will regulate permanent roaming.

Keywords

IoT, permanent roaming, EU, data security, telecommunications

Absztrakt

Jelen írás célja bemutatni a cellás IoT eszközök tartós barangolására vonatkozó eltérő szabályozásokat és azok adatbiztonsági, gazdasági vonatkozásait. A téma aktualitását az IoT eszközök egyre növekvő ütemű elterjedése, a csatlakoztathatóság terén elért fejlődés és az újgenerációs mobilhálózatok (5G) telepítése, valamint az erre épülő új alkalmazási területek megjelenése szolgáltatja. Az IoT eszközök különböző technológiák alkalmazásával képesek kapcsolódni hálózatokhoz és kommunikálni más IoT eszközökkel. Ennek egyik módja a mobilhálózathoz való csatlakozás. Abban az esetben, amennyiben egy IoT eszköz a nyilvános hazai hálózatától eltérő, más államban található nyilvános mobilhírközlő hálózathoz meghatározott időtartamnál tovább csatlakozik, tartós barangolásról beszélünk. Ennek a jelenségnek a szabályozása eltérő koncepciók mentén dinamikusan fejlődik a világban. Bizonyos államok engedélyezik, más államok tiltják, vagy korlátozzák a tartós barangolást, azonban léteznek olyan államok is, ahol a kérdés jelenleg teljesen szabályozatlan. Az IoT eszközök terjedésével és az eltérő szabályozási rendszerek kialakulásával várható, hogy egyre több országban kerül majd szabályozásra a tartós barangolás.

Kulcsszavak

IoT, tartós barangolás, EU, adatbiztonság, telekommunikáció

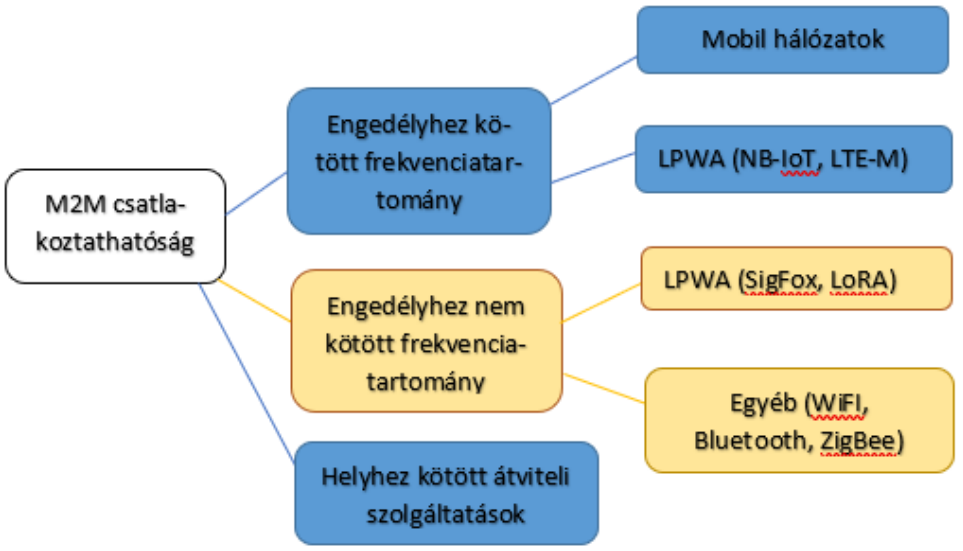
[1] gellert.miklos@gmail.com | ORCID: 0000-0002-3757-6834 | PhD Student, Óbuda University Doctoral School for Safety and Security Sciences | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

BEVEZETÉS

Az IoT eszközök egyre gyorsuló elterjedése a gazdaság szinte minden ágazatában érezteti hatását. Az okos eszközök iránti növekvő igény ösztönzőleg hatott kapcsolódás, a hardware és software fejlesztés terén is. A szabályozás azonban nem tartotta a lépést ezzel a gyors ütemű fejlődéssel, amely jelentős kihívás elé állítja a szabályozó hatóságokat. A szabályozó hatóságok látókörében még mindig az ember és ember közötti kommunikáció a domináns, így a szabályozás logikája is arra épül fel. A frekvenciasávok felosztása, kiosztása és hasznosítása, az eszközök és technológiák szabványosítása, az gépek közötti kommunikáció számára elkülönített számtartományok szabályozása vagy az IoT eszközök biztonsága csak néhány olyan kérdés melyekkel a szabályozó hatóságok az elmúlt évtized során szembesülni kényszerültek. Jelen írás célja bemutatni a cellás IoT eszközök tartós barangolásával kapcsolatos eltérő szabályozási megközelítéseket.

Az IoT eszközök csatlakoztathatósága

Az IoT eszközök – definíciójukból adódóan – más eszközökkel kommunikálnak, a kommunikációhoz szükséges jeleket pedig szabványosított technológia alkalmazásával, valamely hálózathoz történő csatlakozás útján továbbítják. Az eszközök között létrejövő kapcsolódás megvalósulhat engedélyhez kötött frekvencia használatára alapuló technológia által, vagy engedély nélkül használható frekvencia alkalmazásával is. Az előbbire példa az elektronikus hírközlési szolgáltatások nyújtása során alkalmazott mobil hálózatok (2G, 3G, 4G, 5G), vagy az engedélyköteles frekvenciatartományban működő LPWAN (Low Power Wide Area Network) megoldások, mint a Narrowband-IoT vagy az LTE-M technológia. Az utóbbira példa az engedélyhez nem kötött frekvenciatartomány alkalmazására alapul LPWAN megoldások, mint a SigFox, vagy a Low Power Radio (LoRa) technológiák, valamint az egyéb, magánhálózati technológiák, mint a WiFi, Bluetooth és a ZigBee. [1]



1. Ábra: M2M csatlakoztathatóság fajtái, forrás: BEREC, Internet of Things indicators, 18. oldal

A különböző technológiáknak megvannak a maguk specifikációi, melyek meghatározzák annak alkalmazási területét is. Az LPWA technológiák, mint nevükből is adódik, olyan alkalmazási területeken használhatók fel leginkább, ahol fontos szempont az alacsony energiafogyasztás, valamint a nagy átviteli távolság alacsony átviteli sebesség mellett. Erre tipikus példa lehet a precíziós mezőgazdaságban (pl. talajnedvesség mérésére) vagy az okos városok kialakítása során (pl. parkolóhely állapotának jelzésére) alkalmazott szenzorok. Ezek a szenzorok ugyanis jellemzően kisméretű adatcsomagokat továbbítanak, azonban fontos a minél hosszabb élettartam és a

Vannak azonban olyan alkalmazási területek, amelyek esetén az LPWA megoldások nem megfelelőek, mert például nem tudják biztosítani a szükséges adatátviteli sebességet, az alacsony késleltetést vagy az elvárt megbízhatóságot. Ezekben az esetekben megoldást jelenthet a cellás IoT (angolul cellular IoT). További előnye a cellás IoT megoldásoknak, hogy a világ szinte összes országában ki van már építve a mobilhírközlő hálózat, így az IoT szolgáltatók részéről nem szükséges külön infrastrukturális beruházás az okos eszközök működtetéséhez. A legújabb, ötödik generációs mobilhálózatok minden korábbinál nagyobb adatátviteli sebességet tesznek elérhetővé az IoT eszközök és alkalmazások számára, megvalósíthatóvá téve az olyan nagymennyiségű adat gyors átvitelére épülő alkalmazásokat, mint például az önvezető autózás vagy a robotsebészet.

Tartós barangolás

Az elektronikus hírközlő hálózatok működésében és az elektronikus hírközlési szolgáltatások nyújtásában az azonosítók biztosítják a hálózatok, szolgáltatási rendszerek és különösen az előfizetők megkülönböztetését. A legismertebb ilyen azonosító a telefonszám, amellyel a világméretű telefonhálózat minden végpontja egyértelműen azonosítható és a hálózat bármely végpontjáról felhívható, elérhető.[2] A Nemzetközi Távközlési Egyesület (angolul International Telecommunication Union) által kibocsájtott nemzetközi számozási terv (ITU-T E.164 Ajánlás) szabja meg a telefonszámok felépítését és az egyes országok országkódját. Ez Magyarország esetében a +36-os kód. A nemzeti számozási terv kialakítása állami hatáskör, melyet Magyarországon jelenleg a 14/2020. (XII. 15.) NMHH rendelet szabályoz. Az elektronikus hírközlési azonosítók, ideértve a telefonszámokat is, hasonlóan a frekvenciatartományokhoz az állam tulajdonát képező korlátos erőforrásnak minősülnek. Ezekkel a korlátos erőforrásokkal való gazdálkodás jellemzően az államok nemzeti szabályozó hatóságának feladatkörébe tartoznak. Magyarországon erre a gazdálkodási és felügyeleti tevékenységre kijelölt hatóság a Nemzeti Média- és Hírközlési Hatóság (a továbbiakban: NMHH).

A hatályos magyar nemzeti számozási terv külön számtartományt tartalmaz a gépek közötti szolgáltatások (M2M számok) nyújtására, ehhez a 71-es kódot rendeli.[2] A 71-es kód alatt nyújtott gépek közötti szolgáltatás olyan kommunikációt tesz lehetővé a végberendezések vagy alkalmazások között az elektronikus hírközlő hálózaton, ahol az információt legfeljebb csekély emberi beavatkozással továbbítják. [8] Tekintettel arra, hogy a számtartomány elsősorban a gépek közötti kommunikációt szolgálja, ezért hangkommunikáció, il-

[2] 1. Melléklet 2.7.

letve üzenetküldés csak korlátozott jelleggel, az IoT eszközök és alkalmazások között létesíthető. A nemzeti számozási terv külön számtartományt rendel az Európai Unión belüli extraterritoriális használatra.

A hatóság az azonosítók használatára az elektronikus hírközlési szolgáltatókról vezetett nyilvántartásába bejegyzett hírközlési szolgáltatót jelölhet ki. A szolgáltató a kijelölés érdekében kérelmet nyújt be a hatósághoz, a hatóság pedig a számmező kijelölési határozatában a kérelemben meghatározott alkalmazás jellegétől függő számhasználati feltételeket állapíthat meg. Az NMHH egy adott M2M alkalmazás részére a számokat különböző nagyságú számmezőkben jelöli ki és adja át a szolgáltatók részére.

A gyakorlatban ez azt jelenti, hogy amennyiben egy vállalkozás cellás IoT eszközöket kíván forgalomba hozni Magyarország területén és ehhez a nemzeti számozási tervben meghatározott M2M számot kíván felhasználni, úgy a hírközlési szolgáltató a vállalkozást megállapodásuk alapján létrejövő számhasználati jogviszony keretében feljogosítja az M2M számok használatára. Az IoT eszközök azonosítása a beépített SIM-kártya (előfizetői azonosító modul) útján történik. Amennyiben az IoT eszközök az Európai Unión belüli extraterritoriális használatra is engedélyezett tartomány számaival kerültek azonosításra, úgy - amennyiben a tartós barangolás egyéb feltételei fennállnak – azok az IoT eszközök az Európai Unió bármely tagállamában korlátozás nélkül használhatók.

A szolgáltatók az azonosítók használatáért és lekötéséért, valamint az azonosítóengedélyezési eljárásokért díjat fizetnek az NMHH részére. Éppen ez az, ami az adatbiztonság és adatvédelem mellett az egyik leggyakrabban elhangzó érv a tartós barangolás korlátozása vagy tiltása érdekében. Tartós barangolás esetén ugyanis az történik, hogy a vállalkozás fizet egy adott ország szolgáltatója számára a számhasználati jogosultságért és az IoT eszközök kommunikációjához szükséges szolgáltatástért (pl. internet hozzáférés), a szolgáltató pedig az azonosítók használatáért díjat fizet a nemzeti szabályozó hatóság részére. Az IoT eszközök azonban végül tartósan más államban kerülnek telepítésre, használatra. A vállalkozás a célállamban is megszerezhette volna az IoT szolgáltatás nyújtásához szükséges azonosítókat, ez azonban valamely oknál fogva nem történt meg. Ilyen ok lehet a például a globális ügyintézés, hiszen egy globális szolgáltatótól beszerezni egy számos országban használható megoldást egyszerűbb és kisebb költséggel jár, mint minden országban helyi megoldást keresni. Ezért a célállam és az ott működő hírközlési szolgáltatók végeredményben bevételektől esnek el a tartós barangolás miatt.

