

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



On the cover can be seen | A borítón

KOLLÁR Csaba

Keywords | Kulcsszavaink

digital print | című digitális nyomata látható

© KOLLÁR Csaba, 2020

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
<p style="text-align: center;">COLUMNS</p> <p style="text-align: center;">Material Safety Philosophy and History of the Safety and Security Security Policy Security Systems Security Awareness Health Security Food Safety Economic Security War Security and Law Enforcement Information Security Industrial and Operational Safety Legal and Social Security Book Review Security of Environment Traffic Safety Private Security Artificial Intelligence Safety and Security in General Technical Security</p>	<p style="text-align: center;">ROVATOK</p> <p style="text-align: center;">Anyagbiztonság Biztonságfilozófia és -történet Biztonságpolitika Biztonságtechnika Biztonságtudatosság Egészségbiztonság Élelmiszerbiztonság Gazdasági biztonság Hadbiztonság és rendvédelem Információbiztonság Ipar- és üzembiztonság Jog- és társadalombiztonság Könyvismertetés Környezetbiztonság Közlekedésbiztonság Magánbiztonság Mesterséges intelligencia Munkabiztonság Műszaki biztonság</p>
<p>The aim of the journal is to publish studies, research reports, articles, book reviews of the broad discipline of security science for professionals working in or related fields of security science, thereby developing security awareness and security culture.</p> <p>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.</p> <p>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.</p> <p>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).</p>	<p>A folyóirat célja a biztonságtudomány területén, vagy ahhoz kapcsolódó területeken dolgozó szakemberek és a téma iránt érdeklődők számára a biztonságtudomány tágan értelmezett diszciplináris keretébe tartozó tanulmányok, kutatási jelentések, beszámolók, könyvismertetők megjelentetése, s ennek révén a biztonságtudatosság és a biztonsági kultúra fejlesztése.</p> <p>Megjelenés negyedévente, jellemzően magyar, eseti jelleggel idegen nyelven. Konferenciákhoz és témákhoz kapcsolódóan különszámok, tematikus számok alkalmi jelleggel magyar, vagy idegen nyelven jelennek meg.</p> <p>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.</p> <p>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).</p>

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>

Edited by Editorial Board | Szerkeszti a Szerkesztőbizottság

Chairman of the Editorial Board | A Szerkesztőbizottság elnöke

Prof. Dr. RAJNAI Zoltán

rajnai.zoltan@bgk.uni-obuda.hu

Scientific Secretary of the Editorial Board, person responsible for editing | A szerkesztőbizottság tudományos titkára, a szerkesztésért felelős személy

Dr. KOLLÁR Csaba PhD

kollar.csaba@phd.uni-obuda.hu

Members of the Editorial Board | A szerkesztőbizottság tagjai

Prof. Dr. BÁNÁTI Diána banati.diana@unideb.hu

BEREK László berek.laszlo@lib.uni-obuda.hu

Dr. habil. BEREC Tamás PhD berek.tamas@uni-nke.hu

Dr. habil. BESENYŐ János PhD besenyo.janos@phd.uni-obuda.hu

Prof. Dr. CVETITYANIN Lívía cpinter.livia@bgk.uni-obuda.hu

Prof. Dr. Dragan JOVANOVIĆ draganj@uns.ac.rs

Dr. KOVÁCS Tünde PhD kovacs.tunde@bgk.uni-obuda.hu

Dr. Cyprian Aleksander KOZERA PhD c.kozera@akademia.mil.pl

Prof. Dr. Manuela TVARONAVIČIENĚ manuela.tvaronaviciene@vgtu.lt

Staff of the Editorial Board | A szerkesztőbizottság munkatársai

BELÁZ Annamária, SZALÁNCZI-ORBÁN Virág

English language lecturer | Angol nyelvi lektor

BEKE Éva

Technical editor | Technikai szerkesztő

HARTMANN László

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 biztonságstudomány nemzetközi, lektorált, szakmai és tudományos folyóirata

Vol 2, No 2, 2020.

2020. II. évf. 2. szám

Authors of this issue

E számunk szerzői

BESENYŐ János

beseny.o.janos@phd.uni-obuda.hu

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

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

GULYÁS Péter

peter.gulyas@quadron.hu

In parallel with his studies in economics, finance, IT and marketing, he began his career in 2001 as an economic analyst at the Statistical Office. Over the next 13 years, he has developed sales strategies for three major companies and brands at the Central and Eastern European regional level. Since 2002, he has been a sales and project manager at Wincor Nixdorf, selling bank ATM and safe solutions. Since 2004 as a regional partner manager at Xerox, he has achieved double digit growth in several key market segments. Since 2006, as Symantec’s Regional Partner and Strategic Account Manager, he has successfully grew the partner ecosystem in the Central and Eastern European markets. In 2011, he earned an MBA from CEU. From 2014, he built the QUADRON Cybersecurity Ltd.’s reputation as the commercial and marketing manager and since 2016, as Managing Director, he has achieved significant success in both the domestic and Middle Eastern regions.

Felsőfokú közgazdasági, pénzügyi, informatikai és marketing tanulmányai elvégzésével párhuzamosan karrierjét 2001-ben a KSH gazdasági elemzőjeként kezdte. Az ezt követő 13 évben három nagy nemzetközi brand értékesítési stratégiáját alakította ki közép-kelet-európai regionális szinten. 2002-től a Wincor Nixdorf partner és projektmenedzsereként kaszarszarendszerek, valamint banki ATM és trezor megoldások értékesítésével foglalkozott. 2004-től a Xerox regionális partner menedzsereként elérte a cég piaci részesedésének szignifikáns növekedését. 2006-tól a Symantec regionális ügyfélkapcsolati vezetőjeként, stratégia projektek és marketingkampányok menedzsereként sikeres pályára állította a teljes termékportfóliót a helyi, és a közép-kelet-európai piacokon. 2011-ben MBA diplomát szerzett a CEU-n. 2014-től a QUADRON Kibervédelmi Kft. kereskedelmi és marketing vezetőjeként építette a cég hírnevét, majd 2016 óta ügyvezető igazgatóként komoly sikereket ért el mind a hazai és a Közel-Keleti régióban.

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

KÁRÁSZ Balázs

karasz@gmail.com

Balázs Kárász (1992) economist in leadership and management, risk management specialist, consultant. Research topic: role of human factors in the complex approach of information security, especially the development of information security awareness. PhD Student of the National University of Public Science, Doctoral School of Military Engineering, senior consultant at Keys4Corporate Ltd.

Kárász Balázs (1992) okleveles közgazdász, kockázatkezelési szakértő, tanácsadó. Kutatási területe a humán tényezők szerepe az információbiztonság komplex értelmezésében, kiemelten az információbiztonság-tudatosság fejlesztése. A Nemzeti Közszerológati Egyetem Katonai Műszaki Doktori Iskola hallgatója, a Keys4Corporate Kft. vezető tanácsadója.

KÁRMÁN Marianna

karman.marianna@phd.uni-obuda.hu

Marianna Kármán, PhD in African Literary and Cultural Studies, has been researching the oral and written traditions, cultural and religious system and practices of the region for about 20 years - primarily in Nigeria. Her specialization includes Islamic Studies, intercultural discourse, African migration, the process and social context of African neology. Until 2012, she continued her scientific work as a doctoral student at the Doctoral School of Literary Studies at Pázmány Péter Catholic University, and currently as a researcher at the Doctoral School of Security Sciences at Óbuda University.

Kármán Marianna, az afrikai irodalom- és kultúratudományok doktora, mintegy 20 éve kutatja a térség szóbeli és írásbeli hagyományait, kulturális és vallási rendszerét és gyakorlatait – elsősorban Nigériában. Szakterületei közé tartozik az iszlám vallás, az interkulturális diskurzus, az afrikai migrációja, az afrikai nyelvújítás folyamata és társadalmi összefüggései. 2012-ig a Pázmány Péter Katolikus Egyetem Irodalomtudományi Doktori Iskolájának doktoranduszaként, jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskolájának kutatójaként folytatta tudományos munkásságát.

KERÉK Gábor

kerek.gabor@eduvizig.hu

Diploma in Civil Engineering (Eötvös József College, Faculty of Engineering, Baja 2000; Budapest University of Technology and Economics, Budapest 2008), Diploma in Hydroinformatics and Water Management (Budapest University of Technology and Economics, Budapest 2016), Deputy Head of Department – North-Transdanubian Water Directorate, Győr, Department of water protection and river basin management, Hydrological Expert - Subcommittee of the Hungarian-Austrian Water Committee, Danube Subcommittee of the Hungarian-Slovak Border Water Committee, Areas of expertise: hydrologic forecasting and assessment, hydrographic monitoring, river hydrometry, surface water resource management. Currently a doctoral student at the Doctoral School of Military Engineering at the National University of Public Service. Research theme: development possibilities of flood forecasts in the Rába river basin. Member of the Hungarian Hydrological Society since 2006, and currently a member of the board of the Győr regional organization. Member of the water management and hydraulic engineering department of the Győr-Moson-Sopron County Chamber of Engineers with planning permission.

Okleveles építőmérnök (Eötvös József Főiskola Műszaki Fakultás, Baja 2000; Budapesti Műszaki és Gazdaságtudományi Egyetem, Budapest 2008.), Hidroinformatikai és Vízgazdálkodási Szakmérnök (Budapesti Műszaki és Gazdaságtudományi Egyetem, Budapest 2016.), az Észak-dunántúli Vízügyi Igazgatóság Vízvédelmi és Vízügytő-gazdálkodási osztályának helyettes vezetője, a magyar-osztrák vízügyi bizottság albizottságnak hidrológiai szakértője, a magyar-szlovák határvízi bizottság Duna-albizottságának hidrológiai szakértője. Szakterülete: hidrológiai előrejelzés és állapotértékelés, vízrajzi monitoring, folyami hidrometria, felszíni vízkészletgazdálkodás. Jelenleg a Nemzeti Közszerológati Egyetem Katonai Műszaki Doktori Iskolájának doktorandusza. Kutatási területe: árvízi előrejelzések fejlesztési lehetőségei a Rába vízgyűjtőjén. 2006 óta a Magyar Hidrológiai Társaság tagja, jelenleg a Győri területi szervezet elnökségi tagja. A Győr-Moson-Sopron megyei Mérnöki Kamara vízgazdálkodási és vízépítési szakcsoportjának tervezői és felelős műszaki vezetői jogosultsággal rendelkező tagja.

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

KOLLÁR Csaba

kollar.csaba@phd.uni-obuda.hu

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

Kommunikációtechnikai mérnök, okleveles kommunikációs szakember, elektronikus információbiztonsági vezető, a közgazdaságtudományok doktora (PhD), tanácsadó, coach, mediátor. Kutatási területe a digitális kor társadalmi vetületei és gazdasági hatásai, kiemelten az információbiztonság humán aspektusa, az információbiztonság-tudatosság fejlesztése, az ember-robot interakció, az okosváros, a mesterséges intelligencia, a társadalmi kredit rendszere. A SZIE GTK egyetemi docense, a Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola oktatója, témavezetője. Az Igazságügyi Minisztérium regisztrált közvetítője (mediátora), elnök a szakmai képzítő vizsgákon (OKJ). A PREMA Consulting vezető tanácsadója, mediátora és coacha, a Magyar Hadtudományi Társaság és a Humán Szakemberek Országos Szövetsége szakértője. Jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában gyarapítja ismereteit. 2018. negyedik negyedévétől a Mesterséges Intelligencia Konzorcium tagja.

KONDÁS Katalin

kondaskatalin@gmail.com

Katalin Kondás (1981) engineer-IT specialist, technical teacher and security engineer. His area of research is exploring the possibilities of biometric identification. He is currently expanding his knowledge at the Doctoral School of Security Sciences at Óbuda University.

Kondás Katalin (1981) mérnök-informatikus, mérnök-tanár, biztonságtechnikai mérnök. Kutatási területe a biometriai azonosítás lehetőségeinek vizsgálata. Jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában gyarapítja ismereteit.

NINKOV Ivona

ivonakakas@yahoo.com

PhD student at the Doctoral School of the Safety and Security Sciences at the Óbuda University in Budapest, Hungary. She graduated and finished her master studies at the Faculty of Law at the University of Novi Sad, Serbia. She obtained her Postgraduate Diploma in International Human Rights at the University De Montfort, Leicester, United Kingdom. and the title of the Certificite Entrepreneur from the Business Academy in Belgrade, Serbia. Since 2017 she is the leader of the non-governmental organization 'Rights 4 All', Novi Sad, Serbia. Research topics: laws connected with un-manned vehicles, regulation of personal data connected with un-maned vehicle system in the light of human rights, safety and security.

A Budapesti Óbudai Egyetem Biztonságtudományi Doktori Iskola PhD hallgatója. Mesterképzését Szerbiában az Újvidéki Egyetem Jogi Karán végezte. A Nemzetközi Emberi Jogok Posztgraduális diplomáját a Leicesteri De Montfort Egyetemén, az Egyesült Királyságban szerezte meg. Vállalkozó oklevelét a Szerbia Belgrádi Üzleti Akadémián szerezte. 2017 óta a „Rights 4 All” nem kormányzati szervezet vezetője Újvidéken (Szerbia). Kutatási témák: törvények és jogi álláspont a pilóta nélküli járművekkel kapcsolatban, a pilóta nélküli jármű-rendszerrel kapcsolatos személyes adatok szabályozása az emberi jogok, biztonság és védelem fényében.

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

SZÚCS Endre

szucs.endre@bkg.uni-obuda.hu

Endre Szűcs (1963) PhD in Military Science, Certified Security Engineer, Mechanical Engineer, Teacher of Engineering. He is currently a topic leader at the Doctoral School of Security Sciences at Óbuda University and is a lecturer at the Institute of Mechanical Engineering and Security Sciences of the Donát Bánki Faculty of Mechanical and Security Engineering at the Óbuda University.

Szűcs Endre (1963) a hadtudomány PhD fokozatos, okleveles biztonságtechnikai mérnök, gépészmérnök, mérnök tanár. Jelenleg az Óbudai Egyetem Biztonságtudományi Doktori Iskolájában témavezető, illetve az Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar Gépészeti és Biztonságtudományi Intézet óradója.

TAMPU Stelian

stelian@gmail.com

He was born in 1977 in Diószén (Gioseni), a Csángó-Hungarian settlement in Moldva. Between 1995 and 1997 he studied theology at the Roman Catholic Theological College in Gyulafehérvár. From 1997 to 2000, he worked as a teacher at the St. Francis Foundation orphanage in Deva. In 2007 he graduated as a historian and history teacher from the Eötvös Loránd University, Faculty of Humanities. His diploma work is about the emigration of Hungarians from Szeklerland and Transylvania. Between 2003 and 2019 he was the editor-in-chief of the Csángó Tükör, since 2004 he has been an employee of the Hungarian Charity Service of the Order of Malta.

Az egyik moldvai csángó-magyar településén született 1977-ben, Diószénben. 1995-1997 között teológiát hallgatott a Gyulafehérvári Római Katolikus Hittudományi Főiskolán. 1997-2000 között pedagógusként dolgozott a Dévai Szent Ferenc Alapítvány gyermekotthonában, Déván. 2007-ben szerzett történelmi és történelemtanári diplomát az ELTE-BTK-n. Egyetemi szakdolgozatában a székely és az erdélyi magyarok kivándorlásával foglalkozott. 2003-2019 között a Csángó Tükör főszerkesztője, 2004 óta a Magyar Máltai Szeretetszolgálat munkatársa.

ZAKAR Ákos

zakarakos85@gmail.com

Ákos Zakar is an economist. He is graduate student at the University of Óbuda's information security engineer specializing. Besides the CEH certificate, he has an ISMS's auditor qualifications too. As entrant he worked in the private security field, but today he has been serving his country in the field of law enforcement for 13 years. In the course of his criminal work, he tasked with detection and investigation against life and property cases, as well as crimes committed using the IT system. As a professional recognition, he was awarded by one of the biggest domestic financial institutions. Furthermore he also made a report with him on the television show 'Kékkfény' on the topic of credit card fraud series. Continuing his analytical experience at the Police, he works as an investigator in the Hungarian National Bureau of Investigation Cybercrime Department. His research field the human role of information security in preventing attacks against social engineering.

Zakar Ákos közgazdász, az Óbudai Egyetem információbiztonsági szakmérnök képzésének végzős hallgatója. Certified Ethical Hacker tanúsítványa mellett, Információbiztonsági Irányítási Rendszer auditori végzettsége is van. Pályakezdőként a vagyonvédelemben helyezkedett el, de 13 éve már a rendvédelem területén szolgálja hazáját. Bűnügyi munkája során számos élet és vagyon elleni, valamint informatikai rendszer felhasználásával elkövetett bűncselekmények felderítése és vizsgálata volt a feladata. Szakmai elismerésként az egyik legnagyobb hazai pénzügyi juttatásban részesítette, valamint a Kékkfény című televíziós műsorban is készült vele egy riport, bankkártyás csalássorozatok témájában. Folytatva a Rendőrségnél szerzett elemzői tapasztalatát, jelenleg a Nemzeti Nyomozó Iroda Kiberbűnözés Elleni Főosztályán nyomozó beosztásban dolgozik. Kutatási területe az információbiztonság humán szerepe, a social engineering elleni támadások megelőzésében.

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

Vol 2, No 2, 2020. | 2020. II. évf. 2. szám

CONTENT | TARTALOM

Safety Policy column	Biztonságpolitika rovat
-----------------------------	--------------------------------

TAMPU Stelian

Role of the Hungarian Charity Service of the Order of Malta in helping the refugees of the GDR in 1989	A Magyar Máltai Szeretetszolgálat Egyesület szerepe az 1989-es NDK menekültek megsegítésében
1-14	

Security Systems column	Biztonságtechnika rovat
--------------------------------	--------------------------------

KONDÁS Katalin – SZŰCS Endre

Special rules on personal identification in prison	A személyazonosításra vonatkozó speciális szabályok a büntetés-végrehajtásban
15-21	

Security Awareness column	Biztonságtudatosság rovat
----------------------------------	----------------------------------

KOLLÁR Csaba – ZAKAR Ákos

Social engineering and manipulation techniques and methods	A social engineering és a manipulációs technikák és módszerek
23-38	

Health Security column	Egészségbiztonság rovat
-------------------------------	--------------------------------

BESENYŐ János – KÁRMÁN Marianna

COVID-19 pandemic on the African continent	A COVID-19 pandémia az afrikai kontinensen
39-55	

Information Security column	Információbiztonság rovat
------------------------------------	----------------------------------

KÁRÁSZ Balázs

Network of user-related human risk factors in information security	Az információbiztonság felhasználói oldali humán kockázati tényezőinek hálózata
57-68	

Security of Environment column	Környezetbiztonság rovat
---------------------------------------	---------------------------------

KERÉK Gábor

The importance of flood hidrology in environmental protection	Az árvízhidrológia jelentősége a környezetvédelemben
Application of the possibilities of technical hydrology in the prevention of environmental damage and the prevention of water pollution	A műszaki hidrológia lehetőségeinek alkalmazása a környezeti kárelhárításban és a vízszennyezések megelőzésében
69-83	

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

Traffic Safety column | Közlekedésbiztonság rovat

NINKOV Ivona

Basics of developing of the legal regulation in self-driving cars 85-92	Az önjáró járművek jogszabályzata fejlesztésének alapja 85-92
--	--

Artificial Intelligence column | Mesterséges intelligencia rovat

KOLLÁR Csaba

China and information security issues in the social credit system 93-109	Kína és a társadalmi kredit rendszerének információbiztonsági kérdései 93-109
---	--

Book Review column | Könyvismertetés rovat

GULYÁS Péter

Recenzió Solymos Ákos „Frici, Fülöp és hackerek” című könyvéről
 111-114

ROLE OF THE HUNGARIAN CHARITY SERVICE OF THE ORDER OF MALTA IN HELPING THE REFUGEES OF THE GDR IN 1989**A MAGYAR MÁLTAI SZERETETSZOLGÁLAT EGYESÜLET SZEREPE AZ 1989-ES NDK MENEKÜLTEK MEGSEGÍTÉSÉBEN**TAMPU, Stelian¹**Abstract**

Leaving one's home country and choosing a new area to live in equals being a refugee. In my opinion, history of mankind is a series of events interwoven with constant waves of refugees; however, these waves receive sometimes more, sometimes less attention. Nowadays, in a time when refugee phenomenon is intense, we pay serious attention to this. If we look back into the history, we will see that migration was always there but we do not deal with all of these processes. In this study I will take the reader to a short period of the 20th century. I will describe the migration motives of the citizens of the GDR, the processes that had taken place, from the point of view a freshly founded charity organization. When the Hungarian Charity Service of the Order of Malta was founded in February 1989, no one thought that it would be the key player of one of the biggest humanitarian solutions in Europe.

Keywords

divided Europe, Soviet-style dictatorship, leaving of homeland, refugees, embracing

Absztrakt

A szülőföld elhagyása és egy új életterület választása teljes mértékben kimeríti a menekült státusz fogalmát. Úgy gondolom, hogy az emberiség történelme állandó menekült-hullámokkal átszótt cselekménysorozat, melyekre hol kevésbé, hol jobban felfigyelünk. Manapság, mivel a menekültek intenzívebb korszakát éljük, sokkal több figyelmet fordítunk ezen jelenségre, pedig ha visszatekintünk az emberiség történelmére, akkor láthatjuk, hogy mindig is zajlottak kisebb-nagyobb migrációs folyamatok, csak éppen nem foglalkozunk mindegyikkel. Ebben a tanulmányban elkalauzolom az olvasót a XX. század egyik rövid pillanatába, amikor a Német Demokratikus Köztársaság német állampolgárainak migrációs motivációit, annak folyamatait mutatom be egy frissen megalakult segítség-szervezet szemüvegén keresztül. A Magyar Máltai Szeretetszolgálat 1989. februári megalakulásakor még senki sem gondolta, hogy néhány hónap múlva Európa egyik legnagyobb humanitárius megoldásának kulcsszereplői lesznek.

Kulcsszavak

megosztott Európa, Szovjet mintájú diktatúra, szülőföld elhagyása, menekültek, befogadás

¹ sztelian@gmail.com | ORCID: 0000-0001-5493-7358 | program manager / programvezető | Hungarian Maltese Charity Service / Magyar Máltai Szeretetszolgálat

ELŐZMÉNYEK

Jelen tanulmány Kelet-Németország állampolgárainak az 1989-es menekülése részletes tárgyalásával foglalkozik és az akkor frissen megalakult Magyar Máltai Szeretetszolgálat szerepével a menekültek gondozásában. De ahhoz, hogy megértsük ezt a nagyon fontos történelmi pillanatot, nagyon röviden ugyan, de vetnünk kell egy pillantást a második világháború végére, az ezt követő 4-5 évre, a Berlini helyzetre és a két kialakult német-államképződményre (NSZK és NDK), ezen belül a magyarországi eseményekre is.

A német államra vonatkozó „*megosztás parancsa*”² visszanyúlik egészen 1943-ra, amikor az EAC³ (European Advisory Commission) októberben Cordell Hull⁴ vezetésével leszögezi, hogy miután Németországot legyőzik, a szövetséges államoknak kötelessége az ország gazdasági egységének megőrzése mellett, a náciitlanítás, a demilitarizálás és a demokratizálás. Területi struktúrájának kialakítása az 1943-as Teheráni konferencián került tárgyalóasztalra. Az üléselő vezetői javaslatai alapján a birodalmi fogalmat ki kell törölni a német tudatból, Rooseveltnél szerint őt részre kellene osztani Németországot, Sztálin azonban másképp gondolja, ő nem osztja Rooseveltnél ötletét, Németország szétdarabolási terveinek megtárgyalásain tartózkodik és később ki is jelenti, hogy nem akarja a szétdarabolást. 1944 januárja után egy újabb hivatalos ülést követően érdekes módon a szétdarabolás ötlete helyett a megszállás került előtérbe. 1944 szeptemberében Londonban már megszületett a jegyzőkönyv, amely már tartalmaz konkrét határvonalakat, s amelyben leszögezik, hogy a keleti része Németországnak szovjet megszállási övezet lesz, a nyugati része az USA, Nagy-Britannia (és később Franciaország) megszállási övezete lesz. A nyugati határvonalak kialakításáról majd csak a Quebecben tartott kormányfői találkozón állapodtak meg. Nem sokkal később Franciaország is felvételét kérte a szövetséges nagyhatalmak sorába és megszállási övezetet is követelt magának. Mindezek után a szövetséges nagyhatalmak egyetértettek a következő irányelvekben: Németországot, mint a béke veszélyeztetőjét ki kell kapcsolni a nagyhatalmak sorából, meg kell szüntetni a gazdasági hegemóniáját, ártalmatlanná kell tenni a náci ideológia fészket. 1945 februárjában megtartott Jaltai konferencián a következő 4 pontban állapodtak meg a nagyhatalmak [5]: 1. Németországot 4 megszállási övezetre osztották, ami azt jelentette, hogy az ország keleti részét képező öt tartomány szovjet megszállási övezet lesz, amely területen Berlin is elhelyezkedett, nyilvánvalóan Berlin is közös megszállási övezetet képezett, így ezen területekből jön majd létre az NDK, amelyben majd a szovjet kommunista államberendezkedés legnyugatibb állama működik. 2. Felállították a Berlieni székelyű Ellenőrző Bizottságot, amely bizottságba minden nagyhatalom 1-1 tagot delegált. Ebből a bizottságból később Moszkva kiszáll, azzal a szándékkal, hogy ellehetetlenítse a működését, de ennek ellenére a bizottság tovább folytatja munkáját (ezt még érintjük az NDK fejezetben). 3. A nemzetszocializmus megszüntetése és a demilitarizálás, ez elvi és erkölcsi kötelességgé szerepel a kor nagyhatalmi vezetőinek sokszor hangoztatott büntető ígéréseiben. 4. Jóvátetelek megállapítása a rombolások arányában. Akkor még 20 milliárd dollárról beszéltek, amelynek 50%-át a szovjetek kapták volna, a másik

² 1943 környékén még csak a Harmadik birodalom szétdarabolásáról tárgyalnak a nagyhatalmak, majd csak 1944-ben kezdenek el beszélni a megszállásról. In: Németh István, Németország története, Egységtől az Egységig (1871-1990) Aula 2004, 315.o. [5]

³ Európai Tanácsadó Bizottság, melyet a Moszkvai konferencián hoztak létre 1943.10.30.-án Londoni székhellyel, hogy biztosítsa a háború utáni Európa sorsának rendezését. [5]

⁴1933–1944 között az Egyesült Államok külügyminisztere volt.

50%-án osztozott volna az USA, Franciaország és Nagy-Britannia. A behajtás három formáját már ekkor megjelölték, az első a nemzeti vagyomból, a második az évenkénti áruszállítás és folyó termelésből, a harmadik pedig a német munkaerő felhasználásából. Sztálinnak olyan jól sikerült a behajtásokat végrehajtania [1], hogy a végére több mint 15 milliárd értékben vont ki az általa megszállt területről értékeket, elég, ha csak azt említjük meg, hogy körülbelül 1250 gyárat szereltek le és szállították a Szovjetunió területére.

Mindezen tervekről Hitler beszűkült tudata nem tudott vagy nem akart tudomást szerezni, annak ellenére, hogy a hozzá közelálló és mindvégig lojális katonai vezetők igyekeztek jelezni a véget és annak katasztrofális következményeit a német népre nézve. Tudjuk, hogy 1945. április 20-án még utoljára a felszínre jött a bunkeréből, hogy személyes jelenlétével kitüntesse és a további harcokra buzdítsa a most már kamaszkorú fiatalokból álló harcosokat, akik még abban reménykedtek, hogy megvédhetik országukat. [5]

Hitler öngyilkossága után is a nagyhatalmak csak a feltétel nélküli teljes kapitulációt akarták, mert végzetes fenyegetésnek tartották a liberál- demokratikus értékrendszerre nézve a tengelyhatalmak expanzionizmusát, ugyanis az a magánegzisztencia megsemmisítésére törekedett szerintük, ezért majd át kell őket nevelni a közösség békés tagjaivá. [1]

A kapituláció 1945.05.07-én hajnali 2 óra 41 perckor Reimsben, Eisenhower főhadiszállásán történt, ahol az aláíró Alfred Jodl. A szovjetek ragaszkodtak, hogy ők külön írják alá a kapitulációs okmányt, azaz hogy előttük külön tegyék le a fegyvert, ennek jelzés értéke volt. Így május 8-án Berlin- Karlshorstadtban aláírták a kapitulációt, ahol az aláírók Keitel, Friedeburg és Sumpff voltak. A kapituláció május 9-én lépett életbe, majd szeptember 2-án Japánt is térdre kényszerítették, melynek következményeként vereséget szenvedett a világpolitikai háromszög: Berlin-Róma-Tokió.

Az 55 millió halottal lezárult második világháború mindenkit kivéreztetett, aki részt vett benne. A győztes nagyhatalmak öröme sem lehetett felhőtlen, mert bár győztesekként ünnepelték magukat, a győzelem öröme keserű volt mindenki számára. [7] Most már csak az következett, hogy a legyőzött tengelyhatalmakat számon kérjék a háború okozta bűnökért, károkkért, veszteségekért, és mindazért is, amiről nem csak ők tehetek. A szovjetek barbár viselkedését soha senki nem kérte számon, pedig volt elég (terjedelmi okok miatt, sajnos ezekre nem térhetek ki részletesen). A Postdami konferencia, amelyet 1945. július 17-én tartottak meg, minden addigi megállapodást jóváhagyott, pontosították a határvonalakat. A kapituláció után természetesen a szövetségesek átveszik a hatalmat, hogy aztán minden megszálló eltérő politikát folytasson az általa megszállt területen. Így tett Szovjetunió is az általa megszállt Kelet-Németországban és Kelet-Berlinben.

A vétkeseket megbüntették, a Nemzetközi Katonai Törvényszék Nürnbergben levezényelte a pereket, amely perek számos jogi aggályt is felvetettek, mint: sui generis, ex post facto, tu quoque. De a lerombolt Németországot újjá kellett építeni, ezért a megszállók „jóvoltából” keleten Moszkva létrehozta a Német Demokratikus Köztársaságot, míg a nyugati 12 tartományból álló területekből létrejött a Németországi Szövetségi Köztársaság, amelynek területén három nagyhatalom osztozkodott: USA- délen, Nagy-Britannia nyugaton, Franciaország- északon.

NSZK⁵: sorsa mondhatni jól alakult. A három megszálló nagyhatalom nem rendelkezett akkora mohósággal, mint keleti társa, a demokratikus, ám de ellenőrzött intézkedések

⁵ Németországi Szövetségi Köztársaság 1949-1990 között. [5]

nem juttatták arra a sorsra, amelyre az ország keleti része jutott. A Marshall-terv, Adenauer korszaka, mind olyan szerencsés történelmi pillanatok Nyugat- Németország történetében, amelyek a világgazdaság vérkeringésének is jót tettek, nem csak a német embereknek. Az ország keleti részének, melynek neve 1949-től NDK, sajnos nem volt ekkora szerencséje.

NDK⁶: 1945-ben a szovjetek megszállták az akkori Németország 1/3 részét, a másik 2/3 részén osztozott az USA, Nagy-Britannia és Franciaország. 1945-1949 közötti időszakban a kommunisták megerősítették befolyásukat a keleti területen úgy, hogy egyesült az SPD (Németország Szociáldemokrata Pártja) és a KPD (Németország Kommunista Pártja), amely pártokból megalakult az NSZEP (Német Szocialista Egységpárt) és ezen egyesített pártban már a kommunisták lettek a vezérek és az irányítók. Ez a párt szolgálta és garantálta az NDK teljes biztonságát. 1949 októberében alakul meg az NDK azon a területen, amelyet a szovjetek szálltak meg Németországból. Az ország 108 000 négyzetkilométernyi területén mintegy 17 millió lakos élt, köztük majdnem 4,5 millió a hazájából elűzött. Ez az ország lesz Szovjetunió legnyugatibb országa, teljes mértékben beavatkozott úgy a külügyeibe, mint a belügyeibe, s ha nem rendelkezett volna ezen országgal, akkor minden bizonnyal nehezen birkózott volna meg az általa megszállt országok válságaival (1956, 1968, 1980-1981). Az NDK bizonyult a leglojálisabb állammak a szocialista országok közül egészen 1989-ig, még akkor is, amikor a többi szocialista állam már régen távolodni kezdett a Moszkvai vezetés irányvonalaitól. Nyugodt szívvel állíthatjuk, hogy az NDK volt a leglojálisabb szocialista állam a szovjetek vezetéséhez, sőt olyannyira ragaszkodtak a fundamentális alapelvekhez, hogy amikor a Sztálin utáni korszakban a moszkvai vezetők némi reformtörekvéseket kezdenek el szorgalmazni, akkor Erich Honecker kétkedve figyelte ezen megnyilvánulásokat. Az NDK mintegy 40 éves történetét két személyiség határozta meg, s e személyiségek vezetése alatt több árnyalt határvonallal megrajzolható időszak is volt. 1950-től a meghatározó személyiség Walter Ulbricht⁷, aki a NSZEP első főtitkára lett. Ebben az évben alakul meg „Stasi”⁸, amelynek feladata a külföldi hírszerzés és kémelhárítás volt, de fontos feladata volt a „belső ellenség megfigyelése” is. Az ez utáni időszak elég mozgalmas volt az NDK történetében. Sztálin 1952-ben felajánlotta, hogy a két német állam egyesüljön, ezt azonban a másik 3 nagyhatalom elutasította, mert látták Sztálin szándékát, azaz tudták, hogy Sztálin ezáltal szeretne politikai befolyást szerezni az állam nyugati részében is. 1953-ban, miután Sztálin meghalt, némi reményt éreztek az NDK állampolgárai, de az 1953-as megszorítások ezt is aláásták. Az NDK városaiban az év folyamán felkelések törtek ki, a források szerint ekkor az NDK 272 városában voltak sztrájkok, amelyeket, csak a Vörös Hadsereg tudott megfékezni. Az életszínvonal romlott, a nyugati ország irányába való kivándorlás nem szűnt, hiszen ez folyamatos volt 1945-től és csak egyre fokozódott. Hruscsov⁹, Malenkov¹⁰ és Berija¹¹ harca Hruscsov győzelmét hozta, amely győzelem aztán a Hideg Háború egyik legemblematikusabb határvonalát szülte, 1961-ben megépült a Berliini fal, amely fennállt egészen 1989 októberéig. 1955-ben az NSZK csatlakozik a NATO-hoz, ugyanabban a hónapban aláírják a Varsói Szerződést, amelynek tagja lesz az NDK is.

⁶ Német Demokratikus Köztársaság 1949-1990 között. [5]

⁷ Walter Ernst Paul Ulbricht kommunista német politikus, az NDK államtanácsának elnöke 1950-1970 között. Érdekeségként, nagyon akart hasonlítani Leninre, kopaszodása adott volt, ezért neki csak a kecskeszakáll kialakítására volt szüksége.

⁸ Állambiztonsági Minisztérium az NDK-ban.

⁹ 1953-1964 között a Szovjetunió Kommunista Pártja első titkára.

¹⁰ Orosz politikus, Sztálin közeli munkatársa.

¹¹ 1938-1953 között a szovjet titkosszolgálat vezetője.

Így a két németállam két szemben álló katonai szövetségben néztek farkasszemet egymással. A hatvanas – hetvenes években némi enyhülést észlelünk Berlin körül, 1970-ben Walter Ulbricht egészségügyi okokra hivatkozva visszavonul a politikától, utódja Erich Honecker¹² lesz egészen 1989-ig. A Honecker korszak teljesen visszaterelte a Moszkvától távolodni vágyó kelet németeket, új irányvonalat hirdetett meg, újra megerősítette függését Moszkvától, amelynek az lett a következménye, hogy a német egyesítés újra fényévekre került az emberek előtt. Walter iparosítási törekvéseit sem érezte szükségesnek, inkább a szociális intézkedések mintaszerű megtervezését, a „német szociális embertípus” kinevelésének fontosságát hangsúlyozta, míg a nyugatiak a polgárosodás útján jártak. A Kelet- Német statisztikák szerint a szocialista német állam állampolgárai jó életszínvonalon élnek, jobban, mint Magyarországon, ami egyébként nem volt igaz. 1985-ben Moszkvában új vezető vette át Szovjetunió vezetését, mert hatalomra kerül Miháil Gorbacsov, akinek reformpolitikai törekvéseit az NDK politikusok nem fogadják örömmel, sőt el is szigetelődnek és határozottan ellenzik Szovjetunió reformjait. Az 1989-es év teljesen felforgatja Kelet-Közép-Európát. Ebben az évben a már addig is állandó jelleggel kiáramló NDK állampolgárok olyan rohammal kezdenek emigrálni hazájukból, hogy az év végére az 1961-ben felépített fal leomlik, Honecker megbukik, Moszkva elveszíti uralmát a közép-európai szocialista államok felett, s a németek egyesülése immár karnyújtásnyira kerül. 1989. november 10-én Willy Brandt kijelenti: „most összenő, ami összetartozik”. [5]

A MAGYAR MÁLTAI SZERETETSZOLGÁLAT ÉS AZ NDK MENEKÜLTEK GONDOZÁSA

A máltai ispotályos lovagrend a keresztes hadjáratok idején alakult meg a 11. században, akik a Keresztelő Szent Jánosról kapták elnevezésüket (Johanniták), akkor is azzal a szándékkal, hogy a szegények és beteg lovagok, illetve zarándokok gondozását lássák el. A rend már a 12. században megjelenik hazánkban is. A rend majdnem zavartalanul működött az országban a 16. század közepéig, az ország három részre szakadása után azonban felmorzsolódott. Jogilag a 19. század elején szűnt meg. 1925-ben állítottak fel Budapesten követségüket, majd 1928-ban megalakul a Magyarországi Máltai Lovagok Szövetsége. 1945 után működésük ellehetetlenül, emigrációba kényszerülnek, így majd csak 1996-ban helyezik újra székhelyüket a Budai várba, Fortuna u. 10. szám alá. Jelmondatuk: „*Tuitio fidei et obsequium pauperum*”, mely jelmondat a Magyar Máltai Szeretetszolgálaté is, azaz „*A hit védelme és a szegények szolgálata*”. A Szeretetszolgálat Lovagrendi felügyeletét a Magyar Máltai Lovagok Szövetségének ispotályosa látja el. [9]

Az 1989-es év a határnyitások éveként vonult be a történelem könyveibe. A fent tárgyalt DNK állampolgárok állandóan megfigyelt élete ebben az évben sem lazult, és a felülről irányító hazug politikai garnitúra, amely akkor 67 éves átlagkorral rendelkezett nem észlelte a változás szeleit. A Magyar Máltai Szeretetszolgálat akkor alakult meg, amikor Európának nagyon szüksége volt ilyen szerveződésre. Ugyanezt a sorsot járta be indulásakor az Osztrák Máltai Szeretetszolgálat is, amely az 1956-os magyar menekültek megsegítésére került a történelem színpadára.

A Magyar Máltai Szeretetszolgálatnak alapja visszanyúlik 1985-’86-’87-re, amikor Ugron Imre (Székely származású nemesi család leszármazottja) Máltai lovag és Csilla von

¹² 1971-1989 között a NSZEP központi bizottságának főtítkára.

Boeselager (Született: Fényes Csilla) elkezdtek karitatív tevékenységüket Magyarország irányába. Először még külön utakon, majd miután újra találkoztak¹³, karöltve elkezdtek gyűjteni az orvosi és a kórházi felszereléseket, hogy segítsenek az anyaországuknak. 1987-ben már elkezdik a szervezkedést. Csilla először a Katolikus Egyház támogatásában bízik, de a válasz, amit kapott elkeserítette. Az isteni gondoskodásnak köszönhetően egy Mária nevű nővér megsúgta, hogy kit keressen meg, mert az átszállított adományokat valakinek fogadnia kellett és a szétosztásban is kellett a segítség. A Zugligeti plébános a legjobb szervező az egyházban, állította a nővér, csak van egy kis baj vele, és pedig az, hogy nagyon foglalt, nem lehet soha elérni, állandóan rohan, szervez, intézkedik. [2] De Csilla ragaszkodott a találkozáshoz. A női makacs- erős akarat világmegváltó hatással bírt mindig is a történelem folyamán. A találkozásnak az lett az eredménye, hogy ma már csak rébuszokban tudunk beszélni a két történelmi személyiségről. Elindultak a szállítmányok, a karitatív tevékenység csírája, amely megváltoztatta a magyar társadalmat és ezen keresztül az Európai társadalmakra is nagy hatással bírt. Magyarországon ekkor még nem lehetett civil szervezetet bejegyeztetni, de Németországban igen, ezért történt az, hogy Csilla és Ugron Imre 1988-ban megalapították az Ungarischer Malteser Caritas-Dienst (UMCD)¹⁴, „ezt a szervezetet bilaterális szervezetnek tervezték, mert a másik fele Magyarországon lesz majd bejegyezve Magyar Máltai Szeretetszolgálat néven” – jelezte Csilla von Boeselager. Ennek a szervezetnek az elnöke Csilla asszony volt és majd csak 1998-ban szűnik meg, mert ekkor már nem volt rá szükség. Immár megvolt a kinti szervezet, amely háttérszervezetként irányította a magyarországi eseményeket, az adományok gyűjtését, szállítását, olyan hatékonysággal, hogy azt már a Német Máltai Szeretetszolgálat is irigyelte időnként. Az első kórház, amely részesült az jótékonyaságukból a Szent Ferenc Kórház volt, azután a Szent János Kórház és így tovább. A magyarországi események is egyre jobban alakultak, Csilla 1987-ben megismerkedett Dr. Szondy Máriával, aki így emlékezik vissza a történetekre:

„Csillával 1987-ben ismerkedtem meg, mikor először meglátogattam munkahelyemen. Azonnal szoros barátságot kötöttünk, ez haláláig megmaradt. Testvérével és leányaival a mai napig is tartjuk a kapcsolatot, kölcsönös szeretetben. Nagyon gyorsan kiderült, hogy eszmeiségünk, gondolkodásunk közös az elesettekre, segítségre szorulóakra vonatkozóan és azonnal keresni kezdtük a leghatékonyabb megoldást. Így kezdtük tervezni a legális formát. Hamarosan megismerkedtem jó barátjával, Ugron Imrével, ki jelenleg Máltai Nagykövet, a közös gondolkodás rendszeres találkozásokat jelentett. Mikor férjem a Legfelsőbb Bíróság akkori elnökhelyettese jelezte, hogy meg fog jelenni az alapítványokról szóló rendelkezés, azonnal léptünk, 30 taggal megalapítottuk a Magyar Máltai Szeretetszolgálatot. Csilla asszony felkérte elnöknek Kozma Imrét, kit korábbról ismert, és aki helyet biztosított a zugligeti plébánián az addig is érkező adományoknak. Ezek szétosztásában aktívan részt vettem, még hivatalos megalakulásunk előtt. Az MMSZ első alelnöke voltam lemondásomig...” (2020.01.14)

A magyar törvényhozás lehetővé tette, hogy civil szervezetet lehessen bejegyezni, így 1989. február 4-én már elsőként be is nyújtották a dokumentációt a bejegyzéshez.¹⁵ Mint azt Ugron Imre mesélte, már mindenki fel volt készülve, mert az idők szele az fűdőgáta, hogy itt hamarosan változások állnak majd be, s majd hivatalosan is lehet működtetni azt, ami már néhány éve Imre atya plébániáján történik. Február 10-én a szervezet be volt jegyezve, ami nagy örömmel adott okot, mert a szovjet blokkhoz tartozó országban ez addig elképzelhetetlen volt. Csilla tehát Imre atyát kérte fel elnöknek, mellette még négy alelnök

¹³ Csilla von Boeselager és Ugron Imre már a '60-as években ismerkedtek meg, New Yorkban.

¹⁴ Ugron Imre: Interjú, 2020.01.14

¹⁵ A törvény 1989. február 3-án lépett hatályba, a következő napon már be is adták a bejegyzési kérelmet.

lett bejegyezve, köztük Csilla asszony, Ugron Imre, Szondy Mária és Kállay Miklós. Most megvalósult a bilaterális szervezet létrejötte, létezett 1988-tól az UMCD és 1989 februárjától a Magyar Máltai Szeretetszolgálat, így hát folytatódhatott a munka.

A fiatalon megalakult szervezet az év folyamán komoly történelmi helyzet elé került. A romániai Ceausescu¹⁶ rendszer elől menekülő erdélyi magyarok is számíthattak a Szeretetszolgálatra, akkoriban politikai okok miatt majdnem 13 ezer magyar jött át Magyarországra, ez az NDK állampolgárainak is szemet szűrt. Feltették a kérdést magukban, hogy ha a szocialista Magyarország nem toloncolja vissza a szocialista Romániába a román állampolgársággal rendelkező magyarokat, akkor lehet, hogy őket sem adja majd ki az NDK-nak. Ez is egy mozgatórugója volt az elindulásuknak. Nem volt mellékes a magyar kormány azon döntése sem, amelyet az akkori miniszterelnök, Németh Miklós kormánya hozott meg, miszerint le kell bontani a nyugati határzárát. Döntésüket nagyban meghatározta a pénzhány is, hiszen ez a műszaki határzár már elavult, megrongálódott, tatarozásra lett volna szükség, de erre már nem volt pénz. Így úgy döntöttek, hogy május 2-án elkezdik annak lebontását. Az NSZK adásain csüngő NDK állampolgárok ezt is látták és ez reményre adott okot. Az itt nyaraló NDK állampolgárok mindenképp hamar értesültek, de megtudták ezt a Bulgáriában, Romániában nyaraló családok is. Ez év közepén a Budapesti NSZK nagykövetségét, majd konzulátusát olyan sokan meglepték, hogy ott már nem lehetett emberhez méltó körülményeket teremteni. A követség munkája megbénulni látszott, már lehetetlen volt az állapotokat fenntartani. Cselekedni kellett, így merült fel a konzulátus dolgozóiban, hogy hát létezik egy keresztény civil szervezet, ismerik a tevékenységüket, hiszen az akkori magyar kormány tagjai sem akadályozzák tevékenységükben, a szervezet vezetője, Kozma Imre atya mindenképp megtalálja a hangot. Csilla asszony a konzulátus egyik dolgozójánál lakott Budapesti itt tartózkodásának ideje alatt, esténként frusztráltak látták a konzulátus dolgozóját és megkérdezte tőle, hogy mi a baj. Augusztus 13-án Imre atyát is felkeresték a konzulátusról, hogy hivatalosan az NSZK humanitárius katasztrófa- helyzetet hirdetett, és felkéri, hogy vállalja el az itt tartózkodó emberekről való gondoskodást. Ugyanebben az időpontban Csilla asszonynak is feltették ugyanezt a kérdést a reptérről jövet. Atya és Csilla asszony is igent mondanak, függetlenül egymástól. A két „igen” este szembesült egymással. Augusztus 14-én reggel elkezdődtek a telefonhívások, az osztrák máltaiak voltak a legközelebb, ők gyors segítséget tudtak nyújtani, hiszen a szervezet fiatal volt, nem rendelkezett megfelelő infrastruktúrával. Imre atya az augusztusi Mária ünnepén tartott szentmise alatt kihirdette a történeteket. Mint mondotta, „helyzet van” és tenni kell a kötelességet. A máltai lelkeség megköveteli, hogy segítsenek a szükségben szenvedőknek, mert akkor azok az emberek kiszolgáltatott helyzetben voltak. Első nap már több százan megérkeztek, a konzulátus és a nagykövetségen lévő emberek beköltöztek a táborban. A hívek a kihirdetést követően példaértékűen nyilvánultak meg. Szükség volt sátrakra, takarókra, tábori ágyakra, ételre, tisztálkodási lehetőségekre. Este már állt a tábor azon a területen, ahol egykor az angolkisasszonyok nevelő és oktató intézete állt. Az intézet épületében ekkor az állami gyermekvédelem által működtetett gyermekotthon volt, de éppen még vakáción voltak a gyermekek, így az épület zárva volt, a tábor felépítésére a Szeretetszolgálat használta az udvart és a kertet. A nemzetközi médiavisszhangok miatt a Nyugatnémet Vöröskeresztnek feltűnt az a tény, hogy a Magyar Vöröskereszt miért nem kapcsolódik be az eseményekbe. És még

¹⁶ 1965-1989 között gyakorlatilag egyeduralgként vezeti Romániát

sokan mások is feltették a kérdést, hogy a Magyar Vöröskereszt miért nem lett felkérve erre a feladatra, már az elején?¹⁷ Azért, mert akkor a magyar Vöröskeresztnek a vezetője párttag volt, tehát kötődött a kommunista rendszerhez, így a Keletnémetek nem bízhattak a szervezetben, hiszen az államhatalom szerves részét képezte, így volt ez az NDK-ban is. Csak később kaptak utasítást a Genfi központjukból, hogy kapcsolódjanak be a menekültek megsegítésébe. Ezért volt az, hogy majd ők kapták meg a Csillebérci tábor munkaidőben történő feladatok ellátását, a munkaidőn kívül és a hétvégéket ott is a Máltaiak önkéntesei végezték. Rengetek önkéntes jelentkezett, de hamarosan megérkeztek a NSZK-ból a máltai dolgozók és velük együtt az önkéntesek is. A legaktívabbak a Padeborni máltaiak voltak, nyugatnémet máltai részről Wolfgang Wagner volt a vezető egyéniség, őt végig lehet látni az akkor készült felvételeken is. Az osztrák máltaiak is hamar válaszoltak a hívásra, Ugron Imre szólt nekik, mert ő jobban ismerte és jóban volt az Osztrák Máltai Szeretetszolgálattal. Ők akkor is sokkal kisebb szervezet voltak, mint a németek, ezért csak két mikrobusznyi segítő kéz indult útnak telepakolt utánfutókkal. Hoztak takarókat, ruhát, gyógyszereket, élelmet, de nem volt egyebük. Az ő történetükhöz hozzátartozik, hogy a megalakulásuk 1956-ban történt, amikor Európa ugyancsak egy nagyobb belső migrációval nézett szembe, történetesen a magyar '56-os menekültekkel. Így a magyar menekültek megsegítésének céljából jöttek létre, mert akkor mintegy 250 ezer magyar menekült el hazájából a retorziók elől. A Német Máltai Szervezet a második világháborút követő években jött létre, mert a kapitulált Németország demilitarizálása után a humanitárius és a katasztrófavédelmi tevékenységeket a máltaiak vették át. Ők komolyabb infrastruktúrával rendelkeztek, nekik Csilla asszony szólt, hogy jönni kell, és hogy kellene a katonai sátrak, a táborok felállításához. De a sátrak országon kívüli használatához kormányengedélyre volt szükség, de ezt is hamar elintézték. Egy hét múlva már állt a két Hárs-hegyi tábor is, ezt is a máltai önkéntesek tucatjai vezették, gondoskodtak az itt lakó NDK menekültekről. Amint egyre hűvösebb lett és az eddigi táborok is megteltek, megnyitották a Csillebérci tábor is, amelyet hivatalosan a Vöröskereszt kapott meg, de amint már említettem, itt is aktívan részt vett a Szeretetszolgálat. Zánkán is működött egy tábor, amely szeptember elsején vagy másodikán nyitotta meg kapuit a Balatonnál nyaraló NDK állampolgárainak. Ezt a kormány engedélyezte miután egyeztettek Kohl kancellárral, mert a határnyitásról még csak folytak az egyeztetések. A zugligeti plébánia hívei közül nagyon sokan a saját otthonaikba fogadtak be menekülteket, voltak, akik kiköltöztek a saját házukból és a kertjükben felállított sátorban laktak, hogy helyet biztosítsanak a menekülteknek. Olyanok is voltak, akik béreltek saját költségen szobákat, Imre atya visszaemlékezései szerint 154 család jelentkezett, aki több száz embert szállásoltak el. Az étellemezésről azt mesélte Imre atya, hogy telefonon hívta a szállodákat, munkásszállókat, kifőzdéket, mindenki hozta a főtt ételt, senki nem kérdezte, hogy majd ki fog fizetni, mert tudták, hogy ezért nem kapnak pénzt. Mint mesélte, nem voltak olyan kérdések, hogy kinek, miért, hogy érdemes-e, csak tették a dolgukat. A táborral szemben lakó házak tulajdonosai is gyakran jelentkeztek, hogy szívesen várják fürdeni, mosakodni. A tábor szaniter berendezésének megszerzése volt a legnehezebb, ezt végül is az NSZK-ból szereztek be konténer formájában. Eufórikus volt a hangulat, volt olyan család, ahol állítólag 78-an laktak, az önkéntesek annyian jelentkeztek, hogy volt, akit haza kellett küldeni, mert nem volt szükség

¹⁷ Ugron Imre: Interjú, 2020.01.14

annyi emberre. Egyik akkori fiatalot megkérdezve így emlékezett vissza az akkori eseményekre:

Mikor találkoztál először a Magyar Máltai Szeretetszolgálat Egyesülettel és a Lovagrenddel?

