HADMÉRNÖK

Kiemelt közlemények

19. évf. (2024)
4. szám

ISSN 1788-1919 (elektronikus)

LUDOVIKA
EGYETEMI KIADÓ

IMPRESSZUM

Hadmérnök
Katonai műszaki tudományok online folyóirata
ISSN 1788-1919 (elektronikus)

Nemzeti Közszolgálati Egyetem
1101 Budapest, Hungária krt. 9–11.
Postacím: 1581 Budapest, Pf. 15.
„A” épület 9. emelet, 901. iroda
Telefon: +36-1-432-9000/29-289, Fax: +36-1-432-9025
E-mail: hadmernok@uni-nke.hu
Web: https://folyoirat.ludovika.hu/index.php/hadmernok

Kiadó
Nemzeti Közszolgálati Egyetem Ludovika Egyetemi Kiadó
Székhely: 1083 Budapest, Ludovika tér 2.
Kapcsolat: www.ludovika.hu; kiadvanyok@uni-nke.hu
A kiadásért felel: Deli Gergely rektor
Olvasószerkesztők: Farkas-Nagy Judit, Resofszki Ágnes

Tartalom

HADMÉRNÖK
KATONAI MŰSZAKI INFRASTRUKTÚRA

19. évfolyam (2024) 4. szám 5–17.
DOI: 10.32567/hm.2024.4.1

Halász András,[1] Nagy Dominik,[2] Jancsó Mihály,[3]
Varga Krisztina,[4] Bojté Csilla,[5] Csízi István[6]

Erdősávok harctevékenységekre gyakorolt hatása: a hadszíntér-előkészítés erdősítési szempontjai[7]

The Effect of Shelterbelt Forest on Combat Activities: Afforestation Aspects During Preparation the Theatre of War

Absztrakt

Az országvédelmi céloknak alárendelt erdőtelepítés komplex szempontrendszer mentén valósul meg. Az erdészeti szakmai célokon túl, az erdő- és fasortelepítés nagymértékben növelheti egy nyílt terület védelmi szerepét. Manőverutak rejtése, rejtekhelyek és drónvédelmi fedezékek kialakítása válik lehetségessé. A fák gyökérzete talajszerkezet-stabilizáló hatású, ami a nehéztechnika mozgatásánál alapvető fontosságú. Előrelátást igényel a megfelelő fafajok kiválasztása is, ahol figyelembe veszik az elérhető maximális fatörzsátmérőt. Az ipari erdők kitermelőút-hálózata ideális esetben illeszkedik a védelmi tervekhez. Ezek karbantartása az erdőgazdálkodó, a földtulajdonos és a Honvédség közös ügye kell hogy legyen.

Kulcsszavak: hadszíntér-előkészítés, fasor, sártenger, harckocsi, infrastruktúra

[1] Magyar Agrár- és Élettudományi Egyetem Szent István Biztonságkutató Központ, Gödöllő, e-mail: halasz.andras@uni-mate.hu
[2] Magyar Agrár- és Élettudományi Egyetem Állattenyésztési Tudományok Intézet, e-mail: nagy.dominik@uni-mate.hu
[3] Magyar Agrár- és Élettudományi Egyetem Környezettudományi Intézet Öntözési és Vízgazdálkodási Kutatóközpont, Szarvas, e-mail: jancso.mihaly@uni-mate.hu
[4] Nemzeti Éghajlat- és Tájkutatási Központ, Karcag, e-mail: varga.krisztina@uni-mate.hu
[5] E-mail: csillabojte1990@gmail.com
[6] Nemzeti Éghajlat- és Tájkutatási Központ, Karcag, e-mail: csizi.istvan@uni-mate.hu
[7] A szerzők köszönetüket fejezik ki az MH Klapka György 1. Páncélosdandár és a Szent István Biztonságkutató Központ illetékes tagjai felé.

Abstract

Homeland security includes complex preparational measures in forestry. Beyond fundamental forest management objectives, complete afforestation and shelterbelt forests can greatly enhance the defensive potential of exposed areas. Forest plantation can be used to hide manoeuvre tracks, provide concealment and anti-drone cover. The root system of trees has a soil-stabilising effect, which is essential for moving heavy armoury. Foresight is also required in the selection of appropriate tree species, focusing on the maximum trunk diameter available. The logging road network in forest plantations should match with defence plans. Dirt road maintenance should be a joint responsibility of the forest manager, landowner and the Hungarian Defence Forces.

Keywords: preparation theatre of war, shelterbelt forest, mud season, tank, infrastructure

Bevezetés

Az ukrán–orosz konfliktus felhívta a figyelmet a mezőgazdasági területek infrastruktúrájának egyedi vonásaira, illetve az egyes elemek taktikai alkalmazására. Egy szántóföldön végzett tarlóhántás után, de még szántás előtt is, teljesen más talajmechanikai tulajdonságai vannak a talajnak, mint szántást és magágy-előkészítést követően. A talaj fizikai terhelhetőségét a talajnedvesség is befolyásolja, ami csapadékos időszakban szinte lehetetlenné teszi a nehéztechnika, de olykor még a kisebb járművek manőverezési képességeit is. A sártenger (распутица, ejtsd: raszputyica)[8] már a 21. századot megelőző korokban is komoly nehézséget okozott, amikor az utazók szembesültek a járhatatlan utakkal (Marco Polo, karavánok). A képlékeny, mocsaras, szerkezet nélküli talajokon való mozgás ma is nagy kihívást jelent.[9]

A harckocsizó parancsnoki kiképzés során külön hangsúlyt fektetnek a tereptani[10] és növényföldrajzi szempontokra.[11] A szántóföldeket szegélyező fasorok és erdősávok nemcsak rejtekhelyként szolgálhatnak, de szélfogó hatásuk miatt, a ködösítésnél vagy ballisztikai számításoknál is fontos tényezők.[12] Mezőgazdasági szempontból a fák elsődleges szerepe a szélerózió csökkentése (lásd porvihar), illetve a mikroklíma javítása[13] (a fasor magasságának 20-szoros távolságáig) (1. ábra).

[8] Lásd: https://hu.wikipedia.org/wiki/Raszputyica
[9] Wonder World 2018.
[10] WT Info 2018.
[11] Felkai 2022.
[12] Kovács 2004.
[13] Varga et al. 2024.

1. ábra: Széláramlás mérsékelten szélátereszető (A) és erősen zárt, sűrű (B) mezővédő erdősávon át, illetve fölött
Forrás: Caborn 1957

Az I–II. világháborús tapasztalatok már nagyon korán rámutattak, hogy a modern, motorizált járművekkel való közlekedés gyökeresen más kihívások elé állítja mind a harcoló, mind a támogató alakulatokat. A burkolatlan utak, a szűk, keskeny ívek, a hidak terhelhetősége egy sor problémát vetettek fel, ami korábban a málhás állatokkal vagy kerékpárral viszonylag (!) könnyen megoldható volt (lásd hegyi tüzérség, kerékpáros zászlóalj). A védvonalak, fedezékek létesítésénél is lényeges a növényzet, mint ahogy arról Damó Elemér nyá. ezredes igen szemléletesen beszámol:[14]

„Rögtön a tűzkeresztségünk napján tapasztaltuk az erdő egyik sajátosságát. Füves, sima terepen a meredeken érkező akna repeszei a becsapódás helyétől ferdén, fölfelé röpülnek. Ha tehát az ember a suhogást hallva villámgyorsan a földre veti magát, közeli becsapódást is megúszhat. Erdőben azonban a fába ütköző akna repeszei úgy szóródhatnak lefele, mint az 1. világháborús srapnelszilánkok. A 24. ezred parancsnoka a közvetlen közelünkben így sebesült meg. Ezért erdőben az állások azon részei fölé, ahol állandó jelleggel emberek tartózkodtak, gömbfából készített szilánkernyőket építettünk és azokat földdel takartuk."

A fák közötti mozgást megnehezíti, ha nem ipari ültetvényben, hanem természetes örökerdőben kell manőverezni például harckocsival. Mezey[15] leírja, hogy a gumi- és kókuszfaültetvényekben viszonylag könnyű volt mozogni a II. világháború során, hiszen ezeket a területeket gondosan megtisztították az aljnövényzettől, és szabályos közönként voltak beültetve. A fasorok között a látási viszonyok is jók, épp ezért az ott mozgó katonák elég feltűnők. Fedezékként leginkább a fák szolgálnak, de precíziós páncéltörő eszközökkel szemben nem nyújtanak kellő védelmet.[16] A japánok Malájföldön főleg ezzel a típusú mezőgazdasági területtel találkoztak, és a britek is itt próbálták feltartóztatni őket (a műutakat és hidakat leszámítva). Cukornádültetvények

[14] Damó 2008.
[15] Mezey 2015.
[16] Malyasov 2023.

is lehetnek a területen, ilyenkor létrákat vittek magukkal, hogy leküzdjék a magas nádat, vagy fára másztak, hogy jobban lássák a terepet. Támadás során, mivel a nádon túlra nemigen lehet látni, ez nagyon jó hely az ellenség átkarolására és bekerítésére, és védelmi szempontból sem utolsó: az apróra vágott, drótra rögzített nád szögesdrótként vagy bukózsinórként is funkcionálhat.

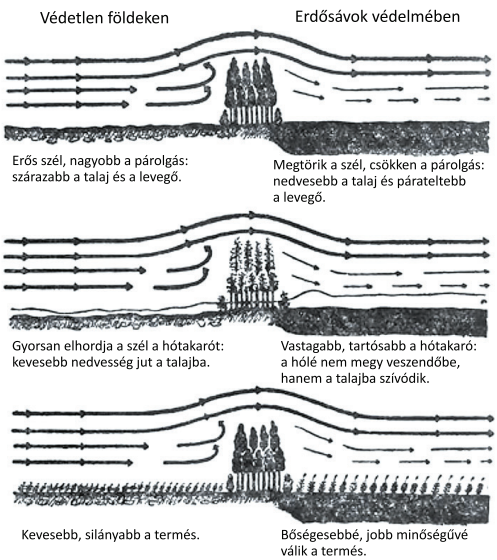
Rögtönzött manővereknél az erdőn való átvágás is felmerülhet, ami egy sor problémát és veszélyforrást jelenthet. A 30 centiméternél vastagabb törzsátmérőjű fák csak láncfűrésszel, tolólappal felszerelt harckocsival vagy erdészeti, bányászati eszközökkel távolíthatók el. Fokozottan figyelni kell az 50 centiméternél magasabb tuskókra és egy esetleges tarvágás vagy tüzérségi tűz után kidőlt fatörzsekre. Ezeken felakadhat a lánctalpas jármű, illetve sérülhetnek a támkerekek. Esetenként egy-egy beszorult fatörzs a lánctalp ledobását is okozhatja. Hóborításnál hatványozottan érvényesek az előbbi szempontok.

A fás szárú növényzet 1944-ben is komoly akadályt jelentett Normandiában. A németek kihasználták a sövényfalak biztosította rejtést, és komoly állásokat építettek ki ezek mentén. A kisebb járműveknek, olykor még a gyalogságnak is, áthatolhatatlan akadályt jelentettek. Az amerikai M4 Sherman, közepes harckocsi, 30 tonnás tömege ellenére is gyakran elakadt a fasorokban, sövényfalakban. A Culin-féle vágóasztal („Rhino-agyar") a harckocsik elején egy rögtönzött megoldás volt, de gyorsan elterjedt. A hatékony áttöréshez nagy sebességre volt szükség, ami időnként boruláshoz vezetett (2. ábra).

2. ábra: Culin-féle vágóasztal és egy felborult Sherman harckocsi
Forrás: National Museum United States Army [é. n.]

Fasorok telepítése

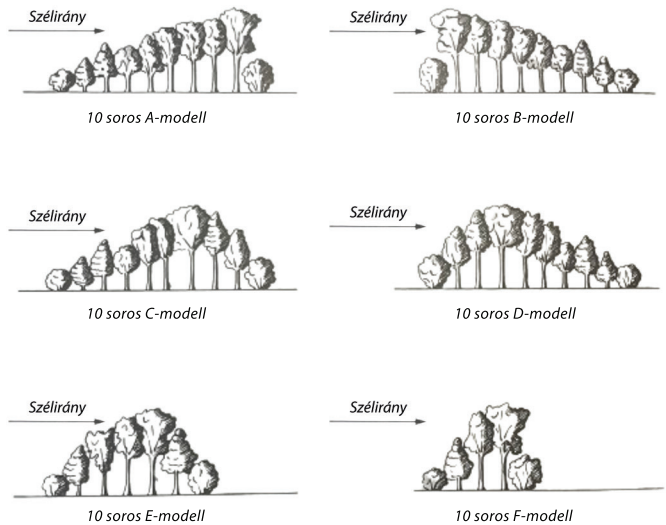
A fasorok telepítését már évszázadok óta alkalmazzák, elsősorban alföldi, lapályterületeken, ahol az erős szél nehezíti a mezőgazdasági munkát. Oroszi[17] feleleveníti a viljamszi mezővédő erdősávkomplexum[18] gondolatát, ahol a növénytermesztés három ágazatát, az erdészetet, a rétgazdálkodást és szántóföldi növénytermesztést egy egészként kell tekinteni. A rét évelő füvei megjavítják a talajszerkezetet, amelyet felszántva a növénytermesztés kitűnő termőtalajt kap. Viljamsz rendszerében nagy feladatot szánt az erdősávoknak is; azok védő hatása mellett folyik a mezőgazdasági művelés (3. ábra).



3. ábra: A viljamszi mezővédő erdősáv szélsebességre és páratartalomra gyakorolt hatása Toma (1953) nyomán
Forrás: Oroszi 2014

Kötött, sziklás talajon különösen nehéz a faültetés, ezért olyan alternatív megoldások is szóba kerülhetnek, mint az ipari robbanóanyaggal való talajlazítás.[19] Fafajtól függően 2,5–4 méteres sortáv javasolt, amivel számolni kell egy esetleges védelmi művelet esetén. Az idősebb elegyes erdőknél, fasoroknál nem feltétlenül vannak szabályos sorok, ami komolyan befolyásolja a szélsebességet és légnyomásviszonyokat (4. ábra).

[17] Oroszi 2014.
[18] Toma 1953.
[19] Lukács 2002.



4. ábra: Woodruff és Zingg (1953) szélcsatorna-vizsgálatai védősávmodellekkel Caborn (1957) nyomán
Forrás: Magyar 1961

Mezővédő erdősávok szerepe a tűzvezetésben

Az orosz–ukrán háború Donyeck-medencei összecsapásai újra rávilágítottak a „látni, de nem látszani" alapvetésre. A nagy kiterjedésű több száz hektáros szántóföldi táblák a kora tavaszi időszakban szinte járhatatlanok a nehéz járművek és harceszközök számára. Ezt abban az esetben fokozottan figyelembe kell venni, ha műszaki zárás céljából puhasávként[20] szántották a területet, a támadás várható irányával párhuzamosan. A rejtekhelyek, ideiglenes fedezékek is korlátozottak. Ilyen körülmények között az öntöző- és belvízelvezető árkok egyszerre számítanak harckocsifedezéknek[21] és komolyabb, leküzdendő akadálynak.[22] Az árkok, rézsűk terelő hatását figyelembe veszik harctéri előkészületnél, előre telepített torlaszokkal, terelőzárakkal.[23]

A csatornahálózattal együtt járnak az azokat szegélyező, esetenként megerősített földutak és erdősávok.[24] A földutak nyilvánvaló előnye a manőverezésben[25] kétségen felül áll, azonban a harctéri tapasztalatok[26] rámutattak, hogy a sok járműből álló konvojok olyan szinten rongálhatják a földutakat, hogy a később érkező járművek elakadhatnak. Talajmechanikailag vizsgált megfigyelés, hogy egy gyepesített

[20] Bodrogi 1997.
[21] Soltész 1949.
[22] Szabó–Kovács–Kovács 2014.
[23] Kim et al. 2022.
[24] Kosztka 2010.
[25] Kovácsházy 2018.
[26] Számvéber 2001.

és erdősávval is rendelkező földút szárazabb tud maradni még komolyabb esőzés után is,[27] ami megkönnyíti a manőverezést.[28] A szélvédett oldalon könnyebben melegszik fel a talaj. Nyáron ezért a párolgás itt gyorsabban megy végbe, viszont télen nagyobb mennyiségű hó és olvadékvíz gyűlhet ugyanitt össze. A domborzati viszonyokat figyelembe véve a nagyobb mennyiségű felszíni vizet/belvizet ideiglenes tárolótavakba érdemes gyűjteni. Ezeknek a tározóknak, tervezett módon, kettős célja lehet a felszíni vízszabályozáson túlmenően. Országvédelmi, területi előkészítés esetén szerepük lehet műszaki vagy karbantartó állomások kiszolgálásában (lásd hadiutak, hadtáp) vagy katasztrófavédelmi (tűzoltás), vízellátó kitelepülések kiszolgálásában.

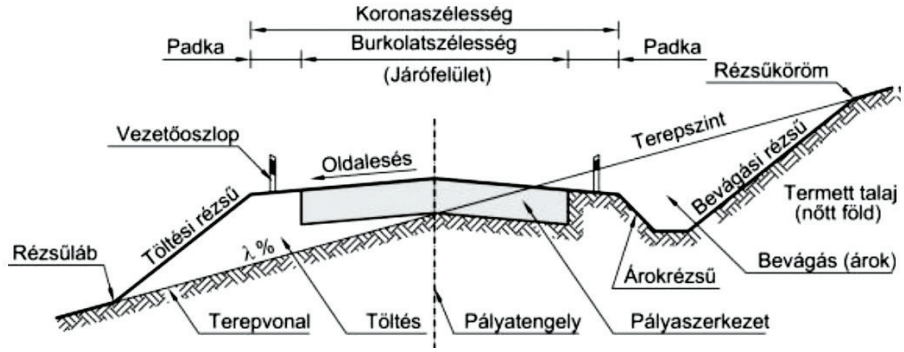
A lőtávolság pontos meghatározásánál fontos paraméter a szélsebesség és a páratartalom. Ezek nagymértékben változhatnak fasorok közelében, amivel számolni kell, főként indirekt irányzás vagy ködösítés esetén. Az erdősávok további előnye, hogy akadályozzák a nyílt, kitett táj könnyű beláthatóságát, így elrejthetnek nagyobb létszámú egységeket is. Az orosz–ukrán konfliktus tapasztalatai rámutattak, hogy a fasorok fontos szerepet játszanak a városok körüli harcokban is. Lövészárokrendszereket rejthetnek, amelyeket városi-harcászati megoldásokkal igyekeznek megtisztítani a támadók (lásd épületharcászat).

Földutak

A földutak, dűlőutak, makadámutak, erdészeti utak és mezsgyék létesítése magával vonja a tulajdoni kérdéseket is.[29] Többnyire helyrajzi számmal rendelkeznek, amely alapján a tulajdonos beazonosítható. A mai fragmentált birtokviszonyoknál azonban nehezen lehet kötelezni a földhasználót (bérlőt) a karbantartásra. Sok esetben az út nem is ott van, ahol a földméréskor kijelölték, illetve ott is kanyarog, ahol szántónak, gyepnek kellene lennie. Ezek a „vándorló" utak a legváratlanabb helyeken is megjelenhetnek, például vízmosásban, nyiladékokban. A legtöbb esetben a domborzati viszonyok és a növényzet határozza meg a vonalvezetést. Így szorosan összefügg egy-egy erdőtömb, fasor vagy csatorna a földúthálózattal.

A talajút szerkezete függ az igénybevételtől, az elérhető építőanyagoktól és a pénzügyi forrásoktól is. Ideális esetben többrétegű, megfelelő alappal, teherhordó réteggel és vízelvezetéssel épülnek. A gyakorlatban, egy-egy talajút-felújítási program keretében, egy gréderezésen és hengerezésen kívül más nem nagyon történik karbantartás címén. A geotextil használata sokat jelent egy homokos területen kialakított út stabilizálásánál. Ennél tartósabb megoldások is léteznek, ahol már komolyabb tervezés szükséges (5. ábra). Itt felhívnánk a figyelmet a rézsű és padka kialakítására, aminek lehet jelentősége egy esetleges útelhagyási vagy útkeresztező manőver esetén (meredek lejtés, kiemelkedő padka).[30]

[27] Kocsis et al. 1992.
[28] Ogorkiewicz 1991.
[29] Herpay–Pankotai 1963.
[30] Kovácsházy 2012.



5. ábra: Az útpálya részei
Forrás: Kosztka 2010

Az útmenti fasorok telepítési tervénél figyelembe kell venni az útburkolat-szélességet, amely manőverút esetén 3,5 méter, után- és hátraszállítási utak esetén 10 méter is lehet.[31] Szélesebb utaknál magasabb fákra van szükség, hogy megfelelő rejtést biztosítsanak.

Telepítés

Az erdősávok telepítésénél az adott termőhely tulajdonságai az irányadók. A lejtésviszonyok, a tengerszint feletti magasság, a fekvés és a domborzat nagyban befolyásolja a telepítés hosszú távú sikerét. Homokon jellemzők az akác-, nyárfa- és az erdeifenyő-telepítések. Meghatározó a talaj kémhatása (pH) is, ahol hazai sajátosságként a meszes talajok jelenthetnek problémát. A turkesztáni szil *(Ulmus pumila Celer)* a szikes talajokhoz is alkalmazkodott fafaj, de cserjeként is használható például sövénytelepítésnél.

A kiválasztott fajokat telepítési terv alapján kell elrendezni, ahol már figyelembe vesznek kettős felhasználású *(dual use)* célokat is. Így a tő- és sortávolság, a növényápolás mellett figyelembe vesznek egyedi paramétereket is, mint például a nyomtáv vagy harckocsi-lövegcső hossz.[32] Az országvédelmi, illetve hadszíntér-előkészítés során kiemelt fontosságú a manőverutak állapota és teherbírása, esetenként rejtése is. A sudaras lombkoronájú jegenyenyár *(Populus nigra 'Italica')* vagy az oszlop típusú, nyírségi fehér akác *(Robinia pseudoacacia)* lombozata elfogadható álcázást nyújt az utak fölött (6. ábra).

[31] Fazekas 1985.
[32] Kurcz et al. 2020.

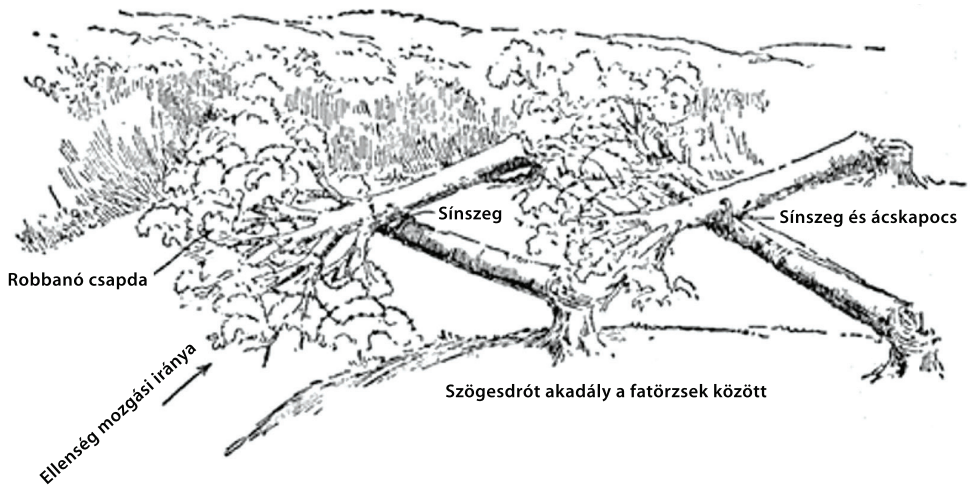
6. ábra: Jegenyenyársor hadiút mentén

Forrás: http://pctrs.network.hu/clubpicture/1/2/7/8/_/jegenyesor__sajnos_mar_csak_fenykepjegenye_1278367_6704_n.jpg

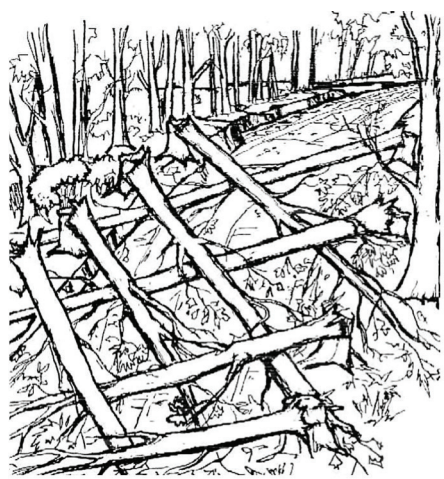
A tervezés során figyelembe kell venni az uralkodó szélirányt is. Ennek az erózióvédelem mellett fontos szerepe lehet ködösítésnél, ballisztikai számításoknál, és a talaj száradásának sebességét is befolyásolja. Ez utóbbi paraméter szenzoros követése[33] is szükséges lehet. Az elmúlt évek tapasztalatai alapján elmondható, hogy a drónok elleni védekezés alapvető fontosságú. A harcjárművek ideiglenes rejtéséhez szükséges valamilyen épített fedezék, amely kombinálva van megfelelő növényzeti takarással. A drónvédelmi lugasok is jó szolgálatot tehetnek egy esetleges művelet során.

Az erdősávok telepítésénél a kitermelő- vagy manőverutak elhelyezkedését, rendszerét is át kell gondolni. Nehezen leküzdhető műszaki akadály létesíthető az erdősített területen, a már a rómaiak által is alkalmazott döntött fatorlasz (abatisz) megoldással (7. ábra). Ennek lényege, hogy a hazai elvek alapján, legalább 100 m hosszan és minimum 30 m mélységben, az érkező járművek irányára 45 fokos szögben fákat döntenek az útra. A fatörzsek egymást keresztezik, és nincsenek teljesen leválasztva a tönkökről (8. ábra). A fatönk magassága 1-2 m. Az akadály leküzdése tovább nehezíthető, ha a fatörzseket szögesdróttal kötik össze, esetenként aláaknázzák.[34]

[33] *SoilScout talajfelderítő* [é. n.].
[34] Matsimus 2020.



7. ábra: Döntött fatorlasz alkalmazása gyalogság, kerekes járművek és harckocsik mozgásának akadályozására
Forrás: HM Government Military 1940



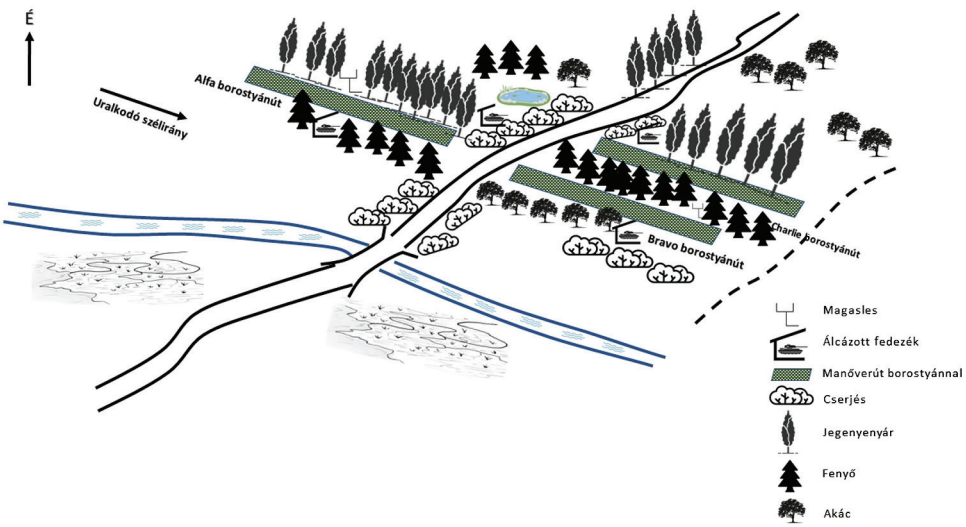
8. ábra: Döntött fatorlasz műszaki zár átlapolt fatörzsekkel és fatönkhöz kapcsolva
Forrás: Chisholm 1911

Javaslat

A hadszíntér-előkészítés, illetve országvédelmi előkészületek során figyelembe veszik a harckocsik paramétereit, hogy maximálisan ki lehessen használni azok tűzerejét. Az épített fedezékek, tüzelőállások, rejtekhelyek, kellően sűrű növényzettel kombinálva

komoly taktikai előnyt biztosíthatnak.[35] E cikk írói javaslatot fogalmaznak meg egy országvédelmi szempontokat is figyelembe vevő mezővédő erdősávrendszer-telepítési tervre (9. ábra). A vázolt terv bemutatja a megvédendő műút mentén létesítendő fasorok elhelyezését annak érdekében, hogy a manőverutak rejtését hatékonyan segítsék. Figyelembe veszi az uralkodó szélirányt, amely hatást gyakorol a ballisztikai számításokra, a ködösítés hatékonyságára és a talajnedvesség változására is.[36] Az útelhagyási manővereket segítheti az előre tervezett UAV-védett beállók (⛺) létesítése. Ezek a fedezékek álcázhatók esetenként borostyánnal, vadrózsával. Az előre kiépített tüzelőállások és harckocsifedezékek az előre kidolgozott harceljárásoknak megfelelően építhetők ki. Csapadékos időjárás esetén a manőverutaknál taktikai előnyt jelenthet azok kedvező nedvességtartalma, köszönhetően az előrelátóan telepített növényzetnek. További kutatást igényel, hogy a kúszó-indás növényzet (borostyán) mennyiben korlátozza a lánctalpas járművek mozgását.

A földutakra vonatkozó, sokszor bizonytalan helyrajziszám-kiosztás (szolgalmi jog miatti viták) nehezíti az utak és az erdősávok ápolását, karbantartását. A magángazdálkodókat, erdőtársulásokat is célszerű bevonni az ápolási munkákba, mivel a jó állapotban tartott manőverutak megléte közös érdek.



9. ábra: Példa telepítési terv

Megjegyzés: A fasorok között húzódó utak stabilizálása és rejtése történhet borostyánnal (Hedera helix)

Forrás: a szerzők szerkesztése

[35] Kunz 2022.

[36] Rásó et al. 2017.

Felhasznált irodalom

Bodrogi László (1997): A műszaki zárás jelene és jövője. *Műszaki Katonai Közlöny,* 7(2), 16–24.

Caborn, J. M. (1957): *Shelterbelts and Microclimate.* Forestry Commission Bulletin, No. 29. Edinburgh: Her Majesty's Stationery Office.

Chisholm, Hugh szerk. (1911): „Abatis". *Encyclopædia Britannica.* 1 (11th ed.). Cambridge University Press.

Damó Elemér (2008): Utászi harctéri tapasztalatok. *Műszaki Katonai Közlöny,* 18(1–4), 175–306.

Fazekas Imre (1985): Hadiutak jellemzése hadműveletben és harcban, azok igénybevételének néhány elvi kérdései, kiemelten a csapathadtáp tagozatban. *Hadtápbiztosítás,* 18(4), 90–97.

Felkai Ádám (2022): Miért kisebbek és könnyebbek az orosz tankok, mint a nyugatiak? *Rakéta.hu,* 2022. március 3. Online: https://raketa.hu/miert-kisebbek-es-konnyebbek-az-orosz-tankok-mint-a-nyugatiak

Herpay Imre – Pankotai Gábor (1963): *Mezőgazdasági útépítés.* Budapest: Mezőgazdasági Kiadó.

HM Government Military (1940): *Training Pamphlet No. 30 Part III: Obstacles.* London: The War Office.

Kocsis István – Daróczi Sándor – Czinkóczky Mihály – Nagy Imre (1992): Nedvességmérős penetrométer gyepen. In Vinczeffy Imre (szerk.): *Természetes állattartás 2.* Debrecen: Debreceni Agrártudományi Egyetem, 75–83.

Kovács Zoltán (2004): *A műszakizár-rendszer felépítésének lehetőségei a Magyar Honvédségben a NATO-elvek és a vonatkozó nemzetközi egyezmények tükrében.* PhD-értekezés. Budapest: Zrínyi Miklós Nemzetvédelmi Egyetem.

Kovácsházy Miklós (2012): A harckocsik önmentésének kérdései. *Hadmérnök,* 7(2), 65–76.

Kovácsházy Miklós (2018): A páncélozott harcjárművek vizsgálata, összehasonlítása és értékelése a mozgékonyság tükrében című doktori (PhD) értekezés bemutatása. *Katonai Logisztika,* 26(1–2), 108–132. Online: https://doi.org/10.30583/2018/1-2/108

Kosztka Miklós (2009): *Erdészeti útépítés.* Budapest: Országos Erdészeti Egyesület.

Kosztka Miklós (2010): *Mezőgazdasági infrastruktúra alapjai 4. A mezőgazdasági utak keresztmetszete.* Székesfehérvár: Nyugat-magyarországi Egyetem Geoinformatikai Kar.

Kukjoo, Kim – Jeon, Youngjoon – Park, Young-Jun – Park, Sangwoo (2022): Sustainable Anti-Tank Obstacle System Applying Civil–Military Cooperation in Highly Urbanized Areas. *Sustainability,* 14(19). Online: https://doi.org/10.3390/su141912715

Kunz, Adam (2022): Selected Problems of Contemporary Tactics of Tank Subunits. *Scientific Journal of the Military University of Land Forces,* 54(4), 508–523. Online: https://doi.org/10.5604/01.3001.0016.1761

Kurcz Kristóf – Vég Róbert – Hegedűs Ernő (2020): A Leopard 2 harckocsicsalád és a Magyar Honvédség 2A4 és 2A7+ típusváltozatai I. rész. *Haditechnika,* 54(5) 2–7. Online: https://doi.org/10.23713/HT.54.5.01

Lukács László (2002): Robbantás a mezőgazdaságban. *Műszaki Katonai Közlöny,* 12(3–4), 89–94.
Malyasov, Dylan (2023): Ukrainian Artillery Blows Up Russian T-80BV Tank Hiding Between Trees. *Defence Blog,* 2023. január 12. Online: https://defence-blog.com/ukrainian-artillery-blow-up-russian-t-80bv-tank-hiding-between-trees/
Magyar Pál (1961): *Alföldfásítás.* II. kötet: Alkalmazott rész. Budapest: Akadémiai Kiadó.
Matsimus (2020): What is the Abatis field fortification? *YouTube,* 2020. november 8. Online: www.youtube.com/watch?v=8zEQtIM7G7k&t=621s
Mezey Csaba Bence (2015): A felkelő Nap a dzsungelben – esőerdei harcok Malajziában 1941–42. In Ferwagner Péter Ákos (szerk.): *Tehetségek a történettudomány szolgálatában II. Történelem szakos hallgatók diákköri dolgozatai.* Szeged: SZTE BTK, 77–97.
National Museum United States Army [é. n.]: *Rhino Tank.* Online: https://www.thenmusa.org/armyinnovations/rhinotank/
Ogorkiewicz, Richard M. (1991): Soil-Vehicle Mechanics. In *Technology of Tanks I–II.* Coulsdon: Jane's Information Group, 341–356.
Oroszi Sándor (2014): Fasorok és erdősávok. *Magyar Mezőgazdaság,* 2014. szeptember 5. Online: https://magyarmezogazdasag.hu/2014/09/05/fasorok-es-erdosavok
Rásó János – Honfy Veronika – Keserű Zsolt (2017): Mezővédő erdősávok talajnedvességre és mikroklimatikus jellemzőkre gyakorolt hatásainak vizsgálata a nagykun-hajdúháti erdőgazdasági tájban. In Kamandiné Végh Ágnes – Nagy Angelika (szerk.): *Alföldi Erdőkért Egyesület Kutatói Nap: Tudományos Eredmények a Gyakorlatban.* Kecskemét: Alföldi Erdőkért Egyesület, 191–198.
SoilScout talajfelderítő [é. n.]. Online: www.gpscom.hu/termek/soilscout-talajfelderito
Soltész László (1949): Természetes harckocsi-akadályok leküzdése. *A Páncélos: katonai folyóirat,* 1.
Szabó Sándor – Kovács Tibor – Kovács Zoltán (2014): Az utak, területek akadálymentesítése I. *Műszaki Katonai Közlöny,* 24(3), 15–29.
Számvéber Norbert (2001): A szovjet csapatok harcászata és vezetése 1945 elején. In *Konrad 3. Páncéloscsata Budapestért 1945.* Budapest: Paktum Nyomdaipari Társaság, 90–94.
Toma Ádám (1953): *Erdőgazdaság és természetátalakító fásítás Magyarországon.* Budapest: Művelt Nép Könyvkiadó.
Varga, Krisztina – Csízi, István – Halász, András (2024): Determination of Pasture Comfort Climate Index between Forest and Open Grassland for Livestock Grazing. *Journal of Rangeland Science,* 14(4), 1–10. Online: https://doi.org/10.57647/j.jrs.2024.1404.26
Woodruff, N.P. – Zingg, A. W. (1953): Wind-Tunnel Studies on Shelterbelt Models. *Journal of Forestry,* 51(3), 173–178.
Wonder World (2018): SHERP ATV – The Ultimate All Terrain Vehicle. *YouTube,* 2018. december 18. Online: www.youtube.com/watch?v=luU6M4TZn7g&t=35s
WT Info (2018): Oroszország megváltoztatta a harckocsik harctéri taktikáját. *WT Info,* 2018. július 12. Online: https://wtinfo.hu/2018/07/12/oroszorszag-megvaltoztatta-a-harckocsik-harcteri-taktikajat/

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG

19. évfolyam (2024) 4. szám 19–29.
DOI: 10.32567/hm.2024.4.2

Kátai-Urbán Maxim,[1] Szakál Béla,[2] Cimer Zsolt[3]

Az oltóvízszennyezés elleni védekezés üzemeltetői biztonságszervezési gyakorlatának felmérése logisztikai raktárakban

Assessment of Operator's Safety Management Practices for the Firewater Pollution Prevention in Logistics Warehouses

Absztrakt

A szennyezett oltóvíz, amely veszélyes anyagok tárolására szolgáló logisztikai létesítményekben bekövetkező ipari balesetek, tüzek oltásánál keletkezik, a felszíni és felszín alatti vizekbe vagy a talajba kerülve jelentős környezeti károkat okozhat. Jelen tanulmányban a szerzők felmérik az oltóvízszennyezés elleni védekezés üzemeltetői biztonságszervezési gyakorlatának tapasztalatait a hazai logisztikai raktárak körében.

Kulcsszavak: ipari balesetek, környezeti károk, veszélyes üzemek, oltóvízszennyezés megelőzése, Magyarország

[1] Osztályvezető, Semmelweis Egyetem Biztonságtechnikai Igazgatóság Biztonságszervezési Osztály, e-mail: katai.urban.maxim@semmelweis.hu
[2] Oktató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: szakalbela1827@freemail.hu
[3] Dékán, Nemzeti Közszolgálati Egyetem Víztudományi Kar, e-mail: cimer.zsolt@uni-nke.hu

Abstract

The industrial accidents occurred at logistics facilities used for the storage of dangerous goods, as a result of contaminated water generated during fires can cause major environment consequences to the surface and ground waters. In this study, the authors assess the experience of operators' safety organisation practices of logistics warehouses in the field of firewater pollution prevention.

Keywords: industrial accidents, environmental impact, dangerous establishment, firewater pollution prevention, Hungary

Bevezetés

A veszélyes anyagok tárolásának kockázatai hazánkban, csakúgy, mint külföldön, az ilyen tevékenységet folytató üzemekben, a küszöbérték alatti, alapanyag, félkész és késztermékeket tároló létesítményekben jelentkeznek. Ezek lehetnek veszélyes anyagot gyártó, feldolgozó, vagy főként kereskedelmi célú tárolók, veszélyesáru-logisztikai raktárbázisok.[4]

A veszélyes anyagok logisztikai raktározását folytató létesítményekben esetlegesen bekövetkező ipari balesetek a tűzoltásnál keletkezett szennyezett oltóvíz által a felszíni és felszín alatti vizekbe vagy a talajba kerülve jelentős környezeti károkat okozhatnak. A környezeti károsodás a veszélyes anyagok és az oltóvíz környezetbe kerülését követően tapasztalható a nem üzemszerű kibocsátás eredményeként. A veszélyes anyag gyártása és tárolása során bekövetkező események a környezetre és az egészségre káros anyagok kibocsátásával kezdődnek, amelynek következménye lehet a tűz vagy a robbanás.[5]

Az oltóvízszennyezés megelőzésének legfontosabb eleme az oltóvízfelfogó és -tároló létesítmények tervezése és telepítése. A műszaki követelményeknek a hazai logisztikai szektorban célszerűen egyenszilárdságúnak kell lenniük. Ugyanez az egységesség szükséges a meglévő és az új fejlesztések vonatkozásában is, ahol kiemelt szerepe van a tűzmegelőzési szabályozásnak, az üzemeltetői vízkárelhárítási rendszernek és nemkülönben az automatikus működésű tűzjelző- és tűzoltó-berendezéseknek.

A felszíni és felszín alatti vizek közvetlen szennyezésével járó környezeti károk megelőzése az ipari tevékenységek vonatkozásában elsősorban környezetbiztonsági kérdés.[6] Az ipari balesetek környezeti hatásainak megelőzésével kapcsolatos nemzetközi szabályok előírása többek között az ENSZ Európai Gazdasági Bizottsága keretében létrejött, *az ipari balesetek országhatáron túli hatásairól szóló egyezmény* (Ipari Baleseti Egyezmény) alapján történik. Az Ipari Baleseti Egyezményt az Európai Unió területén a tagországok az Európai Parlament és a Tanács *veszélyes anyagokkal kapcsolatos súlyos balesetek veszélyének kezeléséről, valamint a 96/82/EK tanácsi irányelv módosításáról*

[4] Cimer–Szakál 2015.
[5] Kátai-Urbán et al. 2024.
[6] Földi–Padányi 2021.

és későbbi hatályon kívül helyezéséről szóló 2012/18/EU irányelve alapján hajtják végre (Seveso III. irányelv). A nemzetközi és az európai uniós szabályozás teljesítése ennek megfelelően Magyarországon *a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény* (a továbbiakban: Kat.) IV. fejezete és a végrehajtását szolgáló, *a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről szóló 219/2011. (X. 20.) Korm. rendelet* (a továbbiakban: Vhr.) előírásai alapján valósul meg. A két jogszabályt együtt alkalmazva „súlyos baleseti szabályozásként" jelölhetjük. A környezeti katasztrófahelyzetek felszámolása a védekezés valamennyi időszakában a vezetés és az irányítás szoros összehangolását, az üzemeltetők hatóságokkal való együttműködését, továbbá komplex infokommunikációs rendszer létrehozását és működtetését igényli.[7]

A jogi szabályozással összhangban a szennyezett oltóvíz kezelésének kérdéseivel elsősorban azoknál a logisztikai raktáraknál kell foglalkozni, ahol veszélyes áru és veszélyes anyagok tárolása is történhet. Az oltóvízszennyezés elleni védekezés jellemző üzemeltetői gyakorlatának vizsgálatához ezért a Kat. IV. fejezet hatálya alá tartozó raktárak vonatkozó gyakorlatának feltárása érdekében végeztek a szerzők elemző munkát.

A kutatómunka a logisztikai raktárak üzemeltetői által rendelkezésre bocsátott biztonsági jelentések, biztonsági elemzések, belső védelmi tervek és súlyoskár-esemény-elhárítási tervek tartalmának vizsgálatára irányult elsősorban. A vizsgálat kiemelt célja volt meghatározni, hogy a raktárak tervezése, építése és üzemeltetése során milyen üzemeltetői intézkedéseket foganatosítottak az esetlegesen keletkező szennyezett oltóvíz által okozott környezeti veszélyek megelőzésére és kezelésére.

Oltóvízszennyezés-megelőzési raktárkövetelmények elemzése

A veszélyesáru-logisztikai raktárak létesítésénél és használatánál a különböző biztonsági szakterületek jogi szabályozásban rögzített követelményeit kell figyelembe venni, amelyek elsősorban a munkavédelmi, a tűzvédelmi, a robbanás elleni védelmi és a környezetvédelmi szabályozásokban jelennek meg.[8]

A tűzmegelőzési célokat szolgáló intézkedések a szerzők véleménye szerint a legfontosabbak, mivel, ha nincs tűz, akkor nincs oltóvíz-felhasználás sem. A nemzetközi szabályozás[9] elemzése alapján a veszélyesáru-raktárak esetében azok létesítését és használatát szabályozó úgynevezett „Tűzvédelmi Koncepció" fontosságát érdemes kiemelni. A koncepció elsősorban a feldolgozóipari gyártó, feldolgozó és tároló létesítmények tűzmegelőzési létesítési és használati szabályaira vonatkozik. A tűzvédelmi koncepció kialakítása kapcsán megelőzési és védelmi, illetve passzív és aktív védelmi intézkedéseket különböztet meg.

A Tűzvédelmi Koncepció egyik fontos eleme a helyi tűzoltó erők vonulási ideje, mivel ezen a ponton kapcsolódik a megelőző és mentő tűzvédelem a leginkább

[7] Farkas 2016.
[8] Kátai-Urbán et al. 2023.
[9] UN Economic Commission for Europe 2019.

meghatározó módon.[10] A kiemelt kockázatot jelentő létesítményekkel és a speciális veszélyforrásokkal, mint például a logisztikai raktárakkal kapcsolatos esetlegesen bekövetkező jelentős tűzesetekre külön fel kell készülni.[11]

A veszélyesáru-logisztikai raktárak esetében a tűz kialakulásának kockázata igen magas, mivel a tűzterhelés meglehetősen nagy, és ideális feltételek vannak a tűz terjedéséhez. A raktárak tűzmegelőzése ezért rendkívül fontos. A raktárakban alkalmazott tűzmegelőzési intézkedések általában a következők: az épület tűzvédelmi követelmények szerinti kialakítása, a gyújtóforrások minimalizálása, automatikus tűzjelző rendszerek és tűzoltó-berendezések alkalmazása, valamint szervezési intézkedések bevezetése.

A tűz bekövetkezésének kockázatát növelő hatások közé tartozik a gyújtóforrások és az egyes vegyi anyagok egymással való veszélyes kölcsönhatásainak lehetősége.[12] Ennek megfelelő védelmi intézkedések az alábbiak lehetnek: a gyújtóforrások elkerülése és kizárása, a tűz átterjedésének megakadályozása (kisebb méretű különálló tűzszakaszok kialakítása), valamint az egymással veszélyes reakcióba lépő anyagok együvé tárolási tilalma érdekében szükséges intézkedések. Egy raktárrészen belül a tűz terjedése biztonsági berendezésekkel (oltóberendezés) és a nem éghető tűzvédelmi osztályú anyagoknak az éghető anyagok közé való betárolásával akadályozható meg.

A tűzgátló falak és ajtók a két raktárrész közötti tűzterjedést előzhetik meg. A tűz felismerése és az ellene való küzdelem szervezeti és építészeti intézkedésekkel (körbejárhatóság), a létesítményi tűzoltóság bevetésével, valamint automatikus tűzjelző rendszer és automatikus oltóberendezések (sprinkler, gázzal vagy habbal oltó) segítségével történik.

A tűz során keletkező égéstermékek környezetbe való kikerülése a szellőztető rendszeren keresztül és ezáltal annak a környezetre gyakorolt hatása megakadályozható a hő- és füstelvezető berendezések lezárásával, valamint a szellőztetés leállításával. A talaj és a vizek védelmére – megfelelő kapacitású – termék és oltóvíz felfogására szolgáló medencék és tárolók alkalmazása szolgál.

Robbanás elleni védelem esetében alapvetően olyan eljárásokat kell megkülönböztetni, amelyek a robbanásveszélyes koncentráció kialakulását megakadályozzák, továbbá a robbanásveszélyes gáz- (gőz, köd) vagy levegőelegyek berobbanását meggátolják. A robbanásveszélyes koncentráció éghető gázok vagy folyadékok (esetleg porok) általi, raktárban való kialakulását megfelelően zárt és tömör csomagolások választásával, biztonságos és stabil felállítással, felügyeleti intézkedésekkel, valamint egy hatékony és teljes körű szellőztető rendszerrel lehet megakadályozni.[13]

A gyújtóforrások kialakulásának kizárásához meg kell akadályozni a forró felületek kialakulását. Figyelembe kell venni az öngyulladásra hajlamos anyagokkal, mint például a piroforos anyagokkal való együvé tárolási tilalom bevezetését is.

A műszaki megoldások közül javasolt megvalósítani a robbanásbiztos kivitelű elektromos berendezések és megfelelő tűzállóságú vezetékek beépítését, az előírások szerinti villámvédelem biztosítását, valamint az elektrosztatikus feltöltődés keletkezésének megakadályozását be- és kirakodáskor. A raktár üzemeltetésekor a használati

[10] Varga 2018a.
[11] Varga 2018b.
[12] Érces–Vass 2018.
[13] Sárosi 2006.

szabályok szerint ezenfelül a dohányzást és a nyílt láng használatát szervezetileg meg kell akadályozni.

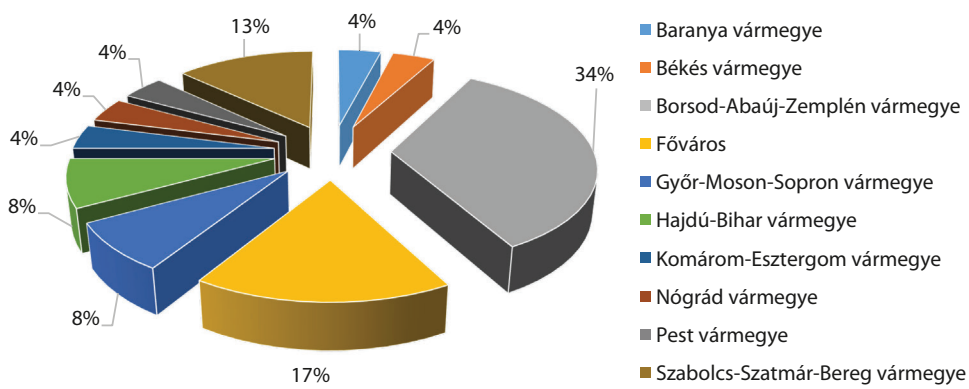
A környezetvédelem talaj- és vízvédelmi szabályait legfőképpen a következő intézkedések által lehet biztosítani: csomagolások tömítése, biztonságos felállítás; a hő- és füstelvezetők bezárása, szellőztetés leállítása a termékek kiömlésekor; illetve a termék- és oltóvízfelfogó és -elvezető rendszer alkalmazása.

További biztonságszervezési feladatot jelent a kémiai ártalmakkal kapcsolatos üzemeltetői munkavédelmi kötelezettségek előírása is.[14]

A veszélyesanyag-raktárakban előforduló tüzek megelőzésének egyik fontos eszköze a tűzjelző rendszerek kialakítása és üzemeltetése, amelyek a tűzoltó rendszerekkel együtt betöltik a rendeltetésüket. A vagyonvédelmi rendszerek is a helyszíni fizikai védelmi rendszer részét képezik.[15] A technológiai fejlődés eredményeként a vagyon- és munkavédelmi feladatok ellátására kiépített kamerarendszerek is előtérbe kerültek.[16] Ez utóbbi rendszerek kettős alkalmazására vonatkozóan további kutatások végezhetők. Hasonlóan fontos gyakorlati tanulságokat sajátíthatunk el a tűzvédelmi hatósági tevékenység fejlesztése szempontjából a rendezvénybiztonság rendészeti kérdéseinek kezelése során is.[17]

Az oltóvízszennyezés-megelőzési üzemeltetői gyakorlat felmérése

Az oltóvízszennyezés elleni védekezés üzemeltetői gyakorlatának felmérése érdekében végzett vizsgálatok összesen 24 logisztikai telephelyre terjedtek ki, amelyek területi eloszlását az 1. ábra szemlélteti.



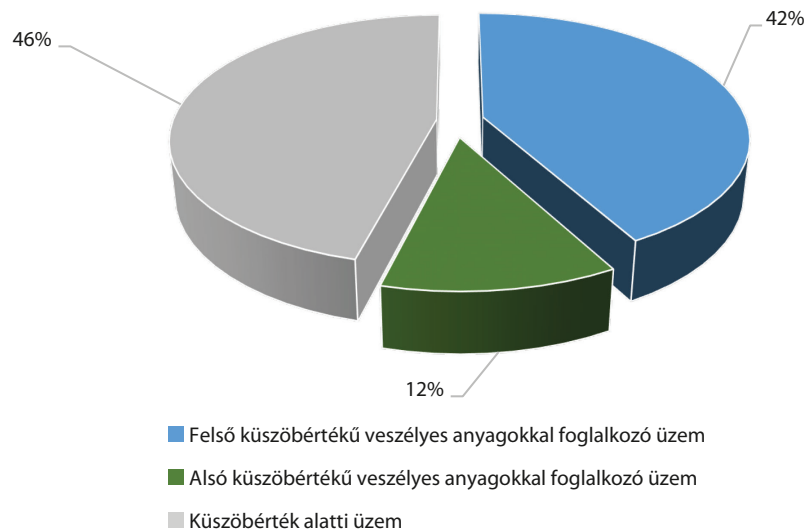
1. ábra: A vizsgált raktárak vármegyei eloszlása
Forrás: a szerzők szerkesztése

[14] Nagy 2023.
[15] Tóth 2024.
[16] Tóth 2016.
[17] Nagy-Tóth 2020.