A TARTÓS BARANGOLÁS SZABÁLYOZÁSA AZ EURÓPAI UNIÓBAN

Az Európai Unió az elmúlt évtizedekben jelentős erőfeszítéseket tett a távközlési szektor harmonizációjára és az egységes belső piac megteremtésére. Ennek részeként került sor a nyilvános mobilhírközlő hálózatok közötti barangolás szabályozására is. A következő tíz éves, 2031-ig terjedő időszakra az átdolgozott roaming végrehajtási rendelet (a továbbiakban: Roaming Rendelet) szabályai irányadók az Európai Unión belül. [9] A Roaming Rendelet alapján a tartós barangolás nincs tiltva, az kereskedelmi tárgyalások tárgyát képezi, és arról két szolgáltató szabadon köthet megállapodást a közöttük létrejövő nagykereskedelmi barangolási megállapodásban.

Ez azonban egyelőre csak lehetőség, de nem kötelezettség a hírközlési szolgáltatók számára. Az Európai Unión belül várhatóan egyre több szolgáltató fogja lehetővé tenni az IoT eszközök közötti kommunikáció esetén a hálózatán történő barangolást, hatékonyabbá

és versenyképesebbé téve ezáltal az IoT eszközök piacát.[3] A mobilhálózat-üzemeltető szolgáltatók a Roaming Rendelet alapján kötelesek referenciaajánlatot közzétenni, ami tartalmazza a nagykereskedelmi barangolási hozzáférésre vonatkozó általános feltételeket.[4] A szolgáltatók ebben a referencia ajánlatban feltételeket szabhatnak meg a tartós barangolás megakadályozása céljából.

A referenciaajánlat tartalmazhat rendelkezéseket arra az esetre, amennyiben feltételezhető, hogy más szolgáltató előfizetőnek jelentős része tartósan barangol a látogatott hálózaton. Ebben az esetben a látogatott hálózat üzemeltetője – a vonatkozó uniós és nemzeti adatvédelmi szabályok betartása mellett – információkéréssel fordulhat a másik szolgáltatóhoz annak objektív mutatók alapján történő megállapítása érdekében, hogy valóban tartós barangolásról van-e szó az adott előfizetők vonatkozásában.

Amennyiben az információkérés, a felszólítás és egyéb intézkedések sem vezettek eredményre, végső eszközként a referenciaajánlat lehetőséget biztosíthat a nagykereskedelmi barangolási megállapodás megszüntetésére, amennyiben objektív kritériumok alapján megállapításra került, hogy a másik szolgáltató előfizetőinek jelentős hányada tartós barangolást végez és erről tájékoztatásra került. A nagykereskedelmi barangolási megállapodás egyoldalú megszüntetésére tartós barangolásra hivatkozással, kizárólag a látogatott hálózatot üzemeltető szolgáltató nemzeti szabályozó hatóságának előzetes engedélye alapján kerülhet sor. A nemzeti szabályozó hatóság a kérelem kézhezvételét követő három hónapon belül dönt, a másik szolgáltató szabályozó hatóságával folytatott konzultációt követően. A hatóság a döntésről tájékoztatja továbbá az Európai Bizottságot is. Az eljárás során mindkét nemzeti szabályozó hatóság dönthet úgy, hogy felkéri az Európai Elektronikus Hírközlési Szabályozók Testületét (rövidítve BEREC), hogy egy hónapon belül hozzon állásfoglalást az alkalmazott intézkedések vonatkozásában.

A fenti, több lépcsős eljárás szabályaiból megállapítható, hogy az jogalkotó szándéka valóban az volt, hogy a nagykereskedelmi barangolási megállapodás felmondására a tartós barangolás következményeképp valóban csak végső megoldásként, a valóban visszaélésszerű helyzetek során kerülhessen sor. Az Unió számára a prioritás a belső piac fenntartása és a verseny, valamint az innováció elősegítése.

Az Európai Unióból történő adatok továbbítására, értve ez alatt az IoT eszközök által kezelt adatok továbbítását is, az Európai Unió általános adatvédelmi rendeletének rendelkezései irányadók. Amennyiben az IoT eszközök az adatokat harmadik országba, például Kínába vagy az Egyesül Államokba kívánják továbbítani, úgy az adattovábbításnak meg kell felelnie a személyes adatok harmadik országba történő továbbítására vonatkozó többletkövetelményeknek is, az Európai Unióban azonban nincs érvényben olyan adatlokalizációs követelmény amely megkövetelné az IoT szolgáltatóktól, hogy infrastruktúrájukat vagy az adatokat az Unió területén belül tárolják.

[3] Roaming Rendelet (21) Preambulumbekezdés

[4] Roaming Rendelet (16) Preambulumbekezdés és 3. cikk (5)

SZAÚD-ARÁBIA

Szaúd-Arábia mind gazdasági erejét, mind lakosságszámát tekintve az Arab-félsziget egyik meghatározó állama. Az ott végbemenő gazdasági folyamatok, a kialakított szabályozási keretrendszer hatással van a szomszédos országokra is. Igaz ez az IoT eszközökre és szolgáltatásokra vonatkozó szabályozásra is.

A szaúdi telekommunikációs szabályozó hatóság, a Communications and Information Technology Commission (rövidítve CITC) 2019-ben fogadta el az IoT Szabályozási Keretrendszert (angolul IoT Regulatory Framework, a továbbiakban: Keretrendszer) amelyben szabályozásra kerültek az IoT szolgáltatások nyújtásával összefüggő főbb kérdések, mint az engedélyköteles frekvenciatartományok, az azonosítóhasználat és a típusjóváhagyás. Ez a keretrendszer volt az első, amely kifejezetten az IoT szektort és az azzal kapcsolatos szolgáltatások nyújtását szabályozta, azzal a deklarált céllal, hogy Szaúd-Arábiát az IoT terén az Arab-félsziget és a világ egyik vezető országává tegye.

A Keretrendszer alapján IoT szolgáltatásokat Szaúd-Arábiában helyhez kötött vagy mobil hálózaton keresztül csak a CITC által megadott engedéllyel rendelkező telekommunikációs szolgáltató nyújthat. Engedély azonban csak az országban bejegyzett gazdasági társaság kérelmezhet, meghatározott feltételek teljesülése esetén. [3] Ez a gyakorlatban azt jelenti, hogy Szaúd-Arábiában csak a helyi hírközlési szolgáltatók nyújthatnak a mobilhírközlő hálózaton IoT szolgáltatást. Ehhez a szaúdi nemzeti számozási tervben kijelölt M2M azonosítókat kell használni. [3]

A fentieken túlmenően a Keretrendszer előírja az IoT szolgáltatók számára azt is, hogy az IoT szolgáltatások nyújtásához használt összes szervert és minden adatot az ország területén belül tároljanak, valamint biztosítsák a hatóság számára az adatok legalább 12 hónapig történő megtekintéséhez szükséges technikai képességeket.[5] Ez erős kontrollt biztosít az adatok felett mind a bűnüldöző szervek, mind a nemzetbiztonsági szolgálatok számára. Az adatlokalizációs követelményt a Keretrendszer megismétli a 8. pontban, amikor a szolgáltatók számára további követelményként előírja, hogy az IoT hálózat összes összetevőjét, eszközét és az adatok tárolására szolgáló szervereket Szaúd-Arábia területén kell üzemeltetni. A tartós barangolásra épülő globális megoldások tehát Szaúd-Arábiában nem engedélyezettek, a cellás IoT eszközök működéséhez helyi hírközlési szolgáltatók által nyújtott mobil hálózati hozzáférés szükséges.

A CITC 2022 márciusában nyilvános konzultációt kezdeményezett a szolgáltatók és iparági szereplők részvételével a Keretrendszer szabályainak felülvizsgálata érdekében. [4] A konzultáció továbbra is fenntartja az engedélyre, valamint a szaúdi M2M számok használatára vonatkozó kötelezettséget, nem tartalmazza azonban az adatlokalizációra vonatkozó korábbi előírást. Ez azonban nem feltétlenül jelenti azt, hogy amennyiben a konzultációban megfogalmazott szabályok elfogadásra kerülnek, úgy abban az esetben már nem szükséges a szerverek és adatközpontok országon belüli fenntartása. 2021 szeptemberében elfogadásra került a személyes adatok védelméről szóló törvény (angolul Personal Data Protection Law vagy röviden PDPL), amely rögzíti, hogy tilos személyes adatot tárolni, vagy kezelni Szaúd-Arábia területén kívül a felhasználó kifejezett engedélye vagy az adatvédelmi hatóság írásos engedélye nélkül, amely engedélyt a hatóság esetről esetre vizsgálva állít ki.

[5] IoT Szabályozási Keretrendszer 7. pont

A fenti szabályokból látható, hogy a szaúdi szabályozás szigorúan tiltja a tartós barangolást, elzárva a globális hírközlési szolgáltatókat a szaúdi piachoz való hozzáféréstől, versenyelőnybe hozva a helyi szolgáltatókat. Ezen túlmenően az adatlokalizációs és adatmegőrzési kötelezettségek útján erős kontrollt biztosít a hatóságok számára az IoT szolgáltatások nyújtása során keletkező adatok felett.

TÖRÖKORSZÁG

Törökország telekommunikációs szabályozó hatósága, az Információs és Kommunikációs Technológiai Hatóság (angolul Information and Communication Technologies Authority, rövidítve a továbbiakban: ICTA) az IoT szektorra két jelentős hatású határozatot tett közzé a közelmúltban, az egyiket 2018 elején, a másikat 2019 elején. Az első döntés a járművekben nyújtott e-Call szolgáltatások szabályaira vonatkozott, míg az utóbbi a távoli konfigurációra alkalmas e-SIM technológiákra vonatkozott. A második döntés előírta az IoT szolgáltatók számára, hogy szolgáltatásukat csak helyi SIM kártyák útján nyújthatják, vagy olyan távoli konfigurációra (angolul over-the-air, OTA) alkalmas SIM technológiát kell alkalmazni, amely lehetővé teszi a helyi szolgáltatók profiljára történő átállást. [5] A tartós barangolást az ICTA fenti eSIM döntése, valamint az elektronikus kommunikációról szóló 5809 számú törvény rendelkezései tiltják, amely a telekommunikációs szektor szabályozásának elsődleges forrása Törökországban. A hatóság jogértelmezése és indokolása alapján a tartós barangolás tiltása és ezzel párhuzamosan a helyi azonosítók használata elősegíti az innovációt és a versenyt az IoT szektorban, valamint megerősíti az adatbiztonság, a személyes adatok védelmének szintjét. [6] Szaúd-Arábiával ellentétben Törökország formális csatlakozási kérelmet nyújtott be az Európai Unióhoz, ezért elviekben szabályozását az Uniós szabályokhoz – beleértve a hírközlési szabályokat is - közelítenie kellene.

A szabályozás 90 napos türelmi időt biztosít a Törökországba érkező IoT eszközök számára. Amennyiben egy barangoló eszköz 90 napnál többet tölt el 120 napon belül egy török mobilhálózaton hanghívás vagy SMS kezdeményezés nélkül, abban az esetben a látogatott hálózat szolgáltatója köteles a tartósan barangoló eszközt a hálózatáról letiltani. A tiltást követően a felhasználók – tehát nem az IoT szolgáltatás nyújtója, hanem az eszköz tényleges tulajdonosai – kötelesek a letiltott eszközöket a hatóság által ebből a célból létrehozott platformján regisztrálni, valamint a regisztrációs díjat megfizetni.

A beágyazott SIM (rövidítve: eSIM) kártyákkal ellátott IoT eszközök esetében a szabályozás előírja, hogy az azok működtetésével összefüggő összes létesítmény, eljárás és rendszer Törökországban kell, hogy létesítésre kerüljön valamely Törökországban bejegyzett és engedéllyel rendelkező hírközlési szolgáltató irányítása alatt. [5]

A tartós barangolást a török szabályozás tiltja, a gyakorlatban tehát az IoT eszközök gyártóinak mindenképpen helyi szolgáltatókkal kell megoldani a cellás IoT eszközök működéséhez szükséges hálózati hozzáférést.