1989 februárjában, mikor megalakult az Egyesület, rögtön beléptem, 54-es a kártyaszámom. Először Németországból jöttek Máltaiak elsősegély-tanfolyamot tartani, már ott is én fordítottam. A Csilla von Boeselager által gyűjtött adományokat szállító kamionokat sokszor a mi hittan csoportunk tagjai pakolták ki a Zugligeti templom pincéjébe, hogy aztán onnan tovább szállítsák a rászorulóknak. A Lovagrend első hazajövő tagjaival is Zugligetben találkoztam, Ugron Imre volt az első.

Mikor csatlakoztál az NDK- menekültek számára létrehozott táborhoz?

Kozma Imre atya augusztusban, egy esti misén felkérte a híveket, hogy aki tud segítsen. Mivel én már akkor jól beszéltem németül, rögtön jelentkeztem.

A tábor egész nyitva tartása alatt jelen voltál?

Lényegében igen. Először Zugligetben, aztán mikor azt a tábort bezártuk, akkor Csillebércen segítettem a novemberi táborzárásig. Abban a félévben csak a legszükségesebb gyakorlatokra jártam be a Főiskolára, a napok nagy részét, néha késő estéig ott voltam. Sokféle feladat volt, hol az Info -sátorban voltam, hol az étkeztetésben segítettem, ha valaki beteg volt orvoshoz vittem, ha kellett bevásárolni mentem.

„Ostályidegen” család gyermekeként nem féltél?

Igazából nem volt időnk félni, annyi volt a teendő. Néha belegondoltunk, mikor láttuk, hogy fényképez a Stasi, hogy mekkora akták lehetnek rólunk? Igazából mi csak a lelket öntöttük az emberekbe, hogy majd megoldódik a helyzetük, magunkkal nem törődünk. Ez szeptember 11-ig tartott, amikor a magyarok kinyitották a határt a kelet-németek előtt.

Milyen hatással volt rád a Máltai lelkiség? A Táborban végzett tevékenységed ideje alatt ez meghatározó volt?

Igazából Csilla von Boeselager és Imre atya segítőkészsége, mindenki iránt kimutatott szeretete, valamint a nyugat-német és az osztrák máltaiak profi önkéntes hozzáállása rám is nagy hatással volt. Mikor megtudtam, hogy Csilla asszony maga is beteg, és mégis minden erejét a menekültek megsegítésére fordítja, attól a pillanattól kezdve még inkább csodáltam.

Meséltek-e a menekültek arról, hogy mit élnek át?

Kevesen voltak beszélgetések, mivel a Kelet-Német államban mindenki a besúgóktól félt. Egy történetet soha nem fogok elfelejteni. Egy délután megérkezett egy fiatal fiú nagyon zaklatott állapotban. Elmondta, hogy a barát-nőjével a Dunán átúszva akartak Magyarországra menekülni, de csak ő ért partot. Azt beszéltek meg, hogy ha elveszítenek egymást, akkor Zugligetben találkoznak. Erre próbáltuk nyugtatni, hogy lehet, hogy a Duna nagy sodrása miatt máshol ért partot a barát-nője. Mondta, hogy akkor marad. Rendszeresen jött az Információs sátorhoz érdeklődni a lány iránt, mi mindig biztattuk, hogy legyen türelemmel! Végül 2 nap után megjött a szerelme. Azt a boldogságot nehéz leírni, ami akkor rajtuk látszott!

Bizalommal voltak-e a Kelet németek a magyarokkal szemben?

Nem igazán, csak ha valamit kértek, akkor jöttek hozzánk.

Hogy érzed, már máltai lelkiséggel vállaltad a kockázatot? Jó volt segíteni? Ma újra megtennéd?

A máltai lelkiség a „levegőben volt”. Az a néhány hónap volt életemnek egyik legizgalmasabb időszaka. Nagyon jó érzés volt segíteni a kelet-németeknek, akik tudtuk, hogy nálunk sokkal rosszabb körülmények közül jöttek. Sokan a családtagok biztattak. Olyan is volt, aki miután lezárták a cseh határt, Kelet-Berlinből Budapestre repült, mert azt lehetett. Innen aztán a máltai busszal ment Passauba, a menekülttáborba, hogy onnan aztán eljuthasson Nyugat-Berlinbe, ahol a testvére várta. Csak néhány ezer kilométerrel kellett többet megtenni ahhoz, hogy átjusson Berlin keleti részéből a nyugatiba, ami a fal megépítése előtt egyszerű volt. Biztos, hogy ma is megtenném, bár lehet, hogy nem tudnék annyi időt a táborban tölteni.

Szerinted mennyire volt fontos a Szeretetszolgálat szerepe a kor eseményeiben? Mekkora szerepet töltött be?

Szerintem nagyon fontos volt a Szeretetszolgálat szerepe és főleg Csilla von Boeselager asszony éleseszűsége, jó szervezőkészsége, nagy szíve. Mikor a nyugat-német Nagykövetségről megkeresték, hogy segítsen a sok embernek valamilyen szállást, ellátást találni, akkor ő a „politikai helyzetet” egy „humán problémának” állította be. Mivel Magyarország is aláírta addigra a genfi egyezményt, így a menekülteknek kötelessége volt segíteni. Csilla asszony nagyon jó diplomata volt, mindenkiel megtalálta a hangot, politikusokkal, menekültekkel, segítőkkel. A máltai kereszt alatt még a kelet-németek is biztonságban érezték magukat. Mi csak részinformációkat

hallottunk, ill. láttuk, hogy magyar és külföldi politikusok is megjelennek a táborban, ill. az Imre atya garázsában berendezett nyugat-német konzuli irodában. Azóta több könyvet olvastam erről az időszakról, melyről egyre több információ kerül elő az évek múlásával.

Tartod-e a kapcsolatot az akkori menekültek közül valakivel?

Igazából csak egy lánnyal, aki az egyik nyugat-német máltai barátom, aki kétszer 1 hónapot volt itt segíteni - felesége lett.

(Czirják Mariann, 2020.01.14, ma már Máltai dáma.)

Ugron Imre máltai lovagtól az egyik keletnémet gyanakodva megkérdezte¹⁸:

„Miért segít nekünk? Ki fizet magának ezért?”

...Senki nem fizet ezért nekünk – magyarázta Ugron. Máltai lovagok vagyunk. Az a dolgunk, hogy segítsünk.

Most már értem – válaszolta. – De kik azok a máltai lovagok?”

Nem mások, mint „állampolgárai” a világ legkisebb államának, amelynek hivatalos neve: Jeruzsálemi, Rodoszi és Máltai Keresztelő Szent János Lovagrendje.”

A táborokban dolgozók egyöntetűen mesélték, hogy a menekültek rettentően féltek, nem mertek senkivel beszélgetni, kerültek minden idegen embert. Voltak, akik befogadó családok otthonaiból visszatértek a táborokba, mert ott nagyobb biztonságban érezték magukat. Imre atya többüktől is megkérdezte, hogy miért jöttek el, nem érezték jól magukat a családoknál? Azt válaszolták, hogy igen, jól érezték magukat, csak itt a táborban nagyobb biztonságban érzik magukat. Nem tudhatták, hogy a Stasi emberei közül hányan vannak köztük, ezért kis csoportokba igyekeztek maradni és minimalizálták a kapcsolatteremtést, amennyire csak tudták kerültek azokat, akiket nem ismertek. A Stasi megfigyeléséről tudtak, azt is tudták, hogy a táborral szembeni egyik házat bérelték, annak a tetejéről figyeltek mindenkit, fényképeztek, feljegyzéseket készítettek. Esténként a tábor önkéntesei egy nagy reflektort irányítottak a tetőre, hogy ne tudjanak fényképezni. A Zugligeti táborban naponta minimum 600 személy lakott. Már az első napokban folyamatosan tele volt zsúfoltságig, mert a német külképviseleteken kitáblázták, hogy hová kell menniük. A menekültek bizalmát talán a szervezet egyházi mivolta is segítette, Imre atya reverendában jelent meg köztük nagyon gyakran, ez bennük bizalmat keltett, mert az a hír járta a táborokban, hogy a magyarok azért gyűjtik össze őket, hogy aztán átadják őket az NDK-nak. Ezeket az álhíreket Imre atya próbálta eloszlatni és bizonygatni, hogy szó sincs ilyesmiről. A Zugligeti táborban folyamatos őrzést szerveztek meg az önkéntes magyar és német segítők bevonásával. Ide nem járkálhattak be idegenek, mert a kapuban megállították őket, így a sajtó is csak engedéllyel léphetett be a tábor területére. A táboron belül komoly térkép-rajzolósi műhelymunka zajlott, a keletnémetek megkapták a megfelelő tájékoztatást, hogy hol és mikor érdemes próbálkozni a határon való átszökésekkel. „A táborban nem hivatalosan meg lett nekik mutatva, hogy hol kell átmenni, térképeket rajzoltak és osztogatták.” Dr. Szondy Mária és férje, aki egyébként a legfelsőbb bíróságon dolgozott, tettek egy „próbautat”, ami abból állt, hogy átsétáltak a határon, majd visszajöttek. Mint utólag kiderült, azért odaszólt valaki a határőrségnek, hogy még véletlenül se lőjenek, de így tettek akkor is, amikor átszökni próbáló NDK- és állampolgárokat észleltek.

„És közben továbbra is ezrek özönlöttek bújva, settenkedve, mászva stb., és sokan útlevelemmel is, Romániából és az NDK-ból Magyarországra és mentek neki az osztrák határnak, ahol a határőröknek tiltva volt a fegyverhasználat, nem volt már nyomsvá, sem elektromos jelzőrendszer. Valójában szinte eszköz nélküli határőrzés folyt,

¹⁸ Az interjú megjelent: Charles Parmiter, Szemenyei Gizella: A Szeretet Önkéntesei, Reader's Digest 1992, II. évfolyam

mert akkor még nem voltak drónok, hőkamerák, éjjel látó műszerek stb. Augusztusra már tele volt a határ, az erdő, Brennbergbánya, a Fertő mente elhagyott trabantokkal, wartburgokkal, skodákkal, ladákkal. Az egész migrációs sokadalomból a Páneurópai piknik lett nevezetes történelmi esemény, de emellett is ezek mentek át a határon. Akiknek kellett, segítettünk. Anikó szervezte a máltai segítséget, az egyetemisták fölöttünk a bükkösben és a fenyvesekben a határ felé mutató táblácskákat szereltek a fákra „Richtung Österreich” nyílal és feliratokkal. Egy NDK-s botanikus barátomat kísértem Ilona akna (Helenenschacht in Österreich) felé, s mielőtt átment a határon, megölelt, megköszönte a segítséget és azt mondta (ezt szándékosan magyarra fordítva írom): „Te Laci! Nálatok már szétmállott a kommunizmus, mint a kutyaszar az esőben.” Így volt. És a határőr tiszt barátaim? Nekik nehéz volt. Egy történet jut most eszembe, ami szépen illusztrálja az ő életüket: esős volt a nyár, sok vargánya termett. Őrsparancsnok barátommal gombásztunk. Ahogy megyünk a Jóremény (régi bánya) felé, zörgést hallunk a bokorból. Előtűnik egy természetes úr, négykézláb. Barátom szól, „mond meg neki, ne hülyéskedjen itt négykézláb. Még kb 200 m a határ, mutasd meg az utat!” Megmondtam. Megmutattam az utat. Szegény ember azt sem tudta, hol van (egy tanár volt Thüringiából), hitte is, nem is, de elindult... S megyünk tovább. Gyereksírás! Egy 5-6 éves forma fiúcska bömböl, „Mutti! Mutti!” Barátom, a határőr százados, őrsparancsnok nyakába kapja a gyereket. „Igyekezzünk! Még tán utolérjük az apját!” Utolértük. (Még most sem volt „blama”, a járőr másutt volt.) A „Mutti” már átért az osztrák oldalra, a magyar-osztrák „közös használatú úton” állt, a papa velünk. Gyerekátadás. Örömkönnye. Ekkor éreztük, hogy „Igen!.. Összeomlott a vasfüggöny!”[14]

Ennek volt köszönhető a táborvezetők által állított 20% fluktuáció, ami azt jelentette, hogy csak a Zugligeti táborból naponta 100 feletti személy próbált átjutni a határon. Azt már nem tudjuk pontosan, hogy hánynak sikerült is. A tábor önkéntesei közül is nagyon sokan saját autójukkal fuvaroztatták a menekülteket a határra, aminek az lett az eredménye, hogy felütötte a fejét az embercsempészet csírája, mert előkerültek haszonleső személyek is, akik nem tartoztak a máltai önkéntesek közé, hogy pénzért szállítsák a menekülteket.

Augusztus 19-re a Magyar Demokrata Fórum debreceni és soproni helyi szervezetei meghirdették a Páneurópai Pikniket, amelynek védnökségét Habsburg Ottó és Pozsgay Imre vállalta, engedélyt kérték a Belügyminisztériumtól, amely misztérium meg is adta az engedélyt. A táborokon belül erre az alkalomra nagyon felkészítették a menekülteket, elmondták nekik, hogy ezen a napon egy rövid időszakra¹⁹(3 órára) nyitva lesz a határ, így esély nyílik arra, hogy átmenjenek, anélkül, hogy bármi baj történne. Ennek eszméje a határok nélküli Európa volt, melynek megszervezéséhez hozzájárultak az osztrákok is. Ennek a napnak az eseményeit sokféle képen értelmezték, voltak, akik azt állították, hogy mintegy 1500-an mentek át a keletnémetek úgy, hogy megrohmozva meglepték a határőröket, volt, aki csak 1000 átjutóról írt, de olyan tudósítás is volt, aki csak 400-600 személyről emleget.

A lezajlott események után a három ország (NSZK, NDK, Magyarország) kormánya folyamatos egyeztetés alatt állt, sőt Kohl kancellár Gorbacsovval is folyamatosan egyeztetett. Az NDK kormánya már kezdte komolyan venni a helyzetet, mert látta, hogy olyan sokan elindultak és „már nem tudták a szőnyeg alá söpörni” – mesélte Ugron Imre. Csak a csillebérci táborban volt nap, amikor körül- belül 7000-en laktak, ennek is azonban 20%-a naponta cserélődött.

A zugligeti templom tornyai sokaknak nagyobb biztonságot jelentett, mert mint mesélték, a tábor lakóinak „nem csak ételt – italt, de bátorítást és megértést is nyújtottak”. Miután a Zugligeti tábor nagyon sokan nem merték elhagyni, Dr. Alexander Arno NSZK nagykövete azzal a kéréssel fordult Kozma Imre atyához, hogy engedélyezze a nagykövetség kiköltözését a táborba. Kozma atya nem adott azonnali választ, gondolkodnia kellett,

¹⁹ Hegyi Margit – önkéntesként vett részt a menekültek fuvarozásában a határra, segített a táborokban és saját költségén bérelt IBUSZ szobákat a menekülteknek.

mert mint fogalmazott, „mert én karitatív szempontból gondolkodtam, ez már politika volt...”, ennek ellenére megengedte, így lett a Zugligeti templom udvara az akkori politikai események színtere. Imre atya rendszeresen egyeztetett a magyar kormánnyal is, Németh Miklós sűrűn megfordult a Zugligeti táborban, de nem csak ő. Járt itt Hans-Dietrich Genscher az akkori NSZK külügyminisztere, megfordult maga Kohl kancellár is, és a magyar kormány tagjai közül is néhányan. Sőt még NDK és NSZK diplomata-találkozó helyé is válhatott néhány pillanatra. Az NDK diplomatái megkérdezték atyától, hogy miért szereti jobban a nyugatnémeteket, Imre atya azt válaszolta, hogy ez nem így van, éppen ellenkezőleg a keletnémeteket szereti jobban, de ők ezt akkor még nem értették. Természetesen, miközben a táborokban zajlott az élet, egyesek elhagyták, mások beköltöztek, a tábort elhagyók a remények szerint átszöktek a határon, addig a politikai háttér munka is zajlott. Németh Miklós felkereste Kohl kancellárt Nyugat - Németországban, hogy közölje kormányának csodálatos döntését, miszerint kinyitják a határokat és engedik, hogy a Kelet- Német állampolgárok nyugat felé menjenek. A határnyitás napját szeptember 10-én jelentették be, 11-én már érvénybe lépett. A táborban fordító Csilla von Boeselager előtti tömeg örömjongásban tört ki, volt, aki sírt örömeiben, de volt, aki pezsgőt nyitott. A zugligeti tábor még tovább nyitva maradt, egészen november 14-ig. Imre atya elmondása alapján a Magyar Máltai Szeretetszolgálat táboraiban 48.600 Kelet- Német állampolgárról gondoskodtak.

A frissen magalakult Magyar Máltai Szeretetszolgálat már első évében akkora történelmi feladatok elé kerül, amit megalakulásukkor álmodni sem mertek. A feladatok nagyok voltak, s bár ekkor a szervezet még kicsinek látszott, de bátran állíthatjuk, hogy e nagy feladatok indították el a növekedés útján, hogy azzá váljon, amit jelent a magyar társadalom és az egész világ előtt ma. A betegeskedő Honecker sem gondolta volna, hogy a magyar társadalom, annak kormánya és ezen keresztül az ország egyik legfiatalabb, de keresztény szervezete, léket üt majd az NDK elsüllyeszthetetlennek látszó szocialista hajóján. Ha ebben a történelmi pillanatban Kozma Imre és Csilla von Boeselager az NDK-ba utazott volna, valószínűleg letartóztatják, de a magyar kormány sem lopta be magát a szívükbe, mert a Genfi egyezményhez való csatlakozásával gyakorlatilag kihátráltak a kétoldalú egyezmények alól. Ez lehetővé tette, hogy a Kelet- Német állampolgárok is menedéjjel tartózkodjanak hazánkban, csakúgy, mint az erdélyi magyarok. A november elején lecsengő NDK menekült hullám után nagyon gyorsan egy másik, szintén humanitárius próba elé állítja a Szeretetszolgálat fáradhatatlan tagjait és önkénteseit, ugyanis november 17-én kitör a romániai forradalom. S miután ez is lecsengett volna, hát kiobbant a délvidéki háború, amely szintén nagy menekülő hullámot indított el. Ekkor sem tétlenkedett a Szeretetszolgálat, miközben már országos szinten felvette a harcot a magyar lakosság perifériájára sodródott emberek sorsának jobbá tételéért. Amikor Ugron Imrét megkérdeztem, hogy a Szeretetszolgálat és a lovagrend teljesítette „kötelességét” ebben a történelmi pillanatban, azt válaszolta, hogy „a válaszom igen, kérdőjel nélkül...”, és a nemzetközi visszhangja is akkora volt, hogy ma is visszacseng az emberek fülében.

FELHASZNÁLT FORRÁSOK

Irodalom

- [1] Davies, Norman: Európa Története, Budapest, Osiris 2002
- [2] Dobos Marianne: A Szeretet Önkéntesei, Budapest, Fórum Rt. Kiadó 1990

- [3] Európa Története, Szerk: Gunszt Péter, Debrecen, Csokonai Kft. Kiadó 1996,
- [4] Egzisztencializmus, Szerk: Köpeczi Béla, Budapest, Gondolat 1966
- [5] Németh István: Németország Története, Budapest, Aula Kiadó 2004,
- [6] Németh István szerkesztésében: 20. század egyetemes történet, I. Európa, Budapest, Osiris Kiadó 2006
- [7] Ránki György: A Második Világháború Története, Budapest, Gondolat Kiadó 1982
- [8] Romsics Ignác: Magyarország Története a XX. században, Budapest, Osiris Kiadó 2005
- [9] Török József - Legeza László: Máltaiak, In: Szerzetesrendek a Kárpát-medencében, Bp., Mikes Kiadó 2009
- [10] Smith, Joseph: A hidegháború 1945-1965, Bp. 1992, IKVA
- [11] Masát Ádám: A menekültkérdés szerepe az NDK rendszerváltásának folyamatában, Diplomáciatörténeti adalékok a berlini fal leomlásához, Kültügyi Szemle 2014
- [12] Nemessányiné Csepreghy Éva: A Zugligeti Szent Család plébánia - tanulmány
- [13] Jeszenkovits Teréz: Az Angolkisasszonyok Zugligeti Intézete – Hegyvidékünk gyöngyszemei, 2001
- [14] Vasfüggöny: Emlékirat, Dr. Kárpáti László - Dr. Kárpátné Ugron Anikó (2020.01.)

Online irodalom

- [15] https://index.hu/belfold/tegnapiujsg/2008/09/10/1989_kiengedjuk_a_keletnemeteket_ausztriaiaba (Letöltve 2019.12.18)
- [16] http://www.archivnet.hu/menekultkerdes_migracio_magyarorszagon_a_20_szazadban/5._az_1989._szeptemberi_h (Letöltve 2019.12.19.)
- [17] <https://444.hu/2015/09/27/ugyanugy-fogadtuk-az-ndk-s-menekulteket-mint-a-mostaniakat> (Letöltve 2020.01.12)
- [18] https://multkor.hu/20140814_keletnemet_menekultek_a_maltai_szeretetszolgalat_taboraban?pIdx=2 (Letöltve 2020.01.12)
- [19] <https://mult-kor.hu/a-nap-amikor-magyarország-kiuttte-az-első-teglát-a-berlini-falból-20180911> (Letöltve 2019.12.20)
- [20] <https://pestisracok.hu/horn-gyula-1989-ben-kategorikusan-az-ellen-vagyunk-hogy-magyarország-me> (Letöltve 2020.01.18)
- [21] <https://www.vaol.hu/hirek/1989-szeptember-megnyilik-a-hatar-az-ndk-menekultek-elott-agyagba-don> (Letöltve 2019.12.18)
- [22] https://hvg.hu/itthon/20190901_HVG_1989_Otthonrol_haza (Letöltve 2019.11.30)
- [23] https://hu.wikipedia.org/wiki/N%C3%A9met_Demokratikus_K%C3%B6zt%C3%A1rsas%C3%A1g (Letöltve 2020.01.11)
- [24] https://hu.wikipedia.org/wiki/P%C3%A1neur%C3%B3pai_piknik (Letöltve 2019.12.18)
- [25] <https://www.arcanum.hu/hu/online-kiadvanyok/TenyekKonyve-tenyek-konyve-1/1990-7B2E/az-ev-198889-7> (Letöltve 2020.01.19)
- [26] <https://www.magyarhirlap.hu/30-eve-szabadon/20190819-a-vasfuggony-lebontasa> (Letöltve 2020.01.12)
- [27] <http://befogadasnapja.maltai.hu/> (Letöltve 2019.12.11)
- [28] <https://maltai.hu/cikk/hir/1516> (Letöltve 2020.01.10)

- [29] <https://magyarmuzeumok.hu/cikk/befogadas-napja-89> (Letöltve 2019.12.17)
- [30] https://multkor.hu/20140814_keletnemzet_menekultek_a_maltai_szeretetszolgalat_taboraban?pIdx=2 (Letöltve 2019.12.21)
- [31] <https://1989.osaarchivum.org/node/9044> (Letöltve 2019.12.21)
- [32] <https://www.magyarKurir.hu/hirek/a-befogadas-napjato-1-maig-maltai-szeretetszolgalat-kerekasztal-besze> (Letöltve 2020.01.14)
- [33] https://mandiner.hu/cikk/20190817_kozma_imre_atya_uj_remenyt_kaptak_nalunk_a_keletnemete (Letöltve 2020.01.14)

**SPECIAL RULES ON PERSONAL
IDENTIFICATION IN PRISON****A SZEMÉLYAZONOSÍTÁSRA
VONATKOZÓ SPECIÁLIS SZABÁLYOK
A BÜNTETÉS-VÉGREHAJTÁSBAN**KONDÁS Katalin¹, SZÚCS Endre²**Abstract**

Today's most advanced authentication methods are biometric identification capabilities. Biometric identification is becoming more and more widespread, but its large-scale application is yet to come. The main reason for this may be the lack of appropriate systems and costly technical implementation. It would also be advisable to develop a biometric system for more reliable authentication in the field of criminal enforcement. Identifying people getting into the penitentiary institute requires significant attention. It could happen that not the right person appear when going to the institution. The aim of the publication is to give a comprehensive overview about prisoner identification, laws and their application in practice. The personnel must check the identity of the convict by checking personal data can be found in the personal documents and in the criminal registration system. Currently according to the Hungarian laws, the biometric identification in the penitentiary institutes is applied during the affiliation.

Keywords

information security, social engineering, manipulation biometrics, identification, security

Absztrakt

A mai legkorszerűbb hitelesítési módszerek a biometrikus azonosítással bíró lehetőségek. A biometrikus azonosítás egyre jobban terjed, azonban nagyfokú alkalmazása még várat magára. Ennek legfőbb oka lehet a megfelelő rendszerek hiánya, illetve a költséges technikai megvalósítás. Célszerű lenne a büntetés-végrehajtás területén is a megbízhatóbb hitelesítés érdekében a biometrikus rendszer kiépítése. A büntetés-végrehajtási intézetbe bekerült személyek azonosítása jelentős figyelmet igényel. Előfordul, hogy nem a megfelelő személy jelenik meg az intézetbe vonuláskor. A publikáció célja átfogó képet adni a fogvatartotti személyazonosításról, a jogszabályokról és gyakorlati alkalmazásukról. A személyi állomány köteles az elítélt személyazonosságát, a bünyügyi nyilvántartási rendszer adatait, illetve az iratokban szereplő adatokat is ellenőrzi. A magyar törvények szerint a biometrikus azonosítást a büntetés-végrehajtási intézetekben jelenleg a befogadás során alkalmazzák.

Kulcsszavak

biometria, azonosítás, biztonság

¹ kondaskatalin@gmail.com | ORCID: 000-0002-3775-4653 | PhD student / doktorandusz | Óbuda University Doctoral School of Safety and Security Sciences / Óbudai Egyetem Biztonságtudományi Doktori Iskola

² szucs.endre@bgk.uni-obuda.hu | ORCID: 0000-0003-2818-262x | senior lecturer / egyetemi adjunktus | Óbuda University Donát Bánki Faculty of Mechanical and Safety Engineering / Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar

BEVEZETÉS

A személyes adatok nagy egész halmazán belül a különleges (vagy más szóval szenzitív, érzékeny) adatok egy részhalmaza. Azok a személyes adatok tartoznak ide, amelyek kezelésére irányadó AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (EGT-vonatkozású szöveg) (a továbbiakban: GDPR) 51. preambulumban bekezdése:

„Az alapvető jogok és szabadságok szempontjából a természetüknél fogva különösen érzékeny személyes adatok egyedi védelmet igényelnek, mivel az alapvető jogokra és szabadságokra nézve a kezelésük körülményei jelentős kockázatot hordozhatnak.”

A GDPR 35. preambulumban bekezdése tartalma szerint is: „Az egészségügyi személyes adatok közé tartoznak az érintett állapotára vonatkozó olyan adatok, amelyek információt hordoznak az érintett múltbeli, jelenlegi vagy jövőbeli testi vagy pszichikai egészségi állapotáról. Ide tartoznak az alábbiak: a természetes személyek vonatkozó olyan személyes adatok, amelyeket egészségügyi szolgáltatások céljából történő nyilvántartásba vétel, vagy ilyen szolgáltatások nyújtása során gyűjtöttek, a természetes személy egészségügyi célokból történő egyéni azonosítása érdekében hozzá rendelt szám, jel vagy adat, valamely testrész vagy a testet alkotó anyag – beleértve a genetikai adatokat és a biológiai mintákat is – teszteléséből vagy vizsgálatából származó információk, és bármilyen, pl. az érintett betegségével, fogyatékosságával, betegségkockázatával, kórtörténetével, klinikai kezelésével vagy fiziológiai vagy orvosbiológiai állapotával kapcsolatos információ, függetlenül annak forrásától, amely lehet pl. orvos vagy egyéb egészségügyi dolgozó, kórház, orvostechnikai eszköz vagy in vitro diagnosztikai teszt.” [1]

A 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (a továbbiakban: Infotv.) a „különleges adat” fogalma a 3.§ 3. pont szerint: „a személyes adatok különleges kategóriába tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyéni azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok”. [2]

Fentieket figyelembe véve a Büntetés-végrehajtási Szervezetben, a fogvatartottak biometrikus adatainak kezelését és fontosságának jogszabályi háttérét foglaljuk össze annak érdekében, hogy átfogó képet adjunk ezen adatok jelentőségéről a mai magyar büntetés-végrehajtási intézetekben.

JOGSZABÁLYI HÁTTÉR A RENDÉSZETBEN

A 2009. évi XLVII. törvény a bünyügyi nyilvántartási rendszerről, az Európai Unió tagállamainak bíróságai által magyar állampolgárokkal szemben hozott ítéletek nyilvántartásáról, valamint a bünyügyi és rendészeti biometrikus adatok nyilvántartásáról (a továbbiakban: Bnyt.) jogszabályban foglaltak szerint, a bünyügyi és rendészeti biometrikus adatok nyilvántartása daktiloszkópiai nyilvántartásból és DNS-profil-nyilvántartásból áll. A daktiloszkópiai nyilvántartás tartalmazza az ujj- és tenyérynymtöredéket, valamint az ujj- és tenyérynymot. A DNS-profil-nyilvántartása dezoxiribonukleinsav-molekula meghatározott

szakaszainak vizsgálata alapján képzett alfanumerikus adatsort rögzíti. A szájnyalakhártya-törlet – a szájúreg belső felületéről, annak sérelme nélkül, steril gézzel vagy más, az egészségügyben használatos hordozóval letörölt anyag – segítségével is azonosítani lehet egy-egy személyt. [3]

A 20/2009. (VI. 19.) IRM rendelet a büntügyi nyilvántartási rendszer egyes nyilvántartásai részére történő adatközlés szabályairól meghatározza, hogy milyen formanyomtatványok kitöltésével és a büntügyi nyilvántartó szerv részére történő megküldésével kell teljesíteni az előírt adatközlést. [4]

A büntügyi nyilvántartó szerv által teljesített adatszolgáltatás, valamint a hatósági erkölcsi bizonyítvány kiállítása iránti eljárás rendjét az 53/2012. (XII. 22.) KIM rendelet a büntügyi nyilvántartó szerv által teljesített adatszolgáltatás, valamint a hatósági erkölcsi bizonyítvány kiállítása iránti eljárás rendjéről és a hatósági erkölcsi bizonyítvány kiállítása iránti eljárásért fizetendő igazgatási szolgáltatási díjról tartalmazza. [5]

A 2013. évi CCXL. törvény a büntetések, az intézkedések, egyes kényszerintézkedések és a szabálysértési elzárás végrehajtásáról (a továbbiakban: Bv. tv.) tartalmazza az elítélt személyazonosságának megállapítását. A Büntetés-végrehajtási Szervezet büntetés-végrehajtási (a továbbiakban: bv.) intézete köteles az elítélt személyazonosságát ellenőrizni, melynek során a befogadás alapjául szolgáló iratokban szereplő adatok szerint átveszi az elítéltnél a büntügyi nyilvántartási rendszer személyazonosító adatok és fényképek nyilvántartásában kezelt adatait, és ellenőrzi az iratokban szereplő adatokat. A bv. intézet az elítélt azonosítása érdekében rögzíti az elítélt ujjnyomatát és kezdeményezi a szakértői nyilvántartó szervnél a Bnytv. 82. § (5) bekezdés b) pontja szerinti összehasonlítást. Az összehasonlítást elektronikus úton, az erre a célra szolgáló elektronikus berendezés révén történő beolvasással kell elvégezni.

A bv. intézet az elítéltről képfelvételt készíthet, amelyet jogosult az arcképelemző tevékenység igénybevétele céljából az arcképprofil nyilvántartás részére megküldeni, ezzel is megállapítva a személy azonosságát.

További lehetőség van az elítélt azonosítására, mely szerint a bv. intézet az elítélt személy-azonosság igazolására alkalmas hatósági igazolványában vagy tartózkodásra jogosító okmányában, vagy a befogadás alapjául szolgáló iratokban szereplő adatok alapján elektronikus úton, adatot igényel a személyi adat- és lakcímnnyilvántartásból, a közúti közlekedési nyilvántartás engedély-nyilvántartásából, az útiokmány-nyilvántartásból vagy az idegen-rendészeti nyilvántartásokból. [6]

A befogadás során tehát a bv. intézet köteles ellenőrizni, hogy a végrehajtásra elővezetett, illetve előállított személy azonos-e az elítélttel. Az elítélt személyazonosságának megállapítása elsősorban a fogvatartás alapjául szolgáló iratok adatainak és az elítélt személyazonosságát igazoló hatósági igazolványban foglalt adatoknak az egybevetését, valamint az elítélt képmásának az összehasonlítását jelenti. [7].

A FOGVATARTOTTAK ADATAINAK NYILVÁNTARTÁSA

A jogerős ítélet kiszabását követően a Büntetés-végrehajtási Szervezet határozza meg, hogy az elítéltnél mikor, és melyik intézetben kell jelentkezni a büntetés letöltésére. A fogvatartottnak ellenőrizni szükséges a személyazonosságát.

Amikor a fogvatartott a büntetés-végrehajtási intézetbe kerül, adatait nyilvántartásba veszik, a rendelkezésre álló minden információt rögzíteni kell, az erre a célra fejlesztett programba. Az információk által létrejött adatbázisban szerepelnek az aktuális és archív, a fogvatartás alapjául szolgáló büntetés, intézkedés végrehajtásával összefüggő adatok, és iratok.



1. kép: Fogvatartott fényképezése [8]

A bv. intézet az elítéltről és az egyéb jogcímen fogvatartottról a befogadást követő három munkanapon belül fényképet készít, ezt illusztrálja az 1. kép. Az arcképmás rögzítését az arcképmás, az ujj- és tenyérynymat, valamint a DNS-profil meghatározásra alkalmas anyagmaradvány rögzítésének, illetve az ujj- és tenyérynymat és a szájnyalakahártya-törlet levételének részletes technikai szabályairól; a DNS-profil meghatározásának szakmai-módszertani követelményeiről; továbbá a nyilvántartás technikai vezetésének részletes szabályairól szóló 12/2016. (V.4.) BM rendelet 2. §-ban foglaltak figyelembevételével kell végrehajtani. [9]

A fénykép készítésekor a fogvatartott áll, szemei nyitva vannak, az arckifejezése nem lehet szándékosan torzított, homloka, fülei, arcéle jól látszódik. Ha általában szemüveget visel, akkor a fotó elkészítése során azt viselnie szükséges. Egy szemből, egy jobb oldalnézetből és egy baloldaltól, negyed profilban készített arcképmás, valamint kettő egész alakos – szemből és baloldaltól – állókép készül. [10]

A fogvatartottak fényképes nyilvántartását szükség szerint, de legalább hathavonta felül kell vizsgálni a teljes fogvatartotti állomány tekintetében. A felülvizsgálat célja annak megállapítása, hogy a nyilvántartásban szereplő fénykép rendelkezésre áll, és személyazonosításra alkalmas. A felülvizsgálat során a fényképet össze kell vetni a fogvatartott aktuális külső megjelenésével.

Amennyiben a felülvizsgálat a fénykép hiányát, vagy személyazonosításra való alkalmatlanságát állapítja meg, akkor új fényképet kell készíteni a fogvatartottról.

Személyazonosításra alkalmatlanná teszi a fényképet:

- a jelentősen megváltozott hajviselet,
- a megváltozott hajszín,
- a jelentősen megváltozott arcszőrzet viselési szokások,
- a sérülés, trauma, betegség vagy orvosi kezelés nyomán, az arcon vagy annak környékén megjelenő elváltozás, különös ismertetőjegy (pl. sebhely, tartós bőrbetegség, égési sérülés),
- a fogvatartott magatartása nyomán keletkező elváltozások (pl. önkárosítás nyoma, tetoválás, amennyiben ezek a fényképen látható területen helyezkednek el),
- a súlygyarapodás, súlyvesztés miatt megváltozott testkép vagy arcvonások,
- a természetes öregedésből eredően, jelentős mértékben megváltozó vonások.

Ha a fogvatartott megjelenésében a fenti változások valamelyike tapasztalható, akkor újabb felvétel rögzítése szükséges a nyilvántartás naprakésszé tétele céljából. Ezen felül valamennyi fogvatartottról naptári évenként legalább egy alkalommal új fényképet kell készíteni.



1.ábra: Ujjlenyomat vétele [11]

Az ujj- és tenyérynymat vételre, illetve a DNS-mintavételre a büntetés-végrehajtási intézetben a büntetés megkezdését követően indult büntetőeljáráásban van szükség. Az 1. ábrán egy ujjlenyomat vétel látható. A nyomozást végző ügyészség vagy katonai nyomozó hatóság a büntetést végrehajtó büntetés-végrehajtási intézetet keresi meg e feladatok ellátására. A megkeresés alapján az ujj- és tenyérynymat vételt, valamint a DNS-mintavételt a büntetés-végrehajtási intézet erre kijelölt és mintavételről oktatásban részesült tagja végzi. A felvett ujj- és tenyérynymatot, DNS mintát a bv. intézet haladéktalanul megküldi a megkereső ügyészség vagy katonai nyomozó hatóság részére. [10]

A fogvatartottak személyazonosság megállapítása (egyén azonossága) az intézetek falai között:

- a befogadás,
- a hozzátartozó látogatás fogadása,
- az elítélt munkába állítása,

- a börtön boltban vásárlás,
- a börtönben kihelyezett fali telefonkészülékkel telefonálás, illetve a jogérvényesítés tevékenységek során fontos.

KÖVETKEZTETÉSEK

Az egyik legrégebben használt azonosító módszer az egyes ember külső megjelenése, így az arca is, ez szinte teljes bizonyossággal megkülönböztet mindenkit a másoktól. A biometrikus adatok már évtizedek óta része az azonosítási rendszereknek. A tudomány jelenlegi állása szerint egyedi azonosításra alkalmas: a retina lenyomata, a tenyérgéometria, a fül geometriája, az emberi test, az arc hőterképe is, ezek az adott egyénre vonatkozó információ tartalmának tekinthetők. A biometrikus adat kapcsolatot teremt az adott információ és az egyén között. Ez a kettősség jelenik meg a DNS-adatoknál is, amelyek információt nyújtanak az emberi testről és egyben lehetővé teszik a személy egyértelmű és egyedi azonosítását.

A biometrikus azonosítások elfogadottságának növelése érdekében a fejlesztés hangsúlya azokra a technológiákra helyeződött át, amelyek nagyon gyorsan és pontosan képesek több millió vagy akár százmillió ember közül kiválasztani az adott személyt. Egyik legfontosabb jellemzője, hogy az ujjnyomatokat és a tenyérvénákat egyetlen művelettel beolvassa, egyidejűleg, pontosan rögzíti. Olyan technológia kidolgozására került sor, amely az adott személy kezének egyszeri beolvasásával pontosan rögzíti mindkét adatsort: a tenyérvéna mintázatot és a három ujjnyomatot is. [12]

A magyar törvények szerint a biometrikus azonosítást a bv.-ben jelenleg a befogadás során alkalmazzák. A befogadást végző bv. intézet köteles az elítélt személyazonosságát, a büntügyi nyilvántartási rendszer adatait ellenőrizni, illetve az iratokban szereplő adatokat is. Az ujj- és tenyérvénamintát, valamint a DNS-mintavételt a büntetés-végrehajtási intézet erre kijelölt tagja végzi. A bv. intézet az elítélt azonosítása érdekében rögzíti az elítélt ujjnyomatát és kezdeményezi a szakértői nyilvántartó szervnél a Bnytv. 82. § (5) bekezdés b) pontja szerinti összehasonlítást. Véleményünk szerint a befogadáson megjelenő személy adatai ellenőrzésével egyidejűleg célszerű lenne a szakértői nyilvántartó szervtől megkérni a fogvatartott ujj- és tenyérvénamintát és a DNS-mintáját is. Azonban, ha a nyilvántartásban nem szerepel, akkor a bv. személyi állományi tag elvégzi a nyomatok, illetve minták vételét és a szakértői nyilvántartásba vétel céljából megküldi azokat.

A biometrikus adatok vonatkozásában még nem belátható az a folyamat vagy fejlődés, hogy az informatikai fejlesztések, a mesterséges intelligencia alkalmazása hová fog vezetni, és hogyan tudja mindezt a jogi szabályozás kezelni, szabályozni.

FELHASZNÁLT FORRÁSOK

Irodalom

[1] AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2016/679 RENDELETE (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (EGT-vonatkozású szöveg) (letöltve: 2019.09.14.)

- [2] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (letöltve: 2019.09.14.)
- [3] 2009. évi XLVII. törvény a büntügyi nyilvántartási rendszerről, az Európai Unió tagállamainak bíróságai által magyar állampolgárokkal szemben hozott ítéletek nyilvántartásáról, valamint a büntügyi és rendészeti biometrikus adatok nyilvántartásáról (letöltve: 2019.09.14.)
- [4] 20/2009. (VI. 19.) IRM rendelet a büntügyi nyilvántartási rendszer egyes nyilvántartásai részére történő adatközlés szabályairól (letöltve: 2019.09.14.)
- [5] 53/2012. (XII. 22.) KIM rendelet a büntügyi nyilvántartó szerv által teljesített adat-szolgáltatás, valamint a hatósági erkölcsi bizonyítvány kiállítása iránti eljárás rendjéről és a hatósági erkölcsi bizonyítvány kiállítása iránti eljárásért fizetendő igazgatási szolgáltatási díjról (letöltve: 2019.09.14.)
- [6] 2013. évi CCXL. törvény a büntetések, az intézkedések, egyes kényszerintézkedések és a szabálysértési elzárás végrehajtásáról, 89. § (3), (4)-(7) (letöltve: 2019.09.20.)
- [7] 16/2014. (XII. 19.) IM rendelet a szabadságvesztés, az elzárás, az előzetes letartóztatás és a rendbírság helyébe lépő elzárás végrehajtásának részletes szabályairól (letöltve: 2019.09.20.)
- [8] <https://bv.gov.hu/hu/befogadasi-eljaras> (letöltve: 2019.09.23.)
- [9] A büntetés-végrehajtás országos parancsnokának 35/2017. (III.9.) OP szakutasítása a fogvatartottak nyilvántartására és egyes ügyeinek intézésére vonatkozó eljárásról
- [10] 12/2016. (V. 4.) BM rendelet az arcképmás, az ujj- és tenyérynymat, valamint a DNS-profil meghatározásra alkalmas anyagmaradvány rögzítésének, illetve az ujj- és tenyérynymat és a szájnyalékahártya-törlet levételének részletes technikai szabályairól; a DNS-profil meghatározásának szakmai-módszertani követelményeiről; továbbá a nyilvántartás technikai vezetésének részletes szabályairól (letöltve: 2019.09.23.)
- [11] VESZELI Dániel János: A FANY rendszer; <https://slideplayer.hu/slide/1953374/> (letöltve: 2019.09.23.)
- [12] KONDÁS Katalin: A biometria jelenlegi megítélése, Hadmérnök VIII. Évfolyam 1. szám, 2013. március

**SOCIAL ENGINEERING AND
MANIPULATION TECHNIQUES AND
METHODS****A SOCIAL ENGINEERING ÉS A MANIPULÁ-
CIÓS TECHNIKÁK ÉS MÓDSZEREK**KOLLÁR Csaba¹, ZAKAR Ákos²**Abstract**

In the first, theoretical part of our two-part study, we review all or most of the manipulation methods and techniques related to the human soul, psychology, and interpersonal communication, which also appear in the field of information security. In describing the techniques and methods, we present, among other things, shoulder surfing, asking for and providing help, personalization, phishing, image and video forgery, fake security applications, and fraudulent calls. In the latter case, we also point out the criminal law implications of the perpetrators' act. Fraudsters have also taken advantage of the psychological effects of the coronavirus, as mentioned in several examples. We hope that we can contribute to the personal and organizational development of information security by reviewing the theory, presenting examples, and then presenting our research results in the next section.

Keywords

information security, social engineering, manipulation

Absztrakt

Kétféle tanulmányunk első, elméleti részében az egészében, vagy zömében az emberi lélekhez, a pszichológiához, a személyközi kommunikációhoz köthető, manipulációs módszereket és technikákat tekintjük át, melyek az információbiztonság területén is megjelennek. A technikák és módszerek ismertetésénél a humán, illetve IT alapú felosztás mentén mutatjuk be többek között a váll feletti leskelődést, a segítségkérést, illetve -nyújtást, a megszemélyesítést, az adathalászatot, a kép- és videohamisítást, a hamis biztonsági alkalmazásokat, a csaló hívásokat. Ez utóbbinál rámutatunk az elkövetők cselekményének büntetőtörvénykönyvi vonatkozásaira is. A csalók kihasználták a koronavírus pszichés hatásait is, ahogy arra több példa kapcsán is utaltunk. Reményeink szerint az elmélet áttekintésével, a példák bemutatásával, majd a következő részben kutatási eredményeink ismertetésével egyaránt hozzá tudunk járulni az információbiztonság személyi és szervezeti fejlesztéséhez.

Kulcsszavak

információbiztonság, social engineering, manipuláció

¹ kollar.csaba@phd.uni-obuda.hu | ORCID: 0000-0002-0981-2385 | PhD student / doktorandusz | Obuda University Doctoral School of Safety and Security Sciences / Óbudai Egyetem Biztonságtudományi Doktori Iskola

² zakarakos85@gmail.com | ORCID: 0000-0002-3919-4098 | detective / nyomozó | Rapid Response and Special Police, Services National Bureau of Investigation, Cybercrime Department / Készenléti Rendőrség, Nemzeti Nyomozó Iroda, Kiberbűnözés Elleni Főosztály

BEVEZETÉS

Tanulmányunk első, elméleti részében a social engineering módszereiről kívánunk egy átfogó képet adni. Szerteágazó technikák gyűjteményéről van szó, hiszen a kibertérben elkövetett támadások 98%-a social engineering technikára támaszkodik [1]. Jelen tanulmányunkban ezek közül a fontosabbakat tekintjük át, alapul véve a kettős felbontást (humán és számítógép alapú) [2]. Ahogy arra Kevin Mitnick [3] is utal, a befolyásolás és rábeszélés módszerét alkalmazva, a technológia használatával vagy a nélkül éri el célját a támadó. Mivel bizonyos módszerekben átfedés tapasztalható, így az „első lépés” jellege alapján soroltuk be az adott kategóriába a támadásokat (1. táblázat), alapul véve a EC-Council CEH [4, p.959-1028] oktatási anyagát.