Az 1. ábra adatai alapján megállapítható, hogy a hazai logisztikai ingatlanpiac jelentős mértékben Budapest-központúvá vált, mivel a raktárkapacitás túlnyomó része a fővárosban és a közvetlen környékén, Pest vármegyében van. A vizsgált raktárak több mint 50%-a a fővárosban és Pest vármegyében üzemel. Az érintett raktárak esetében a Kat. IV. fejezet szerinti üzemeltetői státusz megállapítása – vagyis a veszélyes üzemek azonosítása – kiemelt és összetett üzemeltetői és szakértői feladatot jelent.

A logisztikai tevékenységek esetében nem tudjuk állandó készlet alapján az üzemazonosítást lefolytatni, mivel a tárolt áruk típusa és mennyisége a piaci igényeknek és kereskedelmi változásoknak az okán is folyamatosan változhat. A telephely Kat. IV. fejezet szerinti státuszának üzemeltetői tervezésénél figyelembe kell venni, hogy az üzemeltető csak az iparbiztonsági hatósági engedély birtokában folytathat veszélyes tevékenységet.

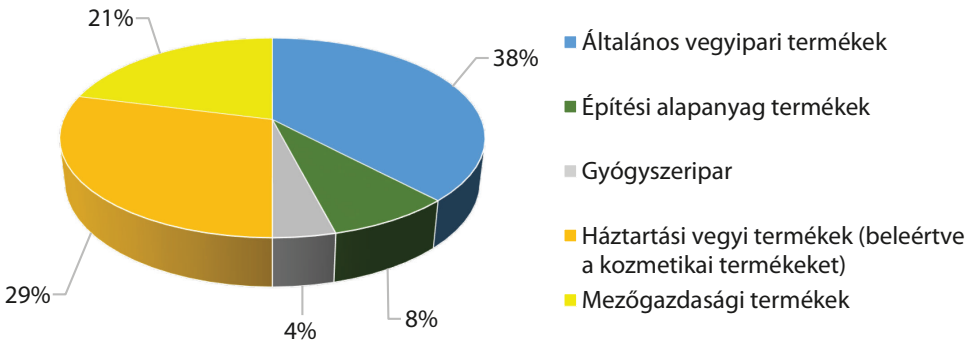
A vizsgált logisztikai raktárak esetében a Kat. IV. fejezet szerinti üzemeltetői státusz megoszlását a 2. ábra szemlélteti részletesen.



2. ábra: A vizsgált raktárak státuszainak megoszlása
Forrás: a szerzők szerkesztése

A 2. ábra adatai alapján megállapítható, hogy a vizsgált raktárak 42%-a felső küszöbértékű veszélyes anyagokkal foglalkozó üzem, 46%-a pedig küszöbérték alatti üzem. A viszonylag alacsony számú alsó küszöbértékű veszélyes anyagokkal foglalkozó üzemraktár 12%-os arányának oka az lehet, hogy a felső küszöbértékű veszélyes anyagokkal foglalkozó üzemekkel és az alsó küszöbértékű veszélyes anyagokkal foglalkozó üzemekkel szemben támasztott követelmény között üzemeltetői szemszögből nem számottevő a különbség.

A vizsgált raktárakban tárolt termékek kategóriáit a 3. ábra mutatja be.



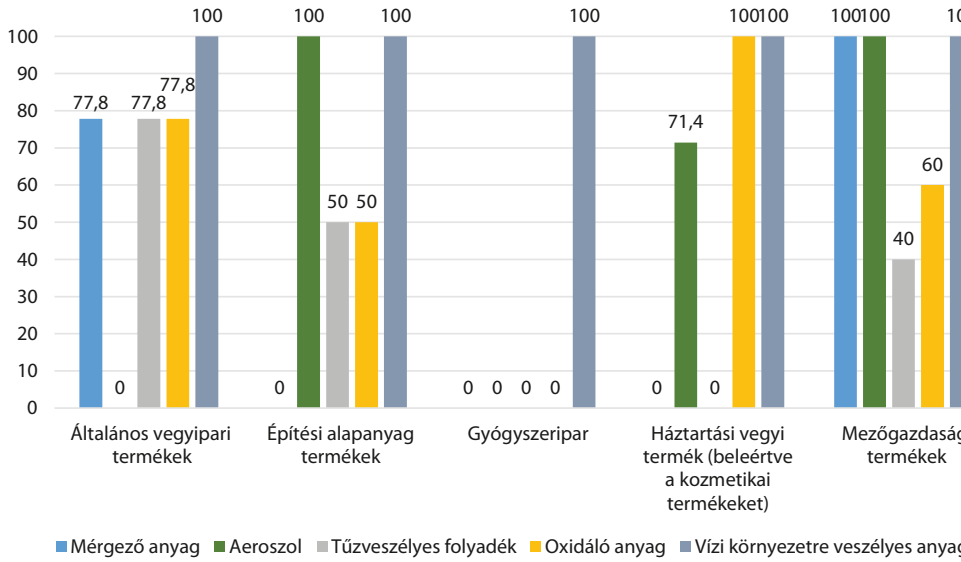
3. ábra: A vizsgált raktárakban tárolt termékek kategóriái
Forrás: a szerzők szerkesztése

A raktárakban tárolt anyagok értékelése alapján az alábbi megállapítások tehetők:

- A vizsgált raktárak 38%-ában általános vegyipari termék tárolása történik, jellemzően folyadék vagy szilárd halmazállapotban. A tárhelyeken jellemzően legnagyobb kiszerelési egység az IBC, ugyanakkor hordó, kanna, zsákos, valamint kisebb küldeménydarabos kiszerelési egységekben is történhet a termékek tárolása.
- A háztartási vegyi termékek, beleértve a kozmetikai termékek raktáraiban – a vizsgált raktárak 29%-a – folyadék, szilárd halmazállapotú termékek és aeroszolok tárolása történik. A tárolásra jellemző, hogy a kiszerelési egységek mérete általában nem haladja meg a 10 litert.
- A mezőgazdasági termékek raktáraiban – amelyek a vizsgált raktárak 21%-át teszik ki – folyadék vagy szilárd halmazállapotú termékek tárolása történik. A legnagyobb kiszerelési egység a big-bag csomagolás, de a csomagolóeszközök teljes – IBC-től a kisebb küldeménydarabos kiszerelési egységekig – spektruma megtalálható ezekben a raktárakban.
- Az építési alapanyag termékek főként folyadék, szilárd halmazállapotban és aeroszol formában vannak jelen. A legnagyobb kiszerelési egység jellemzően az IBC, de hasonlóan a többi raktárhoz, a csomagolóeszközök teljes spektruma előfordulhat a tárolás során.

A gyógyszeripari termékek esetében a késztermék tároló raktárak vizsgálata jelentette a fő célkitűzést.

Az iparbiztonsági engedélyezési eljáráshoz szükséges a raktárakban tárolt termékek besorolása a Vhr. 1. mellékletében megadott módszertan előírásainak megfelelően. Az elemzés eredményeit a 4. ábra foglalja össze. Az esetlegesen jelentős környezeti károsodáshoz vezető szennyezett oltóvíz keletkezése szempontjából releváns az egészségi vagy a környezeti veszélyekkel járó veszélyes anyagok jelenléte. Vízi környezetre veszélyes anyag az összes vizsgált raktárban, a mérgező anyag a mezőgazdasági termékeket, valamint az általános vegyipari termékeket tároló raktárakban van általánosságban jelen.



4. ábra: A vizsgált raktárakban tárolt veszélyes anyagok besorolása

Forrás: a szerzők szerkesztése

A környezeti hatásvizsgálati és az egységes környezethasználati engedélyezési eljárásról szóló 314/2005. (XII. 25.) Korm. rendelet 3. melléklete alapján 30 ezer m^3 össztároló-kapacitástól a vegyi termék tárolása a környezetvédelmi hatóság előzetes vizsgálatban hozott döntésétől függően, az 1. melléklete alapján pedig 200 ezer tonna össztároló-kapacitástól környezeti hatásvizsgálat köteles tevékenység.

A vizsgált raktárak vonatkozásában 4 esetben a 200 ezer tonna, 2 esetben pedig a 30 ezer m^3 össztároló-kapacitás feltétel teljesül. Ugyanakkor a rendelkezésre álló információk szerint csak 1 raktár esetében készült környezeti hatásvizsgálat. Az ok elsősorban arra vezethető vissza, hogy a környezeti hatásvizsgálati rendeleti feltételrendszernek megfelelő raktárak dedikáltan nem vegyi termékek tárolására lettek létrehozva, ezáltal a tárolási tevékenységi funkció váltása már csak az üzemeltetés fázisában jelent meg.

A raktárak műszaki kialakítását tekintve megállapítható, hogy a jogi szabályozási kötelezettségnek – elsősorban a tűzvédelmi megelőző előírások – maradéktalanul az összes vizsgált raktár megfelel. A vizsgált raktárak mindegyikében ipari padló létesült és a megfelelő vízzáróság biztosított. Ezért a létesítményen belül keletkező és benn maradt szennyezett oltóvíz esetében a jelentős mértékű átszivárgás kizárható.

A raktárak 92%-ában (22) az esetlegesen keletkező tűz korai észlelése céljából tűzjelző, 37,5%-ában (9) automatikus tűzoltórendszert alakítottak ki: egy raktárban automatikus gázzal oltó, két raktárban automatikus habbal oltó, a többi raktárban vizes sprinkler tűzoltórendszer üzemel.

A létesítmény kármentőként – dokumentáltan és méretezett módon – való kialakítása 21%-ban (5) valósult meg. Az automatikus oltórendszerek alkalmazása

és a kármentőként való kialakítása között azonban nincs teljes összhang, ugyanis két olyan raktár is kármentőként létesült, ahol nem épült ki oltórendszer.

A veszélyelemzés során a vizsgált raktárak egyike sem azonosította eseménysorként a szennyezett oltóvíz keletkezésének a lehetőségét. Ugyanakkor a súlyos balesetek elleni védekezési szabályozásnak köszönhetően a környezetterheléssel járó eseménysorok kezelésére vonatkozó súlyos baleseti intézkedési sorokat – beleértve a megelőző műszaki megoldások és védelmi infrastruktúra számbavétele – bemutatta.

Megállapítható továbbá, hogy a vizsgált raktárak egyikéből sem kerülhet közvetlen módon a szennyezett oltóvíz a felszíni vízfolyásba, a csapadékelvezető rendszer kiszakaszolása megoldott. Ugyanakkor a szennyezett oltóvíz talajba kerülésének kizárása, illetve a kijutott szennyező anyag minimalizálása kizárólag egy raktár esetében valósulhat meg.

Befejezés

A rendkívüli események környezeti következményeinek felszámolása napjainkban egyre nagyobb kihívás elé állítja az üzemeltetői biztonságszervezési rendszer egészét.

Az oltóvízszennyezés a környezeti hatásait közép- és hosszú távon fejti ki, amelyek mentesítése jelentős feladat elé állítja az üzemeltetőt és a hatóságokat egyaránt. A logisztikai raktárakban bekövetkező súlyos baleseti eseménysorok vizsgálata alapján megállapítható, hogy az eseménysorok a következők lehetnek: a mérgező veszélyes anyag kibocsátása által keletkező mérgező hatás, a tűzveszélyes anyagok kibocsátását követő tűz kialakulása és a tűzben keletkező mérgező égéstermékek általi levegő- és vízszennyezés.

A veszélyes anyagok kibocsátása és esetlegesen bekövetkező tüzek a szennyezett oltóvizek kapcsán hozzájárulhatnak a felszíni és felszín alatti vizek szennyezéséhez, aminek megakadályozása a szennyezett oltóvíz felfogásával és ártalmatlanításával oldható meg. Figyelemmel a külföldön már jól bevált szakmai gyakorlatra megállapítható, hogy a külföldi gyakorlat hazai alkalmazása, a raktárak korszerű felszereltsége, a modern tűzmegelőzési rendszerek, valamint a szennyezéscsökkentés területén jelentős különbségek vannak.

A nemzetközi követelményeknek megfelelő raktárlétesítmények biztonsági szintje – a korszerű raktárlétesítési és -üzemeltetési kötelezettségeknek köszönhetően – többségében meghaladja több, már üzemelő raktárlétesítményét. A több évtizede létesített csarnoképületekből funkcióváltással kialakított veszélyes anyagot és árut tároló logisztikai raktárakat sajnálatos módon még nem a korszerű veszélyesanyag-tárolási szabályozás szerint alakították ki.

A hazai iparbiztonsági felsőoktatásban, valamint a hagyományos iparbiztonsági tevékenységi területeken képzést kell biztosítani az ipari környezetszennyezés megelőzése területén.[18]

[18] Vass 2017.

Felhasznált irodalom

Cimer, Zsolt – Szakál, Béla (2015): Control of Major-Accidents Involving Dangerous Substances Relating to Combined Terminals. *Science for Population Protection,* 7(1), 1–11. Online: www.population-protection.eu/prilohy/casopis/eng/21/98.pdf

Érces Gergő – Vass Gyula (2018): Veszélyes ipari üzemek tűzvédelme ipari üzemek fenntartható tűzbiztonságának fejlesztési lehetőségei a komplex tűzvédelem tekintetében. *Műszaki Katonai Közlöny,* 28(4), 2–22.

Farkas Tibor (2016): A katasztrófavédelmi és válságkezelési tevékenységek általános elemzése az irányítás és az infokommunikációs támogatás tükrében. *Hadmérnök,* 11(3), 135–148.

Földi László – Padányi József (2021): Környezetbiztonsági kihívások a haderők számára. In Gőcze István (szerk.): *Az egyházak és a katonai erők előtt álló kihívások, az együttműködés lehetőségei.* Budapest: Magyarországi Egyházak Ökumenikus Tanácsa, 49–60.

Kátai-Urbán Maxim – Érces Gergő – Vass Gyula – Cimer Zsolt (2024): Veszélyes áru raktározás oltóvízszennyezéssel kapcsolatos tűzvédelmi követelményeinek értékelése. *Polgári Védelmi Szemle,* 16(Különszám), 312–323.

Kátai-Urbán Maxim – Mesics Zoltán – Pimper László – Cimer Zsolt (2023): Veszélyes anyagok tárolása a logisztikai raktárakban. *Műszaki Katonai Közlöny,* 33(3), 63–75. Online: https://doi.org/10.32562/mkk.2023.3.6

Nagy Rudolf (2023): A munkahelyi kémiai ártalmak és az iparbiztonság. *Polgári Védelmi Szemle,* 15(19), 261–279.

Nagy-Tóth, Nikolett Ágnes (2020): Thoughts About the Current Issues of Sports Policing. *Belügyi Szemle,* 68(3), 77–93. Online: https://doi.org/10.38146/BSZ.SPEC.2020.3.6

Sárosi György (2006): *Veszélyes áru raktárlogisztika – korszerű követelmények.* Budapest: CompLex.

Tóth Levente (2024): Hazai közterületi videomegfigyelő rendszerek állapota és fejlesztési lehetőségei. *Belügyi Szemle,* 72(1), 243–265. Online: https://doi.org/10.38146/BSZ.2024.2.4

Tóth, Levente (2016): Limitation in the Application of High Resolution Image Sensors. *National Security Review,* 2. 108–122.

UN Economic Commission for Europe (2019): *Safety Guidelines and Good Practices for the Management and Retention of Firefighting Water.* Geneva: United Nations. Online: www.unece.org/fileadmin/DAM/env/documents/2019/TEIA/Publication/1914406E_web_high_res.pdf

Varga Ferenc (2018a): A mentő tűzvédelem optimális diszlokációjának területi és szervezeti szintű kidolgozása, a meghatározó szempontok elemzése. *Műszaki Katonai Közlöny,* 28(3), 15–40.

Varga, Ferenc (2018b): Internationale Erfahrungen der freiwilligen Feuerwehren. *Hadmérnök,* 13(KÖFOP-különszám), 160–176.

Vass, Gyula (2017): Industrial Safety Training in Disaster Management Higher Education in Hungary. *Pozhary i Chrezvychajnye Situacii: Predotvrashenie Likvidacia,* 8(2), 80–84. Online: https://doi.org/10.25257/FE.2017.2.80-84

Jogi források

2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról
314/2005. (XII. 25.) Korm. rendelet a környezeti hatásvizsgálati és az egységes környezethasználati engedélyezési eljárásról
219/2011. (X. 20.) Korm. rendelet a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről
UN Economic Commission for Europe. Convention on Transboundary Effects of Industrial Accidents, Helsinki, 17 March 1992
Directive 2012/18/EU of the European Parliament and of the Council of 4 July 2012 on the control of major-accident hazards involving dangerous substances, amending and subsequently repealing Council Directive 96/82/EC

HADMÉRNÖK
VÉDELEMGAZDASÁG

19. évfolyam (2024) 4. szám 31–41.
DOI: 10.32567/hm.2024.4.3

Aadi Rajesh[1]

The Dawn of a New Chapter in India–Africa Relationship

The Opportunities and Challenges of Indian Defence Exports to Africa

Abstract

India has come a long way from being a defence importer to becoming a major defence exporter. As India seeks to increase its own geopolitical clout and counterbalance the growing Chinese influence in the developing world, it is adapting to new avenues for partnership with the developing world. With a wide range of indigenous, cost-effective, and reliable weapons, India is seeking to forge a new chapter of defence export in its relations with various developing countries, especially Africa.
While some instances of successes have given a boost to the Indian defence industry and increased its exports, challenges remain with competition from China, Russia, Turkey, the United States, and other Western nations in a growing African defence import market. The paper will explore the recent developments in the Indian defence industry, the trend of current exports to Africa, and the potential opportunities and challenges.

Keywords: India, Africa, South-South Relations, Arms Trade, India–China competition

Introduction

For an independent nation, access to modern military equipment is essential to maintain its internal and external security and protect its sovereignty. This is especially true for India, which has ambitions to become a great power but faces strong

[1] Ludovika University of Public Service, e-mail: nayyaraadi@gmail.com

regional challenges from military powers such as China and Pakistan. But despite having global ambitions, the Indian defence industry has largely underperformed with cost overruns and delays for many of its projects.[2]

The history of the modern defence industry in India can be traced back to the pre-independence era, during the British colonisation of India. During the British era, there was a minimal emphasis on creating a local defence industry. While some Ordinance factory Boards were created to serve British interests in the region, they contributed little to local indigenous innovation and military-industrial development.[3]

Post-Independence, India inherited a weak military-industrial base set up by the British, and due to lack of technological skills, financial stress, and various other factors, the defence industry remained neglected by the Indian state.[4]

For much of its modern independent history, India was a defence importer and used imports to compensate for its small and struggling local defence industry. Furthermore, due to state led industrial policy in India, the private sector remained weak and its participation in the defence industry remained limited.[5]

Following the Sino-Indian War of 1962, there was a realisation in the development of and procurement of modern military equipment. However, due to Pakistan's alliance with the West,[6] and India's policy to remain independent from the cold war politics with its support of the Non-Aligned Movement (NAM), defence exports from western states remained limited.[7]

Furthermore, due to India's nuclear tests of 1974, the United States and various Western nations imposed sanctions on India, preventing it's access to sensitive technologies, materials and equipment. Notable, the former Soviet Union did not impose sanctions on India after its nuclear tests, which strengthened India–Soviet partnership and defence cooperation.[8]

Due to this, the former Soviet Union became a major supplier of defence equipment to India and provided defence equipment at concessional rates with opportunities for domestic licence production. Some major exports by the former Soviet Union include MiG-21 Fighter Jets and T-72 Main Battle Tanks, both of which were also co-produced in India under licenced production.[9]

2 Atif 2024.
3 Roy 2003.
4 Cohen–Dasgupta 2012.
5 Behera 2023.
6 Thapliyal 1998.
7 Hasan 1963.
8 Sengupta–Ponangi 2022.
9 Cohen–Dasgupta 2012.

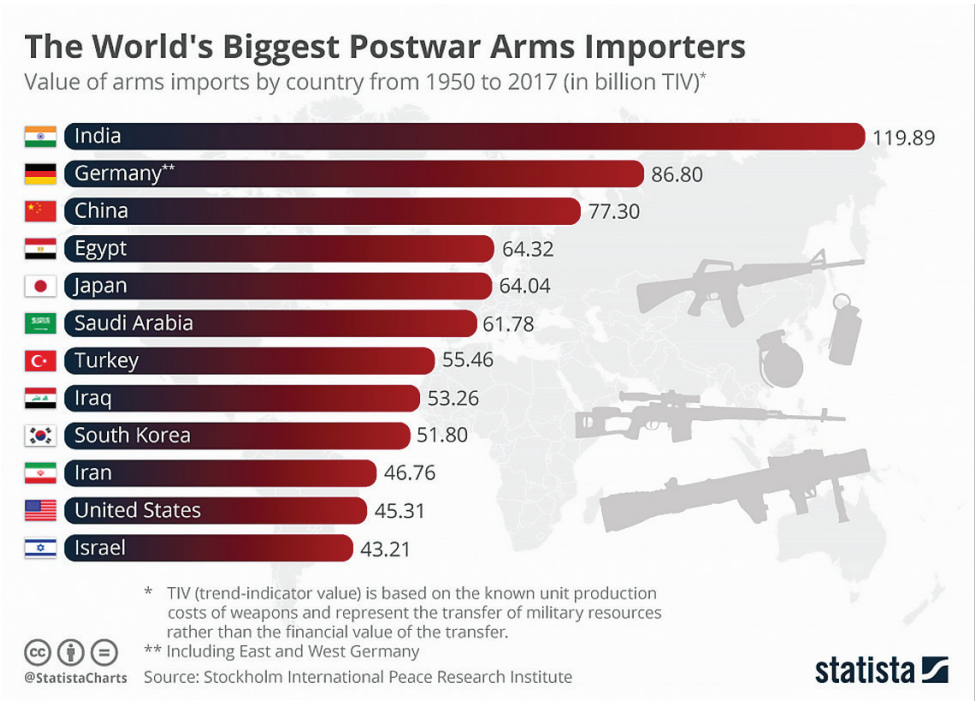


Figure 1: The world's biggest post-war arms importers
Source: www.statista.com/chart/13211/the-worlds-biggest-postwar-arms-importers/

Beyond military support from the former Soviet Union, India also invested in its own indigenous nuclear and space technologies and focused especially on the Integrated Guided Missile Development Programme. The success of this programme assisted India in creating a formidable missile arsenal such as the "AGNI" nuclear capable intercontinental ballistic missiles, "Akash" Surface-to-Air Missile and "Nag" Anti-Tank Guided Missile. India has developed an advance set of missles, with range enceeding 10,000 km (Figure 2).[10]

Although in the 1970s and the 1980s, beyond the success of the missile program, India did attempt to produce various important naval assets such as INS Shakti-Class Frigates, INS Arihant, which is a strategic nuclear strike class submarine, and fighter jets such as the Light Combat Aircraft (LCA) Tejas, the projects faced mixed successes and decades of delay as in the case of LCA Tejas, which got inducted in the Indian Airforce in the 2000s after decades of delay and cost overruns.[11]

With the collapse of the former Soviet Union, India faced severe challenges with maintaining the defence supply chain and transfer of technology and looked for other partners for its domestic needs and started to invest further on home grown alternatives for its military needs.

[10] Behera 2023.
[11] Behera 2023.

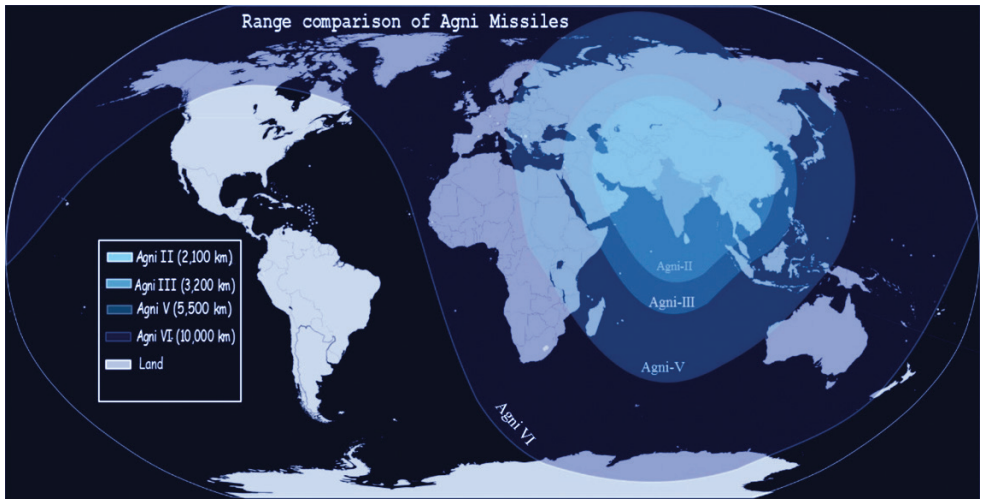


Figure 2: Range of AGNI missiles
Source: Editor8220, CC BY-SA 4.0, https://creativecommons.org/licenses/by-sa/4.0

Following the 1991 liberation in India, which accelerated Indian economic and industrial growth,[12] and the 2001 liberalisation of the defence sector, an emphasis was given on defence investments by the public sector and the liberalisation opened the defence sector for private companies.[13]

A major push for defence production in India and potential exports came following the 2014 election victory of Prime Minister (PM) Narendra Modi. PM Modi emphasised on the Make in India policy and decreasing India's dependence on defence imports. India also established two defence industrial corridors, in the states of Uttar Pradesh and Tamil Nadu.[14]

The privatisation of the defence sector and policies such as Make in India helped the country to reduce its dependence on defence imports which were declining by 33% from the years 2011–2015 to the years 2016–2020.[15]

In the decade since 2014, some major indigenous inductions to Indian defence exports included HAL Light Combat Aircraft (LCA) Tejas which is an indigenously developed 4th generation fighter jet, INS Vikrant, an indigenously developed aircraft career and INS Arihant, which is a nuclear power submarine.[16] India is also undergoing an extensive defence modernisation process with long term projects such as the Project-75 (India) for the Indian Navy[17] and a 5th generation stealth fighter jet "AMCA".[18]

12 BBC 2021.
13 Behera 2023.
14 Ministry of Defence 2024b.
15 Pandit 2021.
16 Ministry of Defence 2024b.
17 Ministry of Defence 2021.
18 Ministry of Defence 2022.

In 2018, the Indian government presented a plan to make India among the top 5 global defence producers and exporters and set an ambitious goal to increase defence export earnings to USD 5 billion.[19] In the year 2022–2023, defence exports by India reached a record USD 2.63 billion, 32% higher than in 2021–2022 and an increase of 31 times in the last 10 years.[20]

Figure 3: Indian Arihant Class Submarine
Source: Charlie Kumar, CC BY-SA 4.0, https://creativecommons.org/licenses/by-sa/4.0

Figure 4: LCA Tejas
Source: Venkat Mangudi, CC BY-SA 2.0 https://creativecommons.org/licenses/by-sa/2.0

[19] Likhachev 2024.
[20] Ministry of Defence 2024a.

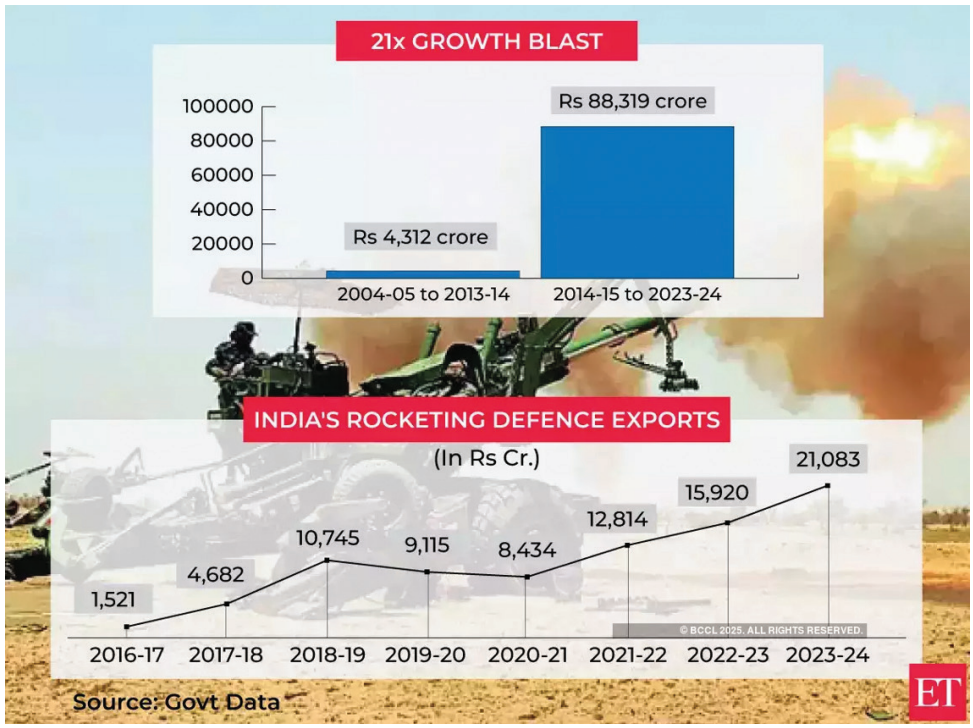


Figure 5: Growth of Indian Defence Exports in Rs Cr.
Source: The Economic Times 2024.

Some of the major public sector defence companies include Hindustan Aeronautics Limited (HAL), Mazagon Dock Shipbuilders Limited (MDL) and Defence Research and Development Organisation (DRDO), while the largest Indian private sector companies include Larsen & Toubro (L&T), Tata Advanced Systems Limited (TASL), Mahindra Defence Systems (MDS), Adani Defence and Aerospace and Ashok Leyland Defence.

India's long-term ability to continue developing its arms industry also stems from the possibilities to create defence research and developmental partnerships with various nations across the world. The globalisation of the armed industry has created opportunities for new players to enter the cutting edge of defence research and partnerships, opening up the defence industrial complex to weapons and technological development.[21]

[21] Devore 2013.

Defence trade in Africa

African needs for defence trade, particularly imports arise due to various factors, including immediate needs due to ongoing civil wars, terrorism threats, and other challenges such as lack of industrial and technological base for defence research and development, etc.

While some African countries, such as South Africa, Egypt and Nigeria etc. have a local defence production base, they face challenges with financial constraints, limited production capacity, or lack of cutting-edge technological research base. Hence most African countries have continued to be major importers of defence.[22] Traditionally, the former Soviet Union was the largest exporter of defence equipment and technologies to Africa and western countries such as the United States, France and Great Britain also were among the major defence exporters.[23] In the present era, Russia remains largest defence supplier of Africa, accounting for more than 40% of defence imports by Africa between 2016–2020, but new powers such as Turkey, India and especially China have also become major defence suppliers to the continent.[24] In sub-Saharan Africa, China has already replaced Russia as the largest supplier of arms and Chinese defence products account for 19% of all imports by the region.[25] Turkey has also become a major partner for defence exports to Africa and has supplied arms to countries such as Algeria and Morocco.[26]

For India, as its indigenous defence industry grew, it actively promoted its arms industry and looked for export partners for its products. Due to its competitive costs and active diplomacy, Indian defence exports to Africa soared in the past few decades. The main African importers of Indian defence include Seychelles, Mauritius and Mozambique.[27] Furthermore, to reach out to more African countries, India has appointed Defence advisors to its embassies in Ethiopia, Djibouti, Tanzania, Mozambique, Egypt, Ivory Coast, Kenya and various others.[28] Major Indian defence exports to Africa include Offshore Naval patrol vehicle, MCGS Barracuda, procured by Mauritius and the Fast Patrol Vessel PS Zoroaster procured by Seychelles and the Advanced Light Helicopter (ALH), HAL Dhruv procured by Mauritius.[29] While smaller countries such as Seychelles, Mauritius and Mozambique dominate Indian defence exports to Africa, India is trying to make major defence deals with other major African nations such as Egypt, Nigeria, DR Congo etc.[30] In 2023, India hosted representatives from 25 African nations for a military exercise and following the exercise showcased its indigenously developed defence equipment.[31] To finance defence exports, India could use the domestic EXIM bank and credit lines, which it has already done in the past

[22] Eureporter 2024.
[23] Eureporter 2024.
[24] Eureporter 2024.
[25] Arduino 2024.
[26] Dedet 2023.
[27] Singh 2024.
[28] Singh 2024.
[29] Singh 2024.
[30] Singh 2024.
[31] Ministry of Defence 2023.

to finance various projects in Africa. Another option could be to offer joint research and development ventures, which could help in capacity building and knowledge transfer.[32] Furthermore, many African nations have expressed interest in various high value, modern Indian defence equipment[33] such as the Arjun Mk1 tank, the Brahmos supersonic missile, the Akash Air defence system, and LCA Tejas fighter jets.

The Indian defence industry is expected to grow at 14% per annum between 2024 and 2030.[34] This boom in defence industrial growth will increase the potential for defence exports to Africa, which would open a new chapter in India–Africa relations.

Challenges

While India has shown considerable growth in its domestic defence industrial investments and produced some major cutting edge defence equipment, its defence exports to Africa remain small and face challenges from other major defence exports such as China, Russia, Turkey, the U.S. and other nations.[35] According to a SIPRI report, India remains a small player in the defence export industry.[36] Other African defence exporters, to such as China and Russia, have significant market shares, which could challenge India's defence export ambitions.

Figure 6: HAL Dhruv
Source: Pritishp333, CC BY-SA 3.0 via Wikimedia Commons

[32] Exim Bank India [s. a.].
[33] The Economic Times 2024.
[34] TOI Business Desk 2024.
[35] Eureporter 2024.
[36] Wezeman et al. 2024.

Furthermore, despite having a robust national defence industry and considerable investment in modern, cutting-edge equipment, India still remains among the largest importers of defence equipment globally.[37] India's current defence import-to-export ratio stands at 194:1, making it one of the largest arms importers in the world.[38] Therefore, the challenges to fulfil domestic demand might cause defence export delays, which could potentially become a major concern for future Indian defence buyers.

Notably, while India was actively seeking to export its indigenous fighter jet, LCA Tejas to Nigeria, the Nigerians choose the CAC/PAC JF-17 Thunder, which is a joint project by key Indian rivals, China and Pakistan. Moreover, Egypt, which is a key strategic partner of India also rejected the Indian fighter jet Tejas Mk1A, despite offers to set up production lines in Egypt by India.[39]

Conclusion

For most of its modern independent history, India has been one of the largest importers of defence equipment globally and has depended on defence procurement and technological transfers from various major powers to satisfy its domestic needs to compensate for its industrial inefficiencies.

As India is aiming to increase its geopolitical footprint and fulfil its growth ambitions, it is modernising its defence industry and is looking for export opportunities to expand its geopolitical interest and subsidise its investments through export earnings. However, due to intense competition from China and other countries, India faces challenges in its defence export ambitions to Africa. Furthermore, as India still remains among the largest defence importers globally, challenges remain for India's ability to export weapons and modern equipment to the developing world.

While the Indian defence industry remains small compared to the U.S., France, China or Russia due to lower procurement and operating costs, India has the potential to increase its defence exports to Africa and open a new chapter for India–African relations.

References

Airforce Technology (2021): Nigerian Air Force Inducts Three JF-17 Thunder Multirole Aircraft. *Airforce Technology,* 21 May 2021. Online: https://www.airforce-technology.com/news/nigerian-air-force-inducts-three-jf-17-thunder-multirole-aircraft/?cf-view

Arduino, Alessandro (2024): China's Expanding Security Footprint in Africa: From Arms Transfers to Military Cooperation. *ISPI,* 30 September 2024. Online: www.

[37] Cohen–Dasgupta 2012.
[38] Kumar–Mehta 2022
[39] Lionel 2024.

ispionline.it/en/publication/chinas-expanding-security-footprint-in-africa-from-arms-transfers-to-military-cooperation-184841

Atif, Noor U. H. (2024): The Weight of Ambition: India's Challenging Path to Modern Military Power. *Modern Diplomacy,* 4 December 2024. Online: https://moderndiplomacy.eu/2024/12/04/the-weight-of-ambition-indias-challenging-path-to-modern-military-power/

BBC (2021): 1991 Reforms: The Year that Transformed India. [Video]. *BBC,* 24 July 2021. Online: www.bbc.com/news/av/world-asia-india-57939341

Behera, Laxman K. (2023): *The State of India's Public Sector Defence Industry.* Observer Research Foundation Occasional Paper. Online: www.orfonline.org/research/the-state-of-indias-public-sector-defence-industry

Cohen, Stephen P. – Dasgupta, Sunil (2012): *Arming without Aiming: India's Military Modernization.* Brookings Institution Press.

Dedet, Joséphine (2023): Turkey's Arms Industry Takes Off in Africa. *The Africa Report,* 17 October 2023. Online: www.theafricareport.com/325048/turkeys-arms-industry-takes-off-in-africa/

Devore, Marc R. (2013): Arms Production in the Global Village: Options for Adapting to Defense-Industrial Globalization. *Security Studies,* 22(3), 532–572. Online: https://doi.org/10.1080/09636412.2013.816118

Eureporter (2024): Who Sells Arms in Africa? *Eureporter,* 3 August 2024. Online: www.eureporter.co/world/africa/2024/08/03/who-sells-arms-in-africa/

Exim Bank India [s. a.]: *Huge Scope for Greater Engagements between India and African Countries: India Exim Bank*. Online: www.eximbankindia.in/press-releases-details.aspx?pressid=439

Hasan, Zubeida (1963): Western Arms Aid to India. *Pakistan Horizon,* 16(4), 333–343. Online: www.jstor.org/stable/41392778

The Economic Times (2024): India Expands Strategic Presence; to Have Defence Attaches in More Countries in Africa, Asia. *The Economic Times,* 10 April 2024. Online: https://economictimes.indiatimes.com/news/defence/india-expands-strategic-presence-to-have-defence-attaches-in-more-countries-in-africa-asia/articleshow/109202546.cms?from=mdr

Kumar, A. – Mehta, M. (2022): Study on Identifying the Opportunities for Defence Exports Initiative towards Make in India Initiative. In Chandani, A. – Divekar, R. – Nayak, J. K. (eds.): *Achieving $5 Trillion Economy of India.* Springer Proceedings in Business and Economics. Springer, Singapore, 215–280. Online: https://doi.org/10.1007/978-981-16-7818-9_12

Likhachev, K. A. (2024): Key Aspects of India's Arms Export Policy amid Military-Industrial Complex Reform. *Vestnik RUDN International Relations,* 24(1), 92–106. Online: https://doi.org/10.22363/2313-0660-2024-24-1-92-106

Lionel, Ekene (2024): Nigeria Interested in Indian-Made Tejas Fighter Jet, but Sale is Highly Unlikely. *Military Africa,* 8 January 2024. Online: www.military.africa/2024/01/nigeria-interested-in-indian-made-tejas-fighter-jet-but-sale-is-highly-unlikely/#google_vignette

Ministry of Defence (2021): *MoD Issues RFP for Construction of Six P-75(I) Submarines for Indian Navy.* Press Release, 20 July 2021. Online: https://pib.gov.in/PressReleasePage.aspx?PRID=1737191

Ministry of Defence (2022): *Government Plans on AMCA*. 14 March 2022. Online: https://pib.gov.in/Pressreleaseshare.aspx?PRID=1805742

Ministry of Defence (2023): *India–Africa Joint Military Exercise* 'Afindex-23' Concluded at *Foreign Training Node, Aundh, Pune.* Press Release, 29 March 2023. www.pib.gov.in/PressReleasePage.aspx?PRID=1911766

Ministry of Defence (2024a): *Defence Exports Touch Record Rs 21,083 Crore in FY 2023–24, an Increase of 32.5% over Last Fiscal; Private Sector Contributes 60%, DPSUs – 40%*. Press Release, 1 April 2024. https://pib.gov.in/PressReleaseIframePage.aspx?PRID=2016818#:~:text=Defence%20exports%20have%20touched%20a,compared%20to%20FY%202013%2D14

Ministry of Defence (2024b): *Marching Towards Atmanirbharta: India's Defence Revolution.* Press Release, 29 October 2024. Online: https://pib.gov.in/PressReleasePage.aspx?PRID=2069090

Pandit, Rajat (2021): India's Weapon Imports Fell by 33% in Last Five Years but Remains World's Second-Largest Arms Importer. *The Times of India,* 16 March 2021. Online: https://timesofindia.indiatimes.com/india/indias-weapon-imports-fell-by-33-in-last-five-years-but-remains-worlds-second-largest-arms-importer/articleshow/81516403.cms

Roy, Kaushik (2003): Equipping Leviathan: Ordnance Factories of British India, 1859-1913. *War in History,* 10(4), 398–423. Online: https://doi.org/10.1191/0968344503wh278oa

Sengupta, Shayak – Ponangi, Rama T. (2022): Russia's Outsized Role in India's Nuclear Power Program. *The Diplomat,* 28 May 2022. Online: https://thediplomat.com/2022/05/russias-outsized-role-in-indias-nuclear-power-program/

Singh, Gurjit (2024): Atmanirbhar in Africa. *Gateway House,* 22 October 2024. Online: www.gatewayhouse.in/atmanirbhar-in-africa/#:~:text=The%20main%20African%20importers%20of,are%20based%20on%20Indian%20exports

Thapliyal, Sangeeta (1998): Indo-Pak Conflict and the Role of External Powers. *Strategic Analysis,* 22(7). Online: https://ciaotest.cc.columbia.edu/olj/sa/sa_98ths01.html

TOI Business Desk (2024): Indian Defence Industry Set for 14% CAGR Growth by 2030: Report. *The Times of India,* 8 September 2024. Online: https://timesofindia.indiatimes.com/business/india-business/indian-defence-industry-set-for-14-cagr-growth-by-2030-report/articleshow/113161269.cms#:~:text=NEW%20DELHI%3A%20The%20Indian%20defence,a%20sectoral%20report%20by%20Jefferies

Wezeman, Pieter D. – Djokic, Katarina – George, Mathew – Hussain, Zain – Wezeman, Siemon T. (2024): *Trends in International Arms Transfers, 2023*. Stockholm: SIPRI. Online: https://doi.org/10.55163/PBRP4239

HADMÉRNÖK
VÉDELEMINFORMATIKA

19. évfolyam (2024) 4. szám 43–59.
DOI: 10.32567/hm.2024.4.4

Harangozó Valentin[1]

Kiberbiztonság a városi mobilitásban, fókuszban az e-rollerek, 1. rész

Cybersecurity in Urban Mobility, Focus on E-Scooters, Part 1

Absztrakt

A tanulmány célja az volt, hogy alaposan megvizsgálja az elektromobilitási eszközök kiberbiztonsági vonatkozásait, azonosítva a lehetséges kockázatokat és veszélyforrásokat, valamint feltárja a felhasználók és az elektromos járművek kiberbiztonsága közötti összefüggéseket. A tanulmány első részében a szerző ismerteti az elektromobilitási eszközöket használók technológiaelfogadási hajlandóságát a TAP-modell alkalmazásával összeállított kérdőíves kutatás alapján. A kutatás eredményei rávilágítanak arra, hogy az elektromobilitási eszközök kiberbiztonsági kockázataihoz való hozzáállás jelentős hatással van az ilyen eszközökkel kapcsolatos technológiai elfogadásra és e járművek használatára, ami kiemelten fontos az elektromobilitás jövőbeli fejlődése szempontjából.

Kulcsszavak: elektromobilitás, kiberbiztonság, elektromos járművek, adatbiztonság

Abstract

The aim of the study was to thoroughly examine the cybersecurity aspects of electromobility devices, identify potential risks and threats, and explore the relationship between users and the cybersecurity of electric vehicles. In the first part of the study, the author presents the willingness of electromobility device users to adopt the technology, based on a survey conducted using the TAP model. The results of the research highlight that perceptions of cybersecurity risks associated with electromobility devices have a significant impact on

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Rendészettudományi Doktori Iskola, e-mail: harangozovalentin1986@gmail.com

the acceptance of these technologies and the use of such vehicles, which is crucial for the future development of electromobility.

Keywords: electromobility, cybersecurity, electric vehicles, data security

Bevezetés

A téma helye, jelentősége, aktualitása

Manapság egyre több közlekedési eszköz közül lehet választani, ha el szeretnénk jutni egyik pontból a másikba. Az elektromobilitás forradalma felgyorsította a közlekedési eszközök átállását hagyományos üzemanyagokról elektromosenergia-felhasználásra. Ennek következtében az elektromobilitási eszközök mint környezetbarát, könnyű és praktikus eszközök elterjedése is rohamosan nő.

Az elektromobilitási eszközök megjelenése változásokat hozott a közlekedési paradigmában, ezzel együtt pedig előtérbe hozta a kiberbiztonság kérdését is. A városi mobilitás átalakulása, amelyet az e-rollerek térnyerése hajt, napjainkban kulcsfontosságú a fenntartható városi élet és a személyes közlekedés terén. Ezen eszközök térhódítása azonban a digitális világba való átmenettel együtt jár, és ezáltal kibertérbe helyezett veszélyeket hordoz magával. A kiberbűnözés folyamatosan fejlődik, és az e-rollerek által használt platformok és alkalmazások a potenciális célpontok között szerepelnek, ezáltal felvetve az adatlopás, a személyazonosság-lopás és más káros tevékenységek veszélyét.

Ezen körülmények közepette az e-rollerek kiberbiztonsági kockázatainak elemzése és kezelése kiemelkedő fontosságú. Az aktualitás ezen a területen éppen abban rejlik, hogy az elektromos közlekedés térnyerése egyidejűleg hozza magával a kiberbiztonsági kihívásokat, így különleges figyelmet igényel az adatvédelem és az eszközök online biztonságának megteremtése. Az elektromobilitási eszközök digitalizációja és a hozzájuk kapcsolódó hálózati funkciók által új kiberbiztonsági fenyegetések merülhetnek fel, amelyekre eddig kevés figyelem irányult. Pontosan ezek a sajátosságok és az ezekből felmerülő kiberbiztonsági problémák kérdésköre az, ami miatt a kutatásomat választottam.

A tudományos probléma megfogalmazása

Az elmúlt években óriási növekedés történt az elektromos járművek értékesítésében és globális elfogadottságában szerte a világon.[2] A zökkenőmentes átmenet egyik fő mozgatórugója az innováció elfogadása és a technológiába vetett bizalom. Az elektromos járművek hatékonyságának javításával a közlekedési ágazat környezetbarátabb, termelékenyebb és agilisabb lehet.[3] Az elektromobilitás térnyerése jelentős áttörést hozott a közlekedés terén, azonban ez a modernizáció nem csupán előnyökkel járt.

[2] IEA 2022.
[3] Muhammad et al. 2023.

Az eszközök használatához szükséges digitális infrastruktúra és kapcsolódó alkalmazások adatainak tárolása és feldolgozása kiemelkedő figyelmet igényel a felhasználók személyes és a szolgáltatók üzleti adatainak védelme érdekében.

Az elektromosjármű-gyártás hatalmas iparág, hatalmas pénzforgalommal. Ennek ellenére korlátozott mennyiségű kutatás áll rendelkezésre, és nagyon kevés erőfeszítést tesznek olyan iránymutatások és szabványok meghatározására, amelyek rávilágítanak arra, hogyan lehet elérni a fenntarthatóságot a kiberbiztonság veszélyeztetése nélkül. Összefüggést kell találni az elektromos járművek fenntarthatósága és az elektromos járműveket célzó kiberfenyegetések között.[4]

Mivel az elektromos járművek rengeteg fogyasztói személyes adatot gyűjtenek, létfontosságú a járműhöz kapcsolódó minden egyes rendszer védelme.[5] Az adatbiztonság és az adatvédelem mellett az e-rollerek fizikai biztonságát érintő problémák is kritikus fontosságúak. A hardveres és szoftveres biztonsági rések kihasználása, például a távoli hozzáférés vagy az eszközön található sebezhetőségek, potenciális támadási felületeket teremtenek a kiberbűnözők számára. Mindez hozzájárulhat az eszközök megbízhatatlanságához és a felhasználók bizalmatlanságához azokkal kapcsolatban. Ezért fontos, hogy az eszközök és az azokat kezelő platformok olyan biztonsági megoldásokkal, stratégiákkal rendelkezzenek, amelyek megfelelő védelmet nyújtanak a felhasználói adatoknak, valamint a fizikai és digitális fenyegetésekkel szemben is ellenállók.

A vizsgálat tárgya és a célkitűzések

Kutatási célkitűzések, fontosabb kérdések

A fontosabb kérdések körét vizsgálva két részre bontható a cikk, ebben a részben elemzem és bemutatom az ezeket a közlekedési eszközöket használók biztonságtudatossági szintjét és hajlandóságukat a technológia elfogadására, a második részben pedig bemutatom a vizsgált elektromos eszközök kiberbiztonsági fenyegetettségeit. A kutatás céljával összhangban annak érdekében, hogy a felhasználók és az elektromos járművek kiberbiztonsága közötti összefüggéseket feltárhassam és megvizsgálhassam, az alábbi kérdéseket fogalmaztam meg.

- Hogyan alakul a felhasználók hozzáállása az elektromobilitási eszközökkel és technológiákkal kapcsolatban?
- Milyen hatása van a kiberbiztonsági fenyegetettségeknek a felhasználói élményre és bizalomra az elektromos járművekkel kapcsolatban? Hogyan befolyásolja ezt a döntést az ilyen eszközök használatáról vagy vásárlásáról?

[4] Kumar et al. 2018.
[5] Ji-Otto–Kostas 2023.

Kutatási hipotézisek

A kutatási téma feldolgozása során az alábbi hipotéziseket fogalmaztam meg:

H1: Az emberek részéről aggodalom tapasztalható az elektromobilitási eszközök kiberbiztonsági kockázatai miatt.

H2: Az elektromobilitási eszközökkel kapcsolatos optimizmus és pozitív hozzáállás eltérő módon nyilvánul meg az eszközök birtoklása függvényében.

H3: Az elektromobilitási eszközökkel kapcsolatos kiberbiztonsági tudatosságot befolyásolja a nem és az iskolai végzettség.

Kutatási módszerek

A kutatásom során első lépésként egy online kérdőíves kutatást készítettem, amelynek célja az volt, hogy megértsem az emberek attitűdjeit és aggodalmait az elektromobilitási eszközök kiberbiztonsági kérdéseivel kapcsolatban. A kérdőívben különös hangsúlyt fektettem olyan témákra, mint az eszközökkel kapcsolatos tapasztalatok, az aggodalmak szintje és a technológia elfogadásával kapcsolatos hajlandóság.

A kérdőíves kutatás egyik fontos része az elektromobilitási eszközökkel kapcsolatos személyes tapasztalatokat vizsgálta. Arra kérdeztem rá, hogy a válaszadók milyen típusú elektromos járműveket használnak, milyen gyakran használják ezeket az eszközöket. Felmértem a válaszadók tudatosságát a kiberbiztonsági fenyegetettségekkel kapcsolatban, és hogy milyen mértékben aggódnak ezek miatt. A kérdőív kiterjedt a technológia elfogadásával és alkalmazásával kapcsolatos hajlandóság vizsgálatára is. Megkérdeztem a válaszadókat, hogy mennyire nyitottak az új elektromobilitási eszközök használatára, milyen tényezők befolyásolják a döntésüket és milyen feltételek mellett éreznék biztonságosnak ezen eszközök használatát.

Összegyűjtöttem, majd részletesen áttekintettem a hazai és nemzetközi szakirodalmat az elektromobilitási eszközökkel és azok kiberbiztonsági kockázataival kapcsolatban.

Az összes adatgyűjtést követően az összegyűjtött információkat analizáltam és összehasonlítottam, hogy átfogó képet kapjak az elektromobilitási eszközök kiberbiztonsági helyzetéről. A fentiek eredményeként alakítottam ki a kutatás végkövetkeztetéseit és ajánlásait.

Az elektromobilitási eszközök

Az elektromos járművek története és fejlődése a 19. századra nyúlik vissza, ám csak az utóbbi években váltak igazán elterjedtté. Az autóipar a világ egyik legfontosabb iparágává vált, nemcsak gazdasági szinten, hanem a kutatás és fejlesztés szempontjából is. Egyre több technológiai elemet vezetnek be a járművekbe mind az utasok, mind a gyalogosok biztonságának javítása érdekében.[6] Az elektromos járművek

[6] Sanguesa et al. 2021.

népszerűségét bizonyítja, hogy a gyártók széles köre mutatja be a plug-in hibrid és akkumulátoros járművek új modelljeit.[7] Az elektromos közlekedés térnyerése számos alternatív járművet hozott magával, mint az elektromos rollerek és kerékpárok. Ezek környezetbarát megoldások, bár még mindig vannak korlátai, mint például a hatótávolság és a töltési infrastruktúra hiánya. Az elektromobilitás jelenlegi helyzete azonban kedvező, az egyre szigorúbb környezetvédelmi szabályozások és a technológiai fejlődés ösztönzi az áttérést az elektromos járművekre.

A közlekedési eszközök, akárcsak a mobiltelefonok vagy a számítógépek, folyamatos fejlődés alatt állnak. A technológiai rendszerek innovációit folyamatosan adaptálják a járműiparba is. Ezért elkerülhetetlen volt, hogy a közlekedési eszközök csatlakozzanak a hálózatra. Egy átlag-járműhasználó életében a választott jármű típusától függően más-más lehetőségek állnak rendelkezésre az internetes hálózathoz való csatlakozásra. Eleinte még csak maximum bluetooth-kapcsolatok létesítésére voltak képesek egyes járművek, például egy személygépkocsi kihangosító rendszere, azonban a felhasználói igények folyamatos fokozódásával megjelentek a GPS-rendszerek, az érintőképernyős fedélzeti számítógépek és a mára már hétköznapinak számító Tesla önvezető járművek rendszerei.