KÖVETKEZTETÉSEK

A tartós barangolás szabályozása kapcsán tehát eltérő megközelítések figyelhetők meg. Az országok egy része, mint például az Európai Unió vagy az Egyesült Államok szabályozása lehetővé teszi a tartós barangolást a szolgáltatók hálózatain a meghatározott feltételek fennállása esetén. Más országok, mint például Szaúd-Arábia, Törökország, Brazília

vagy Kína tiltják a tartós barangolást és szigorú adatlokalizációs szabályokat hoztak, amelyek az IoT szolgáltatókat arra kötelezik, hogy szolgáltatásukat helyi hírközlési szolgáltatók közreműködésével nyújtsák az adott országban. Ez nagyobb kontrollt és betekintést enged a helyi hatóságok számára az IoT szolgáltatásokkal kapcsolatos adatokba, egyúttal azonban a helyi megoldások többletköltséget jelentenek az IoT szolgáltatók számára. Számos esetben a SIM kártya már a gyártási folyamat során behelyezésre kerül az eszközökbe, így azok utólagos cseréje nem feltétlenül megoldható. Az ilyen esetekre is megoldást nyújt a távoli konfiguráció, amely egy olyan technológia, amely lehetővé teszi a SIM kártyán található adatok és profil módosítását anélkül, hogy azt cserélni kellene. Ennek jelentősége az IoT szektor számára jelentős, nem véletlen, hogy az Európai Unió is kötelezi a tagállamokat a távoli konfiguráció előmozdítására amennyiben az technikailag kivitelezhető.[6] [10][11]

Számos olyan állam van, amelynek jogrendszere ma még nem szabályozza a tartós barangolást, így az IoT eszközök probléma nélkül barangolhatnak a helyi hálózatokon időkorlát nélkül. A nemzetközi trendek vizsgálatát követően azonban egyre több állam dönt az IoT szektor szabályozása mellett, beleértve az állandó barangolás kérdését is. Amennyiben jelentős számú állam dönt az állandó barangolás tiltása mellett, az ellehetetlenítheti a globális megoldásokat és így végeredményképp visszavetheti az innovációt az IoT szektorban, továbbá lassíthatja a tartós barangolást tiltó államok digitális átállását és az IoT eszközök széleskörű elterjedését.

Az IoT eszközökre vonatkozó biztonsági előírások, szabványok és ajánlások terén már megfigyelhető hasonló tendencia, amely során egyre több állam teszi közzé saját biztonsági követelményeit, amelyek gyakran eltérnek más államok és nemzetközi szabványok előírásaitól, ezzel megnehezítve az IoT eszközök globális elterjedését és megnövelve a piacra lépés költségeit az IoT szolgáltatók számára.[7]

FELHASZNÁLT FORRÁSOK

[1] BEREC Internet of Things indicators BOR (19) 25 [Online] Elérhető: https://berec.europa.eu/eng/document_register/subject_matter/berec/reports/%208464-berec-report-on-internet-of-things-indicators

[2] Nemzeti Média- és Hírközlési Hatóság Azonosítógazdálkodás [Online] Elérhető: https://nmhh.hu/szakmai-erdekeltek/azonositogazdalkodas

[3] CITC Internet of Things (IoT) Regulatory Framework 2019 [Online] Elérhető: https://www.citc.gov.sa/en/RulesandSystems/RegulatoryDocuments/Documents/IoT_REGULATORY_FRAMEWORK.pdf

[4] CITC Public Consultation Document on Updating the IoT Regulations 2022 [Online] Elérhető: https://regulations.citc.gov.sa/en/Pages/PublishedPublicConsultations.aspx#/PublishedPublicConsulationDetails/10

[5] ICTA 2019/DK-TED/053 döntés Elérhető: https://www.btk.gov.tr/uploads/boarddecisions/uzaktan-programlanabilir-sim-teknolojileri-esim/053-2019-web.pdf

[6] IAPP Turkey's BTK imposes data localization requirements on e-SIM technologies [Online] Elérthető: https://iapp.org/news/a/turkeys-btk-imposes-data-localization-requirements-on-e-sim-technologies/

[6] Európai Hírközlési Kódex 93. § (6) és Eht. 150. § (3)

[7] Miklós Gellért „Overview of the Internet of Things Security Related Threats and Possible Mitigations” In: Eight International Scientific Web-conference of Scientists and PhD. students or candidates Budapest: Óbuda University, pp 209-217 (2020)

Jogszabályok

[8] Az elektronikus hírközlő hálózatok azonosítóinak nemzeti felosztási tervéről és az azonosítógazdálkodás rendjéről szóló 14/2020. (XII. 15.) NMHH rendelet
[9] AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2022/612 RENDELETE az Unión belüli nyilvános mobilhírközlő hálózatok közötti barangolásról (roaming)
[10] AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2018/1972 IRÁNYELVE (2018. december 11.) az Európai Elektronikus Hírközlési Kódex létrehozásáról
[11] Az elektronikus hírközlésről szóló 2003. évi C. törvény

NETWORK ANOMALY DETECTION WITH MACHINE LEARNING

HÁLÓZATI ANOMÁLIÁK DETEKTÁLÁSA GÉPI TANULÁSSAL

NAGY ATTILA[1]

Abstract

Information security is becoming increasingly important these days. Computer network security includes virus scanners, firewalls, intrusion detectors. Intrusion detection systems are being developed year after year. Research with deep learning and quantum computers is being done these days. These two areas have become popular research areas. Intrusion detectors have become faster and more accurate. In this paper, I present what elements are needed to detect network anomalies in computer networks using machine learning models. And finally, we touch on the quantum computer.

Keywords

Network, anomaly, machine learning, deep learning

Absztrakt

Napjainkban egyre fontosabb az információ biztonság. A számítógépes hálózat biztonsághoz tartoznak a vírusírtók, tűzfalak, behatolás érzékelők. A behatolás érzékelő rendszereket évről évre fejlesztik. A mélytanulás és a kvantum számítógépekkel végeznek napjainkban kutatásokat. Ez a két terület népszerű kutatási terület lett. A behatolás érzékelők gyorsabbak, pontosabbak lettek. A tanulmányban bemutatom milyen elemek szükségesek, hogy a számítógépes hálózatokban észlelni tudjuk a hálózati anomáliákat gépi tanulási modellekel. Végezetül a kvantum számítógépet is érintjük.

Kulcsszavak

Hálózatok, anomáliák, gépi tanulás, mélytanulás

[1] Nagy.a@uni-obuda.hu | ORCID: 0000-0003-0214-414X | PhD Student, Óbuda University Doctoral School for Safety and Security Sciences | doktorandusz, Óbudai Egyetem Biztonság-tudományi Doktori Iskola

BEVEZETÉS

A számítógépes hálózat védelme a 21. században egy fontos feladattá nőte ki magát. A nemzetek az információs társadalom kialakításában tevékenykednek. Az ilyen társadalmakban a mindennapi élet részét képezi az információ, a kommunikáció és a tudás. A modern kor információs forradalmat többféle képen lehet jellemezni: a digitális elektronika megjelenése, az informatikai eszközök térhódítása, ezen belül a számítógépes hálózatok fejlődése, a tudomány rohamos fejlődése és terjeszkedése és még a tudásipar és multimédia megjelenése stb. Mint láthatjuk a számítógépes hálózat szerves része az információs forradalomnak. [1] 1995. decemberében az internethasználók száma 16 millió volt. 2021 márciusára ez a szám 5.1 milliárdra ugrott, ami a Föld lakosságának 56,6% teszi ki. [2] Európában az internetfelhasználók száma a Föld lakosságának 14.2% teszi ki. [3] A KSH adatai alapján Magyarországon a 2020-as évben az internethasználók aránya 85% volt. [4] Az internetre csatlakozott internet of things (IoT) eszközök száma 2019-ben 7.74 milliárd volt, 2022-re ez a szám 11.57 milliárdra ugrott és 2030-ra 25.44 milliárd eszközt jósolnak a szakértők. [5] Az adatokból látható, hogy a hálózatok napról napra terjednek méretben és komplexitásban egyaránt. A terjedéssel a támadási felülete is megnő az infrastruktúrának. A számítógép-hálózatok védelmének megvalósítása lehet passzív és aktív. Az Európai Uniós kiberbiztonsági ügynökség (ENISA) 2021-ben az évente kiadott jelentésében, nyolc kiberbiztonsági fenyegetettséget emeltek ki. Zsarolóvírus (ransomware): a kártékony szoftverek családjába tartozik. A támadás az áldozat adatait rejtjelezi és csak pénz ellenében fejtik vissza az adatokat, rosszindulatú szoftverek (malware) vagy kártékony szoftverek egy gyűjtőnév, ami magában foglalja a vírusokat, férgeket, kémszoftvereket stb. A cryptolopás (cryptojacking) vagy rejtett kriptobányászat egy olyan bűncselekmény, ami az áldozat számítógép erőforrásait felhasználva a bűnözőnek hoz hasznot, e-mail-el összefüggő fenyegetések (E-mail related threats) az ide tartozó fenyegetések a phishing, spear-phishing, whaling, smishing, bishing, spam. A fenyegetések az adatok ellen (threats agains data) olyan fenyegetések gyűjteménye, ami az adatok ellen irányul azzal a céllal, hogy jogosulatlan hozzáférést, nyilvánosságra hozatalt szerezzenek. A fenyegetettségek a rendelkezésreállás és a sértetlenség ellen (threats against availability and integrity): a rendelkezésreállásra irányuló támadás az elosztott szolgáltatás-megtagadással járó (DDoS) támadással támadják. Dezinformáció és félretájékoztatás (disinformation - misinformation): a dezinformáció egy szándékos támadás, amely hamis vagy félrevezető információk létrehozásából vagy megosztásából áll. Ez a típusú támadás a COVID-19 pandémia idején exponenciálisan megnövekedtek (pl. az oltás manipulálására használták). A félretájékoztatás nem szándékos támadás. Ebben az esetben az információ megosztása véletlenül történik (pl. az újságíró rossz információról számol be). Minden információ hordozhat magában pontatlan részeket. A nem rosszindulatú fenyegetettségek (non-malicious threats): álltalában emberi hibára vagy hibás beállításra alapoz a támadás. [6] A számítógép-hálózatok védelmének megvalósítása lehet passzív és aktív. Passzív lehet: tűzfal, vírusirtó, hozzáférési szabályozás, behatolás detektálás. Az aktív védelem lehet: megelőző támadás, ellentámadás és aktív megtévesztés. Az említett fenyegetettségeket a számítógépes hálózat forgalmában észlelhető különböző megoldásokkal. Az egyik megoldás a behatolás érzékelő rendszer. A mai technológia fejlettség mellet a klasszikus behatolás érzékelő rendszerek elavultak mivel lassúak, sok fals negatív riasztás jeleznek be és a null-napi támadások ellen sem hatékonyak mivel nem ve-

szik észre a fenyegetést. 2014-ben a mély tanulás megjelenésével esélyünk lett a gépi tanulási algoritmusokkal új behatolás érzékelőket fejleszteni és használni. A régi behatolás érzékelőkkel szemben az új módszerrel a sebessége megnő, precízebb lesz és az ismeretlen támadásokat (null-napi támadások) is felismeri, amivel egy érzékenyebb rendszert fogunk kapni. Ha nem lenne elég a klasszikus számítógépek gyorsasága akkor a nem túl távoli jövőben megjelennek a kvantum számítógépek, ami az észlelő képesség gyorsaságán fog javítani. A következő néhány oldalban a behatolás rézkelő rendszerek fontosabb elemeit részletezzük.