Humán alapú	IT alapú (mediatizált)	
	Számítógép használattal	Telefon használattal
1. Váll feletti leskelődés	1. Elhagyott adathordozó	1. SMS
2. Hallgatóság	2. Billentyűzet naplózó	2. Kártékony alkalmazás
3. Segítségkérés	3. Adathalászat	3. Hamis biztonsági alkalmazás
4. Segítségnyújtás	4. Kéretlen e-mail	4. Újracsomagolt alkalmazás
5. Fordított social engineering	5. Álvírusirtó	5. Instant üzenetküldő
6. Megszemélyesítés	6. Zsarolóvírus	6. Csaló hívás
7. Épületbe való bejutás	7. Trójai program	
8. Kukabúvárkodás	8. Hamis szoftver telepítő	
9. Jelszavak kitalálása	9. Hálózatfigyelés	
	10. Felugró ablak	
	11. Üzleti e-mail kompromittálás	
	12. Kép és videó hamisítás	

1. Táblázat: A fontosabb social engineering technikák csoportosítása (saját szerkesztés)

HUMÁN MÓDSZERREL VÉGREHAJTOTT TECHNIKÁK

Mint ahogy a kategória neve is mutatja, a támadónak ez esetben nem kell műszaki eszközöket igénybe vennie, mivel az ember kommunikációs és pszichológiai képességeire, gyengeségeire épít. Pszichológiai és kommunikációs szempontból ez igényli a legmagasabb fokú felkészültséget a támadó részéről, ugyanakkor a lebukás veszélye is itt a legnagyobb, hiszen – pár kivételtől eltekintve – közvetlen kontaktust létesít a célszeméllyel. Sok esetben kevesebb idő- és energiaráfordítást igényel végrehajtásuk, mint egy technológiai módszernek. További előnyük, hogy olyan jellegű információk birtokába juthatunk, melyekkel más jellegű támadások kivitelezését meg lehet könnyíteni, illetve a célszemélyt rá tudjuk venni arra is, hogy helyettünk hajtson végre valamilyen támadást (pl. adatbázishoz hozzáférés). Ebbe a kategóriába sorolhatók azon módszerek, melyek végrehajtásához nincs szükség az informatika, szűkebb értelemben véve a számítógép használatára. Itt csak a célszemély felkészültsége és tudatossága szabhat gátat a támadás sikerének, ugyanis semmiféle – klasszikus értelemben vett – IT technológiai védelem (pl. tűzfalak, spam szűrők) ez esetben nem működik. [5, p.88] Az alábbiakban ezeket vesszük sorra.

Váll feletti leskelődés

Avagy angol terminológiában „shoulder surfing”, melyet váll-szörfnek is fordíthatunk, de a kifigyelés, leskelődés találhatóbb kifejezések rá. Ez egy viszonylag könnyen kivitelezhető technika, aminek célja az előttünk álló, vagy számítógépnél ülő személy hitelesítő adatainak megszerzése, miközben azokat ő begépel az adott eszközön. Itt ki lehet használni az áldozat bizalmát (pl. közvetlen kollégák esetén) vagy amennyiben erre nincs mód az adott szituációban, akkor mindezt észrevétlenül kell végrehajtani, úgy, hogy se a célszemély se mások ne vegyék észre. Ezt utóbbi kockázatra megoldást jelenthet, ha úgynevezett hatásfok növelő eszközöket vesznek igénybe (pl. távcső, vagy speciális kamerák), amik képesek a távoli mozdulatokat, információkat közelebb hozni vagy rögzíteni. Ez utóbbi példa azonban már túlmutat a kategória keretein, de például egy rejtett kamerás megfigyelés is innen eredeztethető.

Hallgatózás

Tipikus humán alapú technika – mely szinte egyidős a váll feletti leskelődéssel, sőt lehet mondani, hogy az emberi beszéd megjelenésével – amit el lehet követni technikai eszköz használatával is. Az alkalmazás módját az adott szituáció dönti el. Itt a jogosulatlan személy valós időben privát beszélgetést „fog el”, ami kettő vagy több ember közt zajlik. Könnyedén meg lehet hallani bizalmas információkat pl. kávézóban, tömegközlekedési eszközökön, rendezvényeken, várótermekben. Ilyenkor ugyanis nem tűnik fel senkinek a másik ember közelsége, mondhatni ebben a közegben ez természetes. Ha párhuzamba vonjuk a kifigyeléssel, ez az eszközös lehallgatás előszobájának tekinthető, de még mindig működő klasszikus módszer.

Segítségkérés

A segítségnek két oldalát akár egy technikának is tekinthetjük. Az egyik legkönnyebben kivitelezhető módszer, mivel a támadó egész egyszerűen segítséget kér a kiszemelt áldozattól. Bibliai hasonlattal élve „Kérjete, és adatik nektek...” itt (is) értelmet nyer [72]. A támadó persze ezt más céllal használja úgy, hogy eredeti szándéka rejtve maradjon. Mivel az emberek nagy része segítőkész – a kiszolgáló és szolgáltató területen dolgozóktól pedig egyenesen elvárás, pl. helpdesk, recepciós, titkárnő – így könnyű sikert elérni.

Segítségnyújtás

Az előzőnek a fordítottja, vagyis a támadó idéz elő egy hibát, melyet már az elején úgy épít fel, hogy a megoldását az adott helyzetben és időben az ő személyében lássa meg az áldozat. A támadó a mesterséges kényszerhelyzet kihasználásával fog hasznot húzni pl. azáltal, hogy távolról hozzáfér az áldozat számítógépéhez, vagy nyomtató javítást, villanyszerelést imitál. De előnyhöz juthat úgy is, ha az elvégzett szívességért cserébe, fizetség helyett „viszont szívességet” kér, amivel vissza is kanyarodtunk a segítségkéréshez. [5, p.81-82] Egy jól ismert szabály a társadalmi interakcióban, hogy a szívesség szívességet szül, még akkor is, ha az eredeti szívességet kérés nélkül ajánlották fel. Ezt az eljárást hívjuk reciprocitásnak.

Fordított social engineering

Kevin Mitnick ezt a technikát „fordított szűrés”-nek nevezte el, amit már nehezebb kivitelezni, mint az előbb említett segítségnyújtást, de hasonlóhoz [3]. Ennek oka, hogy jóval több előkészületet és speciális képességeket igényel. A támadónak ugyanis még a probléma létrejötte előtt meg kell győznie a dolgozót arról, hogy baj esetén bizalommal fordulhat hozzá. A probléma megoldására irányuló előzetes kérdések feltevésekor már eleve úgy manipulálja a kérdéseit, hogy az áldozat kimondja, elszólja magát a bizalmas információkat illetően, amik elemei lehetnek és megalapozhatnak egy komplexebb támadást.

Megszemélyesítés

Itt kifejezetten nagy jelentősége van a támadó kinézetének, mert az emberek az első benyomás alapján a fejükben bekategorizálják az idegeneket. „A humán alapú technikák nagy része alapvetően arra irányulnak, hogy a támadó egy másik személynek adja ki magát, amely lehet való vagy fiktív személy”. [7, p.9] A támadó célja, hogy elhitesse az áldozattal, hogy ő valóban az – legyen akár fiktív, akár valós személyiség – akinek kiadja magát. Mivel több alkategóriákra lehet bontani eme komplex támadási formát, így erre részletesebben a következőkben fogunk kitérni.

Épületbe való bejutás

Ezen technikának alapvetően három típusa ismert: tailgating, piggybacking, masquerading [8, p.39], s tartalmukban e három fogalom átfedést mutat, illetve a szakirodalom sem egészen következetes a használatukat illetően. A tailgating és a piggybacking egyaránt arra utalhat, hogy a támadó egy jogosultsággal rendelkező személyhez társul, beszélgetésbe elegyedik vele, s így képes bejutni bizonyos (lezárt) területekre, vagy úgy jut be, hogy nem szükséges beszédbe elegyednie mással. Ez a cselekmény nem mindig illegális, bár a belépés rendszerint jogosultsághoz és/vagy engedélyhez kötött, amivel a támadó nem rendelkezik. A támadó nem csak az emberi humánus gyengeségeit használhatja ki (amire a szoros követés, a piggybacking épül), de a biztonsági (nem csak informatikai) rendszer gyengeségeit is (a tailgating fogalma inkább ehhez köthető), például egy ajtó automatikus zárásának késleltetése kellő időt biztosít arra, hogy a támadó is bemenjen, vagy vannak olyan fizikai hátsó ajtók melyek védelmére nem fordítottak kellő figyelmet, s így a támadó minden különösebb nehézség nélkül besétálhat. A masquerading lényege, hogy a támadó meggyőzi a személyzetet arról, hogy neki joga van bizalmas, titkos információk megszerzéséhez (pl.: informatikust, vagy belső ellenőrt játszik, akit a központból küldtek ki). A hitelessége érdekében hamis belépőkártyát, hamis céges egyenruhát használhat. Határozott fellépésének köszönhetően az ellenőrzésért/beléptetésért felelős személy(eke)t viszonylag könnyen meg tudja téveszteni.

Kukabúvárkodás

Ahogy a módszer neve is mutatja, nem túl kifinomult, kommunikációt nem igénylő technikáról van szó, ugyanakkor fontos, hiszen megalapozhat egy későbbi komplex támadást. A támadónak először meg kell szerveznie, hogy milyen módszerrel juthat a kukához úgy, hogy az ne keltsen gyanakvást abban, aki ezt észreveszi. Ezt követően egy nyugodt helyen alaposan át tudja vizsgálni annak tartalmát. Ehhez információt kell gyűjteni a kukák

tárolásáról, elszállításáról is. [5] Beszélhetünk akár vállalati, akár privát szféráról, a felelőtlen emberek rengeteg olyan információt tartalmazó dolgokat dobnak ki a szemetesbe, melyről úgy gondolják, hogy az szinte egyből meg is semmisül. [8, p.39]. Sokan lebecsülik ennek a módszernek a használatát, pedig megannyi értékes dokumentumot tartalmazhat a munkahelyi szemetes:

- Szervezeti ábrákat, helyszínrajzokat: felfedik a részletes struktúráját a cégnek, fizikai felépítését, tiltott területeket (pl. szerver szobák).
- Nyomtatott e-maileket, jelentéseket, faxokat: felfednek személyes információkat dolgozóról, a jelszavak, szerződések, belső utasítások mellett.
- Belső kézikönyveket, utasításokat: felfednek foglalkoztatási adatokkal vagy az alkalmazott IT rendszer használatával kapcsolatos információkat.
- Esemény feljegyzéseket, naptárakat vagy nyomtatott számítógépes logokat: felfednek olyan információkat, amik a felhasználói be- és kijelentkezésekre vonatkoznak, így segíteni fogják a támadót a támadás megfelelő időpontjának kiválasztásában.
- Telefonszám listákat: felfedik a dolgozók neveit és belső telefonszámaikat.

Jelszavak kitalálása

Szándékosan a kitalálás szót használjuk és tesszük a humán alapú technikák közé, mivel itt szó sincs adathalászat útján, vagy különböző jelszó feltörő szoftverek segítségével megszerezhető hitelesítő adatokról. Jelenleg is megállja a helyét Jeff Crume mondása, miszerint „napjainkban, az informatikai rendszerekben a hitelesítés legelterjedtebb formája a jelszó”. [9, p.114] Mint ahogy arra a kutatási jelentést tartalmazó második részben még ki fogunk térni, itt a felhasználó által használt gyenge jelszavak megválasztásában kell keresni a gyengeséget, amit a támadó ki tud használni. A jelszavak nagy része ugyanis bizonyos fokú személyes ismeretség vagy információszerzést követően viszonylag könnyen kitalálható. A jelszavak egy jelentős részénél pedig – ahogy az az alábbi ábrán látható – még a személyes alaposabb ismerete sem szükséges.

What Are the 50 Most Common Passwords?									
Based on most common duplicate passwords within a breach of over 30 million accounts.									
1.	123456	11.	123321	21.	222222	31.	333333	41.	password1
2.	123456789	12.	1q2w3e4r5t	22.	112233	32.	123qwe	42.	q1w2e3r4
3.	qwerty	13.	iloveyou	23.	abc123	33.	159753	43.	qqww1122
4.	password	14.	1234	24.	999999	34.	q1w2e3r4t5y6	44.	sunshine
5.	1234567	15.	888888	25.	777777	35.	987654321	45.	zxcvbnm
6.	12345678	16.	654321	26.	qwerty123	36.	1q2w3e	46.	1qaz2wsx3edc
7.	12345	17.	555555	27.	qwertyuiop	37.	michael	47.	liverpool
8.	1234567890	18.	gfhjkm	28.	888888	38.	lovely	48.	monkey
9.	111111	19.	777777	29.	princess	39.	123	49.	1234qwer
10.	123123	20.	1q2w3e4r	30.	1qaz2wsx	40.	qwe123	50.	computer

1. Ábra: A leggyakrabban használt gyenge jelszavak [10]

Bizonyos munkahelyeken – a „túlzott” bizalom és a baráti légkör miatt – nem ritka, hogy a felhasználók megadják egymásnak a jelszavaikat, ezzel öntudatlanul súlyos kockázatnak kitevé az adott rendszerbeli fiókjuk saját felügyeletét. Egy 785 szervezetet tanulmányozó kutatás [11] a dolgozók jelszóhasználati szokásait elemezte. A vizsgált cégek 61%-nál találtak olyan felhasználókat, akiknek jelszavai nem járnak le. 40%-nál fordultak elő olyan engedélyezett felhasználói fiókok, melyek már elavultnak számítottak, azaz már nem aktív dolgozókhoz tartoztak. Összevetve, átlagosan minden második fiók ebbe a kategóriába tartozott. A felelőtlen magatartás által ez a statisztika is rámutat a jelszó kitalálás módszerében lévő lehetőségekre, melyre kutatási jelentésünkben mi is ki fogunk térni.

IT ALAPÚ MÓDSZERREL VÉGREHAJTOTT TECHNIKÁK

Ide azok a technikák tartoznak, melyek informatikai eszközök – jellemzően számítógépek és okostelefonok – segítségével próbálják meg átéjteni a gyanútlan felhasználót, azonban itt is az emberi mulasztást, hiszékenységet használja ki a támadó. „Ezen technikák jellemzője, hogy a social engineer azt hiteti el az áldozatokkal, hogy egy valódi rendszerrel kommunikálnak, s nem veszik észre, hogy csalás áldozataivá válnak” [8, p.39]. Nagy előnye a humán alapú módszerrel szemben, hogy a személyes kontaktus elkerülésével a lebukás kockázata minimalizálható.

Számítógépes technikák

Elhagyott adathordozó. Alapvetően a kártékony programok terjesztésének egyik módszere. A technika ismert angol neve a baiting, ami csalogatást, beetetést jelent, de „Road Apple” támadásnak is nevezik [12]. Kiindulásként a támadó egy kártékony szoftvert telepít egy, de inkább minél több tetszőleges adathordozóra – többnyire pendrive-ra, SD kártyára, régebben optikai, illetve floppy lemezekre – majd azokat a célszemélyhez közeli helyeken (pl. mosdó, konyha, tárgyaló, recepció, folyosó, nyomtató, iroda, parkoló) elhelyezi, szét-szórja. Kiváló csali lehet egy figyelemfelkeltő felirat pl. „bizalmas” elhelyezése az eszközön. Az emberi kíváncsiságból eredően előbb-utóbb valaki meg be fogja tenni – remélhetőleg – a vállalati számítógépbe és a rajta lévő program már meg is kezdi a működését. Megemlítjük még a kártékony kód terjesztésének egyéb módjait, mint pl. postai úton/futárral beküldött, reprezentációs ajándékként osztogatott vagy újság mellékleteként eljuttatott adathordozót, e-mail melléklet csatolmányát, weboldal látogatását, azonban ezek bővebb bemutatására tartalmi korlátok miatt nem bocsátkozunk [5, p.105-106].

Billentyűzet naplózó. A Keylogerek/Key stroke loggerek lehetnek szoftveres alkalmazások vagy hardveres eszközök is. Működésüket tekintve a felhasználó tudta nélkül rögzítik a billentyűzet leütéseket, beállítástól és típustól függően pedig elküldik a támadónak. A hardveres megoldás választása esetén, mint a baitingnél is, szintén szükséges az ember általi céleszköz elhelyezése. Ez a lebukás veszélye miatt kockázatos is lehet, azonban a telepítés hatékonyabb, mivel semmiféle gyanús szoftvert, weboldalt nem kell igénybe venni a kezdeti működéshez az áldozatnak. Az elhelyezés során felmerült kockázat nagyszerűen csökkenthető pl. takarító, karbantartó személyzet közbenjárásával, akik nem keltenek gyanút egy irodai dolgozóban.

Adathalászat. Az adathalászatot, vagyis a phishing-et jelszóhalászatnak is fordíthatjuk, azonban nem csupán jelszavak, hanem banki adatok, bizalmas információk stb. megszerzése is cél lehet. Amennyiben nem tömegszerűen indítanak „phishing kampányt” az elkövetők, megcélozhatnak a szervezetben belül egy adott személyt (spear phishing) vagy egy felsővezetőt (bálnavadászat/whaling) is. Az adathalász e-mailek általános jellemzői közé tartozik az általános megszólítás, helyesírási hibák használata, sürgetés, számlazárolásra/szolgáltatásból való kizárásra figyelmeztetés, személyes információkra vonatkozó kérés. A phishing levelek óriási mennyiségét az RSA 2019. IV. negyedéves jelentése [13] mutatja be a legjobban, miszerint 2019-ben a phishing levelek 60%-át tették ki éves szinten a csaló szándékú támadásoknak. Előző negyedévhez viszonyítva itt volt tapasztalható a legnagyobb arányú növekedés. A CERT-GIB jelentésében [14] 2020.02.13. és 2020.04.01. között több száz koronavírussal kapcsolatos phishing e-mail analíziséről számol be. Az e-mailekben 65%-ban különböző típusú kémprogramokat (spyware), 31%-ban hátsó ajtókat (backdoor) és 4%-ban zsarolóvírusokat (ransomware) találtak, melyek a csatlományban voltak megtalálhatóak. Az adathalászok a tömeges e-mail üzenetek küldésén felül további módszerekkel is átejtetik áldozatukat, adataik bekérése érdekében. Ezek közül a három leggyakoribbat az alábbiakban ismertetjük.

Ál weboldal. Egy olyan weboldal készítése, mely regisztrációt követően csábító nyereményeket ígér, nem nehéz feladat, az elterjedt és könnyen kezelhető CMS rendszereknek köszönhetően. Természetesen ezek mögött valós nyereményjáték nincs. A regisztráció során begyűjtött e-mail címelekkel már eleve egy adatbázishoz jut az elkövető, amit későbbi adathalászat során felhasználhat, valamint egyben jelszavakat szerez, amik köthetők lehetnek a felhasználó más webes alkalmazásaihoz is, alapot adva egy komolyabb támadáshoz.

Hamisított weboldal. Az ál weboldallal szemben annyiban különbözik, hogy ez esetben egy létező és jól ismert többnyire pénzügyi szektorban érintett vállalat weblapját másolják le. Az eredeti weblappal szemben a hamisított weboldal URL-jében minimális különbség fog jelentkezni, amit a nem kellőképpen figyelmes felhasználó nem fog észrevenni és az oldalra belépve jóhiszeműen megadja hitelesítő adatait, amik elküldésre kerülnek a támadónak. Az oldalra irányítás általában email üzenetben található linkkel történik. Egyes felmérések szerint minden tizedik URL kártékony oldalra irányít [15].

Farmolás. A pharming során a felhasználó nincs és nem is lehet tudatában annak, hogy hamisított weboldalon jár. A támadó a DNS szerverek sérülékenységét használja ki vagy az áldozat számítógépén található host fájl módosítja, ezáltal az URL-ben nem fog különbség mutatkozni a hamisított és eredeti weboldal között. A módszerek eredménye ugyanaz, eltéríteni a felhasználót attól, hogy az általa elérni kívánt URL címen lévő weboldalt megleltesse, helyette más oldalra lesz átirányítva.

Kéretlen e-mail. A spam üzenetek irrelevánsak, kéretlenek és nagy tömegben érkeznek. A többnyire marketing célból érkező, termékek értékesítésének növelését célzó levelek mellett ide sorolhatók a scam típusú, azaz a tipikus átverős üzenetek, valamint a hoaxok, azaz a lánclevelek is. A scam-eknél általában meghamisítják a feladó e-mail címét és

ismert nagy cégek nevével élnek vissza, akik nyereményről értesítik a címzetteket. A lánclevelek célja főként az e-mail címek begyűjtése. De a fentiek akár kártékony csatolmányokat (pl. vírusokat) is tartalmazhatnak. Az ilyen veszély mellett közvetlen kárt is okoznak, mivel egy vállalati felhasználó idejét a produktív munka helyett, az üzenetek törlése, esetenként megnézése köti le. Gyakoriságukat mi sem mutatja jobban, mint az, hogy a Symantec szerint [16] 2018-ban a fogadott e-mailek 55%-a spam volt. Az IBM adatait alapul véve a spam üzenetek URL-jei mintegy 70%-át teszik ki a főbb fenyegetés típusnak.

Álvírusírtó. Ezeket a programokat scarewareknek is hívják, és ahogy a neve is utal rá, félelmet akarnak kelteni. Akár egy felugró ablakként megjelenő animációval is – mely szkennelést imitál – könnyen elhitetik a laikus felhasználóval, hogy a számítógépe vírussal fertőződött meg. Ezt követően felajánlják a saját terméküket, ami megoldást jelent a problémára, ami lehet ingyenes vagy fizetős szoftver is. A valóság ezzel szemben az, hogy a támadó által felkínált program telepítésekor fertőződik meg a felhasználó számítógépe. A program káros kódja információkat is szivárogtathat a készítőjének a megfertőzött gépről, ami előtte lehet, hogy mentes volt a vírusoktól. Jellemzőjük továbbá, hogy a háttérben blokkolhatják a már meglévő hiteles vírusírtónk frissítését vagy elérhetetlenné teszik a program törlését uninstall funkcióval [5, p.98]. A felhasználó az ilyen káros programok telepítésekor kettős kockázatnak is kiteszi magát. Egyrészt fizet egy olyan szoftverért, ami nem tölti be a funkcióját, vagyis nem irtja a vírust, másrészt megfertőzi a számítógépét kártékony programmal.

Zsarolóvírus. A ransomwarek, vagyis a zsarolóvírusok olyan kártékony szoftverek, melyek zárolják az eszközöket vagy titkosítják a rajtuk lévő adatokat annak érdekében, hogy bevételre – manapság jellemzően kriptovalutára – tegyenek szert a tulajdonostól. A fertőzést követően megjelenő képernyőn az elkövetők azt ígérik – természetesen bármiféle garancia nélkül –, hogy egy adott összegért cserébe visszaállítják a hozzáférést és megküldik a titkosítás feloldásához szükséges kulcsot az érintett géphez vagy adatokhoz. Általában email mellékletként, távoli asztal kapcsolat kihasználásával trójai program bejuttatásával, vagy böngészés közben linkre kattintással is terjedhetnek. Típusai közt megtalálhatóak a lemez-kódoló (titkosítja az egész merevlemezt), a képernyőzároló (megakadályozza a hozzáférést az eszköz képernyőjéhez), a crypto (titkosítja a merevlemezen található bizonyos adatokat) valamint az okostelefonra szánt változata a PIN-lezáró (megváltoztatja a hozzáférési kódot) [17]. A legtöbb zsaroló vírus család célpontjai még mindig a Windows alapú számítógépek [18]. Az utóbbi idők egyik legsúlyosabb zsarolóvírus támadás sorozat a WannaCry és a Petya nevű ransomware volt 2017-ben [19]. A 2018-ban ismertté vált Ryuk zsarolóvírus 2019-ben már a legtöbb ágazati szektorban megtalálható volt [20]. Az Interpol közleményében [21] figyelmeztet, hogy napjainkban főként kórházakat valamint más egészségügyi intézményeket – melyek a koronavírus frontvonalában harcolnak – éri a legtöbb zsarolóvírus támadás.

Trójai program. Ahogy Jeff Crume is megfogalmazta a trójai faló olyan „rosszindulatú szoftver, amely funkciója alapján hasznosnak vagy érdekesnek tűnik, de az álca mögött meghúzódó szándék rossz” [9, p.291]. A programok működési elve a mitológiai Trójai falóhoz hasonlóan a megtévesztésen alapul. Mászt csinálnak, mint amit valójában mutatnak,

így az egyik legmegfelelőbb módszer, amikor a támadó távolról akarja átverni áldozatát. Ismertek azonban olyan típusai is, melyek valóban végrehajtják a kínált – esetenként szórakoztató – funkciókat, viszont ezek mellett kártékony, rejtett tevékenységet is végeznek. A trójai programok működési elve különbözik a vírusokétól, ugyanis nem reprodukálják magukat és nem feltétlenül tartalmazznak olyan kártékony kódot, mely a rendszer működését leállítaná. Céljuk a számítógéphez való illetéktelen hozzáférés, kémkedés lehetőségének biztosítása [22]. Funkciójuk alapján így megkülönböztetünk billentyűzet leütést naplózó, hátsó ajtót nyitó, jelszavakat gyűjtő, reklámodalakat megnyitó, felhasználói adatokat begyűjtő trójai programokat. Általában weboldalakon való böngészés, e-mail melléklet megnyitása, vagy elhagyott adathordozón keresztül juthatunk hozzájuk [8, p.50-51].

Hamis szoftver telepítő. Az elmúlt egy évtizedben jelentek meg, céljuk az anyagi haszonszerzés. A támadó ingyenesen letölthető szoftvereket tömörít be és teszi közzé különböző weboldalakon. A kicsomagolási – vagyis a hamis telepítést imitáló – művelet végén megpróbálja rávenni a felhasználót arra, hogy aktiválás címen küldjön pl. emelt díjas SMS-t vagy online fizetéssel rendezze az ellenőrző kód ellenértékét. Amennyiben a felhasználó fizet, a szoftver készen fog állni az installálásra és a használatra. A támadó lényegében egy ingyenes szoftvert nyújt a felhasználónak extra díjért cserébe, ezért is nevezik paid archive technikának [23].

Hálózat figyelés. A hálózatok figyelése, azokon való hallgatóság végrehajtása kellő fokú szakértelmet igénylő feladat. Ezért a laikusok azt is gondolhatnák, hogy inkább a hackerok, mintsem a social engineerek kompetenciájába tartozik. Az igazság azonban az, hogy nem két különálló halmazról beszélünk. Egy hackernek – legyen az jó vagy rossz szándékú – a social engineering is egy szelete a munkájának. Egy aktív MITM (közbeékelődéses) támadás végrehajtása során megtévesztheti mindkét felet, akinek a levelezésébe beékelődik, vagyis hozzáfér az e-mailjeikhez, ezáltal akár módosíthatja is a levelek tartalmát saját érdekeinek megfelelően. Jellemző példa, amikor két pénzügyi partner esetén kicseréli a cél bankszámlaszámot a sajátjára, így a jogosult fél helyett ő fogja megkapni a pénzt. De a közbeékelődésen kívül a normál adatfolyam megszakítása, fals adat generálása és a passzív lehallgatás is ide tartozik. A hacker be tud ékelődni a felhasználó és egy webszerver közti kommunikációba is.

Wi-fi támadás. Egy nem megfelelően megválasztott, azaz túl gyenge, alapértelmezett, régóta használt jelszóval nagy veszélynek tesszük ki akár a céges, akár a magán vezeték nélküli hálózatunkat. Ugyanakkor elavult titkosítási (pl. WPA, WEP) mechanizmusok alkalmazásával szinte pár másodperc alatt törhetővé válik a hálózatunk és az eszközeink. Épp ezért tökéletes célpontjai a támadóknak az olyan helyszínek, ahol ingyenes wi-fi használat van biztosítva, vagy ki van írva a wi-fi jelszó pl. a kávézóban a bárpulton vagy egy szállodában. A támadók akár a nyílt hálózatot is kompromittálhatják vagy létrehozhatnak rogue AP-eket, ami egy rosszindulatú másolatoként tűnik fel az eredeti wi-fi hozzáférési pontnak. Amennyiben a felhasználói készülékeken elmentésre került a lemásolt vezeték nélküli hálózat neve, a támadó már a saját hálózatában fogadva könnyedén ellophatja az áldozat szenzitív információit pl. netbank belépési adatait.

Felugró ablak. A felugró ablakok ráveszik a felhasználókat, hogy egy olyan hivatkozásra kattintsanak, ami átirányítja őket egy hamis weboldalra. Itt személyes információkat kérhetnek tőlük vagy kártékony programok tölthetnek le a számítógépükre úgy, mint a már említett keyloggerek, trójaiak és a vírusok is. A megjelenő pop-up ablakok általában valamilyen nem létező operációs rendszerbeli problémára és egyben megoldására hívják fel a figyelmet. Ezzel csábítják a felhasználókat és kihasználják kíváncsiságukat, hogy rákattintsanak az adott linkre, amivel hozzájuthatnak a szolgáltatáshoz vagy akár egy értékes nyemrényhez. Ellophatnak hálózati login adatokat is azzal, hogy a hálózati kapcsolat megszakadásának színlelése miatt a megjelenő adatmezőkben újbóli bejelentkezést, hitelesítést kérnek a felhasználótól. Amikor a felhasználó követi ezeket az instrukciókat a kártékony program telepítődik a számítógépre, információkat szivároztatva ki a támadónak.

Üzleti e-mail kompromittálás. Business Email Compromise-ként (BEC) ismert jelenség az angolszász államokban jelent meg először, majd lassan szinte az egész világon elterjedté vált. A csalók a pénzügyi tranzakciók lebonyolításában részt vevő illetékes személyeket ejtik tévedésbe azáltal, hogy magukat a felettesüknek vagy partnercég képviselőjének adják ki és idegen bankszámlaszámra kérik az utalás teljesítését. A kivitelezés során a támadók nyílt online forrásokból (pl. cég weblapja, cég adatbázis, közbeszerzési szerződés részletei stb.) vagy akár kuka búvárkodás során megszerzett információkból megtudják az adott vállalatnál dolgozó felső vezető, valamint pénzügyi területen dolgozók nevét és email címét. A profilalkotást követően és a szükséges mennyiségű adatok birtokában, a csaló magát a partnercég képviselőjének kiadva – formailag és tartalmilag hitelesnek tűnő – e-mail üzenetben arról tájékoztatja az áldozatot, hogy a jövőben egy másik bankszámlaszámra utaljanak. Amennyiben a célpont vezetőjét kívánja megszemélyesíteni a támadó, azonnali utalásra utasítja a beosztottját. Amennyiben nem sikerül az e-mail címet teljes mértékben utánozni, az eredetihez nagymértékben hasonlító e-mail címmel és a sürgősség, fontosság látszatának keltésével többnyire sikeresen kivitelezhetőek az e fajta támadások. A magánszemélyeket célzó változatában a támadók privát postafiók felett veszik át az irányítást, ezt a típusát E-mail fiók kompromittálásnak, azaz Email Account Compromise-nak hívják (EAC). 2019-ben az FBI IC3 központja 23.775 db BEC/EAC típusú panaszról kapott bejelentést, ami több mint 1,7 milliárd \$ kárt okozott a sértetteknek.

Kép és videó hamisítás. A deep fake-nek nem kifejezetten célja a közvetlen anyagi haszonszerzés. Elsősorban reputáció csökkenést vált ki, de egyre inkább az emberek véleményének manipulálásának eszközévé vált, mint ahogy a fake news is. Ennek szerepe főleg a választási ciklusok idején éleződik ki. Kezdetben álló képeken lévő személyek arcát vagy a kezükben lévő tárgyakat, háttereket módosították. A technika fejlődésével és a célszoftverek megjelenésével az elmúlt években azonban video anyagok szereplőinek arcát és hangját is sikerült fiktív tartalommal ellátni. A módosítással elérhető hatás lehet akár megalázó (pl. szexuális tartalom esetén) vagy társadalmilag, morálisan elítélendő is. Célpontjainak tekinthetjük akár az egész online közönséget, akik az álvideókat potenciálisan megtekintik, de igazi áldozataik azok a politikusok, celebek, hírességek, akiknek visszaélnek az arcával és hangjával.

Telefonos technikák

A kiberbűncselekmények növekedésének egyik oka a mobil technológia fejlődése. A mobil alapú internetet napjainkban már telefonról, tabletről, különböző okos eszközökről is könnyedén el tudjuk érni. Szinte állandóan online lehetünk a különböző instant üzenetküldő szolgáltatásoknak köszönhetően. Ez a közvetlen hozzáférés kényelmet, egyben kockázatot is jelent a felhasználóknak. A támadók okostelefonra készült mobil alkalmazásokat is használhatnak, hogy végrehajtsanak mobil alapú social engineeringet. Ennek eredményeként sok trükk jelent meg, amivel becsaphatják az embereket.

SMS. A smishingben az SMS szöveg küldő rendszert használják csaliként a hackerek, egy olyan cselekvés kifejtésére, amivel rá tudják venni az áldozatot, hogy megnyissa az üzenetben lévő linket. Ezzel akár közvetlenül letölthetnek egy malwaret, átirányítja őket egy káros weboldalra vagy felhívhatnak egy emelt díjas telefonszámot is. Másik változata az SMS csatorna kihasználásának az adathalászat, amikor különböző ürüggyel (pl. adategyeztetés) személyes adatokat, bankkártya adatokat kérnek a csalók az ügyfelektől. A megszerzett bankkártya adatokat a bűnözők online vásárlásra is felhasználhatják vagy értékesíthetik a darkneten. Jellemző, hogy a social engineerek ezen a csatornán is igyekeznek kihasználni a pandémia okozta helyzetet. Az US Cybersecurity and Infrastructure Security Agency és a UK's National Cyber Security Centre közleményében [14] egy ilyen módszerre hívja fel a figyelmet. Itt az Egyesült Királyságban lévő állampolgároknak ígérnek pénzt, a koronavírus elleni harchoz. A linkre való kattintással a nevüket, e-mail címüket, lakcímüket és banki adataikat gyűjthetik be a csalók az áldozatoktól.

Kártékony mobilalkalmazás. A támadó először létrehozza magát a káros kódot tartalmazó alkalmazást, ami akár egy játéknak vagy más érdekes alkalmazásnak is tűnhet. Általában ezen funkciót is ellátja a valódi célja mellett. Ezt követően feltölti az alkalmazásokat kínáló webes platformokba, majd várja, hogy a felhasználó az applikáció leírása, ikonja, – esetenként manipulált – pozitív vélemények alapján letöltse az alkalmazást. Mivel a legtöbb esetben az emberek eredetinek hiszik a terméket, így letöltik, majd telepítik az eszközükre. Ezzel már kezdetét is vette az eszköz fertőzése és máris veszélyben vannak a felhasználó hitelesítő adatai (pl. login nevek, jelszavak), mivel azokat elküldheti a malware készítőjének. Vagy rosszabb esetben teljesen átvehetik a kontrollt az áldozat telefonja felett, hozzáférve névjegyzékéhez, fotóihoz, feljegyzéseihez, emailjeihez. A Symantec felmérése szerint 2018-ban minden 36. mobiltelefonon magas kockázati besorolású applikáció volt telepítve vagy rendszergazdai jogosultsággal futottak. Ez utóbbiakat rootolt vagy jailbreakelt eszközöknek nevezzük [15]. Az ilyen telefonok használata nagy biztonsági kockázattal jár. Napi aktualitás vonatkozásában megemlítendő, hogy a Checkpoint 2020. áprilisi beszámolójában [24] 16 különböző káros alkalmazásról ad hírt, melyeket a koronavírus járvánnyal összefüggésben hoztak létre a terjesztői. Ezek hivatalos alkalmazásként tüntetik fel magukat, azonban céljuk a felhasználói adatok ellopása, vagy prémium szolgáltatások generálása révén bevételhez jutni.

Hamis biztonsági alkalmazás. A támadó első lépésben megfertőzi az áldozat számítógépét egy olyan kártékony programmal, ami érzékeli a netbank belépési szándékot.

Ekkor a rendszerképernyőn megjelenő felugró ablakban jelzi a felhasználónak, hogy egy mobiltelefonos alkalmazást kell letöltenie a netbankba való bejelentkezéshez, ugyanis ott fogja megkapni a biztonsági üzenetet. Ezzel a kétfaktoros hitelesítés biztonságérzetét használja ki a támadó, elhitetve az áldozattal, hogy ez egy újabb plusz biztonsági funkció a netbank használatához. Az ajánlott alkalmazás természetesen a támadó által írt applikáció lesz. Amikor a felhasználó letölti az appot a támadó megszerzi a bizalmas információkat úgy, mint banki belépési hitelesítő adatok (felhasználónév, jelszó) és utána a valódi, második faktoros hitelesítő kódot is, amit a bank küld az áldozatnak pl. SMS-en keresztül. Felhasználva ezt az információt, egy támadó hozzáfér az áldozat bankszámlájához és anyagi kárt okozhat neki.

Újracsomagolt alkalmazás. Adott egy mobil alkalmazás, ami azt teszi, amit tennie kell mindenféle kártékony mellékhatás nélkül. A támadó egyszerűen letölti a népszerű applikációt az áruházból majd az általa írt malwaret hozzáadja, mintegy újracsomagolja az alkalmazást és ő is feltölti. Amikor a felhasználó letölti a már rosszindulatú alkalmazást, a kártékony program telepítődik a mobiljára, gyűjti a bizalmas információkat és elküldi azokat a támadónak.

Instant üzenetküldő. Egy támadó instant üzenetküldő alkalmazásokon keresztül online cseveghet a kiválasztott áldozattal. Miután a bizalmába férkőzött, megpróbál személyes információt szerezni tőle, amiket felhasználhat arra, hogy feltörje a felhasználó fiókjait. De összetettebb támadást is indíthat, – használva a korábban említett megszemélyesítéses technikát – egy hamis profilt bemutatva az áldozatnak ráveheti különböző jogcímen pénz utalásra is, abban a hiszemben, hogy ezt később busásan vissza fogja kapni. Ide sorolható még az e fajta platformokon kapott üzenetek, melyekben a közvetlen linke rákattintva káros tartalmak tölthetnek le a telefonunkra. A linkek címe, animált képe első ránézésre megnyerő lehet, érzelmekre, egészségre, pénzügyekre utaló címekekkel ellátva nagy csábítást jelent a megtekintésre. Tartalmazhatnak továbbá csaliként kedvezményes utazáshoz, biztonsági frissítéshez vagy adathalász oldalra irányító linkeket is.

Csaló hívás. A telefonon keresztül elkövetett cselekmények közül a csalások igénylik a legkevesebb technikai ismeretet a támadó részéről. Itt viszont annál inkább szüksége van a már korábban említett manipulációs módszerek igénybevételére, ugyanis csak pár perc áll rendelkezésre, hogy végrehajtsa a műveletet. Nehézsége, hogy kizárólag a verbális kommunikációs csatornát használhatja. A telefonos technikákról szóló rész zárásaként három jellegzetes módszer végrehajtását szeretnénk a humán aspektus oldaláról részletesebben bemutatni.

A Büntetőtörvénykönyvről szóló 2012. évi C. törvény 373. § (1) bekezdése kimondja, hogy aki jogtalan haszonszerzés végett mást tévedésbe ejt vagy tévedésben tart és ezzel kárt okoz, csalást követ el [25]. Az utóbbi időkben elszaporodott úgynevezett „unokázós csalások” is ezen alapulnak. A támadó az esti órákban felhívja az idős, jellemzően egyedülálló áldozatát, majd olyan rövid történetet hitet el vele, melyben az érzelmi ráhatásnak nagy szerepe van. Felderítő tevékenységük során a telefonkönyvekben főként az „özv.” előtaggal vagy a hagyományos „-né” utótaggal szereplő személyeket célozzák meg, akikről feltételezik, hogy egyedül élhetnek. A célszemélyeket néha közösségi portálon vagy

lakóhelyük megfigyelése útján is feltérképezik. A hívó magát valamilyen hatóság munkatársának adja ki és azzal keríti hatalmába az aggódó nagyszülőt, hogy elhiteti vele azt, hogy súlyos közlekedési balesetet okozott a gyereke, unokája. A megfelelő egészségügyi ellátás és a rugalmasabb jogi ügyintézés végett hozzátartozójának azonnali készpénzre van szüksége. Itt kihasználják még a sürgetést (pl. mindjárt viszik a rabkórházba), mint időtényezőt, valamint a kitalált életveszélyes helyzetet (pl. a bordája átszúrta a tüdejét). De olyan is előfordul, hogy kifejezetten megkéri a csaló a sértettet, hogy másnak ne mondja el, mert bajba kerülhet. A készpénzért, vagy ennek hiányában ékszerért már személyesen küldi el a csaló az egyik társát, aki adott esetben rendőrnek adja ki magát, ezzel a hitelesség látszatát keltve a rémült áldozatban. Az érték átadásnál már át is lépett a támadó társa a humán technika megszemélyesítés módszerének a használatához, melyben különböző kellékek (pl. Rendőrség feliratos póló, jelvény, stb.) segítenek szerepe eljátszásában. Az aktualitását ennek a módszernek mi sem mutatja jobban, minthogy a csalók alkalmazkodtak a jelenlegi járványügyi helyzethez: „próbálkoznak telefonon is, egy kórház munkatársának kiadva magukat felhívják valakit, majd azt hazudják, hogy az egyik rokonuk megfertőződött a koronavírussal, és ki kell fizetni az orvosi költségeket” [26].

Az elmúlt években ütötték fel fejüket a „feltöltőkártyás csalások”, ahol az elkövetők általában valamelyik telefonszolgáltató nevével élnek vissza. Jellemzően az emberek hiszékenységére, kapzsiságára utaznak. Felderítő tevékenységük nem túl kifinomult, teljesen véletlenszerűen vagy folyamatos növekvő sorrendbe tárcsázva, naponta akár több száz hívást is lebonyolítanak. ATM-en, POS terminálon vagy SMS küldés útján különböző telefonszámok egyenlegeit töltetik fel a gyanútlan sértettel. Az áldozat ezalatt abban a hiszemben van, hogy eközben gyarapodik a begépelte összeggel a számlája vagy éppen a nyerő kódot üti be, mely a nyereség utalásához szükséges. A valóságban azonban az elkövetők vagy hozzátartozóik használatában lévő telefonszámainak az egyenleg feltöltését hajtják végre. A tévedésbeeső szöveg általában sorsoláson nyert pénznyereség, amit esetenként kombinálni szoktak az elkövetők nagyértékű televízió vagy telefonkészülék ajándékkal is. A sértettek általában a következő havi számlakivonaton értesülnek a csalásról, vagy amikor hívás után felhívták a valós telefonszolgáltatójukat, mert mégis gyanakodni kezdenek. Az áldozatok közül szinte senkinek nem tűnik fel, hogy ha nem regisztráltak semmiféle nyereségjátékban, így nem is nyerhettek azon. De olyan tévedésbe eső szöveg is ismert, amiben csak egyszerűen kötelező előfizetői adategyeztetésre, központi rendszer újraindítása miatti ellenőrzésre, mobilkészülék vírusirtásra vagy biztonsági ellenőrzésre hivatkoznak. Ez esetben a személyes adatok megszerzése a cél, melyet későbbi social engineering támadásokban felhasználnak. Fenti módszer továbbfejlesztett változatában az elkövetők különböző ürüggyel (pl. adóvisszatérítés átutalása) magát a hatóság munkatársának kiadva elkérik a sértettektől a bankkártyájuk adatait, mellyel internetes tranzakciókat bonyolítanak le. Ezek jellemzően webáruházból való vásárlások, valamint telefonkártya egyenleg feltöltések. Mivel ez esetben már konkrét felhasználása történik a bizalmas adatoknak (bankkártya adatok), így az elkövető cselekményével a Btk. 375.§ (1) bekezdésébe ütköző információs rendszer felhasználásával elkövetett csalás bűncselekményét valósítja meg [25]. Információs rendszer vonatkozásában adatbevitelnek, megváltoztatásnak, hozzáférhetetlenné tételnek kell történnie vagy olyan műveletnek, ami a rendszer működését befolyásolja. Ennél a bűncselekménynél jellemzően adatbevitelről beszélhetünk, ami a jogos felhasználó tudta és beleegyezése nélkül zajlik.

Végezetül érdemes megemlíteni a klasszikus „telefon betyárkodás”-t, amit akár az utcai fülkés telefonkészülékkel, akár hagyományos mobiltelefonok felhasználásával is végre lehet hajtani. A Btk. 338.§ (1) bekezdésébe ütköző közveszéllyel fenyegetést követ el, aki a köznyugalom megzavarására alkalmas olyan valótlan tényt állít, híresztel, vagy azt a látszatot kelti, hogy közveszéllyel járó esemény bekövetkezése fenyeget, bűncselekményt követ el [25]. Ami a telefonálónak adott esetben vicces vagy szándékosan szabotáló célú (pl. bírósági tárgyalás elhalasztása), az a rendvédelmi szerveknek erő, eszköz és nagy anyagi ráfordítással járó rendkívüli feladatot jelent. Itt jellemzően bombariadóra kell gondolni, amit elkövettek már pénzügyesek, bíróságok, iskolák ellen is. A hívást fogadó diszpécser ez esetben nem lehet áldozatnak tekinteni, hiszen belső szabályzatok sokasága írja elő az ilyenkor szükséges halaszthatatlan intézkedések megtételét. Nem mérlegelhet a hívás valódiságát illetően az ügyeletes, még ha – tapasztalatai és a háttérzajok alapján – előre sejthető is a hívás komolytalansága.

ZÁRÓ GONDOLATOK

Az informatikai rendszerek, eszközök és alkalmazások használatánál nem a technika, hanem az azt használó ember a leggyengébb láncszem, aki többek között pszichikumából, társas lény voltából, szocializációjából és a társadalmi elvárásoknak való megfelelési kényszerből adódóan viszonylag könnyen és meglehetősen változatos módon manipulálható. Ezt használják ki azok a social engineerek, akik vagy a humán, vagy az IT alapú technikák használatával (de ez utóbbinál is az emberi gyengeségre, hiszékenységre alapozva) információkat szereznek meg áldozatuktól, visszaélnak azzal, vagy az általuk elvárt viselkedésre bírnak rá gyanútlan (és gyakran az elkényelmesedés miatt felelőtlen) felhasználókat. Jelen tanulmányunkban a fontosabb módszereket mutattuk be, s ezen elméleti részzsel, valamint a kapcsolódó példákkal alapoztuk meg tanulmányunk következő részét, amelyikben elsősorban az információbiztonság humán oldalával foglalkozó nagymintás kutatásunk fontosabb eredményeit, valamint az ezekből levonható következtetéseket ismertetjük.

FELHASZNÁLT FORRÁSOK

Irodalom

- [1] PurpleSec's Cyber Security Experts, The Ultimate List Of Cyber Security Statistics For 2019, (letöltve: 2020.04.12.) [online] <https://purplesec.us/resources/cyber-security-statistics/#SocialEngineering>
- [2] M. Guenther, „*Social Engineer - Security awareness series*”, M. Guenther LLC., 2001. [online] <https://www.coursehero.com/file/38974373/> (letöltve: 2020.05.14.)
- [3] K. D. Mitnick, W. L. Simon, „*A legendás hacker – a megtévesztés művészete*”, Budapest: Perfact Pro Kft., 2003.
- [4] EC-Council, Certified Ethical Hacker v10 – Social Engineering Module 09. [online] <https://www.eccouncil.org>
- [5] E. D. Oroszi, „Social engineering technikák”, in.: V. Deák, Ed., *Célzott kibertámadások*, Budapest: NKE, 2018.
- [6] Biblia, Máté 7:7, Budapest: Magyarország Ref. Egyház Kálvin János Kiadója, 1990.