Az elektromos járművek térhódítása már évekkel korábban elkezdődött,[8] azonban a 2015-ös év környékére tehető főként, hogy az elektromos autózás hétköznapivá vált és berobbant a köztudatba Magyarországon. Ugyanis 2014. március 13-án a kormány bejelentette, hogy adókedvezményeket és támogatásokat ad az állampolgároknak, annak érdekében, hogy az elektromos autók elterjedhessenek Magyarországon. Az első nagyobb ugrás a zöld rendszámos járművek tekintetében 2016-ban történt. 2015-ben még csak 303 darab elektromos meghajtású jármű közlekedett az utakon, míg 2016 decemberében már ugyanez a szám 1524 darab volt, ami ötszörös növekedést jelentett.[9] A jelenlegi számok tekintetében a 2022-es évben minden rekordot megdöntött a zöld rendszámos autók átadása Magyarországon, köztük is a tisztán elektromos autók eladása nőtt a legnagyobb mértékben, és az év végén már 34 754 közlekedett az utakon. A legfrissebb adatok alapján pedig 2023. június végén 41 386 tisztán elektromos autó közlekedett az utakon Magyarországon, míg a zöld rendszámos autók száma már meghaladta a 74 000 darabot.[10] Az előrejelzések pedig azt mutatják, hogy folyamatosan nő az elektromos és hibrid járművek (EV) száma Európában, így a 2030-ra várhatóan több mint 75 millió jár majd belőlük az utakon.[11]

Az elektromos rollerek elterjedése Magyarországon az előzetes várakozásokat jelentősen meghaladta. A Jövő Mobilitása Szövetség prognózisa alapján 2023-ra 30–40 ezer rollerrel számoltak az ország közútjain. Ezzel szemben a 2023-as adatok szerint már 80–100 ezer elektromos roller vett részt a közúti közlekedésben. Ebből hozzávetőleg 25 ezer a különböző bérlési rendszerek révén elérhető, míg a többi magánszemélyek tulajdonában van.[12]

[7] Viola 2021.
[8] Xu 2023.
[9] Tóth 2017.
[10] Pásztor 2023.
[11] Birkás 2024.
[12] *Hányan roliznak Magyarországon?* 2025.

Az elektromos rollerek gyors elterjedése jól tükrözi a mikromobilitás iránti növekvő igényt, különösen a városi környezetben, ahol a hagyományos közlekedési formák egyre kevésbé bizonyulnak hatékonynak a torlódások és a zsúfoltság miatt. Míg az autóval közlekedők gyakran 30–40 percet töltenek egy adott útszakaszon csúcsidőben, addig a rollerek lehetővé teszik ugyanazon útvonal 8–10 perces megtételét. Ez a hatékonyság egyre több városlakót ösztönöz arra, hogy a személygépkocsi helyett mikromobilitási eszközöket válasszon.

A városi közlekedés dinamikája jelentős változások előtt áll. A rollerek gyors ütemű térhódítása nemcsak a közlekedési szokások átalakulására, hanem a városok infrastruktúrájának átgondolására is kényszeríti a döntéshozókat. Az elektromos rollerek és más mikromobilitási eszközök térnyerése lehetőséget kínál arra, hogy a városok fenntarthatóbban és hatékonyabban működjenek, mindamellett pedig csökkenthetik a forgalmi torlódásokat és a légszennyezést is.

A fentiek alapján megállapítható, hogy az emberek környezettudatossá válása és a fenntartható mobilitásra való törekvés egyre nagyobb figyelmet kap. Ezt bizonyítja az a tény is, hogy az elektromos mobilitási eszközök száma is napról napra növekszik a közúti közlekedésben. Hiszen például az elektromos rollerek, hoverboardok,[13] segwayek[14] kiváló alternatívát nyújtanak a környezetbarát közlekedés terén, a városi közlekedéshez a kompaktságuk miatt is hasznosak, illetve az egyre fejlettebb akkumulátorok és a jobb teljesítményű motorok lehetővé teszik, hogy ezek az eszközök hosszabb távokra is alkalmasak és kényelmesebben használhatók legyenek.

A kutatás eredményei

A kérdőív

Az általam végzett kérdőíves kutatás a konkrét vizsgálathoz kapcsolódóan kvantitatív és nem reprezentatív. A módszertant tekintve véletlenszerű mintavételen alapuló kérdőíves felmérés. A kérdőívben egyes, többszörös választásos és értékelő skálás kérdéseket tettem fel.

A kutatásom először a kérdőív megtervezésével kezdődött. Az ideális objektumszám és a megfelelő kérdéstípusok meghatározása volt az első feladat, olyan szempontok alapján, hogy az adott válaszok alkalmasak legyenek informatikai elemzésre is. Ennek függvényében összesen 28 kérdést állítottam össze, amelyből 11 darab egyszeres választásos, 2 darab többszörös választásos, 14 darab értékelő skálás és 1 darab nyitott kérdés. Az ideális kérdésszámot azon elvárások alapján állapítottam meg, hogy a kérdőíves kutatás megfelelően széles spektrumú legyen, illetve hogy a kapott adatok és eredmények kezelhető mennyiségűek maradjanak.

[13] A hoverboard lapos, kétkerekű, kis elektromos jármű, amelyet a talpunk lenyomásával irányíthatunk. Segítségével könnyedén kanyarodhatunk, gyorsulhatunk és lassulhatunk, mivel beépített giroszkóp és elektronika segíti mozgásunkat.

[14] A segway olyan közlekedési eszköz, amelyet a talpak és testsúly mozgatásával irányítanak. Ez egy kétkerekű jármű, amely elektromos meghajtással rendelkezik, és van rajta kar, amely segíti az irányítást.

A kérdőív megtervezése után a következő lépés a válaszadók elérése volt. A kérdőív online formában készült el, és több internetes közösségi csoportban lett nyilvánosan megosztva, ami lehetővé tette, hogy a résztvevők teljesen véletlenszerűen töltsék ki. Mivel a kérdőív széles körben, online terjesztéssel lett közzétéve, a válaszadás önkéntes és anonim módon zajlott. Ennek a módszernek köszönhetően a kutatás teljesen beavatkozásmentesen folyt, hiszen nem történt célzott mintavétel, sem más külső befolyás. Fontos azonban megemlíteni, hogy a kapott adatok kizárólag az adott mintára vonatkoztathatók. Így a kutatás eredményei elsősorban az adott internetes közösségekben részt vevőkre érvényesek, és nem feltétlenül vonatkoztathatók az egész populációra.

Az általam összeállított kérdőív az alábbiak szerint tagozódik:

- Demográfiai adatok: Az első részben demográfiai kérdések találhatók, amelyek segítségével a válaszadók nemét, életkorát, iskolai végzettségét és lakhelyét rögzítjük.
- Felhasználói szokások: Ez a rész arra irányul, hogy feltárja a válaszadók elektromobilitási eszközökkel kapcsolatos felhasználói szokásait, beleértve a saját eszköz birtoklását és használatát, valamint a közösségi megosztáson alapuló eszközök használati gyakoriságát.
- Közösségi hatások: Ebben a részben a válaszadók az elektromobilitási eszközök közösségi hatásait értékelhetik.
- Kiberbiztonsági tudatosság: A kérdőív eme része arra irányul, hogy feltárja a válaszadók kiberbiztonsági tudatosságát és ismereteit az elektromos mobilitással kapcsolatban.
- Technológiaelfogadással kapcsolatos hajlandóság: Az utolsó részben a válaszadóknak a technológia elfogadásával kapcsolatos hajlandóságát mérik fel a TAP-index segítségével, beleértve az optimizmust, jártasságot, függőséget és sebezhetőséget.

A technológiaelfogadással kapcsolatos hajlandóság kifejezés azt jelenti, hogy menynyire hajlandók az emberek elfogadni és alkalmazni az új technológiákat az életükben. A TAP-modell egy olyan módszer vagy skála, amely segít mérni az emberek e téren mutatott hajlandóságát, és figyelembe veszi a támogató (optimizmus, jártasság) és gátló (függőség és sebezhetőség) tényezőket.[15]

Az optimizmusfaktor azt mutatja, hogy az egyén mennyire hisz abban, hogy a technológiai fejlesztések pozitív hatással lesznek az életére. A jártasság arra utal, hogy az egyén milyen mértékben jártas a technológiák használatában és kezelésében. A függőségfaktor azt méri, hogy az egyén milyen szintű függőséget alakított ki a technológiával való interakciójában. A sebezhetőség arra utal, hogy az egyén mennyire érzi magát sebezhetőnek a technológiai változásokkal szemben.[16]

Ezek a faktorok különböző módon befolyásolják az emberek hajlandóságát az új technológiák elfogadására. A TAP-index segítségével ezeket a faktorokat mérve jobban megérthetjük, hogyan reagálnak az emberek az új technológiákra, és hogyan lehet

[15] Berényi–Deutsch 2023.
[16] Wolff 2021.

ezeket a reakciókat befolyásolni vagy támogatni. Összességében a kérdőív átfogóan vizsgálja a válaszadók kiberbiztonsági tudatosságát és a technológia elfogadásával kapcsolatos hajlandóságát az elektromobilitási eszközök tekintetében.

A vizsgálat módszertana

A kutatásomnak ebben a részében a vizsgálati módszer a kérdőívek statisztikai elemzése. Ez a fázis a kérdőíves kutatás eredményeinek átfogó elemzését és egyes adatok összehasonlítását foglalja magában.

Az adatokat különböző statisztikai módszerekkel elemzem, beleértve az egyszerű leíró (deskriptív) statisztikai adatelemzést és az összefüggéseket vizsgáló statisztikai teszteket. Az adatok kiértékelésére az IBM – Statistical Package for the Social Sciences (SPSS) szoftvert használom. Az SPSS számos analitikai eszközt kínál az adatok elemzéséhez, amelyeket a kutatásomban használni fogok, többek között például a khi-négyzet-próbát,[17] a kereszttábla-elemzést,[18] a Kruskal–Wallis-elemzést,[19] a Cramer's V[20] mutatót és egyéb statisztikai mutatókat is, mint például a minimum és maximum, illetve átlag, szórás, ferdeség, csúcsosság mutatók. Ezek az elemzési módszerek és mutatók segítenek az adatok közötti összefüggések és különbségek feltárásában. Összességében tehát a statisztikai elemzési módszerekkel és az SPSS segítségével részletesen megvizsgálom a kérdőíves válaszokat, keresve a válaszok közötti korrelációkat és az esetleges összefüggéseket.

Demográfiai jellemzők

A kérdőíves kutatásban a demográfiai jellemzőkkel kapcsolatban felmértem a válaszadók nemi arányát, az életkori eloszlását és a válaszadók legmagasabb iskolai végzettségét. A kérdőívet kitöltő 117 személy 47%-a nő, míg 53%-a férfi volt.

Az életkorra vonatkozóan a válaszadók többsége a 18 és 25 év közötti korosztályba tartozik, ami 46,2%-os részesedést jelent. Ezután a második legnagyobb arányt a 26 és 39 év közötti korcsoport képviseli 36,8%-os aránnyal. A 40 és 59 év közötti korosztály 15,4%-ot tesz ki a válaszadók közül, míg a 60 év feletti korcsoport mindössze 1,7%-os részesedéssel rendelkezik.

A legmagasabb iskolai végzettségre vonatkozóan a válaszadók legnagyobb része középfokú vagy annál magasabb végzettséggel rendelkezik. A válaszok alapján azok, akik az általános iskola 8 osztályát végezték el, 18,8%-ot tesznek ki. Ezzel szemben 12% a középfokú végzettséggel rendelkezők aránya érettségivel, míg 31,6% azoké,

[17] A khi-négyzet-próba egy statisztikai módszer, amelyet két minőségi változó közötti kapcsolat elemzésére használnak. Segítségével meghatározható, hogy van-e szignifikáns összefüggés a két változó között.

[18] A kereszttábla-elemzés olyan statisztikai módszer, amely a két vagy több kategoriális változó közötti kapcsolatot vizsgálja.

[19] A Kruskal–Wallis-próba egy nem paraméteres statisztikai eljárás, amelyet három vagy több csoport mediánjainak összehasonlítására alkalmaznak, amikor a csoportok közötti különbségek nem feltételezik a normális eloszlást.

[20] A Cramer's V mutató egy asszociációs mérőszám, amely két nominális változó közötti kapcsolat erősségét jelzi.

akik középfokú végzettséggel és szakmai végzettséggel rendelkeznek érettségivel. A felsőfokú végzettségűek csoportjában 27,4% azok aránya, akiknek alapképzéses, BA vagy BSc fokozatú diplomájuk van. Ezzel szemben 6,8% azoké, akik mesterképzés, MA vagy MSc fokozattal rendelkeznek, és 1,7% azoké, akik tudományos fokozatot igazoló oklevelet (PhD, DLA) szereztek.

A TAP-modell leíró elemzése

Az elektromobilitás elfogadását a TAP-modellel vizsgáltam meg, amely négy faktoron keresztül elemzi a technológiaelfogadási hajlandóságot. Az optimizmus, jártasság mint támogató, a függőség és sebezhetőség pedig mint gátló tényező jelenik meg. A TAP-modell négy dimenziója mentén fontos megfigyeléseket tehetünk. A támogató tényezőknél négy, a gátló tényezőknél pedig három állítást tettem, amelyre a válaszadók egy egytől ötig terjedő skálán válaszolhattak, hogy mennyire értenek egyet az adott állítással. Az egy az egyáltalán nem értek egyet, míg az öt a teljes mértékben egyetértek. Az állításokra adott válaszok és számadatok alapján leíró elemzést végeztem (1. táblázat).

1. táblázat: A TAP-modell optimizmusra vonatkozó állításainak elemzése

	Átlag	Szórás	Ferdeség	Csúcsosság
„Azt gondolom, hogy az elektromobilitás a kulcsa a jövő fenntartható közlekedésének."	3,94	1,053	–0,736	–0,103
„Az elektromobilitási jármű használata segít abban, hogy környezetbarátabb alternatívát válasszak a közlekedési eszközök között."	4,13	1,038	–1,295	1,289
„Az elektromobilitás fejlődő technológiája miatt úgy gondolom, hogy ezek a járművek egyre megbízhatóbbak és hatékonyabbak lesznek."	3,94	0,985	–1,089	1,182
„Az elektromos jármű használata növeli az én hozzájárulásomat a fenntartható közlekedéshez."	3,75	1,09	–0,831	0,214

Forrás: a szerző szerkesztése a kérdőív eredményei alapján

Az optimizmusra vonatkozó állítások

Az optimizmusra vonatkozó állítások esetében az átlagos pontszámok magasak voltak, az átlagértékek 3,75 és 4,13 között mozognak az 5 pontos skálán, ami azt mutatja, hogy a résztvevők pozitívan viszonyulnak az elektromobilitáshoz. Az átlagok közötti kis eltérések a válaszok eloszlását tükrözik, míg a szórás alacsony értékei azt jelzik, hogy a válaszok kevésbé térnek el egymástól. A torzítás- és csúcsosságértékek közelítenek

a nullához, ami azt sugallja, hogy az eloszlás közel van a normális eloszláshoz, de kissé lefelé görbült.[21]

2. táblázat: A TAP-modell jártasságra vonatkozó állításainak elemzése

	Átlag	Szórás	Ferdeség	Csúcsosság
„Az elektromobilitási jármű használata könnyebb számomra, mint másoknak."	3,32	1,401	–0,389	–1,097
„Mások is gyakran kérnek segítséget tőlem az elektromobilitási szolgáltatások és rendszerek használatával kapcsolatban."	3,07	1,685	–0,065	–1,654
„Élvezem, hogy magam fedezem fel az új elektromobilitási funkciókat és szolgáltatásokat, anélkül, hogy mások segítségét kérném."	3,41	1,481	–0,414	–1,219
„El tudom végezni az elektromos járművek szoftveres frissítéseit, és értem, hogy ezek hogyan befolyásolják a járművek biztonságát."	3,35	1,621	–0,363	–1,463

Forrás: a szerző szerkesztése a kérdőív eredményei alapján

A jártasságra vonatkozó állítások

A jártasságra vonatkozó állításoknál az átlagpontszámok változatosabbak 3,07 és 3,41 közötti értékekkel, és a válaszok eloszlása szélesebb skálán mozgott. Magasabb szórásértékek figyelhetők meg, ami azt jelenti, hogy a válaszok nagyobb mértékben térnek el egymástól. A torzítás- és a csúcsosságértékek közelítenek a nullához, ami azt sugallja, hogy az eloszlás kissé balra tolódik. Ez alapján arra lehet következtetni, hogy az emberek általánosságban közepesen érzik magukat jártasnak az elektromobilitási szolgáltatások és rendszerek használatában (2. táblázat).

[21] A normál eloszlás szimmetrikus, és az értékek többsége a középérték körül koncentrálódik. Az eloszlás központi eleme az átlag, amely meghatározza a csúcs helyét. A csúcsosság (kurtózis) az eloszlás csúcsának meredekségét jelzi. Ha az eloszlás normális, akkor a csúcsosság értéke 0. Pozitív csúcsossági együttható esetén az eloszlás a normálishoz képest csúcsosabb, míg negatív csúcsossági együttható esetén az eloszlás laposabb, mint a normális eloszlás. A ferdeség az eloszlás aszimmetriáját jelzi, vagyis a csúcs eltolódását a középértékhez képest. Ha az eloszlás jobbra nyúlik, akkor jobbra ferde; ha balra nyúlik, balra ferde. Az eloszlás ferde lehet, ha valamelyik oldalon rendkívül nagy vagy rendkívül kicsi kiugró értékek jelennek meg.

3. táblázat: A TAP-modell függőségre vonatkozó állításainak elemzése

	Átlag	Szórás	Ferdeség	Csúcsosság
„Az elektromos járműveim nélkülözhetetlenek az életemben, és nehézséget okozna, ha egy időre le kellene mondani róluk."	2,88	1,682	0,114	–1,656
„Úgy érzem, hogy túlzottan számítok az elektromos járművekre mindennapi közlekedéseim során."	2,68	1,552	0,149	–1,559
„Az elektromos járművek nélkül kiszolgáltatottnak vagy hátrányban érzem magam a mindennapi életem során."	2,74	1,678	0,228	–1,634

Forrás: a szerző szerkesztése a kérdőív eredményei alapján

A függőségre vonatkozó állítások

A függőségre vonatkozó állítások esetében az átlagos pontszámok alacsonyabbak voltak, az értékek 2,68 és 2,88 között mozognak, ami azt jelzi, hogy az emberek nem érzik magukat túlzottan függőnek az elektromos járművektől mindennapi életük során. Az alacsony átlagok mellett magasabb szórásértékek figyelhetők meg 1,552 és 1,682 között, ami azt mutatja, hogy az emberek válaszai nagyobb mértékben térnek el az átlagtól. A torzításértékek közelítenek a nullához vagy enyhén negatívak, a csúcsosságértékek pedig negatívak, ami azt jelzi, hogy az eloszlás kissé balra görbült (3. táblázat).

4. táblázat: A TAP-modell sebezhetőségre vonatkozó állításainak elemzése

	Átlag	Szórás	Ferdeség	Csúcsosság
„Úgy érzem, hogy a kiberbiztonsági intézkedések fejlesztése során az iparág nem tesz eleget az elektromobilitási eszközök védelméért."	3,56	1,256	–0,301	–0,902
„Az elektromobilitás terjedése miatt növekedhet a kiberbűnözők érdeklődése ezen eszközök iránt."	4,02	1,098	–0,947	0,173
„Úgy gondolom, hogy az elektromobilitás terjedésével párhuzamosan a kiberbiztonsági megoldások is fejlődnek."	3,88	1,084	–0,708	–0,128

Forrás: a szerző szerkesztése a kérdőív eredményei alapján

A sebezhetőségre vonatkozó állítások

Az átlagos pontszámok magasabbak a sebezhetőségre vonatkozó állításoknál, az értékek 3,56 és 4,02 között mozognak, ami azt jelzi, hogy az emberek aggodalmat éreznek a kiberbiztonsági kockázatok miatt. Ezzel igazolva a H1. kutatási hipotézisemet, miszerint az emberek részéről aggodalom tapasztalható az elektromobilitási eszközök kiberbiztonsági kockázatai miatt. A szórásértékek itt is magasak voltak, ami azt mutatja, hogy a válaszok nagyobb mértékben térnek el az átlagtól. A torzítás- és a csúcsosságértékek közelítenek a nullához vagy enyhén negatívak, ami azt jelzi, hogy az eloszlás kissé balra görbült (4. táblázat).

Következtetés

Összegezve elmondható, hogy általánosságban pozitívan viszonyulnak az emberek az elektromobilitáshoz és a fenntartható közlekedéshez. Bár magas az optimizmus és a jártasság, közepes szintű a függőség, ugyanakkor magasabb a sebezhetőség érzete a kiberbiztonsági kockázatok miatt. Az eredmények alapján a technológiai fejlődéssel és a biztonsági intézkedések javításával tovább növelhető lenne az emberek elfogadása az elektromobilitással kapcsolatban, amit megerősít az a kutatás is, amely szerint az elektromos járművek bevezetésének előmozdítására irányuló erőfeszítések során társadalmi és szabályozási tényezőket is figyelembe kell venni.[22] Továbbá egy másik kutatás szintén kimutatta, hogy a technológiai aggályok negatív hatással vannak az elektromos járművek vásárlási szándékaira.[23]

A nem és a végzettség összefüggése a tudatossággal

A kiértékelés célja az volt, hogy feltárja az összefüggéseket a résztvevők neme, végzettsége és a kiberbiztonsági tudatosság között az elektromobilitási eszközök használatával kapcsolatban. A H3. kutatási hipotézisem vizsgálata érdekében kereszttábla-elemzéssel kiértékeltem, hogy a résztvevők neme összefüggést mutat-e azzal, hogy hallottak-e már arról, hogy az elektromobilitási eszközök használata során a biztonságuk és az adataik veszélyben lehetnek a kiberbiztonsági kockázatok miatt, illetve ezt az elemzést végzetem el abban az aspektusban, hogy a tudatosság összefüggést mutat-e azzal, hogy a válaszadó rendelkezik-e legalább felsőfokú végzettséggel.

[22] Patil 2020.
[23] Lashari–Ko–Jang 2021.

Nemek összefüggései

A khi-négyzet-tesztek és szimmetrikus mértékek elemzése a nem és a kiberbiztonsági veszélyek ismerete közötti kapcsolatot vizsgálta az elektromobilitási eszközök használatával kapcsolatban. Az eredmények azt mutatták, hogy van szignifikáns kapcsolat a nem és a kiberbiztonsági veszélyek ismerete között (Pearson khi-négyzet: $\chi^2(1) = 5{,}445$, $p = 0{,}020$). Ez azt jelzi, hogy valószínűleg a nem befolyásolja az emberek vélekedését a kiberbiztonsági veszélyekről az elektromobilitási eszközök használata során. A Fisher-féle pontos teszt tovább erősítette ezt az eredményt ($p = 0{,}027$, kétoldalas; $p = 0{,}017$, egyoldalas), megerősítve annak valószínűségét, hogy a nem és a kiberbiztonsági veszélyek ismerete közötti kapcsolat valós és szignifikáns.

A szimmetrikus mértékek, mint például a Phi és a Cramer's V is megerősítették a kapcsolatot, közepes erősségű szignifikáns összefüggést mutatva a nem és a kiberbiztonsági veszélyek ismerete között (Phi = 0,216; Cramer's V = 0,216). Ez azt jelzi, hogy a nem befolyásolja az emberek tudását és érzékenységét a kiberbiztonsági kockázatokra az elektromobilitási eszközök használata során, ezzel igazolva a H3. kutatási hipotézisem első részét. Összességében ezek az eredmények alátámasztják, hogy a nem jelentős tényező lehet az egyének kiberbiztonsági tudatosságában az elektromobilitási eszközök használata és a technológiaelfogadás során, amit alátámaszt egy hasonló kutatás is, amelyben a nemnek szintén jelentősége volt a használati és vásárlási szándékban. Azon kutatás eredménye alapján a nők hajlamosabbak elektromos kétkerekűek vásárlására, mint a férfiak.[24]

Végzettség összefüggései

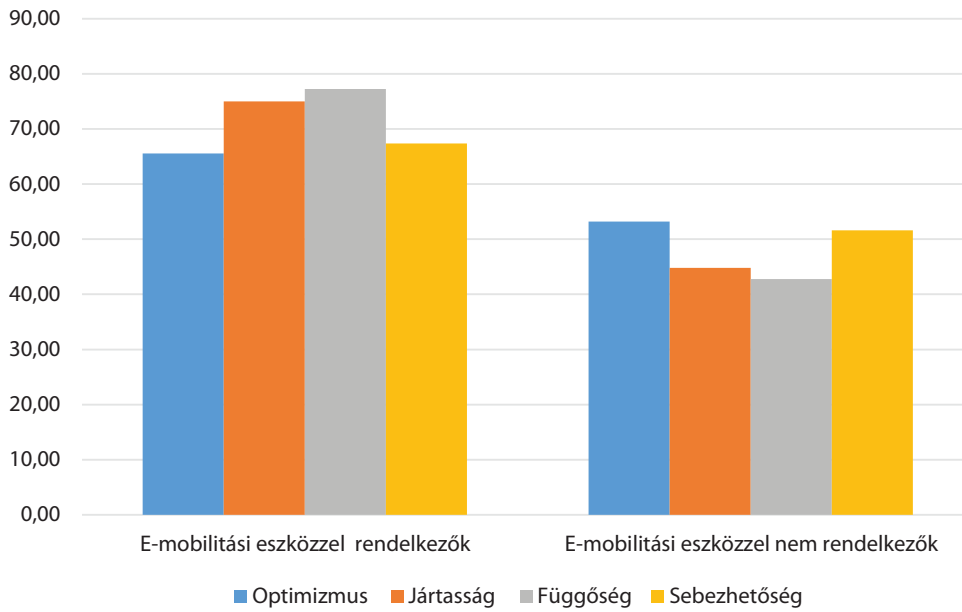
Az elemzés során khi-négyzet-teszteket és szimmetrikus mértékeket alkalmaztam annak érdekében, hogy feltárjam a „Van-e legalább felsőfokú végzettsége?" és a „Hallott-e már arról, hogy kiberbiztonsági szempontból a biztonsága és az adatai is veszélyben lehetnek egy elektromobilitási eszköz használata során?" változók közötti összefüggést. Ezzel a végzettség és az elektromobilitási eszközök kiberbiztonsági veszélyeivel kapcsolatos tudatosság közötti lehetséges kapcsolatot vizsgáltam, és a következő eredményeket kaptam.

A Pearson-féle khi-négyzet-teszt azt mutatta, hogy a két változó közötti kapcsolat nem szignifikáns ($\chi^2 = {,}358$, $df = 1$, $p = {,}550$). A Fisher-féle pontos teszt eredménye szintén hasonlóan volt nem szignifikáns ($p = {,}648$). Ezek az eredmények egyértelműen utalnak arra, hogy nincs szoros összefüggés a legalább felsőfokú végzettséggel rendelkezők köre és a kiberbiztonsági veszélyek ismerete között, ezzel megcáfolva a H3. kutatási hipotézisem második részét. A szimmetrikus mértékek, mint a Phi és a Cramer's V, szintén alacsony értékeket mutattak (Phi = ,055; Cramer's V = ,055). Ezek az értékek is alátámasztják azt a tényt, hogy nincs szignifikáns kapcsolat a vizsgált változók között.

[24] Jayasingh–Girija–Arunkumar 2021.

A TAP-modell és az e-mobilitási eszközökkel rendelkezők összefüggései

A vizsgált adatok alapján elemzést végeztem az optimizmus, jártasság, függőség és sebezhetőség faktorai mentén az elektromos mobilitási eszközökkel rendelkezők és azok között, akiknek nincs ilyen eszközük (1. ábra).



1. ábra: A TAP-modell faktorainak összefüggései az elektromobilitási eszközök birtoklásával
Forrás: a szerző szerkesztése a kérdőív eredményei alapján

Az optimizmus vizsgálata során megállapítható, hogy az elektromobilitási eszközökkel rendelkezők átlagos rangja (68,78) magasabb volt, mint azoké, akik nem rendelkeztek ilyen eszközzel (50,32). A Kruskal–Wallis-teszt kimutatta, hogy ebben a dimenzióban szignifikáns különbségek vannak a két csoport között (khi-négyzet = 9,535, df = 1, p = 0,002). Ezzel igazolva H2. kutatási hipotézisemet, tehát az elektromobilitási eszközökkel rendelkezők optimistábbak és pozitívabbak az elektromos mobilitási technológiákat illetően, mint azok, akik nem rendelkeznek ilyen eszközökkel.

A jártasság vizsgálata szintén jelentős különbségeket mutatott. Az elektromobilitási eszközökkel rendelkezők átlagos rangja magasabb volt (75,03) azokhoz képest, akiknek nincs ilyen eszközük (44,78). A Kruskal–Wallis-teszt eredménye szintén szignifikáns különbségeket mutatott ebben a dimenzióban (khi-négyzet = 13,816, df = 1, p < 0,001).

A függőség és sebezhetőség dimenzióiban is hasonló eredményeket kaptam. Mindkét esetben az elektromobilitási eszközökkel rendelkezők átlagos rangja magasabb volt, mint azoké, akik nem rendelkeztek ilyen eszközzel (függőség: 77,28 és 42,78; sebezhetőség: 67,35 és 51,59). Mindkét dimenzióban szintén szignifikáns

különbségeket találtunk a két csoport között (függőség: khi-négyzet = 35,468, df = 1, p < 0,001; sebezhetőség: khi-négyzet = 18,229, df = 1, p < 0,001).

Ezek az eredmények alátámasztják azt a feltevést, hogy az elektromobilitási eszközökkel rendelkezőknek általában pozitívabb érzelmeik, magabiztosabb jártasságuk, kevesebb függőségük és kevesebb érzékenységük van a sebezhetőséggel szemben, ezzel ellentétben azok, akik nem rendelkeznek elektromos mobilitási eszközökkel, általában alacsonyabb rangokat kaptak az optimizmus, jártasság, függőség és sebezhetőség faktoraiban. Ez arra utal, hogy azok, akik nem rendelkeznek saját elektromobilitási eszközökkel, általában kevésbé pozitívak és magabiztosak az elektromos mobilitási technológiákkal kapcsolatban, valamint nagyobb mértékben érezhetik a függőséget és a sebezhetőséget azok használata során. Ennek érdekében elmondható, hogy olyan intézkedésekre van szükség, amelyek promóciók/kampányok/politikák révén javítják a felhasználók tudatosságát, hogy a jövőben élénkebbé váljon az elektromobilitási eszközök használata.[25]

Kutatási eredmények

Kutatásom során az alábbi eredményeket fogalmaztam meg.

T1: Igazoltam, hogy az emberekben valóban aggodalom van jelen az elektromobilitási eszközök kiberbiztonsági kockázataival kapcsolatban.

T2: Megállapítottam, hogy az elektromobilitási eszközökkel rendelkezők körében valóban optimistább és pozitívabb attitűd tapasztalható az elektromos mobilitási technológiákkal kapcsolatban, mint azoknál, akik nem rendelkeznek ilyen eszközökkel.

T3: Igazoltam, hogy az elektromobilitási eszközökkel kapcsolatos kiberbiztonsági tudatosságban a nem és az iskolai végzettség csak részben bizonyultak befolyásoló tényezőnek, ugyanis a nemnek mint tényezőnek van, míg a végzettségnek nincs befolyása.

Összegzett következtetések és ajánlások

Összefoglalva, a kutatás eredményei rámutatnak arra, hogy az elektromobilitási eszközök kiberbiztonsága fontos és aktuális kérdés, ami megköveteli a tudatosságnövelést, a bizalomépítést, valamint a kiberbiztonsági protokollok és szabványok fejlesztését. Ez növelhetné az emberek tudatosságát és hajlandóságát a kiberbiztonsági intézkedésekkel kapcsolatban, ami hozzájárulhatna az elektromobilitási eszközök biztonságosabb használatához.

Fontos felismerni és kezelni a kiberbiztonsági kihívásokat az e-rollerek és a többi elektromos közlekedési eszköz esetében is. Az adatvédelmi intézkedések erősítése, a kiberbiztonsági szakértők bevonása és a rendszeres auditok lehetőséget teremtenek az emberek bizalmának növelésére és az eszközök biztonságának javítására. Továbbá

[25] Kim–Lim–Kim 2021.

a felhasználók és a gyártók közötti együttműködés és felelősségvállalás elengedhetetlen az innováció és a biztonság egyensúlyának fenntartása érdekében.

Ezen eredmények alapján megerősíthető, hogy az elektromobilitási eszközök kiberbiztonsági kérdései komoly figyelmet igényelnek. Az elektromos járművek sebezhetőségeinek azonosítása és az ezekből eredő kockázatok kezelése kiemelkedő fontosságú a felhasználók szempontjából. A megvizsgált eredmények alapján megállapíthatjuk, hogy a kiberbiztonsági fenyegetettségeknek a felhasználói élményre és bizalomra gyakorolt hatása jelentős. Az effajta fenyegetettségek csökkenthetik a felhasználók bizalmát az elektromos járművek iránt, és negatívan befolyásolhatják a döntésüket az ilyen eszközök használatáról vagy vásárlásáról. Ez pedig jelentős akadály lehet az e-mobilitás terjedése szempontjából, ezzel együtt pedig az okosvárosok és az autonóm közlekedés fejlődése is lelassulhat.

Felhasznált irodalom

Berényi, László – Deutsch, Nikolett (2023): Technology Adoption Among Higher Education Students. *Vezetéstudomány / Budapest Management Review,* 54(11), 28–39. Online: https://doi.org/10.14267/VEZTUD.2023.11.03

Birkás Péter (2024): Európában 2030-ra várható az elektromos járművek piaci áttörése. *24.hu,* 2024. április 3. Online: https://24.hu/tech/2024/04/03/europaban-2030-ra-varhato-az-elektromos-jarmuvek-piaci-attorese/

Hányan roliznak Magyarországon? *Kreszvaltozas.hu,* 2025. április 16. Online: https://kreszvaltozas.hu/hir/hanyan-roliznak-magyarorszagon/

IEA (2022): *Global EV Outlook 2022*, IEA, Paris. Online: www.iea.org/reports/global-ev-outlook-2022

Jayasingh, Sudarsan – Girija, T. – Arunkumar, Sivakumar (2021): Factors Influencing Consumers' Purchase Intention towards Electric Two-Wheelers. *Sustainability,* 13(22). Online: https://doi.org/10.3390/su132212851

Ji-Otto, L. Hannah – Kostas, Stefan R. (2023): Privacy and Cybersecurity Issues in Electric Vehicles. *CPO Magazine,* 2023. február 13. Online: www.cpomagazine.com/data-privacy/privacy-and-cybersecurity-issues-in-electric-vehicles/

Kim, Suk-Hee – Lim, Hyejin – Kim, Junghwa (2021): Exploring Countermeasures from a Psychological Perspective to Create a Safe Driving Environment for Personal Mobility Devices. *Sustainability,* 13(10). Online: https://doi.org/10.3390/su13105450

Kumar, Amara Dinesh – Chebrolu, Koti Naga Renu – Vinayakumar, R. – Soman, KP. (2018): *A Brief Survey on Autonomous Vehicle Possible Attacks, Exploits and Vulnerabilities.* arXiv, 2018. október 3. Online: https://doi.org/10.48550/arXiv.1810.04144

Lashari, Zulfiqar Ali – Ko, Joonho – Jang, Junseok (2021):Consumers' Intention to Purchase Electric Vehicles: Influences of User Attitude and Perception. *Sustainability,* 13(12). Online: https://doi.org/10.3390/su13126778

Muhammad, Zia – Anwar, Zahid – Saleem, Bilal – Shahid, Jahanzeb (2023): Emerging Cybersecurity and Privacy Threats to Electric Vehicles and Their Impact on

Human and Environmental Sustainability. *Energies,* 16(3). Online: https://doi.org/10.3390/en16031113

Pásztor Csaba (2023): Egyre magabiztosabban és többen villanyautóznak Magyarországon. *Totalcar,* 2023. augusztus 2. Online: https://totalcar.hu/magazin/hirek/2023/08/02/egyre-magabiztosabban-es-tobben-villanyautoznak-magyarorszagon/

Patil, Priyadarshan (2020): An Empirical Study of the Factors Influencing the Adoption of Electric Vehicles. *Contemporary Issues in Behavioral and Social Sciences,* 7(1), 1–13.

Sanguesa, Julio A. – Torres-Sanz, Vicente – Garrido, Piedad – Martinez, Francisco J. – Marquez-Barja, Johann M. (2021): A Review on Electric Vehicles: Technologies and Challenges. *Smart Cities,* 4(1), 372–404. Online: https://doi.org/10.3390/smartcities4010022

Tóth, Zoltán (2017): The Electric Vehicle Penetration in Hungary. *International Journal of Engineering and Management Sciences,* 2(4), 551–562. Online: https://doi.org/10.21791/IJEMS.2017.4.45.

Viola, Fabio (2021): Electric Vehicles and Psychology. *Sustainability,* 13(2). Online: https://doi.org/10.3390/su13020719

Wolff, Josephine (2021): How Is Technology Changing the World, and How Should the World Change Technology? *Global Perspectives,* 2(1). Online: https://doi.org/10.1525/gp.2021.27353

Xu, Chuyuan (2023): Research on Range Extended Electric Vehicle Based on Cruise. *Journal of Physics: Conference Series,* 2479. Online: https://doi.org/10.1088/1742-6596/2479/1/012012

HADMÉRNÖK
VÉDELEMINFORMATIKA

19. évfolyam (2024) 4. szám 61–80.
DOI: 10.32567/hm.2024.4.5

Munk Sándor[1]

Újrafelhasználható interoperabilitási szoftverkomponensek NATO informatikai rendszerekben

Reusable Interoperability Software Components in NATO C2 Systems

Absztrakt

A napjaink többnemzeti műveleteiben részt vevő, kormányzati és más (nem kormányzati) szervezetekkel együttműködő katonai szervezetek eredményes működésének folyamatosan növekvő jelentőségű feltétele rendszereik interoperabilitása. A NATO katonai informatikai rendszerek fejlesztése, interoperabilitási képességeik megvalósítása és fenntartása a Szövetségi Műveleti Hálózat (FMN) keretrendszer interoperabilitási követelményei figyelembevételével történik. Bár az újrafelhasználható szoftverkomponensekre épülő fejlesztés csökkenti a fejlesztések időtartamát és költségeit, növeli az interoperabilitási képességek minőségét, ilyen komponensek a NATO vezetési és irányítási rendszerek esetében nem állnak rendelkezésre, kérdéseikkel a katonai szakirodalom sem foglalkozik. Jelen publikáció célja, hogy igazolja azt a hipotézist, miszerint vannak olyan – a NATO FMN követelményekben szereplő – interoperabilitási funkciók, amelyek megvalósíthatók újrafelhasználható szoftverkomponensek formájában. Célja összegezni az újrafelhasználható interoperabilitási komponensek fogalmi alapjait, feltárni főbb típusaikat, összevetve a kapcsolódó NATO-dokumentumokkal, és meghatározni az egyes típusok rendeltetését, főbb jellemzőit.

Kulcsszavak: interoperabilitás, NATO vezetési és irányítási rendszerek, újrafelhasználható szoftverkomponensek

[1] Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Informatikai Tanszék, e-mail: munk.sandor@hotmail.hu

Abstract

An increasingly important condition for the successful operation of military organisations participating in today's multinational operations and cooperating with governmental and other (non-governmental) organisations is the interoperability of their systems. The development of NATO military IT systems, implementation and maintenance of their interoperability capabilities is done according to the interoperability requirements of the Federated Mission Networking (FMN) framework. Although development based on reusable software components reduces development time and costs and increases the quality of interoperability capabilities, such components are not available for NATO command and control systems, nor are their issues addressed in military literature.
This publication validates the hypothesis that there are interoperability functions included in the NATO FMN requirements that can be implemented in the form of reusable software components, summarises the conceptual foundations of reusable interoperability components, explores their main types, comparing them with related NATO documents, and defines the purpose and main characteristics of each type.

Keywords: interoperability, NATO C2 systems, reusable software components

Bevezetés

Napjainkban a katonai műveleteket sok esetben különböző nemzetek, haderőnemek katonai szervezetei többnemzeti műveletben hajtják végre, együttműködve kormányzati és más (nem kormányzati) szervezetekkel is. A műveleteket végrehajtó erők hatékonysága, eredményessége, sőt egyre inkább alapvető működőképessége jelentős mértékben függ a tevékenységüket támogató informatikai rendszerektől. Így a műveletekben érintett szervezetek együttműködésének, információcseréjének folyamatosan növekvő jelentőségű feltétele az informatikai rendszereik közötti jelentésmegőrző adatcsere, a rendszerek interoperabilitása.

Az információcsere-követelményeket kielégítő interoperábilis adatcsere megvalósítása a résztvevők heterogén informatikai rendszerei között jelentős tervezési, fejlesztési és alkalmazói feladatokat igényel. A NATO esetében az interoperabilitási követelményeket a Szövetségi Műveleti Hálózat (Future Mission Networking, FMN) program 2-3 évente megjelenő továbbfejlesztett és új dokumentumai, eljárási és szolgáltatási utasításai[2] tartalmazzák. A katonai informatikai rendszerek fejlesztése, interoperabilitási képességeik megvalósítása és fenntartása ezen utasítások figyelembevételével történik. Az interoperábilis katonai informatikai rendszerek hardver- és szoftvertechnológiájára, architekturális felépítésére az FMN nem tartalmaz előírásokat, kizárólag az együttműködő rendszerekkel megvalósított interfészeiket specifikálja, ezen belül is meghatározva kötelező és választható funkciókat, képességeket.

Az FMN követelményeknek megfelelő katonai informatikai rendszerek beszerzése, fejlesztése és továbbfejlesztése egymástól függetlenül folyik a NATO vagy az érintett

[2] Federated Mission Networking (FMN) Procedural Instructions, Service Instructions.

haderő mint megrendelő követelményeinek megfelelő módon. Minden informatikai rendszerfejlesztés alapvető követelményei közé tartozik a karbantarthatóság és továbbfejleszthetőség, valamint a gazdaságosság. Az ezeknek való megfelelést különböző szoftverfejlesztési megközelítések, módszertanok támogatják. Ezek egyike a komponensalapú szoftverfejlesztés,[3] amely újrafelhasználható komponensek széles körű alkalmazására épül.

Egy korábbi publikáció már vizsgálta az újrafelhasználható komponensek katonai informatikai rendszerekben való alkalmazásának alapjait (indokait, feltételeit, lehetőségeit).[4] Végrehajtott kutatásaim és megszerzett informatikai rendszerfejlesztési gyakorlati tapasztalataim azt mutatják, hogy a fejlesztő szervezetek számára a speciális katonai funkciók esetében nem állnak rendelkezésre újrafelhasználható interoperabilitási komponensek, ilyeneket nem tudnak átvenni és beépíteni a fejlesztés, továbbfejlesztés alatt álló rendszerekbe. Ez növeli a fejlesztések időtartamát és költségét, nehezíti az interoperabilitási képességek megvalósítását.

Alkalmazásuk nyilvánvalónak tűnő előnyei ellenére a katonai szakirodalomban nem találtam az újrafelhasználható interoperabilitási komponensek kérdéseivel foglalkozó publikációkat. Jelen publikációban ezt a hiányt próbálom részben csökkenteni. Alapvető célom annak a hipotézisnek az igazolása, hogy annak a ténynek, hogy az FMN követelményeknek megfelelő katonai informatikai rendszerek fejlesztéséhez nem állnak rendelkezésre speciális katonai funkciókat megvalósítható újrafelhasználható interoperabilitási komponensek, nem az az oka, hogy nincsenek olyan interoperabilitási funkciók, amelyek komponensalapú megvalósítása több fejlesztés során, akár széles körben is használható lenne. A tényleges okok meghatározása további kutatás tárgyát kell képezze.

A fenti cél érdekében a következőkben az újrafelhasználható interoperabilitási komponensekhez kapcsolódóan összegzem fogalmi alapjaikat, meghatározom főbb típusaikat, és mindezt összevetem a legfontosabb kapcsolódó NATO-szabályozókban, -dokumentumokban foglaltakkal, illetve részletesen elemzem a főbb típusokat, meghatározom, hogy melyek lehetnének széles körben használatosak.

A NATO FMN követelmények megvalósítását támogató újrafelhasználható komponensek alapjai

Kutatási célom elérésének megalapozásához elsőként összegzem az újrafelhasználható szoftverkomponensek fogalmi alapjait, értelmezését, ezt követően meghatározom az interoperabilitási komponensek körét meghatározó legfontosabb tényezőket, majd ezek alapján meghatározom az interoperabilitási komponensek körét, fő típusait, és elemzem, hogy ezek közül melyek lehetnek újrafelhasználhatók. Végül az általános szintű eredményeket összevetem a releváns NATO-szabályozókban, -dokumentumokban foglaltakkal.

[3] Component Based Software Engineering (CBSE), Component Based Development (CBD).
[4] Munk 2015.

Újrafelhasználható szoftverkomponensek alapjai

Kutatási témám középpontjában az újrafelhasználható szoftverkomponens áll, amely a komponensalapú szoftverfejlesztés egyik alapfogalma. A következőkben a szakirodalom alapján meghatározom a fogalom általam használt értelmezését, összegzem szerepét és jelentőségét, valamint bemutatom témám szempontjából legfontosabb jellemzőit.

A széles körben használt definíció szerint a *szoftverkomponens* „egy kompozíciós egység, aminek egyeztetett interfészei és konkrétan meghatározott környezeti függőségei vannak. A szoftver komponens önállóan telepíthető és felhasználható."[5] Egy másik, a dolgok internete témakörhöz kapcsolódó definíció szerint a *komponens* „egy rendszer moduláris, telepíthető és cserélhető része, amely magában foglalja a megvalósítást és egy sor interfészt ad közre".[6]

Az UML modellező nyelv specifikációja[7] szerint a komponens egy rendszer moduláris része, amely meghatározott funkciót valósít meg, szolgáltatást nyújt. Szolgáltatásai pontosan specifikált interfészeken keresztül érhetők el, és más komponensek szolgáltatásait is (amennyiben vannak ilyenek) ilyen interfészeken veszi igénybe. A komponens önálló, helyettesíthető egység, amely tervezési és futási időben is lecserélhető egy másik komponensre, amely kompatibilis interfészeken keresztül egyenértékű szolgáltatást nyújt.

Egy szoftverkomponens egy vagy több objektumorientált objektumtípust (osztályt) és kapcsolódó adatokat tartalmazó, egy adott platformhoz, infrastruktúrához kapcsolódó, azon telepíthető és működtethető bináris szoftvertermék. Napjaink két legszélesebb körben elterjedt platformja a .NET platform és az Enterprise Java Beans szerveroldali komponens infrastruktúra. Ennek megfelelően a szoftverkomponensek lehetnek például Nuget vagy JavaBeans csomagok.

Mivel a szoftverkomponens fogalma a legtöbb esetben már magában foglalja annak újrafelhasználhatóságát, így jelen publikációban újrafelhasználható szoftverkomponens alatt egy adott platformon telepíthető és működtethető bináris szoftverterméket értek, amelynek szolgáltatásai meghatározott interfész[ek]en keresztül érhetők el, és a továbbiakban – ahol az elegendő – röviden a szoftverkomponens kifejezést is használom.

Az *újrafelhasználható szoftverkomponensek alkalmazásának előnye,* hogy növeli a szoftverfejlesztés termelékenységét, csökkenti a fejlesztési időt és költségeket, javítja a szoftverrendszerek minőségét és megbízhatóságát. Ezzel egy időben a befektetett tervezői-fejlesztői tudás gazdaságosabb hasznosulását is eredményezi, csökkenti ugyanazon képességek újból és újbóli megvalósításának szükségességét, ami lehetővé teszi, hogy a fejlesztési kapacitások az új képességek, funkciók megvalósítására összpontosulhassanak.

A szoftverkomponensek újrafelhasználhatósága jelentős mértékben függ a *rendelkezésre bocsátott funkciók szoftverkomponensekre tagolásától*, attól, hogy mely

[5] Szyperski–Gruntz–Murer 2002: 41.
[6] Electropedia 741-01-11.
[7] *OMG Unified Modeling Language, Version 2.5.1* 2017: 209.

objektumtípusok, adatok kerülnek egy komponensbe és melyek külön komponensekbe. Ehhez kapcsolódóan a szakirodalomban több tervezési irányelvet fogalmaztak meg, amelyek közül témámhoz kapcsolódóan két irányelvet emelek ki:[8]

- közös újrafelhasználás [common reuse] – csoportosítás felhasználói szempontok alapján: egy komponensbe azok az objektumtípusok kerüljenek, amelyeket közösen használnak fel; a komponensben ne legyenek objektumtípusok, amelyeket egyes felhasználók nem használnak; ha egy objektumtípust a felhasználó önállóan is használhat, külön komponensbe kell kerüljön;
- közös lezárás [common closure] – csoportosítás karbantartási szempontok alapján: egy komponensbe azok az objektumtípusok kerüljenek, amelyeket valószínűleg azonos okok miatt ugyanakkor kell módosítani; a követelmények változása lehetőleg csak egy komponens módosítását igényelje.

Interoperabilitási komponenseket meghatározó tényezők

Az interoperabilitási komponensek egy informatikai rendszer azon szoftverkomponensei, amelyek az informatikai képességeket biztosító funkciókat valósítják meg. Fő típusaik definiálásához először összegzem az informatikai képességeket meghatározó követelmények tartalmát és formáját, majd pedig az interoperabilitási komponenseket meghatározó legfontosabb tényezőket.

Az *interoperabilitási képesség* azt jelenti, hogy az informatikai rendszer eleget tesz egy vagy több interoperabilitási követelményrendszernek, képes annak előírásai szerint adatokat cserélni (küldeni és fogadni) más, a követelményrendszernek megfelelő informatikai rendszerrel. Az interoperabilitási követelmények interoperabilitási profilok formájában fogalmazhatók meg, a követelménynek megfelelő interoperábilis adatcsere-szolgáltatás interoperabilitási pontokon keresztül valósul meg.

A *profil* az ISO értelmezése szerint egy vagy több alapszabvány, vagy szabványos profil együttese, kiemelve szabvány részhalmazokat, meghatározva választható lehetőségeket és paramétereket.[9] A NATO C3 Board Interoperabilitási Profil Képesség Csoportja a fogalom tartalmát kibővítette a NATO architekturális nézetekre (köztük például képességkövetelményekre), protokollokra, megvalósítási lehetőségekre, technikai szabványokra és szolgáltatásinteroperabilitási pontokra vonatkozó összetevőkkel.

Az interoperabilitási követelményeket a NATO informatikai rendszerek esetében *szolgáltatás interfész profilok* (*service interface profile,* SIP) tartalmazzák, amelyek interoperabilitási szolgáltatások esetében szabványok specifikus használatát határozzák meg egy adott szolgáltatásinteroperabilitási ponton, adott körülmények között. A *szolgáltatásinteroperabilitási pont* (*service interoperability point,* SIOP) egy referenciapont egy architektúrán belül, ahol egy vagy több szolgáltatásinterfész fizikailag vagy logikailag összekapcsolódik.[10]

[8] Noback 2015 alapján.
[9] ISO/IEC TR 10000, 3.1.4.
[10] NISP 2.2.

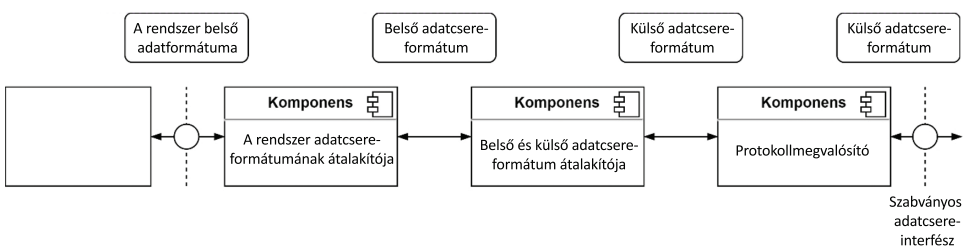
Az interoperabilitási profilban meghatározott követelmények két legfontosabb összetevője az együttműködő rendszerek közötti adatcserére használt protokoll és a cserélt adatok formátuma (külső adatcsere-formátum).

A *protokoll* funkcionális egységek kommunikáció során mutatott viselkedését meghatározó szabályok együttese.[11] Alapvetően annak meghatározása, hogy egy funkcionális egység (esetünkben egy informatikai rendszer vagy annak egy összetevője) milyen feltételek mellett, milyen adatokat, milyen úton küld partnerének, és azokra vár-e választ, illetve a partnere által küldött adatokra küld-e választ, milyen adatokat, milyen feltételek mellett és milyen úton. Az adatok cseréje az online mellett történhet offline módon is (például fájlcsereprotokollok).

Az interoperabilitási profilokban az adatcsere-protokollokat jellemzően alacsonyabb szintű protokollokra, azok specifikációira építve írják le. Ez utóbbiak között a katonai informatikai rendszerek esetében kiemelt szerepet töltenek be a TCP, UDP, HTTP és SOAP protokollok, vagy a HTTP protokollra épülő REST megoldás.