Behatolásérzékelő rendszerek

A behatolásérzékelő rendszer gondolatával először Dorothy Denning és Peter Neumman játszott el. Ők fejlesztették ki 1984 és 1986 között az első valós idejű behatolásérzékelő rendszert (angol nevén: Intrusion Detection System – IDS). A behatolásérzékelő rendszereket két csoportra lehet bontani, host-alapú behatolásérzékelő rendszerre és hálózatalapú behatolásérzékelő rendszerre. A host-alapú rendszer log és állományok monitorozására használják. A hálózatalapú rendszereket pedig a hálózatok monitorozására használják, ami számunkra fontos. A hálózatalapú behatolásérzékelő rendszerek két fő modellt alkalmaznak az észlelésre (rendellenességet észlelő modell és visszaélést érzékelő modell). A rendellenességet észlelő modellhez tartozik az anomália alapú, viselkedés alapú és irányelv alapú észlelés. A visszaélést érzékelő modellnél pedig a tudáson alapúló és helytelen használatra alapúló észlelés használja. [7]

Gépi tanulás

A gépi tanulás térhódítása azért lehetséges mert a 21. században rengeteg adatot gyűjtöttünk és nagy teljesítményű számítógépeket is fejlesztettünk ki. Ennek segítségével a gépi tanulási algoritmusokat képesek vagyunk alkalmazni és olyan kapcsolatokat találhatunk az adatok között, amit máshogy nem lennénk képesek észlelni sem szemmel, sem más eszközökkel. Az 1950-es években jelentek meg az első algoritmusok csak akkor még nem tudtuk őket használni adat és hardware hiánya miatt. A gépi tanulási algoritmusokat fel lehet osztani tanulásuk szerint, ebben az esetben három fő csoportot kapunk (felügyelt tanulás, felügyelt nélküli tanulás és megerősítéses tanulás). Ha a hálózatokban szeretnénk észlelni az anomáliákat akkor a felügyelt nélküli tanulást kell alkalmazni. A felügyelt nélküli tanuláshoz tartoznak a következő algoritmusok: K-közép, SVD mint dimenzió csökkentő, Gauss mátrix, neurális hálózatok és a neurális hálózatokból kifejlődött mély tanulás, amit 2010-ben kezdtek az emberek használni. [8]

Neurális hálózat

A neurális hálózat az emberi agy működését próbálja leutánozni. A neuronok együttműködő processzáló elemek melyek számításokat végeznek el. Ezek a neuronok ún. rétegekből épülnek fel. Az információ csak rétegből rétegre halad egy irányba a bemeneti rétegből a kimeneti rétegig vagy a kimeneti rétegtől a bemenet felé terjed. [8]

Mély tanulás

A mély tanulás a gépi tanulás mesterséges neurális hálózatokon alapuló alkészlete. A tanulási folyamat azért mély mert a neurális hálózatok struktúrája több bemenetet, kimenetet és rejtett réteget tartalmaz. Az összes réteg egységekből épülnek fel, melyek a bemeneti információt úgy alakítja át, hogy a következő réteg eltudja végezni a predektív feladatot. [9]

A kiberbiztonság területén a gépi tanulást, mint módszert több területen lehet alkalmazni. Kártevő alkalmazások észlelésére, az emberi manipuláció detektálására ide tartozik a deepfake, a dezinformáció, személyazonosság analízise. A behatolás észleléshez tartoznak a webszerverek sérülékenysége, a tor hálózaton nyomon követni egyes felhasználót vagy kártevő weboldalak detektálására. Az automatikus behatolás detektáláshoz az adathalász oldalak érzékelése és a hálózati anomáliák észlelése tartozik. [10] A gépi tanulás széleskörű felhasználási lehetőséget nyújt a kiberbiztonság területén is. A továbbiakban az anomáliák detektálásával fogunk foglalkozni.

A gépi tanulási algoritmusokat számos területen alkalmazható, a kiberbiztonság területén egyaránt. A gépi tanulási algoritmusok üzemanyaga az adat. Ezek az adatok adatkörökbe vannak szedve. A mi esetünkben az adatkörök hálózati forgalmat tartalmaznak neutrális és káros adatokat egyaránt, aminek segítségével a gépi tanulási algoritmusok képesek mintákat találni és a hasznos adatforgalmat eltudja különíteni a káros adatforgalomtól.

Adatkörök

A hálózati forgalmat tartalmazó adatkörök beszerzése régen nehéz volt. A hálózati adatforgalom nem publikus ez miatt nem volta egyszerű a beszerzése. Az egyik Kanadai Intézet ami kiberbiztonsággal foglalkozik évről évre újabb és újabb adatköröket készített (pl. Intrusion detection system 2018 vagy a 2017es változat, Túlterhelésestámadási adatköröket is készítettek, Darknet, TOR és VPN adatköröket is). A minőséges kutatáshoz ez nem kielégítő. A tanulmányban mi az IDS 2018-as változatát választottuk mivel ez a legújabb. Az adatkör a következő támadásokat tartalmazza: [11]

- Nyers erő támadás más néven bruteforce támadás (FTP, SSH)
  Az ilyen féle támadással a behatoló kevés információval rendelkezik az áldozatról és úgy próbálja megkerülni a biztonsági védelmet, hogy nyers erő támadást alkalmaz, ami azt jelenti, hogy egy megadott csoportú karakterekkel próbál a jelszóra rájönni. Ha a jelszú gyenge akkor eredményes tud lenni az ilyen féle támadás. [12]
- Szolgáltatásmegtagadó támadás (Slowloris, GoldenEye, Hulk, Slowhttp)
- Webalapú támadás (Nyers erő támadás, xss és DVWA)
  Az XSS vagy Cross site scripting egy számítógépes sebezhetőség, amely webalkalmazásoknál fordul elő. A támadó egy olyan kódot illeszt be a weboldalra, amit minden felhasználó lát. Ez lehet egy HTML kód is. Ha felfedezünk egy XSS sérülékenységet akkor kikerülhetjük a hozzáférési ellenőrzéseket pl. úgy, hogy nem a weblapról számozó eredeti forrást használjuk fel. Napjainkban ezt a támadást az adathalász támadás végrehajtásánál alkalmazzák. [13]
- Zombi hálózat támadás
  „A kiberbűnözők által menedzselt botneteket, olyan internetes kapcsolattal rendelkező szoftver robotok, ún. zombi számítógépek alkotják, amelyeket a gépen futó

valamely program sebezhetőségét kihasználva távolról megfertőznek, vagyis amelyekre valamilyen távoli menedzselésre is alkalmas rosszindulatú programot telepítenek a felhasználó tudta és akarata nélkül" [14]
- Beszivárgó támadás
- Port letapogatás és elosztott túlterheléses támadás (http kérés, LOIC) [11]

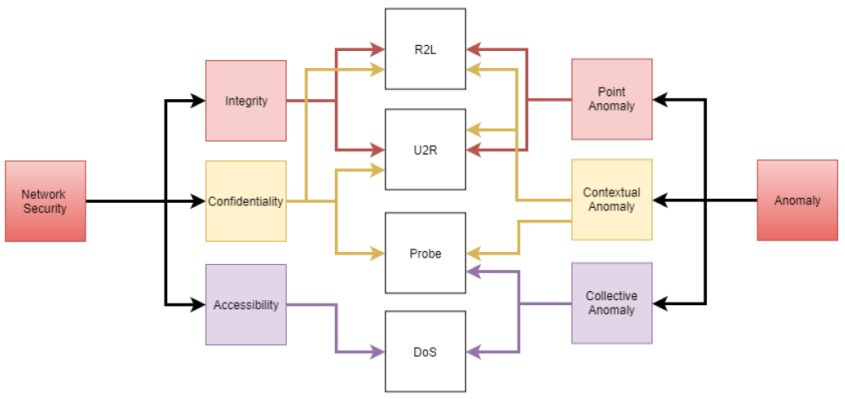
Hálózati támadások

A hálózati támadásokra többféle felosztás létezik. A tanulmányban az egyik fő csoportosítás használtuk fel, ami a következő:
- Túlterheléses támadás (DoS – Denial of Service)
  Az elfogadható válaszidő egy számítógépes alkalmazások esetén a legjobb esetben 0,1 szekundum. Az 1 szekundum válaszidő is még elfogadható a felhasználó számára. De ha 10 szekundum feletti a válaszidő, akkor a felhasználó figyelme máshova terelődik. [15]. Ebből az következik, hogy az internetes szolgáltatásokat nem minden esetben kell a lekapcsolásig terhelni, hanem elég csak annyira, hogy a felhasználók érdeklődése máshova irányuljon. A túlterheléses támadás egy olyan támadás, ami informatikai szolgáltatásokra irányul. A **túlterheléses támadás** álltalában nem veszélyesek, de ha több támadás jön több helyről (végpontról) az már gondod okozhat. Ha több helyről érkezik a támadás akkor azt **elosztott túlterheléses támadásnak** nevezzük. A következő típus a **reflektív támadás**, ami több végpontot használ, de nincs az ellenőrzésük felett. Csak a végpontokat felhasználva sokszorozza meg a forgalmat és irányítja a támadó felé. A fent említett támadásokkal a sávszéleséget, kapcsolatfelvételt vagy a forrásokat terhelik le. [16]
- Információ gyűjtés (Probe)
  Az információ gyűjtő támadás a célpont rendszeréről gyűjt információkat adatokat. Ezen a támadáson keresztül a támadó sok fontos információt tud beszerezni pl. a számítógépes hálózat felépítéséről, milyen operációs rendszert használnak. Ez a támadás nem okoz semmilyen sérülést az áldozatnak, evvel a támadással előkészítjük a következő támadást, ami már sérülést okozhat a rendszerre.
- U2E (Felhasználó a root felé)
  Ez a típusú támadásnál a támadó kísérletet tesz, hogy megszerezze a rendszergazda felhasználó fiókját annak érdekében, hogy fontos adatokat lopjon el. A támadó sérülékenységeket használhat ki vagy bruteforce támadást alkalmaz, hogy betudjon jutni a rendszergazda fiókjába.
- R2U/R2L (Távoli elérés a felhasználó felé vagy lokálisan)
  Ennél a típusú támadásnál a támadó beszivárog az áldozat hálózatába, és ott szerez jogosultságokat úgy, hogy hamis csomagokat küld a támandó számítógépre. Ebben az esetben is működik a sérülékenységek kihasználása vagy a bruteforece támadás. [17]

Anomáliák

Hogy ha egy adat kimagasló, szokatlan vagy az átlagtól eltérő akkor anomáliára lehet következtetni az adatkörben. A mi tanulmányunkban az anomáliák egy támadásra fog utalni, de lehet valami hiba is vagy akár átverés. Az anomáliát más néven is szokták hívni

outlire-nek. Az outlireek észlelése fontos mert nagy kárra is utalhat, amit fontos észlelni és javítani egy szervezetnek. Az outlireek detektálása három kategóriába lehet sorolni felügyelt tanulásra (supervised anomaly detection), felügyelt nélküli tanulásra (unsupervised anomaly detection) és ennek a kombinációjával (semi-supervised anomaly detection). A felügyelt tanulásnál az adatkörök tartalmaznak címkéket angolul lable az alapján határozza meg az anomáliákat. A felügyelt nélküli tanulásnál az adatbázis nem tartalmaz címkéket. Az a modell magától tanulja meg, hogy mi az anomália a minták segítségével.
Az outlireek három csoportját ismertetjük melyek a következők: pont-anomália, környezeti (kontextuális) anomália és együttes kollektív anomália. [17] [18]
„Pont-anomália alatt olyan objektumot értünk, amely önmagában is nagyban eltér a sokaság egészétől". Ami, azt jelenti, hogy ha drámaian eltér az adat a megszokottól akkor az pont-anomáliának nevezzük. Ha egy dolgozó csak délelőtt dolgozik és akkor jelentkezik be egy számítógépbe, de ha ugyan ez a dolgozó az esti órákban is bejelentkezik a számítógépbe azt már pont-anomáliának nevezzük. Ebben az esetben feltételezhetünk egy lehetséges támadást.
„Környezeti anomáliák közé tartoznak például olyan mérési eredmények, amelyek önmagukban véve nem szokatlanok, de az adott szituációban igen". Az anomáliákat kontextusában is kell figyelnünk mivel van olyan esett, hogy ha egy ember kisebb összegeket költ vásárlásra napi szinte, de ünnepekor nagyobb összeget költ ezt nevezzük anomáliának. Nem minden esetben feltételezzük, hogy támadás történt.
„Együttes anomáliák alatt olyan mérési eredményeket értünk, amelyek önmagukban nem tekinthetők anomáliának, együttesen viszont igen." Az együttes anomáliát könnyebb megérteni egy SYN elárasztási támadással. Ha két eszköz szeretne egymással kommunikálni TCP IP kapcsolattal akkor egy sémát kell követni. Ezt a sémát a SYN elárasztási támadással kilehet játszani. A kliens és a szerver között SYN, ACKSYN, ACK csomagot váltanak egymással és evvel a kapcsolat létre jön. A SYN elárasztásnál csak az első csomagot küldjük el, de nem egyszer, mint a sémában, hanem több ezerszer. Evvel a támadással a szervert képesek vagyunk leállítani vagy lelassítani, hogy ne legyen képes a rendeltetés szerű működésre. Szóval, ha csak egy SYN csomagot küldünk az még nem utal támadásra, de ha több ezret akkor azt együttes anomáliának tekintjük és egy támadást feltételezhetünk. [17]
A támadások és anomáliák között kapcsolat van, amit az 1. ábrán lehet látni.