- [7] T. Sörös Tamás, D. Váczi, „*Social engineering a biztonságtechnika tükrében*”, bemutatta XXXI. OTDK Had- és Rendészettudományi Szekció, Budapest, 2013.
- [8] E. D. Oroszi, „*Social Engineering – Az emberi erőforrás, mint az információbiztonság kritikus tényezője*”, B.S. szakdolgozat, Budapesti Corvinus Egyetem, Budapest, 2008.
- [9] J. Crume, „*Az internetes biztonság belülről – amit a hekkerek titkolnak*”, Bicske: Szabad Tér Kiadó, 2003.
- [10] D. Krishnaswamy „World's Worst (Most Common) Passwords,” Security Scorecard.com
<https://securityscorecard.com/blog/worlds-worst-passwords> (letöltve: 2020.04.17.)
- [11] Varonis, 2019 Data Risk Report Stats and Tips You Won't Want to Miss (letöltve: 2020.04.17.) [online] <https://www.varonis.com/blog/data-risk-report-highlights-2019>
- [12] A. O'Donnell „What Is a Road Apple Social Engineering Attack?” Lifewire.com, <https://www.lifewire.com/what-is-a-road-apple-social-engineering-attack-2487194> (letöltve: 2020.03.12.)
- [13] RSA Quarterly Fraud Report Vol. 2, Issue 4, Q4 2019. (letöltve: 2020.04.17.) [online] <https://www.rsa.com/en-us/offers/rsa-fraud-report-q4-2019>
- [14] US DHS CISA and the UK NCSC, Alert (AA20-099A) COVID-19 Exploited by Malicious Cyber Actors [online] <https://www.us-cert.gov/ncas/alerts/aa20-099a> (letöltve: 2020.04.19.)
- [15] Symantec Internet Security Threat Report Volume 24, 2019. február [online] [symantec.com](https://www.symantec.com)
- [16] IBM Security X-force Threat Intelligence Index 2020. (letöltve: 2020.03.12.), [online] [ibm.com/security/data breach/threat intelligence index](https://www.ibm.com/security/data-breach/threat-intelligence-index)
- [17] ESET, Zsarolóvírus, (letöltve: 2020.03.12.), [online] <https://www.eset.com/hu/zsarolovirus/>
- [18] F. Mouton, L. Leenen, M. M. Malan and H.S. Venter, „Towards an Ontological Model Defining the Social Engineering Domain”, In: K. Kimppa et al., Eds. *ICT and Society*. HCC 2014. IFIP Advances in Information and Communication Technology, vol 431. Berlin, Heidelberg: Springer, 2014.
- [19] Kitekintés az elmúlt évek legsúlyosabb kiberbotrányaira, Securinfo.hu <https://www.securinfo.hu/termekek/it-biztonsag/8403-kitekintes-az-elmult-evек-legsulyosabb-kiberbotranysaira.html> (letöltve: 2020.03.12.)
- [20] CrowdStrike 2020 Global Threat Report, (letöltve: 2020.03.12.), [online] [crowdstrike.com/reports](https://www.crowdstrike.com/reports)
- [21] Interpol, Cybercriminals targeting critical healthcare institutions with ransomware, [Interpol.int https://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware](https://www.interpol.int/en/News-and-Events/News/2020/Cybercriminals-targeting-critical-healthcare-institutions-with-ransomware) (letöltve: 2020.04.19.)
- [22] G. Szappanos, „*Kirándulás a számítástechnika sötét oldalára*”, Budapest: VirusBuster Kft., 2003.
- [23] S. Chernyshev, D. Chipiristeanu, „*Less aggressive, more effective: social engineering with paid archives*,” VB2012, Dallas [online] Elérhető: https://www.virusbulletin.com/uploads/pdf/conference_slides/2012/ChernyshevChipiristeanu-VB2012.pdf
- [24] A. Hazum, O. Mana, I. Wernik, B. Melnykov and C. Efrati „COVID-19 goes mobile: Coronavirus malicious applications discovered,” Check Point, 2020.04.09, (letöltve:

- 2020.04.19.) [online] Elérhető:<https://research.checkpoint.com/2020/covid-19-goes-mobile-coronavirus-malicious-applications-discovered/>
- [25] 2012. évi C. törvény a Büntető törvénykönyvről
- [26] Origo, A rendkívüli időszakban még inkább az idősekre vadásznak a csalók, Origo.hu [online] <https://www.origo.hu/itthon/20200318-unokazos-modszerrel-a-koronavirusra-hivatkozva-keresik-a-csalok-az-idosebbeket.html> (letöltve: 2020.04.19.)
- [27] C. Hadnagy, „*Unmasking the Social Engineer – The human element of security*”, Hoboken: Wiley, 2014.

**COVID-19 PANDEMIC ON THE AFRICAN
CONTINENT****COVID-19 PANDÉMIA AZ AFRIKAI
KONTINENSEN**BESENYŐ János¹, KÁRMÁN Marianna²**Abstract**

The emergence of the COVID-19 pandemic has required action by individual governments in all countries of the world following health, political and economic considerations. These provisions were first used to prevent then to stop the spread of infection. As globally, in Africa too, the question arises as for what reason and with what efficiency have these provisions worked or are they operating, and what impact do they have on the lives of African societies. Africa's health preparedness has received strong criticism on a number of levels, yet, according to current data, the continent is slightly infected by the coronavirus. In addition African governments have taken austerity measures that are among the most stringent in the world, and now one of the biggest difficulties in fighting against the coronavirus is the emergence of mass starvation, which experts predicted for 2020 based on several factors even before the coronavirus appeared.

Keywords

Africa, COVID-19, social effects of coronavirus, crisis

Absztrakt

A COVID-19 pandémia megjelenése a világ minden országában egészségügyi, politikai és gazdasági mérlegeléseket követő intézkedéseket követelt meg az egyes kormányoktól. Ezek a rendelkezések eleinte a megelőzést, majd a fertőzés terjedésének megakadályozását szolgálták. Ahogy globálisan, úgy Afrikában is felvetődik a kérdés, hogy ezek a rendelkezések milyen megfontolásból és milyen hatásokkal működtek vagy működnek, és milyen hatást gyakorolnak az afrikai társadalmak életére. Afrika egészségügyi felkészültsége számos szinten kapott erős kritikát, mégis a jelenlegi adatok alapján a kontinens arányaiban kismértékben fertőzött a koronavírus által. Mindezek mellett az afrikai kormányok olyan megszorító intézkedéseket hoztak, melyek a legszigorúbbak közé tartoznak a világon, és a koronavírus elleni harcban az egyik legnagyobb nehézséget a tömeges éhínség megjelenése okozza, melyet már a koronavírus megjelenése előtt is több tényezőre alapozva megjósoltak a szakértők a 2020-as évre.

Kulcsszavak

Afrika, COVID-19, a koronavírus-járvány társadalmi hatásai, válság

¹ beseny.janos@phd.uni-obuda.hu | ORCID: 0000-0001-7198-9328 | researcher / afrikanista, történész | Óbuda University Doctoral School of Safety and Security Sciences, African and Historical Studies / Óbudai Egyetem Biztonságtudományi Doktori Iskola, Afrika Kutató Központ

² karman.marianna@phd.uni-obuda.hu | ORCID: 0000-0002-9907-5082 | researcher / afrikanista, iszlámkutató | Óbuda University Doctoral School of Safety and Security Sciences, African and Historical Studies / Óbudai Egyetem Biztonságtudományi Doktori Iskola, Afrika Kutató Központ

AFRIKA EGÉSZSÉGÜGYI FELKÉSZÜLTSEGE A COVID-19 KONTINENSEN VALÓ MEGJELENÉSE ELŐTT

A COVID-19 megjelenése és Kínán kívüli terjedése után az egész világ rettegve figyelte az amúgy is törekeny afrikai egészségügyi rendszerek reakcióját a vírus rohamos terjedésére. 2020. január 30-án a WHO pedig arra figyelmeztetett, hogy a koronavírus afrikai elterjedése magas kockázatot rejt magában, hiszen a nagy népsűrűségű nyomorregyedekben, illetve menekülttáborokban élők különösen ki van szolgáltatva a vírus terjedésének. Dr. Michel Yao, a WHO közép-afrikai képviselője pedig azt is hangsúlyozta egy interjúban, hogy Afrika egyértelműen nem áll készen egy koronavírus okozta járvány megállítására. [1]

Az egészségügyre fordított közkiadások Afrikában mozognak a legalacsonyabban a világon. Az alacsony nemzeti költségvetés és a humanitárius formában segítséget nyújtó országok következtelen támogatása miatt Afrikának 66 milliárd dolláros hiánya keletkezik az éves egészségügyi kiadások terén. [2] Kenyában, Nigériában és Zimbabwében, valamint a térség más részein az egészségügyi dolgozók szinte már rutinszerűen sztrájkolnak az alacsony fizetés, a hátralékok és a hétköznapi ellátásban fennálló drasztikus eszközhiány miatt – ezek olyan egyszerű eszközökre terjednek ki, mint például a kötszer vagy a gumikesztyű. [3] Az afrikai egészségügyi rendszerekben jelentős az egészségügyi szakemberek hiánya: 5000 emberre jut egy orvos (Magyarországon ez az adat kiemelkedően magas 20-22 orvos/5000 fő a KSH adatai szerint, míg az Egyesült Királyságban 14 orvos/5000 fő). [4] Ezek az állapotok olyan egészségügyi helyzethez vezetnek, amelyben az egészségügyi rendszerek számára küzdelmet jelent a rendszeres egészségügyi ellátás biztosítása is.

A koronavírus elleni felkészülésben az Afrikát „hagyományosan” támogató országok a járvány egész világra való kihatása miatt kevésbé fordítottak figyelmet az afrikai egészségügyi helyzet javítására. Mindezek mellett a Kínával való gazdasági kapcsolatok ellehetetlenülésével, az olajárak év eleje tartó csökkenése és a Kelet-Afrikában pusztító sáskajárás miatt [5] az afrikai országok különösen nehéz gazdasági helyzetbe kerültek, amelynek következtében szinte elképzelhetetlennek tűnt az egészségügyi helyzet gyors felkészítése – nemhogy a járvány megfékezésére, de megelőzésére is.

Afrika Járványügyi Ellenőrzési és Megelőzési Központja (Africa CDC) február 3-án hozta létre az új Afrika Koronavírus munkacsoportját, mely a WHO-val együttműködve végzi tevékenységeit: a megfigyelés területén, ideértve a belépési pontok átvilágítását, a fertőzések megelőzését és ellenőrzését az egészségügyi intézményekben; a súlyos koronavírus-fertőzésben szenvedők klinikai kezelését, a laboratóriumi diagnózist, valamint a kockázatokkal kapcsolatos kommunikációt és a közösségi részvételt. [6]

Az Egyesült Nemzetek Egészségügyi Szervezete erőfeszítéseinek nagy részét a kontinens 13 kiemelt prioritással rendelkező országára összpontosította. A kiemelt fontosságú országok listáján elsősorban olyanok szerepeltek, amelyek vagy közvetlen járatokat szoktak indítani Kínába, vagy nagy mennyiségű utazót vonzanak Kínából. Ide tartozik Algéria, Angola, Elefántcsontpart, a Kongói Demokratikus Köztársaság, Etiópia, Ghána, Kenya, Mauritius, Nigéria, Dél-Afrika, Tanzánia, Uganda és Zambia. [7]

A kiemelt országokon kívül még azokban az országokban is, ahol instabilitás van, mint például Dél-Szudánban, koordinációs mechanizmusokat dolgoztak ki az egészségügyi dolgozók és a betegek elérése érdekében. Az Ebola-járványoknak „köszönhetően” az afrikai országok többségében már megvan az izolációs infrastruktúra.

A Kongói Demokratikus Köztársaságban az év elején még mindig tartott a 2018 októberében kitört Ebola-járvány, amely akkorra már lecsendesülőben volt – összesen több mint 3000 regisztrált esettel és több mint 2000 halottal. [8] Ez a járvány egyelőre a második legnagyobb Ebola-fertőzés a 2014-es nyugat-afrikai Ebola-járvány után, melynek során 28616 ember betegedett meg, és 11310-en haltak meg Guineában, Libériában és Sierra Leonében. A járvány során az orvosok az izolált, vidéki területeket helyezték előtérbe, így mire a városokba ért a betegség, a túlnépesedett területeken óriási pusztítást tudott végezni. A helyzetet megnehezítette, hogy az ápolók és az egészségügyi szakemberek nem tették meg a megfelelő megelőző intézkedéseket, ami egyre növekvő fertőzési arányt eredményezett. A védőfelszerelés és a megfelelő képzés hiánya szintén súlyosbította a terjedést, és az egészségügyi rendszer kezdett összeomlani. Az utcán heverő holttestek drámai képe alapján úgy tűnt, hogy a kormányok nem voltak felkészülve a járvány kitörésére, ami még inkább zavart és félelmet keltett a közvéleményben. Sokan úgy vélték, hogy az Ebola-járvány egy hazugság, amit a vezetés talált ki azért, hogy több nemzetközi segítséghez jusson, ezért a kormány megelőző és védekező rendeleteit figyelmen kívül hagyták. [9] A fertőzések csökkenését végül a lakosság magatartásának és hozzáállásának megváltoztatása okozta. Ez mindenképp egy olyan példa, amelyet Afrika szem előtt tart a COVID-19 Kínán kívül való megjelenése óta.

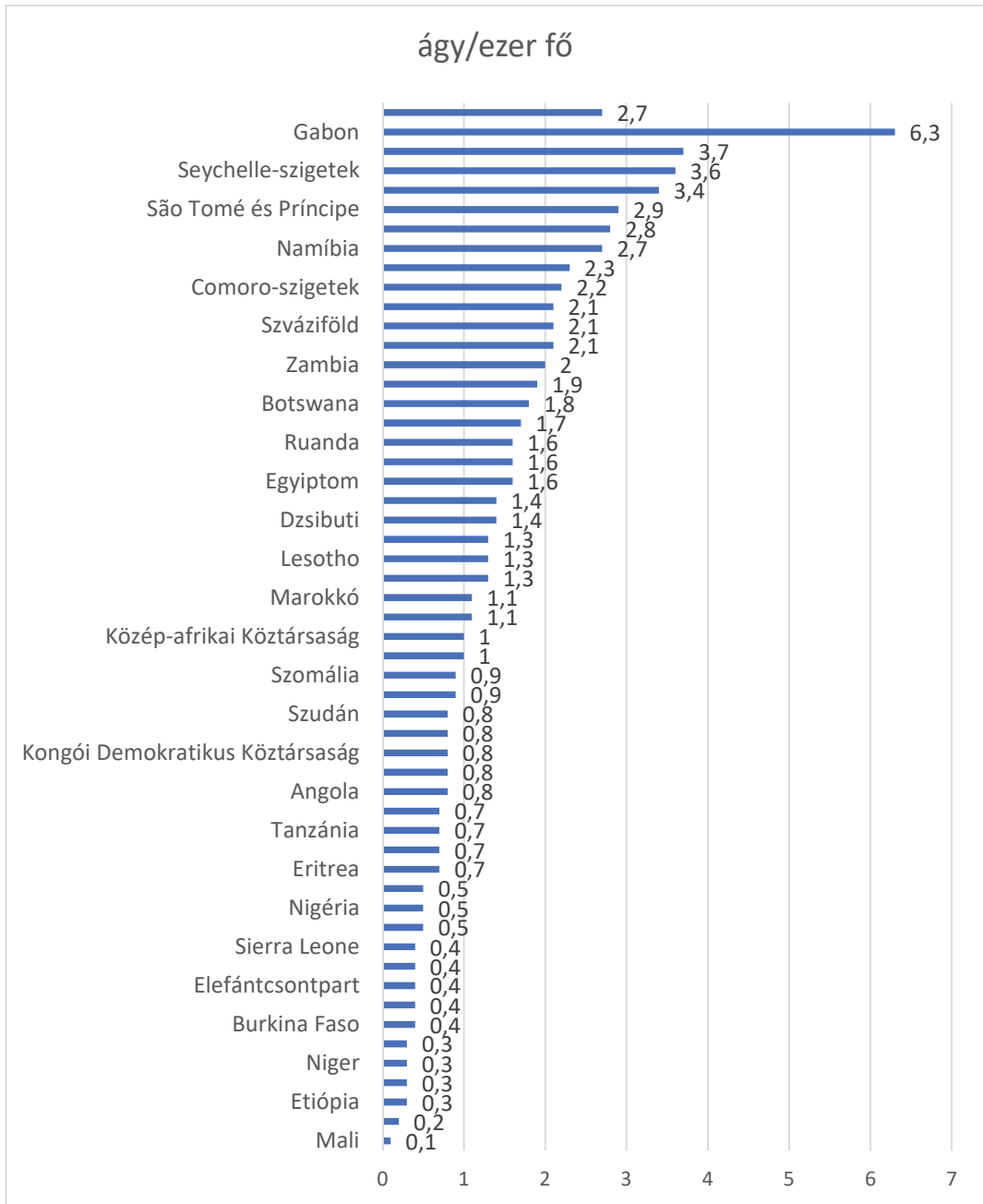
A koronavírus Kínában való tömeges megjelenése az afrikai kormányokat a gyors cselekvésre indította, és mindenekelőtt a megelőzésre fordították figyelmüket, tudva azt, hogy ha COVID-19 bekerül a szubszaharális térségbe az afrikai országok akkori gazdasági és egészségügyi helyzete nem teszi lehetővé a járványok megállítását – különösen, ha az a sűrűn lakott területeket is eléri. A vírus afrikai terjedésének megakadályozása érdekében az országoknak rendelkezniük kellett olyan mechanizmusokkal, amelyek a tünetekkel küzdő embereket felismerik, elkülönítik, vírusmintákat gyűjtenek, ezeket a mintákat laboratóriumokba küldik, majd a megerősített eseteknek a kezelést biztosítják. Az egészségügyi dolgozókat és a laboratóriumi technikusokat szintén ki kellett képezni a vírus kezelésére szolgáló protokollok kidolgozására, valamint védőfelszereléssel kellett rendelkezniük. [10]

A gyenge laboratóriumi kapacitás a kontinens számos országában problémát jelentett, és amíg kereskedelemben még nem állt rendelkezésre diagnosztikai vizsgálathoz szükséges teszt, azokat is a WHO biztosította azon afrikai országok számára, amelyek a járvány afrikai megjelenéséig nem voltak felszerelve. A mintákat a WHO laborjai számára küldték el, ahol tesztelték a mintákat, majd visszaküldték, így több országban is akár napokig eltartott a diagnózis felállítása. Annak ellenére, hogy a Világszervezetnek 28 helyen van felállított laboratóriuma, mindössze kettőben voltak koronavírus-tesztek: Dél-Afrikában és Szenegálban. [11]

Február 4-ig további országok - Ghána, Madagaszkár, Sierra Leoné és Nigéria – szintén képesek lettek tesztelni magukat, majd egy hét után további 11 ország rendelkezett tesztlehetőséggel, így gyorsabb lett a teszteredmények elérhetősége. [12]

A megelőzés érdekében a WHO felkérte az afrikai országokat, hogy készítsenek készenléti terveket, amelyek a lehetséges esetek és az ellátási készülség statisztikáját foglalják magukban. Hasonlóval kellett készülni a Kongóval szomszédos országoknak az Ebola kitörése idején is. [13]

További aggodalomra adnak okot a lakosság széles körében olyan elterjedt fertőző betegségek, mint a HIV vagy a TBC, melyek felerősíthetik COVID-19 okozott megbetegedések súlyosságát. [14]



1. Ábra: Kórházi ágyak száma Afrikában, saját szerkesztés, WHO

MEGELŐZÉSI ÉS VÉDEKEZÉSI STRATÉGIÁK

Február közepéig az afrikai országokban többek között utazási korlátozásokat vezettek be (pl. Gabon megtiltotta a Kínából történő beutazást az ország területére, [15] Mozambikban nem adtak ki több vízumot kínai állampolgároknak [16]), határozatlan időre megszakították a gazdasági, kereskedelmi kapcsolatokat Kínával (pl. Kamerun megtiltotta az élelmiszerimportot Kínából [17]), a Kínában rekedt állampolgárokat – főleg diákokat a WHO fokozott ellenőrzése alatt engedték hazautazni (pl. 5000 zambiai diák tanult Kínában, ebből 186 Vuhanban, evakuálásukat Zambia sokáig nem engedélyezte a szülői követelések ellenére sem [18]), illetve tesztelés nélkül ugyan, de karanténban tartottak veszélyeztetett területről érkező beutazókat (Sierra Leone [19]).

Dél-Afrikában 100 regisztrált eset után Cyril Ramaphosa elnök katasztrófa-helyzetet hirdetett, korlátozva az utazást, elrendelve az iskolák bezárását, a tömeggyűlések tilalmát és a bárók működésének korlátozását: bezárás vagy a létszám korlátozása max. 50 főig. A dél-afrikai országban az a személy, aki koronavírus-intézkedéseket megsérti, pénzbírsággal vagy akár börtönbüntetéssel is sújtható. Az ország betiltotta a kikötői forgalmat minden kikötőjében.

Március folyamán az afrikai nemzetek a Dél-Afrikához hasonló szankciókat vezettek be:

- Lagos állam, Nigéria gazdasági központja, megtiltotta a több mint 50 fős összejöveteleket, az iskolák bezártak; Afrika legnépesebb országa, ahol a szankciók bevezetésekor összesen tizenkét koronavírusos esetet találtak, megtiltotta azon repülőjáratok leszállását, amelyek olyan országokból érkeznek, ahol több mint 1000 fertőzést regisztráltak már.
- Algéria, az egyik legsúlyosabban érintett afrikai ország, bezárta határait és leállította a repülőjáratokat. Az elnök betiltotta a tömeges összejöveteleket is, amelyek egyúttal véget vetettek a nagy kormányellenes tüntetések szervezésének.
- Ruanda kormánya 11 eset jelentése után megtiltotta az utasszállítást, a hó végén pedig ételadományokat osztott a kialakult éhínség miatt.
- Kenyában, talán a kontinens egyik legvallásosabb országában, a legtöbb templomban és mecsetben felfüggesztették az istentiszteletet. A kormány azt is bejelentette, hogy állami szinten fog fertőtlenítőt gyártani, amit ingyen forgalmaznak majd annak érdekében, hogy orvosolják a fellépő hiányt.
- Libériában, ahol néhány évvel ezelőtt az ebola-járvány volt a figyelem központjában, két nyilvántartott Covid-19-es eset regisztrálása után abbahagyták az útlevelek kiadását az emberek utazásának megállítása érdekében, és megtiltották az olyan országokból való belépést, amelyek a világjárvány által leginkább sújtottak.
- Zambia két Covid-19-es eset jelentése után bezárta a parlamentet, az iskolákat és az egyetemeket.
- Szomália egyetlen esettel bezárta légtérét.
- Uganda és Botswana, ahol még akkor nem volt egyetlen eset sem, bezárta az iskolákat. [20]

Március közepére Afrika majdnem minden országában jelen volt a koronavírus alacsony esetszámában. Az egészségügyi felkészültség a terjedés megakadályozására azonban még mindig elégtelen volt.

- Afrika egyik legjobb egészségügyi rendszerével Dél-Afrika rendelkezik, ez azt jelenti, hogy 56 millió lakosra kevesebb mint 1000 intenzív osztályos ágya volt, közülük 160 magánszektorban.
- Malawiban körülbelül 25 ICU ágy található állami kórházakban 17 millió emberre, míg Kenyában 50 millió emberre 578 intenzív ágy jut – ami szintén rendkívül alacsony arány.
- A zimbabwei fővárosban, Harareban a fő fertőző betegségek kórházában nem volt hely - mondta a Zimbabwei Emberi Jogi Orvosok Szövetsége.
- Nigéria, Afrika legnépesebb országa arra törekedett, hogy izolációs ágyakat hozzon létre, és speciális orvosi képzést és felszerelést biztosítson az állami kórházakban, de továbbra is csak a megelőzés és a korai felismerés feladatát tudták megfelelően ellátni Chikwe Ihekweazu, Nigéria Betegségek Ellenőrzési Központjának vezetője szerint. [21]
- Uganda fokozott vészhelyzetet hirdetett a térségben kialakult fertőzöttség miatt, de nem számítottak nagyszámú kritikus esetek kezelésére, Nigériához hasonlóan elsősorban a megelőzésre koncentráltak közösségi tudatosságnövelő kampányokkal és közoktatási formában. Jane Ruth Aceng, ugandai egészségügyi miniszter azt mondta, hogy Uganda „legendő kapacitással rendelkezik az esetleges kitörés kezelésére ágyak, ICU egységek tekintetében”, de kijelentését sokan kétségbe vonták, hiszen a 44 milliós kelet-afrikai ország elsősorban az 1500 kórházi ágyas Mulago National Referral Hospital-ra támaszkodik, ahol 60 beteget képes befogadni az intenzív osztály.
- Szomáliában, Dr. Fawziya Abikar egészségügyi miniszter nyilatkozta, hogy a kormány karantén-létesítményt hozott létre a mogadishui repülőtéren, és kórházat épített fel a Covid-19 esetek kezelésére. Ez azonban mindössze 15 elkülönítő sátrat jelent, a kórházban pedig összesen 100 ágy van.
- Dél-Szudánban, amelyet az ötéves polgárháború teljesen lepusztított, a kormánynak csupán 24 elkülönített ágya van.

Március végére a kontinens nagy része elszigetelte magát a világtól: az afrikai országok nagy része felfüggesztette az Európába és Ázsiába érkező vagy onnan induló repülőjáratokat és más közlekedési kapcsolatokat, vagy szigorúan ellenőrzi a területére történő belépést. A nyilvános összejövetelekre, iskolákra és vallási szolgálatra is korlátozásokat szabtak, megszüntették a tömegrendezvényeket a kontinens egész területén. [22]

A VÍRUS MEGJELENÉSE, ELTERJEDÉSE, KORLÁTOZÁSOK BEVEZETÉSE [23]

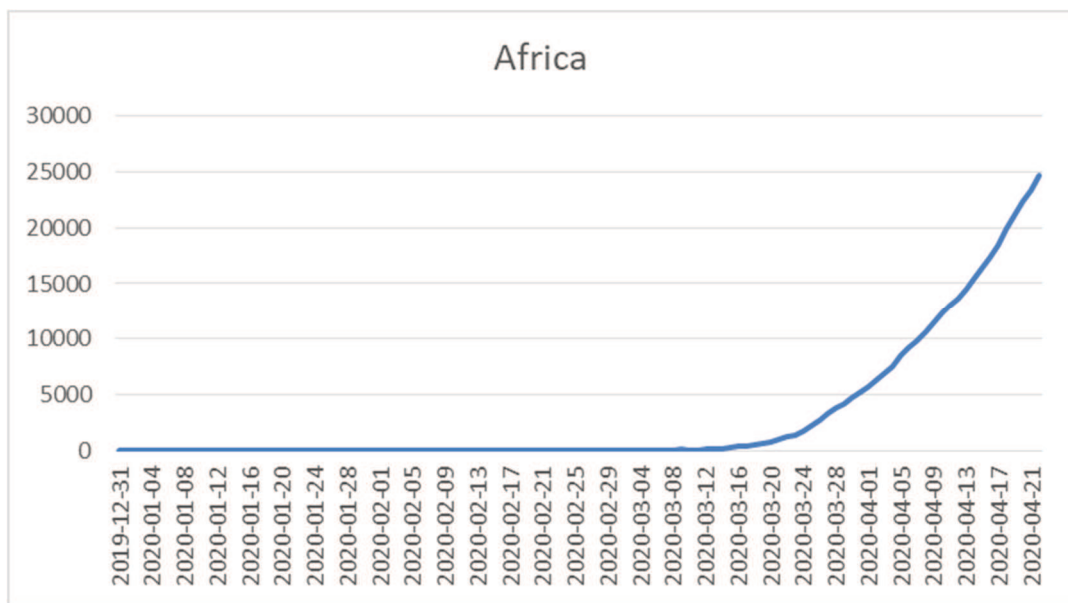
Az első afrikai fertőzöttet, Senou Pavel Daryl kameruni diákot 2020. január 28-án vették fel a Jingzhou Kórházba, Kínában. [24] Az afrikai diák Wuhanba tett utazása során érintkezhetett a vírussal. A kórházban 13 napra izolálták, antibiotikummal és HIV-betegek kezelésére használt gyógyszerekkel kezelték. Két hét ápolás után már a gyógyulás jeleit mutatta, így ő lett nemcsak az első afrikai fertőzött, hanem az első afrikai gyógyult is. [25] Kínában több ezer afrikai diák került karanténba, többen megbetegedtek, de a Kína által biztosított egészségügyi ellátás minősége miatt nem is tértek vissza hazájukba sem a járvány kezdete, sem pedig a tetőzése idején.

Február 14-én jelentették az első koronavírusos esetet a kontinensen: Egyiptomban. A fertőzött egy kínai állampolgár volt, akit a kairói nemzetközi repülőtéren felállított ellenőrzések során szűrtek ki, bár a helyszínen nem mutatta a betegség tüneteit. [26]

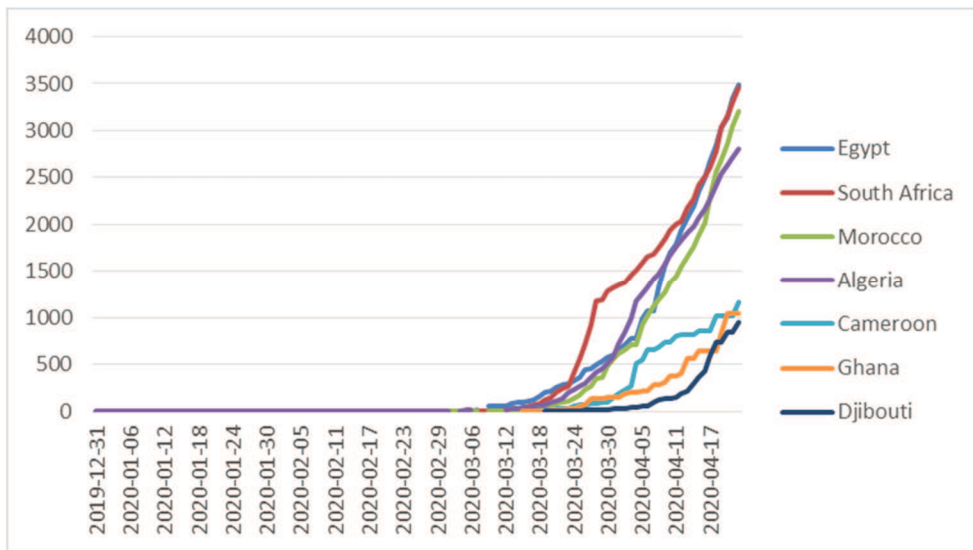
Február 25-én jelentették az első esetet a szubszaharális térségből: az első megbetegedést Nigériában, az egykori fővárosban, Lagosban igazolták egy olasz vállalkozónál, aki Milánóból érkezett a nyugat-afrikai országba. [27][28] Ugyanezen a napon állapították meg az első esetet Algériában, szintén egy olasz férfinél, akit három nappal később Olaszországba deportáltak. [29]

A második szubszaharális térségben megjelenő fertőzést március 2-án regisztrálták Szenegálban, a nyugat-afrikai országban élő francia állampolgárnál, aki korábban Franciaországban volt sielni. [30] Még aznap Marokkóban is egy Olaszországban élő marokkói állampolgárnál állapították meg koronavírus-fertőzést, illetve egy szintén olaszországi lakcímmel rendelkező 89 éves marokkói asszony tesztje lett pozitív. [31] Tunéziában is ezen a napon regisztrálták az első esetet, egy 40 éves tunéziai férfinél, aki Olaszországból tért haza. [32]

Március 5-én jelentették az első esetet Dél-Afrikában, egy Olaszországból hazatérő dél-afrikai állampolgár lett beteg. [33]

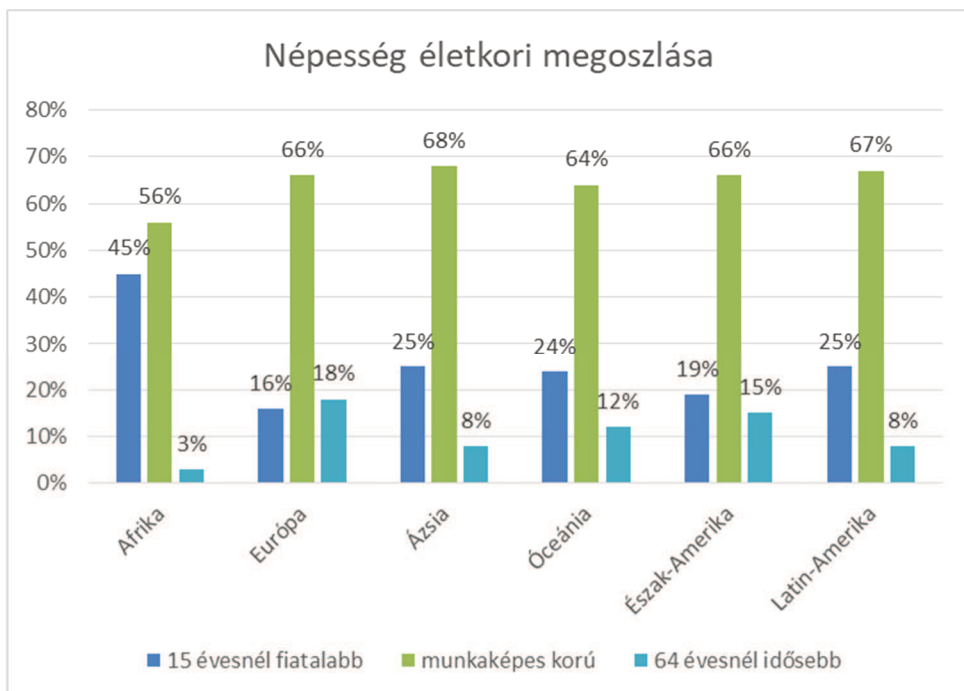


2. Ábra: Koronavírusos esetek számának növekedése Afrikában, saját szerkesztés, WHO



3. Ábra: Koronavírusos esetek számának növekedése a legfertőzöttebb országokban, saját szerkesztés, WHO

Jelen tanulmány írásakor (2020. április 22.) a rendelkezésre álló adatok szerint a COVID-19 elterjedése alacsonyabb mértékű, mint más régiókban, ami egyes feltételezések szerint a kontinensen élők átlagéletkorának, [34] mások szerint az éghajlati körülményeknek köszönhető – egyik feltevés sem bizonyított.



4. Ábra: Átlag életkor Afrikában és a világban, saját szerkesztés, US Population Reference Bureau

Afrikában a lakosság átlag életkora kevesebb mint 20 év, a népesség mindössze 3 %-a idősebb 65 évnél, viszont a népesség 43 %-a nagyvárosokban él, ami kétségtelenül növeli a vírus gyors terjedésének kockázatát.

Afrikában jelenleg összesen 25426 fertőzöttet regisztráltak, 1197-en haltak meg a betegség miatt, 164 fő intenzív ellátást kap. Afrikában összesen 6780 fő gyógyult fel teljesen a vírushalálból.

A legsúlyosabban fertőzött országok: Egyiptom (3490), Dél-Afrika (3465), Marokkó (3209), Algéria (2811), Kamerun (1163) és Ghána (1042). 38 országban jelentettek COVID-19 által okozott haláleseteket, ezek közül a legtöbbet Algériában (392), 100 feletti esetszámot összesen még két országban (Egyiptomban 264, Marokkóban 145) regisztráltak.

A Comore-szigetek és Lesotho nem regisztrált eddig koronavírusos eseteket, bár 2020. április 15-én Mayotte-ban egy Comore-szigetéről érkezőnél állapítottak meg COVID-19 típusú fertőzést. [35]

A koronavírus afrikai megjelenésének és a kontinensen való lassú, de folyamatos terjedésének következtében az afrikai kormányok egyre szigorúbb intézkedéseket hoznak.

Március végén Nigériában és Ghánában a legnépesebb városokat és államokat, a Kongói Demokratikus Köztársaságban a fővárost zárták le és rendeltek el részleges kijárási tilalmat. Botswanában az első esetek után 28 napos korlátozást vezettek be, hasonlóan az egyelőre eset nélküli Lesothóban is. [36] Szenegálban számos afrikai országhoz hasonlóan éjszakai kijárási tilalmat vezettek be, Elefántcsontparton is fokozatosan korlátozták a lakosság érintkezésének lehetőségeit. [37] Többek között Dél-Afrikában, [38] Kenyában, Nigériában és Ugandában a kijárási tilalom betartása katonai és a rendőri ellenőrzés alatt folyik. A legtöbb afrikai ország lezárta határait és valamilyen szintű korlátozást és/vagy kijárási tilalmat rendelt el.

Áprilisban ezek az intézkedések egyre szigorúbbak lettek.

- Április 9-én Dél-Afrika meghosszabbította az éjszakai kijárási tilalmat április végéig. [39] A korlátozások betartásához 70000 katonát vezényelt ki. [38]
- Kenyában a hónap végéig korlátozásokat rendelt el Uhuru Kenyatta elnök április első hetében – még húsvét előtt. A fertőzött területeken és a fővárosban utazási és kijárási tilalmat, míg egyéb területeken éjszakai kijárási tilalmat hirdettek. [40]
- Április 18-án Szudán elrendelte a főváros, Kartúm lezárását három hétre, miután a napi esetszám hirtelen 20-30 főre emelkedett. Mivel a fertőzöttek 90%-a Kartúmhoz köthető, részleges kijárási tilalommal le lett zárva a főváros. [41]
- Marokkóban szintén meghosszabbították a március 20-án bevezetett korlátozásokat, mely alapján az emberek csak élelmiszer- vagy gyógyszervásárlás, illetve nélkülözhetetlen munka végzése miatt hagyhatják el otthonaikat. Az iskolák, a mecsetek, az üzletek és a szórakoztató helyek bezártak. Marokkó kötelezővé tette a maszkok viselését olyannyira, hogy akik elmulasztják, a pénzbírságot és a börtönbüntetést kockáztatják. A marokkói városokban hangszóróval felszerelt autók hívják fel az emberek figyelmét, hogy maradjanak otthon. A tömegközlekedési eszközöket, az utcákat és a piacokat folyamatosan fertőtlenítik. [42]
- Zimbabwében továbbra is tartanak a korlátozások, amelyet március 21-én vezettek be. Egyes pontokon enyhített a kormány. A legnagyobb problémát azonban még

mindig az orvosokkal való együttműködés jelenti. Az orvosi védőfelszerelések hiánya miatt a zimbabwei orvosok pert indítottak a kormány ellen.

- Líbiában a ramadán kezdetével a Nemzeti Egyetértés Kormánya (GNA) 24 órás kijárási tilalmat vezet be, hogy megpróbálja enyhíteni az egészségügyi rendszerre nehezedő nyomást az általa ellenőrzött területeken, ideértve Tripolit is. A polgárháború által sújtott észak-afrikai országban csak kenyér és étel vásárlása lesz engedélyezett, az is kizárólag reggel. [43]

Az elmúlt hónapokban bevezetett korlátozások, ahogy a világ más részein is hatást gyakorolnak az adott ország gazdasági, politikai és társadalmi helyzetére az egészségügyi helyzet javítása érdekében.

A COVID-19 VILÁGJÁRVÁNY GAZDASÁGI, POLITIKAI ÉS TÁRSADALMI HATÁSAI AFRIKÁBAN

A koronavírus megjelenése Kínában nagymértékben kihatott az ázsiai ország afrikai kapcsolataira mind turisztikai, mind gazdasági és diplomáciai szempontból. Az afrikai országok folyamatosan szüntették meg a kapcsolatot Kínával. Törölték a Kínába tartó repülőjáratokat, utazási korlátozásokat vezettek be, megtagadták a vízumkiadást kínai állampolgárok számára, míg végül teljesen lezárták határaikat. Ez az elszigetelődés azonban ideiglenes volt. Mióta Kínában jelentősen csökkent a koronavírusos megbetegedések száma, újra aktívan részt vesz a kontinens gazdasági és egészségügyi helyzetének támogatásában.

Afrika gazdasági helyzetét nemcsak a Kínával való kapcsolatok ideiglenes megszakadása rontotta. Éppen a koronavírussal való globális küzdelem közepén érte el a világot a már korábban előre jelzett energiaválság, melynek következtében az olajárak az elmúlt 25 év legmélyebb pontjára kerültek. A Nemzetközi Energiaügynökség (IEA) pedig azt mondta: „Még ha azt is feltételezzük, hogy az utazási korlátozások enyhülnek az év második felében, akkor is arra számítunk, hogy a globális olajszükséglet 2020-ban napi 9,3 millió hordóval csökken 2019-hez képest, ami egy évtizednyi növekedést semmisít meg.” [44]

A kontinens a koronavírus terjedését követően a légiközlekedésben okozott veszteségekkel is meg kell, hogy küzdjön. Az afrikai légitársaságok akár 4,4 milliárd dolláros bevételt veszítettek el, miután a COVID-19 miatt repülőjáratokat töröltek el és nemzetközi repülőterek zártak be.

A Világbank becslése szerint „a Covid-19 a régióknak 37 és 79 milliárd dollár közötti kibocsátási veszteséget fog okozni 2020-ra a járvány kombinált hatásai miatt”, ideértve a kereskedelem zavarát és a csökkenő átutalásokat, az idegenforgalom és a külföldi segélyek csökkenését.

Míg a régió legtöbb országában a növekedés visszaesése tapasztalható, "a reálbruttó hazai termék növekedése az előrejelzések szerint különösen a régió három legnagyobb gazdaságában fog hangsúlyosan csökkenni – Nigériában, Angolában és Dél-Afrikában – a tartósan gyenge növekedés és csökkenő befektetések következtében"- írja a Világbank jelentése. [45]

A koronavírus megjelenése óta a megszakított mezőgazdasági termelés és élelmiszerimport következményeképpen az egyik legnagyobb veszély az éhezés. Az afrikaiak jövedelmük legnagyobb részét élelemre költik (szemben az amerikaiakkal, akik mindössze

fizetésük 9,7%-át költik ételre. Etiópiában már több mint 1 millió ember veszítette el munkáját. Az idei rendkívüli sáskainvázio miatt pedig Kelet-Afrikát már korábban is az éhínség fenyegette. A munka elvesztésének és az éhezés veszélyének árnyékában a társadalom szegénységben élő rétegei nem tehetik meg, hogy nem hagyják el otthonaikat, így a kijárási korlátozások betartása egyes országokban erőszakos rendőri fellépést eredményez.

Több afrikai ország felismerve a szokásosnál is nehezebb társadalmi körülményeket különböző formában próbálja enyhíteni a lakosság nehézségeit. A Dél-Afrikai Köztársaságban a Dél-Afrikai Statisztikai Hivatal számos gazdasági területen végez felméréseket a koronavírussal kapcsolatos korlátozások következtében kialakult üzleti helyzetről, nehézségekről. Ennek érdekében a hivatal nemrégiben online kvalitatív felmérést indított a COVID-19 vállalkozásokra gyakorolt hatásainak megértése céljából. [46] Emellett Dél-Afrika ígéretet tett arra, hogy minden hajléktalan személynek szállást fognak biztosítani.

Uganda ígérte az élelmiszer-elosztást a kiszolgáltatott lakosság számára, ideértve a szoptató nőket és a nappali munkásokat is, illetve támogatni tervezte a táborokban élő menekülteket is. Áprilisban végül Uganda lezárta határait a menedékkérelmek előtt. Az ENSZ Világélelmiszer-Programjának (UN WFP) területi igazgatója, El-Khidir Daloum azt mondta, hogy a helyi ügynökség 137 millió dolláros finanszírozási forrással küzd (a 219 millió dolláros szükséglethez viszonyítva), ami felveti a kérdést, hogy a 28 menekültügyi településen és az azokon kívül élő kedvezményezettek miként fognak juttatásokat kapni. Mivel az Ugandában élő 1,2 millió menekült nagy részének munkavégzése utazáshoz kötött, illetve a segélyek sem fognak megérkezni, az alultápláltság egészségügyi kockázatai elsősorban őket fenyegetik. [47] Azt is megfigyelték, hogy azok a menekültek, akik nem települések közelében élnek, visszatértek hazájukba. Uganda Afrika legnagyobb létszámú menekülteket befogadó országa – elsősorban Dél-Szudánból és Kongói Demokratikus Köztársaságból érkeznek menedékkérelmeket kérők.

Ruanda 20 000 család támogatására tett ígéretet a fővárosban házról házra járó adományszállítás formájában, de mindkét országban sok más szegénységben élő embert nem fognak elérni ezek a kezdeményezések. [48]

A kialakult krízishelyzet miatt nemcsak a kormányok, önkormányzatok próbálnak enyhíteni a lakosság helyzetén, de a civil szervezetek is részt vesznek nemcsak a humanitárius, de a jogi segítségnyújtásban is. Az emberjogi szervezetek a koronavírus elleni védekezés számos pontján találhatnak jogellenes cselekedeteket egyes afrikai országok részéről.

Az első ilyen cselekmények a kommunikáció ellehetlenítéséről szólnak, mint pl. amikor Egyiptom Kínához hasonlóan kiutasította az újságírókat az országból. Bár tagadhatatlan, hogy Etiópiában a koronavírus miatt pedig éppen hogy feloldották a három hónapja tartó telefon- és internetszolgáltatás általános tilalmát Nyugat-Oromó régióban – de elsősorban a jogi szervezetek tiltakozásának köszönhetően. [49]

A túlzásfoltosságra hivatkozva a jogvédő szervezetek követelték az egyiptomi, líbiai és dél-szudáni politikai foglyok szabadon bocsátását, melynek Egyiptom kisebb mértékben eleget is tett. A vírus terjedésének gócpontjaiként hívták fel a figyelmet a Nigériában, Szudánban és Dél-Szudánban levő menekülttáborok állapotára.

Mivel a koronavírus a kontinensen kívülről érkezett, a lakosság eleinte nem érezte magát veszélyben. Ahogyan terjedt a vírus Európában, annál jellemzőbb lett a nem-afrikai emberekkel szembeni szóbeli atrocitás, ritkán bántalmazás, melynek során a külföldről érkezett állampolgárokat „hazaküldték” vagy a koronavírus szót kiabálták felé fenyegetően.

Szemben ezzel a hozzáállással az emberek mégsem vették elég komolyan a koronavírus veszélyét, annak ellenére, hogy az afrikai elnökök szigorú intézkedéseket vezettek be a vírus elterjedésének megakadályozására. [50]

Marokkóban legalább egy tucat embert tartóztattak le a koronavírussal kapcsolatos álhírek terjesztése miatt március közepén. Ugyanazon a napon a kormány jóváhagyta a szociális média használatát szabályozó törvénytervezetet, amelynek célja a hamis hírek, továbbá a közrendet és a gazdaságot aláásó internetes bűncselekmények elkerülése. A jogi szervezetek meg is vádolták a kormányt a sajtószabadság megcsorbításával, amelyre az elmúlt év során amúgy is sok példa volt.

A vírussal kapcsolatos álhírterjesztők között vannak olyanok, akik tagadják a vírus létezését, ezért az elővigyázatossági intézkedések figyelmen kívül hagyását és a korlátozásokkal való szembeszegülést szorgalmazzák. Ezzel szemben olyan hírek is terjednek, miszerint egy város le van zárva, és azt javasolják, hogy az emberek ne menjenek oda. [51]

A koronavírus megjelenése a vallási szervezetek számára is nehézséget okoz, így felekezettől függetlenül Afrika-szerte vannak felháborodásuknak hangot adó vallási vezetők, akik semmibe veszik a korlátozásokat. Az alapvetően vallásos lelkületű Afrikában pedig ezek a vezetők kedvezőtlenül alakítják a közvéleményt a COVID-19-cel szembeni védekezésben.

Tanzániában John Magufuli elnök szintén megpróbálta minimalizálni a koronavírus fenyegetését szem előtt tartva a vallási vezetők akaratát is, így április elején Magufuli továbbra is azt mondta állampolgárainak, hogy vegyenek részt vallási szolgálatokon, mert az isteni segítségnyújtás az egyetlen dolog, amely legyőzheti a betegséget. „A koronavírus nem maradhat fenn Jézus Krisztus testében, ott megég” – mondta a tanzániai elnök még márciusban. "Pontosan ezért nem félek a szentáldozás közben." [52]

Bár rendkívüli módon még a mekkai mecset is bezárta kapuit – még a ramadáni időszakra is, a szélsőséges felekezetek imámjai, mint például Rachid Eljay, az algériai Brest vallási vezetője azt nyilatkozta, hogy az ima és a fohások megvédenek a koronavírustól – vagyis nincs szükség a tudományokra. Ali Belhadj, az Iszlám Üdvösségi Front vezetője és Abdallah Djaballah, az Igazságügyi és Fejlesztési Front, iszlamista párt elnöke a mecsetek bezárásáról adott ki nyilatkozatokat, melyekben azt követelték, hogy a mecsetek ne legyenek bezárva, mert azok az Isten házai és az Isten megvédi őket. [53]

Április 18-án Kenyában a Mijikenda vallás öregjei – hasonlóan a Njuri Njeke vezetőihez – rituális tisztító szertartásokat végeztek az erdőben, hogy elűzzék a koronavírus ártó szellemeit, majd azt kérték a kormánytól, hogy engedélyezzék a koronavírusos esetek gyógyítását hagyományos módszerekkel, ahogyan erre már az 50-es években is volt példa. [54]

A koronavírussal kapcsolatos tévhitek között olyanok is megjelentek, mely szerint a COVID-19 nem fertőzi meg az afrikaiakat, hogy nem is képes életben maradni az afrikai éghajlaton. Ezek mellett a babonák is elterjedtek, miszerint ha valaki koronavírusos, elég, ha lefújja magát alkohollal kevert klórral, és meggyógyul, Kenyában a fekete tea reggeli fogyasztását ajánlották koronavírusos fertőzés kezelésére, Nigériában a lime-mal és citrommal készített borslevest, míg Ghánában a neem-fából előállított készítményekkel védekeznek a koronavírus ellen. [55]

A korlátozások drasztikus megszegése és a rendőri brutalitás következtében több ember halt meg eddig a Kongói Demokratikus Köztársaságban, Kenyában, [56] Dél-Afrikában és Nigériában, mint koronavírusos megbetegedésben. Nigériában két hét alatt 18 ember vesztette életét a korlátozások betartására irányuló intézkedések alkalmával, míg a közölt adatokkal egy időben, mindössze 12-en veszítették életüket a COVID-19 miatt. [57] Kenyában a tanulmány írásának napján is hat ember esett áldozatul a koronavírus miatti kijárási korlátozásokat végrehajtó rendőri brutalitásnak. [58] A kenyai rendőrök legfiatalabb áldozata egy 13 éves fiú volt, akit a rendőrök a saját erkélyén véletlenül lőttek le. [59] Ugandában a nőket arra kényszerítették, hogy levetkőzzenek a rendőrség erőszakos intézkedései során, illetve a rendőrök új hatáskörükkel az LGBTQ embereket célozták meg. Dél-Afrikában számos videó terjed az interneten a nemzetvédelmi erők polgári személyekkel szembeni visszaéléseiről, legutóbb pedig gyermekek sérültek meg, mikor egy embert a házuk előtt lőttek le az intézkedő rendőrök. A hatóságok minden esetben megígérték, hogy büntetőeljárást indítanak és megbüntetik a felelős tisztviselőket. [49]

KONKLÚZIÓ

2020-ban Afrika gyenge egészségügyi rendszere, a HIV, TBC, malária és egyéb fertőző betegségek, a sáskajárás következtében kialakult mezőgazdasági katasztrófa helyzet, a több országban is jelenlevő politikai instabilitás és a külső szereplőktől függő gazdasági helyzet egy olyan táptalajt ad a COVID-19 fertőzésnek, amire több világszervezet is felhívta a kontinens vezetőinek figyelmét.