A *külső adatcsere-formátum* a partnerrel folytatott adatcsere előírt formátuma, amely legalacsonyabb szinten bitsorozatokat (esetleg bitfolyamokat) jelent. Az interoperabilitási profilokban az adatcsere-formátum napjainkban legtöbb esetben magasabb szinten, elsősorban a strukturált és félig strukturált adatok reprezentációjára (szinte kizárólagosan XML vagy JSON formátumokra) építve van meghatározva. Az informatikai rendszerekben a külső adatcsere-formátumot a használt programnyelv (C#, Java, C++ stb.) elemi és összetett adattípusaival leírt belső adatcsere-formátumban, modellben használják fel.

Egy *informatikai rendszer által használt belső adatformátum* elvileg lehetne egy interoperabilitási profil által meghatározott adatformátum (annak az alkalmazott programozási nyelvnek megfelelő modellje), ez azonban a gyakorlatban szinte lehetetlen. A használt belső adatformátummal szemben támasztott legfontosabb követelmény, hogy feleljen meg a rendszer funkciói, felhasználói által meghatározott – elsősorban tartalmi, valamint strukturális – követelményeknek. Mivel a külső adatcsere-formátumot egy sokkal szélesebb alkalmazói kör adatcsereigényei alapján alakítják ki és szabványosítják, ritka esetektől eltekintve nem fog megfelelni az adott rendszer követelményeinek.



1. ábra: Interoperabilitási komponensek típusai
Forrás: a szerző szerkesztése

[11] ISO/IEC 2382:2015.

Emellett a külső adatcsere-formátumoknak az idők során új változataik jelennek meg, eltérő tartalommal, így a korábban még megegyező belső adatformátum már nem fog azokkal megegyezni.

Végül az is gyakran előfordul, hogy egy informatikai rendszerhez később kell kialakítani egy új interoperabilitási képességet, amelynek belső adatcsere-formátuma eltér a rendszer már alkalmazott belső adatformátumától.

Interoperabilitási komponensek fő típusai, újrafelhasználhatósága

Az interoperabilitási komponens típusai hierarchikus struktúrába, ezen belül az előző pontban foglaltak alapján a komponensek két fő csoportba sorolhatók. Az első csoportot az interoperábilis adatcsere-protokollt megvalósító, a másodikat az adatformátumok közötti átalakításokat végző komponensek alkotják. A következőkben ezek alapjait körvonalazom, majd meghatározom, hogy közülük melyek lehetnek újrafelhasználhatók és melyek nem.

Az *adatcsere-protokollt megvalósító komponensek* felhasználóik számára biztosítják az adott protokollra épülő kapcsolat konfigurálását, a protokollnak megfelelő adatcsere-funkciók végrehajtását és szükség esetén a kapcsolat hiba utáni helyreállítását. Az adatcsere-protokollokban az érintett felek eltérő szerepet töltenek be (lehetnek adatszolgáltatók vagy adatfelhasználók), ennek megfelelően a protokollt megvalósító komponenseknek is két egymástól eltérő altípusuk van.

Egy adott protokollhoz több okból is tartozhatnak különböző komponensaltípusok. Eltérő protokollverziók funkcióit önálló protokollverzió-komponensek valósítják meg. Összetett protokollok esetében lehetséges az egységes komponens-alapképességeket és egyes kiegészítő képességeket megvalósító komponensekre tagolása is. Ezzel biztosítható, hogy a felhasználók csak olyan komponens[eke]t használjanak, amely[ek] funkcióira ténylegesen szükségük van.

Ahogy korábban is megállapítottuk, a felhasználók számára hasznos protokollok szinte mindig alacsonyabb szintű protokollokra épülnek, ennek megfelelően a protokollt megvalósító komponensek más komponensek szolgáltatásaira épülnek.

Az *adatformátumok közötti átalakítást megvalósító komponensek* szükségessége az eltérő adatformátumok létéből következik. Ezek közé felső szinten az adott rendszer által alkalmazott belső adatformátum és a protokoll adatcsere-formátumának belső modellje, valamint a belső modell és a külső adatcsere-formátum közötti átalakítást (szerializációt, deszerializációt) megvalósító komponensek tartoznak.

Az adatcsere irányától függően mindkét formátumátalakító komponenstípusból szükség van egy adatküldés és egy adatfogadás során felhasznált önálló komponensre. Az egyes protokollok különböző verzióihoz tartozhatnak, többnyire tartoznak is eltérő külső adatcsere-formátumok, ezekhez eltérő belső modellek tartoznak és így új, eltérő rendszer belső adatformátuma – belső adatcsere-formátum közötti átalakítást végző komponensekre is szükség van.

A különböző adatformátumokban és adatcsere-formátumokban lehetnek azonos tartalmú, de eltérő formátumú adatösszetevők (elsősorban adatelemek). Ilyenek lehetnek többek között mennyiségi jellemzőket (hossz, idő, sebesség stb.), földrajzi

helyet azonosító koordinátákat, szabványos szimbólumkódokat vagy biztonsági megjelöléseket tartalmazó adatösszetevők. Ezek esetében létrehozhatók és széles körben felhasználhatók *adatelem-formátumok közötti átalakítást megvalósító komponensek*.

A feltárt komponensek közül egyeseket nem érintenek a különböző informatikai rendszerek sajátosságai, másokat viszont igen. Az előbbiek így újrafelhasználhatók, az utóbbiak viszont nem.

A felsoroltak közül az *újrafelhasználható interoperabilitási komponensek közé tartoznak* az adatcsere-protokollt, valamint a belső és külső adatcsere-formátum közötti átalakítást megvalósító komponensek. Ezek ugyanis kizárólag az interoperabilitási profilban foglalt követelményeknek kell megfeleljenek.

Ezzel szemben a rendszer belső adatformátuma és a belső adatcsere-formátum közötti átalakítást megvalósító komponenseket – saját adatformátumuk ismeretében, attól függő módon – az adott rendszerek fejlesztésének részeként egyedi módon kell létrehozni. Ennek során azonban felhasználhatók azonos tartalmú adatösszetevők között átalakítást megvalósító újrafelhasználható komponensek.

Interoperabilitási komponensek és a NATO-dokumentumok

Az interoperabilitási komponensek vizsgálatához több NATO-szabályozó, -dokumentum is tartalmaz felhasználható információkat. Ezek közé tartoznak elsősorban a Szövetségi Műveleti Hálózat utasításai, illetve a NATO C3 Taxonómia és a NATO Interoperabilitási Szabványok és Profilok. A következőkben röviden összegzem ezek témám szempontjából fontos információit.

A *Szövetségi Műveleti Hálózat* (Federated Mission Networking, FMN) egy központilag szabályozott NATO-keretrendszer szövetségi műveleteket támogató informatikai hálózatok tervezéséhez, előkészítéséhez, létrehozásához, használatához és megszüntetéséhez.

Az FMN jövőkép egyik alapelve a költséghatékonyság és maximális újrafelhasználás: amennyire csak lehetséges, létező, egyeztetett szabványok, képességek, közös beszerzések, szolgáltatásiszint-megállapodások és szervezeti struktúrák használata. Ez egyértelműen indokolja az újrafelhasználható komponensek alkalmazását.

A jövőkép másik alapelve a fokozatos megvalósítás: az interoperabilitási képességek műveleti követelményekhez és technikai lehetőségekhez igazodó megvalósítása, egymásra épülő „spirálokban". Az egymásra épülő spirálok képességkövetelményeit eljárási és szolgáltatási utasítások tartalmazzák. A két év alatt kidolgozott specifikációkat négy évvel később egy éven keresztül újonnan megjelenő *(emerging),* majd két évig javasolt *(preferred)* megoldásként alkalmazzák műveletekben. A 2016-ban elkészült Spiral 1 specifikáció hat műveleti és 11 szolgáltatási utasítást tartalmazott. A 2023-ban kiadott Spiral 5 már 18 műveleti és 26 szolgáltatási utasítást foglal magában.

A technikai jellegű interoperabilitási követelményeket tartalmazó FMN szolgáltatási utasítások alapvető szerepet játszanak a katonai, ezen belül a NATO-alkalmazás újrafelhasználható interoperabilitási komponensei körének, lehetőségeinek meghatározásában.

A *NATO C3 Taxonómia*[12] a NATO C3 képességek fejlesztési folyamatait támogató termék, amely közös referenciát képez a képességarchitektúrák tervezéséhez. A taxonómia, a nevéből következően, fogalmak és meghatározásaik hierarchikus osztályozása, amely az 5.0 verzióig egyetlen átfogó taxonómia volt.

Az aktuális 6.0 verzió már hat önálló taxonómiát tartalmaz, amelyek köre a tervek szerint a későbbiekben kilencre fog bővülni. Az önálló taxonómiák közé a képességek, a szervezeti folyamatok, a szervezeti szerepkörök, az információs termékek, a felhasználói alkalmazások, az alkalmazási területi[13] szolgáltatások, az alapszolgáltatások, a kommunikációs szolgáltatások és az eszközök, berendezések taxonómiái fognak tartozni.

Az alkalmazási területi szolgáltatások és alapszolgáltatások a fogalmi osztályozás mellett egy megvalósítási hierarchiát is jelentenek. A több alkalmazási területet támogató, közös funkcionalitást megvalósító szolgáltatásokat az alkalmazásiterület-specifikus szolgáltatások használják fel működésük során.

Témám szempontjából kiemelt szerepe az *alapszolgáltatások taxonómiájának*[14] van, amely három főcsoportot – általános célú támogató szolgáltatásokat, platformszolgáltatásokat és infrastruktúra-szolgáltatásokat – tartalmaz.[15]

Az általános célú támogató alapszolgáltatások (biztonsági, felügyeleti, információcsere és együttműködési, szervezeti erőforrás-kezelési, térinformatikai, információmenedzsment és adatelemzési) alkalmazási területtől független szolgáltatásokat nyújtanak közvetlenül a felhasználók számára, de felhasználhatók alkalmazásiterület-specifikus szolgáltatásokban.

A platform-alapszolgáltatások hálózaton keresztül együttműködő szolgáltatások számára nyújtanak szolgáltatásokat (biztonsági, felügyeleti, üzenetorientált köztes réteg, webszolgáltatásokhoz kapcsolódó, adathozzáférési, kompozíciós, mediációs szolgáltatások). Ezek a felhőalapú informatika második szintjébe (Platform as a Service, PaaS) tartoznak.

Végül az infrastruktúra-alapszolgáltatások a szolgáltatások legalsó rétegét képezik, amelyek minden magasabb szintű szolgáltatás számára (biztonsági, felügyeleti, feldolgozási, tárolási, hálózati) nyújtanak szolgáltatásokat. Ezek a felhőalapú informatika alsó szintjének (*infrastructure as a service,* IaaS) részét képezik.

Az alapszolgáltatásokon belül a platformszolgáltatások között szerepelnek a *mediációs szolgáltatások (mediation services),* amelyek egymással nem kompatibilis információszolgáltatók és információfelhasználók közötti köztesréteg-szolgáltatások. A mediációs szolgáltatások „feldolgozzák az információszolgáltató által nyújtott adatokat és átalakítják olyan formátumra, ami érthető az információfelhasználó számára. Ezzel áthidalják a két fél közötti szakadékot, lehetővé teszik köztük az információcserét, ami korábban nem volt lehetséges."[16]

A mediációs szolgáltatások első csoportját a taxonómiában a protokollátalakító szolgáltatások *(protocol transformation services)* alkotják, amelyek módosítják a két

[12] *C3 Taxonomy Baseline 6* 2022.
[13] Community of Interest (COI) Services.
[14] *C3 Taxonomy Baseline 6. Taxonomy of C3 Core Services* 2022.
[15] Ezek jelentős hasonlóságot mutatnak a felhőalapú informatika három szolgáltatástípusával: szoftver mint szolgáltatás (SaaS), platform mint szolgáltatás (PaaS) és infrastruktúra mint szolgáltatás (IaaS).
[16] *C3 Taxonomy Baseline 6. Taxonomy of C3 Core Services* 2022: 24.

fél közötti adatcsere módját. Lehetővé teszik, hogy az információszolgáltatók és -felhasználók eltérő protokollokat használjanak. A protokollátalakító szolgáltatások átjáró típusú funkciókat biztosítanak, eltérő protokollokat használó hálózatokat kapcsolnak össze. Így nem egyeznek meg a korábbiakban meghatározott protokollmegvalósító komponensek által nyújtott szolgáltatásokkal.

A mediációs szolgáltatások második csoportjába az adatformátum-átalakító szolgáltatások *(data format transformation services)* tartoznak, amelyek nevüknek megfelelően azonos információtartalom különböző adatreprezentációi közötti jelentésmegőrző átalakításokat valósítanak meg. Ezek a szolgáltatások megegyeznek a korábban meghatározott adatformátumok közötti, illetve adatösszetevő formátumok közötti átalakítást megvalósító komponensek által nyújtott szolgáltatásokkal.

A C3 Taxonómiában szereplő valamennyi szolgáltatáshoz készülhet újrafelhasználható komponens, mivel ez utóbbi nem más, mint egy egyeztetett funkcionalitás pontosan specifikált interfészen keresztül elérhető, ismeretlen belső tartalmú megvalósítása.

A *NATO Interoperabilitási Szabványok és Profilok* (NISP) az interoperabilitási követelmények elérését biztosító szabványok és interoperabilitási profilok központilag kezelt katalógusa. A katalógus tartalmaz NATO- és nem NATO-szabványokat és profilokat (utóbbiakat létrehozó szervezeteik felügyelik). Ezek lehetnek kötelező vagy jelölt típusúak, ez utóbbiak projekttervezési és -tesztelési célokat szolgálnak, idővel átkerülhetnek a kötelezők közé. A dokumentumot 2023-ig hagyományos dokumentum formájában adták ki.[17] 2024-től a katalógus már elektronikus formában, egy speciális Tidepedia[18] wikin érhető el.

Az új változat alapelemei a szabványok, amelyekhez profilok kapcsolódnak. A profilok profilcsoportokba tartoznak, és a NATO C3 Taxonómia szolgáltatási területeihez (a taxonómiaalkalmazási területi szolgáltatások, az alapszolgáltatások, a kommunikációs szolgáltatások alacsonyabb szintű összetevőihez) kapcsolódnak. Ezzel teljessé vált a C3 Taxonómia és az NISP közötti összhang. A katalógus a taxonómiánál részletesebb információkat tartalmaz az újrafelhasználható interoperabilitási komponensek körének meghatározásához.

Újrafelhasználható interoperabilitási komponensek típusai

Az előző pontban meghatároztam az újrafelhasználható interoperabilitási komponensek fő csoportjait: adatcsere-protokollt megvalósító és adatformátumok közötti átalakítást megvalósító komponensek. Jelen pontban sorra veszem ezeket a csoportokat, és feltárom, hogy mely funkciókat, szolgáltatásokat megvalósító komponensek lehetnének szélesebb körben is használatosak. Ezt követően egy harmadik, önálló csoportként vizsgálom meg az egyes, a katonai informatikai rendszerekben széles körben használatos adatelem-átalakítási funkciókat megvalósító komponensek lehetőségeit.

[17] *ADatP-34* 2023.

[18] A NATO Allied Command Atlantic által támogatott kezdeményezés (Technology for Information, Decision and Execution Superiority, TIDE) korlátozott hozzáférésű online platformja.

Protokollmegvalósító komponensek

Egy adott interoperabilitási profilnak megfelelő protokollt megvalósító komponensek a partner informatikai rendszerekkel együttműködő valamennyi informatikai rendszer alapvető összetevőit képezik. Ezek napjainkban a gyakorlatban legalacsonyabb szinten[19] mindig szabványosított protokollokra (IP, TCP, UDP) épülnek, amelyekhez rendelkezésre állnak szabadon hozzáférhető megoldások, felhasználható összetevők. Erre a rétegre – több szinten – számos olyan alkalmazásiréteg-szintű protokoll épül (HTTP, REST, SOAP), amelyek szintén széles körben használatosak, és amelyekhez szintén elérhetők hozzáférhető összetevők.

A következőkben a rendelkezésre álló, (újra)felhasználható komponenseket természetesen nem vizsgálom, ezeket adottnak tekintem. Ezeket egyébként az interoperabilitási profilok is felhasználják, építve rájuk (mint profilokra), legfeljebb pontosítva, korlátozva egyes jellemzőiket, funkcióikat. Ezért vizsgálataimat az FMN követelményekben szereplő olyan protokollokra szűkítem, amelyek az előbbiekben említett protokollokra építve egyedi, speciális katonai megoldást valósítanak meg, és az őket megvalósító komponensek újrafelhasználható formában nem állnak rendelkezésre.

Elsőként nézzük meg, mely protokollok szerepelnek az *FMN szolgáltatási utasításokban*. A végleges Spiral 3, Spiral 4 és Spiral 5 specifikációk 20, 22 és 23 szolgáltatási utasítást tartalmaznak. Ezek többsége civil szabványokra épül, speciális katonai alkalmazású protokoll esetükben nem szerepel. A szolgáltatási utasítások NATO-szabványosítási dokumentumokra hivatkoznak, egy dokumentum több protokoll specifikációját is tartalmazhatja. Így a következő listában összesen 17 protokoll található.

1. táblázat: Speciális katonai protokollok az FMN Spiral 3, 4 és 5 szolgáltatási utasításokban

Szolgáltatási terület	**Szabályozó dokumentum**	**Év**	**Spiral**			**Protokoll**	**Felhasznált protokoll**
			3	4	5		
Szárazföldi vezetési információcsere	MIP 3.1 MTIDP	2012	x	–	–	DEM, MEM	TCP, SMTP
	MIP4 IES 4.3	2020	–	x	–	MIP4 IES Request/Response, Polling	WSMP
	MIP4 IES 4.4	2023	–	–	x	MIP4 IES Request/Response, Polling	REST
Szárazföldi harcászati vezetési információcsere	AEP-76(A)(2) Volume IV	2017	–	x	–	JDSSIN IEM	UDP
	AEP-76(A)(3) Volume IV	2023	–	–	x	JDSSIN IEM	UDP

[19] A nyílt rendszerek összekapcsolása (OSI) modell hálózati és szállítási rétegei.

Szolgáltatási terület	Szabályozó dokumentum	Év	Spiral			Protokoll	Felhasznált protokoll
Haditengerészeti vezetési információcsere	OTH-GOLD 2000 (US)	2000	–	x	x	OTH-GOLD	TCP
	OTH-GOLD 2007 (US)	2007	–	x	x	OTH-GOLD	TCP
Összhaderőnemi felderítő információcsere	AEDP-17(A)(1)	2018	x	–	–	CSD Querying, Publishing	SOAP
	AEDP-18(A)(1)	2018	–	x	x	CSD Streaming	SOAP
Tűztámogató információcsere	ASCA-012	2021	–	–	x	ASCA	IP
Sajáterő-nyomkövetés	ADatP-36(A)(1)	2017	x	–	–	IP1, IP2, SIP3	TCP, UDP, SOAP,
	ADatP-36(A)(2)	2021	–	x	x	IP1, IP2, SIP3, FFT WSMP Request/Response, Polling	TCP, UDP, SOAP, WSMP
	ADatP-36(B)(1) draft	2021	–	–	x	IP1, IP2, FFT WSMP Request/Response, Polling	TCP, UDP, WSMP
„Térképvázlat-elosztás (képelosztás)"	NVG 1.5 (TIDE)	2012	x	–	–	NVG Request/ Response	SOAP
	NVG 2.0.2 (TIDE)	2022	–	x	–	NVG Request/ Response, Streaming	SOAP
	ADatP-4733 draft	2023	–	–	–	NVG Request/ Response, Streaming	REST

Megjegyzés: A hivatkozott szolgáltatási utasítások: FMN Service Instructions for Land C2 Information Exchange; FMN Service Instructions for Land Tactical C2 Information Exchange; FMN Service Instructions for Maritime C2 Information Exchange; FMN Service Instructions for Joint ISR Information Exchange; FMN Service Instructions for Fires Information Exchange; FMN Service Instructions for Friendly Force Tracking; FMN Service Instructions for Overlay Distribution (Picture Distribution)

Forrás: a szerző szerkesztése

A felsoroltak közül *a Magyar Honvédség számára* is kiemelt jelentőségűek a szárazföldi vezetési információk cseréjét, a sajáterő-nyomkövetést, a térképvázlatok (különböző helyzetképek és tervösszetevők) cseréjét, valamint a digitális katonai képességhez kapcsolódó szárazföldi harcászati információcserét megvalósító protokollok. Ezek a fejlesztés alatt álló HUNTACCIS tábori vezetési és irányítási (C2) rendszernek is részét képezik. Ezeken kívül már jelenleg is szükség lenne az összhaderőnemi felderítő és a közeljövőben a tűztámogató információcsere képességet támogató protokollokra.

Az FMN szolgáltatási utasításokban meghatározott *protokollokat megvalósító komponensek újrafelhasználhatósága* lényegükből következik. Egy interoperabilitási

profil lényege ugyanis pontosan az, hogy minden együttműködő számára egyértelműen, azonos módon meghatározza a megvalósítandó protokoll (üzenetcsere) folyamatát, rendjét és az üzenetek tartalmát, formátumát (amelynek egy része, az átvivendő adat [payload] lehet tetszőleges vagy csak minimálisan korlátozott). Így a protokollt megvalósító komponens által biztosított interfész (paraméterek és funkciók), mindenki számára azonos. Mivel a speciális protokollok önálló fejlesztési kapacitási igénye protokollonként 12–24 vagy ennél is több emberhónap, ez újrafelhasználható komponensek beépítésével szinte teljes egészében megspórolható lehet.

Mivel a protokollok felhasználóspecifikus jellemzőket, funkciókat nem – legfeljebb választható funkciókat – tartalmaznak, a fejlesztendő katonai informatikai rendszerek egyetlen komponens formájában megvalósított protokoll esetében esetleg annak nem minden funkcióját használják fel, vagy több komponens formájában megvalósított protokoll esetében azok közül csak a számukra szükséges komponenseket használják fel.

Az 1. táblázatban nem szerepelnek a *fájlcsere alapú protokollok,* amelyek több alkalmazási területi információcsere-szabályozó dokumentumban megtalálhatók. Ezek lényege, hogy a partnerek között cserélendő adatokat külső adatcsere-formátumban kimentik fájl formájában, ezt valamilyen módon továbbítják a partnereknek, amelyek azt beolvasva veszik át az adatokat. A fájlok továbbításának módját a szabályozó dokumentumokban általában nem határozzák meg, az együttműködő partnerek számára rendelkezésre álló lehetőségek közül választják ki. Ilyen lehet például elektronikus levél mellékleteként, fájlkiszolgálón történő megosztás segítségével, HTTP URL-lel elérhető módon, vagy például azonnali üzenetküldő alkalmazás[20] fájlátviteli funkciójával. A fájlcsere lehetőségek mindegyikéhez készíthető újrafelhasználható komponens, amely a felhasznált alacsonyabb szintű protokollra (SMTP, FTP, HTTP, XMPP) építve nyújtja szolgáltatásait.

Adatformátum-átalakító komponensek

Egy interoperabilitási profilban specifikált külső – napjainkban elsősorban XML vagy JSON, de elvileg bármely más karakter- vagy bitorientált – adatcsere-formátum és annak belső, az alkalmazott programnyelven megvalósított modellje (adatstruktúra) közötti átalakítás (a szerializáció és deszerializáció) a partnerrendszerekkel együttműködő valamennyi informatikai rendszer megkerülhetetlen összetevője. Rendeltetésük a partnereknek megküldendő adatok szabványos, előírt karakter- vagy bitsorozat-formátumának előállítása, illetve a partnerektől beérkező adatok szabványnak, előírásoknak való megfelelésének ellenőrzése és feldolgozásra alkalmas formára alakítása.

Jelen pontban először elemzem a belső adatcsere-formátum használatának előnyeit, majd megvizsgálom a külső adatcsere-formátum verzióinak létéből következő adatformátum-átalakítási igényeket. Végül meghatározom a belsőadatcsereformátum-verziók közötti átalakítások alapjait, jellemzőiket.

[20] Például Extensible Messaging and Presence Protocol (XMPP), kiterjesztett azonnali üzenetküldő („csevegő") és jelenlétjelző protokoll.

Elvileg *a külső adatcsere-formátum és a belső adatformátum közötti átalakítás közvetlenül* is megvalósítható. A saját informatikai rendszer összetevőinek nem kell tudniuk arról, nem is „érzékelik", hogy az általuk használt, a rendszer funkciói által meghatározott belső adatformátum és a külső adatcsere-formátum közötti átalakítás egy vagy két lépésben (egy belső adatcsere-formátum közbeiktatásával) történik.

A kétlépcsős megvalósítás indokát a programozás SOLID[21] tervezési alapelveinek egyike, az egyetlen felelősség elve adja. Az alapelv szerint egy összetevő egyetlen funkció megvalósításáért legyen felelős. A közvetlen átalakítás esetében viszont mind a belső adatformátum, mind a külső adatcsere-formátum változása az átalakítás módosítását igényli. Az átalakítás két részre bontásával a belső adatformátum átalakítása csak a belső adatformátum – belső adatcsere-formátum átalakítását érinti, a belső adatcsere-formátum – külső adatcsere-formátum közötti átalakítás érintetlen marad. Ez utóbbi így független lesz a rendszer által használt belső adatformátumtól, kizárólag a külső adatcsere-formátumtól fog függeni, éppen ez teremti meg a komponens újrafelhasználható jellegét.

Az egyes interoperabilitási protokollok alapvető jellemzője, hogy a felhasználói igényekhez alkalmazkodva *újabb verziók, új verziójú interoperabilitási profilok* jelennek meg.[22] Ezekben a protokoll működése mellett az alkalmazott külső adatcsere-formátumok is sokszor változnak.[23] A külső adatcsere-formátum változása (amennyiben a saját rendszer az új interoperabilitási profilnak is meg akar felelni) értelemszerűen szükségessé teszi a belső adatcsere-formátum új verzióinak létrehozását, valamint egy új adatformátum-átalakító komponens létrehozását.

A külső adatcsere-formátum új verziójának megjelenése a saját rendszer igényeitől függően hatással lehet a belső adatcsere-formátumra, szükségessé teheti annak módosítását (kibővítését új adatokkal, egyes adatok értékkészletének módosítását). Természetesen előfordulhat, hogy a saját rendszer – mivel az az interoperabilitási profil szerint nem kötelező – az új adatokat, azok új értékeit nem, vagy egyelőre még nem használja, és így ilyen adatokat partnereinek sem küld. Ebben az esetben a belső adatcsere-formátum módosítása szükségtelen, a rendszer az új interoperabilitási profil követelményeit így is kielégíti.

Amennyiben a rendszer belső adatformátumát módosítják, a visszafelé kompatibilitás érdekében (amíg ennek fenntartása saját cél, vagy külső követelmény) módosítani kell a meglévő belső adatformátum – korábbi verziójú belsőadatcsere-formátum-átalakító komponenseket is.

Egy rendszernek lehet átjáró típusú rendeltetése is, vagyis képessége arra, hogy egy adott protokoll segítségével adott külső adatcsere-formátumban beérkező adatot egy másik protokoll segítségével másik külső adatcsere-formátumban továbbítsa anélkül, hogy azt maga felhasználná, saját felhasználói számára rendelkezésre bocsátaná. Az átjáró képesség kapcsolódhat egy adott protokollhoz, amikor a funkció lényege az adott protokollhoz tartozó különböző verziójú külső adatcsere-formátumok

[21] Single responsibility, Open/closed, Liskov substitution, Interface segregation, Dependency inversion = egyetlen felelősség, nyílt/zárt, Liskov-féle helyettesítési, interfész-elválasztási és függőségmegfordítási alapelvek.

[22] FFT: ADatP-36(A)(1), ADatP-36(A)(2), ADatP-36(B)(1); MIP4: MIP4IES 4.0, 4.1, 4.2, 4.3, 4.4; NVG: 1.5, 2.0.2, ADatP-4733(A)(1); KML 2.0, 2.1, 2.2, 2.3; stb.

[23] FFT: NFFI, FFI-MTF-D; MIP4: MIM 1.0, 2.0, 3.x, 5.0, 5.1, 5.2, 5.3; NVG: 1.5, 2.0.2, ADatP-4733(A)(1) stb.

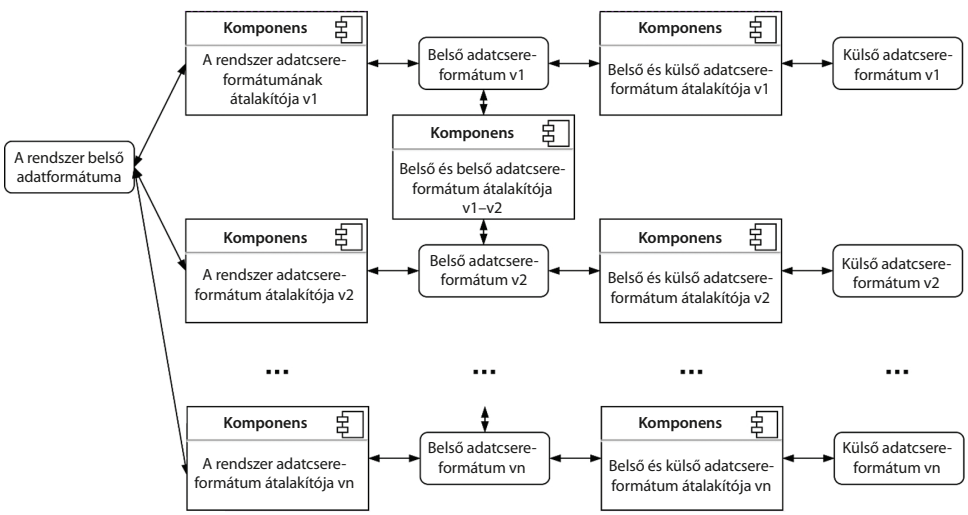
közötti átalakítás. Ehhez szükség van az eltérő verziók közötti átalakításokat végző komponensekre.

Amennyiben egy rendszer egy interoperabilitási protokoll több verzióját is támogatja, mindenképpen meg kell valósítania az adott profilokban meghatározott külső, illetve belső adatcsereformátum-verziók és a saját belső adatformátuma közötti átalakítást. Ennek segítségével elvileg a belső adatformátumon keresztül rendelkezésre állnak a belső adatcsere-formátumok közötti átalakítások is, azonban csak akkor, ha a belső adatformátum a belső adatcsere-formátumok valamennyi adatát teljes részletességgel, pontossággal átveszi, tartalmazza. Ez azonban nem feltétlenül van így, előfordulhat, hogy egy adott rendszernek nincs, vagy kevésbé részletesen, alacsonyabb pontossággal van szüksége egyes adatokra. Ebben az esetben szükség van önálló átalakító komponensre is.

A *belső adatcsere-formátum – belső adatcsereformátum-átalakító komponensek* specifikációja van, amikor szerepel az új protokollverzió specifikációjában[24] vagy egy verziók közötti átalakítást specifikáló hivatalos dokumentumban, de legtöbbször nem. Ennek hiányában a verziók közötti átalakítást az egyes rendszerek eltérő módon valósítják meg, az interoperabilitás teljes mértékben nem valósul meg.

Összességében tehát az újrafelhasználható adatformátum-átalakító komponenseknek a 2. ábrán látható módon két típusa lehetséges:

– belső adatcsere-formátum – külső adatcsere-formátum közötti átalakító;
– belső adatcsere-formátum – belső adatcsere-formátum közötti átalakító.



2. ábra: Adatformátum-átalakító komponensek
Forrás: a szerző szerkesztése

[24] Például ADatP-36(A)(2) Table 14 NFFI to FFI Mapping és Table 15 FFI MTF to NFFI Mapping.

Adatelemeket átalakító komponensek

Az eddig említett interoperabilitási – protokollmegvalósító és adatformátum-átalakító – komponensek mellett van még egy, önálló komponensek formájában megvalósítható funkció, amely az interoperabilitási képességek megteremtésében jelentős szerepet játszik: ez az adatelemek különböző formátumai közötti átalakítás.

Az interoperabilitási profilokban specifikált és az informatikai rendszerek által használt összetett adatstruktúrák, adatformátumok adatelemekből állnak, amelyek az adatformátumok átalakítása részeként maguk is átalakításra szorulhatnak. A helyzetképeket leíró térképvázlatok interoperabilitási szempontból kiemelt jelentőségű esetében ezek közé tartoznak többek között a szabványos szimbólumkódok, a földrajzi pozíciók leírásai vagy a különböző mérhető jellemzők (távolságok, mélységek, hosszúságok, időpontok, sebességek, irányok stb.).

A következőkben meghatározom az adatelem-átalakító komponensek értelmezését, legfontosabb jellemzőit, igazolom újrafelhasználható formájú megvalósításuk lehetőségét és röviden áttekintem néhány főbb típusukat. Az adatelem-átalakító komponensek széles körű, részletes vizsgálata annak terjedelme miatt önálló kutatást igényel.

Egy *adatelem-átalakító komponens* rendeltetése, hogy egy adott tartalmú jellemzőt egy vagy több adott formátumról egy vagy több másikra alakítson át. Az adatelemek lehetnek összetevői belső adatformátumnak (adatcsere-formátumnak) vagy külső adatcsere-formátumnak. Az első csoportba tartozók típusa az alkalmazott programnyelv adattípusai (numerikus, logikai, szöveges, ezekből felépülő összetett stb.) közül kerülhet ki, míg az utóbbi csoport adattípusa napjainkban jellemzően karakteres, de elvileg lehet bináris típus is.

Egy adatelem-átalakító komponens képességei alapvetően azt írják le, hogy az adott jellemző (például szimbólumkód, földrajzi hely, hossz stb.) milyen formátumai között képes átalakítást megvalósítani. Külső adatcsere-formátumok részét képező adatelemek esetében ezek a formátumok az interoperabilitási profilban, a kapcsolódó specifikációkban pontosan meg vannak határozva. Ez teszi lehetővé a megvalósítást újrafelhasználható komponensek formájában.

Az adatelem-átalakító komponensek megvalósíthatók egymásra, más komponensek szolgáltatásaira építve is. Így több komponens képességei integrálhatók egy komponensbe, ami a felhasználás könnyebbségét növeli. Ilyen esetben két formátum között új átalakítási képesség is kialakítható egy közbenső formátumon keresztüli átalakítással. Ez a megoldás azonban nem minden esetben tökéletes, mivel előfordulhat, hogy két adatelem-formátum (például szimbólumszabvány szerinti kód) között pontosabb közvetlen átalakítás lehetséges, mint egy közbenső formátumon keresztül. Ennek ellenére a közvetett megoldás is jobb, hasznos lehet alkalmazója számára, mint a saját fejlesztés.

A *szimbólumkódok* a katonai alkalmazásban széles körben használt térképvázlatokhoz *(overlay)* kapcsolódnak. Ezek olyan grafikus harci okmányok, amelyek rendeltetése

az aktuális helyzet, a különböző helyzetképek,[25] valamint a tervezett műveletek, azok különböző fázisai legfontosabb adatainak szabványos szimbólumokra épülő térképi alapú megjelenítése. A térképvázlat a műveleti szempontból jelentős harctéri objektumok helyzetét, főbb jellemzőit tartalmazza. A térképvázlat-elemek (szimbólumok, harctéri objektumok) interoperábilis cseréje katonai szimbólumszabványokban rögzített, szabványos szimbólumkódokkal azonosított szimbólumokkal történik.

A különböző külső adatcsere-formátumok egy szimbólum típusának cseréjére meghatározott – egy vagy több – szimbólumszabvány[26] szerinti kódokat használnak, a saját informatikai rendszer pedig belső használatra egy adott szimbólumszabvány szerinti kódot használ. Emiatt mind a belső adatcsere-formátum és a belső adatformátum, mind két belső adatcsere-formátum között szükség lehet és a gyakorlatban mindig szükség is van az azokban szereplő szimbólumkódadatok átalakítására egyik szabványról a másikra.

A szimbólumkód-átalakító komponensek megvalósítását megnehezíti, hogy a különböző szimbólumszabványok között nincsenek hivatalos leképezések. Ezek hiányában a szimbólumtípusok leképezése megnevezésük, szimbólumuk, esetleg a kapcsolódó rövid kiegészítő leírások alapján lehetséges. A leképezés során a pontos leképezés mellett lehetséges, hogy egy szimbólumkódhoz a másik szabványban csak egy általánosabb tartalmú szimbólumkód rendelhető, vagy nincs megfelelő szimbólumkód.[27] Így viszont az egyes rendszerek megvalósításai eltérhetnek, az interoperabilitás sérül. Újrafelhasználható szimbólumkód-átalakító komponens egységes használata esetén viszont az interoperabilitás biztosítható.

A *földrajzi pozíciók* szintén kiemelt szerepet játszanak a térképvázlatok cseréjében. A katonai alkalmazásban a földrajzi pozíciók megadhatók többek között földrajzi (szélességi és hosszúsági) koordinátákkal, vagy a Katonai Rács Referencia Rendszer[28] zónái és az azon belüli pozíció megadásával. A fenti megoldások épülhetnek eltérő vetületi rendszerekre,[29] így mind az egyes típusokon belül, mind a két típus között szükség lehet átalakításra. A bonyolult algoritmusokra épülő átalakítás megvalósítása újrafelhasználható formában mindenképpen célszerű.

A földrajzi pozíciók megadásához a koordináták mellett számos (például légierő vagy haditengerészeti) alkalmazás esetében szükség van a pont vertikális helyzetének (magasságának vagy mélységének) megadására is. Az adatcsere során ez számos különböző formában megadható,[30] például:

- a WGS84 ellipszoid felszínétől mért (pozitív vagy negatív) távolság;
- a földfelszín feletti magasság;

[25] Közös helyzetképek (Common Operational Picture) és azonosított helyzetképek (Recognized Ground Picture, Recognized Air Picture, Recognized Maritime Picture, Recognized Intelligence Picture, Recognized Logistic Picture stb.).

[26] APP-6(A), APP-6(B), APP-6(D), MIL-STD-2525B, MIL-STD-2525C, MIL-STD-2525D.

[27] Az adott szimbólumtípus a másik szabványra nem képezhető le, a szimbólum nem jeleníthető meg (például vezetési intézkedések [Control Measures], kibertéri szimbólumok stb.).

[28] Military Grid Reference System (MGRS).

[29] World Geodetic System 1984 (WGS84), Egységes Országos Vetület (EOV), korábban a Varsói Szerződés hadseregeiben a Gauss–Krüger-vetület.

[30] Például a katonai szimbólum szabványok X Altitude/Depth kiegészítő adata, vagy a Multilateral Interoperability Programme (MIP) Information Model (MIM) 5.2 adatmodell VerticalDistance adata.

- az átlagos tengerszint feletti magasság/alatti mélység;
- a légnyomás alapján meghatározott repülési magasság szintje.[31]

A fenti magasság-adatformátumok közötti átalakítás további adatok nélkül általában nem végezhető el. Szükség van a pozíció földrajzi koordinátáira, illetve a földfelszín, tengerszint WGS84-hez viszonyított magasságához az adott pozícióban. Ezért erre az átalakításra újrafelhasználható komponens csak korlátozott funkciókkal készíthető.

A helyzetképek a fentiekben már említettek mellett széles körben tartalmaznak a *harctéri objektumok mérhető tulajdonságait* leíró adatelemeket is, amelyek a különböző adatformátumokban különböző módon jelennek meg. Ezek közé tartoznak többek között a hosszúság- (szélesség, hosszúság, sugár, hatótávolság stb.), sebesség-, irány-, valamint időpontadatok. A különböző formátumú adatok közötti átalakítások megvalósítására alkalmazhatók újrafelhasználható komponensek.

A mérhetőtulajdonság-értékek lehetnek numerikus értékek, amelyek egy megadott, rögzített mértékegységben értendők, és lehetnek összetett formátumúak (mérőszám és mértékegység). Az adatcsere során ehhez kapcsolódhat harmadikként az érték pontossága is.

A hosszúságadatok megadása legtöbbször méterben történik, de a katonai alkalmazásban előfordul a lábban, kilométerben, angol mérföldben, tengeri mérföldben mért hosszúság is.

A sebességadatok katonai alkalmazásban használatos mértékegységei a kilométer/óra, méter/másodperc, mérföld/óra, valamint a csomó (tengeri mérföld/óra).

Az irányadatok egy adott alapirányhoz mért, az óramutató járásával megegyező irányszöget jelentenek. Az alapirány háromféle is lehet: geodéziai (vetületi, térképi) észak, csillagászati (földrajzi) észak és mágneses észak. Az irányszög általában fokokban mért érték, de a katonai alkalmazásban szerepel a vonás mértékegysége is.

Az időpontadatok dátum részét alapvetően a Gergely-naptárrendszerben adják meg, de ritkán előfordulhatnak más naptárrendszerben megadott dátumok is. A napon belüli időpont megadható zónaidőben (az időzóna és az azon belüli idő), illetve helyi időben (egy adott pont időzónájában érvényes zónaidőben). Az időzónák közötti eltéréseket kiküszöbölve egy időpont megadható az egyezményes koordinált világidő[32] hivatkozási időzónája szerint is (UTC idő).

Összegzés

A publikációkban foglaltak legfontosabb eredményének a bevezetésben foglalt hipotézis, az újrafelhasználható interoperabilitási szoftverkomponensek NATO informatikai rendszerek fejlesztése során való alkalmazása lehetőségének, gazdaságosságának és célszerűségének igazolását tartom. A publikációban rendszereztem, meghatároztam azokat az interoperabilitási funkciókat, amelyek megvalósítása újrafelhasználható

[31] A MIM 5.2 adatmodellben vannak további alapszintek is: legalacsonyabb apályszint, tengerfenék; repülési szint esetében: szabványos repülési szint vagy a repülőtér szintje.

[32] Coordinated Universal Time (UTC).

komponensek formájában lehetséges, az általuk nyújtott szolgáltatások függetlenek az egyes katonai – elsősorban vezetési-irányítási – informatikai rendszerek sajátosságaitól, felhasználásuk csökkentené a fejlesztések időtartamát és költségét, megkönnyítené a követelményként kitűzött interoperabilitási képességek megvalósítását.

A publikáció az interoperabilitási képességet informatikai rendszerek közötti, szabványos szolgáltatás interfész profiloknak megfelelő adatcsere-képességként értelmezi. Ezek a NATO Szövetségi Művelet Hálózat (FMN) keretrendszerében kétévenként frissített, bővített specifikációkban jól szabályozottak. Az FMN szolgáltatási utasítások rögzítik az együttműködő rendszerek közötti adatcserére használandó/használható protokollokat és a cserélt adatok formátumait (külső adatcsere-formátumokat).

A publikáció azonosítja az interoperábilis adatcsere során használt adatformátumokat (belső adatcsere-formátumok, valamint a rendszer által használt belső adatformátumok), meghatározza ezek legfontosabb tulajdonságait. Erre építve meghatározza, hogy a különböző adatformátumok között milyen átalakítástípusokra és ezeket megvalósító szoftverkomponensekre van szükség, és ezek közül melyek valósíthatók meg széles körben alkalmazható, újrafelhasználható formában.

A publikáció meghatározza az újrafelhasználható formában elkészíthető és alkalmazható komponensek körét, amelyek közé legmagasabb szinten a protokollokat, valamint a belső és külső adatcsere-formátumok közötti átalakítást megvalósító komponensek tartoznak. A protokollmegvalósító komponensek szabványos hálózati, szállítási és alkalmazási réteg szintű protokollokra épülnek, amelyekhez széles körben rendelkezésre állnak szoftvermegoldások, összetevők. Az FMN dokumentumokban 17 olyan protokoll szerepel, amelyek megvalósítása újrafelhasználható módon lehetséges. Ezek mellett lehetségesek további, a fájlcsere alapú protokollokhoz kapcsolódó újrafelhasználható komponensek is.

A publikáció az interoperabilitási profilok, külső adatcsere-formátumok új verzióinak létéből vezeti le a belső adatcsere-formátum használatának célszerűségét. Ennek megfelelően csoportosíthatók az adatcsere-formátumok közötti átalakítások belső és külső, illetve belső és belső adatcsere-formátumok közötti átalakításokra, amelyek mind megvalósíthatók újrafelhasználható formában.

Végül a publikáció meghatározza egy további funkció, az összetett adatformátumokat alkotó egyes adatelemek közötti átalakítások szükségességét, és igazolja újrafelhasználható módú megvalósításuk lehetőségét. Ezek közül három adatcsoport (szabványos szimbólumkódok, földrajzi pozíciók, mérhető jellemzők) esetében röviden meghatározza az átalakító komponensek értelmezését, főbb jellemzőiket.

Jelen publikáció nem tűzte ki céljául annak vizsgálatát, hogy ha az újrafelhasználható interoperabilitási komponensek alkalmazása valóban lehetséges és gazdaságos, célszerű lenne, a NATO informatikai rendszerek fejlesztésében vajon miért nem találkozunk ilyen komponensekkel, miért nincsenek alkalmazásuknak kialakult keretei, rendje. Ebből következően további kutatási feladatok körvonalazhatók. Az újrafelhasználható interoperabilitási komponensek lehetőségének igazolása után fel kellene tárni annak okait, hogy a NATO-ban a katonai informatikai rendszerek fejlesztéseinek támogatására ilyen komponensek még nem állnak rendelkezésre. Önálló kutatási feladat lehet annak meghatározása, hogy funkcionális és szoftvertechnológiai szempontból milyen általános követelményeknek kellene az ilyen komponenseknek megfelelniük.

Végül vizsgálat tárgyát képezheti az is, hogy az újrafelhasználható interoperabilitási komponensek rendelkezésre bocsátása, minőségbiztosítása, validációja milyen rendben történhetne.

Felhasznált irodalom

ADatP-34 NATO Interoperability Standards and Profiles. Volume 1 Introduction. Edition N Version 2 (2023). Brussels: NATO Standardization Office.

ADatP-36 Friendly Force Tracking Systems (FFTS) Interoperability. Edition A Version 2 (2021). Brussels: NATO Standardization Office.

C3 Taxonomy Baseline 6 (2022). Norfolk: NATO Allied Command Transformation.

C3 Taxonomy Baseline 6. Taxonomy of C3 Core Services (2022). Norfolk: NATO Allied Command Transformation.

Electropedia: The World's Online Electrotechnical Vocabulary (2024). Internal Electrotechnical Commission. Online: www.electropedia.org

Federated Mission Networking Spiral 5 Specification (2023). FMN Management Group.

Hasselbring, Wilhelm (2002): Component-Based Software Engineering. In Chang, S. K. (szerk.): *Handbook of Software Engineering and Knowledge Engineering*. Singapore: World Scientific Publishing, 289–305. Online: https://doi.org/10.1142/9789812389701_0013

ISO/IEC 2382:2015 Information technology – Vocabulary. Geneva: International Organization for Standardization – International Electrotechnical Commission.

ISO/IEC TR 10000-1:1998 Information Technology – Framework and Taxonomy of International Standardized Profiles. Part 1: General principles and documentation framework. Geneva: International Organization for Standardization–International Electrotechnical Commission.

MIP Information Model (MIM) Version 5.2 (2023) – Model Overview. Greding: Multilateral Interoperability Programme.

Munk, Sándor (2015): Reusable Interoperability Components in Military IT. *Revista Academiei Forțelor Terestre,* (20)3, 373–380.

NATO Architecture Framework 4.0 (2018). Architecture Capability Team, NATO Consultation, Command and Control Board.

Noback, Matthias (2015): *Principles of Package Design: Preparing your code for reuse*. Lean Publishing.

OMG Unified Modeling Language, Version 2.5.1 (2017). Object Management Group.

Pai, Praseed – Shine, Xavier (2017): *.NET Design Patterns*. Birmingham: Packt Publishing.

Szyperski, Clemens – Gruntz, Dominik – Murer, Stephan (2002): *Component Software: Beyond Object-Oriented Programming. 2nd Edition*. London: Addison-Wesley.

HADMÉRNÖK
VÉDELEMINFORMATIKA

19. évfolyam (2024) 4. szám 81–107.
DOI: 10.32567/hm.2024.4.6

Ollári Viktor,[1] Haig Zsolt[2]

5G-alapú passzív rádiólokáció városi környezetben

Az 5G egyes alkalmazási lehetőségei a hon- és rendvédelem területén

5G Passive Sensing in Urban Areas

Exploiting 5G as Illuminator of Opportunity

Absztrakt

A passzív rádiólokációs megoldások költséghatékonysága, egyre csökkenő méretei, gyors telepíthetősége, a lehetséges megvilágító források sokrétűsége, alacsony felderíthetősége okán úgy katonai, mint civil alkalmazhatósága igen sokrétű lehet. Passzív rádiólokáció során arra alkalmas külső megvilágító forrás által kibocsátott és a céltárgyról reflektálódó jeleket detektálja a rendszer. Lehetséges potenciálját tekintve az 5G figyelemre méltó megvilágítóként azonosítható. A passzív rádiólokáció szempontjából a városi térnek kaotikus fizikai és elektromágneses jellemzői vannak, így olyan detektálást támogató technológiák alkalmazása válhat szükségessé, mint a dolgok internete és a mesterséges intelligencia. Jelen tanulmány a releváns szakirodalom feldolgozásával, az 5G-ben mint városi passzív rádiólokációs ökoszisztéma megvilágító forrásában rejlő lehetőséget vizsgálja.

Kulcsszavak: 5G, radar, passzív érzékelés, mesterséges intelligencia, IoT

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: ollari.viktor@protonmail.com

[2] Iskolavezető-helyettes, egyetemi tanár, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: haig.zsolt@uni-nke.hu

Abstract

The cost-efficiency, decreasing size, rapid deployment, variety of possible illumination sources and low detectability of passive radar solutions make them suitable for a wide range of military and civil applications. A passive radar system detects signals emitted by an illuminator of opportunity and reflected from the target. The potential of 5G technology can make it a remarkable illuminator. The chaotic physical and electromagnetic characteristics of the urban space may require the use of detection-enhancing technologies such as the Internet of Things and artificial intelligence. Based on relevant publications, this paper examines the potential of 5G as an illumination of opportunity for a passive radar ecosystem in an urban environment.

Keywords: 5G, radar, passive sensing, artificial intelligence, IoT

Bevezető

Passzív rádiólokáció során egy arra alkalmas külső, nem együttműködő megvilágító forrás (IoO)[3] által kibocsátott és a céltárgyról reflektálódó jeleket detektálja a rendszer.[4] IKT-intenzív korunk az IoO-k széles körét kínálja. Az IoO-k esetében jellemzően nincs ráhatásunk a kibocsátási paraméterekre (például időváltozós karakterisztikák, kisugárzás iránya stb.), illetve számos tényező generálhat zavart, módosíthatja a visszavert jel sajátosságait, akadályozhatja annak terjedését, különösen települési környezetben. A városi IoO ökoszisztémák összetettsége és a város (mint földrajzi tér) passzív rádiólokáció szempontjából kaotikus fizikai és elektromágneses jellemzői olyan detektálást támogató technológiák, mint a dolgok internete (IoT)[5] és a mesterséges intelligencia (MI) alkalmazását teszik egyre inkább szükségessé. A multisztatikus[6] passzív rádiólokációs rendszerek kialakítását támogató városi környezet az olyan kihívásokra is, mint az alacsony radar-keresztmetszetű objektumok detektálása is optimális választ kínálhat.

Jelen tanulmány az 5G-ben mint IoO-forrásban rejlő lehetőséget vizsgálja, a releváns szakirodalom feldolgozásával. A publikáció rá kíván mutatni arra, hogy az 5G-t olyan sajátosságai, mint a nagy sávszélesség, MIMO és nyalábformálás *(beamforming),* illetve az OFDM moduláció alkalmazása potenciális, hatékonyan kiaknázható IoO-vá tehetik a passzív rádiólokációs rendszerek számára városi környezetben. A kutatás célja az 5G-t mint lehetséges IoO-t kiaknázó, IoT- és MI-elemeket tartalmazó, komplex passzív rádiólokációs keretrendszer felvázolása.

[3] Illuminator of Opportunity.
[4] Haig et al. 2014.
[5] Internet of Things (dolgok internete) – Minden olyan eszköz, amelyek egymással összekapcsolódva infrastruktúrát alkotnak, hozzáférnek az egyes infrastruktúra-elemek által generált, gyűjtött adatokhoz, aktuátorként viselkedhetnek. Tóth 2023a: 99.
[6] A rádiólokátor berendezései kettőnél több települési helyen találhatók. Lásd Ferenczy–Szűcs–Balog 1998.

A passzív radar és az 5G mint megalapozó technológiák

Passzív radar

A passzív rádiólokáció az IoO felől közvetlenül beérkező („referencia") és a célobjektumról visszavert jelek beérkezési ideje közti különbséget (illetve a beérkező jel Doppler-eltolódását) vizsgálja; a két jel közti keresztkorreláció a kétdimenziós távolság Doppler-mátrixban ölt testet.[7] Egy dinamikus, az IoO jelének változásait követő eljárás során a rendszer a referenciacsatornán vett jel Doppler-eltolásos mutációit létrehozva vizsgálja a felderítő csatornán vett jelet, azaz megfelelteti a célobjektumról visszavert jelet a létrehozott változatokkal, azonosítva azokat, amelyek a legjobban illeszkednek az IoO aktuális jeléhez.[8] Mivel a vevőegységhez érkező referenciajel elfedheti a visszavert jelet, szükséges ezek szétválasztása, referencia- és megfigyelő-/felderítőcsatornákba irányítása. Ez megvalósítható segédantennákkal, illetve fázisvezérelt antennarendszerek alkalmazásával.[9]

A célobjektum helyzetének meghatározására több lehetőség adott passzív rádiólokáció esetén. Bisztatikus[10] rendszer esetén a detektált objektum egy ellipszis test (ellipszoid) felszínén van, amelynek fókuszpontjaiban az IoO és a vevőantenna van. A pozíció a távolságmérés (ellipszoid) és a célpont által visszavert jel beérkezési irányának (DoA)[11] azonosításával határozható meg. A céltárgy az ellipszoid és a DoA-nyaláb metszéspontjában található.