1. ábra A hálózati támadások és anomáliák kapcsolata [17]

Kvantum számítógép

Az emberiség lassan, de biztosan felkészülhet a kvantum számítógépek korára. A kvantum számítógép ereje abban rejlik, hogy több állapotot vehet fel, ellentétben a mostani hagyományos számítógépekkel szemben. [19] A világ fel kell, hogy készüljön a kvantum utáni titkosításra is. [20]
A kvantum számítógéppel is lehetséges az anomáliák detektálása, kvantum anomália detektálásnak hívják. A gépi tanuláson alapuló anomália-észlelő algoritmusok széles választéka létezik, amelyek kiterjeszthetők a kvantum birodalomra. Ezek az új kvantum-algoritmusok nemcsak új kvantumjelenségek azonosításában, hanem biztonságos kvantumadatátvitelben, biztonságos kvantumszámításban és felhőn keresztüli ellenőrzésben is alkalmazhatók lehetnek. Ezek a kérdések még fontosabbá válhatnak, ahogy a felhőalapú kvantumszámítási rendszerek kvantuminternetté fejlődnek. [21]
A kvantumszámítás és a mélytanulás népszerű kutatás terület lett. A kvantumneruális hálózatokat (QNN) fejlesztik. Óriási lehetőség rejlik a két kutatási terület metszéspontjában. Ricks és Ventura volt az egyik legkorábbi, aki olyan QNN-t javasolt, amelyet kvantumáramkör-kapu segítségével modelleztek, amelynek súlyait kvantumkeresés és darabonkénti súlytanulás segítségével tanulták meg. [22]

ÖSSZEGZÉS

A számítógépes hálózatok védelme egy fontos terület. A mérnökök többféle védelmet építettek ki az idők során (tűzfal, vírusírtó, behatolás érzékelő rendszerek). Az új technológiák új védekezési lehetőségeket hoztak magukkal. A behatolás érzékelő rendszereket most már a gépi tanulási algoritmusokkal tovább fejlesztettük. Ezen belül a mélytanulási hálózatokat is alkalmazhatjuk. Ennek segítségével a behatolás érzékelés gyorsabb, pontosabb és a nulnapi támadások ellen is véd. A nem túl távoli jövőben pedig a kvantum számítógépek segítségével még gyorsabb behatolás érzékelő rendszerek megépítésére leszünk képesek. A kvantum számítógép és a mélytanulási hálózat napjainkban egy népszerű területé alakult ki.

FELHASZNÁLT IRODALOM

[1] Kritikus infrastruktúrák és kritikus infrastruktúrák (Letöltve: 2022.05.08)
[2] Internet growth statistics [Online]. Elérhető: https://www.internetworldstats.com/emarketing.htm (Letöltve: 2022.05.08)
[3] Internet usage statistics – The internet big picture [Online]. Elérhető: https://www.internetworldstats.com/stats.htm (Letöltve: 2022.05.08)
[4] Központi statisztikai hivatal – Internethasználók aránya [Online]. Elérhető: https://www.ksh.hu/stadat_files/ikt/hu/ikt0029.html (Letöltve: 2022.05.08)
[5] Statista – Number of internet of things connected devices worldwide from 2019 to 2030 [Online]. Elérhető: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/ (Letöltve: 2022.05.08)
[6] ENISA threat landscape 2021 [Online]. Elérhető: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021/@@download/fullReport (Letöltve: 2022.05.08)
[7] Behatolás-érzékelők [Online]. Elérhető: http://old.sztaki.hu/~btoth/sztaki/IDS.pdf (Letöltve: 2022.05.08)

[8] Gépi tanulás a gyakorlatban [Online]. Elérhető: https://www.inf.u-szeged.hu/~rfarkas/ML21/index.html (Letöltve: 2022.05.11)
[9] Mély tanulás és gépi tanulás a Azure Machine Learning [Online]. Elérhető: https://docs.microsoft.com/hu-hu/azure/machine-learning/concept-deep-learning-vs-machine-learning (Letöltve: 2021.12.11)
[10] Emmanuel Tsukerman – Machine Learning for Cybersecurity [Online]. Elérhető: packpub.com (Letöltve: 2022.05.11)
[11] IDS 2018 [Online]. Elérhető: https://www.unb.ca/cic/datasets/ids-2018.html (Letöltve: 2022.05.11)
[12] Próbálgatásos technikák – nyers erő támadás [Online]. Elérhető: https://gyires.inf.unideb.hu/KMITT/c12/ch06s08.html (Letöltve: 2022.05.11)
[13] Cross site scripting (XSS)[Online]. Elérhető: https://www.cert.hu/cross-site-scripting-xss (Letöltve: 2022.05.11)
[14] Botnetek kialakulása, használatuk, trendjeik [Online]. Elérhető: http://hadmernok.hu/archivum/2008/2/2008_2_illesi.pdf (Letöltve: 2022.05.11)
[15] Response times 3 important limits [Online]. Elérhető: https://www.nngroup.com/articles/response-times-3-important-limits/ (Letöltve: 2022.05.11)
[16] Gyányi Sándor – Túlterheléses informatikai támadási módszerek és a velük szemben alkalmazható védelem [Online]. Elérhető: https://nke-repo.uninke.hu/xmlui/bitstream/handle/123456789/12255/ertekezes.pdf;jsessionid=CFF905A5AF971170147C040AD8536437?sequence=1 (Letöltve: 2022.05.11)
[17] Kahraman Kostas – Anomaly detection in networks using machine learning 2018.,[Online]. Elérhető: https://www.researchgate.net/publication/328512658_Anomaly_Detection_in_Networks_Using_Machine_Learning/link/5bd1d1bf458515343d58eddc/download (Letöltve: 2022.05.11)
[18] Bodon Ferenc, Buza Krisztián: Adatbányászat 2014., [Online]. Elérhető: https://regi.tankonyvtar.hu/hu/tartalom/tamop412A/20110064_55_adatbanyaszat/ar01s08.html (Letöltve: 2022.05.11)
[19] Beginner's guide to quantum machine learning [Online]. Elérhető: https://blog.paperspace.com/beginners-guide-to-quantum-machine-learning/ (Letöltve: 2022.05.11)
[20] ENISA – Post-quantum cryptography [Online]. Elérhető: https://www.enisa.europa.eu/publications/post-quantum-cryptography-current-state-and-quantum-mitigation/@@download/fullReport (Letöltve: 2022.05.11)
[21] Nana Liu, Patrick Rebentrost – Quantum machine learning for quantum anomaly detection [Online]. Elérhető: https://www.researchgate.net/profile/Nana-Liu-10/publication/320564334_Quantum_machine_learning_for_quantum_anomaly_detection/links/59ee00a84585154350e7fb85/Quantum-machine-learning-for-quantum-anomaly-detection.pdf (Letöltve: 2022.05.11)
[22] Siddhant Garg, Goutham Ramakrishnan – Advances in quantum deep learning: an overview [Online]. Elérhető: https://www.researchgate.net/publication/341311377_Advances_in_Quantum_Deep_Learning_An_Overview/fulltext/5eba1a614585152169c84087/Advances-in-Quantum-Deep-Learning-An-Overview.pdf (Letöltve: 2022.05.11)

OCCUPATIONAL HEALTH, OCCUPATIONAL SAFETY IN RELATION TO THE EMPLOYMENT OF DISABLED PERSONS AND ICF (OVERVIEW)

MUNKAEGÉSZSÉGÜGY, MUNKABIZTONSÁG A MEGVÁLTOZOTT MUNKAKÉPESSÉGŰ SZEMÉLYEK FOGLALKOZTATÁSA SORÁN ÉS AZ FNO (KITEKINTÉS)

NAGY Sarolta[1]

Abstract

The disabled persons'employment is a special area aslo of occupational safety and of occupational health as well. For all experts (engineers, doctors, occupational safety specialists) understandable and useful directives regarding disabled persons' employment, which are known and accepted internationally, are still under development. The „International Classification of Functioning, Disability and Health" published by WHO in 2001, the ICF is an internationally accepted code system, primarly used to assess and measure disabilty during medical treatment and clinical rehabilitation. We reviewed in the international and domestic literature the areas of use of ICF. According to the international literature and our research team, the ICF code system could be used during the assessment of jobs and in the assessing the skills and disability of the disabled person applying for job, and in fitting the job to the employee based on the ICF. The several stages of development will result, that the ICF will be able to used regurarly in occupational safety and occupational health.

Keywords

Occupational Safety, Occupational Health, ICF, Functioning, Disability,

Absztrakt

A fogyatékos személyek foglalkoztatása a munkaegészségügynek és a munkavédelemnek is speciális területe, melyhez nemzetközileg is ismert, elismert, illetve minden szakterület (mérnök, orvos, munkavédelmi szakember) által érthető és használható segédletek még csak fejlesztés alatt állnak. A WHO által 2001-ben kiadott „A funkcióképesség, fogyatékosság és egészség nemzetközi osztályozása" az FNO, egy nemzetközileg elfogadott kódrendszer, melyet elsősorban az akadályozottság felmérésére, mérésére használnak a gyógykezelés és a klinikai rehabilitáció során. Az FNO felhasználásának területeit áttekintettük a nemzetközi és a hazai irodalomban. A nemzetközi irodalom és a kutató csoportunk szerint is az FNO kódrendszerét használni lehetne a munkakörök felmérése során és a munkára jelentkező megváltozott munkaképességű személy képességeinek, akadályozottságának felmérésében és ezek alapján a munkakör munkavállalóhoz történő illesztésében is. Több lépcsős fejlesztés eredményeként fogjuk tudni használni rendszeren az FNO-t a munkaegészségügyben.

Kulcsszavak

munkabiztonság, munkaegészségügy, FNO, funkcióképesség, fogyatékosság,

[1] nagy.sarolta@nnk.gov.hu | ORCID: 0000-0002-8560-1002 | PhD student, Óbuda University Doctoral School for Safety and Security Sciences | occupational health specialist, National Center for Public Health | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola | foglalkozás-egészségügyi szakorvos, Nemzeti Népegészségügyi Központ

BEVEZETÉS

A munkát végző személyeknek joguk van a biztonságos és egészséges munkafeltételekhez, az egészséget nem veszélyeztető és biztonságos munkavégzés körülményeinek megvalósításáért a munkáltató felelős. [1] A sérülékeny munkavállalói csoportba tartozó munkavállalókat (megváltozott munkaképességű személyek, fiatalkorúak, terhes, nemrégen szült nők, idősödők) óvni kell az őket különösen érintő egészségkárosító kockázatoktól. [1] A sérülékeny munkavállalói csoportba tartozó munkavállalók esetében a testi, lelki adottságaik, speciális igényeik, az általuk használt segítőtechnológiák miatt a többi munkavállalóhoz képest eltérően kell felmérni, értékelni a munkahelyi kockázatokat és mindig egyénileg kell a munkaköri, illetve szakmai alkalmasságot megítélni, a munkakört adaptálni a munkavállalóhoz.

Az idősödő társadalom és egyéb okok miatt időről időre munkaerőhiánnyal küzd a munkaerőpiac, aminek eredményeképpen a nyugdíjas, és a megváltozott munkaképességű személyek közül elsősorban a fogyatékos személyek bekapcsolódnak, illetve visszatérnek a munkavilágába. Mindegyik esetben a sérülékeny munkavállalói csoportba tartozó személyekről van szó, tehát mind foglalkozás-egészségügyi, mind munkavédelmi szempontból külön figyelmet igényelnek.