Saját helyzetét felismerve így Afrika elsősorban megelőzésre koncentrált, mert a vírus megjelenésének és kiszűrésének feladata még megvalósíthatónak tűnt, míg a terjedés megakadályozása minden szakmai vélemény szerint lehetetlen feladat. Az afrikai kormányok a WHO, majd Kína segítségével gyorsan reagáltak, illetve voltak olyan országok, ahol az ebola-járvány miatt ez a rendszer már eleve megvolt, tehát egyes régiók gyakorlati tapasztalattal is rendelkeztek. Bár a vírus már minden országban jelen van, a megjelenések időpontja a Kínával való közvetlen kapcsolat ellenére Európához képest kései.

A vírus megjelenése után a lakossági érintkezés megakadályozása érdekében hozott szigorú intézkedéseket a gyenge egészségügyi ellátó rendszerek miatt vezették be, azonban a korlátozások gazdasági nehézségeket, társadalmi feszültséget és politikai harcot eredményeznek. A fennálló nehézségek: a teljes kontinensre kiterjedő éhezés, a gazdasági válság, a rendőri brutalitás felvetik a közvéleményben a koronavírussal való küzdelem szükségességét és hitelességét, ami miatt a vírussal kapcsolatos tévhitek és álhírek gyorsan elterjednek a kontinensen. Az álhírek és tévhitek pedig növelik a kormányokkal való szembeszegülés mértékét és a vírus terjedésének kockázatát.

FELHASZNÁLT IRODALOM / JEGYZETEK

- [1] S. Jerving. „Africa needs early detection of coronavirus, WHO says.” [online] devex.com. <https://www.devex.com/news/africa-needs-early-detection-of-coronavirus-who-says-96460> (letöltve: Apr. 18, 2020).
- [2] O. Ogbuoji, I. Bharali, N. Emery and K. K. McDade. „Closing Africa's health financing gap.” Future Development [online] <https://www.brookings.edu/blog/future-development/2019/03/01/closing-africas-health-financing-gap/> (letöltve: Apr. 22, 2020).

- [3] „Zimbabwe doctors reject 'return to work offer'.” Africanews [online] <https://www.africanews.com/2019/11/30/zimbabwe-doctors-reject-return-to-work-offer/> (Apr. 22, 2020).
- [4] Africa has about one doctor for every 5000 people.” Quartz, qz.com [online] <https://qz.com/520230/africa-has-about-one-doctor-for-every-5000-people/> (letöltve: Apr. 22, 2020).
- [5] „East Africa locusts threaten food security across subregion, alerts UN agriculture agency.” UN News [online] <https://news.un.org/en/story/2020/01/1055631> (letöltve: Apr. 22, 2020).
- [6] M. Makoni. „Africa prepares for coronavirus.” The Lancet [online] [https://www.thelancet.com/journals/lancet/article/PIIS0140-6736\(20\)30355-X/fulltext](https://www.thelancet.com/journals/lancet/article/PIIS0140-6736(20)30355-X/fulltext) (letöltve: Apr. 22, 2020).
- [7] S. Smith. „What the Coronavirus Means for Africa.” Africa Center for Strategic Studies [online] <https://africacenter.org/spotlight/what-the-coronavirus-means-for-africa/> (letöltve: Apr. 22, 2020).
- [8] „Crisis Update” Medecins Sans Frontieres [online] <https://www.msf.org/drc-ebola-outbreak-crisis-update> (letöltve: Apr. 22, 2020).
- [9] W. G. Moore and T. Nyenswah. „How can we prepare for Coronavirus? Learn from Liberia’s experience with Ebola.” Mail&Guardian [online] <https://mg.co.za/article/2020-03-08-how-can-we-prepare-for-coronavirus-learn-from-liberias-experience-with-ebola/> (letöltve: Apr. 18, 2020).
- [10] N. Kapata, C. Ihekweazu, F. Ntoumi, T. Raji, P. Chanda-Kapata, P. Mwaba, V. Mukonka, M. Bates, J. Tembo, V. Corman, S. Mfinanga, D. Asogun, L. Elton, L. B. Arruda, M. J. Thomason, L. Mboera, A. Yavilinsky, N. Haider, D. Simons, L. Hollmann, S. A. Lule, F. Veas, M. M. Abdel Hamid, O. Dar, S. Edwards, F. Vairo, T. D. McHugh, C. Drosten, R. Kock, G. Ippolito, and A. Zumla. *“Is Africa prepared for tackling the COVID-19 (SARS-CoV-2) epidemic. Lessons from past outbreaks, ongoing pan-African public health efforts, and implications for the future”* International Journal of Infectious Diseases, Vol. 93, pp. 233-236, Feb. 2020. DOI: <https://doi.org/10.1016/j.ijid.2020.02.049>
- [11] „Standard Operating Procedures For Preparedness, Detection and Response To A Coronavirus (2019-NCOV) Outbreak in South Africa.” National Department of Health Directorate: Communicable Diseases, [Online]. https://www.hpcsa.co.za/Uploads/Publications%202020/Resources/SOP_Coronavirus_29_Jan_2020.pdf (letöltve: Apr. 22, 2020).
- [12] M. Gilbert, G. Pullano, F. Pinotti, E. Valdano, C. Poletto, P-Y. Boëlle, E. D’Ortenzio, Y. Yazdanpanah, S. P. Eholie, M. Altmann, B. Gutierrez, M.U.G. Kraemer, V. Colizza. „Preparedness and vulnerability of African countries against introductions of 2019-nCoV.” www.epicx-lab.com [online] https://www.epicx-lab.com/uploads/9/6/9/4/9694133/africa_capacity_ncov_risk.pdf (letöltve: Apr. 22, 2020).
- [13] „2019 Novel Coronavirus (2019-nCoV): Strategic Preparedness and Response Plan.” WHO, Feb. 3, 2020. [Online]. <https://www.who.int/docs/default-source/coronaviruse/srp-04022020.pdf> (letöltve: Apr. 22, 2020).
- [14] L. Nordling. „‘A ticking time bomb’: Scientists worry about coronavirus spread in Africa.” <https://www.sciencemag.org/news/2020/03/ticking-time-bomb-scientists-worry-about-coronavirus-spread-africa> (letöltve: Apr. 22, 2020).

- [15] „Coronavirus: Gabon bans entry of passengers from China.” Africanews/AFP [online] <https://www.africanews.com/2020/02/08/coronavirus-gabon-bans-entry-of-passengers-from-china/> (letöltve: Apr. 22, 2020).
- [16] „Southern Africa: Visas Between Mozambique and China Suspended.” All Africa [online] <https://allafrica.com/stories/202001300838.html> (letöltve: Apr. 22, 2020).
- [17] „Cameroon announces food import ban amid coronavirus threat.” dw.com[online] <https://www.dw.com/en/cameroon-announces-food-import-ban-amid-coronavirus-threat/av-52372500> (letöltve: Apr. 22, 2020).
- [18] C. Okello. „Zambians want students repatriated from China as coronavirus spreads.” [online] <http://www.rfi.fr/en/international/20200205-Coronavirus-Zambians-want-students-repatriated-China> (letöltve: Apr. 22, 2020).
- [19] M. M. Kamara. „Coronavirus: Sierra Leone introduces compulsory quarantine for travelers from China.” Politico SL [online] <https://www.politicosl.com/articles/coronavirus-sierra-leone-introduces-compulsory-quarantine-travelers-china> (letöltve: Apr. 22, 2020).
- [20] „WHO head tells Africa to 'wake up' to coronavirus threat.” BBC [online] <https://www.bbc.com/news/world-africa-51960118> (letöltve: Apr. 22, 2020).
- [21] A. A. Mumin and C. Pensulo. „Africa's fragile health systems rush to contain coronavirus.” The Guardian [online] <https://www.theguardian.com/world/2020/mar/20/africas-fragile-health-systems-rush-to-contain-coronavirus> (letöltve: Apr. 22, 2020).
- [22] B. Adebayo. „African countries shut doors against Europe, America to combat coronavirus.” cnn.com [online] <https://edition.cnn.com/2020/03/16/africa/africa-coronavirus-travel-restrictions-foreigners/index.html> (letöltve: Apr. 22, 2020).
- [23] A tanulmányban szereplő adatok a <https://covid19.who.int/> és a <https://www.worldometers.info/coronavirus/> 2020. április 22-ei jelentéseihez igazodnak.
- [24] „Cameroonian student infected with Coronavirus in good health, China says.” Journal du Cameroon, <https://www.journalducameroun.com/en/cameroonian-student-infected-with-coronavirus-in-good-health-china-says/> (letöltve: Apr. 22, 2020).
- [25] D. Vincent. „Coronavirus: A Cameroon student on how he recovered.” BBC [online] <https://www.bbc.com/news/world-africa-51502711> (letöltve: Apr. 22, 2020).
- [26] „Egypt announces first Coronavirus infection.” Egypt Today [online] <https://www.egypttoday.com/Article/1/81641/Egypt-announces-first-Coronavirus-infection> (letöltve: Apr. 22, 2020).
- [27] R. Maclean and A. L. Dahir. „Nigeria Responds to First Coronavirus Case in Sub-Saharan Africa.” nytimes.com. [online] <https://www.nytimes.com/2020/02/28/world/africa/nigeria-coronavirus.html> (letöltve: Apr. 18, 2020).
- [28] „Coronavirus: Nigeria confirms first case in sub-Saharan Africa.” BBC [online] <https://www.bbc.com/news/world-africa-51671834> (letöltve: Apr. 22, 2020).
- [29] „Algerian health minister confirms first COVID-19 case.” Africa Times [online] <https://africatimes.com/2020/02/25/algerian-health-minister-confirms-first-covid-19-case/> (letöltve: Apr. 22, 2020).
- [30] D. Ba. „Senegal confirms first coronavirus case: Health Ministry.” Reuters [online]

- <https://www.reuters.com/article/us-health-coronavirus-senegal/senegal-confirms-first-coronavirus-case-health-ministry-idUSKBN20P2JX> (letöltve: Apr. 22, 2020).
- [31] S. Kasraoui. „Morocco Records First Case of Coronavirus.” Morocco World News [online] <https://www.morocoworldnews.com/2020/03/295120/morocco-records-1st-case-of-coronavirus/> (letöltve: Apr. 22, 2020).
- [32] „Italian returnee confirmed Tunisia’s first coronavirus case.” Punch [online] <https://punchng.com/italian-returnee-confirmed-tunisia-first-coronavirus-case/> (letöltve: Apr. 22, 2020).
- [33] L. Kiewit. „First SA corona patient, doctor, and family in quarantine.” Mail&Guardian [online] <https://mg.co.za/news/2020-03-06-first-sa-corona-patient-doctor-and-family-in-quarantine/> (letöltve: Apr. 22, 2020).
- [34] Az átlagéletkor kevesebb, mint 20 év, a népesség mindössze 3 %-a idősebb 65 évnél, viszont a népesség 43 %-a nagyvárosokban él.
- [35] B. Minas. „Un cas de Coronavirus a été importé des Comores.” Mayotte la 1re [online] <https://la1ere.francetvinfo.fr/mayotte/un-cas-de-coronavirus-a-ete-importe-des-comores-823226.html> (letöltve: Apr. 22, 2020).
- [36] E. Smith. „Lockdowns, curfews and doorstep testing: Africa’s crackdown on the coronavirus.” CNBC [online] <https://www.cnbc.com/2020/04/02/lockdowns-curfews-and-doorstep-testing-africas-crackdown-on-the-coronavirus.html> (letöltve: Apr. 22, 2020).
- [37] „Coronavirus: curfews in Senegal and Ivory Coast, lockdown in South Africa.” France24 [online] <https://www.france24.com/en/20200324-coronavirus-curfews-in-senegal-and-ivory-coast-lockdown-in-south-africa> (letöltve: Apr. 22, 2020).
- [38] N. Maseko. „Coronavirus: South Africa deploys 70,000 troops to enforce lockdown.” BBC [online] <https://www.bbc.com/news/world-africa-52387962> (letöltve: Apr. 22, 2020).
- [39] S. Wild. „South Africa’s president and ministers are taking a 33% pay cut and extended its lockdown.” Quartz [online] <https://qz.com/africa/1835996/south-africa-president-takes-pay-cut-extends-lockdown/> (letöltve: Apr. 22, 2020).
- [40] „COVID-19: Kenya bans travel in and out of Nairobi, other areas.” Al Jazeera [online] <https://www.aljazeera.com/news/2020/04/covid-19-kenya-bans-travel-nairobi-areas-200406163601579.html> (letöltve: Apr. 22, 2020).
- [41] „Sudan locks down capital Khartoum after coronavirus cases rise.” Al Jazeera [online] <https://www.aljazeera.com/news/2020/04/sudan-locks-capital-khartoum-coronavirus-cases-rise-200418134801982.html> (letöltve: Apr. 22, 2020).
- [42] „Morocco extends coronavirus lockdown till May 20 – Government.” Reuters [online] <https://www.reuters.com/article/health-coronavirus-morocco/morocco-extends-coronavirus-lockdown-till-may-20-government-idUSL8N2C60EW> (letöltve: Apr. 22, 2020).
- [43] „Libyans Rush to Stock Up for Ramadan Before Coronavirus Curfew Kicks In.” Reuters [online] <https://www.nytimes.com/reuters/2020/04/16/world/africa/16reuters-health-coronavirus-libya-curfew.html> (letöltve: Apr. 22, 2020).
- [44] J. Ambrose. „Oil prices slump as market faces lowest demand in 25 years.” The Guardian [online] <https://www.theguardian.com/business/2020/apr/15/oil-prices-slump-as-market-faces-lowest-demand-in-25-years-covid-19> (letöltve: Apr. 22, 2020).
- [45] B. Feleke. „Sub-Saharan Africa to fall into its first recession in 25 years due to coronavirus, says World Bank.” CNN [online]

<https://edition.cnn.com/2020/04/09/africa/africa-recession-coronavirus/index.html> (letöltve: Apr. 22, 2020).

[46] „Coronavirus - South Africa: COVID-19 lockdown impacts publication of economic statistics.” Africanews/APO Group [online]

<https://www.africanews.com/2020/04/17/coronavirus-south-africa-covid-19-lockdown-impacts-publication-of-economic-statistics/> (letöltve: Apr. 22, 2020).

[47] F. Basiime. F. Warom. S. Iceta, and A. Tumushabe. „Refugee food cut exposes mothers, children to hunger.” Daily Monitor [online] <https://www.monitor.co.ug/News/National/Refugee-food-cut-exposes-mothers-children-to-hunger/688334-5526338-nv58s0z/index.html> (letöltve: Apr. 22, 2020).

[48] L. Mutanganshuro. „Govt begins distribution of essential goods to citizens affected by COVID-19 lockdown.” The New York Times [online]

<https://www.nytimes.com/news/govt-begins-distribution-essential-goods-citizens-affected-covid-19-lockdown> (letöltve: Apr. 22, 2020).

[49] Coronavirus - Africa: A Human Rights Checklist.” Africanews/APO Group [online] <https://www.africanews.com/2020/04/18/coronavirus-africa-a-human-rights-checklist/> (letöltve: Apr. 22, 2020).

[50] A. L. Dahir. „Africa Braces for Coronavirus, but Slowly.” The New York Times [online] <https://www.nytimes.com/2020/03/17/world/africa/coronavirus-africa-burkina-faso.html> (letöltve: Apr. 22, 2020).

[51] „Morocco Makes a Dozen Arrests Over Coronavirus Fake News.” Reuters [online] <https://www.usnews.com/news/world/articles/2020-03-19/morocco-makes-dozen-arrests-over-coronavirus-fake-news> (letöltve: Apr. 22, 2020).

[52] A. Ward. „Africa has so far been spared the worst of the coronavirus. That could soon change.” VOX [online] <https://www.vox.com/2020/4/21/21225002/coronavirus-africa-cases-death-food-debt-economy> (letöltve: Apr. 22, 2020).

[53] K. Abderrahmani. „Islamists angry over mosque closures, use COVID-19 as a propaganda tool.” AsiaNews.it [online] <http://www.asianews.it/news-en/Islamists-angry-over-mosque-closures,-use-COVID-19-as-a-propaganda-tool-49654.html> (Apr. 22, 2020)

[54] „We have COVID cure: Mijikenda elders claim they may have the cure to COVID-19.” KTN News [online] <https://www.standardmedia.co.ke/ktnnews/video/2000188079/we-have-covid-cure-mijikenda-elders-claim-they-may-have-the-cure-to-covid19> (letöltve: Apr. 22, 2020)

[55] „Debunking 9 popular myths doing the rounds in Africa about the coronavirus” The Conversation [online] <https://theconversation.com/debunking-9-popular-myths-doing-the-rounds-in-africa-about-the-coronavirus-135580> (letöltve: Apr. 22, 2020)

[56] R. Ombuor and M. Bearak. „‘Killing in the name of corona’: Death toll soars from Kenya’s curfew crackdown.” The Washington Post [online]

https://www.washingtonpost.com/world/africa/kenya-coronavirus-curfew-crackdown-death-toll/2020/04/15/740a8c4e-79be-11ea-a311-adb1344719a9_story.html (letöltve: Apr. 22, 2020).

[57] A. Sargent. „Curfew crackdowns in several African countries kill more people than Covid-19.” France24 [online] <https://www.france24.com/en/20200417-papers-curfew-crackdowns-in-several-african-countries-kill-more-people-than-covid-19> (letöltve: Apr. 22, 2020).

[58] „Six killed by Kenyan police enforcing coronavirus curfew: HRW.” Al Jazeera [online] <https://www.aljazeera.com/news/2020/04/killed-kenyan-police-enforcing-coronavirus-curfew-hrw-200422144016333.html> (letöltve: Apr. 22, 2020).

[59] „Kenyan teen shot during coronavirus curfew” AFP [online] <https://www.news24.com/Africa/News/kenyan-teen-shot-during-coronavirus-curfew-20200331> (letöltve: Apr. 22, 2020).

**NETWORK OF USER-RELATED HUMAN
RISK FACTORS IN INFORMATION
SECURITY****AZ INFORMÁCIÓBIZTONSÁG
FELHASZNÁLÓI OLDALI HUMÁN
KOCKÁZATI TÉNYEZŐINEK HÁLÓZATA**KÁRÁSZ Balázs¹**Abstract**

Critical and weak points of developing information security awareness can be mapped by conducting a process-based analysis of particular human risk factors influencing information security as well as the common effect of the coherence of relations between these factors. This paper aims to delineate the network of human risk factors related to information security considered on the users' behalf, on both employee and leadership levels, with the help of creating suitable clusters. In the knowledge of all above, learning and other professional service conceptions can be set up and tailored to the organization, the effectiveness of which depends to that of information security purposes. In practice, with the help of such conceptions, information security can be improved in the organization, the effectuation of which has its roots in the command function of leadership.

Supported by the ÚNKP-19-3-I-NKE-14 New National Excellence Program of the Ministry for Innovation and Technology.

Keywords

information security, network of human risk factors, organizational learning concepts, security awareness

Absztrakt

Az egyes, az információbiztonságot befolyásoló humán tényezők, valamint a közöttük fennálló összefüggések együttes hatásának folyamat alapú elemzésével feltérképezhetők az információbiztonság-tudatosság kialakításának és fejlesztésének kritikus és gyenge pontjai. Jelen közlemény célja, hogy a megfelelő klaszterek kialakítása segítségével felvázolja a felhasználói oldalon, beosztotti és vezetői szinten kockázati hatással bíró humán tényezők információbiztonsági vonatkozású hálózatát. Ennek ismeretében testre szabott képzési és egyéb szakmai szolgáltatási koncepciók állíthatók fel, amelyek hatékonysága szervesen kapcsolódik az információbiztonsági törekvések hatékonyságához. A gyakorlatban segítségükkel fejleszthető az információbiztonság-tudatosság a szervezetben, melynek megvalósulása a vezetés irányítási funkciójában gyökerezik.

Az Innovációs és Technológiai Minisztérium ÚNKP-19-3-I-NKE-14 kódszámú Új Nemzeti Kiválóság Programjának szakmai támogatásával készült.

Kulcsszavak

információbiztonság, humán kockázati tényezők hálózata, szervezeti képzési koncepciók, biztonságtudatosság

¹ karasz@gmail.com | ORCID: 0000-0003-2065-4928 | PhD hallgató / PhD Student | National University of Public Science Doctoral School of Military Engineering / Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola

BEVEZETÉS

Napjaink vállalati, szervezeti tudása az adatokon és az információkon alapul, amelyek elemző, feldolgozó, továbbító, tároló stb. rendszerek összességében összpontosulnak. Adatbányászati megközelítése szerint az adatelemzés az adatok értékelésének, azaz ellenőrzésének, letisztításának, átalakításának és modellezésének folyamatát jelenti, amely hasznos információ feltárásán, következtetések levonásán keresztül az analitikus, logikus érveléshez, döntéstámogatáshoz szükséges. Az adatelemző rendszerek védelme komplex módon értelmezendő, mivel civil és katonai szervezetek, így köztük kritikus infrastruktúrát fenntartó és üzemeltető vállalatok szervezeti egységei számára az információbiztonság műszaki megközelítése elképzelhetetlen a humán tényezők vizsgálata nélkül.

A humán tényezők jelentős része (pl. emberi teljesítmény, munkavállalói attitűd, biztonságtudatosság, vezetés minősége, vezetői példamutatás stb.) alapvető hatást gyakorolhat a komplex informatikai rendszerek megbízhatósági és biztonsági szintjére. A hibrid hadviselés elterjedésével a social engineering növekvő szerepe is befolyással bír a szervezeti információbiztonsági folyamatokra, ezért elengedhetetlen a kibertámadási pontok azonosítása, a kockázatok kezelése.

Tudományos probléma és kutatási célkitűzés

A fentiekből következően felmerül az a komplex kérdés, hogy milyen mértékben, ill. egymáshoz viszonyítva milyen arányban járulhatnak hozzá az információbiztonságtudatosság fejlesztéséhez a civil szférában alkalmazott menedzsment módszerek – az egyes social engineering és egyéb típusú támadások befolyásoló hatása részleteinek fényében.

Jelen közlemény a probléma tágabb vizsgálatához kíván részkutatási eredményeket nyújtani, amelynek hipotézise, hogy az információbiztonságtudatosság fejlesztésének hatékonysága a vezetés irányítási funkciójában gyökerezik. A közlemény célja, hogy az elméletkép módszerének segítségével felrajzolja azon humán tényezők hálózatát, amelyek vezetői és beosztotti szinten kockázati hatással bírnak az információbiztonságtudatosságra a szervezetben. E hálózat ismeretében bármely szervezet képes lehet olyan képzési és egyéb szakmai szolgáltatási koncepciókat felállítani, amelyek segítségével fejleszthető a szervezeti biztonságtudatosság.

HUMÁN TÉNYEZŐK AZ INFORMÁCIÓBIZTONSÁGBAN

A humán tényezők szerepét az információbiztonság holisztikus értelmezésében több szakirodalom feldolgozta, melyek közül Cains és társai közleménye [1] megfogalmazta, hogy az emberi viselkedés több irányból befolyásolja a biztonságot: ezért fontos annak megértése a felhasználói, a védelmi és a támadói oldalról egyaránt. Kiemelve a bizalom kérdéskörét, a szerzők kifejtik, hogy a bizalom kéttényezős, az egyén részeként megnyilvánuló inherens tulajdonságok, valamint az egyénen kívülről érkező, ún. szituációs tulajdonságok alkotják. Alapvető befolyással bír továbbá a kockázattudatosság és a kockázatok kezelésével kapcsolatos attitűd alakításában.

Jelen közlemény fenti kategóriák közül kizárólag a felhasználói oldal (egyúttal a három közül a legszélesebb kör) részletesebb tárgyalására szorítkozik, kiemelve ugyanakkor a felhasználói viselkedésnek a támadói oldal jelentette fenyegetésekkel szemben megmutakozó tulajdonságait.

Az emberi viselkedés sebezhetőségből fakadó kiszámíthatatlan természete mögött egy komplex, személyközi, meghatározott csoport viszonylatában értelmezhető interakció-halmaz áll, mely Oroszi [2] és Kollár [3] gyűjtését kiegészítve a következő klasszifikáció mentén számba vehető emberi tulajdonságokban érhető tetten:

- Hanyagság
- Kihasználható emberi tulajdonságok
- Vezetői viselkedés és interakciók
- Tudatosság hiánya

Az alábbi felsorolásban részletesebb áttekintést kívánok nyújtani a fenti kategóriákba sorolható egyes felhasználói oldalon jelentőséggel bíró emberi tulajdonságokról. Amelyek esetében elérhető, információbiztonsági vonatkozású példák segítségével szemléltetem a mindennapi vállalati gyakorlatban előforduló eseteket. A felsorolás és a jellemzések továbbá a beosztotti és vezetői szint összehasonlító elemzésének alapját képezik.

Hanyagság

1. Figyelmetlenség: tetten érhető a hardvereszközök, helyiségek őrizetlenül hagyásában, fizikai biztonsági előírások nem tudatos megkerülésében.
2. Feledékenység: hatása megmutatkozik pl. a jelszókezelési kultúrában.
3. Kényelem: leggyakrabban biztonsági előírások megkerülésével érhető el.
4. Konfliktuskerülés: adatvédelmi előírások betartására való felszólítás tudatos elmulasztása más érdekek előbbre helyezése miatt.
5. Munka-magánélet nem megfelelő elválasztása: megnyilvánul a saját és vállalati eszközök és az azokon tárolt információk kezelésekor.
6. Közönyösség: „tudatos figyelmetlenség”, biztonsági szabályok hiányos vagy elhanyagolt figyelembevétele.

Kihasználható emberi tulajdonságok

1. Segítőkészség: a támadó tudatlanul, de készségesen történő segítése a jogosulatlan információszerzés végrehajtásában.
2. Befolyásolhatóság: a támadó manipulációjának való áldozatul esés, jogosulatlan módon történő információszerzésének segítése.
3. Bosszúállás, félelem: megtestesülhet meggondolatlanságból, számításból fakadó tudatos cselekvésben, pl. dezinformálásban.
4. Kíváncsiság, nyitottság, érdeklődés: információk kezelése a megfelelő jogosultsági körökön túl, szivárogtatás, egyes információk félremagyarázása.
5. (Lét)bizonytalanság: a támadó zsarolásának áldozatául esés, a szabályok beszűkült tudatállapotban történő áthágása, akár radikalizáció útján a kiberterrorizmusba történő bevonódás, kompromittálhatóság.
6. Leterheltség, fáradtság, monotonitás, stressz: elsődlegesen a hanyagság csoportjába tartozó tényezők előidézése.
7. Viszonzási igény: mind szívességtevés, mind szakmai segítségnyújtás esetében előforduló, kimondott vagy meg nem fogalmazott igény.

Vezetői pozíció sajátosságaiból adódó tulajdonságok

1. Tekintélyelvűség - felsőbbrendűségi érzés: megnyilvánulhat a vezetői utasítás, iránymutatás megkérdőjelezhetetlenségének kommunikációjában.
2. Felelősségvállalás és annak hiánya: információbiztonsági erőfeszítések finanszírozásáról szóló döntéshozatal és következményeinek vállalása, kommunikációja.
3. Előítéletesség: hiányos ismereten alapuló vagy megalapozatlan, túlnyomórészt befolyáson és személyes elgondolás vagy meggyőződés által befolyásolt döntéshozatal.

Tudatosság hiánya

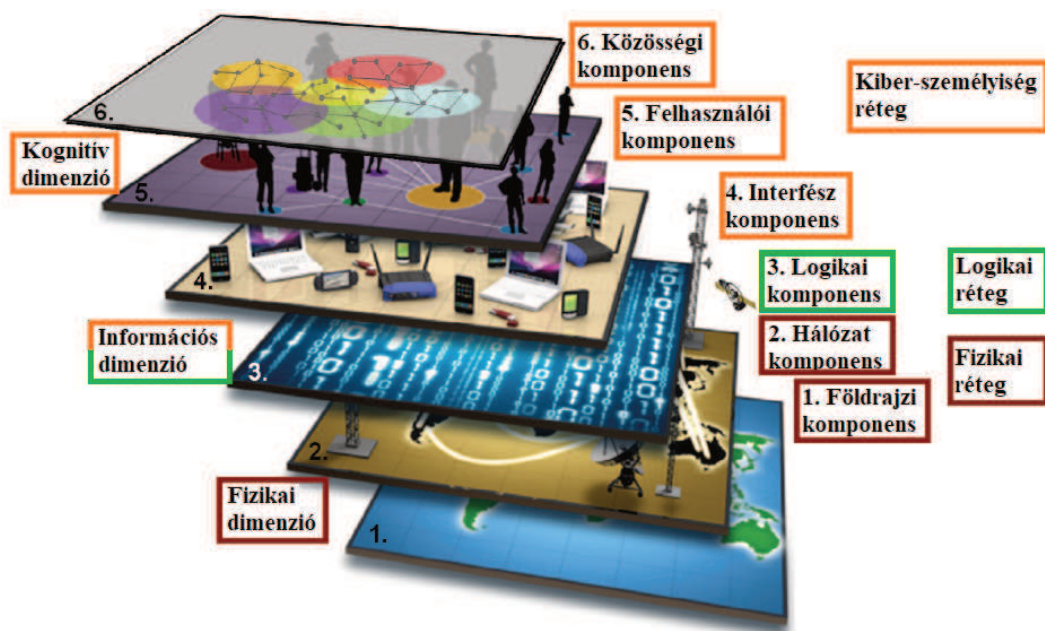
1. Tudatlanság (ismerethiány): hiányos/rendszeretlen információbiztonsági képzés, illetve az azon való részvétel nem kielégítő előmozdításának eredménye lehet – mind a szervezetekben, mind iskolai keretek között.
2. Szakképzetlenség: saját szakterülethez, valamint a magánélethez kapcsolódó informatikai és információbiztonsági ismeretek nem megfelelő elsajátítása.
3. Hiszékenység (naivság, jóhiszeműség): a racionalitás és a biztonsági szabályok fényében történő józan ítélőképesség háttérbe szorulása.

A HOZZÁFÉRÉS, JOGOSULTSÁG SZEREPE

Bármely szervezet informatikai rendszereiben az egyes funkciókhoz, területekhez, fájlappákhöz, programokhoz való jogosultságok szigorú rendszerben kerülnek hozzárendelésre a felhasználókhöz. Az ún. jogosultságkezelés ennek megfelelően dokumentált módon történik, az egyes felhasználók a szervezete által kezelt és tárolt adatokhoz és rendszerekhez kizárólag az ahhoz hozzáférési jogosultsággal férhetnek hozzá meghatározott ideig, illetve módon (írás-olvasás, csak olvasás, csak írás, törlés). Alapelvként kerül megfogalmazásra számos szervezet vonatkozó szabályozó dokumentumaiban (a szabványok ajánlásainak megfelelően), hogy minden felhasználó csak a számára szükséges és elégséges jogosultságokkal rendelkezzen (pl. az indokolatlan többletjogosultságok visszavonandók).

A jogosultságkezelés szigorának fontossága nem csupán a szabályozottság, a felelősségre vonás szempontjából jelentő visszakövethetőség, hanem az információbiztonság megvalósulása miatt is kiemelkedő. Bármely támadás a kibertér virtuális dimenziójában addig terjedhet ugyanis, ameddig a megtámadott felhasználó és ezáltal az ahhoz rendelt, már megváltozott irányítású jogosultsági kör terjed. Ennek megfelelően az adminisztrátor (vagy magasabb) szintje magasabb biztonsági kockázatú, így magasabb védelmi szintet követel meg – a technikai és a humán kockázati tényezők oldaláról egyaránt.

A jogosultság ellenőrzésére is szolgálnak az autentikációs vagy azonosítási megoldások, melyek biztonsági és a technikai oldalról megvalósuló megbízhatósági problémái mentén társadalmilag is jelentős, de fontos jogi vonatkozású kérdések is megfogalmazhatók [4]. Az 1. ábrán látható információs környezeti dimenziók és a párhuzamos értelmezés szerinti kibertéri rétegek felépítéséből kiindulva megállapítható, hogy az egyes rétegek és komponenseik jól körülhatárolható funkciói és önálló voltak ellenére számos módon kapcsolódnak egymáshoz. Az autentikáció közvetítő szerepet tölt be annak értelmezésében, hogyan épülnek egymásra a kibertéri rétegek.



1. ábra Az információs környezet dimenziói és a kibertéri rétegek komponensei (saját szerkesztés [5] alapján)

Az autentikációs megoldások használata annak ellenére nem korlátozódik a kiber-személyiség rétegre, hogy gyökereik a felhasználói komponensben találhatóak (egyedi felhasználói, IP és e-mail címek stb.), továbbá elsődleges funkciójuk, hogy kapcsolatot teremtsenek az interfész és a felhasználók között, segítve a felhasználókat közösségi hálózatok kialakításában. Sokkal inkább meghatározó kapcsolódás szerepét tölti be az azonosítás a logikai réteg felé (amelybe a következő elemek sorolhatók: információ, átviteli protokollok, szoftveres alkalmazások, felhasználói adatok, internetes tartománynevek), sőt a fizikai réteg felé is (ennek néhány releváns eleme: szerverek, rádiófrekvencia-továbbító eszközök, elektromágneses spektrum).

SOCIAL ENGINEERING

Az ún. social engineering (más kifejezéssel pszichológiai manipuláció) minden olyan technikát magába foglal, amelyik révén az emberi természetet, lélek, társas- és csoportkapcsolatok és azok dinamikája ismeretében, a személyközi, illetve csoporton belüli interakciók felhasználásával a manipulátor kijátssza az embereket, feltöri és megfertőzheti az alapszintű védelemmel ellátott informatikai rendszereket (bizalmas adatokhoz, adatbázisokhoz fér hozzá). Mitnick biztonságtechnikai tanácsadó könyvében [6], mely szemléletesen mutatja be e technikák mibenlétét, kivitelezésének részleteit, saját korábbi, elkövetőként szerzett tapasztalataiból merít a megtévesztés művészetének megfogalmazásához, ami hitelessé, életszerűvé teszi az abban foglaltakat.

Oroszi értekezése [2] alapján egy támadás kivitelezése során leggyakrabban alkalmazott technikák között megkülönböztethetünk humán és számítógép alapú social engineering technikákat az alábbiak szerint:

Humán alapú social engineering technikák

- Segítségkérés
- Segítségnyújtás
- Valamit valamiért
- Megszemélyesítés (fontos/új munkatárs)
- Felhatalmazás
- Reverse social engineering
- Dumpster diving – kukaátvizsgálás
- Shoulder surfing – „váll-szörf”
- Tailgating – szoros követés
- Elejtett, „csali” adathordozó
- Piggybacking
- Helpdesk átverése

Számítógép alapú social engineering technikák

- Ál-weboldalak
- Phishing, vishing, smishing
- Trójai programok
- Keyloggerek
- Man in the middle
- Brute force

A felsorolt technikák többsége ellen foganatosítható védelmi megoldásként a támadás lehetőségének tudatosítása, szigorított beléptetési rend, irodai hulladék szakszerű megsemmisítése, infokommunikációs eszközök, munkavégzési platformok szabályozott használata stb. merülhet fel. Mindez átfogó megközelítésből úgy lehetséges, ha egy szervezet koordinált adatbiztonsági és adatvédelmi stratégiával rendelkezik, amely lehetővé teszi a szabályozásban bekövetkezett változások, sőt fejlesztések szervezeten belüli, illetve tevékenységbe történő átültetését. Az előírások betartására komplex képzés-fejlesztési program megvalósítása nyújthat megoldást, melynek pillérei lépésenként: esettanulmányok és szimulációs helyzetgyakorlatok, elmélet levezetése, alkalmazás, majd akcióterv készítése egyéni és szervezeti szinten. [4]

A Social Engineering szerepe a jogosultságokkal kapcsolatban

A technikai megközelítésű háttértől visszakanyarodva témánk társadalomtudományi aspektusaihoz, számba veendő, hogy nem csupán a szervezeten kívülről érkező támadások jelentenek veszélyforrást az információbiztonságra, hanem a szervezeten belülről is számítani kell rosszindulatú tevékenységre, amelynek tehát az alábbi megvalósulási formái lehetnek:

- a szervezeten kívüli személy vagy számítógép jut be a szervezet belső hálózatába,
- a szervezetbe beépülve fejti ki tevékenységét a támadó,
- a szervezethez tartozó személy válik támadóvá.

A jelszókezelési hiányosságokat pontosan megnevezve és kategóriákba sorolva megtalálhatók a kapcsolódásokat az előző fejezetben leírt emberi tulajdonságokkal:

- jelszavas védelem hiánya, hivatkozások előzetes ellenőrzés nélküli megnyitása,
- alapértelmezett, illetve túl egyszerű jelszavak használata,

- „túl bonyolult” jelszavak nem megfelelő kezelése (pl. felírása cetlire),
- azonos jelszó használata különféle felületeken – akár többszintű autentikáció miatt,
- ritka jelszócsere, jelszó megjegyeztetése böngészővel számítógépen, ill. mobil eszközön,
- alapértelmezett ellenőrző kérdés és egyszerű válasz alkalmazása visszaállításhoz,
- jelszótároló alkalmazás nem megfelelő használata („saját” jelszavak tárolása),
- mobil eszköz nem megfelelő védelme (pl. feloldása mintával vagy számkóddal),
- fizikai biztonsági előírások (pl. üres íróasztal politika) figyelmen kívül hagyása,
- nem megfelelő hulladékkezelési és iratmegsemmisítési gyakorlat,
- felületesség az előírások elsajátításában és tudatossági képzésen való részvételben.

Nevezett hiányosságok egyenként az emberi alaptulajdonságok közül összefüggésben állnak a hanyagság több tényezőjével, különösen a kényelem, feledékenység, közönyösség és figyelmetlenség tényezőjével. Kevesebb szerep jut, de nem elhanyagolható jelentőséggel bír a jelszóhasználat során a munka-magánélet nem megfelelő szétválasztása és a konfliktuskerülés. Negatívan hat a jelszóhasználati kultúrára továbbá a tudatosság hiánya, azon belül pedig elsődlegesen a naivság, jóhiszeműség tényezője, melynél fogva a felhasználó nem tulajdonít megfelelő mértékű jelentőséget a biztonsági előírások betartása fontosságának.

A VEZETÉS RELEVÁNS FUNKCIÓI

A rendelkezésre álló szakirodalom feltárása és összegzése fényében az alábbi hangsúlyos gondolatok emelendők ki arra vonatkozóan, hogy a Social Engineering-típusú támadások elleni hatékony védekezés fő pillére a tudatosítás, melynek szervezeti keretek között történő előmozdítása a vezetői elkötelezettség és példamutatás függvénye.

Deák közleményében [7] megállapítja, hogy a támadási módszerek ismeretében jelentősen csökkenthető az információ kiszivárgása és illetéktelen felhasználása, egyúttal pedig növelhető az állami szervek működésének stabilitása, a társadalom és a gazdaság résztvevőinek biztonsága. E fejlesztési tevékenység során az első lépés a vezetők, majd pedig a beosztottak információbiztonság-tudatosságának fejlesztését és elköteleződésük erősítését kell, hogy célozza, komplex fejlesztési stratégiába ágyazva, de operatív szinten elsősorban a célképzésekbe emelt esettanulmányok, illetve valós környezetbe ágyazott, de mesterséges kibertámadási helyzetek elemzése útján. Ezt annak alapján állapítható meg, hogy alapvető kockázatkezelési módszertan a precedensestek vizsgálata, trendek, minták azonosítása.

Erre alapozta közleményének fő mondanivalóját Wilson és Hash [8] is, publikációjukban a tudatosság, képzés és oktatás fogalmainak tisztázását követően azt fogalmazzák meg, hogyan tervezhető meg egy biztonságtudatossági tréningprogram. A tervezés főbb kapcsolódó lépései a program személyre szabott tervezése célcsoportok meghatározása útján (ennek elsődleges szempontjai: szervezetben betöltött szerep, hierarchiában elfoglalt szint, fenyegetettség célja szerinti veszélyeztetettség), valamint a belső PR mind személyes, mind csoportos (szervezeti egység szintű) megvalósítása. Ezt egészíti ki iránymutatásuk, hogy a programhoz kapcsolódóan hogyan építhető fel oktatóanyag, majd legfontosabb tényezőként figyelembe veszik a program és az anyag hasznosulását egyfelől az implementáció lehetőségeinek számba vételével, majd az utánkövetés szerepének hangsúlyozásával.

Chestnut értekezésében [9] gondosan felépített, a biztonsági kockázatokat érintő bemutatását követően az elkövetett/előfordult hibák valós hatására helyezi a hangsúlyt. Számos módszertant áttekint és vizsgál annak fényében, hogy milyen adminisztratív és irányítási feladatok vannak közvetlen hatással az emberi tényezőre az információbiztonság szintjének befolyásolása kontextusában. Gazdasági megfontoláson alapuló ajánlásokat tesz a kockázatok csökkentésére, és javaslataiban összességében a visszamérés és ellenőrzés fontosságára helyezi a hangsúlyt.

A vezetői elkötelezettség szerepe

Napjainkban bármely szervezet egyik legfőbb vagyona az adat, ennek jelentős része az általa kezelt személyes adat, amely egyúttal az adott személyé is, akire vonatkozik. A megfelelő adatbiztonsági gyakorlatok és adatvédelmi eljárások kialakítása, és a vonatkozó előírásoknak való folyamatos megfelelés biztosítása azonban a személyes adatot kezelő szervezetet terheli. Az adatvédelem és az információbiztonság megvalósulása érdekében nem elegendő szabályokat életbe léptetni, technológiai kontrollokat kialakítani, naplózni és tesztelni, magának a vállalati kultúrának is ösztönöznie kell a tudatos adatkezelésre vonatkozó gyakorlat kialakítását és alkalmazását.

Ennek egyik alapja a személyzetfejlesztési rendszer hatékony kialakítása és folyamatos fejlesztése, melyet Karoliny és társai kézikönyvének vonatkozó fejezete [10], amely elhelyezi a tréninget a személyzetfejlesztési rendszerben, és a karriervezetésre helyezve a hangsúlyt, a vezetés funkcióit emeli ki mind a tudásmenedzsment, mind pedig a karriervezés során elsődleges szerepet játszó tényezőkként. Megfogalmazódnak a vezető személyével, vezetőként betöltött szerepével szemben kialakult újszerű követelmények, valamint az ezekre válaszként kínált személyzetfejlesztési rendszer.

Fentiekén kívül a témakör feldolgozásával foglalkozik még többek között Hámornik és társa konferenciáikban [11], amely elsődlegesen a csoportközi interakciók fényében tárgyalja a kiberbiztonság emberi tényezőit, illetve Stewart és társa hosszabb tanulmányában [12] szintén a szervezetben megnyilvánuló humán kockázatok és az információbiztonsági irányítás kapcsolatát vizsgálja. Közös megállapításuk – mellyel a mindennapokban a leginkább szembetűnő módon a tanúsított információbiztonsági vagy egyéb vállalati irányítási rendszert működtető vállalatok szembesülne: az ISO irányítási rendszerekre vonatkozó szabványok egységes szerkezetének első fejezeteként feltüntetve –, hogy a vezetői elkötelezettség kiemelt helyen szerepel minden rendszer hatékony működtetésében.

A vezetői példamutatás szerepe

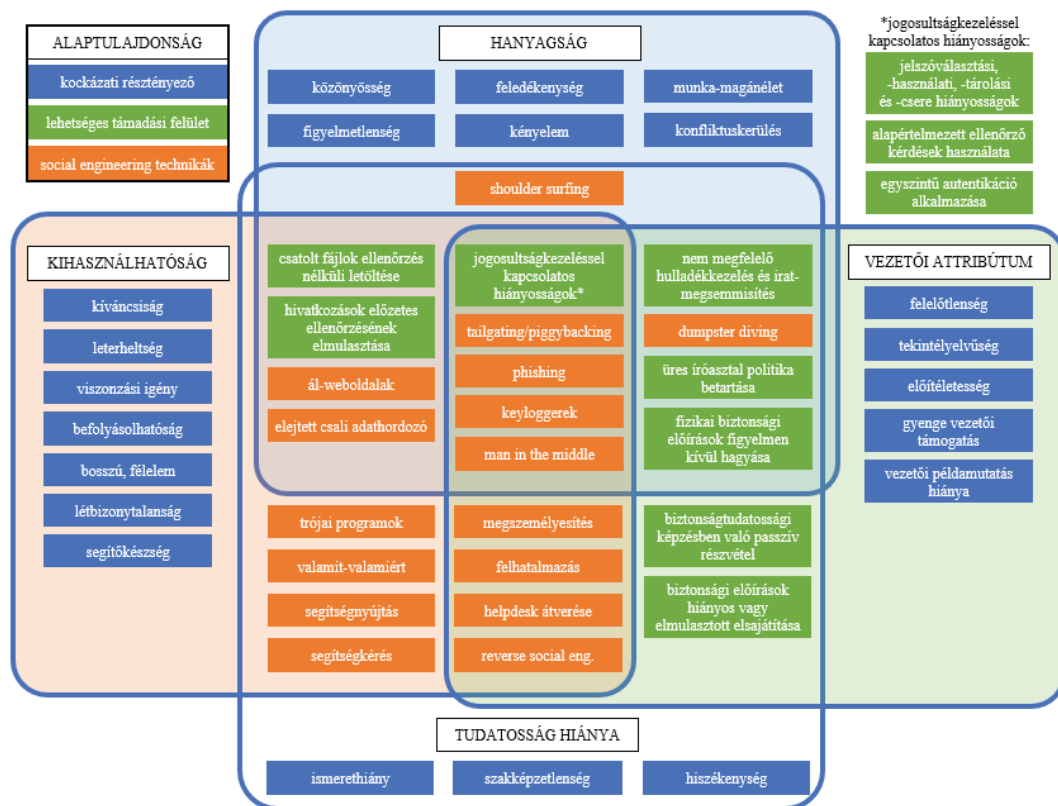
Különösen a vezetői szintekhez kapcsolódó, adott esetben bővebb vagy érzékeny adatokat kezelő tárhelyhez hozzáférést nyújtó jogosultság védelmében fontos a vezetői példamutatás a biztonsági előírások betartásában, azok betartatásának támogatása érdekében. A példamutatás azonban nem értelmezhető önállóan létező vezetői attribútumként vagy készségként, az a főbb vezetői felelősségek maradéktalan vállalásában és megfelelő feladatvégzésben, továbbá azok kommunikációjában teljesezhető ki.

Bármely szervezetben vezetői beosztásban – szintenként eltérő hangsúllyal – a közvetkező területek megfelelő egyensúlyban tartása szükséges a példamutatáshoz: célkitűzés, döntéshozatal, változáskezelés, delegáció, értékelés, irányítás, visszajelzés, problémakezelés (korrekció), konfliktuskezelés, tárgyalás (értekezletvezetés), hierarchikus eligazodás és

kreativitás. [13] Kiemelendő az irányítás, mint az egyetlen funkció, amely nem delegálható, hiszen a vezetői felelősség és pozíció lényegéhez kötött.

EREDMÉNYEK: A HUMÁN KOCKÁZATI TÉNYEZŐK HÁLÓZATA I.

A közlemény kutatási célkitűzésénél fogva a felhasználói oldal szempontjából szemlélteti a humán tényezőket, annak tükrében, hogy az egyes technikák milyen kapcsolódást mutatnak a támadási felületeken keresztül. Kutatásom későbbi szakaszában fogom elvégezni a hálózat kiegészítését, kiteljesítését mind a védelmi, mind a támadói oldal vonatkozásában felmerülő tényezőkkel.



2. Ábra: Az információbiztonság felhasználói oldali humán tényezőinek összefüggései a támadási felületekkel és technikákkal (saját szerkesztés)

A feltárt humán tényezők, az azok által képzett támadási felületek és a kapcsolódó social engineering technikák összefüggéseinek hálózata a 2. ábrán a lehetséges vizualizációs módszerek közül választott halmazábra segítségével kerül felrajzolásra, az elkészítés során azonban az elmetérkép módszerét alkalmaztam. Megjegyzendő az ábra kapcsán, hogy egyes social engineering technikák akár körvonalazható támadási felületek hiányában is hatékonyan működhetnek a humán kockázati résztényezőkön keresztül. A következő oldalon

szövegesen kiegészítem az ábrán látható viszonyok egy kiemelt részét, a halmazok elemei közötti összefüggések felrajzolása ugyanis az ábrázolás áttekinthetőségének rovására lett volna kivitelezhető. A halmazokkal történő felrajzolás ugyanakkor segít a jelenlegi korlátok között az összefüggések értelmezésében.