Multisztatikus rádiólokációs ökoszisztéma alkalmazása esetén az ellipszoidok metszéspontjait kiszámítva is meghatározható a célpont pozíciója. Városi környezetben lehetséges opció, hogy az IoO és a vevőantenna egyazon helyen található, így nincs köztük érdemleges távolság, azaz a monosztatikus rádiólokációs helymeghatározási eljárás alkalmazandó. Monosztatikus jelleg esetén a célobjektum egy gömbszelet felszíne és a DoA-nyaláb metszéspontjában van.[12]

IoO lehet, a teljesség igénye nélkül, minden aktív radar, mobilkommunikációs rendszerek (4G, 5G, WiFi, mikrohullámú hozzáférési [WiMAX] szolgáltatások), analóg és digitális rádió- vagy TV- (FM-/DAB-/DVB-T-) sugárzók, az űrbe telepített technológiák.[13] Az utóbbiak kapcsán a GNSS-[14] hálózatok kutatói megállapítják, hogy alacsony adóteljesítményük okán alkalmazásuk kevéssé „költséghatékony", ezért érdemesebb a jelentős elemszámú konstellációval rendelkező, széles sávú adatkommunikációs szolgáltatásokat nyújtó szolgáltatók műholdjaira építeni.[15] Ilyen lehet a 600 LEO és 35 GEO műholdat üzemeltető Eutelsat OneWeb, illetve az 5800 elemből álló LEO konstellációval rendelkező StarLink.[16]

[7] Colone–Filippini–Pastina 2023; NATO STO 2017.
[8] Núñez-Ortuño et al. 2023: 2–5.
[9] Pető 2013; Núñez-Ortuño et al. 2023: 7–9.
[10] A lokátor adója és vevőberendezése egymástól távol települ. Lásd Haig et al. 2017.
[11] Direction of Arrival.
[12] Kuschel–Cristallini–Olsen 2019; Skolnik 1981.
[13] Balajti 2019a.
[14] Global Navigation Satellite System.
[15] Núñez-Ortuño et al. 2023.
[16] Pultarova 2025.

5G

Az újgenerációs mobilkommunikációs hálózatok már inkább az informatikai hálózatokhoz sorolhatók.[17] A 4G–5G–6G közti generációs léptékváltás mértékét mutatja be az alábbi, 1. táblázat.

1. táblázat: Egyes 4G-, 5G- és 6G-mérőszámok összehasonlítása

	4G	**5G**	**6G**
Adatátviteli sebesség	1 Gbps	20 Gbps	1000 Gbps
Felcsatlakoztatható eszközök száma	100 000 / km^2	1 000 000 / km^2	100 / m^3 [18]
Késleltetési idő	10 ms	1 ms	0.1 ms
Max. csatorna sávszélesség	20 MHz	0.1/0.4/2 GHz (FR1/ FR2-1/FR2-2) [19]	100 GHz
Maximum spektrális hatékonyság	15 bps/Hz	30 bps/Hz	100 bps/Hz
Vertikális lefedettség	n/a	300 m	10 000 m

Forrás: a szerzők szerkesztése a 3GPP Műszaki jelentés (2022): 3GPP TR 21.916 V16.1.0, ETSI Műszaki Specifikáció (2022): TS 138 104 V17.7.0 adatai alapján

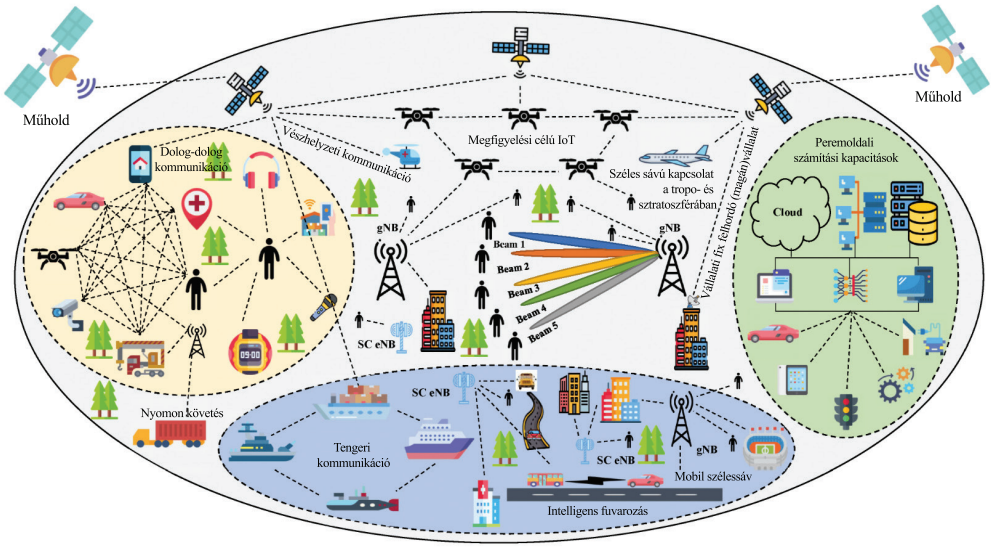
Az 5G-rendszerarchitektúrában 3 fő elem különíthető el:[20]

- végponti készülékek (UE)[21] – minden olyan eszköz, amely az 5G-hálózatra képes csatlakozni;
- rádiós hozzáférési hálózat (RAN)[22] – az UE és az 5G-maghálózat közti kapcsolatot létrehozó eszközök ökoszisztémája;
- CORE (5G-maghálózat) – egy szolgáltatásalapú, az úgynevezett hálózati funkciókat felölelő keretrendszer.

Az 5G-nél már teljesen különválnak a RAN és CORE az átviteli (transzport) funkcióktól, továbbá a felhasználói és vezérlési síkok. Mindez kiegészül azzal, hogy a hálózat egy adott fizikai csomópontja számos logikai csomópontot „megtestesíthet". Azaz a teljes rugalmasság, a szolgáltatások magas szintű biztosítása és szegmentálása érdekében.

A megcélzott teljes lefedettség megvalósítása érdekében a szabványalkotók alapvető jövőbeni hálózati elemként számolnak a műholdas, valamint a nagymagasságú (18–22 km) platformrendszerekkel (HAPS),[23] a 6G esetében az intelligens jeltükröző/-továbbító felületekkel (IRS).[24] A HAPS légköri és műholdas 5G-/6G-jelforrások kiegészítő IoO-ként szolgálhatnak a passzív rádiólokáció számára.

[17] Tóth 2023b: 79.
[18] A 6G a lefedett tér vertikális kiterjedését is figyelembe veszi, ezért térfogat alapon határozza meg a célértéket.
[19] FR1 = 0,41–7,125 GHz (UHF, L-sáv, UWB, S-sáv, C-sáv); FR2-1 = 24,25–52,6 / FR2-2 = 52,6–71 GHz (Ka-sáv, V-sáv).
[20] Tóth 2023b.
[21] User Equipment.
[22] Radio Access Network.
[23] Jellemzően drónokra/léghajókra telepített gNB-k (High Altitude Platform Systems, Towers in the Skies 2021).
[24] Farkas 2023: 24; Tóth 2023b: 55; Liu et al. 2024; 3GPP TR 21.918 V0.2.0 (2024-02).



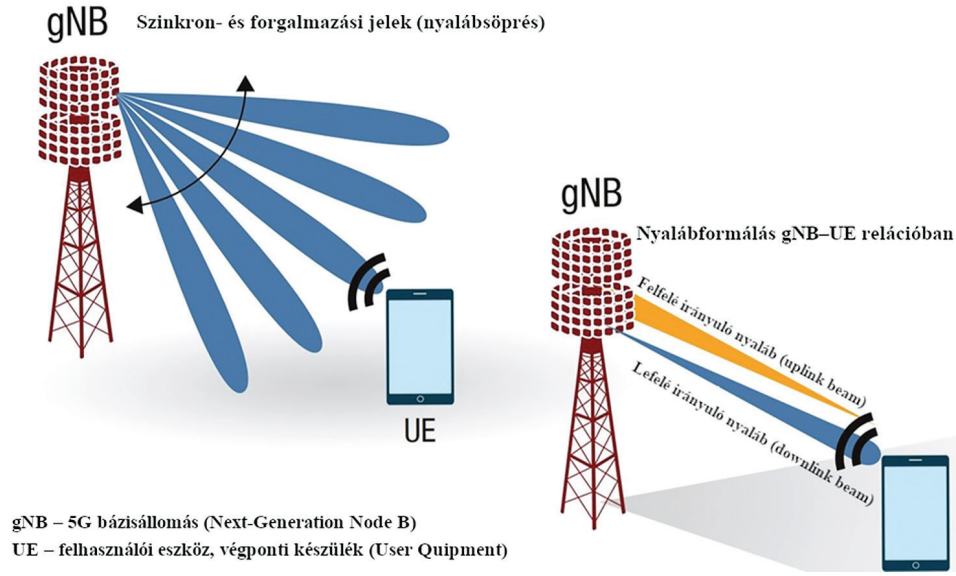
1. ábra: 5G-/6G-ökoszisztéma

Forrás: www.mdpi.com/electronics/electronics-11-00121/article_deploy/html/images/electronics-11-00121-g001.png alapján a szerző fordítása

A passzív rádiólokáció szempontjából kiemelendő még a technológia kínálta csatorna-sávszélesség és a heterogéncellás ökoszisztéma. Míg az FR1 a nagy területi lefedettséget biztosítja korlátozott bázisállomás (gNB)[25] darabszám mellett (makrocellás struktúra), az 1. táblázatban vázolt mérőszámok elsődlegesen az FR2 alkalmazása mellett teljesülnek. Az FR2 kiaknázása, annak terjedési sajátosságai (jelentős útvonalveszteség) okán, csak kiscellás ökoszisztémában lehetséges. A passzív rádiólokáció szempontjából lényeges szempont, hogy az FR2-ben érhető el a legnagyobb csatorna-sávszélesség (2GHz). Igaz, az FR1-hez képest jelentősen kisebb teljesítmény (0,25–2 W) mellett.

Az 5G gNB-k képesek párhuzamos, az adott UE pozíciójára fókuszáló rádiónyalábokat generálni (2. ábra). A nyalábképzés során az 5G MIMO antennatömbök egyes elemi antennáit külön-külön táplálják a továbbítandó jellel. A jel fázisát és amplitúdóját úgy módosítják, hogy ennek eredményeként az elemi antennák adott klasztere egy irányított rádiónyalábot hozzon létre. A masszív MIMO és a nyalábképzés technológiák, hatékonyabb adatátvitelt biztosítása mellett mérsékelhetik az interferenciák zavaró hatásait.

[25] Next Generation NodeB: újgenerációs bázisállomás.



2. ábra: Nyalábmenedzsment
Forrás: Ramalingam 2018 alapján a szerző fordítása

Az 5G-rendszerek hatékonyságának, ellenálló képességének növelése érdekében aktívan vizsgálják az MI alkalmazási lehetőségeit a MIMO, a nyalábképzés, az útvonalválasztás, zavartatás és zavarásdetektálás terén.[26] Az 5G-hálózatok szofisztikált támadása, a szabvány által támogatott nagy szabadságfokú (dinamikus) jelkeretfeltöltési, -kialakítási lehetőség, a szinkronizációs jelek szabad elhelyezése (stb.) okán, kihívást jelent.[27] Az időszinkront biztosító GNSS-jelek zavarása, a vonatkozó védelmi funkciót aktiválva, eredményezheti a támadott gNB kényszerített leválasztását a hálózatról.[28] Azonban megfelelő paraméterezéssel, alternatív időszinkronforrások biztosításával ezek a támadások hatékonyabban elháríthatók, különösen a kiscellás ökoszisztémával kiegészült hálózatok esetén. Passzív rádiólokáció szempontjából az 5G IoO-k zavarása csak olyan egyértelmű művelettel lehetséges, amely felhívná a védelemért felelős szervezetek figyelmét a behatolás tényére.

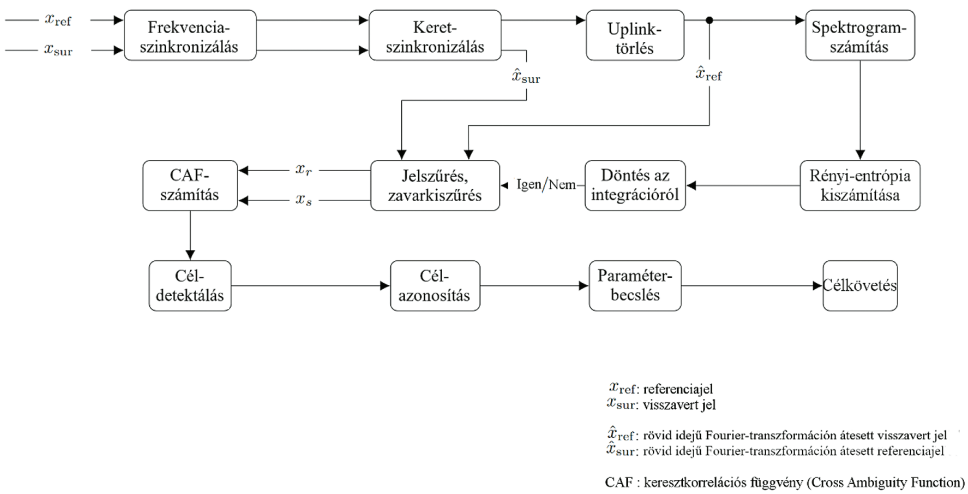
5G-alapú passzív rádiólokáció városi környezetben

Az intenzív városi EM környezet napjainkban már lehetővé teszi költséghatékony (rejthető) passzív rádiólokációs érzékelő hálózatok kialakítását, amelyek közel teljes körű területi lefedettség mellett biztosíthatják a célobjektumok detektálását, mozgásuk követését. Elméleti szinten, frekvenciaosztásos (FDD)[29] üzemmódot és szabvány

[26] Khedkar et al. 2023.
[27] Birutis et al. 2022.
[28] Wührl et al. 2023.
[29] Frequency Division Duplex.

szerinti maximális alvivő frekvenciát (2 GHz) feltételezve, akár 30 m/s sebességgel mozgó, kis méretű objektumok detektálása is biztosított lehet egy 5G-t kiaknázó passzív rádiólokációs ökoszisztémában.[30] Jelenleg azonban az időosztásos (TDD)[31] üzemmód alkalmazása jellemző.

TDD esetében a passzív rádiólokáció célú jelfeldolgozás jellemzően a „hagyományos" eljárás szerint történik, azzal a módosítással, hogy a keresztkorreláció számítása előtt szükséges elvégezni a frekvencia- és keretszinkronizálás mellett az uplink kiszűrését a jelből. Számos szerző javasolja azon magas erőforrás-allokációval rendelkező jelek, jeltöredékek azonosítását, amelyek adaptív integrálásával biztosítható a kis RCS-ű célobjektumok hatékony detektálása (3. ábra). Mindemelett a gépi és mélytanulás-algoritmusok, az MI-technológia releváns megoldásainak alkalmazása ma már nélkülözhetetlen a hatékonyabb detektálás, osztályozás és követés érdekében.[32]



3. ábra: 5G-alapú passzív rádiólokációs jelfeldolgozás
Forrás: Maksymiuk et al. 2023 alapján a szerző fordítása

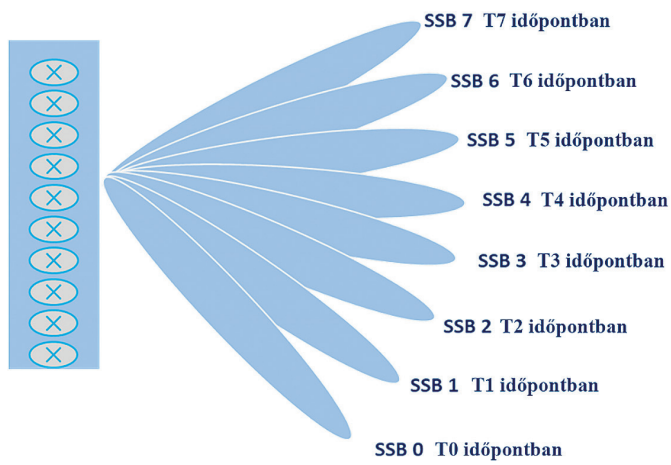
Az 5G 3GPP szabvány szerinti sávszélessége (5 MHz – 2 GHz)[33] optimális távolságfelbontást eredményezhet. Valós alkalmazási környezetben az 5G aktuális sávszélessége függ a továbbított tartalomtól. Az adattartalom ingadozása az 5G-hullámforma (keret erőforrás-allokáció, jel időtartam) módosulását, a keresztkorrelációs függvény váltakozását, a távolságfelbontási érték változékonyságát vonhatja maga után.[34]

A keresztkorreláció szempontjából azon IoO-k a legoptimálisabbak, amelyek periodicitásszegények, spektrális komponensei közel kiegyenlítettek és egyenletesen szétterítettek („zajszerűek").[35] Az 5G-jel modulálása (OFDM) a hatékony kereszt-

[30] Liu et al. 2022.
[31] Time Division Duplex.
[32] Maksymiuk et al. 2023.
[33] 3GPP TS 38.102-1 V18.5.0 (2024-03).
[34] Księżyk et al. 2023.
[35] Seller et al. 2019.

korrelációhoz járulhat hozzá. Szemben a 4G fix 15 kHz-es alvivő-távolságú OFDM modulációjával az 5G-szabvány már rugalmasabb megközelítést biztosít. 15 és 960 kHz között a 2 hatványaival multiplikálható az alvivőtávolság. Mindezek együttesen biztosítják a jel spektrális szétterítését, zajszerű viselkedését.

Amennyiben nincs adatforgalom, a gNB csak titkosítatlan szinkronizációs jelblokk- (például SSB[36]) sorozatokat sugároz ki a tér különböző pontjai felé (SSB „sörprés" – 4. ábra). Az SSB a downlink felépítéséhez és szinkronizáláshoz szükséges információkat tartalmazza, amelyek alapján az UE azonosítja és kiválasztja a cellát, a számára leghatékonyabb nyalábot, megismeri a gNB-hez, hálózathoz kapcsolódást biztosító információkat. Az SSB-sorozatokat, konfigurálásától függően, 5–160 milliszekundumonként, előre definiált pozícióra[37] és nyalábszámban (FR1-ben 4/8, FR2-ben legfeljebb 64) sugározza ki a gNB. Az SSB-k helyspecifikus információkat tartalmaznak, amelyeket az UE visszaküld a gNB-nek. A gNB ez alapján engedélyezi a kapcsolatot, és csökkenti a szomszédos UE-k interferenciáját. Amennyiben a gNB támogatja a nyalábformálást, egyidejűleg több SSB-nyalábot bocsát ki, amelyek az alkalmazott frekvenciatartománytól és hálózati beállításoktól függően legfeljebb 7,2/57,6/230,4 MHz (FR1/FR2-1/FR2-2) sávszélességűek lehetnek. Az SSB demodulálásával és a fizikai forgalmazási csatorna (PBCH)[38] információkinyerésével, a kibocsátott nyalábok egyedileg azonosíthatóvá válnak a passzív rádiólokáció számára. A referenciacsatornán vett SSB jel (kvázi) félaktív rádiólokációs adatfeldolgozásával a céltárgy sebessége alacsony pontossággal, de pozíciója jól azonosítható.[39]



4. ábra: SSB söprés

Forrás: www.linkedin.com/pulse/illustration-5g-ssb-beam-sweep alapján a szerző fordítása

[36] Synchronization signal block.
[37] Vertikális és horizontális nyalábszélesség, azimuth, vertikális döntés stb.
[38] Physical Broadcast Channel.
[39] Lin et al. 2019; Abratkiewicz et al. 2023; ETSI Műszaki Specifikáció (2024): TS 138 213 V17.8.0.

Városi környezetben, különösen kiscellás 5G hálózati struktúrában, az SSB-t kiaknázó passzív rádiólokáció esetében a maximális egyértelmű hatótávolság jellemzően figyelmen kívül hagyható, azonban ha a sebesség mérése szempont, akkor a maximális egyértelmű sebességgel számolni szükséges. Így valójában nem Doppler-, inkább alkalmazásdilemmával szembesülünk. A detektált objektumról visszavert jel frekvenciája a (radiális) mozgás sebességétől és irányától függően megváltozik (Doppler-csúszás). Amennyiben ez a változás meghaladja a kibocsátott SSB-impulzus ismétlődési frekvenciáját (PRF),[40] a sebesség meghatározása bizonytalanná válik.

$$V_{max} = \frac{\lambda \cdot f_{PR}}{4}$$

(V_{max}: maximális egyértelmű sebesség, f_{PR}: az SSB impulzus ismétlési frekvenciája, λ: vivő hullámhossz.)[41]

Figyelembe véve az SSB PRF-ének maximális értékét (200 Hz) a fenti képlet, a már elérhető (700 MHz, 3.6 GHz) és a tervezett (24 GHz) 5G-frekvenciák ismeretében meghatározható az elérhető V_{max}. Tehát: 700 MHz-nél 21,41 m/s, 3,6 GHz-nél 4,16 m/s, 24 GHz-nél 0,62 m/s. Azaz a frekvencia növekedésével csökken a V_{max}.

A városi környezet egy további kihívása, hogy a gNB felől közvetlenül érkező, illetve az egyéb objektumokról visszaverődő jelek okozta interferencia mellett, a nagyszámú, szomszédos csatornákon kommunikáló UE-k által generált zavarokat (IUI)[42] is kezelnie kell a passzív rádiólokációs rendszernek. Habár az IUI hatása a mobilkommunikációra jellemzően nem jelentős, a célobjektum által visszavert jel elnyomására képes lehet.[43]

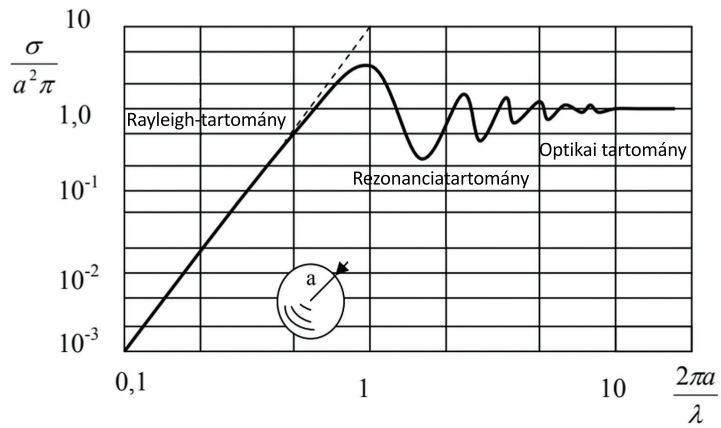
Detektálás szempontjából elsődlegesen az UAV[44]-ok esetében okoz jelentős kihívást a kis méretű hatásos keresztmetszet (RCS),[45] amely a célobjektum felületére jutó energiasűrűség mellett függ:

- a megvilágítás szögétől;
- a megvilágított felület méretétől és annak jellemzőitől (anyag, alak, kiterjedés stb.);
- a célobjektum mérete és a hullámhossz viszonyától;
- a rádióhullám polarizációjától stb.

A megvilágítás szempontjából egy 5G-t kiaknázó városi IoO ökoszisztémában az FR1 gNB antennák magas telepítése, viszonylag nagy száma, pozicionálása egyszerre előny és hátrány. Elméletileg eséllyel sugározzák be – adott esetben több irányból – a célobjektumokat úgy, hogy a megfigyelőantenna értékelhető jelet fogjon be. Városi környezetben, földközeli magasságban, csökken a közvetlen FR1 megvilágítás lehetősége. Az FR2 és annak mikrocellás ökoszisztémája nagyobb földfelszínközeli lefedettséget, megfelelő megvilágítási szög esetén magasabb RCS értéket biztosíthat.

[40] Pulse-repetition frequency.
[41] Księżyk et al. 2023: 13.
[42] Inter User Interference (felhasználók közti interferencia).
[43] Lyu–Liu–Fan 2022.
[44] Unmanned Aerial Vehicle – pilóta nélküli légi jármű.
[45] Radar Cross Section.

A méret és a hullámhossz viszonya az elektromos méret *(ka szorzat)*[46] révén elemezhető, ahol „a" azon legkisebb gömb sugara, amely befoglalja a célobjektumot. Amennyiben a *ka* szorzat 1-nél kisebb, a hatásos keresztmetszet a Rayleigh-tartomány szerint viselkedik (fordítottan arányos λ^4-nel). 1 körüli eredménynél az RCS már a Mie/rezonanciatartomány sajátosságai szerint értelmezhető, az RCS az optikai tartományban jellemző érték körül oszcillál. A hullámhosszváltozásokra az RCS erősen reagál. Az optikai tartományban a *ka* 10 feletti értéket vesz fel, és a célobjektum apertúrasugárzóként kezelhető (5. ábra).[47]



5. ábra: Lokátor céltárgy-gömb hatásos keresztmetszete a hullámhossz függvényében
Forrás: Ferenczy–Szűcs–Balog 1998: 81

A *ka*-t vizsgálva, az FR1 GHz alatti tartományában csak az 5 cm-nél kisebb „*a*" értékkel rendelkező célobjektumok értelmezhetők a Rayleigh-tartományban. A GHz-es FR1 tartományban a potenciális célobjektumok többségénél a rezonancia és mérettől függően az optikai tartomány szerinti RCS-jellemzők veendők figyelembe. Mindez azt is jelenti, hogy FR2-ben alig akad rezonanciatartományhoz sorolható céltárgy.

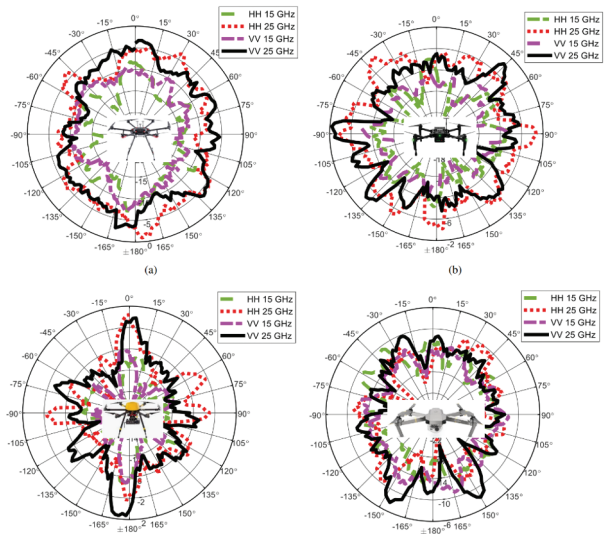
Egyes forgatókönyvek

Az objektumdetektálás jellemzően két fő forgatókönyv-főcsoportra (jármű-, emberalak-detektálás) különíthető el. Az 5G IoO célú kiaknázásakor szükséges figyelembe venni, hogy a makrocellás 5G rádiós hálózati struktúrában, városi környezetben a többutas terjedés jelentősége hatványozottan érvényesül. Továbbá a jelenlegi 5G-hálózatokban elérhető maximális sávszélesség esetén a radarfelbontás többméteres lesz. Ez a tervezett tömeges üzleti és kedvtelési célú UAV-alkalmazás, illetve a jármű- és gyalogosforgalom detektálásának igénye esetében már problematikus érték.[48]

[46] $k = 2\pi/\lambda \Rightarrow (2\pi/\lambda) \times a \Rightarrow 2\pi a/\lambda$ – *k*: a hullámszám, *a*: azon legkisebb gömb sugara, amely befoglalja a célobjektumot, λ: vivő hullámhossz.
[47] Ferenczy–Szűcs–Balog 1998; Koncz 2007.
[48] Seller et al. 2020; Księżyk et al. 2023.

UAV-detektálás

A polgári UAV-ok kis mérete, szerkezeti kialakítása, a gyártásukhoz felhasznált anyagok sajátosságai, a reptetésüket jellemző haladási magasság és annak dinamikus változása, amely kiegészül a manőverezési sokszínűséggel, jelentős kihívások elé állítja a passzív rádiólokációt, különösen városi környezetben. Esetükben RCS-növelő tényező lehet az eszköz akkumulátora, illetve egyéb hasznos teher (például kamera és egyéb érzékelők), feltéve, hogy a megvilágítás szöge láthatóvá teszi azt (6. ábra). Mivel a hasznos teher és akkumulátor jellemzően a drónok hasrészén találhatók, az FR1 megvilágítás korlátozottan, a célobjektum repülési iránya, vertikális emelkedésének és horizontális elfordulásának szögétől függően teszi lehetővé a kiegészítők RCS-növelő hatásának kiaknázását.

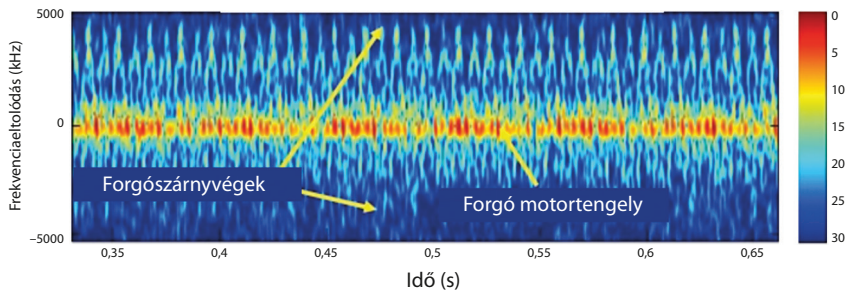


(a):DJI Matrice 600 Pro, (b):DJI Matrice 100, (c):Trimble zx5, (d):DJI Mavic Pro 1
Vivőfrekvencia 15 és 25 GHz, horizontális (HH) és vertikális (VV) polarizációkkal

6. ábra: Négy UAV RCS-szignatúrája (dBm²) az azimuth relációjában
Forrás: Ezuma et al. 2021

A kültéri FR2-es mikrocellás ökoszisztémák már magasabb valószínűséggel biztosíthatnák az alacsonyan repülő UAV-ok magasabb RCS-értéket eredményező megvilágítását. FR2-ben az alacsony hullámhossz okán jelentősebb szerepet kap az UAV-ok formavilága, az élek és kiszögellések generálta diffrakció és szórás. Mindemellett a megfigyelőantennák optimális elhelyezése is kihívást jelent. Amint arra a 6. ábra is rámutat, a megvilágítás szöge alapvető jelentőségű a minél nagyobb RCS-elérés szempontjából. Mivel nem szűken körülhatárolható repülési magasságban mozgó eszközök detektálása a feladat, városi környezetben a visszavert és referenciajelek vételét biztosító antennák komplex hálózatának alkalmazása lehet hatékony, de költségnövelő megoldás.

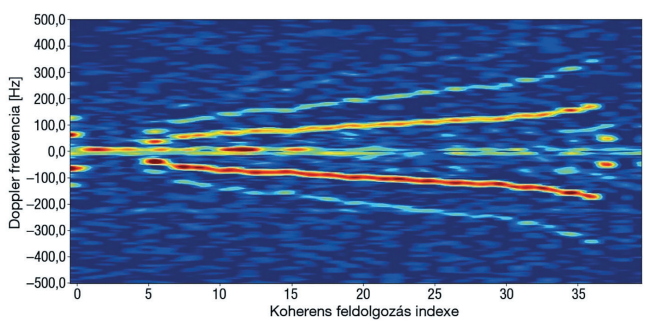
Egyes kutatások, a forgószárnyas modellekre fókuszálva, a mikro-Doppler-jelenség kiaknázhatóságára mutatnak rá. Az UAV-ok forgószárnyai szintén frekvenciaeltolást hoznak létre, amelyek periodikus, időben változó modulációt generálnak az eszköz által visszavert jel vivőfrekvenciájában. A moduláció a vivőfrekvenciától, a forgási sebességtől, a forgás- és a beeső jel által bezárt szögtől függő harmonikus frekvenciákat tartalmaz, amelyek azonosíthatóvá válhatnak az UAV által visszavert jel Doppler-spektrumában (7. ábra).[49] 5G-környezetben a 3 GHz feletti FR1 IoO-k már biztosíthatják a kisebb méretű drónok felderítését. FR2-es IoO-k esetén az UAV-ok túlnyomó hányadánál az optikai szórástartomány sajátosságai veendők figyelembe, amelyben a szóráspont modell alkalmazható a mikro-Doppler-szignatúra kinyerésére. Ekkor a célobjektumról visszavert jel szóródása diszkrét pontokban realizálódik.



7. ábra: 45°-ban besugárzott, négy forgólapátos UAV radiális sebesség generálta mikro-Doppler szignatúrája – a szerző fordítása

Forrás: Jian–Lu–Chen 2017

Alacsonyabb frekvenciák esetén a forgószárny mérete összemérhetővé válik az IoO jelének hullámhosszával, így a mikro-Doppler nem aknázható ki, azonban a rotor által a vevő irányába sugárzott jel periodikus változásait vizsgálva az FR1 tartomány is alkalmas lehet a drón detektálására (8. ábra), egyértelműen megkülönböztetve azokat más objektumoktól (például madárraj).[50]



8. ábra: Gyorsuló forgószárny spektrumképe

Forrás: Seller et al. 2020

[49] Chen et al. 2006; Seller et al. 2020; Beasley et al. 2020.
[50] Seller et al. 2020.

Az egynél több forgószárnnyal rendelkező UAV-ok detektálásának kihívásaira jellemzően gépitanulás-algoritmusokra épülő, a mikro-Doppler-jellemzők azonosítását célzó megoldásokat javasol több szerző. A javasolt eljárások figyelemre méltók, azonban a szerzők jellemzően optimális lefedettséggel, hálózati forgalommal, illetve a ma még alig alkalmazott FR2 tartomány kiaknázásával számolnak, említés szintjén érintve a nyalábformálás lehetséges hatásait.[51]

Az 5G-alapú passzív rádiólokáció tartalomfüggőségének csökkentésére egy Rényi-entrópiára épülő megoldást javasolnak más szerzők.[52] Megállapításuk szerint az entrópia és a downlink erőforrás-kiosztás közti direkt összefüggés kiaknázható egy, a passzív rádiólokációs rendszerek hatékonyságát növelő, adaptív jelintegrációs algoritmus megalkotásához. Az ismertetett megoldás a vevő által fogott OFDM-jelet idő-frekvencia raszterré alakítja rövid idejű Fourier-transzformációval (STFT),[53] ezzel biztosítva az alvivők kiosztásának és az időjellemzőknek a közvetlen elemzését. A Rényi-entrópia segítségével vizsgálja az 5G-hálózat aktuális erőforrás-kiosztását. Az 5G-hálózat maximális terhelésével (például nagy méretű fájl letöltése) meghatározható a maximális entrópia (kalibrálás). A magasabb entrópiaszint több alvivőt, ezek növekvő időtartamát feltételezi, ami növelheti a hatékony integrációs időt, így lehetőséget biztosít például távolabbi célpontok detektálására. A kalibrálást követően a rendszer csak azon jeleket, jeltöredékeket veszi figyelembe (akkor végez adaptív integrációt), ha azok megfelelő entrópiaszinttel[54] rendelkeznek. A kutatók által elvégzett kísérletek igazolták, hogy az eljárás biztosíthatja egy kisebb méretű drón detektálását is. Azonban, mint a szerzők is rámutatnak, a nyalábformálásos forgatókönyveket a jövőben tervezik vizsgálni.[55]

Más kutatók javaslata az SSB-ben rejlő, rövid idejű Fourier-transzformációval kinyert adatok felhasználására épít, egy tanulni képes neurális háló rendszerbe iktatásával. Megállapításuk szerint az SSB, relatíve rögzített struktúrája okán, egyértelműbben reagál külső (például UAV okozta) zavarokra. A detektált zavarokat a neurális háló elemzi, a zavarjellemzők osztályozásával elkülöníti a háttérzajt a lebegő/mozgó UAV generálta jellemzőktől. A bemutatott eljárás jelentős részt immunis az 5G kihívásaira, mint a nyalábképzés és adatfüggő forgalmazási paraméterek, azonban az elvégzett kísérletek viszonylag zavartatásmentes környezetben zajlottak, továbbá a javasolt megoldás inkább egy 5G-alapú jelenlét- és mozgásérzékelő.[56]

Emberi jelenlét detektálása

A humán jelenlét esetében a távolság és sebesség meghatározásához a legtöbb jelet a törzsről visszavert jelek biztosítják. A mikro-Doppler-jellemzők mélytanulás-támogatású elemzésével például a végtagok mozgásával, a légzéssel és szívveréssel kapcsolatos

[51] Xu et al. 2019.
[52] Maksymiuk et al. 2023.
[53] Short-time Fourier Transform.
[54] Pl. a maximális entrópiaérték 90%-át meghaladó kitöltésű jelkeretek.
[55] Maksymiuk et al. 2023.
[56] Lin et al. 2023.

információk is kinyerhetők.[57] Az emberi járás mikro-Doppler-karakterisztikája lehetőséget nyújt az állati mozgás kiszűrésére. Másfelől az emberi mozgás komplexitása akár dinamikusan váltakozó radarkeresztmetszetet is eredményezhet. Kihívást jelent továbbá az emberi test összetett struktúrája, illetve azon sajátossága, hogy magasabb frekvenciák mellett kevésbé tükrözi, hanem inkább szórja a megvilágító által kisugárzott jeleket.[58] Emellett, magasabb frekvenciatartományokban, maga a ruházat anyaga és formája (például gyűrődések) alakíthat ki kiugró visszaszórási pontokat.[59]

A releváns tanulmányok jelentős része a csatornaállapot információs referenciajel (CSI-RS)[60] kiaknázhatóságára épít. A felmutatott eredményeket – mint az emberi jelenlét, mozgás, gesztusok (például egyes kézjelek), életfunkciók (például légzés) detektálása – nem kisebbítve szükséges rámutatni, hogy az elvégzett kísérletek zárt terekre fókuszáltak, limitált létszámú célponttal és az adatforgalmazást folyamatosnak feltételezve, ami valós 5G-környezetben nem biztosítható, továbbá a CSI-RS alkalmazása közvetlen hozzáférést feltételez az adott hírközlési hálózathoz. A vázolt kihívások kezelésére az SSB kiaknázása megoldás lehet.[61]

A jövő technológiai kilátásai

A passzív rádiólokációs technológia jelenlegi alkalmazási és fejlesztési trendjeit figyelembe véve előrevetíthető, hogy a rádiólokáció is egyfajta szimbiotikus, hálózatos ökoszisztémává válik.[62] A magas EM zajterhelésű városi környezetben három kiemelt kihívást szükséges kezelnie a technológiának:

- közvetlen IoO-célobjektum rálátással nem rendelkező területek minimalizálása;
- nagy hatékonyságú zavartatás- és zavarásállóság, azaz a nem kívánt jelek eliminálása;
- a célobjektumok detektálására, osztályozására és akár azonosítására, követésére alkalmas jelek befogása.

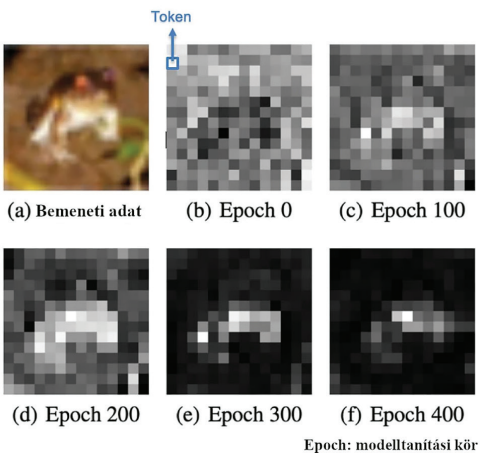
A kihívásokra adott válaszok részét képezhetik a:[63]

- polarimetrikus diverzitást kiaknázó,[64] komplex IoO- (5G FR1, FR2, GNSS stb.) felhasználást biztosító referencia-/megfigyelőantenna-hálózatok;
- kiegészítő, detektálás, osztályozás, azonosítás feladatait támogató érzékelő technológiák, mint például
  - akusztikus;
  - elektro-optikai;
  - szeizmikus érzékelők;

[57] Caro–Bloice 1971; Fereidouni et al. 2022; Huan et al. 2023; Deep et al. 2020.
[58] Adib et al. 2015; Kim–Ha–Kwon 2015.
[59] Yamada–Tanaka–Nishikawa 2005.
[60] Channel State Information Reference Signal.
[61] Tang et al. 2020; Ashleibta et al. 2021; Li et al. 2021.
[62] Balajti 2019b.
[63] Colone–Filippini–Pastina 2023; Gomez-Del-Hoyo–Gronowski–Samczynski 2022; Maksymiuk et al. 2024.
[64] Duál-polarimetrikus antennák alkalmazásával a visszavert és a referenciajel horizontális és vertikális verziója is befogható.

- dinamikus antenna és érzékelő platformok (UAV, UGV[65]);
- a passzív radar ökoszisztéma hatékony vezérlését biztosító MI-megoldások.

A rádiólokáció területén is alkalmazott gépitanulás-algoritmusok mellett a mélytanulás és a multimodalitás[66] felé mozduló, figyelemre méltó absztraháló, adaptációs, szemantikai és szentimentelemzési, következtetési, osztályozási képességekkel rendelkező LLM[67]-ek jelenthetik az MI célirányos alkalmazásának közvetkező lépcsőfokát.[68] A nagy nyelvi modellek jellemzően az úgynevezett transzformerek[69] által létrehozott és súlyozott logikai egységekkel (token)[70] dolgoznak.[71] A tanítási és éles munkafolyamataik során a tokenek egymásutániságának valószínűségeit vizsgálják. A modellek megtaníthatók arra, hogy mire fókuszáljanak, a vizsgált információ mely része releváns számukra, így azokra helyezik a figyelmet, kirekesztve az irreleváns adatszegmenseket (9. ábra).[72]



9. ábra: LLM figyelemmechanizmus – a szerző fordítása
Forrás: Tarzanagh et al. 2023

A vázoltak alapján további vizsgálatok tárgya lehet, hogy a multimodális LLM-ek milyen hatékonysággal:

- segíthetik a radarképek kiértékelését, a gyenge radarjelek kiaknázását, a zavarjelek eliminálását, a kiegészítő érzékelőkből származó adatok feldolgozását;

[65] Unmanned ground vehicle – vezető nélküli földfelszíni jármű.
[66] A modell képes a szöveges, képi, hangalapú információ kezelésére és generálására.
[67] Large Language Model.
[68] Chang et al. 2024; Wu et al. 2024.
[69] A transzformátor modell egy figyelem- *(attention)* mechanizmusra épülő, mélytanulási architektúra (neurális hálózat). A szekvenciális adatokban lévő kapcsolatok megfigyelése révén képes kontextus- és jelentésazonosításra. A figyelemmechanizmus teszi lehetővé a modell számára, hogy a bemeneti adatok bizonyos részeire szelektíven fókuszáljon. Vaswani et al. 2017.
[70] A modell által kezelt (be-/kimeneti) adat egy kisebb szeletének numerikus reprezentációja.
[71] Bingli–Vargas 2024.
[72] Kirillov et al. 2023; Tarzanagh et al. 2023; Zhang et al. 2024.

- támogathatják a fázisvezérelt antennarendszerek vezérlését, azok akár valós idejű finomhangolásával, a rendszerparaméterek folyamatos értékelése és automatikus módosítása révén;[73]
- ismerhetik fel, és orvosolhatják a passzív rádiólokációs ökoszisztéma IT-elemeinek sebezhetőségeit;[74]
- segíthetik elő a rádiólokációs rendszerek proaktív kiber- és zavarás elleni védelmét a szokványostól eltérő, lehetséges támadási mintázatokat megjelenítő rendszeresemények azonosításával.

Szükséges azonban a technológia kihívásait szem előtt tartani. Egy multimodális LLM tanító adatbázisa olyan mennyiségű adatot igényel, amellyel a rádiólokáció terén kevesen rendelkeznek. Ez a tanító adatok mesterséges generálásával, modellezéssel áthidalható.[75] Továbbá a radarszignatúrák összetettsége és azok jellege számos környezeti körülmény függvénye, különösen városi környezetben. Tehát a modell mintafelismerő képessége ki kell terjedjen valamennyi, a detektálást befolyásoló környezeti körülmény azonosítására.

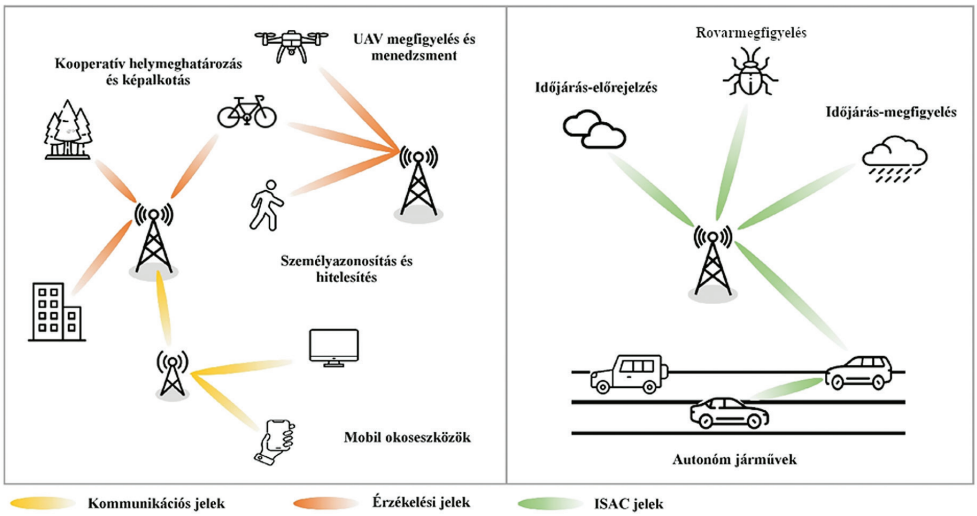
A technológia korlátai között meg kell említeni az úgynevezett „hallucinációt",[76] illetve adatkezelő képességeiknek – erőforrásigényük mellett – korlátot szab az is, hogy adott időintervallumban mekkora mennyiségű tokent képesek feldolgozni (kontextusablak).[77]

A fent vázoltak alapján a passzív rádiólokáció valószínűsíthető, középtávú fejlődési iránya a komplex, dinamikus adaptációra képes, kognitív rendszerek felé mutat. Egy kognitív rendszer, rádiólokációs és egyéb érzékelői révén, valós időben képes:

- környezetét felmérni és értékelni;
- a megszerzett ismereteit tárolni;
- a fentiekre alapozottan, proaktívan kezelni a felmerülő feladatokat és problémákat.[78]

Városi környezetben alkalmazott rádiólokáció szempontjából a 6G hozhat jelentős paradigmaváltást, feltételezve a mikrocellás struktúrák dinamikus elterjedését és a Terahertz tartomány kiaknázását. Az ITU-R M.2160-0 (11/2023) ajánlásban szereplő 3D pozicionálást és leképezést biztosító ISAC[79] forgatókönyv kapcsán olyan irányokban is folynak kutatások, mint az autonóm járművek közlekedésének monitorozása és irányításuk támogatása, gyalogosforgalom megfigyelése, a „ruhán és takarófelületen átlátó" objektumdetektálás (10. ábra).[80]

[73] Li et al. 2024; Wang et al. 2024.
[74] Xu et al. 2024.
[75] Karlsson 2023.
[76] Elégtelen mennyiségű információ esetén a modell nem koherens kimeneti eredményt produkál.
[77] Karsa 2024; Gartenberg 2024; OpenAI et al. 2024 (GPT-4: 8192 token, GPT-4o: 128 000 token, Gemini 1.5: 1M token).
[78] Gurbuz et al. 2019.
[79] Integrated Sensing and Communications – integrált érzékelés és kommunikáció.
[80] Strinati et al. 2024.



10. ábra: Az ISAC alkalmazás okosvárosi környezetben – a szerző fordítása
Forrás: Kim et al. 2024

Következtetések

A passzív rádiólokáció szempontjából problematikus az alacsony sugárzási energia, de a relatíve kis detektálási távolság és a városi (sűrű) 5G gNB ökoszisztéma kompenzálhatja e kihívások egy részét. A 5G gNB „bőség" lehetővé teszi a multisztatikus passzív rádiólokációs ökoszisztéma kialakítását, eliminálva a mono-/bisztatikus bizonytalanságot, biztosítva a célobjektumok nagyobb pontosságú pozicionálását. Az 5G MIMO- és nyalábképzés technológiák támogathatják a célobjektumok térbeli pozíciójának további pontosítását, mozgási sajátosságainak azonosítását. Az alkalmazott jelmoduláció, az elérhető frekvenciatartományok, a kiaknázható maximális sávszélesség, elméleti szinten magas hatékonyságú passzívradar-megoldások kiszolgálását tenné lehetővé.

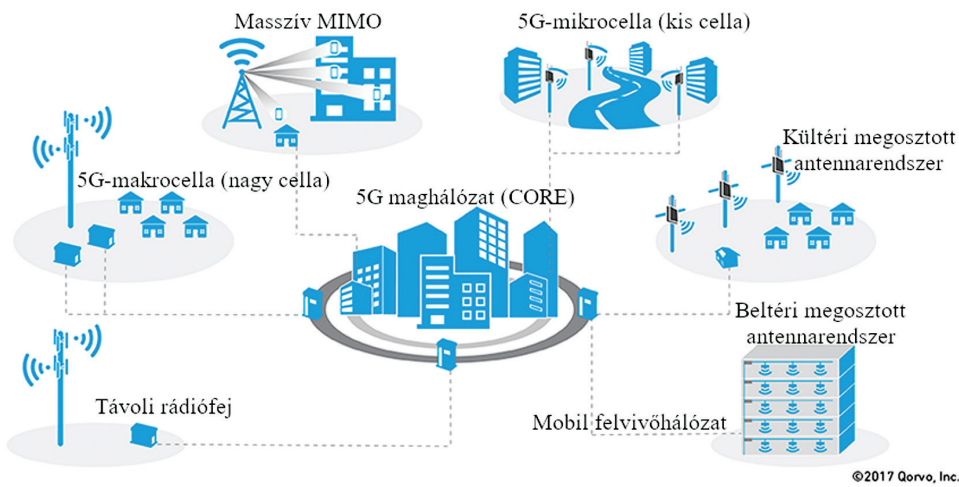
Számos kutatás érvel az 5G IoO-kénti kiaknázhatósága mellett az UAV, földi jármű, emberi jelenlét detektálási forgatókönyvek esetén. A mikro-Doppler-hatás kiaknázására épülő, elsődlegesen az FR2 tartományban hatékony, UAV- és emberi jelenlétet detektáló megoldások a Doppler-spektrogram célobjektum-specifikus – például rotormozgás, emberi tevékenység (járás, légzés) – sajátosságait elemzik.[81] A Rényi-entrópia számításán alapuló, az FR1 tartományban is eredménnyel alkalmazható eljárás, az optimális erősségű (RCS-növelő) jelek, jeltöredékek kinyerésére fókuszál.[82] Az elemzett javaslatok azonban optimális alkalmazási környezetet (belteret, nagyobb és „üresebb" külső területet, légteret) és/vagy folyamatos, jelentős adattartalmú (egyetlen, széles

[81] Kim–Ha–Kwon 2015; Tang et al. 2020.
[82] Maksymiuk et al. 2023.

nyalábon továbbított) forgalmazást, egyes megoldásoknál együttműködő IoO-t feltételeznek. A vizsgált szakirodalom nem kínál egyértelmű megoldást egy 5G-alapú, nem együttműködő IoO ökoszisztémát feltételező passzív rádiólokációs eljárásra.

Az emberi jelenlét, mozgás, illetve a közeltéri objektumok detektálását biztosító „mozgócél-felderítő" (kis méretű, mobilis) katonai és polgári rádiólokációs megoldások jellemzően kis hatótávolságú, folyamatos sugárzású, aktív eszközök.[83] Ehhez hasonló, „kvázi-folyamatos" jellegű sugárzás az FR1 tartomány 1 GHz alatti szegmensével kiszolgált területeken, illetve az *SSB kiaknázásával* érhető el az 5G-hálózatokban. Azonban az SSB-nyalábok paraméterezése, az alkalmazott nyalábok maximális száma tekintetében magas szabadságfok mellett járhatnak el a hálózatüzemeltetők, így az SSB-paraméterezés „végeredménye" nem szükségszerűen esik egybe a rádiólokáció céljaival.[84]

A napjainkban alkalmazott városi FR1 (~3,6 GHz) 5G gNB ökoszisztéma területileg korlátozottan (szektoriálisan) tekinthető praktikus IoO-nak. A jellemzően több tíz méter magasba telepített antennák által kiszolgált városi térnek csak bizonyos hányada rendelkezik közvetlen antennarálátással, amely arány utcaszinten akár 50% alá is csökkenhet.[85] Az FR1 gNB telepítési struktúra az UAV detektálás szempontjából hatékony lehet, de szükséges számolni azzal, hogy a referenciaantennák telepítési pontjainak meghatározása az átlagosnál részletesebb tervezést igényel, a városi környezetben diffrakció és reflexió okozta zavarjelek kezelése jelentős kihívást jelent, valamint, hogy a céltárgy közvetlen megvilágítása nem folytonosan biztosított, különösen a felszínközeli térszegmensekben.



11. ábra: 5G heterogén hálózati struktúra
Forrás: Nguyen 2017 alapján a szerző fordítása

[83] Ferenczy–Szűcs–Balog 1998.
[84] Dreifuerst–Heath 2023.
[85] Az adott térpont megvilágítása függ pl. annak vertikális pozíciójától, a környező tér beépítettségétől, az épített tér sajátosságaitól és egyéb földrajzi jellemzőitől, járműforgalomtól. Lásd Thomas–Willis–Craig 2006.