A fogyatékos személyek foglalkoztatása, újra foglalkoztatása az esetek többségében speciális helyzet, feladat a foglalkozás-egészségügy és a munkavédelem számára is. Minden esetben körültekintőbben járnak el a szakemberek, sok esetben morális és infokommunikációs akadálymentesítés szükséges és esetenként a munkakörnyezet, a munkaeszköz akadálymentesítésére, adaptálására is szükség van. A helyesen megválasztott munkakör, jól adaptált munkakörnyezet csökkentheti a munkabalesetek esélyét is. Sem a KSH, sem az Európai Bizottság munkabalesetekről szóló statisztikáiban nem szerepel, hogy megváltozott munkaképességű személyek milyen arányban szenvednek balesetet munkavégzés közben. Az EU jelentésben a 55-64 év [2], a Magyarországi statisztikákban a 45-64 év [3] közötti korosztály szenvedett el leggyakrabban halálos, illetve súlyos munkabalesetet. A WHO szerint, az idősödés folyamatában 50 év felett az áthajlás kora, 60 év felett az idősödés koráról beszélünk, azaz az idősödő személyekről, akik a sérülékeny munkavállalói csoportba tartoznak. Mind az idősödő, mind a valamelyik fogyatékossági csoportba tartozó személyek esetében hasonló okokból kell körültekintőnek lennünk fokozottan balesetveszélyes munkakör esetén. A leggyakoribb munkával kapcsolatos egészségkárosodások: mozgásszervi, szív-érrendszeri, érzékszervi és pszichés elváltozások [4], ha ezen balesetek során maradandó károsodást szenved a munkavállaló, akkor már, mint megváltozott munkaképességű, esetenként fogyatékos személy fog visszatérni a munkavilágába. Ezek alapján nem kérdés, hogy mennyire fontos és hasznos minden munkavállaló és a munkáltatók számára is, a munkahelyek, munkakörök kockázatértékelésekor külön figyelmet fordítani a sérülékeny munkavállalói csoportba tartozó munkavállalók igényeire, védelmére és ezek alapján végrehajtani a javasolt intézkedéseket.

A munkahely adaptálása során nem ugyanazt a „nyelvet” használja a mérnök, a munkavédelmi szakember, a munkahigiénikus és az orvos, sőt előfordul, hogy egy betűszó, rövidítés mást jelent a mérnöknek és mást az orvosnak. Jelentősen felgyorsítaná és leegyszerűsítené a munkakörök leírását, a munkavállalók és a munkakörök illesztését, adaptálását, ha közös, mindenki által egyformán értelmezett nyelvet, kódrendszert használnának a munkavédelemben dolgozó szakemberek. A nemzetközi irodalom és véleményünk szerint

is a „A funkcióképesség, fogyatékosság és egészség nemzetközi osztályozása" kódrendszer, azaz az FNO ezeknek az elvárásoknak megfelelne.

CÉLKITŰZÉS ÉS MÓDSZER

Magyarországon az FNO rendszert a mozgásszervi rehabilitációban, elsősorban végtag amputáció és gerincsérülés után, illetve mozgáskorlátozott és látássérült személyek rehabilitációja során használják. Első lépésként meg kellet ismerni az FNO rendszer célját, logikáját, tartalmát. A nemzetközi és a hazai szakirodalmat néztük át, illetve felkerestük az Eötvös Loránd Tudományegyetemen a korábban az FNO-val foglalkozó szakembereket. A megszerzett ismeretek alapján lehet megkeresni az FNO helyét és alkalmazásának módját a munkavédelem, ezzel együtt a foglalkozás-egészségügy területén. Következő kutatási fázisban az FNO munkavédelemben történő használatához kérdőíveket és kategória készleteket kell összeállítani. A munkakörök felméréséhez és fogyatékosság specifikus, illetve a megváltozott munkaképességű személyek akadályozottságát általánosan felmérő, jól használható kérdőívek és kategória készletek összeállítása után lehet felvenni a kapcsolatot a WHO-val, hogy egy nemzetközi szakemberekből összeállított kutatócsoport elemezze, javítsa és elfogadja a kérdőíveket, illetve a kategória készleteket. A WHO-val való kapcsolatfelvétel és közös munka több egyetem és kormányzati intézmény közös munkájaként, évek múlva valósulhat meg.

SZAKIRODALMI ÁTTEKINTÉS, LEHETŐSÉGEK FELTÉRKÉPEZÉSE

Az FNO szerint a fogyatékosság különböző tényezők közötti kölcsönhatás lsd. 1. ábra. Az egészségi állapotunk, a környezet és a személyes tényezőink is befolyásolják az életünk három dimenzióját, ezekkel együtt hatnak a funkcióképességünkre és mindezek között kölcsönhatás is van. A fogyatékosságot, akadályozottságot nem kizárólag a testi funkciók kiesése eredményezi, hanem a környezeti és a személyes tényezőknek is jelentős szerepük van. Hiszen egy küszöb és lépcső nélküli épületben kerekesszékkel akadályok nélkül lehet közlekedni, míg magas küszöbökkel és lépcsőkkel teli épületben nem, tehát a fogyatékosságot, az akadályozottságot nem a mozgásszervek funkciókiesése eredményezte, hanem a környezet. Az FNO nem magát a betegséget, az elváltozást veszi figyelembe, hanem a teljesítőképességet, a részvételt, a tevékenység elvégzését, illetve akadályozottságát, és a környezet támogató, vagy akadályozó szerepét, attól függően, hogy milyen hatása van az ember funkcióképességére. [5]

1. Ábra: Az FNO alkotóelemeinek kölcsönhatása, [5]

Az FNO az embert három aspektusból értékeli, biológiai oldalról, a test, szervek épségét, érintettségét és működését, diszfunkcióját (testi funkciók és struktúrák), az embert, aki cselekszik, tevékenykedik (tevékenységek) és az embert, aki a társadalom része, szerepeket tölt be családban, lakhelyén, munkahelyén (részvétel). Az FNO rendszerben kategóriákba kell sorolni (1494 kategóriát tartalmaz az FNO) a problémát, eltérést, elváltozást és egy ötfokozatú skálán minősíteni, az FNO egy ordinális skála. Az FNO kódolási rendszere négy fő alkotóelemből áll, melyeket előtaggal (betűjellel) jeleznek.

A fő alkotóelemek:

- testi funkciók (betűjele: b), mint mentális funkciók, érzékelési és fájdalom funkciók, hangadás és beszédfunkciók, stb. (pl. b2300 hangfelismerés);
- testi struktúrák (betűjele:s), mint idegrendszeri struktúrák, mozgáshoz kapcsolódó struktúrák, a szem, fül és kapcsolódó struktúrák, stb. (pl. s260 belső fül struktúrája);
- tevékenység és részvétel (betűjele: d), mint tanulás és ismeretek alkalmazása, mobilitás, önellátás, fő életterek, kommunikáció, stb. (pl. d3501 társalgás fenntartása, párbeszéd);
- környezeti tényezők (betűjele: e), mint támaszok, kapcsolatok, szolgáltatások, természetes környezet és emberi beavatkozással létrehozott változások a környezetben, termékek és technológia, stb. (pl. e1301 segítő termékek és technológiák az oktatás céljára) .

A kategóriákba sorolás után ötfokozatú skálán kell a probléma mértékét jelölni nincs probléma, illetve akadályozottság és a teljes akadályozottság között, lsd 1. táblázat. [5]

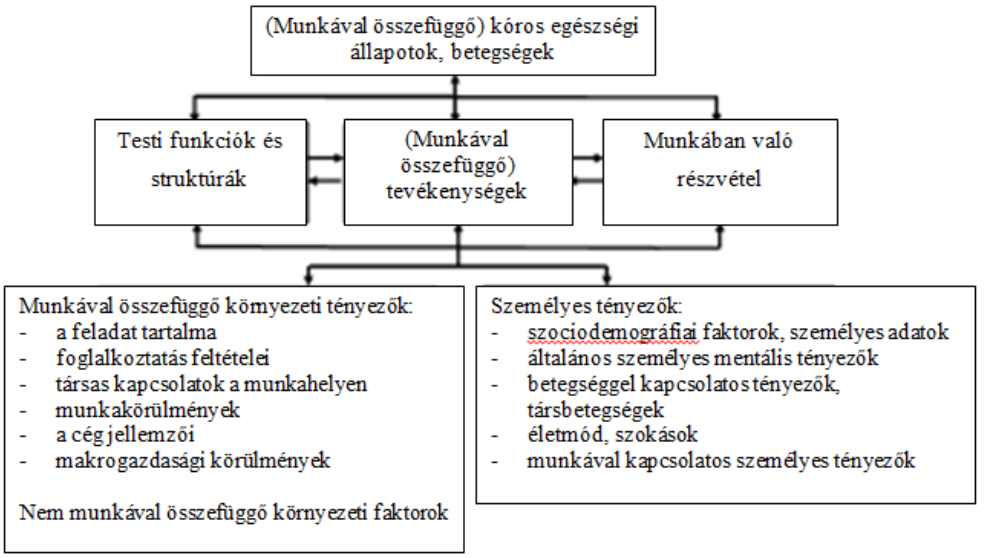
		Testi funkciók, struktúrák, tevékenység, részvétel		**Környezeti faktor**			
nincs, hiányzik	0-4%	xxx.0	nincs probléma	xxx.0	nincs akadály	xxx+0	nem támogató
enyhe, csekély	5-24%	xxx.1	enyhe probléma	xxx.1	enyhe akadály	xxx+1	enyhén támogató
közepes, meglehetős	25-49%	xxx.2	mérsékelt probléma	xxx.2	mérsékelt akadály	xxx+2	mérsékelten támogató
nagymértékű, extrém	50-95%	xxx.3	súlyos probléma	xxx.3	súlyos akadály	xxx+3	jelentősen támogató
teljes, totális	96-100%	xxx.4	teljes probléma	xxx.4	teljes akadály	xxx+4	teljesen támogató
		xxx.8	nem meghatározott	xxx.8	nem meghatározott	xxx+8	nem meghatározott
		xxx.9	nem alkalmazható	xxx.9	nem alkalmazható	xxx+9	nem alkalmazható
magyarázat: xxx a főkategória betűjele és a szintek számjele							

1. Táblázat: Az FNO minősítők általános skálája, saját szerkesztés „A funkcióképesség, fogyatékosság és egészség nemzetközi osztályozása” alapján [5]

A WHO nemzetközi munkacsoportjai kidolgoztak un. core setteket, kategória készleteket, melyek egy-egy állapotra legjellemzőbb FNO kategóriákat tartalmazzák és ezekhez kérdőívet, ellenőrző listát is összeállítottak. Ezeket a core setteket és ellenőrző listákat használva nem kell az FNO összes alfejezetét és az alfejezetek alatt található szinteket végig kérdezni, átbeszélni a vizsgált személlyel. Ezeket a kategória készleteket frissítik, újakat készítenek, illetve a már kész core setteket a tapasztalatok alapján módosítják. A WHO által elfogadott kategória készletek szabadon elérhetőek az interneten. [6] Az FNO kódrendszere elsőnek bonyolultnak és időigényesnek tűnik, de gyakorlás után és a már kész állapotspecifikus kategória készletek, core settek és ellenőrző listák használatával rutinszerűen végezhető feladat. [7]

Az FNO kódrendszert tesztelő kutatócsoportok közül a Vakok Állami Intézetében dolgozó szakemberek az FNO-val történt állapotfelmérés után megkérdezték a vizsgált személyek véleményét az FNO-ról és a visszajelzéseket is értékelték. A látássérült személyek az FNO használatakor sokkal jobban meg tudták fogalmazni, hogy milyen elvárásaik vannak a rehabilitációjuk során, pontosan mire van szükségük. [8] Ez is bizonyítja, hogy ha a munkakörnyezetek, munkakörök FNO segítségével történő adaptálási folyamatába bevonják a fogyatékos személyeket, sokkal jobban illeszkedő, támogatóbb munkakörnyezet alakítható ki. Személyes interjúkkal végzik az állapotfelmérést, így az FNO adatfelvétel a kommunikációt is segíti, a szakemberek és a páciensek, munkavállalók között. A megfelelő kategóriakészlet használatakor a felmérésben résztvevők jobban megértik a fogyatékosságot, akadályozottságot eredményező különböző tényezők közötti kölcsönhatást, kapcsolatot és azt, hogy az egyénnek és a környezetnek is nagy szerepe van a rehabilitáció sikerességében. [7] A már kész core settek jól használhatóak rehabilitáció, egyéni fejlesztés sikerességének mérésére, nyomon követésére is. Gyógypedagógiai fejlesztésben résztvevő tanulók esetében tesztelték a CP (cerebrális paretikus) specifikus core settet egy tanéven át és jól követhetőek voltak az időbeni változások és az egyes csoportok közötti különbségek is. [9] Ez azt jelenti, hogy az FNO folyamatok, és a funkcióképesség dinamikus változásának felmérésére is használható.