A szöveges kiegészítések elé bocsátom, hogy az ábrán látható egyes halmazok, metszeteik és az elemek elhelyezkedése egyik elem vonatkozásában sem jelent kizárólagosságot, azaz pl. egy social engineering technika lazán kapcsolódhat más metszethez, más alaptulajdonság által befolyásolt, illetve a szervezeti sajátosságok által meghatározott egyéb körülményekre tekintettel. Fennállnak továbbá olyan összefüggések is, amelyekben egy social engineering technika más metszetben helyezkedik el, mint amelybe elsődlegesen sorolható a kapcsolódó támadási felület (ilyen viszony mutatkozik pl. a trójai programok és a velük összefüggésben álló, technikai fókuszú ellenőrzés elmulasztása között).

Az egyszerűbb támadási felületképző hiányosságok egyszerű, valamilyen alapszintű cselekvéssel megvalósítható, ezáltal kevesebb kockázati tényező által befolyásolt social engineering technika alkalmazását (pl. shoulder surfing) vonják magukkal. A fizikai biztonsággal, előírások betartásával és szintén egyszerűen kialakuló támadási felületekkel kapcsolatos hiányosságok már minden esetben feltételezik a vezetői attribútumok hiányát, nem megfelelő megnyilvánulását, amely a tudatosság hiányának köszönhető.

Megközelítem szerint és a rendszerezésem alapján a tudatosság hiánya minden támadási felület képzésénél tetten érhető, ennél fogva foganatosíthatók a különféle social engineering technikák attól függően, hogy a szervezetben milyen szinten (általában nem azonos szinten) szerveződik a másik három alaptulajdonság. Elmondható továbbá, hogy a legtöbb összefüggésben annak ellenére történhetnek meg a támadások, hogy belső képzésekkel, tudatosság-fejlesztéssel a támadási felületek kialakulása jelentős mértékben csökkenthető (ld. következő fejezet).

A humán alapú social engineering technikák a humán kockázati résztényezők összefüggéseinek fényében javarészt a kihasználhatóságban, mint alapszintű felhasználói tulajdonságban gyökereznek. A szervezeti viszonyok ismeretén alapuló technikák (pl. megismerés, felhatalmazás, helpdesk átverése) minden esetben a vezetői hiányosságokat használják ki, hiszen megelőzhető az ilyen támadási felületek képzése a vezető általános jelenlétével, támogatásával, példamutatásával, továbbá a kapcsolódó képzések, tudatosítás elvégzésével.

A számítógép-alapú social engineering technikák összességében a legbonyolultabb összefüggésekkel rendelkeznek (ld. a 2. ábrán pl. a négy alaptulajdonság közös metszetét). Esetükben szerepet kap ugyanis a hozzájuk kapcsolódó támadási felületek képzésében mind a tudatosság hiánya, mind a kihasználhatóság, mind pedig a hanyagság. A jogosultságkezeléssel kapcsolatos, feljebb részletesen kifejtett hiányosságok adnak lehetőséget a támadói oldal részére a legváltozatosabb technikák alkalmazására, így ebben a körben szerepet kapnak már vezetői attribútumok is.

KÖVETKEZTETÉSEK, KITEKINTÉS

A biztonságtudatossági programok megvalósítása önmagában nem eredményezi a biztonságtudatosság megvalósulását (ld. előző fejezet). Az ilyen tekintetben hatékony és sikeres fejlesztés érdekében elengedhetetlen a tervezéshez szükséges információk teljes körű feldolgozása, a vezetői elkötelezettség és az ezt leképező példamutatás, a program

megvalósítását követően pedig korrekciók foganatosítása a programhoz kapcsolódó visszajelzések alapján. Következtetéseimet a fenti elemekkel kapcsolatos megállapítások formájában fogalmazom meg.

A vezetői példamutatással szemléltethető a vezetés irányítási funkciójának kiemelt szerepe az információbiztonság-tudatosság megvalósulásában, hiszen annak „célközön-sége” lehet közvetlen beosztott, nem közvetlen beosztott, azonos vagy alacsonyabb szervezeti szintű munkatárs, de akár magasabb beosztású vezető is, azaz potenciálisan a teljes szervezet. Kiemelt fontosságú a példamutatás a biztonsági területen, ahol nem csupán a vezető, hanem a teljes szakterülethez tartozó minden munkatárs felelőssége egyaránt megmutatkozik

A korrekciók implementálásához (PDCA: Act) szükséges visszajelzés (PDCA: Check) változatos formában, változó számszerűsíthetőség mellett történhet biztonságtudatossági programok esetén. Ilyen módszerek például: közvetlen reakcióértékelés, munkateljesítmény mérése a képzést követő longitudinális értékelés, a munkatársak és vezetők informális értékelése az érintett munkavállaló fejlődéséről, online valós idejű adatgyűjtés, magatartásváltozás. [14]

A számszerűsített visszajelzések elemzése objektivitást kölcsönöz, hiszen a teljesítmény, a kockázat és az ellenőrzési mutatók közötti statisztikai összefüggés kulcsfontosságú visszacsatolás, amelyre a szervezetnek szüksége van ahhoz, hogy meggyőződhessen arról, hogy a kiberbiztonsági intézkedései megfelelőek. Ugyanakkor nagy mennyiségű adat kezelésére, és megvalósítható output-ra van szükség, egyúttal a következetes és megbízható információbiztonsági mutatók felállítása bonyolult, és szakértelmet igényel. [15] Az információbiztonsági kockázatok valós idejű azonosításához és kezeléséhez segítséget nyújtanak a kulcs teljesítménymutatók, amelyekből mélyebb összefüggések mérésére alkalmas komplex mutatószámok származtathatók.

Kutatásom további szakaszára nézve az alábbi célkitűzéseket fogalmazom meg a jelen közleményben bemutatott eredményekre alapozva. Egyrészt a humán kockázati tényezők információbiztonsági vonatkozású hálózata kiegészítendő, teljessé tehető a támadói és a védelmi oldal teljes körű feldolgozásával. Másrészt tudományos-szakmai kutatási céloom egy keretrendszer felállítása, mely a hálózat alapján végzett folyamat alapú elemzés outputjától függő szakmai szolgáltatási koncepció kidolgozását teszi lehetővé.

Folyamatban van továbbá részkutatásom, mely a kockázatok számszerűsítését támogató módszerek, mutatószámrendszerek egységesítését célozza, beemelve a kulcs teljesítménymutatók mellé a ROI (befektetés-megtérülési mutató) megközelítést is, így módszertani segítséget nyújtva polgári és katonai szervezeteknek egyaránt abban, hogy a most tárgyalt humán tényezők komplex kezelésének hatékonysága is mérhetővé váljon. A hálózat, valamint az egységes számszerűsítési módszertan lehetőséget teremt a vállalatok számára folyamat alapú elemzés, visszamérés elvégzéséhez: ennek ismeretében testre szabott képzési és egyéb szakmai szolgáltatási koncepciók állíthatók fel a szervezet egésze tekintetében, amelyek hatékonysága így szervesen kapcsolódik az információbiztonsági törekvések hatékonyságához, sőt abból származtatott módon kifejezhető.

FELHASZNÁLT IRODALOM

- [1] M. G. Cains, B. Hoffman, T. Kelly and D. S. Henshel, „*Trust as a Human Factor in Holistic Cyber Security Risk Assessment*” presented at 6th International Conference on Applied Human Factors and Ergonomics 2015.
- [2] E. D. Oroszi, „*Social Engineering. Az emberi erőforrás, mint az információbiztonság kritikus tényezője*,” B.S. szakdolgozat, Budapesti Corvinus Egyetem GK, Budapest, 2008.
- [3] Cs. Kollár, „*Social engineering a gyakorlatban – Manipulációk értelmezése a SPEAKING modellben*” Jel-Kép 2017/3. pp. 62-77, 2017.
- [4] B. Kárász, „*Social Aspects of Reliability and Security Issues of Authentication Solutions*,” Hadtudományi Szemle vol. XIII. No 1
- [5] Zs. Haig, „*Információs műveletek a kibertérben*,” Budapest: Dialóg Campus Kiadó, 2018.
- [6] K. D. Mitnick, W. L. Simon, „*The Art of Deception. Controlling the Human Element of Security*,” Indianapolis, IN: Wiley Publishing, Inc., 2002.
- [7] V. Deák, „*Biztonságtudatosság az információs környezetben*,” Katonai Nemzetbiztonsági Szolgálat Szakmai Szemle Vol, XV. No. 3., pp. 59-76, 2017
- [8] M. Wilson, J. Hash, „*Building an Information Technology Security Awareness and Training Program*,” National Institute of Standards and Technology, Gaithersburg, MD, NIST Special Publication (SP) 800-50, October 2003.
- [9] J. A. Chestnut, „*Assessing the Impact of Human Error in Information Security Incidents*,” Mississippi, MI: Bell & Howell Information and Learning Company, December 2000.
- [10] M. Karoliny, J. Poór Eds., „*Emberi erőforrás menedzsment kézikönyv – Rendszerek és alkalmazások*,” Budapest: Wolters Kluwer Kiadó, pp. 365-383, 2015.
- [11] B. P. Hámornik, Cs. Krasznay, „*A Team-Level Perspective of Human Factors in Cyber Security: Security Operations Centers*” In: D. Nicholson Ed. *Advances in Human Factors in Cybersecurity: Proceedings of the AHFE 2017 International Conference on Human Factors in Cybersecurity*; Springer International Publishing, pp. 224-236. 2017.
- [12] H. Stewart, J. Jürjens, „*Information Security Management and the Human Aspect in Organizations*,” Information & Computer Security Vol. 25 No. 5, pp. 494-534, 2017.
- [13] D. Eppling, L. Magnien, „*Leadership in Action – What Great Managers Really Do*” Krauthammer, 2005.
- [14] B. Kárász, „*Biztonságtudatossági tréningek hatékonyságának vizsgálata*,” Hadmérnök, Vol. XIV. No. 2., pp. 313-324. [online] http://hadmer-nok.hu/192_26_karasz.pdf (Letöltés ideje: 2020.03.31.)
- [15] Cs. Kollár, „*Mutatószámok a szervezetek életében, különösen az információbiztonság területén*,” pp. 111-125. In. B. Bencsik, I. Sabjanics Eds., I. „*Digitális környezetünk fenyegetettsége a mindennapokban*,” Budapest: Dialóg Campus 2018.

**THE IMPORTANCE OF FLOOD HIROLOGY
IN ENVIRONMENTAL PROTECTION****AZ ÁRVÍZHIDROLÓGIA JELENTŐSÉGE A
KÖRNYEZETVÉDELEMBEN**KERÉK Gábor¹**Abstract**

The fight against river floods is a historical heritage in our country. Hungary is constantly exposed to the anomalies of surface water entering the country in both quantitative and qualitative aspects. We have been living together for centuries with the destructions of waters and we strive to mitigate their harmful effects. Recently, floods have also become an environmental factor due to overuse of river basins, urbanization and anthropogenic impacts. In this paper, the author analyzes the importance of hydrologic forecasts for operational water quality remediation operations, as well as the importance of hydrologic statistical studies onto the determination of the relevant flood level in context with the planning and permitting tasks. Finally presents - in context with last year's "Hableány disaster" - the relationship between hydrology and environmental protection by representing its hydrological and flow regulational aspects.

Keywords

hydrology, flood protection, environmental protection, hydrologic forecasting, PET-cup, Hableány-disaster, Danube flooding, flow regulation

Absztrakt

Hazánk történelmét végigkíséri a folyók elöntései elleni küzdelem. Magyarország folyamatosan kitett az országba érkező felszíni vizek mennyiségi és minőségi anomáliáinak. A vizek kártételeivel évszázadok óta élünk együtt, és törekszünk a káros hatásaik mérséklésére. Az utóbbi időszakban a vízgyűjtők túlhasználata, az urbanizáció és antropogén hatások miatt környezetvédelmi tényezővé is váltak az árvizek.

A szerző ebben a cikkben elemzi a hidrológiai előrejelzések fontosságát a folyók operatív vízminőségi kárelhárítási műveleteinek vonatkozásában, valamint a hidrológiai statisztikai vizsgálatok jelentőségét a tervezési-engedélyezési feladatok alapját jelentő mértékadó árvízszint meghatározásában, és a nagyvízi mederkezelési tervek kapcsán. Végezetül a tavalyi évi „Hableány-tragédia” hidrológiai és vízkormányzási feladatain keresztül mutatja be a hidrológia és a környezetvédelem kapcsolatait.

Kulcsszavak

hidrológia, árvízvédelem, környezetvédelem, hidrológiai előrejelzés, PET-kupa, Hableány-katasztrófa, Duna-árhullám, vízkormányzás

¹ kerek.gabor@eduvizig.hu | ORCID: 0000-0002-5804-3594 | doktorandusz / PhD Student | National University of Public Science Doctoral School of Military Engineering / Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola

BEVEZETÉS

A lakosság veszélyek elleni védelme a kezdetektől fogva régi törekvése a társadalmaknak. A különböző államok mindig gondot fordítottak az országuk és annak állampolgárai védelmére. Ez a kezdetekben „csak” az adott ország határainak, szuverenitásának, diplomáciai és szükség esetén fegyveres megóvásában nyilvánult meg. A védelem intézményesített formái eleinte az ország idegen erők behatolása elleni katonai védelmét jelentették, de később kiterjedt a lakosság más jellegű veszélyek elleni védelmére, életének és anyagi javainak megóvására is [1, 132. o.].

Ilyen veszélyt jelent napjainkban a környezet terhelése és károsítása, amelynek az emberek egészségére, életére is komoly kihatása van. A környezetvédelmi világprogramok és egyezmények ellenére, a környezet terhelése olyan méreteket öltött, hogy minden területnek el kell gondolkodnia, hogy hogyan járulhat hozzá a környezet védelméhez. A vizek kártétele az egyik legősibb környezetterhelő tényező. Az árvizek nemcsak a természeti, de az épített környezetet is sújtják. Az emberiség örök törekvése az ellenük való védelem. Az árvizek kezelésének, az ellenük való védekezésnek egyik fontos területe az árvízhidrológia, amely nem csupán egy szakmai terület, hanem a környezeti károk mérséklésének is egy fontos eszköze. Felmerül a kérdés, hogy milyen módon segítheti az árvízhidrológia a környezet terhelésének csökkentését, a környezet védelmét. Kérdés továbbá, hogy milyen szerepe lehet a hidrológiai előrejelzéseknek és elemzéseknek a vízbaleseteket követő vizsgálatokban. A kérdések megválaszolása érdekében bemutatom hazánk árvízi kitétséget, annak általános összefüggéseit a védelmi szférával, majd bemutatom az árvízi előrejelzések és az árvízhidrológiai vizsgálatok jelentőségét a folyóinkat érő szennyezések elleni operatív védekezésben és azok tervszerű prevenciójában. Megvizsgálom továbbá a 2019. májusi Hableány-katasztrófa során elrendelt vízkormányzási beavatkozások hatásait, azok kimenetelét a mentési munkákra.

MAGYARORSZÁG ÁRVÍZI KITÉTTSÉGE ÉS ENNEK KAPCSOLATA A VÉDELMI SZFÉRÁVAL

Hazánk medencejellege okán folyamatosan kitétt az Alpokból és a Kárpátokból érkező vizek mennyiségi és minőségi ingadozásainak. A XVIII. század második felében megkezdődött folyamszabályozási és árvíz-mentesítési munkák megkezdéséig a hegyvidéki területekről leérkező, és a síkvidéken „elterülő” árvizek jelentős területeket öntöttek el. E tény bizonyítéka az ún. „pocsolyatérkép”, mely a Kárpát-medence vízborította és időszakosan vízjárta területeit ábrázolja az árvízmentesítések megkezdése előtt [2]. A vizek hiányából, de sokkal inkább káros többletből fakadó kitétség a civil lakosság és a katonai erő számára is talán a legjelentősebb természeti veszélyforrást jelentette a múltban, és jelenti ma is hazánkban. A múltban a folyók rendezetlensége miatt egyes katonai műveletek végrehajtását közvetlenül nehezítette, vagy lehetetlenné tette el egy-egy árvíz. Ezzel szemben napjainkban a katonai tevékenység e téren sokkal inkább az árvízi védekezés támogatásában jelentkezik.



1. ábra A Kárpát-medence vízborította és árvízjárta területei az ármentesítő munkálatok megkezdése előtt[2]

Jelenleg Magyarország területének mintegy harmada mentesített ártér², ez a tény már önmagában meghatározza az ország árvíz-veszélyeztetettségét. Ez a kiterjedtség napjainkban az árvíz elleni védekezésért felelős szervezetek - Országos Vízügyi Főigazgatóság (továbbiakban: OVf) és az ország területén vízgyűjtőhatárok mentén szervezett 12 területi vízügyi igazgatóság³ - és a Magyar Honvédség együttműködésére erős befolyással bír, hiszen egy jelentősebb árvízi védekezés esetén a katonai erő és eszközállománya számos esetben elengedhetetlen a sikeres védekezés megoldásában. Ennek az együttműködésnek a közelmúlt nagy árvizei során számos jó példája felsorolható. Ilyen volt a Duna-völgyi 2013-as rekordárvíz során pl. Győrújfalú védelmében végrehajtott közös védekezés, a 2006-ban a Tisza-völgyében kialakult hosszú árvízi helyzet közös megoldása a Hármas-Körös torkolati szakaszán, Csépa és Szelevény térségében, vagy a 2001. évi beregi árvíz során tapasztalt együttműködés, melynek során hazánk mindezülig utolsó töltésszakadással járó árvízi helyzetét kellett megoldani a Felső-Tiszán, Tarpa térségében. Valamennyi védekezési munka közös jellemzője volt, hogy sikere jelentős részben a katonai erő hatékony alkalmazásának volt köszönhető, ami kombináltan jelentette az élőerő alkalmazását, és légi, valamint kételtű szállítójárművek használatát. A fent felsorolt három eset mindegyike szintén megegyezett abban, hogy a kritikus helyzet csak a bevetett katonai erő hatékonysága okán volt kezelhető. A vízügyi szolgálat eszköz- és élőerő-állománya egy esetben sem volt elegendő az egyedüli sikeres védekezéshez, kulcsfontosságú volt a közös védekezés. Ezekben az esetekben a Rendőrség közreműködése is elengedhetetlen volt a rend fenntartása érdekében. Ezen túlmenően, a védelmi igazgatás szervei, valamint a civil védelmi szervezetek bevonására is szükség volt. A védelmi feladatok ellátása során tehát megvalósul a védelem komplex rendszerének működtetése. Ennek célja a károk mérséklése, az eszkalálódás megakadályozása és a károk felszámolása, mely egyben a környezet védelmét is szolgálja.

² az a terület, amelyeket az árvizek árvízvédelmi létesítmények hiányában elöntենek

³ Észak-dunántúli – Győr, Közép-Duna-völgyi – Budapest, Alsó-Duna-völgyi – Baja, Közép-dunántúli – Székesfehérvár, Dél-dunántúli – Pécs, Nyugat-dunántúli – Szombathely, Felső-Tisza-vidéki – Nyíregyháza, Észak-Magyarországi – Miskolc, Tiszántúli – Debrecen, Közép-Tisza vidéki – Szolnok, Alsó-Tisza vidéki – Szeged, Körös-vidéki - Gyula

AZ ÁRVIZEK ÉS EGYÉB VÍZKÁRELHÁRÍTÁSI ESEMÉNYEK KÖRNYEZETI KOCKÁZATAI

Az árvíz, mely a klasszikus értelmezés szerint a vizek káros mennyiségi többlete, napjainkra elsősorban a vízgyűjtők intenzív mezőgazdasági hasznosítása, másrészt az egyre jellemzőbb urbanizáció és antropogén hatások miatt, több szempontból, környezetvédelmi-környezetterhelési tényezővé is vált. A folyók ár- és hullámterein létesített, vagy illegálisan elhelyezett hulladék napjaink egyik legnagyobb és egyben legköltségesebb kihívását jelenti az árvizek és a hulladék kezelésében. Különösen hazánk keleti szomszéd államai (Ukrajna, Románia) felől érkező folyóink esetében igaz, hogy a felső folyószakaszok árterét (vagy hullámterét) illegális hulladéklerakóként használják, melyeket a hirtelen vízszintváltozások, árhullámok rendszeresen mosnak el, és szükségképpen – úszó hulladékként – a magyar folyószakaszokon hatalmas mennyiségben jelenik meg a zömében műanyag hulladék. Az utóbbi időszak tiszai árvizei (jellemzően a 2006. évi tavaszi árvíz óta) esetében rendszeresen visszatérő problémaként jelentkezik, hogy a vízgyűjtőterület Kárpátaljai felső részéről a levonuló árhullámok jelentős mennyiségű műanyag hulladékot szállítanak a folyó magyar szakaszára. Ezek a környezetterhelési kockázatok számottevő mértékben rendszerint határon túlról érkeznek, ennek okán az ellenük való védekezés szinte kizárólag operatív kárelhárítással oldható meg, azok tervszerű megelőzésére gyakorlatilag nincs mód, a szennyezés haváriaszerű.



2. ábra PET palackkal jelentősen szennyezett uszadék a Tiszán 2010-ben (készítette a Szerző)

Hazai viszonyok között folyóink és kisvízfolyásaink környezetterhelési kockázatait az ipari üzemek szintén haváriaszerű szennyezései jelenthetik. Ilyen volt 2010 októberében hazánk egyik legjelentősebb ipari katasztrófája a MAL Zrt. ajkai vörösiszap-tárolójának gátszakadása, mely a Torna-patak völgyén keresztül a Marcal folyón okozott jelentős környezetszennyezést és természetkárosítást. A haváriaszerű szennyezéseken túlmenően, a mezőgazdasági területekről a vízfolyásokat terhelő diffúz tápanyagterhelés jelenthet további jelentős környezetterhelést, kiváltképp olyan heves vízjárású kisvízfolyásokon, amelyek esetében fennáll a völgyi elöntések veszélye, ahol intenzív mezőgazdasági termelés folyik.

Tipikusan ilyen kisvízfolyás a Cuhai-Bakonyér, amely 2010 tavaszán a Zsófia és Angéla névre keresztelt ciklonok nyomán kialakult árhullámok alkalmával jelentős árvízhozamokat szállított a Bakony É-i lejtőiről. A síkvidéki mederszakaszokon számottevő völgyi elöntés alá kerültek a mezőgazdasági területek, amelyekről jelentős tápanyagterhelés érte a vízfolyást. A 3. ábrán a Cuhai-Bakonyér széles völgye látható Bőny mellett, a 2010. májusában, illetve 2020. márciusában. A képek jól érzékeltetik, hogy a patak medre a jelentősebb árvízhozamokat nem képes kiöntés, és károkozás nélkül levezetni, így az árvíz egy része azt megkerülve a völgyben vonul le. Intenzív mezőgazdasági hasznosítás esetén ilyen esetben növényi tápanyagokban (nitrogén- és foszforformák) gazdag, esetleg növényvédőszerrel szennyezett víz kerül a vízfolyásba, illetve annak befogadójába, amennyiben a teljes kiömlött árvíz tömeg a völgyben marad. Az ilyen jellegű vízszennyezések általános jellemzője, hogy területi kiterjedésük okán monitorozásuk gyakorlatilag nem lehetséges.



3. ábra , A Cuhai-Bakonyér völgye, Bőny, 2020. március, és ugyanaz a helyszín 2010 május 17. (készítette a Szerző)

Hajózható folyóink jellemző környezetterhelési kockázatát jelentik a különböző szénhidrogén-származékok okozta szennyeződések, amelyek szintén a haváriák kategóriájába sorolhatók.

A vízminőségi problémák közös jellemzője, hogy szemben az ár- és belvizekkel, valamint az aszálykárokkal rendszerint nincsenek determinisztikus kapcsolatban természeti tényezőkkel, vagyis vízminőségi kár gyakorlatilag bárhol, bármikor, bármekkora volumenben előfordulhat. Ellentétben egyéb – mennyiségi – vízkárelhárítási eseménnyel (árvíz, belvíz, villámárvíz-helyi vízkár) a vízminőségi káresemények rendszerint közvetlen vagy közvetett antropogén hatások eredményei. Természetesen kedvezőtlen meteorológiai, – biokémiai folyamatok eredményeként természetes okok is kiválthatnak vízminőségromlást, de ezek a jelenségek viszonylag ritkák.

Folyóink hidrológiai jellemzőinek operatív vagy statisztikai vizsgálata a mennyiségi jellemzőkön kívül, számos esetben szolgálhatja a vízminőségvédelem, és ezzel a környezetvédelem érdekeit. Az árvízhidrológia a vízjárás jellemzők statisztikai alapú meghatározásán keresztül fontos alapadatokat szolgáltat a tervezési feladatok, stratégiai tervek megalapozásához. Az árvízi előrejelzés, mint a vízkárelhárítás egyik alappillére kulcsfontosságú döntéstámogató eszköz a vízminőségvédelmi intézkedések előkészítésében.

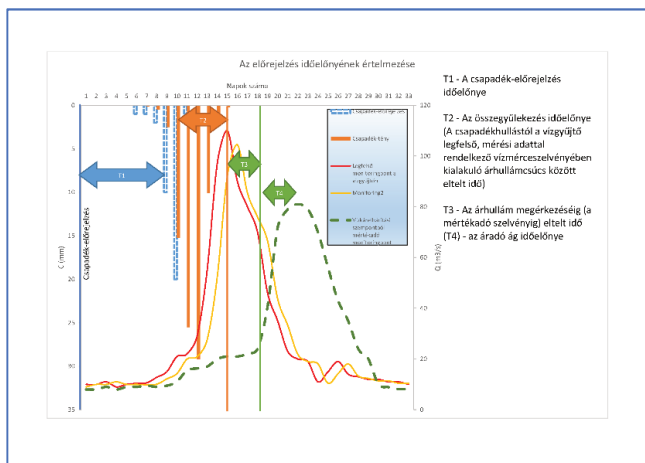
A VÍZKÁROK KÖRNYEZETI KOCKÁZATAINAK CSÖKKENTÉSI LEHETŐSÉGEI MŰSZAKI HIDROLÓGIAI MÓDSZEREKKEL

Az operatív hidrológiai monitoring és előrejelzés szerepe a vízszennyezések kezelésében

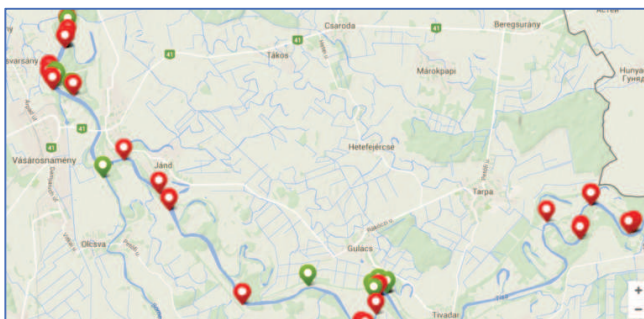
Folyóink és vízfolyásaink vízjárásának mindenkori ismerete és várható alakulásának monitorozása, előrejelzése számos vízgazdálkodási feladat alapja, így az árvízi védekezésért felelős szervezetek munkájában, valamint a katasztrófavédelmi veszélyhelyzeti tervezésben is kiemelt jelentőségű. A vízminőségi kárelhárításban a kritikus védelmi szituációk elkerülését segíthetik a hidrológiai előrejelzések, amelyek segítségével egy-egy meteorológiai-hidrológiai esemény várható nagyságrendje, ezáltal várható hatásai számszerűsíthetők. Az előrejelzések két legfontosabb mérőszáma az ún. védekezési időelőny, és a beválási pontosság. A beválási pontosságot az árvízi előrejelzési gyakorlatban minden esetben egy ún. bizonytalansági sávval jellemezzük, az időelőny alatt pedig egy-egy előrejelzési produktum publikálását és az előrejelzett esemény bekövetkezéséig hátralévő idő megállapítását értjük. Ez az idő egy-egy, esetleg katonai erőt, vagy ágazati operatív beavatkozó egységet is igénylő művelet tervezése és levezénylése szempontjából kritikus fontosságú. Ezt a 4. sz. ábrán szemléltettem. Jól látható, hogy mivel egy-egy hidrológiai eseménynek minden esetben meteorológiai előzményei vannak, a meteorológiai előrejelzés publikálásának időpontja jelenti egy műszaki beavatkozás első becsülhető időszükségletét (az ábrán T1). Az esetek döntő többségében ez az időelőny operatív beavatkozások tervezéséhez nem nyújt megfelelő támogatást, hiszen magában hordozza a meteorológiai előrejelzések által magukban hordozott – olykor jelentős – tér- és időbeni bizonytalanságot; azonban egy-egy esemény nagyságrendi előrebecslésére (korai figyelemfelhívásra, figyelmeztetésre) alkalmas lehet. Egy műszaki beavatkozás (pl. vízszennyezés felszámolására) operatív tervezésére a lehullott csapadékból számított felszíni lefolyás előrejelzési időelőnyje ad kielégítő támogatást (az ábrán T2), mivel már valós eseményeken alapuló, analitikus meghatározás eredménye. Ez az időelőny természetesen az árhullám levonulásának ütemében növekszik a folyó- vagy vízrendszer alsóbb vízmérceszelvényeiben⁴. Hazánkban az OVF szervezeti keretein belül működő Országos Vízjelző Szolgálat (továbbiakban: OVSz) a felelős szervezet a folyóink vízjárásának előrejelzésére. Eredményeik a <http://www.hydroinfo.hu/> honlapon érhetőek el, diszkrét vízmérceszelvényekben 144 órás időelőnyű folyamatos vízjárás előrejelzést adnak közre. Árvizek levonulásának esetén azonban a helyi védekezésért felelős szervezetek az árvízi védekezés műszaki, logisztikai, gazdasági támogatása érdekében saját előrejelzéseket is készítenek. Közös jellemzőjük az OVSz előrejelzéseivel, hogy diszkrét vízmérceszelvényre korlátozódnak, azonban kiszolgálhatnak speciális helyi igényeket is, és jellemzően csak az árhullámkép előrejelzésére terjednek ki időben. Az igazgatóságokon alkalmazott módszerek a közelmúltig zömében papír alapú grafikus kapcsolat elemzések alapján történtek, azonban az elmúlt évtizedben a számítástechnika, a térinformatika és a hidrológiai monitoring robbanásszerű fejlődése (pl. nagy tér- és időbeli felbontású

⁴ egy folyó vagy állóvíz vízszintjének (vízállásának) meghatározására szolgáló eszköz a folyó meghatározott szelvényeiben telepítve

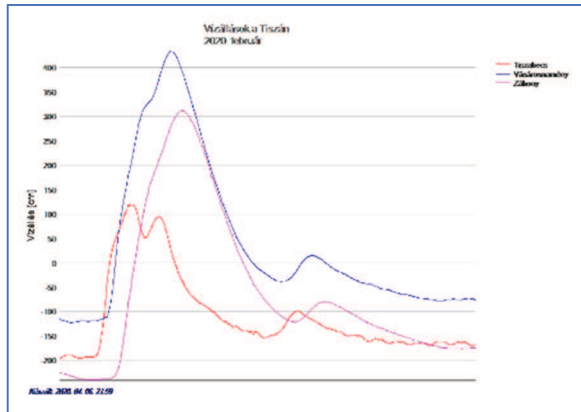
vízhozammérő eszközök, vízszint-távmérés, hidrodinamikai modellek széleskörű elterjedése és alkalmazásuk oktatása a műszaki felsőoktatásban stb.) magával hozta a hidrológiai előrejelzések fejlesztésének igényét is. Ennek eredményeként e szakterületen is megjelentek az online, folyamatos rendelkezésre állású előrejelző modellek, matematikai-statisztikai alapú kapcsolat elemző szoftverek, és a nagy tér- és időbeli felbontású monitoring-rendszerek [3].



4. ábra, Az árvízi előrejelzés időelőnyének értelmezése (szerkesztette: a Szerző)



5. ábra, PET-kupa hulladékmonitoring applikáció képe [4]

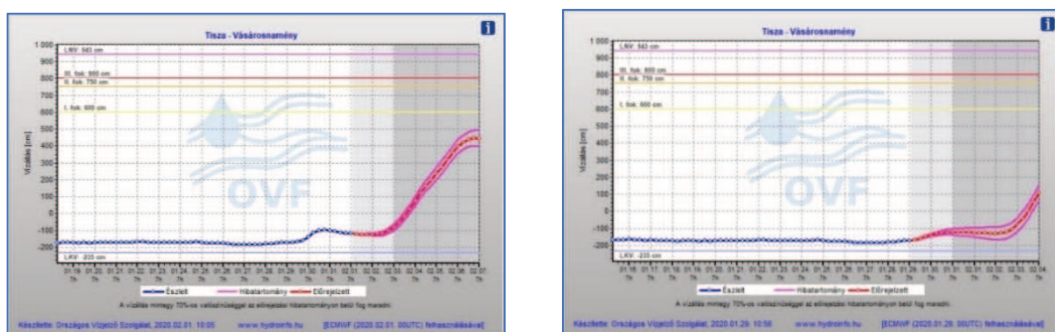


6. ábra Mért vízállások a Felső-Tiszán, 2020. február [5]

Az árvízi előrejelzés mindezek mellett hatékonyan szolgálhatja a vízminőségi kárelhárítást is, hiszen az utóbbi idők tapasztalatai és helyszíni felmérései alapján, főként a Tisza vízgyűjtőterületén továbbra is jelentős a lakosság és az ipar részéről a hulladék felhalmozása a hullámtereken és a folyók vízjárta területein. Számottevő kezdeményezésként említhető az ún. tiszai PET-kupa, amely 2013 óta számos civil kezdeményezéssel hívja fel a figyelmet a probléma súlyosságára, és visszatérő mivoltára [4]. A szemétszedő akciók mellett állami és intézményi támogatással hulladék-monitoring, és ahhoz kapcsolódó adatbázist és vízminőségi mérési programot hoztak létre. Az eredményeket a vízminőségi kárelhárítást végző vízügyi igazgatóságok rendelkezésére bocsátották a védekezés támogatása céljából. Korunk technikai lehetőségeit kiaknázva a hulladék-monitoring adatbázis mobilapplikációkon keresztül is hozzáférhető, és szerkeszthető [4]. Mivel a hulladék annak hullámtéri deponálása okán fokozottan kitett a folyók vízszint-változásaiból fakadó elmosásnak, a védekezés szempontjából a hidrológiai előrejelzések kulcsfontosságúak, mivel egy megfelelő helyen elvégzett műszaki beavatkozással szinte a teljes magyar folyószakaszt mentesíthetik a hulladékszennyezéstől. 2020 februárjának első napjaiban intenzív vízszintemelkedés alakult ki a felső-Tiszán, mely a folyó kárpátaljai vízgyűjtőterületeiről jelentős mennyiségű úszó hulladékot indított útjára Magyarország felé. A magyar szakasz felső vízmércéin mért vízállások a 6. ábrán láthatók. Jól látható, hogy a folyó felső vízmércéin intenzív vízszint-emelkedéseket mértek, amely árvízvédelmi szempontból nem tekinthető jelentősnek, azonban a vízgyűjtők felső szakaszán deponált hulladékot képes volt a hullámterek mélyebb részéről elmosni. Az Országos Vízeljáró Szolgálat az árhullámot 144 óra időelőnyvel, kielégítő pontossággal előrejelezte. A 7. ábrán látható grafikonokon az OVSz által publikált árhullámképeket ábrázoltam, melyeken látható, hogy a Tiszán az árhullám érkezését már a vásárosnaményi tetőzés előtt 8 nappal jelezte a Szolgálat. 5 napos időelőnyvel pedig a tetőzés várható szintje és időpontja is előrejelezhető volt [6]. Ez az időelőny megfelelőnek bizonyult, hogy az OVF és a Felső-Tisza vidéki Vízügyi Igazgatóság (továbbiakban: FETIVIZIG) felkészüljön az operatív vízminőségi kárelhárításra, aminek keretében már nem sokkal az országhatár alatt, Vásárosnamény térségében lokalizálni lehetett az árhul-

lámával menetrendszerűen megérkező zömében műanyag hulladékot. Emellett ez az időelőny a lakosság védelme érdekében is jól kiaknázható, hiszen szükség esetén időigényes döntések meghozatalára adhat módot. A művelet során a 8. ábrán látható géplánc segítségével a FETIVIZIG több tonna hulladékot távolított el a folyóból. A feladat sikeres végrehajtása a tervszerűen lebonyolított kárelhárítási munkán túl, nem kis arányban a civil hulladék-monitoringnak, a FETIVIZIG online webkameráinak és megfelelő hidrológiai előrejelzésnek volt köszönhető.

Az operatív hidrológiai monitoring és előrejelzés kapcsolata a környezetvédelemmel tehát meglehetősen szoros a vízminőségi anomáliák kezelése és megelőzése terén is. Azok megelőzésében a hidrológiai és árvízi előrejelzések mellett, a monitoring-adatok hosszú idejű statisztikai vizsgálatait, valamint az azok felhasználásával készült hidrodinamikai modellek tapasztalatai adnak segítséget.



7. ábra Tisza-Vásárosnamény, előrejelzett vízállások, 2020. január 29-február 1. [6]



8. ábra Úszó műanyag hulladék lokalizálása a Felső-Tiszán, 2020. február [7]

Hidrológiai statisztikai vizsgálatok – Mértékadó nagyvízhozamok, és környezetvédelmi jelentőségük

A vízszennyezések elleni tervszerű védekezés alapja töltésezett folyókon, és az azokba torkolló vízfolyások torkolati szakaszain az ún. mértékadó árvízszint (a továbbiakban: MÁSZ). Ennek a vízszintnek a biztonsággal növelt értékére kell valamennyi vízlétesítményt, vagy azzal összefüggésben minden építményt tervezni és megvalósítani a folyók hullámterében, illetve vízjárta területein. Jelentőségéről és jelentéséről a folyók mértékadó árvízszintjeiről szóló 74/2014. (XII. 23.) BM rendelet 1. § (1) (2) bekezdés ír:

1. § (1) A folyók mentén és az azokba torkolló vízfolyások, csatornák visszatöltésezett szakaszain az árvízvédelmi műveket, továbbá a folyók nagyvízi medrét vagy az árvízvédelmi műveket keresztező, vagy a nagyvízi mederben elhelyezkedő építményt, vezetékét vagy egyéb létesítményt (a továbbiakban együtt: létesítmény) a folyókra jellemző hidrológiai viszonyok alapján, az 1. mellékletben meghatározott mértékadó árvízszintek figyelembevételével kell megtervezni, méretezni és megvalósítani.

(2) A mértékadó árvízszint a jégmentes árvíznek az 1%-os valószínűségű vízhozamból származtatott vízszint, amelyet hatévenként felül kell vizsgálni. A felülvizsgálatnak minden esetben meg kell előznie a nagyvízi meder, a parti sáv, a vízjárta és a fakadó vizek által veszélyeztetett területek használatáról, hasznosításáról, valamint a folyók esetében a nagyvízi mederkezelési terv készítésének rendjére és tartalmára vonatkozó szabályokról szóló 83/2014. (III. 14.) Korm. rendelet 17. § (3) bekezdésében előírt nagyvízi mederkezelési tervek felülvizsgálatát.

A MÁSZ valamennyi töltésezett folyókon egy vízfelszín-görbe magasságilag abszolút értelmű helyzetét jelenti. Meghatározásának alapja a statisztikailag 100 évente egyszer előforduló (vagy 1%-os előfordulási valószínűségű) nagyvízhozam jelenti, melynek levonulását 1 dimenziós hidrodinamikai modellel szimuláljuk a folyórendszeren.

Az 1%-os árvízhozam meghatározása a műszaki hidrológia egyik legfontosabb alapfeladata, melyet hazánkban a vízrajzi-hidrológiai monitoring-adatok immár 120 éves múltja visszatekintő strukturált tárolása és hozzáférhetősége tesz lehetővé. A szükséges információkat egy-egy vízmérceszelvény vízhozam-idősorainak hidrológiai (matematikai) statisztikai eloszlásvizsgálatával határozhatjuk meg. A Duna és mellékfolyóinak vonatkozásában a legutolsó átfogó hidrológiai statisztikai vizsgálat a 2013. évi dunai rekordárvízvet követően történt, ami a jelenleg hatályos MÁSZ meghatározásának alapja volt. Ennek környezetvédelmi vonatkozásai a jövőben tervezett árvízvédelmi és hullámtéri beruházások vízjogi és környezetvédelmi engedélyeztetési eljárásaiban jelennek meg, hiszen árvízjárta területen bármilyen létesítmény e szintek betartásával tervezhető és engedélyezhető.

Szintén az 1%-os előfordulási valószínűségű árvízhozam az alapja az ún. nagyvízi mederkezelési terveknek (továbbiakban: NMT), melyek a 2013. évi Duna árvíz tapasztalatainak hatására készültek. A Kormány 1979/2013. (XII. 23.) a vízkárelhárítás és az öntözés hatékonyságának növelését biztosító intézkedésekről szóló határozatának 2. pontjában az árvízszintek további emelkedésének megakadályozása érdekében, felhívta a belügyminisztert és a vidékfejlesztési minisztert a vízgazdálkodásról szóló 1995. évi LVII. törvény (a

továbbiakban: Vgtv.), valamint a nagyvízi medrek és a parti sávok hasznosításával és kezelésének rendjével kapcsolatos szabályozás felülvizsgálatára, továbbá a belügyminisztert a nagyvízi mederkezelési tervek elkészítésére [8].

Ezek a nagyvízi mederkezelési tervek 2015-ben elkészültek, és részletes intézkedési programokat tartalmaznak a hullámterek, árterek, árvízlevezető sávok rendezésével, hasznosításával összefüggésben. A nagyvízi mederkezelési terv célja az árvízlevezető képesség hosszú távú biztosítása. Minimális célkitűzés, hogy a kialakuló árvízszintek további növekedését el kell kerülni, mivel az exponenciálisan növeli a kialakuló veszélyhelyzetet. Alapelvként kell tekinteni, hogy a nagyvízi meder elsődleges funkciója a mértékadó vízhozam kártétel nélküli levezetése. Ebben az összefüggésben tehát a környezet védelmét is szolgálja. Az integrált vízgazdálkodási tervezés irányelveit követve a nagyvízi medrek árvízlevezető funkciója mellett, figyelembe kell venni minden olyan tevékenységet, funkciót, amely ezekhez a területekhez kötődik. Az árvízi vízszállító-képesség javítása érdekében lehetséges egyes beavatkozások műszaki, hidrológiai-hidraulikai, hajózási, ökológiai, vízminőségi, vízbázis védelemi, turisztikai, mezőgazdasági erdészeti, halászati, idegenforgalmi várható hatásait értékelni kell [8]. Itt kell feltétlenül említést tennünk a tervek környezetvédelmi vonatkozásairól, mivel azok jó támpontot adnak egy-egy környezetvédelmi beruházás tervezéséhez is.

Az NMT-k a nagyvízi medrek funkcióit az árvízlevezető képesség prioritásait (hidraulikai ellenállás, területhasználatok, beépítettség) figyelembe véve jelölik ki, melyeket 2 dimenziós hidrodinamikai modellek segítségével határoztak meg [8].

A MŰSZAKI HIDROLÓGIA NYÚJTOTTA LEHETŐSÉGEK KIAKNÁZÁSA EGY KÖZELMÚLTBAN TÖRTÉNT HAJÓBALESET TAPASZTALATAI ALAPJÁN

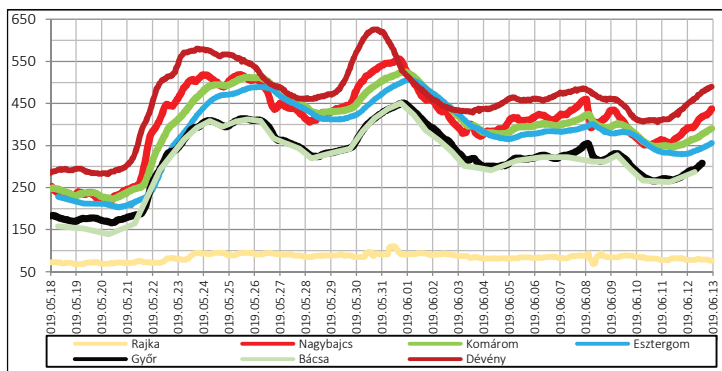
A Budapesti Rendőr-főkapitányság 2019. május 29-én 21:14-kor kapott bejelentést arról, hogy a Dunán felborult és elsüllyedt egy turistákat szállító sétahajó, a Kossuth Lajos tér közelében. Mint később kiderült a Panoráma-Deck Hajózási Kft. által rendezvényhajóként üzemeltetett, 60 ember befogadására képes, 27 méter hosszú, 150 lóerős motorral felszerelt, Hableány nevet viselő hajó volt a balesetben elsüllyedt hajó, amelyen 35-en tartózkodtak, egy dél-koreai turistacsoport 33 tagja és a kétfős magyar személyzet. A balesetet a Viking Sigyn nevű szállodahajó okozta [9].

Az eseményt rögzítő ipari kamerák felvételei és a katasztrófa minden részletét felmérő rendőrségi vizsgálat alapján valószínűsítik, hogy a maximálisan 28 km/h sebességre képes, ezer tonnás Viking Sigyn 13-14 km/h sebességgel utolérve a negyven tonnás Hableányt, a tatjának ütközött, és megperdítette a jóval kisebb méretű hajót majd maga alá gyűrve tovább görgette a víz alatt. Van olyan feltételezés is, hogy nem maga a sebességkülönbség okozta az ütközést, hanem amikor a Viking Sigyn orra a Hableány fara mellé ért, akkor a hajók közötti kis távolság és az erős áramlás miatt Bernoulli törvénye szerint a nagyobb hajó magához „szippantotta” a kisebbiket. A Hableány az oldalára fordult és hét másodperc alatt elsüllyedt [9]. Vizsgáljuk meg a hidrometeorológiai összefüggéseket!

A tragédia napjaiban a következő hidrometeorológiai helyzet jellemezte a Duna vízjárását:

Egy lassan mozgó, hullámozó frontrendszer hatására 2019. május 20-22. között területi átlagban is jelentős csapadék hullott a Duna felső szakaszának térségében, majd a Morva és a Vág vízgyűjtőin. Néhány nap szünetet követően egy dél felől felhúzódó mediterrán ciklon hatására 2019. május 27-29. között területi átlagban ismét számottevő csapadék hullott a Duna több részvízgyűjtőjén és az Észak-dunántúli Vízügyi Igazgatóság (továbbiakban: ÉDUVIZIG) területén. Az ezt követő napokban már sehol nem volt jelentős csapadék. 2019 júniusától pedig lényegében csapadékmentessé vált az időjárás, határozott felmelegedés kezdődött [10].

A csapadék hatására a magyarországi Duna-szakaszon két egymást követő, készült-ségi szintet elérő árhullám alakult ki. Az egyes vízmércéken mért vízállásokat a 9. ábrán követhetjük nyomon:



9. ábra Vízállások a Dunán, 2019. május-június [10]

A balesetet követő napokban megkezdődött műszaki mentést a Terrorelhárítási Központ koordinálta. A hajótest kiemelését több napos műszaki-logisztikai tervezési fázis előzte meg, amiben a hidrológiai – hidraulikai viszonyok feltárása és előrejelzése, valamint intenzív figyelőszolgálat ellátása a vízügyi ágazat (OVF, és a Duna-menti vízügyi igazgatóságok) feladata volt.

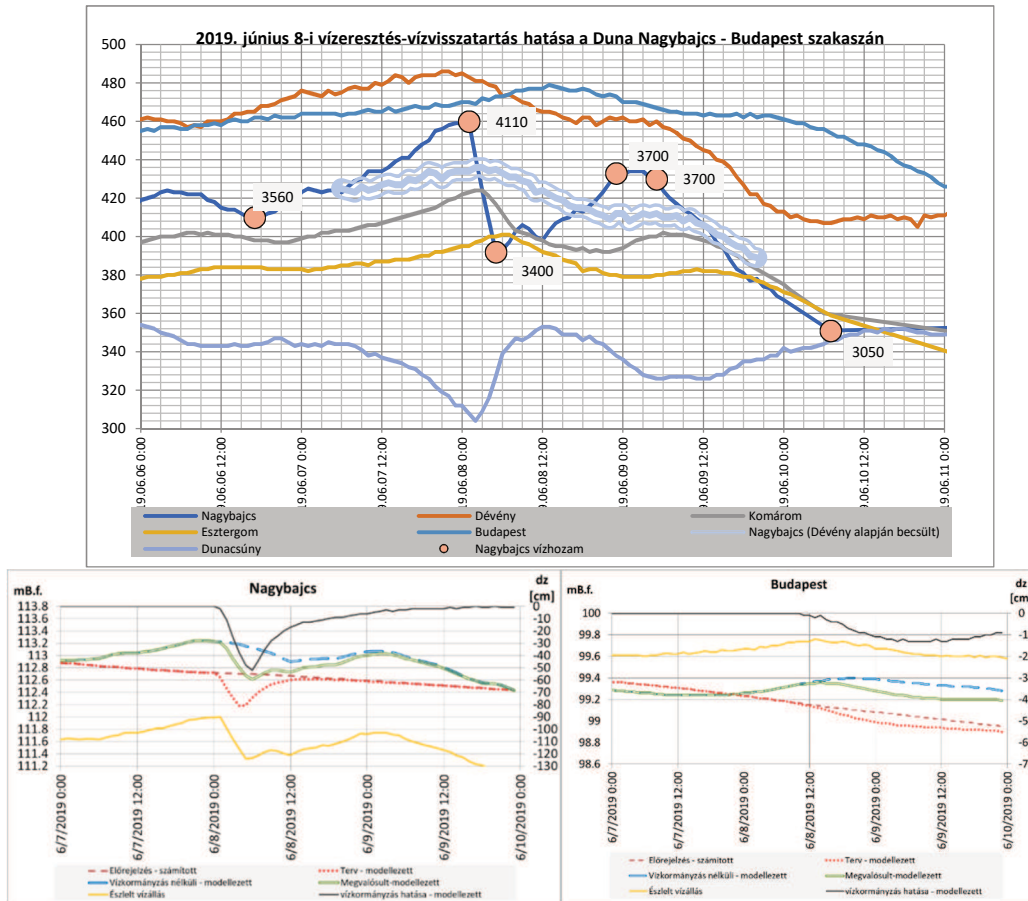
A Dunán a baleset idején levonuló kisebb árhullám a műszaki mentés körülményeit döntően befolyásolta. Vízminőségi kárelhárítás elrendelését is indokoltta, hogy a Hableány üzemanyagtartályában lévő mintegy 7 m³-nyi gázolaj potenciális vízszennyezés forrása volt, aminek vízbe jutása elleni lokalizálást a mentéssel egyidejűleg el kellett végezni.