Egy városi komplex (FR1 + FR2) gNB ökoszisztéma (11. ábra) optimális IoO-hálózatot és többirányú (RCS-növelő) célobjektum-megvilágítást biztosíthat.[86] Az FR1 vázolt rálátási sajátosságai és az FR2 gNB-k alacsony kisugárzási teljesítménye azonban korlátozó tényezőt jelenthet. Ezért a detektálás optimalizálása érdekében kiemelt fontosságú a megfelelően pozicionált, a polarimetrikus diverzitást kiaknázó, akár dinamikus platformra telepített elemekkel kiegészített számos IoO típus kiaknázására képes, többsávos referencia-/megfigyelőantenna ökoszisztéma.[87]

Az FR2 frekvenciatartomány terjedési sajátosságai szükségessé teszik a több cella átfedéses kiszolgálását biztosító antennák sűrű, jellemzően alacsony magasságú telepítését. Mindez biztosíthatja a potenciális felszíni és ahhoz közeli célobjektumok akár több IoO általi megvilágítását.

FR2-ben elvárás az UE és a gNB antennája közti közvetlen rálátás, így a szolgáltatók az SSB-nyalábok paraméterezésekor kerülni fogják a magasabb térpontok és az épületek meddő besugárzását.[88] Azon fiktív esetben, amikor az adott kültéri FR2-es gNB lesz hivatott kiszolgálni[89] a környező épületek kommunikációs igényeit, vagy ha az olyan szolgáltatások, mint az 5G-alapú UAV-vezérlés azt „kikényszerítik", a magasabb térpontok SSB-söprése is megvalósulhat.

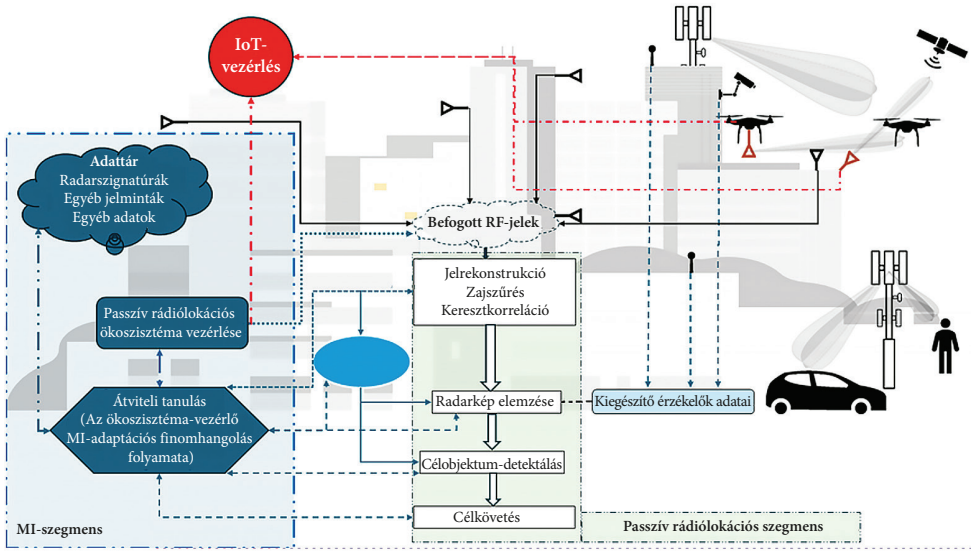
További kihívás, hogy az FR2-es gNB-k esetében várhatóan dinamikusan váltakozik majd az SSB-söprés mintázata, a nyalábok paraméterezése, igazodva a gNB aktuális forgalmazási, igénybevételi sajátosságaihoz. Mindemellett a kis nyalábszélesség, a legfeljebb 200 Hz-es PRF és az FR2-1 esetében az elérhető legnagyobb SSB-sávszélesség (57,6 MHz) további hatékonyságkorlátozó tényezőként jelentkezhet, különösen a kis méretű légi objektumok és az emberi jelenlét detektálása terén.

A vonatkozó hazai jogszabályok[90] által csak közvetetten támogatott kiskapu lehet a mobilkommunikációs szolgáltató által biztosított hozzáférés az 5G RAN-hoz. Ezzel csökkenthető a passzív rádiólokáció referenciajelnek való kitettsége, mivel a szükséges (kisugárzott jelet leíró) információk közvetlenül kinyerhetők az érintett gNB-kből. Emellett a szolgáltató által fel nem használt SSB-nyalábokat a vizsgált térszegmensek felé aktiválva, kibocsátási paramétereiket az adott detektálási feladathoz optimalizálva jelentős többletinformáció kinyerése is biztosítható.

A fent vázoltak alapján egyedüli, nem együttműködő IoO-ként, jelen ismereteink szerint, az 5G korlátozott hatékonyságú. Optimális hatékonyságú megvilágítás az FR1 és FR2 cellastruktúrák egyidejű kiaknázása esetén lehetséges. Egy városi passzív lokációs ökoszisztéma hatékonysága tervezetten telepített (a kiemelt fontosságú területek megvilágítását optimalizáló), IoT-eszközök, valamint az MI alkalmazásával növelhető. Az IoT-szegmens hármas előnyt jelent: aktiváló, pontosító technológiákkal (hang, kép, hő, szeizmikus érzékelők) támogathatja a passzív rádiólokációs szegmenst; megnövelt adatforgalmat generálva biztosíthatja a szükséges (RCS-optimalizáló) megvilágítási

[86] Semkin et al. 2020, Ezuma et al. 2021.
[87] Colone–Filippini–Pastina 2023.
[88] Az FR2 frekvenciák nem hatolnak át a falakon.
[89] Pl. átjátszók révén, amelyek biztosítják az FR2 5G-jel épületbe jutását.
[90] Pl. 2003. évi C. tv., 2021. évi XCIII. tv.

hatékonyságot; illetve dinamikus, automatikusan pozicionálható platformot[91] képezhet az ökoszisztéma érzékelő és adatgeneráló elemei számára.



12. ábra: Egy MI-vezérlésű passzív rádiólokációs ökoszisztéma
Forrás: a szerző szerkesztése

A javasolt ökoszisztémát az alábbi három fő szegmens szimbiózisa alkotja:

- *MI-szegmens biztosítja*
  - az ökoszisztéma feladatspecifikus, a környezet változásait és a detektált célobjektum sajátosságait figyelembe vevő vezérlését;
  - a beérkező RF-jelek és egyéb adatok elemzésének, értékelésének, feldolgozásának, valamint
  - a célobjektum-detektálás és -követés funkciók támogatását;
  - az ökoszisztéma adaptív jellegét és rezilienciáját az átviteli tanulás[92] révén;
  - a releváns adatok tárolását.
- *A passzív rádiólokációs szegmens végzi*
  - az 5G, illetve egyéb IoO-k referencia- és a célobjektumok jeleinek befogását és feldolgozását;
  - a radarkép elemzését, a célobjektumok detektálását és célkövetést, figyelembe véve az IoT-szegmensből származó adatokat, az MI-szegmens támogatásával.
- *Az IoT-szegmens tartalmazza*
  - az ökoszisztémába integrált egyéb (például akusztikus, szeizmikus, videó, LiDAR stb.) szenzorokat;

[91] Pl. UAV, UGV.
[92] Átviteli vagy transzfertanulás. MI-modell tanítási technika, amely lehetővé teszi korábbi feladatokból származó ismeretek felhasználását egy új feladat megoldásához, hatékonyságának növeléséhez. A javaslat vonatkozásában, annak folyamatos önfejlesztő, adaptációs képességére utalok az elnevezéssel.

– a szegmens statikus elemeit (5G-kommunikátorok, megfigyelő- és referenciaantennák); illetve
– dinamikus platformjait (például a fenti pontban jelzett eszközökkel felszerelt UAV-ok).

A városi környezet heterogén, volatilis környezeti jellege és célobjektumok vázolt sajátosságai okán, az MI-szegmens rálátással és irányítási kompetenciákkal kell rendelkezzen, illetve folyamatos tanulás, adaptálódás révén biztosítja a rendszer rezilienciáját. A javasolt ökoszisztéma (lásd 12. ábra) alaphelyzeti állapotban multimodális felderítést végez 5G SSB pásztázás és más IoO-k kiaknázásával, illetve az integrált szenzorhálózat révén. A detektált potenciális célobjektumok mozgását és egyéb paramétereit MI-támogatással elemzi a rendszer. A kiemelt figyelmet igénylő célobjektum detektálása esetén, amennyiben a rendelkezésre álló adatok nem elégségesek, az MI dönthet nagyobb pontosságú információ beszerzéséről. Ennek érdekében célspecifikusan hangolhatja a csatlakoztatott referencia- és megfigyelőantennákat, további adatokat gyűjthet a szenzorhálózatból. Az RCS növelése érdekében hatékonyabb megvilágítási és jelbefogási helyzetbe pozicionálhatja a dinamikus platformokat. Továbbá a célobjektum útvonala mentén a statikus és dinamikus IoT-elemek kommunikátorait aktiválva magas adattartamú, akár 400 MHz sávszélességű nyalábok révén pontosíthatja a kapcsolódó méréseket. A vázolt megoldás hátránya, hogy szemben a hagyományos passzív rádiólokációval, kevéssé mobilis, magasabb a beszerzési és üzemeltetési költsége.

Összegzés

Jelen publikáció rá kívánt mutatni arra, hogy kiemelten városi környezetben az 5G – *köszönhetően olyan jellemzőinek, mint a nagy sávszélesség, masszív MIMO, nyalábformálás, OFDM moduláció stb.* – magas potenciállal rendelkező IoO lehetőség a passzív rádiólokációs ökoszisztémák számára. A releváns szakirodalom elemzését követően, bemutatva alkalmazásának korlátozó tényezőit, az alaphipotézis teljes mértékben nem igazolható. A jelzett hátrányok kompenzálására egy komplex, passzív radar, MI és IoT fő szegmenseken nyugvó megoldást mutattunk be vázlatosan.

Városi környezetben az 5G egy diverz, az IoO-k széles körét (4G, DAB, DVB-T, FM, GNSS, WiFi stb.) alkalmazni képes ökoszisztéma részeként, makro- (FR1) és mikrocellás (FR2) RAN struktúra egyidejű alkalmazása mellett tekinthető egy hatékony passzív rádiólokációs rendszer magas rezilienciájú összetevőjének. IoT-megoldások rendszerbe iktatásával az 5G IoO-k hatékonysága célirányosan és rugalmasan növelhető. MI-támogatással nemcsak a jelfeldolgozás sebessége és komplexitása, de az 5G-t IoO-ként alkalmazó passzív rádiólokációs rendszer alkalmazási köre is rugalmasan növelhető, kitágítva annak katonai/rendvédelmi/civil biztonsági alkalmazását.

Felhasznált irodalom

3GPP.org (2022): *The 5G standard, Release 18.* Online: www.3gpp.org/ftp/Inbox/Marcoms/3GPP_Poster%20v2.pdf

Abratkiewicz, Karol – Księżyk, Adam – Płotka, Marek – Samczyński, Piotr – Wszołek, Jacek – Zieliński, Tomasz Piotr (2023): SSB-Based Signal Processing for Passive Radar Using a 5G Network. *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing,* 16, 3469–3484. Online: https://doi.org/10.1109/JSTARS.2023.3262291

Adib, Fadel – Su, Chen-Yu – Mao, Hongzi – Katabi, Dina – Durand, Frédo (2015): Capturing the Human Figure Through a Wall. *ACM Transactions on Graphics,* 34(6). Online: https://doi.org/10.1145/2816795.2818072

Ashleibta, Aboajeila Milad – Taha, Ahmad – Khan, Muhammad A. – Taylor, William – Tahir, Ahsen – Zoha, Ahmed – Abbasi, Qammer H. – Imran, Muhammad A. (2021): 5G-Enabled Contactless Multi-User Presence and Activity Detection for Independent Assisted Living. *Scientific Reports,* 11. Online: https://doi.org/10.1038/s41598-021-96689-7

Balajti István (2019a): Új kihívások a hazai légtérellenőrzésben. Rendszerintegrálási alapok, passzív rádiólokáció. *Haditechnika,* 53(2), 2–7. Online: https://doi.org/10.23713/HT.53.2.01

Balajti István (2019b): A XXI. századi radarrendszerekkel szemben támasztható elvárások. *Haditechnika,* 53(3), 3–7. Online: https://doi.org/10.23713/HT.53.3.01

Beasley, Piers – Ritchie, Matthew – Griffiths, Hugh – Miceli, William – Inggs, Michael – Simon, Lewis (2020): *Multistatic Radar Measurements of UAVs at X-band and L-band.* 2020 IEEE Radar Conference, Florence, Italy, 2020, 1–6. Online: https://doi.org/10.1109/RadarConf2043947.2020.9266444

Bingli, Liao – Vargas, Vasconcellos (2024): *Extending Token Computation for LLM Reasoning.* arXiv:2403.14932v3. Online: https://doi.org/10.48550/arXiv.2403.14932

Birutis, Agnius – Mykkeltveit, Anders – Ulversøy, Tore – Borlaug, Øystein Dag – Kårstad, Jørn (2022): *A Study of 5G New Radio and Its Vulnerability to Jamming.* Norvegian Defence Research Establishment. Online: www.ffi.no/en/publications-archive/a-study-of-5g-new-radio-and-its-vulnerability-to-jamming

Caro, C. G. – Bloice, J. A. (1971): Contactless Apnoea Detector Based on Radar. *The Lancet* 298(7731), 959–961. Online: https://doi.org/10.1016/S0140-6736(71)90274-1

Chang, Yupeng – Wang, Xu – Wang, Jindong – Wu, Yuan – Yang, Linyi – Zhu, Kaijie – Chen, Hao – Yi, Xioyuan – Wang, Cunxiang – Wang, Yidong et al. (2024): A Survey on Evaluation of Large Language Models. *ACM Transactions on Intelligent Systems and Technology,* 15(3). Online: https://doi.org/10.1145/3641289

Chen, Victor C. – Li, Fayin – Ho, Shen-Shyang – Wechsler, Harry (2006): Micro-Doppler Effect in Radar: Phenomenon, Model, and Simulation Study. *IEEE Transactions on Aerospace and Electronic Systems,* 42(1), 2–21. Online: https://doi.org/10.1109/TAES.2006.1603402

Colone, Fabiola – Filippini, Francesca – Pastina, Debora (2023): Passive Radar: Past, Present, and Future Challenges. *IEEE Aerospace and Electronic Systems Magazine,* 38(1), 54–69. Online: https://doi.org/10.1109/MAES.2022.3221685

Deep, Yoshana – Held, Patrick – Ram, Shobha Sundar – Steinhauser, Dagmar – Gupta, Anshu – Gruson, Frank – Koch, Andreas – Roy, Anirban (2020): Radar Cross-Sections of Pedestrians at Automotive Radar Frequencies Using Ray Tracing and Point Scatterer Modelling. *IET Radar, Sonar & Navigation,* 14(6), 833–844. Online: https://doi.org/10.1049/iet-rsn.2019.0471

Dreifuerst, Ryan M. – Heath, Robert W. (2023): Massive MIMO in 5G: How Beamforming, Codebooks, and Feedback Enable Larger Arrays. *IEEE Communications Magazine,* 61(12), 18–23. Online: https://doi.org/10.1109/MCOM.001.2300064

Ezuma, Martins – Anjinappa, Chethan Kumar – Semkin, Vasilii – Guvenc, Ismail (2021): *Comparative Analysis of Radar Cross Section Based UAV Classification Techniques.* arXiv:2112.09774v1. Online: https://doi.org/10.48550/arXiv.2112.09774

Farkas Tibor (2023): A kommunikációs és információs rendszerek értelmezése napjainkban: Követelmények és kihívások. In Tóth András (szerk.): *Új típusú kihívások az infokommunikációban.* Budapest: Ludovika Egyetemi Kiadó, 11–30.

Fereidouni, Farshad – Mohammadi, Seyed T. – Shahraki, Vahed F. – Jahantigh, Farhad (2022): Human Health Risk Assessment of 4-12 GHz Radar Waves using CST STUDIO SUITE Software. *Journal of Biomedical Physics Engineering,* 12(3), 285–296. Online: https://doi.org/10.31661/jbpe.v0i0.1272

Ferenczy Gábor – Szűcs Péter – Balog Károly (1998): *Rádiólokáció alapjai.* Budapest: Bolyai János Katonai Műszaki Főiskola.

Gartenberg, Chaim (2024): What is a Long Context Window? *Blog.google,* 2024. február 16. Online: https://blog.google/technology/ai/long-context-window-ai-models

Gomez-Del-Hoyo, Pedro – Gronowski, Konrad – Samczynski, Piotr (2022): *The STARLINK-Based Passive Radar: Preliminary Study and First Illuminator Signal Measurements.* 23rd International Radar Symposium (IRS), Gdansk, Poland, 2022, 350–355. Online: https://doi.org/10.23919/IRS54158.2022.9905046

Gurbuz, Sevgi Z. – Griffiths, Hugh D. – Charlish, Alexander – Rangaswamy, Muralidhar – Greco, Maria Sabrina – Bell, Kristine (2019): An Overview of Cognitive Radar: Past, Present, and Future. *IEEE Aerospace and Electronic Systems Magazine,* 34(12), 6–18. Online: https://doi.org/10.1109/MAES.2019.2953762

Haig Zsolt – Kovács László – Ványa László – Vass Sándor – Németh András (2014): *Elektronikai hadviselés.* Budapest: Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar.

Huan, Sha – Wu, Limei – Zhang, Man – Wang, Zhaoyue – Yang, Chao (2023): Radar Human Activity Recognition with an Attention-Based Deep Learning Network. *Sensors,* 23(6). Online: https://doi.org/10.3390/s23063185

Jian, Michael – Lu, Zhenzhong – Chen, Victor C. (2017): *Experimental Study on Radar Micro-Doppler Signatures of Unmanned Aerial Vehicles.* IEEE Radar Conference, Seattle, USA, 2017, 0854–0857. Online: https://doi.org/10.1109/RADAR.2017.7944322

Karlsson, Alexander (2023): *Radar Signal Processing using Artificial Neural Networks.* PhD-disszertáció. KTH, School of Electrical Engineering and Computer Science

(EECS), Intelligent systems, Information Science and Engineering. Online: https://kth.diva-portal.org/smash/record.jsf?pid=diva2%3A1797382

Karsa Róbert (2024): Tűzvédelmi szakértői rendszer létrehozása nagy nyelvi modellek segítségével. *Rendvédelem,* 13(2), 26–36. Online: https://doi.org/10.53793/RV.2024.2.3

Khedkar, Ashok – Musale, Sandeep – Padalkar, Ganesh – Suryawanshi, Ravikant –Sahare, Shashikant (2023): An Overview of 5G and 6G Networks from the Perspective of AI Applications. *Journal of the Institution of Engineers (India): Series B,* 104(6), 1329–1341. Online: https://doi.org/10.1007/s40031-023-00928-6

Kim, Youngwook – Ha, Sungjae – Kwon, Jihoon (2015): Human Detection Using Doppler Radar Based on Physical Characteristics of Targets. *Geoscience and Remote Sensing Letters,* 12(2), 289–293. Online: https://doi.org/10.1109/LGRS.2014.2336231

Kim, Hahyun – Kim, Gayeong – Shim, Sunghoon – Jang, Sukbin – Song, Jiho – Lee, Byungju (2024): Key Technologies for 6G-Enabled Smart Sustainable City. *Electronics,* 13(2). Online: https://doi.org/10.3390/electronics13020268

Kirillov, Alexander et al. (2023): *Segment Anything.* arXiv:2304.02643. Online: https://doi.org/10.48550/arXiv.2304.02643

Koncz Miklós Tamás (2007): Lunenberg reflektor radarkeresztmetszetének mérése összehasonlító módszerrel. *Hadmérnök,* 2(3), 100–185. Online: http://hadmernok.hu/archivum/2007/3/2007_3_koncz.pdf

Księżyk, Adam – Płotka, Marek – Abratkiewicz, Karol – Maksymiuk, Radosław – Wszołek, Jacek – Samczyński, Piotr (2023): Opportunities and Limitations in Radar Sensing Based on 5G Broadband Cellular Networks, *IEEE Aerospace and Electronic Systems Magazine,* 38(9), 4–21. Online: https://doi.org/10.1109/MAES.2023.3267061

Kuschel, Heiner – Cristallini, Diego – Olsen, Karl Erik (2019): Tutorial: Passive Radar Tutorial. *IEEE Aerospace and Electronic Systems Magazine,* 34(2), 2–19. Online: https://doi.org/10.1109/MAES.2018.160146

Li, Wenda – Piechocki, Robert J. – Woodbridge, Karl – Tang, Chong – Chetty, Kevin (2021): Passive WiFi Radar for Human Sensing Using a Stand-Alone Access Point. *IEEE Transactions on Geoscience and Remote Sensing,* 59(3), 1986–1998. Online: https://doi.org/10.1109/TGRS.2020.3006387

Li, Xiang – Wen, Congcong – Hu, Yuan – Yuan, Zhenghang – Zhu, Xiao Xiang (2024): Vision-Language Models in Remote Sensing: Current Progress and Future Trends. *IEEE Geoscience and Remote Sensing Magazine,* 12(2), 32–66. Online: https://doi.org/10.1109/MGRS.2024.3383473

Lin, Luning – Yu, Ningning – Wang, Yong – Shi, Zhiguo (2023): *5G Spectrum Learning-Based Passive UAV Detection in Urban Scenario.* IEEE/CIC International Conference on Communications in China (ICCC), Dalian, China, 2023, 1–5. Online: https://doi.org/10.1109/ICCC57788.2023.10233342

Lin, Xingqin – Li, Jingya – Baldemair, Robert – Cheng, Jung-Fu Thomas – Parkvall, Stefan – Larsson, Daniel Chen (2019): 5G New Radio: Unveiling the Essentials of the Next Generation Wireless Access Technology. *IEEE Communications Standards Magazine,* 3(3), 30–37. Online: https://doi.org/10.1109/MCOMSTD.001.1800036

Liu, Hongshan – Qin, Tong – Gao, Zhen – Mao, Tianqi – Ying, Keke – Wan, Ziwei – Qiao, Li – Na, Rui – Li, Zhongxiang – Hu, Chun – Mei, Yikun – Li, Tuan – Wen, Guang-

hui – Chen, Lei – Wu, Zhonghuai – Liu, Ruiqi – Chen, Gaojie – Wang, Shuo – Zheng, Dezhi (2024): *Near-Space Communications: the Last Piece of 6G Space-Air-Ground-Sea Integrated Network Puzzle.* arXiv:2401.00283. Online: https://doi.org/10.34133/space.0176

Liu, Yan – Dan, Yangpeng – Wan, Xianrong – Yi, Jianxin (2022): *Investigations on 5G-Based Passive Sensing for IoT Applications.* IEEE 8th International Conference on Computer and Communications (ICCC), Chengdu, China, 2022, 823–828. Online: https://doi.org/10.1109/ICCC56324.2022.10065876

Lyu, Xiaoyong – Liu, Baojin – Fan, Wenbing (2022): Signal Processing in Passive Radar with Multi-User MIMO-OFDM Signal. *EURASIP Journal on Advances in Signal Processing,* 113. Online: https://doi.org/10.1186/s13634-022-00947-3

Maksymiuk, Radosław – Hoyo, Pedro Gomez del – Abratkiewicz, Karol – Samczynski, Piotr – Kulpa, Krzysztof (2024): 5G-Based Passive Radar on a Moving Platform – Detection and Imaging. *IET Radar, Sonar & Navigation,* 18(12), 2414–2426. Online: https://doi.org/10.1049/rsn2.12559

Maksymiuk, Radosław – Płotka, Marek – Abratkiewicz, Karol – Samczyński, Piotr (2023): *5G Network-Based Passive Radar for Drone Detection.* 24th International Radar Symposium (IRS), Berlin, Germany, 1–10. Online: https://doi.org/10.23919/IRS57608.2023.10172437

NATO STO (2017): *Passive Coherent Locator History and Fundamentals.* 2017. augusztus 23. Online: www.sto.nato.int/publications/STO%20Educational%20Notes/STO-EN-SET-243/EN-SET-243-01.pdf

Nguyen, Tuan (2017): Small Cell Networks and the Evolution of 5G (Part 1). *Qorvo.com,* 2017. május 17. Online: https://www.qorvo.com/design-hub/blog/small-cell-networks-and-the-evolution-of-5g

Núñez-Ortuño, José M. – González-Coma, José – López, Rubén Nocelo – Troncoso-Pastoriza, Francisco – Álvarez-Hernández, María (2023): Beamforming Techniques for Passive Radar: An Overview. *Sensors (Basel),* 23(7). Online: https://doi.org/10.3390/s23073435

OpenAI et al. (2024): *GPT-4 Technical Report.* arXiv:2303.08774v6. Online: https://doi.org/10.48550/arXiv.2303.08774

Pető Tamás (2013): *Több csatornás DVB-T alapú passzív radar.* BME Villamosmérnöki és Informatikai Kar. 2013. október 25. Online: https://tdk.bme.hu/VIK/HWBeagy/Tobb-csatornas-DVBT-alapu-passziv-radar

Pultarova, Tereza (2025): Starlink Satellites: Facts, Tracking and Impact on Astronomy. *Space.com,* 2025. március 28. Online: https://www.space.com/spacex-starlink-satellites.html

Ramalingam, Manoharan (2018): 5G NR Beam Management and Beam Scheduling (everything about the beams). *LinkedIn,* 2018. július 12. Online: www.linkedin.com/pulse/5g-nr-beam-management-scheduling-everything-beams-ramalingam

Skolnik, Merrill I. (1981): *Introduction to Radar Systems. Second Edition.* Singapore: McGraw-Hill.

Seller Rudolf – Pető Tamás – Dudás Levente – Kovács Levente (2019): Passzív radar. I. rész. *Haditechnika,* 53(6), 51–55. Online: https://doi.org/10.23713/HT.53.6.10

Seller Rudolf – Pető Tamás – Dudás Levente – Kovács Levente (2020): Passzív radar. II. rész. *Haditechnika,* 54(1), 43–47. Online: https://doi.org/10.23713/HT.54.1.09

Semkin, Vasilii – Haarla, Jaakko – Pairon, Thomas – Slezak, Christopher – Rangan, Sundeep – Viikari, Ville (2020): Analyzing Radar Cross Section Signatures of Diverse Drone Models at mmWave Frequencies. *IEEE Access,* 8, 48958–48969. Online: https://doi.org/10.1109/ACCESS.2020.2979339

Strinati, Emilio Calvanese – Alexandropoulos, George C. – Amani, Navid – Crozzoli, Maurizio – Madhusudan, Giyyarpuram – Mekki, Sami – Rivet, Francois – Sciancalepore, Vincenzo – Sehier, Philippe – Stark, Maximilian – Wymeersch, Henk (2024): *Towards Distributed and Intelligent Integrated Sensing and Communications for 6G Networks.* arXiv:2402.11630. Online: https://doi.org/10.1109/MWC.001.2400056

Tang, Chong – Li, Wenda – Vishwakarma, Shelly – Chetty, Kevin – Julier, Simon – Woodbridge, Karl (2020): *Occupancy Detection and People Counting Using WiFi Passive Radar.* 2020 IEEE Radar Conference (RadarConf20), Florence, Italy, 2020, 1–6. Online: https://doi.org/10.1109/RadarConf2043947.2020.9266493

Tarzanagh, Davoud Ataee – Li, Yingcong – Zhang, Xuenchen – Oymak, Samet (2023): *Max-Margin Token Selection in Attention Mechanism.* arXiv:2306.13596v4. Online: https://doi.org/10.48550/arXiv.2306.13596

Thi Phuoc Van, Nguyen – Tang, Liqiong – Demir, Veysel – Hasan, Syed F. – Minh, Nguyen D. – Mukhopadhyay, Subhas (2019): Review-Microwave Radar Sensing Systems for Search and Rescue Purposes. *Sensors,* 19(13). Online: https://doi.org/10.3390/s19132879

Thomas, Nicholas J. – Willis, Mike J. – Craig, Ken H. (2006): The Relative Importance of Different Propagation Mechanisms for Radio Coverage and Interference Prediction in Urban Scenarios at 2.4, 5.8, and 28 GHz. *IEEE Transactions on Antennas and Propagation,* 54(12), 3918–3920. Online: https://doi.org/10.1109/TAP.2006.886571

Tóth András (2023a): Az Internet of Things rendszerek biztonsági kihívásai. In Tóth András (szerk.): *Új típusú kihívások az infokommunikációban.* Budapest: Ludovika Egyetemi Kiadó, 99–136.

Tóth András (2023b): Az 5G-technológia jellemzői és a kialakításában rejlő kihívások. In Tóth András (szerk.): *Új típusú kihívások az infokommunikációban.* Budapest: Ludovika Egyetemi Kiadó, 51–98.

Vaswani, Ashish – Shazeer, Noam – Parmar, Niki – Uszkoreit, Jakob – Jones, Llion – Gomez, Aidan N. – Kaiser, Lukasz – Illia Polosukhin (2017): *Attention Is All You Need.* arXiv:1706.03762v7. Online: https://doi.org/10.48550/arXiv.1706.03762

Wang, Siqin – Xiao, Huang – Li, Yun – Zhang, Ce – Ning, Huan – Zhu, Rui – Li, Zhenlong – Ye, Xinyue (2024): GPT, Large Language Models (LLMs) and Generative Artificial Intelligence (GAI) Models in Geospatial Science: A Systematic Review. *International Journal of Digital Earth,* 17(1). Online: https://doi.org/10.1080/17538947.2024.2353122

Wu, Shengqiong – Fei, Hao – Qu, Leigang – Chua, Tat-Seng (2024): *NExT-GPT: Any-to-Any Multimodal LLM.* arXiv:2309.05519v3. Online: https://doi.org/10.48550/arXiv.2309.05519

Wührl, Tibor – Baross, Márk Tamás – Gyányi, Sándor – Varga, Péter János (2023): *5G Synchronization Problems with GNSS Interference.* IEEE 6th International CANDO-EPE Conference, Budapest, Hungary, 2023, 149–154. Online: https://doi.org/10.1109/CANDO-EPE60507.2023.10417998

Xu, Fengtong – Hong, Tao – Zhao, Jincheng – Yang, Tao (2019): Detection and Identification Technology of Rotor Unmanned Aerial Vehicles in 5G Scene. *International Journal of Distributed Sensor Networks,* 15(6). Online: https://doi.org/10.1177/1550147719853990

Xu, HanXiang – Wang, Shenao – Li, Ningke – Wang, Kailong – Zhao, Yanjie – Chen, Kai – Yu, Ting – Liu, Yang – Wang, Haoyu (2024): *Large Language Models for Cyber Security: A Systematic Literature Review.* arXiv:2405.04760v2. Online: https://doi.org/10.48550/arXiv.2405.04760

Yamada, Naoyuki – Tanaka, Y. – Nishikawa, Kunitoshi (2005): *Radar Cross Section for Pedestrian in 76GHz Band.* European Microwave Conference, Paris, France, 2005. Online: https://doi.org/10.1109/EUMC.2005.1610101

Zhang, Duzhen – Yu, Yahan – Dong, Jiahua – Li, Chenxing – Su, Dan – Chu, Chenhui – Yu, Dong (2024): *MM-LLMs: Recent Advances in MultiModal Large Language Models.* arXiv:2401.13601v5. Online: https://doi.org/10.18653/v1/2024.findings-acl.738

HADMÉRNÖK
VÉDELEMINFORMATIKA
19. évfolyam (2024) 4. szám 109–120.
DOI: 10.32567/hm.2024.4.7

Pozderka Gábor[1]

A NATO kiberműveleti szervezeti elemeinek evolúciós vizsgálata

Evolutionary Analysis of the Elements of NATO's Cyber Operations Organisations

Absztrakt

A NATO 2016-os varsói csúcstalálkozóján az országok vezetői egyetértettek abban, hogy a kibertér önálló hadszíntér (domain), és a védelme részét képezi a NATO kollektív védelmi feladatainak. Ennek megfelelően megkezdődött a korábban széttagoltan létező képességek, és az ezek irányításáért felelős szervezeti elemek feladatrendszerének újragondolása, a feladatok végrehajtásához szükséges akciótervek kialakítása. Jelen publikáció célja a NATO kibervédelmi és kiberműveleti szervezeti elemeinek evolúciós vizsgálata, illetve annak elemzése, hogy ennek következtében milyen feladatok azonosíthatók a nemzeti végrehajtás során. Értelemszerűen ez az evolúciós folyamat nem fejeződött be, a terület sajátosságából adódóan folyamatosan új feladatok jelennek meg akár napi szinten, ezen változások hatással vannak a szervezeti struktúra kialakítására is.

Kulcsszavak: NATO, kibertér, szervezetek, evolúció

Abstract

At the NATO's Warsaw Summit in 2016, leaders agreed that cyberspace is a separated domain and that its defence is part of NATO's collective defence mission. Accordingly, the rethinking of the previously fragmented capabilities and the system of tasks of the organisational elements responsible for managing them began, and the development of action plans necessary for the implementation of tasks. The aim of this publication is to

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: pozderka.gabor@hm.gov.hu

examine the evolutionary elements of NATO's cyber defence and cyber operations and to analyse what tasks can be identified during national implementation as a result. Obviously, this evolutionary process has not yet been completed, due to the peculiarity of this field, new tasks are constantly appearing even on a daily basis, and these changes also affect the formation of the organisational structure.

Keywords: NATO, cyberspace, organisation, evolution

Bevezetés

Az információs technológia és az internet globális elterjedésével párhuzamosan a kiberfenyegetések is egyre nagyobb jelentőséget nyertek a mindennapi életben és a védelmi szektorban egyidejűleg.[2] A North Atlantic Treaty Organization (NATO), mint vezető katonai szövetség, felismerte, hogy a hagyományos katonai fenyegetések mellett a kiberbiztonság, kibervédelem és az ezekre épülő kiberműveletek is fokozatosan kulcsfontosságúvá váltak. Ennek eredményeként a NATO 2016-os varsói csúcstalálkozóján az országok vezetői egyetértettek abban, hogy a kibertér önálló hadszíntér *(domain),* ezért a védelme részét képezi a NATO kollektív védelmi feladatainak, ebben a tekintetben a Szövetségnek ugyanúgy képesnek kell lennie megvédeni a tagállamokat, mint a hagyományos hadszíntereken vívott harcok során.[3]

Természetesen a fenti kinyilatkoztatást számos korábbi lépés előzte meg, aminek egyik fontos előkészítő eleme volt a NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE – NATO Kibervédelmi Kiválósági Központ) megalakítása Észtországban. A lokáció kiválasztásának szimbolikus jelentősége is volt, így üzenve a világnak, hogy a kibertérben elkövetett cselekedeteknek súlyuk van, azokat a NATO figyelemmel kíséri, és megkezdi a szükséges eljárásrendek kidolgozását. A kibervédelmi feladatok megjelenésével értelemszerűen a korábban kialakított infokommunikációs és információvédelmi szervezeti elemek feladatrendszerének újragondolása vált szükségessé, ami a szervezeti elemek strukturális átalakítását is magával hozta.

Jelen publikáció fókuszterülete a műveleti szintű képességelemek és feladatrendszer vizsgálata, azonban érintőlegesen megjelenik a komplexitás megértéséhez szükséges stratégiai keretrendszer is. Ismertetem azokat a szervezeti elemeket, amelyek az evolúciós folyamat részét képezték, valamint elemzem azokat a folyamatokat, amelyek a kibertér jelenleg kialakult keretrendszerét meghatározták. Hipotézisként megfogalmazható, hogy a NATO-ban zajló, kiberteret érintő evolúciós folyamatok hatással voltak a nemzeti szabályzói struktúra kialakítására, illetve a szövetségi szinten jelenleg is zajló átrendeződés befolyásolni fogja a jövőbeni képességek kialakulását, ebben a formában is irányt mutatva a szakterületnek.

[2] Haleliuk 2024.
[3] NATO 2016.

Kezdeti lépések

Fontos megjegyeznünk, hogy mint minden más szakterület esetében, így a kiberterületen is a North Atlantic Council (Észak-atlanti Tanács, NAC), a NATO legfőbb politikai döntéshozó testülete hozza meg azokat a stratégiai döntéseket, amelyek meghatározzák a stratégiai irányokat, figyelembe véve a NATO Military Committee (Katonai Bizottság, MC) által megfogalmazott javaslatokat, amely a tagállamok legfelsőbb katonai vezetőit, a vezérkari főnököket tömörítő testülete a szervezetnek. A vezérkari főnökök általában az úgynevezett állandó katonai képviselők személyével képviseltetik az országukat, de csakúgy, mint a Tanács, időről időre a legmagasabb szinten, a vezérkari főnökök személyes jelenlétével folynak az ülések. A NAC alatt több bizottság végzi feladatait, szakterületet érintően a NATO Cyber Defence Committee (Kibervédelmi Bizottság, CDC), amelynek az evolúció eredményeként jelenleg feladata a NATO kibervédelmi politikáinak és kezdeményezéseinek felügyelete és irányítása, továbbá fő célja, hogy politikai irányítást és stratégiai iránymutatást adjon a kibervédelem területén. A szakterületi képességfejlesztésre szintén hatással vannak a Security Committee (Biztonsági Bizottság, SC) és a Defense Policy and Planning Committee (Védelmi Politikai és Tervezési Bizottság, DPCC) javaslatai.

A NATO számára a kibervédelem jelentősége az évek során egyre nőtt, különösen a 2000-es évek közepétől kezdődően. Kezdetben a tevékenységek a probléma elméleti megértésére korlátozódtak, kerekasztal-beszélgetések során kezdték meg azonosítani a lehetséges sérülékenységi vektorokat. Észtország 2003-ban, már a hivatalos NATO-csatlakozása előtt javaslatot tett egy kiválósági központ létrehozására. A 2006. évi rigai csúcstalálkozó felsorolta a lehetséges számítógépes támadásokat a közös biztonságot érintő aszimmetrikus fenyegetések között, és az információs rendszerek hosszú távú védelmét szolgáló programok szükségességét szorgalmazta. A 2007-es Észtország elleni kibertámadások[4] először világítottak rá a NATO-országok, intézményeik és társadalmaik, sőt maga a NATO esetleges sebezhetőségére az információs és kommunikációs rendszerük megzavarásával. A 2008. áprilisi NATO-csúcstalálkozón Bukarestben a részt vevő államfők közleményben nyilvánították ki elkötelezettségüket amellett, hogy erősítsék a kiberbiztonsági folyamatokat, és felkészülnek a kibertámadások kivédésére.[5]

A kibertérben érzékelhető fokozódó nyomás hatására a valós, kézzelfogható produktumok előállítása nem volt tovább halogatható, ennek eredményeként az első valóban jelentős lépés 2008-ban történt meg, amikor létrehozták Tallinnban a NATO CCD COE-t a NATO teljes jogú szervezeti elemeként. Célja a tapasztalatok és a konzultáció alapján javítani a kibervédelem hatékonyságát, az együttműködést és az információ megosztását a tagországok és a kibervédelemben részt vevő partnerei között. Ez a központ kutatási, elemzési, képzési, valamint gyakorlati támogatást nyújt a tagállamoknak a kibervédelem terén. A tallinni Kibervédelmi Központ egyike annak a 21 akkreditált NATO Kiválósági Központnak, amely a szövetség precíziós technikai műveleteivel kapcsolatos képzést nyújt. Nemzeti és multinacionális alapon

[4] Bányász–Orbók 2013.
[5] Ottis 2007.

finanszírozzák, mivel a központok szorosan kapcsolódnak a Szövetséges Transzformációs Parancsnoksághoz, és elősegítik a szövetség által jóváhagyott fejlesztési célok megvalósulását. Magyarország 2010-ben csatlakozott a központhoz,[6] ezzel is erősítve a nemzeti és nemzetközi információáramlás hatékonyságát, valamint növelve a központ kibertérben való lefedettségét. A Központhoz 2024. év végéig 32 ország csatlakozott szponzorként (további 7 ország jelezte jövőbeni csatlakozási szándékát), feladatrendszeréből adódóan együttműködési kapcsolatokat létesíthet a nem NATO-államokkal, egyetemekkel, kutatóintézetekkel és vállalkozásokkal is, mint közreműködő résztvevőkkel.

Feladatrendszere az évek során folyamatosan bővült és átalakult, jelenlegi portfóliója tartalmazza az alábbi tevékenységeket:

Kezdeti funkciók:

- a kibervédelmi együttműködés javítása a NATO Network Enabled Capability (NATO Hálózat Alapú Képesség – NNEC) környezetében;[7]
- megtervezni a doktrína- és koncepciófejlesztést, valamint előkészíteni azok jóváhagyását;
- az információbiztonsági és a kibervédelmi oktatás, a tudatosság erősítése és a képzés fejlesztése;
- kibervédelmi támogatás biztosítása kísérletekhez (beleértve a helyszínen is);
- a kibervédelem jogi szempontjainak elemzése.

Tapasztalatok alapján bővített funkciók:

- a hozzájárulás a Kibervédelmi Központ gyakorlataihoz és sztenderdjeinek fejlesztéséhez a NATO-val, a PfP[8]-vel, a NATO-jelöltekkel és a nem NATO-államokkal;
- hozzájárulás a kibervédelemmel kapcsolatos NATO biztonsági gyakorlatok kidolgozásához, a katonai felelősségi kör meghatározása a kibervédelemben;
- kibervédelem-központú képzés, figyelemfelkeltő kampányok, workshopok és tanfolyamok szervezése;
- kibervédelem-központú gyakorlatok fejlesztése és lebonyolítása, valamint kibervédelmi gyakorlatok támogatásának képessége;
- kibervédelem biztosítása a NATO-val kapcsolatban álló kkv-k részére, és e kibervédelem hatékonyságának vizsgálata, megerősítése.

Szervezeti változások

Az oktatás és felkészítés mellett fokozatosan egyre nagyobb hangsúly helyeződött a technikai feladat-végrehajtásra, a kiberbiztonsági incidensek egyre nagyobb számban jelentek meg a hagyományos üzemeltetési incidensek mellett. Erre válaszul a NATO Kommunikációs és Információs Rendszerszolgáltatási Ügynöksége (NCSA) szervezetén

[6] CCD COE [é. n.].

[7] NNEC – a Szövetség azon kezdeményezése, amelynek célja, hogy erősítse a képességek integrálását minden szinten, a stratégiai szinttől a taktikaiig, valamint a katonai és polgári területeken egyaránt, egy robusztus információs infrastruktúra segítségével.

[8] Az egyes euroatlanti partnerországok és a NATO közötti kétoldalú együttműködési program.

belül már 2007-től kezdődően egyre jelentősebb mértékben jelen volt a kezdetben INFOSEC[9] terület részeként megjelenő kibervédelem, amely fokozatosan átalakította a rendszerek üzemeltetéshez kapcsolódó feladatrendszerét is. A NATO NCIRC (NATO Computer Incident Response Capability), a NATO Számítógépes Incidens Reagálási Képesség kezdeti kialakítása erre az időszakra tehető. Feladataként határozták meg, hogy észlelje, megelőzze és elhárítsa a NATO informatikai rendszereit fenyegető kiberbiztonsági incidenseket.

A NATO Kommunikációs és Információs Ügynöksége (NCIA) 2012. július 1-jén jött létre a NATO Konzultációs, Vezetési és Irányítási Ügynöksége (NC3A), a NATO ACCS Menedzsment Ügynöksége (NACMA) és az NCSA elemeinek összevonásával. Az Ügynökség létrehozása egy szélesebb körű NATO-reform részeként valósult meg, amely nemcsak a kibervédelemmel kapcsolatos feladatok hangsúlyosabb megjelenését jelentette, hanem a biztonság és üzemeltetés kérdéskörének újragondolását is előrevetítette. Az NCIA feladatrendszerét tekintve mai napig kiszolgálja a NATO szervezeteit és a nemzeteket, mint a NATO informatikai, kibervédelmi és C4ISR szolgáltatója. Az NCIA feladatrendszere fokozatosan egészült ki a NATO-műveletek támogatásához szükséges mobil kommunikációs elemekkel, valamint a szükséges kibervédelmi eljárásokkal.

A NATO annak érdekében, hogy súlyos kibertámadások esetén azonnali segítséget legyen képes nyújtani a NATO-tagállamok részére, 2012-ben létrehozta az első Cyber Rapid Reaction Team (RRT) képességet. Ez egy speciális csapat, amely túlnyomóan civil kiberbiztonsági szakértőkből áll, szükség esetén bevethetők a NATO bázisain vagy a tagállamok támogatására akár helyszínen is. Ezzel a lépéssel kívánták nyomatékosítani, hogy a NATO kollektív védelmi kötelezettségének a kibertér is szerves részét képezi, amely kimondja az Észak-atlanti Szerződés 5. cikkében, hogy egy tag elleni támadást minden tag elleni támadásnak tekintenek. A csapat rendszeres gyakorlatokon vesz részt, annak érdekében, hogy fenntartsa és javítsa felkészültségét és reagálási képességeit. Fontos megjegyezni, hogy ez egy igen korlátozott képesség, a tagállamok csak limitáltan lesznek képesek igénybe venni, ezért saját hasonló képességeik fejlesztése prioritásként kell hogy megjelenjen.

A NATO Cyber Security Centre (NCSC) 2016 októberében kezdte meg működését, székhelye a belgiumi Monsban, a Szövetséges Erők Európai Főparancsnokságán (SHAPE) található. Az NCSC az NCIA része, és elsődlegesen a szövetség kiberbiztonsági képességeinek fejlesztésére és fenntartására irányul, központosított és éjjel-nappal működő kibervédelmi támogatással védi a NATO saját hálózatait. Ez a képesség folyamatosan fejlődik, és lépést tart a gyorsan változó fenyegetési és technológiai környezettel.

A NATO funkciójából adódóan saját, offenzív képességek kialakítására nem fókuszál, ezért 2017-ben a NATO Védelmi Tanácsa döntést hozott arról, hogy SCEPVA (Sovereign Cyber Effects Provided Voluntarily by Allies) megnevezés alatt a tagállamok önkéntes vállalás alapján felajánlhatják nemzeti kiberképességeik integrálását a szövetséges hadműveletek és küldetések támogatására. Ebben a formában offenzív kiberhatásokkal is hozzájárulhatnak a szövetséges hadműveletek és küldetések

[9] INFOSEC – Information Security.

sikerességéhez, a NATO-tagállamok közötti együttműködés keretében a nemzetközi jog szabályainak alkalmazásával.[10]

A kiberszervezeti evolúció egyik jelentős mérföldköve volt, hogy 2018 októberében a NATO bejelentette a NATO Cyber Operation Centre (NATO Kibertér Műveleti Központ, CyOC) kezdeti felállítását és kísérleti fázisban való alkalmazását. A CyOC a NATO kibertérbeli hadszíntéri komponenseként látja el feladatait, felelős az aktuális kiberhelyzetkép kialakításáért, a központosított kibertérműveletei tervezésért, valamint a kibertérműveleti kihívások koordinálásáért. A CyOC parancsnoka szorosan együttműködik az Infokommunikációs szakterület (CIS-J6) vezetőjével, feladatuk összehangolásáért a DCOS (Cyber) felelős, aki közvetlenül a Szövetséges Fegyveres Erők Európai Főparancsnoka (Supreme Allied Commander Europe, SACEUR) részére teszi meg jelentését. Talán kevesen tudják, de fontos megjegyeznem, hogy e nemzetközi szervezeti elem legelső parancsnokának Vass Sándor dandártábornokot választották ki számos nemzetközi jelölt közül. Szakmai munkájával megteremtette a szervezet mindennapi működéséhez szükséges keretrendszert, valamint meghatározta a jövőbeni feladat-végrehajtás irányát.

A VCISC-t (Virtual Cyber Incident Support Capability), magyarul Virtuális Kiberesemény-támogató Képességet 2023-ban, a vilniusi NATO-csúcstalálkozón ratifikálták és vezették be. Ez egy olyan központi NATO-szolgáltatás, amely támogatja a tagállamok nemzeti szintű kiberbiztonsági intézkedéseit jelentős kiberfenyegetések esetén. A VCISC portfóliójának kialakítása jelen pillanatban is zajlik, a csatlakozás hozzá önkéntes alapon állandó vagy megfigyelő nemzetként lehetséges.

A korábban felsorolt erőfeszítések koordinációja érdekében jött létre a NATO Cyber Commanders Forum (CCF), magyarul NATO Kiberparancsnokok Fóruma. Ezen a platformon a NATO-tagállamok és partnerországok kiberparancsnokai évente 2 alkalommal megvitatják a kibervédelemmel kapcsolatos erőfeszítések és feladatok aktuális helyzetét, irányokat határoznak meg az elkövetkező időszakra. A fórum célja, hogy erősítse a szövetséges kibervédelmi képességeket, megoszthassák a legjobb gyakorlatokat és fejlesszék a közös válaszokat a globális kiberkihívásokra. Mivel a NATO- és EU-nemzetek számos esetben átfedést mutatnak, így nem meglepő módon az EU Cyber Commanders Conference (CyberCo)[11] feladatai nagyobbrészt e feladatokkal összhangban vannak, így megvalósítva és biztosítva a szoros szakmai együttműködést.

A szabályzói környezet változása

Az átalakítás fontos része volt az egyes tagállamok nemzeti kiberbiztonsági stratégiáinak kidolgozása és elfogadása. Magyarország már 2013-ban elfogadta a Nemzeti Kiberbiztonsági Stratégiáját, amely hangsúlyozta a kritikus infrastruktúrák védelmét és az információs biztonságot. Ezeket a stratégiákat a NATO szintjén is integrálták, biztosítva ezzel a koherens és hatékony együttműködést.[12] A NATO több straté-

[10] CCD COE 2017.
[11] EU Kiberparancsnokok Konferenciája: https://hungarian-presidency.consilium.europa.eu/hu/esemenyek/eu-kiberparancsnokok-konferenciaja
[12] Kovács 2019.

giai dokumentumot és politikát fogadott el, amelyek a kibervédelem fejlesztésére és koordinálására irányultak. Az egyik ilyen jelentős dokumentum a NATO 2014-es Kibervédelmi Politikai Irányelvei, amely meghatározta a kibervédelemmel kapcsolatos elvárásokat és irányelveket. Emellett létrehozták a korábban említett NCSC-t, amely hatékonyabb technikai szakértelmet, incidenskezelést és kiberbiztonsági szolgáltatásokat biztosít a NATO rendszerei számára.

2016-ban megkezdődött a Cyber Defence Pledge vállalások kialakítása, amelyben a NATO-tagállamok elkötelezték magukat a nemzeti kibervédelmi képességeik megerősítésére és összehangolására, ez szoros kapcsolatban áll a NATO Defence Planning Process (NATO Védelmi Tervezési Folyamat, NDPP)[13] vállalásaival. Ennek további erősítése céljából 2020-ban véglegesítették a 2016-os vállalások végrehajtási tervét, amely konkrét intézkedéseket tartalmaz a tagállamok közötti együttműködés erősítésére. Ez a kidolgozói munka folyamatos megújulást tesz szükségessé a részt vevő nemzetek részéről is, Magyarország ebben aktív szerepet vállal, a meghatározott célok megvalósulására kiemelt figyelmet fordít. 2020-ban a NATO elfogadta a kibervédelmi stratégiáját, amely az országok közötti együttműködést és az információs védelmet hangsúlyozza.[14]

2022-ben az Atlanti Tanács kiadta a *Kibervédelmi Kézikönyv*et, amely részletes útmutatást ad a tagállamok számára a kiberbiztonság megvalósítására, információt nyújt a NATO kibervédelmi megközelítéséről. A kézikönyv különböző kibervédelmi kihívásokat fogalmaz meg, beleértve a kibervédelmi elveket, stratégiákat és a legjobb gyakorlatokat, amelyeket a NATO és tagállamai követnek a hálózataik és információs rendszereik védelme érdekében.

A kézikönyv tartalmazza az alábbi fontos irányelveket:

- *kibervédelmi elvek:* a kibervédelem alapvető fogalmainak és irányelveinek bemutatása;
- *stratégiai és taktikai megközelítések:* a fenyegetések észlelésére, megelőzésére és reagálására vonatkozó részletes stratégiákat és taktikákat;
- *legjobb gyakorlatok:* a múlt kiberincidenseikből származó példák és tanulságok;
- *képzések és gyakorlatok:* információ a képzési programokról és gyakorlatokról, mint például a Cyber Coalition, amely az egyik legnagyobb kibervédelmi gyakorlat a világon;
- *együttműködés és koordináció:* irányelvek a NATO-tagállamok közötti együttműködés és koordináció érdekében a kibervédelmi képességek erősítésére.

A NATO a fenti folyamatok erősítése és tesztelése érdekében kibervédelmi gyakorlatok rendszerét alakította ki, amelyek több szinten valósulnak meg. Némelyek a döntéshozatali szintet célozzák meg és a mandatálási folyamatokra fókuszálnak, másokban a technikai feladatok jelennek meg túlnyomó részben. Tendenciaként megfigyelhető, hogy a komplex gyakorlatok irányába tolódik el a fókuszpont, így is szimulálva a valós, mindennapi élethez hasonlító feladat-végrehajtást. Mivel a nemzetek véges erőforrásokkal rendelkeznek, így megkezdődött e kibervédelmi és kiberműveleti gyakorlatok

[13] NATO 2022.
[14] Păunescu 2021.