Holland kutatócsoport vizsgálta az FNO használhatóságát a foglalkozás-egészségügyben. A holland kutatócsoport összegyűjtötte a munkával kapcsolatos, elsősorban munkakörnyezeti tényezőket és párhuzamba állította az FNO-ban található környezeti tényezőkkel. Elkészítették a környezeti és személyes tényezők bővített listáit, melyeket a kutatócsoport szerint jól lehet használni a munkaképesség, illetve fogyatékosság mérésére, a foglalkoztathatóságot javító beavatkozások kiválasztására, szakmai útmutatók készítésére a foglalkozás-egészségügyben, oktatásban, kutatásban. Az FNO alkotóelemei közötti kölcsönhatást szemléltető diagramot adaptálták a munkára. lsd. 2. ábra. A kutatócsoport véleménye is alátámasztja, hogy a megváltozott munkaképességű munkavállalók foglalkoztatása során minden munkával kapcsolatos un. környezeti tényezőt figyelembe véve kell megvalósítani a munkába állást, illetve a visszatérést a munkába. [10]



2. Ábra: Az FNO alkotóelemeinek kölcsönhatása munkára adaptálva. Holland kutatócsoport ábrájának fordítása [10]

A foglalkozási rehabilitáció célja, hogy a megváltozott munkaképességű személyek munkaerőpiaci és társadalmi integrációja sikeres legyen. A rehabilitáció teljes folyamatában, megtervezésben, végrehajtásban, nyomon követésében több ágazat szakemberei vesznek részt, ezért fontos ebben az esetben is egy közös nyelv, egy mindenki által ugyanúgy használható és értékelhető mérési módszer, melynek megfelel az FNO. Annak érdekében, hogy az FNO kódrendszere használható legyen a munkába való visszatérés folyamatában és a foglalkozási rehabilitáció során, szükséges egy egységes felmérési és értékelési módszer, ehhez dolgoztak ki egy kérdőívet (WORQ –kérdőív a foglalkozási rehabilitációhoz), mely szabadon elérhető [11]. A WORQ kérdőív a foglalkozási rehabilitációban résztvevő személy munkaanamnézisét és funkcióképességét, munkaképességet méri fel, ezáltal egyénre szabottan lehet meghatározni az adott személyt érintő akadályokat, problémákat a munkavállalás során és követhető a foglalkozási rehabilitáció folyamata. Szükség esetén közbe lehet lépni, változtatni a rehabilitációs terven, hogy a lehető legjobb munkaképességet érje el a beteg és ezáltal a munkába állása is sikeres legyen. [12], [13]

A munkaképesség hatással van az elvégzett munkára, a munka minőségére, ugyanakkor a munkavégzésnek, a munkahelyi kóroki tényezőknek lehetnek rövid távú és hosszú távú hatásaik a munkát végző személyre, változásokat okozhatnak az emberi szervezetben, ezek az egészségi változások pedig hatással vannak a munkaképességre. Az FNO használható ezen egészségi változások, munkaképesség változások beazonosítására, felmérésére, a változások követésére. [14] Ezek a felmérések megfelelnek az FNO eredeti céljának, csak munkakörnyezetre, munkavállalóra adaptálva.

ÖSSZEFOGLALÁS, KÖVETKEZTETÉSEK

A WHO által készített „A funkcióképesség, fogyatékosság és egészség nemzetközi osztályozása", FNO kódrendszert elsősorban a klinikumban használják, krónikus betegek, balesetben maradandó sérülést szenvedett emberek, mozgáskorlátozott személyek, állapotának felmérésére és rehabilitációjának megtervezéséhez, nyomon követéséhez. Az FNO megjelenése óta érdeklődnek a munkaegészségügyben dolgozó szakemberek a kódrendszer iránt. Több nemzetközi kutatócsoport átnézte, tesztelte az FNO-t a munkával, munkakörnyezettel kapcsolatban. Minden esetben a foglalkozási rehabilitáció és munkába való visszatérés támogatásában látták az FNO használhatóságát.

A szakirodalomban talált kutatások alapján az FNO nem csak állapotfelmérésre használható, hanem folyamatok, pl. a foglalkozási rehabilitáció, munkába való visszatérés, egyéni fejlesztés megtervezésére, sikerességük értékelésére, nyomon követésére és így a fogyatékos személyek mellett a sérülékeny munkavállalói csoportba tartozó többi munkavállaló foglalkoztatásának, újra foglalkoztatásának elősegítésére.

A szakirodalomban nem találtunk arra vonatkozóan konkrét eredményeket, hogy munkakörök felmérésére használták volna az FNO kódrendszerét. A már elkészített kategória készletek és kérdőívek alapján elképzelhető a munkakörök FNO szerinti bekódolásához használható core settek elkészítése. A foglalkozási rehabilitációs intézkedések, munkakörillesztések alapjául szolgáló segédleteket elkészítésének különböző fázisaiba be kell vonni a már dolgozó és a még nem dolgozó megváltozott munkaképességű személyeket, a munkavédelmi és a foglalkozás-egészségügyi szakembereket is. Így biztos semmilyen körülmény, tényező nem kerül el az FNO kódrendszer fejlesztőinek figyelmét. Eddig az FNO felméréseket személyes interjúk és kérdőívek alapján végezték, viszont a munkavállalók pontos fizikai állapotának, funkcióképességének meghatározásához eszközös vizsgálatok is szükségesek. A munkacsoportunk következő célja a Magyarországon elérhető képességmérő eszközök illesztése az FNO rendszerhez.

Az FNO rendszeres használata a munkaegészségügy területén megkönnyítené a megváltozott munkaképességű személyek foglalkoztatását, bejutását a nyílt munkaerőpiacra, számukra is biztonságos, egészséget nem veszélyeztető munkakörnyezetbe. Egy könnyen használható segédlet, kódrendszer, mely segítségével a munkahely, munkakör adaptálása, a munkavállaló és a munkakör illesztése egyszerűen kivitelezhető lenne, mind a munkaerőpiacra most belépni szándékozó és a munkából baleset, betegség miatt kiesett, de visszatérni szándékozó személyeknek is megkönnyítené a munkavállalást.

FELHASZNÁLT IRODALOM

[1] 1993. évi XCIII. törvény a munkavédelemről https://net.jogtar.hu/jogszabaly?docid=99300093.tv

[2] *A munkabalesetek okai és körülményei az EU-ban*, Európai Bizottság, Foglalkoztatási, Szociális és Esélyegyenlőségi Főigazgatóság F.4. egység: Luxemburg, 2008. Elérhető: http://www.ommf.gov.hu/nyomtatvanyok/MV.kiadv.amunkabalesetek.okai.pdf

[3] *Tájékoztató a munkabalesetek alakulásáról a feldolgozott munkabaleseti jegyzőkönyvek alapján 2022. I. félév*, Technológiai és Ipari Minisztérium, Munkavédelmi Irányítási Főosztály:, Budapest, 2022. Elérhető: http://www.ommf.gov.hu/index.php?akt_menu=223

[4] *Munkabalesetek és a munkával kapcsolatos egészségkárosodások, 2007,* Életszínvonal- és Munkaügy- statisztikai főosztály, Munkaügy-statisztikai osztály, in Staisztikai tükör II. évfolyam 6. szám. Elérhető: https://www.ksh.hu/docs/hun/xftp/stattukor/munkabaleset07.pdf

[5] FNO *A funkcióképesség, fogyatékosság és egészség nemzetközi osztályozása,* World Health Organization hozzájárulásával az ESzCsM, az OEP, a Medicina Könyvkiadó együttműködésében, 2004. Elérhető: https://apps.who.int/iris/bitstream/handle/10665/42407/9632428382-hun-LR.pdf?sequence=124&isAllowed=y

[6] https://www.icf-research-branch.org/icf-core-sets

[7] L. Kulmann, „A modern rehabilitációs szemléletet tükröző egyéni állapotfelmérő módszer, A funkcióképesség, fogyatékosság és egészség nemzetközi osztályozása (FNO) elméleti és gyakorlati alkalmazásának tapasztalatai. A módszer alkalmazási lehetőségei a mozgássérült emberek rehabilitációjában" Eötvös Loránd Tudományegyetem Bárczi Gusztáv Gyógypedagógiai Kar, Budapest, 2012. Elérhető: http://gurulo.hu/sites/default/files/tanulmanyok/fuzet_5_kullmann.pdf

[8] R. Falvai, É. Kovács, „Az FNO alkalmazása a látássérült személyek rehabilitációjában" Vakok Állami Intézete, Budapest, 2010. Elérhető: http://213.181.192.30/~vakokint/wp-content/uploads/2016/10/fno.pdf

[9] Z. Lénárt, „Spasztikus cerebrális paretikus tanulók felső végtagi mozgásainak fejlődése egy tanév alatt: Vizsgálati lehetőségek pedagógiai színtéren és egyes mérhető változások" Ph.D. disszertáció, " Eötvös Loránd Tudományegyetem Pedagógiai és Pszichológiai Kar Neveléstudományi Doktori Iskola, Budapest, 2019. Elérhető: https://ppk.elte.hu/dstore/document/170/lenart_zoltan_disszertacio.pdf

[10] Y. F. Heerkens, C. P. M. de Brouwer, J. A. Engels, et al., „Elaboration of the contextual factors of the ICF for Occupational Health Care" *Work,* 57 (2017) pp. 187-204, doi: 10.3233/WOR-172546, Letölthető: https://www.researchgate.net/publication/317321349_Elaboration_of_the_contextual_factors_of_the_ICF_for_Occupational_Health_Care

[11] Work Rehabilitation Questionnaire (WORQ) Elérhető: https://www.myworq.org/quest/nrs/WORQ_IA_NR_A17_B42_English.pdf https://www.myworq.org/quest/nrs/WORQ-Brief_SR_NR_English.pdf https://www.myworq.org/quest/nrs/WORQ_SR_NR_English.pdf

[12] M. E. Finger, R. Escorpizo, C. Bostan, et al., „Work Rehabilitation Questionnaire (WORQ): Development and Preliminary Psychometric Evidence of an ICF-Based Questionnaire for Vocational Rehabilitation", J. Occup. Rehabili. (2014) 24, pp. 498-510, doi: 10.1007/s10926-013-9485-2, Letölthető: https://www.researchgate.net/publication/258955530_Work_Rehabilitation_Questionnaire_WORQ_Development_and_Preliminary_Psychometric_Evidence_of_an_ICF-Based_Questionnaire_for_Vocational_Rehabilitation

[13] R. Escorpizo, M. F. Reneman, J. Ekholm, et al., „A Conceptual Definition of Vocational Rehabilitation Based ont he ICF: Building a Shared Global Model", *J. Occup. Rehabil.* (2011) 21, pp. 126-133, Letölthető: https://www.researchgate.net/publication/49842638_A_Conceptual_Definition_of_Vocational_Rehabilitation_Based_on_the_ICF_Building_a_Shared_Global_Model

[14] Y. Heerkens, J. Engels, C. kuipers, et al., „The use of the ICF of describe work related factors influencing the health of employees", *Disability and Rehabilitation,* vol. 26, no. 17, pp.1060-1066, March. 2004. Letölthető: https://www.researchgate.net/publication/8343891_The_use_of_the_ICF_to_describe_work_related_factors_influencing_the_health_of_employees

REVIEW ABOUT THE BOOK AMY B. ZEGART: SPIES, LIES, AND ALGORITHMS: THE HISTORY AND FUTURE OF AMERICAN INTELLIGENCE

RECENZIÓ AMY B. ZEGART: SPIES, LIES, AND ALGORITHMS: THE HISTORY AND FUTURE OF AMERICAN INTELLIGENCE CÍMŰ KÖNYVÉRŐL

GULYÁS Attila[1]

Key sentence: "America's intelligence agencies must adapt or they will fail."