A roncsok megközelítéséhez, feltárásához és kiemeléséhez az akkori vízállás és vízsebesség sem volt megfelelő. A hajóroncs környezetének 3 dimenziós áramlási viszonyait több cég (pl. Norbit) és a Nemzeti Közszolgálati Egyetem Víz tudományi Kara is vizsgálta. A hajóroncs kiemelését az akkor a Komáromi Duna híd építésében résztvevő Clark Ádám úszódaru segítségével tervezték a mentés irányítói. A daru azonban a magas vízállás miatt nem tudott a budapesti Margit híd alatti hídnyíláson áthaladni. Ezzel összefüggésben az Országos Vízügyi Főigazgatóság és az Észak-dunántúli Vízügyi Igazgatóság feladatot kapott annak vizsgálatára, hogy a Duna felső szakaszán, a szlovák fél közreműködésével van-e reális lehetősége egy rendkívüli vízkormányzásnak, amivel elérhető a hajó áthaladásához szükséges vízszintcsökkentés [11].

A feladat teljesítése érdekében az ÉDUVIZIG a kiemeléshez szükséges vízjárási viszonyok rövid ideig történő kedvezőbbé tételéhez kérelemmel fordult a Szlovák Vízügyi Igazgatóság (SVP) Főmérnökéhez, a Magyar-Szlovák Határvízi Bizottság Duna Albizottság Szlovák Tagozatának Vezetőjéhez. A kérés arra irányult, hogy 2019. június 8-án (szombaton) hajnalban 01:00-tól 4 óra hosszan a Bösi Alvízcsatornán az átadott vízhozamot 1000 m³/s-al csökkentették, ezzel egyidejűleg az Öreg-Dunába átadott hozamot 200 m³/s-al növelték meg [11].

Várható hatások kimutatása, előrejelzése és megvalósult vízkormányzás, tényleges hatásainak vizsgálatát az ÉDUVIZIG hidrológus és HD⁵ modellezésben jártas munkatársai, valamint a Budapesti Műszaki Egyetem szakértője végezték. A vízkormányzás vízjárásra gyakorolt összegzett hatását a 10. ábrán a modellezett és mért hidrológiai adatok idősoraival szemléltetem. Az ábrán látható, hogy a Dévényi szelvény becsült vízhozama alapján a nagybajcsi vízhozam miként változott a dunacsúnyi tározó vízszintjét is figyelembe véve. Megállapítható, hogy a vízkormányzás előtt a tározó szintjét kis mértékben felemelték, majd a vízkormányzásból adódó csökkentés után vissza is töltötték. Emiatt a negatív árhullám két tényleges árhullám között alakult ki, ami idővel egymásra is futott. A Duna magyarországi felső szakaszán elvégzett vízkormányzás hatására a Duna teljes szakaszán – az árhullám-ellapulás törvényszerűségét követve – egyre kisebb amplitudójú „negatív árhullám” alakult ki, amely a modellezett eredmények szerint mintegy 1 – 1,5 dm-es vízszintcsökkenést eredményezett a Duna budapesti szakaszán a természetes vízjáráshoz képest. Az értékelés előzetes becslését a monitoring adatok visszaigazolták; eszerint a Budapesten elérhető vízszint-csökkenés 10 cm körüli volt. A vízszint-csökkenés időben a vízkormányzás megkezdése után már 12 órával érzékelhető volt Budapesten, a maximális értékét 28-36 óra között érte el. Összefüggésben a kért manipulációval is, a Clark Ádám úszódaru végül sikeres manőverrel átjutott a kritikus szakaszon, majd 2019. június 11-én, 13 napos előkészítő munkát követően kiemelte a Hableány roncsait a Dunából [9]. A hajótestben lévő gázolaj lokalizálására a mentés során nem kerülhetett sor, mivel a Duna áramlási viszonyai miatt az anyag teljes egészében eltűnt a hajó üzemanyag-tartályából, és a napokon át működő figyelőszolgálat sem azonosította a Duna teljes magyar alsó szakaszán. Az esemény jól világított rá a hidrológia, a műszaki mentés és a környezetvédelem szoros összefüggéseire, a hidrológiai előrejelzések és elemzések pedig jól támogatták a komplex mentési munkát.

⁵ Hidrodinamikai modellezés – Számítógépi szimuláció a folyórendszerek hidraulikai vizsgálata céljából



10. ábra 2019. június 8-i vízeresztés-vízvisszatartás hatása a Duna Nagybjacs - Budapest szakaszán, modellezett és mért vízszintek [11]

EREDMÉNYEK, KÖVETKEZTETÉSEK

A tanulmány legfontosabb következtetése az, hogy az operatív és statisztikai hidrológiai analízis jelentősége a környezet védelme szempontjából kiemelkedő fontosságú. Ennek jelentőségét különböző – általános és konkrét védekezési események – vízszennyezési esetek és tervezési-engedélyezési eljárások jogszabályi háttérének vonatkozásában vizsgáltam. Fontosságát alátámasztja, hogy folyóink árvízvédelmi létesítményei, és ezzel összefüggésben valamennyi környezetvédelmi beruházás mértékadó tervezési paramétere, a mértékadó árvízszint is hidrológiai statisztikai vizsgálatok alapján kerülnek meghatározásra. A tiszai hulladékszennyezés során elvégzett kárelhárítási művelet fontos tanulsága, hogy a civil kezdeményezések (és bármilyen, több területet érintő szakmai, katonai és civil szervezet együttműködése) rendkívül eredményesek lehetnek nagy volumenű káresemények elleni

védekezésben, valamint azok megelőzésében. Mindkét konkrét esettanulmány fontos következtetése, hogy az operatív hidrológiai monitoring és előrejelzés a komplex kárelhárítási – műszaki mentési műveletek támogatásának jelentős tényezője.

FELHASZNÁLT IRODALOM

- [1] HORNYACSEK Júlia: A lakosságvédelem korszerű értelmezése, helye, szerepe a védelmi rendszerben és a védelmi igazgatással való összefüggései. 132. In: Hornyacsek Júlia (szerk.): A védelmi igazgatás rendszere és a honvédelmi igazgatással való kapcsolatának elméleti és gyakorlati összefüggései. Dialóg Campus, Budapest, (2019) pp. 133-152.
- [2] Közöld Környezeti Portál, Magyarország „pocsolyatérképe”; <http://kozold.hu/cikk/magyarország--pocsolyaterkepe-/192721/egeszseges-no> (letöltve: 2018.12.01)
- [3] KERÉK Gábor: Környezetbiztonsági kockázatok csökkentése – árvízi elöntési területek kiterjedésének valós idejű előrejelzése – a Rába-vízgyűjtő magyarországi szakaszán. Hadmérnök, v. 14, n. 4, p. 113–125, 16 ápr. 2020.
- [4] Tiszai PET Kupa, Rólunk; https://petkupa.hu/hu_HU/rolunk (letöltve: 2020. április 5.)
- [5] Országos Vízügyi Főigazgatóság: „Magyar Hidrológiai Adatbázis (Egységes online hidrológiai adattároló és adatfeldolgozó rendszer)” Budapest, 2015.
- [6] Országos Vízügyi Főigazgatóság: Országos Vízjelző Szolgálat tárolt képparchívuma, elérhető az Országos Vízügyi Főigazgatóságon (Budapest, Márvány u. 1/D) 2020. Budapest
- [7] Sokszínű vidék, Uszályok állják útját a szemétnak a Felső-Tiszán; <https://sokszinuvidek.24.hu/viragzo-videkunk/2020/02/07/tisza-hulladek-folyo-viz-szem-et-pet-palack/> (letöltve: 2020. április 6.)
- [8] Észak-dunántúli Vízügyi Igazgatóság: Nagyvízi mederkezelési tervek, tervezési segédlet, elérhető az Észak-dunántúli Vízügyi Igazgatóságon (Győr, Árpád út 28-32.) 2014. Győr
- [9] 2019-es budapesti hajókatasztrófa: https://hu.wikipedia.org/wiki/2019-es_budapesti_haj%C3%B3katasztr%C3%B3fa (letöltve: 2020. április 10.)
- [10] Észak-dunántúli Vízügyi Igazgatóság: A 2019. május-júniusi árhullámok hidrometeorológiai jelentése, elérhető az Észak-dunántúli Vízügyi Igazgatóságon (Győr, Árpád út 28-32.) 2019. Győr
- [11] Észak-dunántúli Vízügyi Igazgatóság: A „Hableány” hajó katasztrófája kapcsán végzett vízkormányzás kiértékelése, elérhető az Észak-dunántúli Vízügyi Igazgatóságon (Győr, Árpád út 28-32.) 2019. Győr

**BASICS OF DEVELOPING OF THE LEGAL
REGULATION IN SELF-DRIVING CARS****AZ ÖNJÁRÓ JÁRMŰVEK JOGSZABÁLY-
ZATA FEJLESZTÉSÉNEK ALAPJA**NINKOV, Ivona ¹**Abstract**

Recently, a significant number of cars are partly self-driving, i.e. some operation are commended by human and partly automatically. However, in the future it is expected that the self-driving cars will be navigated entirely self-sufficiently without human intervention. It requires high technology progress. In addition, the corresponding law regulation for the self-driving cars has to be developed. In this paper the connection between the increase of self-driving properties and the necessary law regulation is presented. Due to large number of sensors and effective computers, newer vehicles may, pick up and record data on how, when, and where individuals drive. These information could raise privacy concerns if the information is stolen or improperly handled. Some of data may directly interrupt the safety and security conditions in the environment. The Data security regulation has to be improved. As the possibility of accident rates decrease, the Insurance law has to be changed. In addition, if there is an accident with a car with self-driving elements the new regulation is necessary which will give the answer about guilty: if it is the creator or purveyor of a self-driving car's algorithm or the human operators.

Keywords

self-driving car, insurance law, data security regulation, traffic accidents

Absztrakt

Az utóbbi időben jelentős számú autó részben önállóan működik, azaz egyes működések ember és részben automatikusan végez. A jövőben azonban várható, hogy az önjáró autók emberi beavatkozás nélkül teljesen önállóan navigálnak. Ez magas technológiai haladást igényel. Ugyanakkor be kell vezetni az önjáró személygépkocsikra vonatkozó törvényi szabályozást is. Ebben a cikkben megvizsgálom az önjáró tulajdonságok növekedése és a szükséges törvényi szabályozás összefüggését. Az újabb járművek a nagyszámú érzékelő és hatékony számítógép miatt felvehetnek és rögzíthetnek több olyan adatot, amely rámutat a vezetési módra és mikor és hol történik. Ezek az információk adatvédelmi aggodalmakat vethetnek fel. Ezért javítani kell az adatbiztonsági szabályozást. Mivel a balesetek aránya csökken, a biztosítási törvényt meg kell változtatni. Ezen túlmenően, ha baleset merül fel egy önjáró és egy konvencionális autóval, akkor szükségessé válik az új szabályozás, amely választ ad a bűnösre: az önálló vezetésű autó algoritmusának alkotója vagy szállítója, vagy a jármű emberi kezelője, vagy mindkettő.

Kulcsszavak

Kína, társadalmi kredit rendszere, információbiztonság

¹ ivonakakas@yahoo.com | ORCID: 0000-0002-0116-2453 | PhD student / doktorandusz | Obuda University Doctoral School of Safety and Security Sciences / Óbudai Egyetem Biztonságtudományi Doktori Iskola

INTRODUCTION

During the third industrial revolution the computerization is brought into automobile industry making the driving function independent on human driver. The automated cars are designed where some of the functions and operation in driving process need not to be controlled by driver, but by corresponding software. Nowadays, in the era of the 4th Industrial revolution the tendency is to eliminate humans from the position of driver sitting with the steering wheel and to produce autonomous cars to fulfil the driving task without human action. It requires significant improvement in technology and in addition in computer power and sensors (which could include cameras, radar, and ultrasonic detections) which will be strictly connected with the driving function. Such autonomous vehicles are expected to change the whole transportation system. The prediction is that autonomous vehicles (AV) will become the reality in a short time on public roads. Analyst predict that completely autonomous cars will be for sale by 2025-2030 [1].

The aim of this paper is to point out that this new type of transport requires not only technical innovation but also a new legal regulation that will accompany the product implementation and vehicle operation. The legal instructions have to help such vehicles to come to life. These regulations has to be applicable for both, manufacturers and users of vehicles. The legal documents have to make changes in already known infrastructure regulations. In addition, the legal regulation of liability in the case of accident between AV and convention vehicle or two AV has also to be developed. In general, the traffic regulation has also to be modified. In some sense the urban plan needs some changes, as the number of parking places can be reduced. Namely, the number of individual vehicles will reduce and parking in front of the homes or in front of the workplace will be not necessary.

Based on the advantages and disadvantages of AV in all sphere (technical, ethics, social) in the paper the areas of legal regulation modification are suggested. The responsibility, liability, safety and security aspects for AV has to be defined in the future legal regulations.

SELF-DRIVING CAR: DEFINITION AND PROPERTIES

The term ‘self-driving car’ is widely used in a very wide concepts and the definition in technical sense is necessary to be mentioned. The ‘self-driving car’ is an autonomous vehicle (AV) which drives itself in most or all conditions [2]. In technical concept ‘autonomous’ means more or less that the system works independently of human inputs while fulfil certain tasks. Thus, ‘autonomous vehicle’ is driving without human commands [3]. However the most precise definition of AVs is given by the International Society of Automotive Engineers (SAE) in 2014 where the extent of automation is said to depend on the human driver’s role in performing the dynamic driving task [4]. So, AVs have different levels of autonomy. SAE made a classification on the level of autonomy of vehicle which is widely used by manufacturers and regulators.

SAE introduced 6 levels of automation: 0 is the lowest level – without automation and 5 is the highest level – with full automation [5]. The factors which define the level are:

- A. The agent responsible for executing steering and throttle control: human driver or autonomous technology (AT)

- B. The agent responsible for monitoring the external environment: human driver or AT
- C. The agent responsible for serving as ‘back up’ when a failure prompts a disengagement of the AT: human driver or AT
- D. Autonomous operations are allowed: without restriction – all modes of operation, or only for special conditions – some mode of operations (e.g. good visibility).

SAE level	Name	Narrative Definition	Execution of Steering and Acceleration/Deceleration	Monitoring of Driving Environment	Fallback Performance of Dynamic Driving Task	System Capability (Driving Modes)
Human driver monitors the driving environment						
0	No Automation	the full-time performance by the <i>human driver</i> of all aspects of the <i>dynamic driving task</i> , even when enhanced by warning or intervention systems	Human driver	Human driver	Human driver	n/a
1	Driver Assistance	the <i>driving mode</i> -specific execution by a driver assistance system of either steering or acceleration/deceleration using information about the driving environment and with the expectation that the <i>human driver</i> perform all remaining aspects of the <i>dynamic driving task</i>	Human driver and system	Human driver	Human driver	Some driving modes
2	Partial Automation	the <i>driving mode</i> -specific execution by one or more driver assistance systems of both steering and acceleration/deceleration using information about the driving environment and with the expectation that the <i>human driver</i> perform all remaining aspects of the <i>dynamic driving task</i>	System	Human driver	Human driver	Some driving modes
Automated driving system (“system”) monitors the driving environment						
3	Conditional Automation	the <i>driving mode</i> -specific performance by an <i>automated driving system</i> of all aspects of the <i>dynamic driving task</i> with the expectation that the <i>human driver</i> will respond appropriately to a <i>request to intervene</i>	System	System	Human driver	Some driving modes
4	High Automation	the <i>driving mode</i> -specific performance by an <i>automated driving system</i> of all aspects of the <i>dynamic driving task</i> , even if a <i>human driver</i> does not respond appropriately to a <i>request to intervene</i>	System	System	System	Some driving modes
5	Full Automation	the full-time performance by an <i>automated driving system</i> of all aspects of the <i>dynamic driving task</i> under all roadway and environmental conditions that can be managed by a <i>human driver</i>	System	System	System	All driving modes

In Fig.1 the classification made by SAE is shown.

(AV levels of automation. Reproduced AS-IS with permission from SAE-International J3016TM, [4]).

Vehicles at levels 1, 2 and 3 are named ‘semi-autonomous’ or ‘automated’. Nowadays, mostly the semi-autonomous vehicles are developed [6]. In automated car the human driver makes the driving tasks on the roads, but the vehicle has systems that automate certain functions such as parking, adaptive cruises control, lane drift detection, automatic breaking i.e. emergency brake application which is without human driver control. Thus, the parking assist systems allows cars to steer themselves into parking spaces and the adaptive cruise control maintains a certain distance from the vehicle in front of the car. In semi-autonomous vehicle the driver is allowed to cooperate with the software which is the ‘brain’ of the vehicle, specially, if there is a failure. However in the level 3 of automation a problem appears which is not solved yet: there is not found a way how to redirect the control of the car to the human driver just in a fraction of a second as it is necessary in emergency. Some

manufacturers solved the problem by giving the limitation to the Level 3 only for lower speeds and small power vehicles.

Some companies already produced the so called ‘fully-autonomous’ cars of the level 4 and 5. Vehicles can drive themselves on existing roads and can navigate many type of road ways and environmental contexts with almost no direct human input. Recently, for these AVs it is prohibited to be sold on the market and to be freely included into the public traffic. The vehicles of level 4 and 5 can be only tested on public roads but it is required a human driver, who has undergo a specific training prescribed by the authorities, to be included into the driving process. The test drivers have to be always ready to take control of the prototypes of self-driving cars. In the second half of 2015, Tesla Motors began allowing owners (not just test drivers) to switch on its Autopilot mode [7-9]. In these cars the human being (professional driver or Tesla owner) has to sit in the driver’s seat and to keep hands near the wheel and eyes on the road. Special beeps and other warnings are installed into the vehicle to make sure they fulfil this requirement. That makes the vehicles street legal for now in California and Nevada in U.S.A. European regulators have allowed limited tests of self-driving cars and even tractor-trailers. The United Kingdom has begun reviewing road regulations to figure out how to eventually allow a fully autonomous shuttle. Japan allowed its first road test of an autonomous car in 2013, although much of the research being done by Japanese car companies is happening in the United States.

Thousands of kilometers of testing drive are necessary to be done in the future which will give the real features of the vehicle. Unfortunately the legal regulation for testing AV is very poor. California is one of rear countries to regulate the testing of AV on public roads by introducing the CA DMV rules in 2016. In other countries and states regulation for testing AV is necessary.

Remark: Due to the terminology of the National Highway Transportation Safety Administration (NHTSA) the autonomous and automated cars are in common called ‘highly automated vehicles HAVs.

BENEFITS AND PITFALLS OF SELF-DRIVING CARS

The purpose of introduction of self-driving cars, as a new cyber-physical product, will be to impact following requirements:

- Averting deadly crashes
- Decreasing the number of accidents
- Provide mobility for elderly and disabled
- Increase road capacity
- Save fuel
- Lowering emission in environment during transport.
- Reduce the necessity of parking areas

The AV will increase the person mobility and specially it would be very convenient for elderly and also disabled who are not able to drive the car. The AV may be a personal vehicle, or an on-demand one. If it is the last, shared rides may be realized. Then, some complementary benefits are evident. For example, the efficiency on roads is increased. The

explanation is, that the number of cars on the road is decreased and the fuel application would decrease and as the result emission of pollutions in the environment would decrease, too [10]. So, the human impact on environment is minimized. Due to decreased traffic, the road capacity would increase.

The improvement obtained with AV is the possibility to increase the work productivity and better time use of potential drivers, as the previous drivers may use the driving time for their work special if it is in the field of IT technology [11].

However, the greatest benefit in applying AVs is the reduction of traffic fatalities and the elimination of death-accidents. Level of safety in the traffic would be increased. Namely, it is proposed that the number of accidents would tremendously decrease and specially the death-ones. It is expected that 50 years from now, in the world there will be no traffic accidents. People will look back and conclude that human drivers were a design defect.

AVs have some disadvantages. The cost of the AV is very high. The question is what will be the cost of the on-demand service. In addition, the vehicle is proposed to be unsafe due to the fact that there is a risk to be hacked. In spite of continual monitoring the cyber-security may be interrupted. The privacy would be highly disturbed as self-driving cars are ultimate connected with each other, but also with a central station. The exact location and route of all passengers is known. In addition, self-driving cars continuously monitor other drivers on the road and obtained information could be applied in negative sense. Whether the gigabytes of generated information can be permanently stored—and how they can be used later—is not settled yet.

Using the benefits and pitfalls of semi-driving vehicles it is important to determine the challenges we will face in the near future and how to avoid them. The legal regulation system has to be improved and extended but also new documents have to be introduced in legal systems. Thus, at the moment there are no legal regulations which will give the answers for the case of accident: Who is guilty for the case when the accident is between two AVs or an AV and a conventional car? Is it the manufacturer of the AV or the vehicle owner liable for accident? To which limit is the liability of the producer or the person who makes the software. If the accident is due to sudden fail on cyber or in physical part, who is liable? Is it possible to introduce some legal regulation for cyber security and protecting AV from unsafety? Legal regulation of the road traffic with AVs is also necessary to be introduced.

The space for public transit has to be reconsidered. Self-driving cars will have a profound effect on city design. Parking spaces in the city center will take up and reconstructed into pedestrian zones, parks, shopping centers, etc. Self-driving cars will park themselves in peripheral areas of the city and pick up the passengers in the way as the taxis do it nowadays.

LEGAL ASPECTS OF SELF-DRIVING CARS

Every new step in progress of artificial intelligence in vehicle poses potential legal questions and requirements [12,13]. Some legal regulation already exist, but is important to be applied in a proper manner. Thus, for example, the regulation for intellectual property exists, but engineers developing new products in the sphere of AV will need to be advised on avoid it. However, legislation for protection autonomy and intellectual property has to

be extended with the aspects for patents and innovations in cyber-physical systems. The application the patent infringement and to regulation of intellectual property [5,14] is mandatory.

In some sphere of legal regulation there are some lacks. It is the case for:

- Liability and Product Liability
- Security including cyber security
- Data protection
- Safety issues

An enormous number of data are recorded by AV: how, when, and where individuals drive. Control of the position of the person travelling by AV is known at every moment. The privacy of the person is hardly damaged due to travelling by AV. The collected information obtained from self-driving cars may include proprietary codes, too. Because of that, data security protection is necessary. Security and cyber security of the AV has to be included into legal consideration. The rules have to be connected with data protection. New regulation is necessary to protect these data. However, the security of the persons has to be increased in spite of the fact that some private data are widely evident. The cyber security system has to eliminate the possibility of privacy interruption if the information are stolen or improperly handled.

Civil liability shifts has to be introduced and liability of manufacturers, owners and users of AV has to be defined. It is not clear which are the liability limits for all of these subjects in the matter. Besides, the object of liability has to be strictly defined. To determine the liability in this matter is a very complex and heavy task. Let us suggest two examples:

1. If there is an accident litigation the main problem is to define the liability: if in motor vehicle accident who was struck by a car with self-driving elements, is it possible to argue that the creator or purveyor of a self-driving car's algorithm shares some liability with human operators for a vehicle's actions. The criminal law has also to be changed. Namely, the person in AV who is sleeping is not guilty for happening in transportation. In conventional car the driver falling asleep at the wheel is guilty.
2. Second key question which is given in lawsuit concerning the product liability: whether the product had a "defective condition" that was "unreasonably dangerous." This often involves determining whether the product designer could have made the product safer at an acceptable cost. But what's "reasonable" for a new technology? Is "reasonably safe" defined by the average human driver, the perfect human driver, or the perfect computer driver?

Safety issues are mainly addressed on the manufacturer of AV and road traffic. It is necessary to prescribe the level of safety of the AV control system. This rules would be quite new, but has to be included into the legal system for protection in traffic. Some countries in Europe and in U.S. already included some law for road traffic with AV enable the AV to drive on public roads. However, all of these rules are quite strict and not enough for traffic regulation.

Some additional legal recommendation have to be developed. Thus, a very interesting question is given: if the employee has the work to check email or performs other tasks by driving AV, could he raise the wage and hours of work and ask for compensation issue from employer?

Problem with insurance law is very actual. Due to decrease of accidents number with AV, it is supposed that there will be crash savings. It suggests the Insurance regulation to change. Namely, may be the traditional car insurance can be moved away from the user as the accident number is thought to be decreased.

The final aim is to create a recognized licensing and testing framework and standards for AV, liability standards, security standards, privacy/default lack of privacy standards and norms for personal travel and regulation for impacts and interactions with other components of the transportation system. Thus, the progress of technology in AV requires the development of regulations. Somehow, it is obvious that the self-driving cars will be ready much earlier than the laws [15].

CONCLUSION

In this paper the basics of developing of the legal regulation in self-driving cars are presented. First, the term ‘self-driving car’ is determined and the level of automation in vehicle is considered. Advantages and disadvantages of autonomous vehicle in comparison to conventional car are discussed. Based on the research, the legal regulation of the AV is suggested. It is suggested to be done in two directions: firstly, to develop the laws considering the road conditions and secondly, in extending the security and safety regulation, liability conditions, privacy and data protection. Also, the introduction of AV in traffic and on the public roads requires some changes in insurance and public law.

REFERENCES

1. Driverless Volvo 560 – car review (2014), <http://www.theguardian.com/technology/2014/jun/07/driverless-volvo-s60-car-review>
2. Autonomous car definition, <https://www.techopedia.com/definition/30056/>, accessed 28 February 2020
3. HILGENDIRF E. (2015) Autonomous cars and the law, http://cgd.swissre.com/global_dialogue/topics/Autonomous_cars/Autonomous_cars_and_the_law.html, 2015
- 4.SAE International (2014) Taxonomy and definitions for terms related to on-road motor vehicle automated driving systems, Standard J3016, USA
5. JONES J.J., KARTNER R.W., LITTLE J., MOELLENBERG C.H., PAEZ M.F., RAFFERTY P.F., WEBER-BRULS D.M. (2019) Legal issues related to the development of automated, autonomous and connected cars, Jones Day, White paper 1-24
6. FAVARO F., EURICH S., NADER N. (2018) Autonomous vehicles’ disengagements: Trends, triggers, and regulatory limitations, Accident Analysis and Prevention 110, 136-148
7. <https://www.tesla.com/autopilot>, 2016

8. INGLE S., PHUTE M. (2016) Tesla autopilot : semiautonomous driving, an uptick for future autonoming, International Research Journal of Engineering and Technology, IRJET, 3(9), pages 8.
9. DIKMEN M., BURNS C.M. (2017) Trust in autonomous vehicles: the case of Tesla autopilot and summon, 2017 International Conference on Systems, Man, and Cybernetics (SMC 2017), Bariff, Canada, doi.:10.1109/SMC2017.8122757
10. Federal Automated vehicles policy (2016) Accelerating the next revolution in roadway safety, U.S. Department of Transportation – National Highway Traffic safety administration, USA
11. FAGNANT D.J, KOCKELMAN K. (2015) Preparing a nation for autonomous vehicles: opportunities, barriers and policy recommendations, Transportation Research Part A 77, 167-181
12. ILKOVA V., ILKA A. (2017) Legal aspects of autonomous vehicles – an overview, Conference paper, June 2017, 6 pages
13. SIMKIN J.S. (2019) Top 8 Legal implications of self-driving vehicle technology: Every new shade of increased artificial intelligence participation in vehicle operation poses potential legal questions.
14. RYAN M. (2019) The future of transportation: ethical, legal, social and economic impacts of self-driving vehicles in the year 2025, Science and Engineering Ethics, <https://doi.org/10.1007/s11948-019-00130-2>, Published online:03 September 2019
15. GREENBLATT A.N. (2018) Self-driving cars will be ready before our laws are: Putting autonomous vehicles on the road isn't just a matter of fine-tuning the technology, in *"Self-Driving Cars and the Law"*.

**CHINA AND INFORMATION SECURITY
ISSUES IN THE SOCIAL CREDIT SYSTEM****KÍNA ÉS A TÁRSADALMI KREDIT
RENDSZERÉNEK
INFORMÁCIÓBIZTONSÁGI KÉRDÉSEI**KOLLÁR Csaba¹**Abstract**

In China, the social credit system officially announced in 2014 is likely to be introduced this year after six years of development and testing. The antecedents of the social credit system – that is, the evaluation, rating, scoring of citizens – can be found in almost all countries, as I point out in the theoretical part of my study. This paper is the final study of my research started in September 2019 with the support of the New National Excellence Program, in which I summarize the results of my data mining, document analysis, online questionnaire survey and expert focus group discussion with five experts. I organize my concluding remarks around the probability of the introduction of the system, its impact on national security, the barriers to introduction, responsibilities of the introductory country, and the ideas of the system as an export product.

Keywords

China, social credit system, information security

Absztrakt

Kínában a hivatalosan 2014-ben bejelentett társadalmi kredit rendszerét nagy valószínűség szerint a hatévnyi fejlesztés és tesztelés után ebben az évben vezetik be. A társadalmi kredit rendszerének előzményei – vagyis az állampolgárok értékelése, minősítése, pontozása – szinte valamennyi országban megtalálhatók, ahogy erre tanulmányom elméleti részében is rámutatok. Jelen írásom az ÚNKP támogatásával 2019. szeptemberében elkezdett kutatásom zárótanulmánya, amiben a rendszer működésének bemutatása mellett összefoglalom az adatbányászat, a dokumentumelemzés, az online nagymintás kérdőíves felmérés, valamint öt szakértővel folytatott szakértői fókuszcsoportos beszélgetésem eredményeit. Ez utóbbinál megállapításaimat a rendszer bevezetésének valószínűsége, a nemzetbiztonságra gyakorolt hatása, a bevezetés gátló tényezői, a bevezető ország feladatai, valamint a rendszer, mint exportcikk gondolatok köré rendezem.

Kulcsszavak

Kína, társadalmi kredit rendszere, információbiztonság

¹ kollar.csaba@phd.uni-obuda.hu | ORCID: 0000-0002-0981-2385 | PhD student / doktorandusz | Obuda University Doctoral School of Safety and Security Sciences / Óbudai Egyetem Biztonságtudományi Doktori Iskola

BEVEZETÉS

Az elmúlt évtizedekben, s különösen az elmúlt szűk évtizedben Kína potenciálja szinte valamennyi területen megerősödött. (Makro)gazdasági mutatói – ahogy arra még később részletesen utalni fogok – egyre jobbak, termelési kapacitása közel kiaknázhatatlan, termékei minősége, vagy legalábbis a Kínában gyártott termékek többségének a minősége jó/kiváló. Az online piactereken (is) jelenlevő kínai (kis)kereskedők megbízhatóak, egyre nagyobb részük nem csak kiváló angolsággal, hanem fejlett üzleti intelligenciával, a legmagasabb elvárásoknak is megfelelő módon kezeli az értékesítési folyamatokat, illetve az esetleges reklamációkat. Kínára már hiba lenne csak bérgyártóként tekinteni, mivel egyre több világmárka indul újtárra az országból, s a digitális kort, majd az adatok korát leváltó mesterséges intelligencia korának meghatározó és befolyásoló kilenc nagy vállalatából három Kínában található. Kína és a mesterséges intelligencia párhuzamos és számos ponton egymással összefüggő fejlődése megfelelő alapot jelentett ahhoz, hogy a 2014-ben bejelentett társadalmi kredit rendszere 2020-ra országosan realizálódhasson. Bizonytalanságot csak a koronavírus megjelenése jelent az indulás dátumát illetően (egyres források reálisabbnak látják a 2021-es indulást), de magának az indulásnak a tényét a vírus nem befolyásolja. Tanulmányom kutatási részénél utalok majd az elemzett dokumentumok kapcsán a kínai ellenzékre, illetve a társadalmi kredit rendszerének bírálatára, ami azért érdekes, mert előzményei, illetve egyes elemei szinte valamennyi országban, akár több ezer évvel ezelőtt is megjelentek.

A TÁRSADALMI KREDIT RENDSZERE ÉS ELŐZMÉNYEI

Valamennyi társadalmi szerveződésre igaz, hogy annak tagjai valamilyen szempont szerint értékelésre, majd kiválasztásra kerülnek, illetve, hogy a szűkösön rendelkezésre álló javak igazságos(nak mondott) szétosztásánál nem mindenki lehet részese e javaknak. A társadalom, vagy egy kisebb csoport demokratikusan megválasztott elöljárójánál is érvek és ellenérvek ütköznek a többi jelölttel szemben, s a választó(polgáro)knak értékelniük kell a jelölteket, hogy ennek alapján ki lehessen hirdetni a győztest. A kisiparosokat évszázadok óta minősítik a különböző céhek/kamarák. A mesterlevél nem csak az önálló tevékenység megkezdésének lehetőségét jelentette, de bizalmat és megbízhatóságot is kommunikált a mester, illetve termékei, portékái iránt. Kutatásomban az elmúlt évtizedek értékelő/minősítő rendszerei és megoldásai közül először kilencet neveztem meg, majd a marketinget és az online kereskedelmet, valamint a társadalombiztosítást és az adózást külön kategóriaként kezeltem (ezekkel kapcsolatban saját online kérdőíves kutatásomban is tettem fel kérdéseket). A tizenegy értékelő/minősítő rendszer a következő:

- (1) Magyarországon a közúti közlekedési előéleti pontrendszer (2000. évi CXXVIII. törvény) határozza meg, hogy hány büntetőpont adható az adott közúti szabályszegés esetén. Járművezetői eltiltás, végleges eltiltás, utánpéztés, járművezetői vizsga lehet a büntetőpontok következménye.
- (2) A játékosítás (gamification) lényege, hogy a problémák megoldásában (vagy akár a tanulásban) részt vevő személy haladásának és így fejlődésének függvényében, vagy a probléma megoldásának folyamatában elért teljesítményéért valamilyen jutalmat kap. A jutalom – pl.: jutalompont, magasabb szintre lépés, státuszjutalom, bónusz – fenntartja az érdeklődést, az aktivitást.

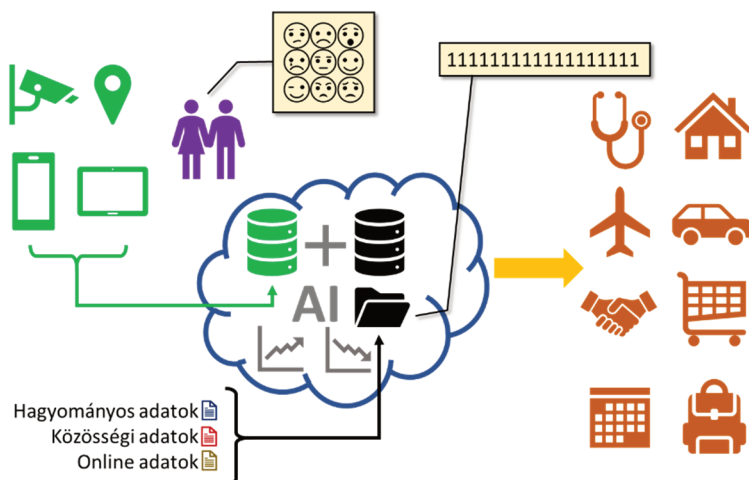
- (3) Az egészségügyi és közigazgatási informatikai rendszerek bevezetése és fejlődése révén valós időben lehet ellenőrizni a társadalombiztosítási (TAJ), vagy más azonosító szám segítségével (országtól és a rendszer fejlettségétől függően), hogy az egyén jogosult-e, s ha igen, milyen egészségügyi ellátásra, illetve, hogy a múltban milyen ellátásokat vett igénybe, milyen gyógyszereket, gyógykezeléseket írtak fel a számára.
- (4) Az adószám révén az adószámmal rendelkező egyén, illetve társas vállalkozás adófizetési hajlandósága ellenőrizhető a nyomozóhatóság, vagy az adóhivatal munkatársai számára. A személy beazonosítása után lehetősége van a hatóságoknak a társas vállalkozások kapcsolati hálójának a feltérképezésére is, ami elősegítheti a szervezett (gazdasági) bűnözés elleni hatékonyabb fellépést.
- (5) A pénzügyi/banki területen a bankszámla nyitását követően a bank pontosan nyomon tudja követni a pénzügyi tranzakciókat, ha pedig az ügyfél (rendszeresen) használ bankkártyát, akkor közel teljes kép alakulhat ki róla pénz-, illetve bankkártya-használati, valamint vásárlásai vonatkozásában, ami alapján elég megbízhatóan lehet besorolni különböző klaszterekbe. A klaszterizáció nem csak az ügyfél számára szóló egyéni ajánlatok összeállításánál lehet a bank segítségére, de a hitelfelvételnél is része lehet a hitelképesség-bírálatnak. A hitelképesség-bírálat során az ügyfél rendszerint (szükségszerűen) megannyi dokumentumot csatol a kérelméhez, ezek, s a már említett klaszterbe tartozás a banki ügyintéző esetleg szubjektív véleménye mellett viszonylag objektív, reális képet ad az ügyfélről.
- (6) A fogyasztóról/vásárlóról már a klasszikusnak számító marketingben is megpróbálták minél több információt gyűjteni. A marketingen belül a direkt- és adatbázis marketing alapját rendszerint olyan adatbázisok jelentették, amelyek a fogyasztók/vásárlók statikus adatai (pl.: név, cím, e-mail cím, telefon) mellett a szokásairól (pl.: mit, mikor, mivel együtt, mekkora értékben rendelt, milyen gyakran rendel) is szolgáltatott információt a szakemberek számára. A törzskártyák, nyereményakciók, pontgyűjtőkártyák, kuponok révén nem csak a vásárlás/fogyasztás aktivizálható, hanem a különböző adatbázisok összekapcsolása által a fogyasztóról még átfogóbb ismeretek állhatnak a szakemberek rendelkezésére. A GDPR ugyan Európában szabályozza a személyes adatok gyűjtését és kezelését, de általánosságban azt lehet mondani, hogy az egyén hozzájárulása révén a direkt- és adatbázis marketing eszközei továbbra is használatosak.
- (7) Az online kereskedelem – amelyik az utóbbi időben világviszonylatban egyre nagyobb arányt képvisel a hagyományos kereskedelemhez képest – piacterein árult termékek és szolgáltatások jelentős részénél a vásárlás regisztrációhoz kötött, ami révén a direkt- és adatbázis marketinghez hasonlóan nem csak statikus adatok, hanem a vásárlással, vásárlási szokásokkal, a weblap használatával, a vásárlói viselkedéssel (pl.: betette a terméket a virtuális kosarába, de már több napja nem veszi meg) kapcsolatban is megannyi adat áll rendelkezésre. Ezek a személyre szabott ajánlatok mellett a dinamikus klaszterizációt is lehetővé teszik.
- (8) Az online kereskedelemhez hasonlóan a közösségi média használata is regisztrációhoz, bejelentkezéshez kötött. Fontos, hogy a médiafelületeket a felhasználók gyakran, szinte állandóan használják, ezért ezeket a felületeket úgy alakítják ki, hogy lehetővé tegyék és aktivitásra buzdítsák a látogatókat. Ilyen lehetőség többek között a lájkolás, a posztolás, a vélemény írása, más véleményének megosztása, hozzászólás más poszt-

jához, saját médiatartalmak gyártása és mások médiatartalmának megosztása, barátkozás, kapcsolati háló kialakítása és építése, csatlakozás hasonló érdeklődésű emberek csoportjához. A közösségi oldalak többségénél és egyre több online kereskedelmi oldalon a tartalmakat értékelni is lehet, ami révén az adott tartalom és/vagy tartalomtulajdonos és/vagy termék/szolgáltatás iránti bizalom erősíthető/gyengíthető. Az online márkák és piacterek építésénél ennek nagy jelentősége van.

- (9) A mobiltelefonok fejlődésének és a széles sávú mobilhálózat elérhetőségének köszönhetően, valamint a telefonokban levő szenzorok és alkalmazások révén – különösen – az okostelefonok megannyi kényelmi, szórakoztató, hasznos funkciót kínálnak a tulajdonosnak, így a lakosság egyre nagyobb hányadának lettek a szinte állandóan használt és magánál tartott eszközei. A mobiltelefon aktuális földrajzi helyzete viszonylag exakt módon határozható meg, tulajdonosának mobiltelefonálási és okostelefon-használati szokásai (pl.: melyik alkalmazást mikor, s mennyi ideig használja, honnan és milyen tartalmakat oszt meg, kikkel van egy helyen) pedig lehetővé teszik egy közel teljesnek mondható fogyasztói/felhasználói profil elkészítését is.
- (10) Az emberi erőforrás gazdálkodás folyamatában és tevékenységében több területen is régóta használják a különböző értékelő/minősítő eljárásokat, módszereket, technikákat, mint pl.: az álláshirdetésre küldött pályázók önéletrajzáinak és egyéb dokumentumainak vizsgálata, értékelése, rangsorolása, a felvett munkavállalók teljesítményének objektív és szubjektív értékelése, az adott munkavállaló értékeltetése a vezetőjével, közvetlen kollégáival, a különböző belső képzéseket tartó oktatók értékeltetése a résztvevők segítségével, a vállalatnál kilépő munkavállalónak a kérdőíves véleménye a vállalatról, a munkakörnyezetről, a foglalkoztatásról.
- (11) A pedagógia munka elengedhetetlen része, hogy az oktatásban részt vevőket a tanár – lehetőleg – objektív módon értékelje. Az értékelés legegyszerűbb módja az osztályzat, de egyre gyakrabban igénylik a diákok az osztályzat mellett a szöveges tanári visszajelzést is. Az osztályzatok idősoros elemzése jó visszajelzés lehet a tanárnak, a diáknak és a szülőnek is a tanuló fejlődéséről. A tandíjfizetős, illetve magán oktatási intézményeknél, valamint a hazai és nemzetközi rangsorok szerint minősített elit közép- és felsőfokú tanintézményeknél – különösen azoknál, ahol a férőhelyek száma erősen korlátos – a jelentkezőket szelektálni, rangsorolni kell. Szelekció lehet a szülők bőven átlag feletti anyagi helyzete (ki tudják fizetni gyermeküknek a magas tandíjat), rangsor a korábbi iskolai- és/vagy sportteljesítmény alapján. A felsőoktatási intézmények egy része is többletpontokkal díjazza a nyelvvizsga meglétét, több nyelvvizsga meglétét, igazolt sportolói/versenyzői múltat, a középiskolai tanulmányi versenyeken történő részvételt/helyezést, államilag elismert szakma meglétét. Azok a felvételizők, akik nem érik el a felvételhez szükséges minimumpontszámot nem kezdenek el az adott intézményben felsőfokú tanulmányaikat.

Az általam beazonosított és vizsgált értékelő rendszerek, mint építőelemek részei lehetnek, s ahogy alább látható is, többségük része is – természetesen a kínai gazdasági, politikai, társadalmi környezetre adaptáltan – a társadalmi kredit rendszerének. A kínai társadalmi kredit rendszeréről több tanulmányt is írtam [1], [2], [3], így az alábbiakban csak a rendszer alapvető leírását és jellemzőit adom meg, mielőtt saját kutatásomat és annak eredményeit ismertetem.

A kínai társadalmi kredit rendszerének alapvető elgondolása az, hogy a kínai lakosságot a lakosságról már rendelkezésre álló adatok és információk, valamint a róluk (folyamatosan) gyűjtött adatok és információk alapján pontozza, értékeli, s a viselkedésük alapján besorolja (klaszterizálja). A rendszer a lakosság mellett a vállalatokat és az intézményeket is értékeli. A rendszer olyan etikai-morális értékeket kíván társadalmi, gazdasági és politikai szinten elfogadottá tenni, mint őszinteség a kormányzati ügyekben, üzleti becsületesség, társadalmi becsületesség, igazságügyi hitelesség. Ezeknek az értékeknek az elfogadása, illetve az ezek szerinti viselkedés az üzleti és magánéletben plusz pontokat jelent az egyéneknek, s így előnyökhöz juttatja őt, illetve gyermekét, a szabályszegők pedig büntetésben részesülnek. A társadalmi kredit rendszeréhez technikai értelemben több technológia, illetve megoldás/alkalmazás kapcsolódik, úgymint: mobilkommunikációs eszközök, (közterületen elhelyezett) biztonsági kamerák, közösségi média, kiterjesztett és kevert valóságok, GIS és GPS rendszerek, vezeték és vezeték nélküli kommunikációs hálózatok, robotizáció és automatizálás, felhő alapú számítástechnika, IoT és szenzorhálózatok, big data analitika, valamint a rendszer hatékony működését lehetővé tevő mesterséges intelligencia. A rendszer működésének vázlatát az 1. ábrán látható.



1. Ábra: A társadalmi kredit rendszerének rendszerábrája (saját szerkesztés)

Az ábra alapján a társadalmi kredit rendszerének a működése a következő. Az egyének és a vállalkozások egy, a beazonosításukra alkalmas egyedi azonosítószámot kapnak, s ez az az azonosítószám, aminek a segítségével össze tudják kapcsolni az egyénekről és a vállalkozásokról rendelkezésre álló, s (folyamatosan) gyűjtött adatokat, melyek a felhőben tárolódnak. Alapvetően háromféle adatcsoport különböztethető meg: (1) hagyományos adatok, mint pl.: rezsizsámlák és ezek fizetési hajlandósága, bírósági perköltségek megfizetése, büntetések és ezek megfizetési hajlandósága, hitelkártya számlák, kölcsön visszafizetése, jövedelemadó mértéke, illetve hajlandóság a befizetésére, (2) a közösségi (társas együttéléssel kapcsolatos) adatok, mint pl.: bűnözési aktivitás, szülői szerep tudatos megélése (jó szülő eszményképe), önkéntesen vállalt feladatok a közösség érdekében, becsületesség és szavahihetőség, fizetés a tömegközlekedés használatáért (jegy-, illetve bérletvásárlás, uta-

zási kártya feltöltése), a családtervezési korlátozások betartása, a közlekedési szabályok betartása, (3) online (közösségi médiában) felületekről származó adatok, mint pl.: vásárlási szokások online piacereken, az online felületeken megosztott hírek szavahihetősége (hamis/valós hírek gyártása), kapcsolat a többi felhasználóval. A felhőben levő adatokat – melyekhez hozzákapcsolódnak a köztéri kamerák képeinek elemzéséből származó, illetve az állampolgár földrajzi helyzetéről szóló adatok is – a big data analitika módszereinek segítségével a mesterséges intelligencia révén feldolgozzák, s az értékelő, minősítő algoritmusok által kap, vagy veszít pontokat az állampolgár. A pontoknak komoly jelentősége van az állampolgár, illetve gyermeke számára a különböző erőforrásokhoz történő hozzáférés tekintetében, ahogy az az 1. táblázatban látható.

Erőforrás	Jutalmazás	Büntetés
Autóvásárlás	Feliratkozás a legfrissebb modellek VIP-várólistájára, kedvező hitelek vásárláskor	Nem, vagy csak kedvezőtlenebb feltételek mellett lehet hitelt felvenni
Egészségügyi ellátás	A várólistás egészségügyi ellátásoknál előrébb sorolás, kiemelt ellátás lehetősége 1-2 ágyas kórtermekben	várólistáknál hátrébb sorolás, alapvető ellátás lehetősége (pl.: sokágyas kórtermekben)
Lakhatás	A megbízható állampolgár könnyebben kap albérletet, kedvezményes hitelfelvétel ingatlanvásárláshoz	Nehezebben adják ki számára az albérletet, nem tud felvenni hitelt ingatlanvásárláshoz
Oktatás	Képzéseken, továbbképzéseken történő részvétel állami támogatása, a gyermek elitiskolába járhat, tanulmányi ösztöndíjak	Bizonyos képzésekre nem lehet bekerülni, nincsen tanulmányi támogatás és ösztöndíj sem
Utazás	korlátlan utazás lehetősége a világ bármely országába, VIP ellátás, gyors becsekkolás, lazább és gyorsabb ellenőrzés, csomagátvizsgálás	korlátozott utazás, kiutazás tiltása, hosszú várakozás a becsekkolásra, alapos és sok időt igénybe vevő ellenőrzés, csomagátvizsgálás
Ügyintézés	azonnali információ határidős lehetőségekről, hatékony, gyors, gördülékeny ügyintézés, előrébb sorolás	lassú ügyintézés, több hivatalnoki akadékoskodás, hátrébb sorolás, lemaradás határidős lehetőségekről
Üzleti élet	vállalkozás gyors indításának lehetősége, kedvező vállalkozói hitelek, gyors és kedvező hitelbírálat, azonnali információ határidős lehetőségekről	vállalkozás elindításának hátráltatása, lassú, idegőrlő folyamatok, nem lehet hitelt felvenni az induláshoz, lemaradás a határidős lehetőségekről
Vásárlás	hozzáférés a legújabb termékekhez, felvétel VIP-listára, kedvező hitelek, gyors hitelbírálat, vásárlási kedvezmények	hitel nincs, vagy csak sokkal rosszabb feltételek mellett, nincsenek vásárlási kedvezmények, hosszú várakozási, sorban állási idők

1. Táblázat: *Jutalmazás és büntetés a társadalmi kredit rendszerében (saját szerkesztés)*

A fentiek alapján látható, hogy megéri „jó gyereknek” lenni, vagyis olyan állampolgárnak, illetve vállalkozásnak, aki/ami a kormányzati elvárások szerint viselkedik, cselekszik. Egy ilyen méretű, több mint 1 milliárd ember, s sokmillió vállalkozás adataival

dolgozó, s az állampolgárokat és vállalkozásokat folyamatosan értékelő rendszer megtervezése, megvalósítása, tesztelése, elindítása, javítása, fejlesztése nagyon komoly szakmai és technikai fejlettséget követel meg, s megannyi (nem csak) adat- és információbiztonsági kihívást jelent a rendszer fejlesztésével, üzemeltetésével, javításával foglalkozó informatikusoknak, hivatalnokoknak és egyéb szakmák képviselőinek. A kínai társadalmi kredit rendszerének sikeres működése így nem csak politikai-társadalmi célokat szolgál, de igazolja azt a gazdasági és tudományos potenciált is, amit Kína tudatosan épített fel ez elmúlt évtizedekben. Ezért kutatásomban – ahogy arról lentebb számot is adok – nem csak az adat- és információbiztonsági problémákat nevesítettem, hanem bemutatom a társadalmi kredit rendszerének többdimenziójú beágyazódását és kínai hátterét is.