újragondolása is, annak érdekében, hogy a valóban releváns folyamatok gyakoroltatása szerepeljen elsődleges prioritásként a jövőben. Egyre hangsúlyosabban jelenik meg eme gyakorlatok során a katonai műveletek sikeres végrehajtása érdekében biztosított civil infrastruktúra védelme, amely előrevetíti a civil szolgáltatókkal való szorosabb együttműködést.

A NATO a nemzetközi együttműködést kiemelt fontosságú területként kezeli, ennek érdekében komplex szervezeti rendszert üzemeltet.[15] Az együttműködés más nemzetközi szervezetekkel, mint például az EU, az ENSZ és az EBESZ, lehetőséget biztosít az információk és legjobb gyakorlatok megosztására, valamint a közös kiberhadgyakorlatok megszervezésére. A NATO és az Európai Unió (EU) közötti technikai szintű kiberbiztonsági kapcsolatokért felelős szervezet a NATO NCIRC és a CERT-EU.[16] Ezek a szervezetek együttműködnek a kiberfenyegetések megelőzése, észlelése és reagálása, valamint az információcsere és a technikai együttműködés érdekében.

Folyamatban lévő változások

A NATO-tagországok 2024. július 10-én megállapodtak egy új központ létrehozásáról az egyre kifinomultabb kiberfenyegetésekkel szembeni hatékonyabb védelem érdekében. A NATO Integrált Kibervédelmi Központja (NICC)[17] a tervek szerint fokozni fogja a NATO és a szövetséges hálózatok védelmét és a kibertér műveleti területként való használatát. Feladata lesz a NATO katonai parancsnokainak tájékoztatása a kibertér lehetséges fenyegetéseiről és sebezhetőségeiről, ez magában foglalja a katonai tevékenységek támogatásához szükséges, magántulajdonban lévő polgári kritikus infrastruktúrák fokozott védelmét is, így erősítve a katonai-civil kapcsolatokat. Nem elképzelhetetlen, hogy a korábban CIMIC[18] funkcióként azonosított feladatrendszer új alapokat fog kapni, és részlegesen kapcsolati link alakul ki a kiberszakterülettel. Ez az új központ különbözik a NATO Kiválósági Központjaitól, amelyeket a tagállamok függetlenül működtetnek, és amelyek a képzésre és a kutatásra összpontosítanak. Az NICC közvetlenül a NATO parancsnoki struktúrája alá tartozik, ötvözve a polgári és katonai vezetést a műveleti támogatás nyújtása és a jövőbeli kiberképességek fejlesztése érdekében.

A pontos tervek jelen pillanatban még nem nyilvánosak, az NICC felépítésére és funkcióira vonatkozó részleteket az elkövetkező hónapokban dolgozzák ki, azonban az már most is látszik, hogy az évek alatt kialakult szervezetek feladatrendszerét ismételten át fogják tekinteni, az integráció elkerülhetetlen a hatékonyság növelésének érdekében. Elhelyezése Belgiumban a Supreme Headquarters Allied Powers Europe (SHAPE)[19] bázisán tervezett, feltételezhetően a publikációban korábban felsorolt szervezeti elemek jelentős része érintett lesz az átalakulásban.

[15] Bányász–Krasznay–Tóth 2021.
[16] Az Európai Unió Kibereseményekre Reagáló Csoportja.
[17] NATO 2024.
[18] Civil-Military Cooperation.
[19] Lásd: https://shape.nato.int/

A tervek szerint 2028-ra teljesen működőképes központi fejlett technológiákat fog alkalmazni a kibertér helyzetismeretének és ellenálló képességének fokozása érdekében, igénybe fogja venni a mesterséges intelligencia által biztosított technikai megoldásokat is. Finanszírozása a NATO közös költségvetéséből és a tagállamok önkéntes hozzájárulásaiból származik majd. Ennek a központnak a létrehozása tükrözi a szövetség válaszát a növekvő kiberfenyegetésekre, amelyeket felerősítenek az olyan geopolitikai feszültségek, mint az ukrajnai háború.

Jövőbeni igények és lehetőségek

A NATO kibervédelmi szervezeti elemeinek folyamatos fejlesztése kulcsfontosságú, hogy lépést tartsanak a gyorsan változó és egyre összetettebb kibertámadásokkal. Az alábbi pontokban megfogalmazott javaslatok figyelembevétele elősegítheti az ezekre a feladatokra való felkészülést nemzeti szempontból is:

- *Innováció és kutatás:* Nagyobb hangsúlyt kell fektetni az új technológiák és kiberbiztonsági megoldások kutatására és fejlesztésére. Ez magában foglalja a mesterséges intelligencia, a gépi tanulás és a kvantum-számítástechnika alkalmazását a kiberfenyegetések észlelésében és elhárításában.
- *Képzés és oktatás:* Folyamatosan frissített és bővített képzési programok biztosítása a kibervédelmi szakemberek számára. Ezzel javítható a szakemberek felkészültsége és reakcióképessége az új típusú támadásokkal szemben.
- *Nemzetközi együttműködés:* Erősíteni kell az együttműködést a NATO részéről más nemzetközi szervezetekkel. Ez lehetővé teszi az információk és legjobb gyakorlatok megosztását, valamint a közös kibergyakorlatok megszervezését. Nemzeti téren ennek szintén kiemelt prioritásként kell megjelennie.
- *Incident Response Capability:* Fejleszteni kell a kibertámadásokra való gyors reagálás képességét, beleértve a jelentős incidensek koordinálását és elhárítását. Ez magában foglalja a gyorsreagálási csapatok (a NATO esetében az RRT) bővítését és az új eszközök és technikák bevezetését.
- *Kiberfegyverzetek szabályozása:* Fontos, hogy a NATO támogassa a nemzetközi szinten elfogadott szabályokat és irányelveket a kiberfegyverzetek használatára vonatkozóan. Ez hozzájárulhat a kiberhadviselés szabályozottabbá és kiszámíthatóbbá tételéhez. A kibertérben való feladat-végrehajtás jogi aspektusainak vizsgálatát tovább kell folytatni, biztosítani kell a kibertérerők számára szükséges felkészülést a kibertérben történő fegyveres konfliktusokra.
- *Integrált kiberbiztonsági stratégiák:* Az egyes tagállamok nemzeti kiberbiztonsági stratégiáinak integrálása és harmonizálása a NATO általános stratégiájával. Ez koherensebb és hatékonyabb védekezést eredményezhet.

Ezek a fejlesztések hozzájárulhatnak ahhoz, hogy a NATO kibervédelmi képességei még hatékonyabbak és ellenállóbbak legyenek a jövőbeni kihívásokkal szemben.

Összegzés

A publikációban felsorolt szervezeti elemek együtt dolgoznak a NATO kibervédelmi képességeinek folyamatos fejlesztésén és fenntartásán, együtt alkotják a szövetség kibervédelmi és kiberműveleti képességeit az ismertetett szabályzói környezetnek megfelelően. A NATO kibervédelmi rendszerének átalakítása egy átfogó és komplex folyamat volt, amely magában foglalta a stratégiai és szervezeti változásokat, a kiberbiztonsági stratégiák és keretrendszer kidolgozását, új szervezetek létrehozását, folyamatos képzéseket és a nemzetközi együttműködést. A NATO ezen evolúciós folyamat következő állomásaként döntött az NICC megalakításáról, a szervezeti elemek ismételt felülvizsgálatáról. Ezek az intézkedések biztosítják a NATO számára a rugalmas és hatékony kibervédelmi képességeket a jövőbeni kihívásokkal szemben.[20]

A NATO rendszereinek alrendszerként részét képezik a nemzeti rendszerek is, ezzel számos jövőbeni veszélyforrás jelentkezik a kibertérből. Ezek közül a jellemzőbb veszélyforrások:

- *Agresszív kiberhadviselés:* Az Oroszország és más államok által végrehajtott agresszív kiberhadviselési támadások jelentős fenyegetést jelentenek. Ezek a támadások gyakran célba veszik a NATO-tagállamok kritikus infrastruktúráit, mint például az energia- és vízszolgáltatási rendszerek, a közlekedési hálózatok és a pénzügyi szektor.
- *Hibrid támadások:* A hibrid támadások kombinálják a kiberfenyegetéseket a fizikai támadásokkal, amelyek célja az infrastruktúra megrongálása és a társadalmi káosz kiváltása. Ezek a támadások komplexek és nehezen megelőzhetők.
- *Szabotázs és káosz:* Az ismert hacker- és APT (Advanced Persistent Threat) csoportok által végrehajtott szabotázsakciók célja a rendszerek leállítása és a hálózatok megrongálása ideológiai vagy financiális célból. Ezek a támadások komoly kárt okozhatnak, különösen akkor, ha célba veszik a kritikus infrastruktúrákat.[21]
- *Erősödő kiberfegyverzetek:* Az országok folyamatosan fejlesztik kiberfegyvereiket, amelyek egyre hatékonyabbak és veszélyesebbek lesznek. Ezek a fegyverek képesek lehetnek komplex támadások végrehajtására, amelyeket nehezen lehet azonnal azonosítani és elhárítani. A korai előrejelző rendszerek alkalmazása fel fog értékelődni, és megjelennek a mesterséges intelligencia használatával kapcsolatos félelmek.
- *Közösségi média és dezinformáció:* A kiberfenyegetések nem korlátozódnak a technikai támadásokra. A dezinformáció és a manipulált információk terjesztése is jelentős veszélyforrás, ami negatív irányba befolyásolja az emberek gondolkodását és a társadalmi bizalmat. A PSYOPS[22] egyre inkább összekapcsolódik a kiberszakterület műveleti feladat-végrehajtásával, valamint a műveleti tervezéssel. Ezeknél a folyamatoknál az előzetes tervezés mellett fontos szerepet játszik az időtényező, a bekövetkezett eseményekre adott válaszidő.

[20] Brent 2019.
[21] Johnson 2015.
[22] PSYOPS – Psychological Operations.

Ezek a veszélyforrások folyamatosan változnak és fejlődnek,[23] így a NATO rendszereinek, folyamatainak, szabályzóinak és szervezeti elemeinek rendszeres felülvizsgálata, modernizálása elengedhetetlen a biztonság megőrzése érdekében. Megállapítható, hogy a nemzeti rendszerek és képességek során elsődlegesen a fenti veszélyforrások kezelésére kell felkészülni, oly módon, hogy a kihívásokra adott válaszok kielégítsék a NATO-szerepvállalásból adódó követelményrendszert is.[24]

A kezdetben megfogalmazott hipotézis igazolása a folyamatok vizsgálata során beigazolódott, egyértelművé vált, hogy a NATO-ban végbement, kiberteret érintő evolúciós folyamatok hatással voltak a nemzeti szabályzói struktúra és szervezeti elemek kialakítására. Ezen logikát követve bizonyítható, hogy a szövetségesi rendszerben jelenleg zajló változások meg fogják mutatni az irányt a nemzeti képességfejlesztés számára, a „jövőbeni igények és lehetőségek" pontban megfogalmazott követelmények minden szervezeti elem számára feladatokat fognak meghatározni, amelyek már most körvonalazódnak. A vállalások összehangolását nagymértékben elősegíti a Cyber Defence Pledge során megfogalmazott irányelvek szisztematikus követése, azonban a nemzeti sajátosságok beépítése prioritást kell hogy élvezzen. A nemzetek hasonló problémákkal fognak szembesülni a feladat-végrehajtás folyamán, a hagyományos határok csekély mértékben értelmezhetők a kibertérben végrehajtandó műveletek során, a civil szolgáltatok szerepe fel fog értékelődni.[25]

Felhasznált irodalom

Bányász Péter – Krasznay Csaba – Tóth András (2021): A NATO kibervédelmi szakpolitikája. In Szenes Zoltán (szerk.): *A mai NATO: a szövetség helyzete és feladatai.* Budapest: HM Zrínyi Térképészeti és Kommunikációs Szolgáltató Nonprofit Kft., 130–149.

Bányász Péter – Krasznay Csaba – Tóth András (2022): A kibervédelem szakpolitikai szintjének helyzete és kihívásai Magyarországon, az EU-banés a NATO-ban. *Military and Intelligence Cybersecurity Research Paper,* (8), 1–30. Online: https://bit.ly/3TUU2lf

Bányász Péter – Orbók Ákos (2013): A NATO kibervédelmi politikája és kritikus infrastruktúra védelme a közösségi média tükrében. *Hadtudomány,* 23(E-szám), 188–209.

Brent, Laura (2019): NATO's Role in Cyberspace. *NATO Review,* 2019. február 12. Online: www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html

CCD COE [é. n.]: Hungary Joins the Centre. Online: https://web.archive.org/web/20130430095220/http:/www.ccdcoe.org/188.html

CCD COE (2017): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations to Be Launched.* Online: https://assets.cambridge.org/97811071/77222/frontmatter/9781107177222_frontmatter.pdf

[23] Kovács 2023.
[24] 2024. évi LXIX. törvény.
[25] U.S. Cyber Command 2023.

Dinnis, Heather Harrison (2012): *Cyber Warfare and the Laws of War.* Cambridge: Cambridge University Press.
Haleliuk, Ross (2024): *Cyber for Builders: The Essential Guide to Building a Cybersecurity Startup.* Venture in Security.
Johnson, Thomas A. (2015): *Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare.* New York: Routledge.
Kovács László (2019): *Kiberbiztonság és -stratégia.* Budapest: Ludovika.
Kovács László (2023): *Hadviselés a 21. században: kiberműveletek.* Budapest: Ludovika.
NATO (2016): *Warsaw Summit Communiqué. Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Warsaw 8–9 July 2016.* Online: www.nato.int/cps/en/natohq/official_texts_133169.htm
NATO (2022): *NATO Defence Planning Process.* 2022. március 31. Online: www.nato.int/cps/en/natohq/topics_49202.htm
NATO (2024): *Allies Agree New NATO Integrated Cyber Defence Centre.* 2024. július 10. Online: www.nato.int/cps/en/natohq/news_227647.htm
Ottis, Rain (2007): *Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective.* CCD COE. Online: https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf
Păunescu, Dragoș-Mihai (2021): NATO's Encounters in the Cyber Domain. In Ghiba, Daniel – Popescu, Lucian – Olariu, Cosmin – Mustață, Adi (szerk.): *Proceedings of the 17th International Scientific Conference "Strategies XXI" – Strategic Changes in Security and International Relations*, XVII. 153–158.
Samtani, Sagar – Chai, Yidong – Chen, Hsinchun (2022): Linking Exploits from the Dark Web to Known Vulnerabilities for Proactive Cyber Threat Intelligence: An Attention-Based Deep Structured Semantic Model. *MIS Q, Computer Science,* 46(2), 911–946. Online: https://doi.org/10.25300/MISQ/2022/15392
U.S. Cyber Command (2023): *2023 Posture Statement of General Paul M. Nakasone.* 2023. március 7. Online: www.cybercom.mil/Media/News/Article/3320195/2023-posture-statement-of-general-paul-m-nakasone

Jogi források

2024. évi LXIX. törvény Magyarország kiberbiztonságáról. Online: https://net.jogtar.hu/jogszabaly?docid=a2400069.tv

HADMÉRNÖK
VÉDELEMINFORMATIKA
19. évfolyam (2024) 4. szám 121–130.
DOI: 10.32567/hm.2024.4.8

Szűcs Attila[1]

Mit ad és mit vesz el tőlünk a mesterséges intelligencia?

What Does Artificial Intelligence Give and Take Away from Us?

Absztrakt

Az a kijelentés, hogy a mesterséges intelligencia megváltoztatja az életünket, manapság kissé közhelyesen hangzik. Megváltoztatja. De hogyan? Úgy, mint minden új technológia, amit a mindennapi életben használni kezdünk, ahogyan ez akkor történt, amikor a kézi erő helyett a munkafolyamatokat gépek kezdték végezni? Vagy ami most zajlik, az a változás még ennél is mélyebb, a civilizáció egészére nézve hoz gyökeres változást? Olyat, amilyen változást a tűz használata hozott? Jelen tanulmány célja, hogy túllépve a közhelyeken, mélyebb, strukturált elemzést nyújtson arról, hogy a mesterséges intelligencia (MI) hogyan formálja át civilizációnkat. Ennek érdekében elemző-értékelő módszer segítségével vizsgálom meg, hogy az MI alkalmazásának négy fő területén – kutatás, egészségügy, közlekedés, adatbiztonság – mi az, amivel az MI hozzájárult az emberek jólétéhez, biztonságához, biztonságérzetéhez, és mi az, amiben ennek éppen az ellenkezője tapasztalható. A vizsgálat során kiemelten kívánok foglalkozni az MI alkalmazásának az oktatásra gyakorolt hatásaival mint olyan területtel, amely a jövő szempontjából meghatározó jelentőségű.

Kulcsszavak: mesterséges intelligencia, biztonság, biztonságérzet

Abstract

The claim that Artificial Intelligence will change our lives is a bit of a cliché these days. It is changing. But how? Like all the new technologies we start using in our daily lives, as it

[1] Tanársegéd, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Híradó Tanszék, e-mail: szucs.attila@uni-nke.hu

happened when work processes started to be done by machines instead of by hand power? Or, is what is happening now a change even more profound, a radical change for civilisation as a whole? A change like that brought by the use of fire? The aim of this paper is to go beyond the clichés and provide a deeper, structured analysis of how artificial intelligence (AI) is reshaping our civilisation. To this end, I will use an analytical evaluation method to examine what AI has contributed to people's well-being, security and sense of security in four main areas of AI application – research, health, transport, data security – and what it has done in the opposite direction. In this study, I want to focus on the impact of the use of AI in education as a key area for the future.

Keywords: artificial intelligence, security, sense of security

Bevezetés

A technológia használatát ugyan vissza lehet utasítani, de nem érdemes. Kevés kivétellel elmondható, hogy aki a technológia változásával nem tart lépést, az lemarad a versenytársakkal szemben. Ezzel a kijelentéssel csak kevés kivétel állítható szembe, és azok is nagyon speciálisak. Olyanok, akik a fejlődés helyett egyfajta állandóságra törekvést igyekeznek megvalósítani, és ezzel üdítő színfoltként képesek a fennmaradásra a modern, versenyalapú gazdasági, politikai életben. Ilyenek az amerikai amisok, a kanadai hutterita közösségek önfenntartó farmjai.[2] Hiába kisebbek az általuk elérhető hektáronkénti hozamok, ha kisebb költségekkel is termelnek, akkor ez kiegyenlítődik. Ezt erősíti az is, ha ehhez nem párosul a folyamatos növekedésre, meggazdagodásra való törekvés, mert így a mérleg egyensúlyban van és fenntartható. Ők a köréjük épült nimbusz[3] miatt képesek arra, hogy a termékeiknek állandó, biztos piacot biztosítsanak. Ez egyfajta védjegy, amelyet egy sajátos spirituális hangulat is körülleng. Ez az a plusz, amivel képesek biztosítani helyüket a szabad piacon az ott meglévő versenyhelyzetben is.

A cégek és vállalkozások azonban normálisan a profit maximalizálásában érdekeltek. Ez lebeg minden részvénytársaság menedzsmentjének szeme előtt. A versenyben haladni kell, előnyösebb pozíciót kell elfoglalni akkor is, ha az adott technológia hatásaival kapcsolatban megbízható hosszú távú vizsgálatok még nem történtek. Ami viszont pillanatnyilag áldás, az hosszabb távon átokká válhat. Legismertebb példa erre a DDT[4] rovarirtó szer története, amiért Paul Hermann Müller 1948-ban orvosi Nobel-díjat kapott, végül az 1970-es évek második felére az egész világon betiltották.[5] Amikor bevezették az alkalmazását, csak azt nézték, hogy mi az, amit a DDT mint technológia adni tud, az esetleges negatív hatásokat nem vagy alig vizsgálták. Az energetika szektorban hasonló az 1950-es években az emberiség energiaéhségét egy csapásra megoldani képes technológiaként kikiáltott maghasadás elvén működő atomerőmű. Bár ebben az esetben nem került sor nemzetközi tilalom kimondására, csupán egyes országok hirdették ki atomsemlegességüket és hagytak fel az atomerőművek üzemeltetésével

[2] Bárkai 2017.
[3] Dicsfény, hírnév, kivívott tekintély.
[4] Diklór-difenil-triklóretán.
[5] Turusov–Rakitsky–Tomatis 2002.

és építésével.[6] Történt ez az évtizedek során bekövetkezett nagy környezeti károkkal járó nukleáris balesetek, katasztrófák nyomán.[7]

A mesterséges intelligencia használatával kapcsolatosan volt olyan kezdeményezés, amelyben annak vezető amerikai fejlesztői azt kérték, hogy 6 hónapra függesszenek fel minden, a GPT-4-nél erősebb MI-fejlesztést. Legalább addig, amíg a törvényi szabályozás el nem készül.[8] Ez a kezdeményezés azóta csendben elsikkadt.

Ezek figyelembevételével a kutatás során a következő kérdésekre keresek választ. A MI alkalmazásának civilizációnkra gyakorolt hatása mennyire tekinthető radikális fordulatnak? Ez csupán egy új eszköz, vagy teljes életmódváltást eredményező körülmény? Célom feltárni, hogy a technológiában rejlő lehetőségek hogyan hatnak a társadalmi egyenlőség kérdésére és az egyén biztonságára, biztonságérzetére. A mérleg nyelve ugyanis e tekintetben korántsem egyértelműen pozitív. Mint látni fogjuk, a veszélyek legalább akkora kihívást jelentek, mit ahány problémára megnyugtató választ kapunk.

Amit a mesterséges intelligenciának köszönhetünk

Ha valakinek hirtelen nekiszegezik a kérdést, hogy mit kaptunk a mesterséges intelligenciától, akkor, ha az illető nem napi szinten foglalkozik a kérdéssel, el kell gondolkozzon. Mert első ránézésre semmi különöset nem tulajdonítunk ennek azon kívül, hogy gyorsabbak és pontosabbak lettek az internetes kereséseink és az online fordítóprogramok, valamint hogy a tanulók az iskolai feladatokat meg tudják íratni valamelyik MI-alkalmazással.[9] De ez csupán a jéghegy csúcsa.

Az MI hatalmas plusz potenciált jelent a tudományos kutatások során, amikor nagy mennyiségű adatot kell elemezni, amikor nagy adatbázisokban kell összefüggéseket feltárni. Az MI olyan strukturált adatbázisokkal és strukturálatlan adathalmazokkal képes dolgozni, amelyeket nevezhetünk akár felhőnek (Cloud), adattónak (Data Lake), vagy hivatkozhatunk rá big data-ként, az mindenképpen elmondható róla, hogy sokkal nagyobb és összetettebb, mint ami az ember számára átlátható.

Tipikusan ilyen terület a történelem során oly sokszor a megszámlálhatatlan szinonimájaként használt csillagok világával foglalkozó tudomány.[10] A csillagászatban hatalmas segítséget jelentenek a kutatóknak az MI-alkalmazások, hiszen nemcsak a vizsgált objektumok száma „megszámlálhatatlan", hanem az objektumok tulajdonságai is csak hatalmas skálán mozgó paraméterekkel írhatók le. Az MI segít az adatgyűjtésben a „fényes pontokról", az összehasonlításban, kiértékelésben, olyan változókra is ráirányítva a kutatók figyelmét, amelyek adott esetben nem is szerepeltek a vizsgált kritériumok között. Az MI továbbá nem csupán sokkal nagyobb adatbázisokban képes keresni, eligazodni, hanem a feldolgozás sebessége is sokkal kedvezőbb a korábbi eljárásokkal összehasonlítva.

[6] Németország 2022 végéig leállította atomerőműveit.
[7] 1986 Csernobil, 2011 Fukusima.
[8] *Pause Giant AI Experiments: An Open Letter* 2023.
[9] ChatGPT, Google Bard, Snapchat MY AI stb.
[10] Lao et al. 2021.

Az űr nagyságához képest persze eltörpül, de nem kevésbé összetett az emberi szervezet és annak működése, hát még a működésben fellépő rendellenességek és azok okai. Az MI az orvosi diagnosztika területén is hatalmas előrelépést adott.[11] A már meglévő adatbázisokban tárolt eredmények alapján betanított diagnosztikai rendszerek sokkal pontosabban és gyorsabban képesek kiértékelni a képalkotó vizsgálatok felvételeit, mint az ember. Továbbá nem jelentkezik a leterheltségből, a fáradtságból adódó figyelmetlenség, ami a mai egészségügyi ellátórendszerben sajnos elkerülhetetlenül jelen van. Nem befolyásolják érzelmi tényezők, hogy egy szimpatikus, bájos idős hölgyet vizsgál vagy egy zsörtölődő, mosdatlan hajléktalant. Az MI nem kisebb segítség a megfelelő terápia vagy étrend kialakításánál sem. Nincs szükség hosszas táblázatokban keresgélésre, kalóriaszámolgatásokra, ezeket a kívánt paraméterekkel másodpercek alatt előállítja, rengeteg időt és energiát spórolva az egészségügyi szakszemélyzetnek.

Az egészségügyi ellátásban dolgozók terheinek csökkentése mellett az egyéni biztonságérzetet is nagyban növelik a személyi használatú okoseszközök, amelyek lehetővé teszik a távoli adatgyűjtést és a távdiagnosztikát.[12] Az ezeket viselők számára az, hogy nem kell elmenniük az orvoshoz és ott vizsgálatokra várakozniuk, nem csupán kényelmi, de egyben biztonsági kérdés is. Hiszen a folyamatos felügyelet így a nap 24 órájában biztosítható az idős, krónikus betegségben szenvedők részére.

A mesterséges intelligencia szintén sokat adott az emberek mindennapi életét alapvetően meghatározó nagy ellátórendszerek optimális működtetéséhez. Ezek azok az alapvető szolgáltatások, amelyek nélkül a modern technikai civilizáció elképzelhetetlen. A villamosenergia-hálózat irányítása, a logisztikai elosztó rendszerek, hogy ott és olyan mennyiségű áru legyen, amennyi szükséges, a tömegközlekedés koordinálása, a telekommunikációs rendszerek kiszolgálása. Ha csupán az elsőt, a villamosenergia-hálózatot nézzük, a megújuló „zöldenergia" termelő egységek[13] nagyszámú megjelenése okozta rendszerirányítási kihívás az MI nélkül kezelhetetlen fennakadásokat okozna.[14] Az optimális időszakokban a termelés helyén keletkező, sok helyen egyszerre fellépő pluszkapacitást kell koordinálni és elirányítani a felhasználás helyére. Kompenzálni kell továbbá azokat az időszakokat is, amikor nem süt a nap és a szél sem fúj. Ilyenkor nagyon gyorsan van szükség arra, hogy a rendszerben meglévő pufferkapacitást jelentő, általában fosszilis energiát elégető erőműveket bekapcsoljuk a termelésbe, hiszen a szolgálatatáskiesés nem lehet opció. Egy ilyen erőmű, akár szén-, akár kőolaj- vagy földgázüzemű, azonban nem egy gombnyomásra indul. Azt fel kell fűteni, „fel kell pörgetni". Egy MI, amely figyeli a hálózati kapacitásváltozásokat, előzetes betanítás során megismerte a fogyasztási görbéket, figyelembe veszi a meteorológiai előrejelzéseket, az tudja stabilan biztosítani a korlátozásmentes működést.

A mindennapi életben a kényelmi szolgáltatások terén a személyi asszisztens és okosotthon-alkalmazások azok a területek, ahol az MI a legkézenfekvőbben járul hozzá az életminőségünk javításához. Ennek a területnek a legszélsőségesebb formáját a Japán Gateboxnál fejlesztették ki, kombinálva azt egy szociális chatbot lehetőségeivel.

[11] Devosa–Grósz–Kardos 2020.
[12] Tisóczki 2022.
[13] Otthoni naperőművek, szélerőművek.
[14] Csatár 2018.

Itt már az ember személyes törődés és figyelem iránti szociális igényit is figyelembe vették a személyi asszisztens szolgáltatási csomagban.[15] Az asszisztensünk formát is ölt egy csinos hologram képében, érdeklődik hogylétünk felől, a hangulatunkat analizálva szabadidős programot ajánl, az okos háztartási eszközök használatával biztosítja a napi szükségletek ellátását. Erről már tényleg elmondható, hogy ez már a technológia pihe-puha ölelése.

Amit a mesterséges intelligencia elvesz

Mint minden éremnek, így az MI használatának is két oldala van. Ami jótékonyan körbevesz, az egyszersmind be is zár. Az az algoritmus, amely a saját érdeklődési körünk szerint ajánl tartalmat az interneten, azt is elfedi, hogy léteznek más hírek is, mint amikre általában rákeresünk, és létezik a világnak más megvilágítása is, mint ami szerint általában szemléljük azt. Az amúgy is könnyen kialakuló véleménybuborékok jelensége így sokkal markánsabban jelentkezhet. Ha pedig ezt valamilyen gazdasági vagy politikai befolyásolás céljával manipulálják, akkor az már nem pusztán etikátlan, de bizonyos helyeken törvénytelen is. De lássuk be, a hatalom megszerzése és megtartása sohasem volt az átláthatóság pozitív példája. A pártok és a politikában befolyásra törekvő szervezetek egy-egy lejáró kampány során az alapvető etikai normákat is simán figyelmen kívül hagyják.[16] Az apokalipszis négy lovasa, a járványok, a háborúk, az éhínség és a katasztrófák mára kiegészültek a hamis hírrel, amely ha sikeresen működik, ugyanolyan pusztító hatású lehet. Bedönthet egy céget, megbuktathat egy politikust, de akár áruhiányhoz vagy extrém esetben háborúhoz vezethet.[17] Ha a világról alkotott nézeteink formálásában a minket kiszolgáló MI véleményvezérekhez irányít, azzal elveszi, vagy legalábbis érzelmileg lekorlátozza az önálló értékítélet alkotásának szabadságát.

A képszerkesztő és egyéb képzőművészeti MI-alkalmazások pedig az emberi kreativitásnak jelentenek kihívást. A mesterséges intelligencia által generált tartalmak szerzői jogi szempontból amúgy is kívül esnek a szabályozáson, és jelenleg is szakértői viták tárgyát képezik.[18] Az ilyen alkalmazások az alkotás folyamatában így általános megközelítésben egyszerűen segédeszköznek számítanak.[19] Ezeknek a használata ugyanakkor akaratlanul is egyfajta uniformizálódás felé vezet. Elég megnéznünk azokat az arcokat és alakokat, amelyek ezeken a műveken megjelennek. A rendszer mindig optimalizál, azaz középértékre közelít. Minél több lesz a középértékre generált tartalom az újabb tartalom létrehozása során, az annál inkább egységesedik, uniformizálódik.

A képalkotó és videószerkesztő alkalmazások egyre tökéletesebbé válásával igazzá válik az, hogy ne higgyünk a saját szemünknek se! Az ilyen alkalmazások nem csupán fake pornó előállítására képesek, hanem arra is alkalmasak, hogy velük eltüntessük egy valós fényképen szereplő személy ruháját. Az ilyen módon manipulált tartalmak

[15] Singh et al. 2019.
[16] Négyesi 2020.
[17] Lányi–Réger 2022.
[18] Grad-Gyenge 2023.
[19] Google's DeepDream vizuális tartalmakra; Magenta, Sony Flow Machines zenei tartalmak generálására stb.

már nem csak az egyéni biztonságérzetünkre vannak negatív hatással. Az MI ilyen módon elveszi a látott képek és videók hitelességébe vetett hitet, ami ilyen nehéz háborús időkben – amikor a propagandagépezetek amúgy is maximális erőbedobással működnek a közvéleményt formálásában – kritikus kihívást jelent a globális biztonságra. Kérdésessé teszi a közölt bizonyítékok hitelességét. Minden és mindenki megkérdőjelezhetővé válik.

A demokráciába vetett bizalom is így inoghat meg. Az MI-alkalmazások, mint például a térfigyelő és beléptető rendszerek, amelyek az objektív biztonságérzetet hivatottak javítani, arra is alkalmasak, hogy a polgárok felett gyakoroljanak állami szintű felügyeletet.[20] Kínában ezekre az okosváros-alkalmazásokra építve dolgozták ki az úgynevezett társadalmi kreditrendszert. Az arcfelismerés, a mimika és egyéb érzelemkifejezések elemzése lehetővé teszi a viselkedésminták meghatározását, a nem kívánt viselkedésminták kiszűrését. A személyi szabadságjogok nagyon könnyen a társadalmi érdekre való hivatkozással szoríthatók háttérbe.

Az Amerikai Egyesült Államok kormánya ugyan úgy döntött, hogy bojkottálja a Dahua, a Hikvision, a Huawei vállalatok és 118 kapcsolható cég termékeit, de ezt az intézkedést nem a polgárok szabadságjogainak tiszteletben tartása miatt hozta. Tette ezt nemzetbiztonsági okokra hivatkozva, egyszerűen azért, mert ezekben a technológiákban potenciális kínai kémkedési lehetőséget lát.

Ebben az esetben az állam mint gondoskodó rendszer lép fel, hasonlóan a gondoskodó személyi asszisztens által működtetett digitális környezethez.

Ne feledkezzünk meg a katonai felhasználásról sem.[21] Az MI ezen a területen szépen lassan a „piros gomb" megnyomását veszi ki a katonák kezéből. Ami az automatizált légvédelmi rendszerek esetében a sebesség és az összetettség miatt magától értetődik, az egyéb területeken lassan és a látszólagos humán kontroll megtartása mellett történik. A kontroll azért látszólagos, mert bár a mesterséges intelligenciának csupán a döntés-előkészítésben szánunk szerepet, de valójában ezt az „előkészített döntést" már véglegesnek is tekinthetjük. Ha a döntéshozó kap is arról értesítést, hogy a döntési alternatíva felállítása során mely rendszerek hogyan vettek részt, az annak részleteit aligha fogja tartalmazni.[22] Ugyan ki lesz az a parancsnok, aki, amikor villog a piros gomb, hogy „Tüzelj!", akkor hezitálni kezd és megerősítést kér? Ha kér is, akkor ugyan kitől kérne? Éppen ezért katonai berkeken belül fokozottan elmondható az, ami általánosan az MI döntéshozatali előkészítést támogató funkciókra igaz, hogy aki a nagy szent és érthetetlen szerint cselekszik, azt aligha vonják felelősségre, még ha hibázik is. Aki viszont ezt kétségbe vonva hibázik, azt biztosan.

Az önálló gondolkodásról való leszoktatás egy másik nem kevésbé problematikus jelenség, amikor egy MI-alkalmazás megold helyettünk minden feladatot. Megírja az iskolai dolgozatot, összeállítja a munkahelyi beszámolót, megoldási javaslatokat tesz az éppen aktuálisan minket foglalkoztató problémákra. A tanulás-tanítás évszázados modellje felbomlik. Az ismeretek így nem véső dnek be, nem születnek meg az önálló gondolkodás során kialakuló összefüggések, egyfajta digitális demencia alakulhat ki.[23]

[20] Nagy 2021.
[21] Négyesi 2023.
[22] Szűcs 2023.
[23] Szűts 2024.

Ez pedig már nem csupán fizikai függés a technológiától, mint ahogyan az elektromos hálózat esetén mára kialakult, hanem valóban annak létezésünkké válása.

Összegzés

Sokan és sok területen várják, hogy az MI mint megváltó minden problémát megold majd. Sokat emlegetett tétel, hogy az új MI-alapú technológiák megoldást jelentenek a klímaváltozás okozta élelmiszerválságra, lehetővé téve az erőforrások optimálisabb kihasználását,[24] hiszen új távlatokat nyit a kórokozók terjedésének megakadályozásában, a kártevők gyors észlelésében és elhárításában, az élelmiszer-elosztásban az elosztóláncokban fellépő problémák gyors kezelésében. A termelési helyen a várható öntözési igény előrejelzésében és biztosításában, vagy éppen a szarvasmarhák tejhozamának optimalizálásában a szenzorok és az MI-vezérelt okoseszközök alkalmazásával. Segíti a változó környezethez alkalmazkodó új termelési eljárások kialakítását. Egyvalamit azonban ezek a megoldások sem képesek létrehozni: új erőforrásokat.

A csodavárás másik területe a konfliktuskezelés. Ha mindenki ismeri a másik szándékait és lehetőségeit, akkor a kihívásokra megfelelően tud majd válaszolni. Nem történik túlreagálás, felesleges erőfitogtatás, a technológia kiegyenlíti a képességeket. A helyzet ezzel szemben az, hogy a hozzáférés nem demokratikus, és ezért a konfliktusokat nem mérsékelni fogja, hanem az erőfölényben lévő erejét sokszorozza meg. Persze egy konfliktust ez a megoldás is képes lehet elfojtani, ha az abban részt vevők közül valamelyik hegemón szerepbe kerül. Akkor annak az akarata érvényesül, a többi pedig ennek fogja alávetni magát.

Más megközelítésben a konfliktusok akkor is hatékonyan kezelhetők, ha a döntéshozatali mechanizmusba egy abszolút pártatlan, érdekek felett álló, mindenki által elismert felsőbb tekintély a meghatározó. Ez lehet egy mesterséges intelligencia, amely államok és kormányok felett áll. A kérdés az ebben az esetben, hogy ezt ki hozná létre, és ki milyen módon gyakorolna ellenőrzést fölötte.

Az oktatás terén szintén nagy várakozás előzi meg a személyi asszisztens megoldásokhoz hasonló tanító rendszerek megjelenését, amelyek a tanítás-tanulással kapcsolatos feladatokat látnak el. Biztosítják a személyre szabott tananyagokat, az automatikus értékelő funkciókat, ellátják a motivációs és adminisztratív feladatokat kiváltva ezzel a pedagógusokat. A rendszer mentorál, vizsgáztat és meg is dicsér, ha jól végeztük a feladatunkat. A nap 24 órájában azonosan rendelkezésre áll, nincs tanteremhez kötve. A virtuálisvalóság-alkalmazásokkal kombinálva még a gyakorlati feladatok ellátására is képes felkészíteni. Nincsenek előítéletei, teljes az esélyegyenlőség. Legalábbis első ránézésre. Az önálló tanuláshoz is kell egyfajta felkészültség, amit az Alpha Minihez[25] hasonló tanító robotok segítségével aligha lehet elsajátítani. Hasonlóan kihívást jelent a technológiai hozzáférés lehetősége is. Akinek a számára ez nem vagy csak korlátozottan biztosított, az aligha tud élni a technológia adta lehetőségekkel.

[24] Kakani et al. 2020.
[25] Dél-koreai óvodák neveléssegítő robotja, lásd Eduline 2021.

Az új aranykor eljövetelére tehát, még úgy tűnik, egy darabig várni kell, azt a mesterséges intelligencia nem fogja elhozni.

Szerencsére a túlzott szkepticizmus, a világvégevárás sem tűnik ma megalapozottnak. Bár vannak autonóm fegyverrendszerek, ezeknek korlátozottak a képességei. A Skynet[26] kora sem jött még el. Ha a fentiek szerint a „piros gomb" megnyomásának lehetőségét tételesen nem adjuk ki a humán ellenőrzés alól, akkor a kontroll lehetősége továbbra is adott.

A gépek hatalomátvételének másik lehetséges útja az MI fetisizálása.[27] Ez akkor következhet be, ha a felhasználók teljesen vak ráhagyatkozással, mintegy vallásos hittel vetik alá magukat annak, amit az MI javasol.[28] Ezt, mint a „nagy szent és érthetetlen" kinyilatkoztatását követve. Ez bizonyos kultúrákban könnyebben bekövetkezhet. Például az indiai sokistenség-tiszteletben akár több MI-alkalmazás is megjelenhet mint tiszteletreméltó, nagy tudású, az emberi lehetőségeket meghaladó képességű fétis. A szigorú egyistenhívő kultúrák esetében ennek a bekövetkezése valószínűleg lassabban, de ugyanúgy megtörténhet, azonban ha ezt a hatást kellő tudatosítással, már kisiskolás korban, illetve a különböző biztonságtudatot erősítő felkészítések során időben tompítjuk, akkor ez elkerülhető.

Ugyanez igaz a korábbi fejezetben megfogalmazott digitális demencia jelenségének elkerülésére. A tanulás-tanítás folyamatát kell újraértelmezzük.[29]

A fentiek alapján, ha azt még nem is tudjuk megmondani, hogy az MI hoz-e akkora változást az emberiség életében, mint a tűzhasználat, azt azonban kijelenthetjük, hogy legalább a puskapor elterjedésével egyenrangúnak tekinthető.

Úgy, ahogy a puskapor elterjedése az addigi lovagi életmódot folytató, egész életét a fegyverforgatásnak szentelő, a csatákban a döntő rohamokat vezető lovas páncélos végét jelentette, teljesen megváltoztatva nemcsak a csataterek képét, hanem például a várak szerkezetét is, így az építészetet, megváltoztatva ezzel a városok látképét és átalakítva az ipart.

Ma ugyanígy elmondhatjuk, hogy nincs az életnek olyan területe, ahol az MI alkalmazása ne hozott volna hasonló változást, előrelépést. Kezdve a tudományos alapkutatásokat segítő eljárásoktól a konkrét orvosi kezelésekig. Ugyanakkor ez nem csupán hozzáad az emberiség fejlődéséhez, hanem sok mindenben korlátoz, és el is vesz tőlünk bizonyos dolgokat.

A társadalmi egyenlőtlenség kérdésével kapcsolatban megállapítható, hogy a hatékonyság növelése gyakran együtt jár a hosszú távú társadalmi egyenlőtlenségek növekedésével. Ha a mesterséges intelligenciára mint eszközre tekintünk, akkor a gazdaság terén annak birtokosa lesz annak legnagyobb haszonélvezője. Jobb a helyzet az egészségügyben megjelenő új lehetőségekhez való hozzáférés terén, hiszen aki az egészségügyi ellátórendszerhez hozzáfér, az élvezheti az ebben rejlő lehetőségeket is.

Az egyéni biztonság és biztonságérzet vonatkozásában sajnos elmondható, hogy nem csupán az önálló gondolkodásról szoktat le, hanem a szabadságunkat is korlátozza,

[26] A *Terminátor* című film öntudatra ébredő stratégiai vezérlőrendszere, amely az emberiség elpusztítására tör.
[27] Természetfeletti erővel való felruházás.
[28] Efimov 2023.
[29] Seres 2019.

vagy legalábbis megadja a korlátozás lehetőségét azoknak, akik e technológiákat erre akarják használni.

Az oktatás az a terület, ahol mindenki számára lehetővé lehet tenni a hozzáférést, természetesen ennek az anyagi és személyi feltételeinek tanintézeti biztosítása mellett. Annak érdekében, hogy a negatív hatások minél kevésbé érvényesüljenek, az szükséges, hogy a népesség minél nagyobb hányada tisztában legyen a mesterséges intelligenciában rejlő reális lehetőségekkel. Ezért szükséges még az általános iskolai digitális kultúra tantárgy keretében megismerkedni vele. Nem tiltva a használatát például a házi feladat elkészítése során, hanem rávezetni a helyes használatra. Megtanulni ezt eszközként kezelni, és akkor a fetisizálás jelensége is elkerülhető. Mindennek megvalósulása érdekében javaslom további vizsgálat tárgyának a tanulás-tanítás folyamatának újraértelmezését.[30]

Felhasznált irodalom

Bárkai Levente András (2017): A növekedés kérdései. *Studia Ingatiana,* 9(1), 93–104.

Csatár János (2018): Elosztóhálózati okos eszközök közös rendszerbe integrálhatóságának alapjai. In *VIII. Mechwart András Ifjúsági Találkozó* (*MEE).* Budapest: Magyar Elektrotechnikai Egyesület, 1–6. Online: www.mee.hu/files/files/id23_csatarj_mait_cikk.pdf

Devosa Iván – Grósz Tamás – Kardos Péter (2020): A mesterséges intelligencia (AI) az egészségügy szolgálatában. *Gradus,* 7(3), 141–144. Online: https://doi.org/10.47833/2020.3.CSC.001

Eduline (2021): Robotok (is) foglalkoznak a gyerekekkel a dél-koreai óvodákban. *Eduline,* 2021. november 28. Online: https://eduline.hu/campus_life/20211126_szoul_ovoda_robotok

Efimov, Albert (2023): The Fetish of Artificial Intelligence. In Response to Iason Gabriel's "Towards a Theory of Justice for Artificial Intelligence". *Philpapers.* Online: https://philpapers.org/rec/EFITFO

Grad-Gyenge Anikó (2023): A mesterséges intelligencia által generált tartalmak értelmezésének lehetőségei a szerzői jog útján. *MTA Law Working Papers,* (2), 1–14. Online: https://real.mtak.hu/175842/1/5.Magyar_Jog_AI.pdf

Kakani, Vijay – Nguyen, Van H. – Kumar, Basivi P. – Kim, Hakil – Pasupuleti, Visweswara R. (2020): A Critical Review on Computer Vision and Artificial Intelligence in Food Industry. *Journal of Agriculture and Food Research,* 2. Online: https://doi.org/10.1016/j.jafr.2020.100033

Lányi Márton – Réger Béla (2022): Havária események hatása az ellátási láncokra, különös tekintettel a biztonsági készletek várható változásaira. *Logisztika,* 8(1), 43–49. Online: https://doi.org/10.21405/logtrend.2022.8.2.43

Lao, Baoqiang – An, Tao – Wang, Ailing – Xu, Zhijun – Guo, Shaoguang – Lv, Weijia – Wu, Xiacong – Zhang, Yingkang (2021): Artificial Intelligence for Celestial

[30] Seres 2019.

Object Census: The Latest Technology Meets the Oldest Science. *Science Bulletin,* 66(21), 2145–2147. Online: https://doi.org/10.1016/j.scib.2021.07.015

Nagy Milada (2021): A kínai „okosváros"-eszközök biztonsági kockázatai. *Nemzet és Biztonság,* 14(2), 27–35. Online: https://doi.org/10.32576/nb.2021.2.3

Négyesi Imre (2020): A mesterséges intelligencia és az etika. *Hadtudomány,* 30(1), 103–113. Online: https://doi.org/10.17047/HADTUD.2020.30.1.103

Négyesi Imre (2023): A mesterséges intelligencia katonai felhasználásának társadalmi kérdései. *Honvédségi Szemle,* 149(1), 133–144. Online: https://doi.org/10.17047/HADTUD.2022.32.2.74

Pause Giant AI Experiments: An Open Letter (2023). Online: https://futureoflife.org/open-letter/pause-giant-ai-experiments/

Seres György (2019): A Life-to-Life Teaching-Learning Process as a System. *Journal of Applied Multimedia,* 2(14), 21–25. Online: https://doi.org/10.26648/JAM.2019.2.002

Singh, Monica – Lehmann, Mariam – Aljuneidi, Saja – Hadidi, Ahmad (2019): *GATEBOX – An Analysis on Assistive Technology Companion.* Online: www.research-gate.net/publication/332081893_GATEBOX_-_An_analysis_on_assistive_technology_companion

Szűcs Attila (2023): A mesterséges intelligencia alkalmazása a katonai műveletek tervezése, szervezése és végrehajtása során. In Tóth András (szerk.): *Új típusú kihívások az infokommunikációban.* Budapest: Ludovika Egyetemi Kiadó, 137.

Szűts Zoltán (2024): A mesterséges intelligencia hatásai. *Educatio,* 33(1), 24–33. Online: https://doi.org/10.1556/2063.33.2024.1.3

Tisóczki József (2022): A mesterséges intelligencia alkalmazása az egészségügyi ellátásban. *Biztonságtudományi Szemle,* 4(2), 137–153. Online: https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/294/252

Turusov, Vladimir – Rakitsky, Valery – Tomatis, Lorenzo (2002): Dichlorodiphenyltrichloroethane (DDT): Ubiquity, Persistence, and Risks. *Environmental Health Perspectives,* 110(2), 125–128. Online: https://doi.org/10.1289/ehp.02110125

HADMÉRNÖK
VÉDELEMINFORMATIKA
19. évfolyam (2024) 4. szám 131–142.
DOI: 10.32567/hm.2024.4.9

Kreitz Zsuzsanna[1]

A chain of custody digitalizálásának lehetőségei

Opportunities for the Digitalisation of the Chain of Custody

Absztrakt

A chain of custody (CoC) – a bizonyítékok nyomonkövethetőségének láncolata – folyamata elengedhetetlen a kriminalisztikai tárgyi bizonyítékok kezelésében, biztosítva, hogy a bizonyítékok eredete, integritása és kezelése mindvégig nyomon követhető és hiteles maradjon. A digitalizáció gyors fejlődése új lehetőségeket kínál arra, hogy a hagyományosan papíralapú, manuálisan vezetett CoC-folyamatok hatékonyabbá és megbízhatóbbá váljanak. A digitális megoldások – mint például a blokklánc-technológia, rádiófrekvenciás azonosító (RFID) chipek és intelligens szerződések – jelentősen növelhetik a bizonyítékkezelési folyamatok átláthatóságát és megbízhatóságát, miközben csökkenthetik az emberi hibákból, csalásokból vagy mulasztásokból eredő kockázatokat. Jelen tanulmány célja a CoC digitalizálásának lehetőségeit feltárni, különös tekintettel a jogi, technológiai és adatbiztonsági szempontokra. A tanulmány kitér továbbá a digitális CoC megvalósításának kihívásaira is, úgymint a személyes adatok védelmére vonatkozó előírások (GDPR) betartása és a meglévő rendszerekkel való integráció problémái. Összességében a digitális CoC-megoldások jelentős előrelépést hozhatnak a bizonyítékkezelés pontosságában és gyorsaságában, de bevezetésük alapos jogi és technológiai elemzést, valamint előkészítést igényel.

Kulcsszavak: chain of custody, blokklánc, RFID, bizonyíték, digitális bizonyíték

Abstract

The chain of custody (CoC) process is essential in the management of forensic evidence, ensuring that the origin, integrity, and handling of evidence can be continuously traced and authenticated. Rapid advances in digitalisation offer opportunities to make traditionally

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Rendészeti Doktori Iskola, e-mail: kreitzzsu@gmail.com

paper-based and manually managed CoC processes more efficient and reliable. The use of digital solutions – such as blockchain technology, RFID chips, and smart contracts – can significantly increase the transparency and reliability of evidence handling, while reducing the risks arising from human error, fraud, or negligence. The aim of this paper is to explore the possibilities for CoC digitisation, with a focus on legal, technological, and data security aspects. The paper also addresses the challenges of implementing a digital CoC, such as compliance with personal data protection regulations and the integration of new systems with existing processes. Overall, digital chain-of-custody solutions can bring significant improvements in the accuracy and speed of evidence management, but their implementation requires thorough legal and technological analysis and preparation.

Keywords: chain of custody, blockchain, RFID, forensic evidence, digital evidence

Bevezetés

A bizonyítékok nyomonkövethetőségének folyamata – az úgynevezett *chain of custody,* azaz CoC – alapvető fontosságú a büntetőeljárásokban és kriminalisztikai nyomozásokban. A CoC biztosítja, hogy a bűnjelként szolgáló tárgyi vagy digitális bizonyítékok eredete, épsége és kezelése minden pillanatban ellenőrizhető legyen, így a bizonyíték hitelessége a bírósági eljárásban nem kérdőjelezhető meg. A hagyományos gyakorlatban a bizonyítékkezelés jellemzően papíralapú nyilvántartásokkal és manuális átadás-átvételi jegyzőkönyvekkel történik. Ez a megközelítés nemcsak idő- és munkaigényes, de növeli az emberi mulasztásból vagy adminisztrációs hibából fakadó láncszakadás kockázatát is.

Napjainkban a rendvédelmi szerveknek, ügyészségeknek és bíróságoknak még nem sikerült olyan egységes, minőségbiztosított és szabványosított CoC-rendszert kialakítaniuk, amely biztosítja a bizonyítékok sérthetetlenségét, ugyanakkor nem ró aránytalan adminisztratív terhet a szakemberekre. A klasszikus bűnjelkezelési eljárások során rendszerint csak utólagos ellenőrzésre van lehetőség, és gyakran nem látható át teljes egészében, hogy a bizonyíték a lefoglalástól a bírósági felhasználásig milyen utat járt be. A digitalizáció és a korszerű informatikai megoldások térnyerése azonban lehetőséget ad arra, hogy ezen a területen is paradigmaváltás következzen be. A blokklánc alapú elosztott főkönyvi rendszerek, az RFID-alapú azonosítás és nyomon követés, az okoseszközök hálózatba kapcsolása (Internet of Things, IoT), valamint az ezekhez társítható intelligens szerződések mind új utakat nyitnak a CoC folyamatainak megerősítésére. E technológiák alkalmazásával a bizonyítékok útja valós időben, manipulálhatatlan módon rögzíthető, és akár automatizált riasztások, értesítések is kiadhatók szabálytalanság esetén (például jogosulatlan hozzáférési kísérlet).