Amy B. Zegart[2] is the Morris Arnold and Nona Jean Cox Senior Fellow at the Hoover Institution and Professor of Political Science (by courtesy) at Stanford University. She is also a Senior Fellow at Stanford's Freeman Spogli Institute for International Studies, Chair of Stanford's Artificial Intelligence and International Security Steering Committee, and a contributing writer at The Atlantic. She specializes in U.S. intelligence, emerging technologies and national security, grand strategy, and global political risk management. Zegart has been featured by the National Journal as one of the ten most influential experts in intelligence reform. Most recently, she served as a commissioner on the 2020 CSIS Technology and Intelligence Task Force (co-chaired by Avril Haines and Stephanie O'Sullivan) and has advised the National Security Commission on Artificial Intelligence. She served on the Clinton administration's National Security Council staff and as a foreign policy adviser to the Bush 2000 presidential campaign. She has also testified before the Senate Select Committee on Intelligence and advised senior officials on intelligence, homeland security, and cyber security matters.

Amy B. Zegart's name is a guarantee for the high quality content as a leading national expert on the United States Intelligence Community and national security she has comprehensive knowledge about the actual state of the American Intelligence Community and the challenges it faces now and in the future.

As an outsider, Amy B. Zegart faced challenges in accessing to classified information so she could study only the publicly available sources, but she realized the inherent possibilities in this situation and articulated her own independent opinions and critics. She masterfully exploited the potential in her special position to present the history of the American Intelligence, the essence of the intelligence in generally, the pitfalls of the

[1] gulyas.attila@phd.uni-obuda.hu | ORCID: 0000-0001-5645-144X | PhD Student, Óbuda University Doctoral School for Safety and Security Sciences | doktorandusz, Óbudai Egyetem Biztonságtudományi Doktori Iskola

[2] Amy B. Zegart is the Morris Arnold and Nona Jean Cox Senior Fellow at the Hoover Institution and Professor of Political Science (by courtesy) at Stanford University. She is also a Senior Fellow at Stanford's Freeman Spogli Institute for International Studies, Chair of Stanford's Artificial Intelligence and International Security Steering Committee, and a contributing writer at The Atlantic. She specializes in U.S. intelligence, emerging technologies and national security, grand strategy, and global political risk management. Zegart has been featured by the National Journal as one of the ten most influential experts in intelligence reform. Most recently, she served as a commissioner on the 2020 CSIS Technology and Intelligence Task Force and has advised the National Security Commission on Artificial Intelligence. She served on the Clinton administration's National Security Council staff and as a foreign policy adviser to the Bush 2000 presidential campaign. She has also testified before the Senate Select Committee on Intelligence and advised senior officials on intelligence, homeland security, and cyber security matters. [1]

intelligence collection and analysis. Zegart also demonstrate how complicated to find the balance between secrecy and openness and sheds some light on the intricate interrelations that underlie the democratic control of the American intelligence services. In addition to the organizational intelligence collection, she gave a glimpse of the peculiarities of the amateur, non-governmental OSINT intelligence collectors activities and the implications on the intelligence community. She dedicates a separate chapter to cyber security which is one of the most burning security question of our era.

The author flooded the reader with case studies, reports from the real life, collected citations from politicians making them more understandable by tables, figures.

The first chapter is on the new security landscape of our era in which the Intelligence Community has to face the gamut of security challenges. The author articulates the problems one by one with short explanations to make them and clear, and where it needs she illuminates their contexts.

The challenges of the social media emerged in the near past seem to fading away in the light of challenges of AI or the Quantum Supremacy, not to mention the gene technology. The AI reforms the way as we see the world, it can release human capacity in many aspects of everyday life. AI makes decisions on behalf of the human causing ethical problems. Can (at all) AI blamed for decisions? Our present cryptography system would collapse by a single blow when someone win the Quantum Supremacy, and until new technology won't be elaborated we won't have digital secrets. Only few of us take into account the inherent possibilities of the synthetic biology that has endless possibilities in the change of our life and poses boundless security risks. The gene modified plants, animals, human, not to mention the race tailored pathogens are just to name a few.

With the end of Cold War, the security landscape has dramatically changed. Instead of a clearly defined enemy the Intelligence Community faces many different threatens from different directions. The balance of power has also changed because earlier the super powers threatened the smaller, weaker countries, but it is not the situation anymore. Today, these “weak” countries, or even terrorist organizations having the new technologies are capable to threaten super powers.

Until the last decade only the super powers had resources to process big amount of information while today countries with modest resources are also capable to collect, and process information in bigger volume. Due to the technical development new devices with sci-fi like capabilities are available for average people, so practically anyone can be intelligence collector as we could see after the siege of the capitol when volunteers helped to identify the participants by the social media pictures. Although this a Janus- faced phenomenon, because these OSINT activist with lack of intelligence analysis training often conclude wrong causing misunderstanding that the Intelligence Community has to correct them drawing away resources from the really important tasks.

Earlier in history threatens had perceptible signs, today threatens come from the cyber space which doesn’t exist physically. The strikes come anonymously from the out of blue, in many cases without any prior notice so in cases there is no chance for the retaliation.

The second chapter of the book demonstrates how much know American citizens about intelligence and the intelligence services. The fictional books and movies shaped their knowledge painting a false deceptive picture of the intelligence itself. Unfortunately,

this is the hot bed of the conteos, the deep state fantasies, misunderstanding of the role of intelligence services. Owing to the lack of education of intelligence, including the politicians, only few know the real possibilities and capabilities of intelligence services so in cases they have unreal expectations towards the services.

The second factor that hinders the recognition of intelligence activity is the secrecy. Without this intelligence service doesn't exist, but at the same time it doesn't let scientist and researchers to study and hone its efficiency.

The third chapter is dedicated to the history of the American intelligence which is definitely shorter than some of the European or Asian counterparts. The author with ruthless honesty reveals the childhood diseases of the American intelligence evolution including the democratic tensions, the fragmentations, halting development. We can see the arch from the George Washington's spies trough the spy satellites to the remote controlled spy and striker UAVs in parallel with the evolving role geopolitical of the United States. In this chapter the reader is introduced to the endless conflict between the secrecy and need for openness in democracy. This conflict is inherent in the world of intelligence, because it must keep in secret its sources, procedures, technics and capabilities to be capable to carry out its secret information collection function. Simultaneously, the society tries to keep under control the services, which is a cumbersome process because of aforementioned reasons. Further, Zegart presents the American Intelligence community's structure and gives the readers a glimpse of the background of the creation Director of National Intelligence position.

The next chapter is the backbone of the book. It tells what intelligence is and what is not. Zegart carefully explains what is the aim of the intelligence, what are the core missions, and how it is supposed to support the policymaking. Their job is to provide the best available intelligence and leave the policy making to the politicians. Yet, despite the best efforts there are frictions between intelligence services and politicians because they came from different worlds and see the world differently.

Further, she examines intelligence basics through the analytic lens, a human lens and an operational lens which is an interesting approach of this topic.

She made vivid this chapter by interviewing current and former intelligence officers whose jobs included briefing the president, catching traitors, handling assets and defectors. The interviewees reveal their ethical dilemmas, their success and worst moments.

She crowned this chapter with the story of catching Osama Bin Laden putting the story in intelligence context.

The fifth chapter presents the intelligence analysis, the different analysis methods with their advantages and disadvantages including the seven deadly biases. She explains why it is so hard to provide user-friendly, user -tailored reliable intelligence. She cites as a deterrent example the "Curveball" case which is the epitome of the bad intelligence analysis. In this chapter she also studies the possibilities of the AI usage in the analysis examining it strong and weak sides.

The following section of the book is about traitors, which is a very sensitive and unpleasant question within the intelligence community. The author takes the possible motives through what can turn our insiders to be a turncoat. She demonstrates through the three intelligence challenges the Robert Hanssen and Aldrich Ames cases, which are

undeniably among the most notorious cases in the twenty-first history of the American Intelligence community. James Jesus Angleton's "blessed reign" is also a part of the deterrent examples in this book demonstrating how hard it is to find the balance between trust and paranoia. She also deals with question of the technical development that is double-edged swords since it provides our activity with sophisticated encrypted communication, but it also support our enemies with hindering our fight against them.

The seventh chapter is touching a widely debated hot topic burdened with ethical dilemmas. The covert actions divide not only the politicians, but the civil society, as well. After reading this part of the book we will know what covert action is, and who can approve it under what circumstances. What happens if a covert action fails? Does US have right to kill someone in a foreign country without any trial, and judgment? The author walks with us through the dilemmas in connection with the covert actions. We well know the possible reasons why presidents prefer covert actions.

The following pages in the book are dedicated to the mysterious world of congressional oversight. Zegart explains from multi aspects view how it developed, why it is so important, what difficulties burden this institution, and why it works with so bad efficiency. She offers a valuable glimpse into the world of Senate Committees revealing the reasons why senators shy away from membership of Intelligence Committee. The CIA detention and interrogation program along with the NSA warrantless wiretapping program are also discussed as the two notorious controversial scandals that generated heated debates both in the world of policy and in civil society.

Chapter nine is about the change caused by digital technology in nuclear sleuthing. In the 21st century the nuclear intelligence is not the privilege of superpowers anymore. Non-governmental organizations or even individuals can investigate illicit nuclear activities worldwide using open source technologies. This dramatic change has undeniable benefits, but it also has disadvantages as well, since the publicized wrong analysis can lead to international tensions that the intelligence services have to correct, and in cases it takes many resources from the services.

The last part of the book deals with the newly emerged pervasive cyber threats and their consequences in the light of intelligence services. The topic is actual, interesting and puts into spotlight how important having controlled the cyber space where nefarious actors employ deception, carry out cyber espionage campaigns, wage information warfare trying to influence the society. The traditional domain like land, air, and sea totally differ from the manmade cyber domain that is inherently insecure. Nature can provide geographic advantages for some countries and vulnerabilities for others while in the cyber domains it is not valid anymore. The natural sources have no effect on the outcome of cyber warfare. The cyber threat is a special act if it hacks not only the computers or computer networks but it hacks minds as well. The cyber-attacks aim to destroy the confidentiality, integrity, availability, and reliability. In the course of a cyber-attack it is hard to identity the perpetrator and the real nature of the weapon used in the action since it can be a simple malware or a part of a sophisticated cyber espionage software system. Further, Zegart demonstrates how social media can influence the mindset and opinions of the society, how dangerous it can be if it used by nefarious intentions.

Later, the author points out that we can only see a little portion of AI capabilities and it is only the beginning, and no one can foresee where it ends. The deep fake videos and photographs are so real that by using them one can create a forged reality.

She also brings up the inevitable role of the leader of techgiants as they form our future giving citizens new technologies that can have harmful effect on national security so they have unalienable responsibilities in the national security.

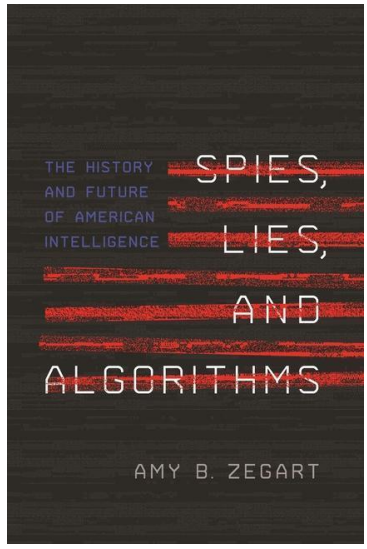
I recommend this book for those who are interested in intelligence, especially in American intelligence, because after reading this book the reader will be aware of the intelligence basics, and the challenges the American intelligence faces now and in the future. Due to its structure this book is applicable for educational purposes as well.

REFERENCES

[1] Stanford Center for International Security and Cooperation, Freeman Spogli Institute, Institute Faculty and Researchers: Amy Zegart, PhD Biography, https://cisac.fsi.stanford.edu/people/amy_zegart [Accessed: May 12,2022]

LIBRARY DATA

Editorial: Princeton University Press (February 1, 2022)
Language: English
Hardcover: 424 pages
ISBN-10: 0691147132
ISBN-13: 978-0691147130
Item Weight: 1.9 pounds
Dimensions: 6 x 0.25 x 9 inches



1. ábra: The cover of the book. Source: https://www.amazon.com/Spies_Lies_and_Algorithms_The_History_and_Future_of_American_Intelligence/dp/0691147132

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