KUTATÁS

A társadalmi kredit rendszerét, illetve annak információbiztonsági kérdéseit több módszer segítségével vizsgáltam meg, úgymint: adatbányászat, eset-, dokumentum- és tartalomelemzés, online kérdőív, szakértői megkérdezés. Az alábbiakban az egyes módszerek rövid módszertani összefoglalását ismertetem.

Az adatbányászat során a Kínával és a világgal kapcsolatos adatok forrása a Világbank, valamint a worldpopulationreview.com adatbázisai voltak. Elsősorban idősoros elemzéseket végeztem, melyek módszertani hátterét Schmarzo [4], Pierson [5] és Natinga [6] munkái biztosították.

Bár a szigorúan vett eset-, dokumentum-, illetve tartalomelemzés gyakran külön-külön módszerként szerepel, én ezt a három módszert összevontam. Tettem ezt azért, mert a céloom nem a módszerek közötti (markáns) módszertani határok szerinti elkülönítés volt, hanem az, hogy a téma médiareprezentációját, vagyis a különböző forrásokból származó, nyilvánosan elérhető tartalmak – melyekben megtalálhatóak voltak többek között az esetleírások, a kritikai észrevételek, a hivatalos kormányzati nyilatkozatok, a pártkongresszusok dokumentumai – saját szempontjaim szerint elemezzem. A módszertan tekintetében Cseh-Szombathy és Ferge [7], Horváth és Mitev [8], Krippendorff [9], illetve Langer [10] munkáira hagyatkoztam. Fontosnak éreztem, hogy kutatásomba a Kínáról szóló meghatározó könyveket is bevonjam. A továbbiakban az említett módszerekre összefoglaló névvel dokumentumelemzésként hivatkozom írásomban.

Az online, nagymintás kérdőív – melyet a Google űrlap segítségével készítettem – linkjét saját facebook oldalamon, illetve releváns városi facebook-csoportokban tettem elérhetővé 2020 április elejéig. A kérdőív elkészítése, illetve kiértékelése módszertanában Halter [11], Sajtos és Mitev [12], Freedman, Pisani és Purves [13], Moksony [14], Babbie [15], valamint Scipione [16] munkáit vettem alapul.

A dokumentumelemzés, valamint az online, nagymintás kérdőív használata mellett azt is fontosnak tartottam, hogy a kapott eredmények alapján egy reálisnak tekinthető jövőképet – amibe a tanulmányom írásának idején (nem csak) Kínában megjelenő koronavírusjárvány is komoly befolyásoló tényező – vázoljak fel a kínai, illetve általánosságban a társadalmi kredit rendszerek, illetve ezek információbiztonsági kihívásaival kapcsolatban. Ennek érdekében saját megállapításaimat öt szakértővel folytatott szakértői fókuszcsoporthoz beszélgetés során vitattam meg. A szakértői kiválasztással kapcsolatban Kollár [17] módszertanára hagyatkoztam.

Az adatbányászat eredményei

Kína társadalmi és gazdasági erejének és fejlődésének bemutatásánál jelen tanulmányomban néhány (makrogazdasági) mutatót ismertetek komparatív módon a világ és Kína viszonylatában. A legfrissebb – 2018-as – adatok alapján a világ lakosságának közel egyötöde (1 392 730 000 fő) él Kínában. Az országban az egy főre jutó GDP ugyan még a világátlag alatt van, ugyanakkor a GDP növekedésének az üteme a világátlag feletti, s ha hozzávesszük ehhez azt, hogy a világátlaghoz (45%) képest 11 százalékponttal több ember vesz részt a kínai GDP előállításában, akkor a GDP további növekedési üteme valószínűsíthető az országban. A villamosenergia-hálózat szinte az egész országban kiépült, ami azt is jelenti, hogy rendelkezésre áll a szükséges elektromos áram az internetezésre alkalmas eszközök (számítógépek, laptopok, tabletek, okostelefonok) áramellátásához, illetve töltéséhez. A világ 2016-ban érte el, hogy statisztikai átlag alapján azt lehet állítani, hogy mindenkinek van legalább egy mobiltelefon-előfizetése. Bár Kína ehhez képest egy évvel lemaradt, jelenleg már a világátlag feletti – 115 mobiltelefon-előfizetés/100 lakos – értéket mutat. Ha ehhez a tényhez hozzávesszük, hogy Kínában az elmúlt években az eladott telefonok döntő hányada az internetezésre alkalmas okostelefon volt, akkor látható, hogy a lakosság nagy része képes mobiltelefonon keresztül is elérni a világhálót. Hasonlóan jó a helyzet a széles-sávú internet-előfizetések tekintetében. 2009-ig Kína lemaradásban volt a világátlaghoz képest, azóta azonban a világátlag kétszerese (28 előfizetés/100 fő) ez az érték. Az okostelefon-használat, illetve mobiltelefon-, valamint szélessávú internet-előfizetés együttesen azt jelenti, hogy a kínai lakosság jelentős része rendszeresen hozzá tud férni az online elérhető tudás- és információjához, valamint egyéb online (erő)forrásokhoz, így például online tudja intézni vásárlásai egyre nagyobb részét, aktív közösségi életet tud folytatni. Az adatbányászat megállapításai között célszerű megemlíteni azt is, hogy világviszonylatban 2007 óta többen élnek a városokban, mint vidéken. Kínában ugyan csak 2011 óta igaz ez az állítás, de a városiasodás üteme lényegesen gyorsabb, mint a világ többi részén. Így különböző becslések alapján azt lehet mondani, hogy 2024-2037 között három kínaiából kettő városi lesz. A kínai urbanizációt jól jelzi az is, hogy a worldpopulationreview.com legfrissebb adatai szerint 5 olyan város van, amelyik megacity, s 160 olyan, amelyiknél a lakosság lélekszáma meghaladja az egymillió főt.

A fentiek alapján is megállapítható, hogy a társadalmi kredit rendszerének műszaki háttere – elektromos ellátottság, széles sávú internet, mobilkommunikációs eszközök és hálózatok – adott, s a sűrűn lakott, bekamerázott városokban a lakosság megfigyelése révén nagyon sok adat „termelődik” folyamatosan.

A dokumentumelemzés eredményei

A dokumentumok elemzése során előbb két nagy halmazt – könyvek, szabadon elérhető online források – majd azt követően több részhalmazt képeztem.

A könyveket témájuk és szerzőik alapján a következő részhalmazokba soroltam:

- (1) általános témájú könyvek Kínáról [18], [19]
- (2) könyvek a kínai (üzleti) kultúráról [20], [21], [22], [23]
- (3) könyvek a kínai kormányzásról, politikáról és annak kritikájáról [24], [25], [26], [27], [28], [29]
- (4) könyvek Kína világra gyakorolt hatásáról [30], [31]

A könyvekből meglehetősen heterogén kép alakítható ki Kínáról. Abban azonban szinte valamennyi szerző egyet ért, hogy Kínában az elmúlt néhány évtizedben számos olyan változás indult el, amelyik révén egyre nagyobb hatalomra tett szert a világban, technikai, technológiai potenciálja folyamatosan erősödik. Kína nem csak „mindent gyárt”, de a 2019-es Világgazdasági Fórumon elhangzott álláspont szerint a világ jövőjét meghatározó, mesterséges intelligenciával foglalkozó kilenc vállalatból három (Alibaba, Baidu, Tencent) kínai. A korábbi bérnyújtás mellett (s egyre inkább helyett) önálló kínai márkák jelennek meg, s válnak a globális piacokon is ismert és keresett márkákká. A kínai kereskedelmi mentalitás is átalakult, a nagyobb kínai elektronikus piacterek olyan biztonságos adásvételeket tesznek lehetővé, ahol a vevőt megannyi megoldás védi az esetleg tisztességtelenül kereskedő eladóval szemben, akinek egyébként is megéri tisztességesen eljárni vevői irányába, mert ellenkező esetben komoly szankciókkal sújthatják (pl.: büntetőpontok, ideiglenes, vagy végleges kizárás a piacterről).

A szabadon elérhető, publikus forrásokat három csoportba soroltam:

- (1) hivatalos – zömében kínai nyelven elérhető – források (a kínai kormány sajtóközleményei, felelős vezetőinek nyilatkozatai, az állami médiában megjelent információk, pártkongresszusok jelentései, hivatalos tanulmányok, hivatalos eseteírások, stb.)
- (2) a kínai ellenzék – zömében angol nyelven elérhető – véleménye a társadalmi kredit rendszeréről (kritikai állásfoglalások, vélemények, problémás esetek bemutatása, egyéni sorsok bemutatása, szubjektív életképek, beszámolók, stb.)
- (3) angol nyelven elérhető – feltételezhetőleg nem a kínai ellenzékhez köthető – dokumentumok (független (nek gondolt) szakértői vélemények és értékelések, az USA kormányzatához és háttérintézményeihez köthető vélemények, állásfoglalások, kutatási jelentések, beszámolók, demokráciajelentések és -riportok, stb.)

Kutatásomban próbáltam figyelmen kívül hagyni a Kína-USA között érezhető (nem csak) politikai feszültségeket, s elsősorban a társadalmi kredit médiareprezentációjának objektív, több szempont és dimenzió mentén történő elemzésére helyeztem a hangsúlyt, az adat- és információbiztonság fókuszában. Több olyan hivatalos leírást is olvastam (a kínai nyelven elérhető forrásokat google fordító segítségével fordítottam angolra), amelyek tartalmában nem volt elfogadható mértékben kongruens más hasonló tartalommal. Ennek okát abban látom, hogy a társadalmi kredit rendszerét különböző társadalmi és gazdasági helyzetű kínai városokban tesztelték, s pont a rendszer tesztüzemében („társadalmi kísérlet”) a különböző városokban egymástól eltérő elvárások és súlyok mentén alakították ki az értékelő algoritmusokat.

Elsőként tizenkét (nem csak) adat- és információbiztonsági problémát azonosítottam, majd még további kettőt, így kutatásom jelen zárótanulmányában az alábbi tizennégy problémát nevesítem:

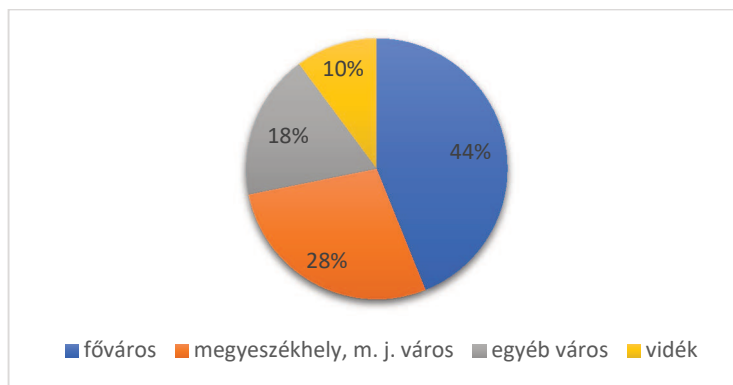
- (1) Visszaélés az egyén arcával, az arc módosítása, takarása
- (2) Visszaélés az egyén adataival és eszközeivel
- (3) Egyén illetéktelen követése
- (4) Hibásan működő szenzorok és aktuátorok
- (5) Rendszerelemek közötti kommunikációs hiba
- (6) Adatbázis – struktúrahiba

- (7) Adatbázisok összekapcsolási hibája
- (8) Rossz, hibás adatelemzés és algoritmusok
- (9) Gépi tanulási hibák
- (10) A mesterséges intelligencia hibái
- (11) Hivatalnokok és informatikusok (szándékos) károkozása
- (12) Hackerek támadása
- (13) Külföldi gyártók és a mögöttük álló titkosszolgálatok
- (14) A társadalom tagjainak védekező mechanizmusa

Elsősorban nem az adat- és információbiztonsághoz köthető a nem hivatalos kínai (elsősorban kínai ellenzék, USA) álláspontok, melyek ugyancsak heterogén képet mutatnak, s más-más hangsúlyokat tartanak fontosnak, de abban egyet értenek, hogy a társadalmi kredit rendszere nagymértékben káros a demokráciára, veszélyezteti az emberi (szabadság)jogokat, a véleménynyilvánítás és szólásszabadságot, az ember privát szféráját. Azt is aggályosnak tartják, hogy a büntetést nagyon nehéz jóvá tenni, s komoly hatása van nem csak az adott egyénre, hanem például gyermekére is.

Az online nagymintás kérdőív eredményei

Online kérdőívemet – mely a demográfiai kérdések mellett négy területen tartalmazott 1-1 kérdést, illetve az utolsó kérdés a kitöltő szabadszavas válaszára volt kíváncsi – összesen 394-en töltötték ki, közülük közel 60% (236 fő) volt férfi, s közel 40% (148 fő) nő. A legfiatalabb kitöltő 17 éves, a legidősebb 64 éves volt, a kitöltők átlagéletkora 32 év. A kitöltők lakóhelyi településtípusainak arányát a 2. ábrán lehet látni.



2. Ábra: A válaszadók lakóhelyi településtípusainak aránya (saját szerkesztés)

Magyarországon a városlakók aránya 70% körül van, mintámban a városlakók felülprezentáltak, számszerűsítve: a válaszadók közül a fővárosban 173-an, megyeszékhelyen, illetve megyei jogú városban 110-en, egyéb városban 71-en laknak (összesen 90%), s csak 40 fő (a kitöltők 10%-a) lakik vidéken. A mintám iskolai végzettség szerinti megoszlása a következő: 13% (50 fő) alapközü, 32% (126 fő) középözü, s 55% (218) fő rendelkezik felsőözü végzettséggel. Mintám demográfiai leírásának utolsó kérdése a családi helyzetre vonatkozott, melynek eredménye a 2. táblázatban látható.

	hajadon, nőtlen	nős, fér- jezett	alkalmi kapcsolat	tartós pár- kapcsolat	bejegyzett élet- társi kapcsolat	elvált	özvegy
férfi	16	75	56	42	17	27	3
nő	12	37	26	52	10	14	7
összesen	28	112	82	94	27	41	10

2. Táblázat: A válaszadók családi állapota nemek szerint (saját szerkesztés)

A demográfiai kérdések után arra kértem a válaszadókat, hogy ötfokú Likert-skálán négy területen értékeljék tudásukat, ismereteiket, illetve azt, hogy a tanulmányom elméleti, valamint dokumentumelemzéssel foglalkozó részeinél leírt módszereket, eljárásokat mennyire tartják elfogadhatónak. A válaszoknál a Likert-skála mellett lehetőség volt a „nem tudom megítélni” válaszlehetőséget is bejelölni. Az értékelés során együttesen kezeltem a „nem tudom megítélni” választ, illetve azt, amikor nem érkezett semmilyen válasz az adott állításra.

A válaszadó önértékelős tudását, ismereteit a felhő alapú számítástechnika, a big data elemzés, a mobiltechnológia, a közösségi média, az információbiztonság, a kiterjesztett és kevert valóságok, az IoT (dolgok internete) a robotok, drónok, illetve a mesterséges intelligencia területein vizsgáltam. Az eredményeket a 3. táblázat szemlélteti.

Milyennek értékeled tudásodat az alábbi területeken?	átlag	rangsor	válaszok száma	nem tudom megítélni, nincs válasz
Közösségi média	4,6	1	393	1
Mobiltechnológia	4,4	2	393	1
Felhő alapú számítástechnika	4,2	3	383	11
Mesterséges intelligencia	3,9	4	381	13
Big data elemzés (adatelemzés)	3,8	5	381	13
Robotok, drónok	3,7	6	378	16
Kiterjesztett és kevert valóságok	3,3	7	370	24
Információbiztonság	3,2	8	382	12
IoT (dolgok internete)	3,1	9	362	32

3. Táblázat: A válaszadók önértékelése a társadalmi kredit rendszeréhez (is) kapcsolódó területek vonatkozásában (saját szerkesztés)

Az eredmények alapján megállapítható, hogy a minta a közösségi média és a mobiltechnológia vonatkozásában értékeli a tudását a legtöbbre, míg az információbiztonság az utolsó előtti helyen végzett.

A következő kérdés arra vonatkozott, hogy a válaszadók mennyire tartják elfogadhatónak a társadalmi kredit rendszerének előzményei között felsorolt megoldásokat, alkalmazásokat. Az eredmények a 4. táblázatban láthatók.

Mennyire tartod elfogadhatónak az alábbi megoldásokat, alkalmazásokat?	átlag	rangsor	válaszok száma	nem tudom megítélni, nincs válasz
Pedagógiai értékelés	4,6	1	391	3
Játékosítás, gamifikáció	4,4	2	359	35
Munkahelyi (teljesítmény)értékelés	3,9	3	389	5

Mennyire tartod elfogadhatónak az alábbi megoldásokat, alkalmazásokat?	átlag	rangsor	válaszok száma	nem tudom megítélni, nincs válasz
TAJ szám alapján történő keresés	3,8	4	391	3
A közúti közlekedési előéleti pontrendszer	3,7	5	389	5
Adószám alapján történő keresés	3,4	6	388	6
Vásárlás csak regisztrációval	3,1	7	385	9
Szereplés marketing adatbázisokban	2,8	8	389	5
Mobiltelefonos aktivitásom elemzése	2,4	9	393	1
Megfigyelnek a közösségi médiában	2,3	10	393	1
Bank elemzi pénzügyi aktivitásodat	2,1	11	387	7

4. Táblázat: A válaszadók véleménye a társadalmi kredit rendszerének előzményeinél felsorolt megoldásokról és alkalmazásokról (saját szerkesztés)

Látható, hogy a válaszadók leginkább a pedagógiai értékelést és a játékosítást fogadják el, vélhetőleg azért, mert ezek a megoldások tiszteletben tartják az egyén privát szféráját. A válaszadók leginkább a pénzügyi aktivitásaik elemzését, a közösségi médiában történő megfigyelésüket és a mobiltelefonos aktivitásaik elemzését utasítják el. Ez összességében azt jelenti, hogy amegkérdezettek markánsan húzzák meg (vagy legalábbis próbálják meghúzni) azt a határt, amin belül már nem szeretnék, ha bárki is kíváncsi lenne aktivitásaikra, s adatokat gyűjtene, majd azokat elemezné velük kapcsolatban.

A társadalmi kredit rendszerében a szűkösen, korláatosan rendelkezésre álló erőforrásokhoz való igazságos hozzáférés, illetve a társadalmi békés együttélés érdekében pontrendszer alapján rangsorolják az állampolgárokat. Ennél a kérdésnél arra voltam kíváncsi, hogy a megkérdezettek mennyire tartják igazságosnak a pontrendszer bevezetését, használatát a felsorolt erőforrásoknál, lehetőségeknél. Az eredményt az 5. táblázat szemlélteti.

Igazságosnak tartod az algoritmizált (automatizált szoftveres) értékelést/pontozást a következő területeken?	átlag	rangsor	válaszok száma	nem tudom megítélni, nincs válasz
Oktatásnál	4,5	1	392	2
Autóvásárlásnál	4,2	2	389	5
Üzleti életben	4,2	2	379	15
Utazásnál	4,1	4	390	4
Ügyintézésnél	3,9	5	387	7
Vásárlásnál	3,8	6	392	2
Lakhatásnál	3,6	7	384	10
Egészségügyi ellátásnál	2,7	8	391	3

5. Táblázat: A válaszadók véleménye az algoritmizált (automatizált szoftveres) értékelésről, pontozásról (saját szerkesztés)

Ennél a kérdésnél a válaszadók a legelfogadóbbak az oktatásnál, az autóvásárlásnál, illetve az üzleti életben használt algoritmusos értékelés/pontozás területén voltak. Az oktatásra adott magas átlag okát abban látom, hogy a tanulmány idején az országban távoktatás folyt, s vélhetőleg a számítógéppel segített/támogatott (táv)oktatás színvonalának gondolták a válaszadók az automatizált szoftveres megfogalmazást. A válaszadók a legkevésbé az

egészségügyi ellátásnál bíznak magukat az algoritmizált értékelésre/pontozásra. Ez a vélemény megfeleltethető annak az általánosan elfogadott nézetnek, miszerint a beteg, gondozásra szoruló emberek jelenleg még igénylik a humán orvosi, szakszemélyzeti közvetlen beavatkozást (pl.: anamnézis felvétele, diagnózis, kezelési terv, ápolás, gondozás, műszerek eredményeinek értékelése).

A dokumentumelemzés módszerével beazonosított (nem csak) adat- és információbiztonsági problémákat hasonló megfogalmazással vizsgáltam meg az online kérdőíves kutatásomban is. A válaszokat a 6. táblázat szemlélteti.

Mennyire tartod veszélyesnek az alábbiakat?	átlag	rangsor	válaszok száma	nem tudom megítélni, nincs válasz
visszaélés a személy arcával	4,7	1	393	1
visszaélés a személy személyes adataival	4,7	1	393	1
egyén illetéktelen követése	4,6	3	392	2
hivatalnokok, informatikusok szándékos károkozása	4,5	4	392	2
hackerek támadása	4,3	5	393	1
kommunikációs hiba az egyes eszközök között	3,9	6	390	4
adatok hibás elemzése	3,8	7	380	14
rossz, hibás adatok	3,7	8	384	10
mesterséges intelligencia hibái	3,7	8	380	14
hibásan működő szenzorokból eredő rossz döntés	3,6	10	385	9
hibásan működő adatbázisok	3,6	10	382	12
külföldi titkosszolgálatok tevékenysége	3,2	12	389	5
gépi tanulás hibái	3,1	13	376	18

6. Táblázat: A válaszadók véleménye a társadalmi kredit rendszerében azonosított hibákról (saját szerkesztés)

Az erre a kérdésre adott válaszok kongruálnak a társadalmi kredit rendszerének előzményeivel kapcsolatban kapott válaszokra. Ott megállapítottam, hogy a vizsgált minta markánsan meghúzza (vagy próbálja meghúzni) azt a határt, ami védelmet jelent(het) a számára. A válaszadók a legveszélyesebbnek a személy arcával, személyes adataival való visszaélést, valamint az illetéktelen követést tartják. Ugyancsak magas átlagosztályzattal (4. és 5. hely) szerepel a humán típusú információbiztonsági problémák, vagyis a hivatalnokok, informatikus szándékos károkozása, illetve a hacker által elkövetett támadások. A zömében technikai eredetű problémákat az említettekhez képest kevésbé gondolják veszélyesnek a válaszadók. Ez összességében arra enged következtetni, hogy a vizsgált minta véleménye hasonlatos azzal az általános megállapítással, miszerint az informatikai rendszerek leggyengébb láncszeme az ember.

ÖSSZEFOGLALÓ GONDOLATOK – A SZAKÉRTŐI MEGKÉRDEZÉS EREDMÉNYEI

Jogos lehet a felvetés, hogy mi szükség volt egy alapvetően Kínával, a Kínában bevezetésre kerülő társadalmi kredit rendszerével foglalkozó kutatásban megvizsgálni azt

is, hogy hogyan vélekedik 394 magyar ember a témával kapcsolatban. Mivel a társadalmi kredit rendszerének előzményeinél már utaltam arra, hogy a módszerek alapvetően nem Kínából származnak, így kíváncsi voltam arra, hogy vajon Magyarországon mennyire fogadnák el az emberek egy hasonló rendszer bevezetését. A kérdőív nem vizsgálta az adatbázisok összekapcsolását, mivel meglátásom szerint egy átlagos kitöltő nem biztos, hogy tisztában van ennek műszaki-informatikai megoldásaival, illetve az összekapcsolás segítségével megvalósuló adat-multiplikáció mélyelemzésre gyakorolt hatásával és lehetőségeivel. A felvetésre a választ szakértői fókuszcsoportos online beszélgetés segítségével adtam meg, illetve a szakértői vélemények summázata jelenti egyben tanulmányom összefoglalását is. Az öt szakértőre igazak a következő állítások: mindannyian felsőfokú oklevéllel rendelkeznek (1 fő főiskolai, 3 fő egyetemi, 1 fő doktori oklevéllel), legalább 10 éve dolgoznak releváns területen (1 fő informatikai rendszerek fejlesztése, 1 fő adatbányászat, 1 fő információbiztonság, 1 fő szociológia/társadalomkutatás, 1 fő műszaki felsőoktatás), a társadalmi kredithez kötődő, vagy kapcsolódó témában (robusztus adatbázis rendszerek tervezése, megvalósítása, nagy rendszerek adat- és információbiztonsága, mesterséges intelligencia felhasználása a biztonság területén, ember a mesterséges intelligencia korában, stb.) legalább 3 előadást tartottak és/vagy 3 szakmai cikket írtak. Bár a szakértői megkérdezésnél rendszerint a szakértők nevesíthetők, mivel az öt fő közül három anonimitást kért az aktuális munkáira és megbízásaira hivatkozva, így a másik kettőt sem nevezem meg. A szakértők az online fókuszcsoportos beszélgetés előtt megkapták a jelen tanulmányomban bemutatott kutatási eredményeimet, illetve korábbi releváns kutatási anyagaimat. Ennek alapján a közösen kialakított véleményünket kutatásom zárásaként alább ismertetem.

- 1) A társadalmi kredit rendszerének kínai, vagy hasonló rendszerek nem kínai bevezetésének nagy a valószínűsége (Kínában ebben az évben, vagy jövőre, más országokban a közeljövőben), mivel
 - a) Kína mellett több ország rendelkezik olyan technológiai potenciállal, aminek a révén a rendszer egyes elemei integrálhatók a társadalmi kredit rendszerébe
 - b) egyre komolyabb nemzetbiztonsági igény jelentkezik olyan rendszerek használatára, amelyek nagymértékben elősegítik a bűnüldözést, s eredményesen javítják a bűnügyi statisztikákat
- 2) A nemzetbiztonságra gyakorolt hatás az említettek mellett megjelenik a következőkben is:
 - a) (közel) valós idejű nemzetbiztonsági átvilágítás lehetősége
 - b) a csoportos bűnelkövetés, a szervezett bűnözői csoportok hatékonyabban deríthetők fel
 - c) a viselkedésalapú elemzés bevezetésével meg lehet jósolni, hogy ki akar terrorcselekményt elkövetni, s még az elkövetés előtt ártalmatlanítani lehet
 - d) álhírek visszaszorítása azáltal, hogy a netes felületek csak regisztrációt követően használhatók
 - e) ha a rendszer nem ismeri fel az egyén arcát, akkor az vagy rejtőzködik (smink, maszk), vagy külföldi, könnyebben lehet kiszűrni a tömegben
 - f) hamarabb kiszűrhetők a gyanús elemek
 - g) nevelési célzattal nyomon lehet követni az egyén fejlődését (a társadalmi kredit rendszerével támogatott pártfogói felügyelői szolgálat)

- h) nyomozás forró nyomon a feltételezett elkövető arcának és telefonjának beazonosítása segítségével
 - i) szakemberek hatékonyabb munkavégzése
- 3) A bevezetésnek több gátló tényezője is lehet, úgymint:
- a) nem, vagy nem megfelelő mennyiségben állnak rendelkezésre a rendszer biztonságos bevezetéséhez szükséges erőforrások (humán, pénzügyi, informatikai (hardver))
 - i. viszonylag kevés szakember mozog magabiztosan, több éves releváns tapasztalattal a mesterséges intelligencia, a valóban robusztus mennyiségű adatok közel valós idejű elemzése területén (tehát a témához egyébként értő szakembereknek is tanulni, tesztelni, kísérletezni kell)
 - ii. egy ilyen rendszer elindítása nagyon sokba kerül, ráadásul ez nem csak egyszeri költség, hanem a fenntartása, a fejlesztése, az üzemeltetése, a javítása egyaránt jelentős kiadást jelenthet nemzetgazdasági szinten
 - iii. bizonyos hardvergyártók felé megrendült a bizalom (Kína ezt úgy oldotta meg, hogy az elkövetkező néhány évben a kormányzati területen használt nem kínai gyártású informatikai (rendszer)eszközöket kínaira cseréli le)
 - b) a társadalom nem feltétlenül fogadja el az olyan rendszereket, amelyek alapfeladata az állampolgárok folyamatos megfigyelése, értékelése, pontozása. Éppen ezért:
- 4) Nagyon fontos kérdés, hogy az adott ország
- a) a rendszer bevezetésével kapcsolatban milyen politikai narratívumokat használ
 - b) hogyan készíti fel a lakosságát a rendszer bevezetésére
 - c) biztosítja-e a rendszer működésének törvényi hátterét, illetve
 - d) biztosítja-e a rendszer hibás működéséből származó, az állampolgárok sorsát negatívan befolyásoló rendszer-döntések miatti károk jogorvoslati lehetőségét (hasonlóan az ártatlanul elítélt állampolgárok kártérítéséhez)
- 5) A társadalmi kredit rendszerének bevezetése nagy valószínűség szerint új társadalmi normák és viselkedési formák megjelenését is eredményezi, mint pl.: digitális nomádok, technofókok, „géprombólók” (a rendszer tanuló algoritmusait szándékosan hamis adatokkal tanító állampolgárok)
- 6) A kínai szakembereknek a társadalmi kredit rendszerének fejlesztése, tesztelése, bevezetése, üzemeltetése, hibajavítása során szerzett tapasztalatai akár a rendszer, vagy bizonyos elemei, akár a know-how vonatkozásában nemzetközi szinten is kiváló exportcikket jelentenek.

Köszönetnyilvánítás

A tanulmány az Innovációs és Technológiai Minisztérium ÚNKP-19-3-I-OE-38 kódszámú Új Nemzeti Kiválósági Programjának szakmai támogatásával készült.

FELHASZNÁLT FORRÁSOK

Irodalom

- [1] Cs. Kollár, „A társadalmi kredit rendszerének információbiztonsági kérdései”, in: *XXXV. Jubileumi Kandó Konferencia 2019*, Zs. Temesvári, Ed., Budapest: Óbudai Egyetem, KVK, 2020:a, pp. 150-161.

- [2] Cs. Kollár, „A társadalmi kredit rendszeréből következő oktatási és képzési feladatok”, in: *Neveléstudományi kutatások a Kárpát-medencei oktatási térben. Pedagogical Research in the Carpathian Basin Educational Space*, P. Tóth, K. Horváth, E. Maior, M. Bartal, J. Duchon, Eds., Komárno: Selye János Egyetem Tanárképző Kar, 2019, pp. 531-547.
- [3] Cs. Kollár, „Kína és a társadalmi kredit rendszere nem csak az adat- és információbiztonság fókuszában” *Hadtudomány* (megjelenés alatt) 2020
- [4] B. Schmarzo, „*Big Data MBA*,” Indianapolis: John Wiley & Sons, Inc., ISBN: 978-1-119-18111-8, 2016.
- [5] L. Pierson, „*Data Science*,” Hoboken, New Jersey: John Wiley & Sons Inc, ISBN 13: 9781119327639 2017.
- [6] D. Nattanga, „*Data Science Algorithms in a Week*,” Birmingham – Mumbai: Packt Publishing, 2017.
- [7] L. Cseh-Szombathy, Zs. Ferge, „*A szociológiai felvétel módszerei*,” Budapest: Közgazdasági és Jogi Könyvkiadó, 1971.
- [8] D. Horváth, A. Mitev, „*Alte, natív kvalitatív kutatási kézikönyv*,” Budapest: Alinea Kiadó, 2015.
- [9] K. Krippendorff, „*A tartalomelemzés módszertanának alapja*,” Budapest: Balassi Kiadó, 1995.
- [10] K. Langer, „*Kvalitatív kutatási technikák*,” Gödöllő: Szent István Egyetem, 2009.
- [11] C. Halter, „*The PSPP Guide Expanded Edition*,” S.l.: CreativeMinds Press Group, 2014.
- [12] L. Sajtos, A. Mitev, „*SPSS Kutatási és Adatelemzési Kézikönyv*,” Budapest: Alinea Kiadó, 2007.
- [13] D. Freedman, R. Pisani és R. Purves, „*Statisztika*,” Budapest: Typotex, 2005.
- [14] F. Moksony, „*Gondolatok és adatok*,” Budapest: Osiris Kiadó, 1999.
- [15] E. Babbie, „*A társadalomtudományi kutatás gyakorlata*,” Budapest: Balassi Kiadó, 2017.
- [16] P. A. Scipione, „*A piackutatás gyakorlata*,” Budapest: Springer-Verlag, 1994.
- [17] Cs. Kollár, „*A szakértővé válás, illetve a szakértők kiválasztásának és megkérdésének módszertani kihívásai*,” *Vezetéstudomány* (49), pp. 63-75, 2018.
- [18] E. L. Shaughnessy, „*Kína*,” Budapest: Saxum Kiadó, 2011.
- [19] L. Mark: *Mit gondol Kína?* Budapest: Gondolat Kiadó, 2008.
- [20] E. G. Hinkelman, „*World Encyclopedia of Business Culture*,” San Rafael: World Trade Press, 1998.
- [21] P. Ostrowski, M. B. Christensen és G. Penner, „*It's All Chinese To Me: An Overview of Chinese Culture, Travel & Etiquette*,” North Clarendon: Tuttle Publishing, 2018.
- [22] S. D. Seligman, „*Chinese Business Etiquette: A Guide to Protocol, Manners, and Culture in the People's Republic of China*,” New York: Warner Books, 1999.

- [23] J. Trosclair, „*Chinese Business Dinner Culture: Mistakes to Avoid and Critical Must Do's to Gain Face, Impress Decision Makers and Close More Deals,*” Independently published, 2019.
- [24] X. Jinping, „*Kína kormányzásáról,*” Budapest: Antall József Tudásközpont, 2017.
- [25] H. Kissinger, „*Kínáról*” Budapest: Antall József Tudásközpont, 2017.
- [26] H. D. Burgh, „*Kína - Barát vagy ellenség?*” Budapest: HVG Könyvek kiadó, 2007.
- [27] C. Fang, „*A kínai reform és nyitás – Negyven év tapasztalata,*” Budapest: Antall József Tudásközpont, 2019.
- [28] P. Hessler, „*Kína országútjain – Az újjászülető birodalom mindennapjai,*” Budapest: Park Kiadó, 2013.
- [29] J. Hua, „*Kína tíz szóban,*” Budapest: Magvető Könyvkiadó, 2018.
- [30] W. Hirn, „*Kína, a nagy falat – Miként változtatja meg életünket Kína felemelkedése,*” Budapest: HVG Könyvek Kiadó, 2006.
- [31] F. Sisci, „*Merre tart Kína? - A nagy átváltozás,*” Budapest: KKETTK Közalapítvány, 2015.

Adatbázisok

worldpopulationreview.com adatbázisa (letöltés ideje: 2020. 03. 01., adatbázis legutóbbi frissítése: nincs jelölve)

Világbank adatbázisa (letöltés ideje: 2020. 03. 01., adatbázis legutóbbi frissítése: 2020. 02. 27.)

RECENZÍÓ SOLYMOS ÁKOS „FRICI, FÜLÖP ÉS A HACKEREK” CÍMŰ KÖNYVÉRŐL

GULYÁS Péter¹

Amikor 2018 őszén kollégám, Solymos Ákos megkeresett a társszerzőként az NJSZT-nek (Neumann János Számítógép-tudományi Társaság) írt, és cégem, a QUADRON Kiberbiztonsági Kft. által támogatott IT Biztonság közérthetően című könyv sikere után egy újabb könyvtámogatási ötlettel, nagy nyitottsággal fogadtam, mert tudtam, hogy Ákos továbból eddig csupa közérthető és hasznos tartalom került ki a közoktatás és szakképzés számára. Azonban amikor elmondta a részleteket, nagyon rácsodálkoztam: az elmúlt három évben szabadidejében – ami tudtommal nem nagyon akadt – írt egy gyerekeknek, szülőknek és talán tanároknak is szóló, teljesen közérthető nyelvű, IT biztonsági aktualitásokról szóló ismeretterjesztő könyvet és örülne, ha cégünk támogatná őt a kiadásban. Egy pillanatra sem gondolkodtam el azon, hogy vajon sikeres lesz-e, vagy hogy fatális hibát követünk el azzal, ha egy félresikerült könyv hátuljára cégünk logója felkerül. Ákos pedagógia képességeinél csak IT biztonsági tudásában és mindenki számára érthető előadásmódjában vagyok biztosabb, így egy percig sem gondolkodtam, azonnal rávágtam – a piszkozat elolvasása nélkül –, hogy természetesen támogatjuk. Tettem ezt azért is, mert a könyvhöz hasonló témában még nem tudtam akkor ahhoz foghatóról és magam is azt éreztem, hogy hiánypótló tud lenni a kiadvány, illetve természetesen abban is gondolkodtam, hogy cégünk karácsonyi ajándékként mennyire egyedi meglepetéssel tud majd egy év múlva kedveskedni ügyfeleinknek. Közel egy évet kellett várni a könyv megjelenésére, de amikor az első dedikált tiszteletpéldányt a kezembe kaptam Ákostól és kezdet fogtunk, azt éreztem, hogy egy fontos és nemes célt szolgálunk és ki tudja még milyen lehetőségek rejlenek Ákos első bátor lépésében, amelyet többek között kedves Felesége unszolására lépett meg.

Amikor a kezembe fogtam a könyvet, belelapoztam és a tartalomjegyzéket átfutva azonnal tudtam, hogy telitalálat. A címlap kifejezetten visszaadja az egész könyv szellemiségét, nyelvezetét és egyértelműen tükrözi a témát anélkül, hogy a címet elolvasnánk. A hátlap különösen megfogott, azonnal megkerestem az inspirációt adott képet, amelyhez ezután már a könyv miatt érzelmi szálak is kötődtek és még akkor decemberben egy Washingtoni konferencián beköszönő képként használtam egy előadásomban. A hátsó grafikai anynyira jól sikerült, hogy Feleségemnek komoly fejtörést okozott egy külföldi utam során, amikor távollétemben neki kellett elmagyarázni Kisfiamnak, hogy kik azok a hackerek és hogy apának mi köze hozzájuk (a válasz: „apa a jó hackerek főnöke”). A könyvet az első adandó alkalommal végigolvastam, és hát azt kell mondjam, hogy az oldalszámok csalókák: nem tudtam a könyvet letenni, mert annyira könnyed nyelvi környezetben mutatja be az

¹ peter.gulyas@quadron.hu | executive director / ügyvezető igazgató | Quadron Cybersecurity Services Ltd. / Quadron Kibervédelmi Kft.

egyébként sokak számára érthetetlen digitális világot, hogy az akár gyerekek, szülők, pedagógusok, orvosok, vagy akárki számára – akinek semmilyen számítástechnikai ismerete nincs – olvasmányosan, történeteken keresztül leírva minden apró részletre játékosan kitérve megérthetővé válik. A helyszín a szolnokporcsai Lakinger Béla Általános Iskola és környéke, ahol Frici és Fülöp, a két – az informatikát két kanállal habzsoló – jóbarát jár és mindenféle digitális és iskolai történetbe keveredik. Csupa olyan számunkra, informatikai biztonságban tapasztalt szakember számára alapesetben dolgoz fel tíz-húsz oldalas terjedelemben, amelyekről tudjuk, hogy a mindennapokban rendszeresen előfordul(hat) mindannyiunkkal, de a többség nemhogy nem ismeri fel, de a miértjeivel és a következményeivel sincsen tisztában. Játékosan leírja a ransomware-ek és a Facebook privacy beállítási rejtelmeinek lényegét vagy az internetes nyereményjátékok mögötti valóságot és hatásait, de az iskolai routerek feltörésének történetére, az adathalászat és a kéréstlen spam levelek világára is hoz gyermeki történetekbe bújtatott ismeretterjesztő példákat. „Csuka bácsi” a könyvben megjelenő, mindig naprakész IT biztonsági szakértő – akárcsak egy Google kereső – mindenről tud és pontos információkkal, gyakorlati példákkal magyarázza el a fiúknak a tudnivalókat, és hogy mit is kell tenni egy incidens esetén. De a helyzet megoldása után kitér mindig arra is, hogy hogyan kell majd megelőzni hasonló eseteket a jövőben. Nagyon pontos tükröt tart az iskolák informatikai rendszereinek helyzetéről és az azokat – sok esetben megosztott figyelmű – üzemeltető kollégák nehéz helyzetéről is. A történetek egyébként egymásra épülnek és visszautalások is vannak a korábbi tanmesékre, így tényleg mindenki számára hétköznapi nyelvre fordítja az egyébként érthetetlennek tűnő szakzsargont is. A kedvenc történetem egyébként az iskolai router feltörésének meséje, amely teljes szélességében leírja a mai világ egyik legnagyobb vívmányának a legkegyetlenebb hátulütőjét: az internet tényleg minden megtalálható. Vagyis, ha meg akarunk tanulni egy nyelvet, az épp annyira elérhető, mint hogy hogyan kell feltörni bármit, amihez egy kis érdeklődéssel hozzá szeretnénk férni. Emellett bemutatja az iskolák, a tanulók és az iskolai informatikai adottságainak valós világát mind a tanár, az iskolaigazgató „Sárkány úr” és a rendszergazda szemszögéből egyaránt.

A könyvet aztán a nappaliban Édesapám is megtalálta – akinek a mai informatikai ismeretek időnként azért kihívást jelentenek – és azonnal, mivel nagy könyvmoly, el is olvasta és elkért belőle pár másik példányt, mert elvitte jó pár ismerősének, akik mind nagyon pozitív visszajelzésekkel illették és külön felhívtak engem ezt elmondani. A legszebb az a hívás volt, amikor unokatestvérem, aki az Oktatási hivatalban dolgozik, odaadta olvasásra a Hivatal biztonsági vezetőjének. A könyv meg sem állt a vezetőségig, ahonnan azt a visszajelzést kaptuk, hogy minden pedagógusnak oda kellene adni, hogy ők is meg tudják közelíteni egyszerű olvasmányos formában a náluk erre sokkal fogékonyabb gyermekek informatikai ismereteinek szintjét. Erre felbuzdulva a könyvből azonnal további példányokat rendeltünk, és nem csak karácsonyi ajándékként adtuk ügyfeleinknek, hanem baráti, ismerősi körben is elkezdtük terjeszteni, amely azóta is nagy sikert arat. Nagyon fontosnak tartom, hogy ez a típusú ismeretterjesztés főleg egy ilyen nehezen internalizálható témában a leghatékonyabb: történetekbe bújtatva minden alapismeretet átad a napjainkban legismertebb biztonsági fenyegetettségek témájában. Nagyon fontos azt is megemlíteni, hogy ezen

kívül még nagyon sok ilyen jelenséggel találkozunk a QUADRON-nál nap-mint-nap, amelyek hónapról hónapra folyamatosan fejlődnek és változnak, így a könyv tartalma és tanítási hamarosan frissítésre szorulnak majd. Ezért Ákost szeretném továbbra is bátorítani, hogy írja meg a következő kötetet, pont ebben a terjedelemben és nyelvhasználattal, mert telitalát.

Érdekességképpen megemlítendő, hogy a könyv a 2019 szeptemberi megjelenése után pár nappal már fenti volt több nem-hivatalos terjesztő oldalon – ezzel is alátámasztva sikerét. A visszajelzések és a tanítási jellegénél fogva Ákos aztán 2020 április 14-én .pdf és e-book formátumokban közkinccsá tette (<http://frici.soan.hu>) az interneten is – jelezve ezzel is, hogy nem profitszerzés volt a könyv megírásának is kiadásának a célja –, és mára már tízezer felett van bőven a letöltések száma.

A KÖNYV SZERZŐJE

Solymos Ákos 2000-ben végzett az ELTE Tanító és Óvóképző Főiskolai karán, mint informatika műveltségi területen tanító. Egy rendszergazda tanfolyam elvégzését követően a kétezres évek elején informatikai biztonsági tanácsadóként dolgozott, majd 2005-ben csatlakozott az Ertse Bank Hungary információbiztonsági csapatához. Több éven keresztül vezette is ezt a csapatot, felelve a bank és leányvállalatai információvédelméért. A bankban töltött közel tíz év alatt komoly tapasztalatokat szerzett, több sikeres nemzetközi szakmai vizsgát és minősítést is magáénak tudhat (CISM, CRISC, ISO27001 vezető auditor, ISO22301 vezető auditor). 2015. év közepén csatlakozott a Quadron Kibervédelmi Szolgáltató Kft.-hez, ahol a mai napig is dolgozik és vezeti a tanácsadási, oktatási és kutatás – fejlesztési üzletágat. Az elmúlt három évben társszerzőként részt vett a Neumann János Számítógép-tudományi Társaság (NJSZT) IT Biztonság közérthetően című tankönyvének létrehozásában, hozzájárult szakmai anyagokkal a Nemzeti Közszerződési Egyetem Elektronikus Információbiztonsági vezető szakirányú továbbképzés tudásanyagához. 2019-ben megjelent első önálló információbiztonsági tudatosítással foglalkozó, gyerekeket és szülőket célzó könyve, Frici, Fülöp és a hackerek címmel. Rendszeresen megjelennek elsősorban biztonságtudatossággal kapcsolatos szakmai cikkei az elektronikus és nyomtatott médiában is. Gyakori szereplője a Karc FM, Kossuth Rádió és a Forrás Rádió információvédelemmel kapcsolatos szakmai műsorainak és beszélgetéseinek.

PUBLIKÁCIÓK

1. Erdősi Péter Máté – **Solymos Ákos**: IT Biztonság közérthetően, Neumann János Számítógép-tudományi Társaság (2017., 2018., 2019.) ISBN: 978-615-5036-12-5
2. Berzsenyi Dániel – Gyarak Réka – Hámornik Balázs Péter – Hirsch Gábor – Kiss Attila – Marsi Tamás – Orbók Ákos – Simon Béla – **Solymos Ákos** – Tikos Anita – Zsíros Péter: Incidensmenedzsment – Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára (2017.) Dialóg Campus Kiadó ISBN 978-615-5764-99-8

3. Dr. Bodó Attila – PálCser Orsolya Anikó – Dr. Gyaraki Réka Eszter – Kaczur Gábor – Dr. Lattmann Tamás – **Solymos Ákos** – Szabó Zsolt Mihály – Tikos Anita – Váczi Dániel – Dr. Zámbó Nóra: Célzott kibertámadások – Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára (2018.) Nemzeti Közszolgálati Egyetem ISBN: ISBN 978-963-498-062-9
4. **Solymos Ákos**: Frici, Fülöp és a hackerek, Underground Kiadó (2019.) ISBN: 978-615-0056-87-6

A KÖNYV KÖNYVÉSZETI ADATAI

Nyomtatott formátum:

Kiadó: Underground Kiadó és Terjesztő Kft.

Oldalak száma: 118

Borító: PUHATÁBLÁS, RAGASZTÓKÖTÖTT

Súly: 170 gr

ISBN: 9786150056876

Nyelv: MAGYAR

Kiadás éve: 2019

EPUB és MOBI formátum:

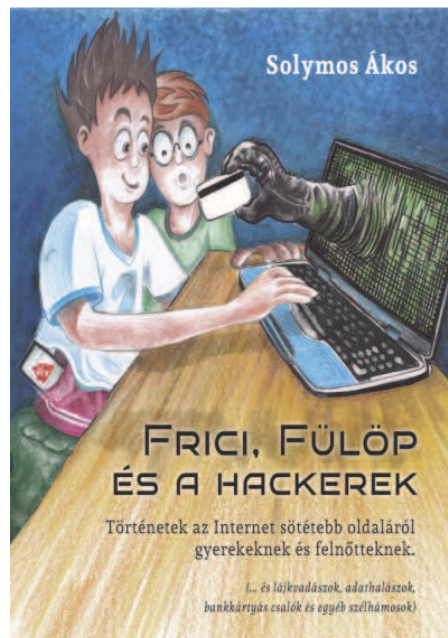
Kiadó: Underground Kiadó és Terjesztő Kft.

Oldalak száma: 118

ISBN: 9786156066046

Nyelv: MAGYAR

Kiadás éve: 2019



1. Ábra: Solymos Ákos „Frici, Fülöp és a hackerek” című könyv borítója