A CoC követelményei a különböző jogrendszerekben eltérő módon jelentek meg. Az angolszász *(common law)* jogrendszerekben a bizonyítékok elfogadhatóságának alapfeltétele a folytonos és dokumentált láncolat, ennek hiánya a bizonyíték kizárásához vezethet az ítélkezés során. Ezzel szemben a kontinentális *(civil law)* jogrendekben – így Magyarországon is – a bizonyítékok kezelését és nyilvántartását részben központi jogszabályok határozzák meg, és a bíróság, illetve hatóság maga is részt vesz a bizonyítékok beszerzésében. Magyarországon a *chain of custody* kifejezés nem

honosodott meg a jogi terminológiában, de a büntetőeljárási törvény és kapcsolódó rendeletek tartalmaznak a bizonyítékok kezelésére vonatkozó előírásokat. Ugyanakkor jelenleg hiányzik egy integrált, digitális eszközökre támaszkodó CoC-rendszer, amely a nemzetközi legjobb gyakorlatokat átültetné a hazai gyakorlatba. Ezek a különbségek történeti okokból is adódnak, és mélyen beágyazódtak a két jogrendszer bűnügyi eljárásaiba.[2]

Kutatási célkitűzések és hipotézisek

A tanulmány elsődleges célja, hogy elemezze, miként javíthatják a modern digitális technológiák (különösen a blokklánc, RFID és kapcsolódó eszközök) a bizonyítékok nyomon követésének folyamatát, és hogyan illeszthetők ezek a megoldások a magyar jogi keretrendszerbe a nemzetközi szabványokkal összhangban. E célt szem előtt tartva az alábbi hipotéziseket fogalmaztuk meg:

- **H1:** A digitális technológiák alkalmazása a chain of custody folyamatában jelentősen növeli a bizonyítékok kezelésének integritását és átláthatóságát a hagyományos módszerekhez képest.
- **H2:** Az RFID-alapú azonosítás és nyomon követés bevezetése csökkenti a bizonyítékkezelés során előforduló hibákat és késedelmeket, és javítja a folyamat hatékonyságát.
- **H3:** A magyar jogszabályi környezet megfelelően alakítható oly módon, hogy lehetővé tegye a CoC-folyamatok digitalizációját – beleértve a blokklánc és más új technológiák alkalmazását –, bár bizonyos területeken (például adatvédelem, eljárásjogi szabályok) szükség lehet a jogszabályok módosítására vagy kiegészítésére.

Az alábbiakban e hipotézisek vizsgálatára egy nemzetközi és hazai szabályozási összehasonlítást, valamint a technológiai lehetőségek értékelését mutatjuk be, majd javaslatot teszünk empirikus vizsgálati módszerekre a felvetett megoldások tesztelésére.

Módszertan

A kutatás elsősorban kvalitatív módszertanon alapul, irodalmi és jogszabályi elemzésre épít. Áttekintettük a vonatkozó nemzetközi szabványokat, ajánlásokat és szakirodalmi forrásokat a chain of custody témájában, valamint elemeztük a magyar jogi környezet idekapcsolódó elemeit. Ennek keretében összehasonlító elemzést végeztünk a hazai szabályozás és a nemzetközi standardok között, azonosítva az esetleges hiányosságokat és fejlesztési lehetőségeket. Ezenfelül áttekintettük a blokklánc, RFID, IoT és más releváns technológiák alkalmazásáról szóló nemzetközi kutatásokat (beleértve gyakorlati esettanulmányokat és prototípus-alkalmazásokat), hogy feltárjuk, milyen konkrét megoldásokkal és eredményekkel járhat a CoC-folyamat digitalizálása.

[2] Azarenok 2022.

Mivel empirikus adatgyűjtésre a kutatás keretében nem került sor, a tanulmány javaslatokat fogalmaz meg a jövőbeni gyakorlati tesztelésre. A *H1* és *H2* hipotézisek vizsgálatára például egy kísérleti pilotprojekt szolgálhatna: egy bűnjelraktárban vagy kriminalisztikai laborban prototípus jelleggel bevezethető egy blokklánc alapú, RFID-címkékkel támogatott bizonyítéknyilvántartó rendszer. Az új rendszer mellett párhuzamosan futtatott hagyományos eljárásokkal összehasonlítva mérhető lenne a feldolgozási idő (például a bizonyíték átvételének és kiadásának ideje), a dokumentáció teljessége és az esetleges hibák száma. Például elemezhető, hogy egy adott bizonyíték útját hány ponton és milyen részletességgel sikerül rögzíteni a digitális rendszerben, szemben a papíralapú nyilvántartással, valamint hogy egy illetéktelen beavatkozási kísérletet azonnal jelzett-e a rendszer. A kísérlet eredményeit statisztikai módszerekkel lehetne kiértékelni (például hibaarányok összehasonlítása, átlagos ügyintézési idők különbségeinek tesztelése).

A *H3* hipotézis (jogi keretek illeszthetősége) vizsgálatához jog-összehasonlító módszertant alkalmaztunk. Ennek során egyrészt megvizsgáltuk a hazai jogszabályokat [különösen a büntetőeljárásról szóló törvény és a 11/2003. (V. 8.) IM–BM–PM együttes rendelet előírásait], másrészt összevetettük azokat olyan nemzetközi ajánlásokkal, mint az ISO/IEC szabványok és a SWGDE, ASTM, ENFSI által közzétett iránymutatások. A jogi illeszkedés empirikus tesztelése a gyakorlatban történhet például szakértői interjúk vagy fókuszcsoportos megbeszélések formájában, amelyek során bírák, ügyészek, nyomozók és igazságügyi szakértők értékelik a javasolt digitális CoC-rendszer alkalmazhatóságát és elfogadhatóságát a jelenlegi jogi környezetben.

A vizsgálat során nyert eredményeket tematikusan rendeztük: először a nemzetközi és hazai szabályozási keretek elemzését mutatjuk be, majd ismertetjük a lehetséges digitális megoldásokat és azok előnyeit/kihívásait. Ezt követően a kapott eredményeket megvitatjuk, külön kitérve a hipotézisekre és a gyakorlati megvalósítás feltételeire.

Eredmények

Nemzetközi szabványok és legjobb gyakorlatok a CoC terén

A bizonyítékok kezelésére és a CoC fenntartására számos nemzetközi szabvány és iránymutatás létezik. A legjelentősebb szervezetek és dokumentumok az alábbiak:

- ISO/IEC-szabványok: Globális szabványok írják elő a kriminalisztikai laboratóriumok működésének és a bizonyítékkezelésnek a követelményeit. Idetartozik például az ISO/IEC 17025:2017, amely a vizsgáló laborok kompetenciájának általános követelményeit rögzíti, valamint az ISO/IEC 27037:2012 és 27042:2015 szabványok, amelyek a digitális bizonyítékok gyűjtésének, elemzésének és értelmezésének módszertanára adnak útmutatást. Ezek a szabványok globálisan elfogadott keretet biztosítanak a bizonyítékkezeléshez, elősegítve az eljárások egységességét és megbízhatóságát.
- SWGDE-irányelvek: A Scientific Working Group on Digital Evidence egy nemzetközi szakértői csoport, amely nem kötelező erejű, de széles körben hivatkozott ajánlásokat fogalmaz meg a digitális és multimédiás bizonyítékok

kezelésére. Irányelvei lefedik a bizonyítékgyűjtés, dokumentáció, tárolás, feldolgozás és szállítás legjobb gyakorlatait, kiemelve például a veszteségmentes adatformátumok (RAW, TIFF stb.) használatát és a részletes jegyzőkönyvezést. Bár ezek nem formális szabványok, globális referenciapontként szolgálnak a digitális bizonyítékok kezelése során, és hozzájárulnak a bevált gyakorlatok terjedéséhez.

- ASTM-szabványok: Az ASTM International az anyagvizsgálatok és egyes kriminalisztikai elemzések szabványosítására szakosodott szervezet. Szabványai részletes protokollokat nyújtanak a fizikai bizonyítékok (például eszköznyomok, fegyverek, dokumentumok, biometrikus minták) vizsgálatára és a laboratóriumi CoC fenntartására. Az ASTM hangsúlyozza a bizonyítékok gyűjtésének és kezelésének pontos dokumentálását és a laboratóriumi folyamatok validálását.
- ENFSI-ajánlások: A European Network of Forensic Science Institutes (ENFSI) európai kriminalisztikai intézetek hálózataként működik, és célja a szakértői módszerek harmonizációja. Best practice útmutatóik kiegészítik az ISO, SWGDE, ASTM által lefektetett kereteket, európai kontextusra szabva azokat. Az ENFSI például kiadta a *Digitális technológia igazságügyi vizsgálatának legjobb gyakorlata* kézikönyvet (2015), amely a digitális bizonyítékok vizsgálatának és láncolatának európai szemléletű standardjait foglalja össze.
- Interpol-kézikönyvek: Nemzetközi rendészeti szervezetek is készítettek útmutatókat a bizonyítékok kezeléséhez. Az Interpol 2014-ben kiadott egy környezeti bűncselekményekre fókuszáló igazságügyi nyomozati kézikönyvet, amely hangsúlyozza a helyszíni mintavétel és a bizonyíték-nyilvántartás szakszerű végrehajtását, biztosítva a bizonyítékok nyomonkövethetőségét és integritását a nemzetközi együttműködésekben is.

E nemzetközi standardok és ajánlások közös célja, hogy növeljék a bizonyítékkezelés megbízhatóságát és elősegítsék a különböző országok gyakorlatainak közelítését. Összességében az ISO, SWGDE, ASTM és ENFSI szervezetek eltérő fókuszuk ellenére egymást kiegészítve járulnak hozzá a CoC-folyamatok fejlesztéséhez. Míg az ISO globális érvényű keretet ad az interoperabilitás érdekében, addig a SWGDE specifikusan a digitális bizonyítékokra koncentrál, az ASTM a fizikai bizonyítékok laboratóriumi kezelésére kínál standardokat, az ENFSI pedig regionális (európai) szinten harmonizálja a gyakorlatot. A nemzetközi előírások mindegyike a bizonyítékok integritásának megőrzését, a folyamatok dokumentáltságát és szükség szerint a modern technológiák bevonását szorgalmazza.

Hazai jogszabályi keret

A magyar jogrendszer a chain of custody fogalmát külön nem nevesíti, de több előírás szolgálja a bizonyítékok hitelességének megőrzését. A büntetőeljárásról szóló 2017. évi XC. törvény (Be.) 204. §-a határozza meg a *tárgyi bizonyítási eszköz* (fizikai bizonyíték) fogalmát, míg a 205. § az *elektronikus adat* (digitális bizonyíték) definícióját. A lefoglalt tárgyak kezelésének részleteit a 11/2003. (V. 8.) IM–BM–PM együttes rendelet rögzíti,

amely szabályozza a lefoglalt dolgok nyilvántartását, őrzését, előzetes értékesítését, megsemmisítését, valamint az elkobzás végrehajtását. E rendelet alapján a hatóságoknak minden bizonyítékot egyedi azonosítóval kell ellátniuk és nyilvántartási rendszerben szerepeltetniük.

A gyakorlatban a bizonyítékok útját a különböző eljárási szakaszokban (lefoglalás, szállítás, szakértői vizsgálat, bíróság) papíralapú jegyzőkönyvek és átadás-átvételi dokumentumok kísérik. Egy központosított, elektronikus CoC-nyilvántartás azonban jelenleg nem létezik, így az információk széttagolódhatnak a rendőrség, ügyészség, bíróság és szakértői intézetek saját nyilvántartásai között. Ez a fragmentáltság azt eredményezheti, hogy a bizonyítékok teljes életciklusának nyomon követése nehézkes, és utólagos ellenőrzéskor hiányosságok merülhetnek fel (például nem dokumentált mozgatás vagy késedelem). Digitális bizonyítékok esetén a hatályos jog csak annyit mond ki, hogy azokat hasonló módon kell kezelni, mint a tárgyi bizonyítékokat; speciális technológiai megoldások (például hash-értékkel való lezárás vagy elektronikus naplózás) alkalmazását nem írja elő a jogszabály.

1. táblázat: A chain of custody folyamat néhány kulcselemének összehasonlítása a nemzetközi ajánlások és a magyar gyakorlat között

Szempont	Nemzetközi ajánlások / standardok	Magyar gyakorlat
Nyilvántartás módja	Részletes, folyamatos dokumentáció minden átadásról digitális naplóban (pl. blokklánc alapú vagy elektronikus rendszer).	Papíralapú jegyzőkönyvek, különálló (esetleg elektronikusan iktatott) dokumentumok szakaszonként; nincs egységes, központi elektronikus nyilvántartás.
Integritás ellenőrzése	Kriptográfiai módszerekkel (hash-algoritmusok) biztosított bizonyítékintegritás; minden módosítás kizárása vagy naplózása.	Fizikai plombák, pecsétek a csomagoláson; hash használata csak digitális adatoknál eseti jelleggel, nem egységes követelményként.
Technológia használata	RFID-címkék és szenzorok a valós idejű helymeghatározásra, környezeti adatok rögzítésére; automatizált riasztások eltérés esetén.	Hagyományos vonalkód vagy leltári szám; manuális ellenőrzés, fizikai tárolás felügyelete emberi erővel. Elektronikus érzékelők használata nem jellemző.
Szabványok és protokollok	Nemzetközi szabványok (ISO 17025, ISO 27037 stb.) és ajánlások (SWGDE, ASTM, ENFSI) által kidolgozott protokollok a teljes CoC-folyamatra.	A Be. és a 11/2003-as rendelet alapvető kereteket ad; részletes protokollok intézményenként eltérők, nem egységesek. Nemzetközi szabványok átvétele korlátozott.
Adatvédelem és hozzáférés	Szigorú hozzáférés-kezelés, naplózás és auditálás (pl. szerepkör alapú hozzáférés a digitális rendszerben).	Hozzáférés jogszabályban korlátozott (pl. csak az eljáró hatóságok férhetnek hozzá), de a nyilvántartások ellenőrzése jellemzően utólagos és manuális.

Forrás: a szerző szerkesztése

Fontos kiemelni, hogy az adatkezelésre vonatkozó általános előírások – különösen az Európai Unió általános adatvédelmi rendelete (GDPR) – a bizonyítékok digitalizált nyilvántartása esetén is érvényesek. Ez azt jelenti, hogy a személyes adatokat tartalmazó bűnügyi nyilvántartásoknak szigorú hozzáférés-kezeléssel és auditálhatósággal kell rendelkezniük, hogy megfeleljenek az adatvédelmi követelményeknek.

Emellett a hazai kriminalisztikai laboratóriumok esetenként alkalmazzák az ISO/IEC 17025:2017 szabvány előírásait a saját minőségirányításukban, amely magában foglalja a minták és bizonyítékok kezelésének nyomonkövethetőségét. Ez azonban szakintézményi gyakorlat, nem pedig minden hatóságra kiterjedő kötelező szabály. Összességében a jelenlegi hazai keretrendszer biztosít néhány alapvető garanciát (például nyilvántartási kötelezettség), de nem terjed ki a modern digitális eszközökkel támogatott, valós idejű és automatizált nyomon követésre.

Technológiai megoldások a CoC digitalizálására

Blokklánc és kriptográfia a bizonyítéklláncban

A blokklánc- *(blockchain)* technológia alapja egy decentralizált, elosztott főkönyvi rendszer, amelyben az egymást követő tranzakciók blokkok formájában, kriptográfiailag összefűzve tárolódnak. Ennek köszönhetően minden egyes művelet (például egy bizonyíték átadása a helyszínről a laborba, vagy a vizsgálati eredmény továbbítása a bírósághoz) egy új blokként rögzül, amely visszakereshető és utólag nem módosítható. A blokklánc rendkívül ellenálló a manipulációval szemben: egy blokk utólagos megváltoztatása csak úgy lehetséges, ha az utána következő összes blokkot is megváltoztatják, ami a konszenzusos hálózat miatt gyakorlatilag kivitelezhetetlen.

A kriptográfiai hash-algoritmusok kulcsszerepet játszanak a digitális bizonyítékok integritásának védelmében. Minden digitális fájlhoz, vagy akár egy elektronikus nyilvántartó bejegyzéshez generálható egy egyedi „lenyomat" (például SHA-256 hash), amely bizonyítja, hogy a tartalom nem változott. A korábban széles körben használt MD5 és SHA-1 algoritmusokról időközben kiderült, hogy bizonyos ütköztetési támadásokkal kijátszhatók, ezért ma már korszerűbb hash-eket alkalmaznak. A blokklánc-technológia ötvözése a hash-alapú integritásvédelemmel olyan többrétegű biztonsági megoldást eredményez, amely a szakirodalom szerint hatékonyan biztosítja a digitális bizonyítékkezelés sérthetetlenségét. Az intelligens szerződések *(smart contracts)* tovább növelhetik a hatékonyságot, mivel ezek olyan, blokkláncra telepített programok, amelyek automatikusan végrehajtják a meghatározott üzleti logikát.[3] Például beállítható, hogy egy bizonyíték átadására csak akkor kerüljön sor, ha a rendszerben az ahhoz szükséges összes jogosultságot és engedélyt rögzítették – enélkül a tranzakció nem teljesül. Így az okosszerződések biztosíthatják, hogy a CoC-protokollokat minden esetben betartsák, emberi beavatkozás nélkül is.

Számos nemzetközi kutatás foglalkozott már a blokklánc alapú CoC-rendszerek fejlesztésével. Ahmad és társai (2020) egy privát Ethereum-hálózaton megvalósított bizonyítéklánc-modellt javasoltak, amely valós idejű, hamisításbiztos naplózást tett lehetővé.[4] Santamaría és kollégái (2023) egy működő prototípust építettek, amelyben okosszerződésekkel kezelték a digitális bizonyítékok láncolatát, és sikeresen demonstrálták a rendszer gyakorlati alkalmazhatóságát. Hasonlóképpen Miller

[3] Santamaría et al. 2023.
[4] Ahmad et al. 2020.

és Singh (2024) kutatása egy innovatív modellt mutatott be a digitális bizonyítékok integritásának ellenőrzésére és megőrzésére, amely tovább erősíti a CoC-folyamat megbízhatóságát a kibervédelmi vizsgálatokban.[5] Ezek az eredmények azt sugallják, hogy a blokklánc-technológia megfelelő alkalmazása esetén jelentős mértékben fokozható a bizonyítékkezelés átláthatósága és biztonsága. Ugyanakkor érdemes megjegyezni, hogy a blokkláncrendszerek bevezetése alapos tervezést igényel, különös tekintettel az interoperabilitásra és a skálázhatóságra, amire a tanulmány későbbi részében még visszatérünk.

RFID- és IoT-alapú nyomon követés

A rádiófrekvenciás azonosítás (RFID) olyan technológia, amely lehetővé teszi tárgyak érintés nélküli azonosítását és nyomon követését rádióhullámok segítségével. Egy teljes RFID-rendszer tipikusan három fő elemből áll: RFID-címkékből (mikrochippel ellátott azonosítók, aktív vagy passzív kivitelben), olvasóberendezésekből és a háttérben működő adatkezelő szoftverből. A bizonyítékokra erősített RFID-címkék egyedi azonosítót és szükség esetén további adatokat (például ügyszám, gyűjtés helye/ideje) hordoznak. Az olvasók a bűnjelraktárakban, laborokban vagy akár szállító járművekben folyamatosan figyelhetik a bizonyítékok jelenlétét, helyét, és a rendszer automatikusan rögzíti, amikor egy bizonyíték elhagy egy adott zónát vagy belép annak területére.

Az IoT- (dolgok internete) eszközök integrálása tovább bővíti a lehetőségeket. Például a bizonyítékokat tároló helyiségekben vagy konténerekben elhelyezett szenzorok valós időben mérhetik a környezeti paramétereket, mint a hőmérséklet és a páratartalom, hogy biztosítsák az optimális tárolási feltételeket. Smith és munkatársai (2019) rámutattak, hogy egyes érzékeny nyomok (például lábnyomok gipszöntései) esetében az RFID-címkékkel ellátott minták folyamatos felügyelete – beleértve a környezeti feltételek monitorozását is – nagyban hozzájárul a bizonyítékok épségének megőrzéséhez. Az RFID-alapú rendszerek képesek valós idejű riasztások kiadására is: például ha egy bizonyíték engedély nélküli mozgatása történik, vagy a tárolási körülmények kritikus szintre romlanak, a rendszer azonnal jelez (akár automatikus értesítést küld a felelős személyeknek).

Az RFID- és IoT-technológiák alkalmazásával a fizikai bizonyítékok kezelése lényegesen hatékonyabbá válhat. A leltározás és keresés ideje lerövidül, mivel nem kell manuálisan azonosítani minden egyes tárgyat, hanem az olvasók automatikusan beolvassák a jelenlétüket. A rendszer naplózza a pontos időpontokat, amikor egy bizonyíték megérkezik vagy távozik egy adott helyről, ezáltal precíz, percre kész láncolati naplót hozva létre.

Természetesen e technológiák bevezetése nem mentes a kihívásoktól. Az RFID-rendszer kezdeti kiépítése költséges lehet, különösen nagy mennyiségű bizonyíték és több telephely esetén. A rádiójelek zavara vagy árnyékolása okozhat adatkihagyást (például fémtárolók vagy vastag falak gyengíthetik a jelet). Továbbá biztosítani kell hogy az RFID-/IoT-rendszer összekapcsolódjon a meglévő rendőrségi és bírósági informatikai

[5] Miller–Singh 2024.

rendszerekkel, hogy az adatok áramlása zökkenőmentes legyen. E nehézségek ellenére számos példa igazolja az RFID sikeres alkalmazását a bűnjelkezelésben: több ország igazságügyi laboratóriumaiban már kísérleti jelleggel vezettek be RFID-alapú nyomkövetést, és arról számoltak be, hogy a nyilvántartások pontossága és az ellenőrzések gyorsasága javult.[6]

Mindezek alapján kijelenthető, hogy az RFID- és az IoT-technológiák a fizikai és digitális bizonyítékok kezelésének modernizálásában kulcsszerepet játszhatnak, kiegészítve a blokklánc által kínált adatintegritási garanciákat.

Konklúzió

A fenti eredmények fényében megállapítható, hogy a kitűzött hipotézisek helytállók. A H1 (a digitális technológiák növelik a CoC integritását és átláthatóságát) hipotézisünket alátámasztják mind a szakirodalmi források, mind a nemzetközi kísérletek tapasztalatai. A blokklánc alapú nyilvántartások és a hash-algoritmusok kombinációja ténylegesen képes szavatolni, hogy a bizonyítékokkal kapcsolatos adatokat ne lehessen észrevétlenül megváltoztatni vagy eltüntetni. Az RFID bevezetése pedig demonstrálható módon csökkenti az adminisztratív hiányosságokat: a rendszer automatikus jelzései révén időben kiderül, ha egy láncszem kimaradna vagy szabálytalanság történne. Mindez azt eredményezi, hogy a bizonyítékok útja sokkal átláthatóbbá válik, ezáltal nő a bűnüldözési folyamatokba vetett bizalom is. H2 (az RFID csökkenti a hibákat és gyorsítja a folyamatot) szintén igazolást nyer, hiszen a vizsgálatok rámutattak, hogy a fizikai azonosítás és leltározás digitalizálása nemcsak tehermentesíti a humán erőforrásokat, de pontosabb nyilvántartást is eredményez. Rövidebbé válik a bizonyítékok keresésének ideje, és kevesebb esély van arra, hogy egy tételeltévesztés miatt egy bizonyíték „elvész" a rendszerben.

A H3 (a jogi keret igazítható a digitális CoC igényeihez) hipotézis kapcsán a nemzetközi és hazai szabályozás összehasonlítása alapján megállapítható, hogy bár a magyar joganyagban jelenleg nincsenek expliciten rögzítve a digitális CoC eszközei, a meglévő keret nem zárja ki azok alkalmazását sem. Sőt, bizonyos területeken már most is megfigyelhető a közelítés a nemzetközi standardokhoz – például a szakértői intézetek ISO 17025 szerinti akkreditációja vagy az elektronikus ügykezelési rendszerek terjedése. Mindazonáltal a sikeres implementációhoz szükség lesz a jogi környezet finomhangolására. Célszerű lehet külön szabályozni a digitális CoC-nyilvántartások hitelességét (például minősített elektronikus aláírás vagy pecsét használata a digitális naplók lezárásához), továbbá egyértelműsíteni kell hogy a blokklánc alapú naplózás során keletkező adatok a bíróság előtt bizonyító erővel rendelkeznek. Emellett az adatvédelmi megfelelésnek is eleget kell tenni: biztosítani kell hogy a rendszerben tárolt személyes adatokat csak a szükséges mértékben és ideig kezeljék, és azokhoz csak az arra jogosultak férjenek hozzá auditálható módon. Ezek a jogi-szabályozási finomítások hozzájárulnak ahhoz, hogy a digitális CoC-megoldások bevezetése zökkenőmentes és sikeres legyen.

[6] Kumar–Singh 2021.

A technológiai újítások bevezetése kapcsán további fontos szempont a szervezeti és kulturális tényezők szerepe. Egy ilyen átfogó változás – a papíralapú adminisztrációról a digitális rendszerre való áttérés – nem pusztán technológiai upgrade, hanem szemléletváltás is egyben. Elengedhetetlen, hogy a rendszer végfelhasználói (nyomozók, raktárosok, szakértők, ügyészek stb.) megfelelő képzésben részesüljenek az új eszközök használatát illetően, és megértsék azok előnyeit. A folyamatos oktatás és a változáskezelés kulcsfontosságú a bizalom kiépítéséhez az új rendszer iránt. Ha a személyzet látja, hogy a digitális CoC nem többletterhet jelent, hanem éppen ellenkezőleg, megkönnyíti a munkáját (kevesebb papírmunka, gyorsabb visszakeresés, egyértelmű felelősségi lánc), akkor a kezdeti ellenállás leküzdhető.

További gyakorlati kihívások is megfontolandók. A rendszer kiépítésének költségei jelentősek lehetnek – ideértve a technikai infrastruktúra (szerverek, hálózat, RFID-olvasók stb.) telepítését, valamint a szoftverfejlesztést és -integrációt. Ugyanakkor hosszú távon ezek a beruházások megtérülhetnek a hatékonyságnövekedés és a hibák miatti pótlólagos eljárások elkerülése révén. A blokkláncrendszerek skálázhatósága és energiaköltsége szintén szempont; valószínűleg egy privát vagy konzorciumi blokklánchálózat alkalmazása célszerű a bűnüldözési szervek között, hogy kontrollált környezetben működjön a megoldás. Az interoperabilitás biztosítása érdekében nyílt szabványokat kell követni, hogy a későbbiekben más rendszerek (például európai szintű bűnügyi nyilvántartások) is tudjanak csatlakozni vagy adatot cserélni a CoC-rendszerrel.

Összességében elmondható, hogy a digitalizált chain of custody bevezetése reális és szakmailag megalapozott törekvés. A nemzetközi trendek egyértelműek. Számos ország és szervezet kísérletezik ilyen rendszerekkel, és a globális szabványok adaptálása elengedhetetlen ahhoz, hogy a magyar igazságszolgáltatás lépést tartson a nemzetközi elvárásokkal. A tanulmány eredményei rámutatnak, hogy a technológiai feltételek adottak, a jogi feltételek megteremthetők, és a gyakorlati tapasztalatok alapján megfelelő tervezéssel és képzéssel a kihívások leküzdhetők. A CoC digitalizációja nem csupán technológiai innováció, hanem az igazságszolgáltatás hatékonyságának, átláthatóságának és hitelességének növelését szolgáló átfogó fejlesztés, amely hosszú távon hozzájárulhat a kriminalisztikai bizonyítékkezelés és ezáltal a bűnüldözés és a bírósági munka magasabb színvonalához.

Következtetések

A vizsgálat rávilágított, hogy a chain of custody folyamat digitalizálása időszerű és indokolt lépés a bizonyítékkezelés terén. A tanulmány keretében áttekintettük a CoC jelentőségét és hagyományos gyakorlatát, összehasonlítottuk a magyar szabályozást a nemzetközi standardokkal, valamint felmértük a legmodernebb technológiai eszközök – így különösen a blokklánc, az RFID és az IoT – alkalmazásának lehetőségeit. Megállapítottuk, hogy a digitális megoldások integrálása jelentős előnyökkel jár: növelhető a bizonyítékok nyomon követésének pontossága, csökkenthetők az emberi mulasztásokból fakadó kockázatok, és gyorsíthatók az eljárások. Ugyanakkor hangsúlyoztuk, hogy a sikeres bevezetés feltétele a megfelelő jogi és szervezeti keretek kialakítása – ideértve az adatvédelmi szempontok figyelembevételét és a felhasználók képzését is.

Összefoglalva, a CoC digitalizációja olyan innováció, amely egyszerre javítja a bűnüldözés hatékonyságát és erősíti a büntetőeljárások tisztességét. A nemzetközi példák és a jelenlegi technológiai trendek azt mutatják, hogy Magyarország is képes lehet a digitális bizonyítéklánc alkalmazására, bevezetésére, amennyiben az ehhez szükséges jogszabályi módosításokat és infrastrukturális fejlesztéseket végrehajtja. A változás eredményeként a bizonyítékok kezelése a 21. századi elvárásoknak megfelelően válhat átláthatóvá és hitelessé, ami végső soron hozzájárul az igazságszolgáltatásba vetett közbizalom erősítéséhez. Jövőbeli kutatások és pilotprojektek segíthetnek azonosítani a gyakorlati megvalósítás további részleteit, azonban az eddigi eredmények alapján egyértelmű, hogy a digitális CoC-rendszerek bevezetése a büntető igazságszolgáltatás terén komoly hozzáadott értéket képvisel.

A cikk a 2024. október 15-i II. Alverad-Bánki Nemzetközi Kiberbiztonsági Konferencián elhangzott előadás kivonata.

Felhasznált irodalom

Ahmad, Liza – Khanji, Salam – Iqbal, Farkhund – Kamoun, Faouzi (2020): *Blockchain-Based Chain of Custody: Towards Real-Time Tamper-Proof Evidence Management.* Proceedings of the 15th International Conference on Availability, Reliability and Security (ARES 2020), 1–8. Online: https://doi.org/10.1145/3407023.3409199

Alruwaili, Fahad F. (2021): CustodyBlock: A Distributed CoC Evidence Framework. *Information,* 12(2). Online: https://doi.org/10.3390/info12020088

Azarenok, N. (2022): Conditionality of Anglo-Saxon and Romance-Germanic Types of Criminal Procedure. *Vestnik Tomskogo Gosudarstvennogo Universiteta – Pravo,* 478, 219–228. Online: https://doi.org/10.17223/15617793/478/25

ENFSI (2015): *Best Practice Manual for the Forensic Examination of Digital Technology.* European Network of Forensic Science Institutes.

Garcia, L. – Taylor, R. (2020): Advanced Storage Solutions for Evidence Management. *International Journal of Criminal Justice,* 29(3), 150–165.

Interpol (2014): *Pollution Crime Forensic Investigation Manual.* Interpol Environmental Crime Programme.

Interpol (2014): *Pollution Crime Forensic Investigation Manual.* Interpol Environmental Crime Programme.

ISO/IEC 17025:2017. General requirements for the competence of testing and calibration laboratories.

ISO/IEC 27037:2012. Guidelines for identification, collection, acquisition and preservation of digital evidence.

Kumar, S. – Singh, P. (2021): RFID in Forensic Science: Applications and Challenges. *Indian Journal of Forensic Sciences,* 12(2), 55–70.

Miller, Adir – Singh, Avinash (2024): *CoC and Evidence Integrity Verification Using Blockchain Technology.* Proceedings of the 19th International Conference on Cyber Warfare and Security (ICCWS 2024), Johannesburg, South Africa, 2024. Online: https://doi.org/10.34190/iccws.19.1.2025

Santamaría, Pablo – Tobarra, Llanos – Pastor-Vargas, Rafael – Robles-Gómez, Antonio (2023): Smart Contracts for Managing the Chain-of-Custody of Digital Evidence: A Practical Case Study. *Smart Cities,* 6(2), 709–727. Online: https://doi.org/10.3390/smartcities6020034

Smith, J. et al. (2019): RFID and Digital Evidence Management: A Modern Approach. *Forensic Science Today,* 10(4), 200–220.

SWGDE (2017a): *SWGDE Best Practices for Digital & Multimedia Evidence Video Acquisition from Cloud Storage.* Scientific Working Group on Digital Evidence.

SWGDE (2017b): *SWGDE Best Practices for Data Acquisition from Digital Video Recorders.* Scientific Working Group on Digital Evidence.

SWGDE (2021): *SWGDE Best Practices for Computer Forensic Acquisitions.* Scientific Working Group on Digital Evidence.

Schmitt, Veronica – Jordaan, Jason (2013): Establishing the Validity of MD5 and SHA-1 Hashing in Digital Forensic Practice in Light of Recent Research Demonstrating Cryptographic Weaknesses in These Algorithms. *International Journal of Computer Applications,* 68(23), 38–46. Online: https://doi.org/10.5120/11723-7433

Jogi források

2017. évi XC. törvény a büntetőeljárásról

11/2003. (V. 8.) IM–BM–PM együttes rendelet a lefoglalás és a büntetőeljárás során lefoglalt dolgok kezelésének, nyilvántartásának, előzetes értékesítésének és megsemmisítésének szabályairól, valamint az elkobzás végrehajtásáról

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 (GDPR)

HADMÉRNÖK
VÉDELEMINFORMATIKA

19. évfolyam (2024) 4. szám 143–152.
DOI: 10.32567/hm.2024.4.10

Mandić Dorottya,[1] Kiss Gábor[2]

Informatikai oktatási tananyag Magyarországon és Szerbiában

IT Education Curriculum in Hungary and Serbia

Absztrakt

Az informatikának fontos szerepe van az oktatásban, hiszen a felhasználói szintű informatikai ismeretek megszerzése egyre fontosabbá válik napjainkban. Több tanulmány is foglalkozik Magyarország és Szerbia informatikai oktatási tananyagával. Mivel napjainkban egyre több felhasználó használ különféle okoseszközöket, ezért egyre fontosabbá válik, hogy a felhasználók megfelelő ismeretekkel rendelkezzenek ezen a téren is, illetve megfelelő körültekintéssel használhassák ezeket a személyes adataik védelmében. Várhatóan a jövőben még több okoseszköz lesz jelen, és a felhasználók közül sokan nem tudják, hogyan kell biztonságosan használni az okoseszközeiket, sokan még csak alapvető ismeretekkel sem rendelkeznek. Ezért fontos, hogy a felhasználók tudatában legyenek annak, hogy ezek használata milyen veszélyeket rejthet. Jelen tanulmány azt vizsgálja, hogy Magyarország és Szerbia informatikai oktatási tananyagában megtalálható-e az információbiztonsági tudatosság fejlesztése, és hogy a két ország informatikai tananyaga, valamint jelszóhasználati szokásai között van-e különbség.

Kulcsszavak: informatika, oktatás, információbiztonság, tudatosság, jelszóhasználat

Abstract

IT has an important role in education, as acquiring user-level IT knowledge is becoming more important nowadays. Several studies deal with the IT education curriculum of Hungary and Serbia. As more and more users are using various smart devices these days, it is becoming more important that they have the right knowledge in this area and that

[1] Óbudai Egyetem Biztonságtudományi Doktori Iskola, e-mail: mandic.dorottya@uni-obuda.hu
[2] Óbudai Egyetem Biztonságtudományi és Kibervédelmi Intézet, e-mail: kiss.gabor@bgk.uni-obuda.hu

they can use it with the right amount of care to protect their personal data. It is expected that more smart devices will be present in the future and smart device users generally do not know how to use their smart devices safely, many users do not even have basic knowledge. Therefore, it is important for users to be aware of the dangers of using smart devices. This study examines whether information security awareness can be found in the IT education curriculum of Hungary and Serbia, and whether there is a difference between the IT curriculum and password usage habits in the two countries.

Keywords: IT, education, information security, awareness, password usage

Bevezetés

Napjainkban egyre nagyobb az igény a különféle okoseszközök iránt. A felhasználók sokszor úgy vásárolják meg ezeket az eszközöket, hogy nem rendelkeznek megfelelő ismeretekkel.[3] A felhasználói szintű informatikai ismeretek megszerzése napjainkban kiemelten fontossá vált.[4] Az információbiztonság manapság komoly problémát okoz, hiszen „az egyén a leggyengébb láncszem az információbiztonsági láncban".[5] Ezért fontos növelni az egyének biztonságtudatosságát. Számtalan tanulmány készült már arról, hogy mivel lehetne növelni az egyének információbiztonság-tudatosságát.[6]

Az okoseszközök elterjedésével a felhasználók olyan veszélyeknek vannak kitéve, amelyeknek sokszor nincsenek a tudatában. A támadók olyan információkhoz juthatnak, mint például a felhasználók mindennapi szokásai, az adott személy tartózkodási helye vagy akár a fogyasztási szokásai.[7] Az IoT-eszközök biztonsága nagyon fontos napjainkban, hiszen az IoT ellen irányuló támadások veszélyeztethetik a felhasználók biztonságát, mivel személyes adatokat gyűjtenek, elemeznek, használnak, ami által adatvédelmi aggodalmak merülhetnek fel.[8] A tanulmány első részében szakirodalmi áttekintést végeztünk a két ország informatikai oktatási tananyaga között, majd felmérést hajtottunk végre Magyarországon és Szerbiában az okoseszköz-használók körében, hogy hányan használnak okoseszközöket, illetve jelszóhasználati szokásaikról kérdeztük a felmérésben részt vevőket.

Magyarország informatikai oktatási tananyaga

Az informatikai tanterv követelményei 1988-ban a Művelődési Minisztérium tantervében jelentek meg minden diák számára. A követelmény az általános iskolások számára a 4. és a 8. osztály technikai tantárgyában jelent meg, majd a gimnáziumok számára az első, valamint a második évfolyamban. A külön tantárgyra való igény a '80-as

[3] Mandić 2023.
[4] Mandić–Kiss 2023.
[5] Bak–Kelemen-Erdős 2022.
[6] Busa 2023.
[7] Kerti–Koller 2021.
[8] Horváth 2019.

évek vége felé egyre fontosabbá vált. A Nemzeti alaptantervet 1995-ben fogadták el, majd ezt követően 1998-ban az informatika önálló műveltségterületként jelent meg.[9]

Magyarországon a kormány az „internetről és a digitális fejlesztésekről szóló 2015. évi nemzeti konzultáció eredményei alapján fogadta el a magyar társadalom és a magyar nemzetgazdaság digitális fejlesztését célzó Digitális Jólét Programot, melynek egyik legfontosabb stratégiai eleme Magyarország Digitális Oktatási Stratégiája (DOS)".[10] Hazánkban 2020 szeptemberében az informatika tantárgyat felváltotta a digitális kultúra tantárgy.[11] Míg a „digitális kultúra fejlesztése 3–4. évfolyamon gyakran digitális eszközök közvetlen használata nélkül történik, addig az 5–6. évfolyamon a tanulók már rendszeresen használják a számítógéptermet és az iskola számítógépes hálózatát".[12]

A digitális kultúra tantárgy a Nemzeti alaptantervben rögzített olyan kulcskompetenciákat fejleszti, mint például a tanulás, kommunikáció, személyes és társas kapcsolatok, kreativitás és digitális kompetenciák. Az 5–6. évfolyamon a digitális kultúra tantárgy alapóraszáma 68 óra, ahol a diákok olyan témakörökről tanulhatnak, mint például az online kommunikáció, az információs társadalom, e-Világ vagy a digitális eszközök használata. Az online kommunikációs témakörnél a diákok már arról tanulnak, hogy tisztában legyenek a hálózatokat és a személyes információkat érintő fenyegetésekkel, valamint hogy tudják alkalmazni az adatok védelmét biztosító lehetőségeket önállóan, és hogy kezelni tudják az operációs rendszer mappáit, fájljait és a felhőszolgáltatásokat.[13]

Az 1. táblázatban láthatjuk a 2020-ban kiadott Nemzeti alaptantervet és kerettantervet a digitális kultúra tantárgyra.

1. táblázat: A digitális kultúra tantárgy óraszámai évfolyamok szerint a 2020-ban kiadott Nemzeti alaptanterv és kerettantervek alapján

Évfolyam	Heti óraszám	Összesen
1–2.	Nem jelenik meg önálló tantárgyként.	
3–4.	1+1	68
5–6.	1+1	68
7–8.	1+1	68
9–10.	2+1	102
11.	2	68

Forrás: Farkas–Lénárd–Siegler 2020

Az információs társadalom és e-Világ megnevezésű témakör az 5–6. évfolyamnak 6 órából áll, amelynek célja, hogy például tudjanak információt keresni és találatokat tudjanak szűrni. Ezenkívül „ismerjék az információs társadalom múltját, jelenét, valamint a várható jövőjét".[14] A digitális eszközök használata témakör 4 órából áll,

[9] Kőrösné Mikis 2009.
[10] 2012/2015. (XII. 29.) Korm. határozat.
[11] Eduline 2020.
[12] Farkas–Lénárd–Siegler 2020.
[13] Farkas–Lénárd–Siegler 2020.
[14] Lásd *Kerettanterv az általános iskola 5–8. évfolyama számára.*

amelyben a diákok elsajátítják az informatikai eszközök használatát, illetve azt, hogy miképpen tudják elkerülni a tipikus felhasználói hibákat.[15]

A 7–8. évfolyamon a digitális kultúra tantárgy alapóraszáma szintén 68 óra. Ennél az évfolyamnál a tananyag kapcsolódik az 5–6. évfolyam tananyagához. „A 8. évfolyam végére a tanulók a digitális írástudás alapjainak elsajátítását lezárják."[16]

A 9–10. évfolyam feladata a tanulók „tudásának egy szintre hozása, hogy felkészítse őket a középiskolában elvárt, a korábbinál bonyolultabb feladatok megoldására".[17] A 9–10. évfolyamban az információs társadalom és e-Világ témakör 3 órából áll, amelynek keretében a tanulók megtanulják például „az adatok védelmét biztosító lehetőségeket a gyakorlatban".[18]

Az online kommunikáció témakör 4 órából áll, amely során cél, hogy a tanulók elsajátítsák például a viselkedési kultúrát és szokásokat. „Önállóan tudja használni az informatikai eszközöket, és el tudja kerülni a tipikus felhasználói hibákat, és hogy el tudja hárítani az egyszerűbb felhasználói hibákat."[19]

Magyarországon a középiskolás tananyag a diákokat felkészíti például „az okoseszközök, okos használatára, a tudatos felhasználói és vásárlói magatartás alakítására, a biztonsági okokból bevezetett korlátozások megismerésére és elfogadására".[20]

A középiskolában a 9–10. évfolyamon a digitális kultúra tantárgy 102 órából áll. A 11. évfolyamon az óraszám 68 órából áll, „ahol fontos szerepet kap az olyan összetett problémák digitális eszközökkel történő megoldása, melyek akár egy munkahelyen vagy egy felsőoktatási intézményben végzett kutatómunka során is előfordulhatnak".[21]

Szerbia informatikai oktatási tananyaga

Szerbiában 1985–1986-ban vezették be a 8. évfolyam számára a műszaki oktatásban első alkalommal az elektronika és informatika tantárgyat. Majd 2004/2005-ben bevezették az általános iskolások számára első osztálytól az ötödik osztályig választható tantárgyként az informatikát.

A Szerb Köztársaság Oktatásfejlesztési Stratégiája felismerte a fontosságát annak, hogy új technológiákat vezessen be az oktatási rendszer javítása érdekében, ezért az általános iskolák a 2017/2018-as tanévben már új, innovatív tanterv alkalmazását kezdték meg, amikor bevezették az informatika és számítástechnika tantárgyat, majd a technika és technológia alapfokú oktatását.[22]

A Tanjug hírügynökség 2016-os jelentése szerint az Országos Oktatási Tanács úgy döntött, hogy az informatika és számítástechnika az általános iskolások számára választható tantárgy fog maradni, és nem fogják kötelező tantárggyá tenni. Ezenkívül

[15] Lásd *Kerettanterv a gimnáziumok 9–12. évfolyama számára.*
[16] Lásd *Kerettanterv az általános iskola 5–8. évfolyama számára.*
[17] Lásd *Kerettanterv a gimnáziumok 9–12. évfolyama számára.*
[18] Lásd *Kerettanterv a gimnáziumok 9–12. évfolyama számára.*
[19] Lásd *Kerettanterv a gimnáziumok 9–12. évfolyama számára.*
[20] Lásd *Kerettanterv a gimnáziumok 9–12. évfolyama számára.*
[21] Lásd *Kerettanterv a gimnáziumok 9–12. évfolyama számára.*
[22] Ilić 2020.

2016-ban az informatika és számítástechnika tantárgy a középiskolákban kötelező tantárggyá vált.[23]

A 2020/2021-es tanévtől az informatikai tantárgy kötelezővé vált az általános iskolások számára, és alapfokú informatikai oktatást kapnak az 1. évfolyamtól a 4. évfolyamig a digitális világ tantárgy keretében.[24] Az 5. évfolyam számára szintén kötelező tantárgy lett az informatika, ami 36 órából áll.[25]

Az informatika és számítástechnika tantárgyból a következő témákat tanulják, mint például az információ- és kommunikációtechnológia, digitális írástudás, számítástechnika és projektoktatás. A digitális írástudásnál tanulnak például az IKT-eszközök felelősségteljes és biztonságos használatáról, előírásokról a biztonságos internet használatára, valamint a személyes adatok védelméről.[26]

A 6. évfolyamban a tanulók az internet témaköréről 4 órában olyan témákról tanulnak, mint például keresés az interneten, biztonsági kód a számítógépen és vírusok.[27] A 7. évfolyamban a tanulók az internet témakörénél összesen 6 órában tanulnak olyan témakörökről, mint például az elektronikus kommunikáció biztonsága az interneten, valamint a blog, fórum, vita és megjegyzések megfogalmazása.[28] A 8. évfolyamon az Informatika és Számítástudomány tantárgyból tanulják például a táblázatkezelést vagy projektkészítést.[29]

A 2. táblázatban láthatjuk az informatika megjelenését az évek során a szerbiai tantervben.

2. táblázat: Az informatika megjelenése az általános és középiskolák tantervében Szerbiában

Év	Évfolyam
1985/1986	A 8. évfolyam számára első alkalommal jelenik meg az elektronika és informatika tantárgy.
2004/2005	Az általános iskolások számára első osztálytól az ötödik osztályig választható tantárgy az informatika.
2016	Az informatika és számítástechnika az általános iskolások számára választható tantárgy, viszont az 5. évfolyamtól a 8. évfolyamig továbbra is kötelező a heti két óra Műszaki és Informatika tantárgy, valamint a heti egy óra informatika és számítástechnika tantárgy.
2016	2016-tól az informatika és számítástechnika tantárgy kötelező a középiskolákban.
2017/2018	Az innovatív tanterv alkalmazása az általános iskolákban az informatika és számítástechnika tantárgy bevezetése.
2020/2021	Az általános iskolások számára az informatikai tantárgy kötelező az 1. évfolyamtól az 5. évfolyamig.

Forrás: a szerzők szerkesztése

[23] Zakon o osnovama sistema obrazovanja i vaspitanja.
[24] Informatika postaje obavezan predmet od prvog razreda osnovnih škola u Srbiji.
[25] Информатика и рачунарство обавезан предмет за ученике петог разреда.
[26] Годишњи програм информатика и рачунарство – 5. разред.
[27] Годишњи програм информатика и рачунарство – 6. разред.
[28] Информатика и Рачунарство – 7. разред.
[29] Годишњи програм информатика и рачунарство – 8. разред.

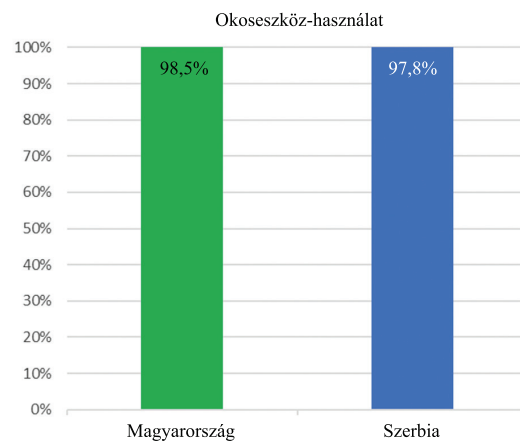
Szerbiában azokban az állami középiskolákban, amelyek nem az IT és a digitális ágazatokhoz tartoznak, csak az első évben kötelező a számítástechnika és informatika tantárgy. A lakosságnak szóló tanfolyamok, valamint képzések esetében a pénzügyi szempont nagyon fontos szerepet kap, hiszen aki szeretné fejleszteni digitális kompetenciáit, annak szüksége van például külön tanfolyamok elvégzésére, amit legtöbbször saját maga kell hogy kifizessen. Ezenkívül nagyon kevés tanfolyam és képzés foglalkozik a lakosság digitális kompetenciáival, mint például az eszközök és az adatok védelmével.[30]

Felmérés Magyarországon és Szerbiában az okoseszközt használók körében

Magyarországon és Szerbiában felmérést végeztünk az okoseszköz-használók körében. A kérdőívet online lehetett kitölteni, önkéntesen és névtelenül. A kutatás 2023-ban kezdődött, és 2024. február 3-án zárult. A felmérésben Magyarországon 135-en vettek részt, míg Szerbiában 274-en, így mindösszesen 409 fő lett megkérdezve.[31]

A felmérés alapján Magyarországon a résztvevők 98,5%-a válaszolta azt, hogy használ okoseszközöket, míg Szerbiában 97,8%-a. Ez alapján megállapítható, hogy mindkét országban népszerű az okoseszközök használata.

Az 1. ábra az okoseszközök használatát mutatja be a felmérés alapján Magyarországon és Szerbiában.



1. ábra: Az okoseszköz-használat Magyarországon és Szerbiában a felmérés alapján
Forrás: a szerzők szerkesztése

A felmérésben vizsgáltuk még az okoseszköz-használók jelszóhasználati szokásait, mint például, hogy a jelszó, amit használnak, tartalmaz-e kis- és nagybetűket, számokat, speciális karaktereket, személyes információt vagy értelmes szót, ugyanazt a jelszót használják-e több helyen, vagy hogy milyen hosszú jelszavakat használnak.

[30] Годишњи програм информатика и рачунарство – 8. разред.
[31] Mandić–Kiss–Rajnai 2024.

Amíg Magyarországon a felmérésben részt vevők közül 94% válaszolta azt, hogy az általuk használt jelszó kis- és nagybetűket, számokat, speciális karaktereket is tartalmaz, addig Szerbiában a felmérésben részt vevők közül 76,1% válaszolta ugyanezt. Magyarországon 23,1% válaszolta, hogy az általuk használt jelszó személyes információkat tartalmaz, Szerbiában ez az arány 47,1% volt. Magyarországon arra a kérdésre, hogy a jelszó tartalmaz-e értelmes szót, a résztvevők 51,9%-a válaszolta, hogy az általuk használt jelszó értelmes szót tartalmaz, míg Szerbiában 71,8%. Magyarországon a válaszadók 64,7%-a használja ugyanazt a jelszót több helyen, míg Szerbiában 72,5%. Magyarországon a válaszadók 31,8%-a soha nem változtatja meg a jelszót, Szerbiában a válaszadók 61%-a jelölte meg ezt. Magyarországon a megkérdezettek 43,6%-a válaszolta, hogy az általuk használt jelszó 12 vagy ennél is több karakterből áll, Szerbiában ugyanez az érték 21,4%.

A 3. táblázatban láthatjuk a jelszóhasználati szokásokat az okoseszköz-használók körében a felmérés alapján.

3. táblázat: A jelszóhasználati szokások az okoseszköz-használók körében a felmérés alapján Magyarországon és Szerbiában

Jelszóhasználati szokások	Magyarország (%)	Szerbia (%)
Jelszó tartalmaz kis- és nagybetűket, számokat, speciális karaktereket		
Igen	94	76,1
Nem	6	23,9
Jelszó személyes információkat tartalmaz		
Igen	23,1	47,1
Nem	76,9	52,9
Jelszó értelmes szót tartalmaz		
Igen	51,9	71,8
Nem	48,1	28,2
Ugyan azt a jelszót több helyen használja		
Igen	64,7	72,5
Nem	35,3	27,5
A jelszó változtatása		
Napi szinten	0	0,4
Heti szinten	0,8	1,8
Minden hónapban	5,3	4
Félévenként	18,9	16,4
Évenként	43,2	16,4
Soha	31,8	61
A jelszó hossza		
Kevesebb mint 8 karakter	3	15,6
8–10 karakter	53,4	63
12 vagy ennél is több karakter	43,6	21,4

Forrás: a szerzők szerkesztése

Láthatjuk, hogy Magyarországon a jelszó tartalmát illetően az okoseszköz-használók tudatosabban választanak olyan jelszót, amely tartalmaz kis- és nagybetűket, számokat, speciális karaktereket, valamint kevesebben használnak személyes információkat vagy értelmes szót tartalmazó jelszavakat, mint Szerbiában. Szerbiában a válaszadók 61%-a soha nem változtatja meg a jelszót, amit használ. Ezenkívül Magyarországon többen használnak olyan jelszót, amely 12 vagy ennél is több karaktert tartalmaz, mint Szerbiában.

A Mann–Whitney U-teszt egy statisztikai teszt, amelyet arra használnak, hogy összehasonlítsanak két csoportot, hogy azok szignifikánsan különböznek-e egymástól. A Mann–Whitney U-teszt szignifikáns különbséget mutat, ha $p < 0,05$.[32]

A 4. táblázatban láthatjuk a jelszóhasználatot Magyarországon és Szerbiában a Mann–Whitney U-teszt által.

4. táblázat: Jelszóhasználat Magyarországon és Szerbiában, Mann-Whitney U-teszt

Mann–Whitney U-teszt	**p**
A jelszó tartalmaz kis- és nagybetűket, számokat, speciális karaktereket	0,003
A jelszó személyes információkat tartalmaz	0,545
A jelszó értelmes szót tartalmaz	0,002
Ugyanazt a jelszót több helyen használja	0,963
A jelszó változtatása	0,837
A jelszó hossza	0,910

Forrás: a szerzők szerkesztése

A jelszóhasználat esetében, amikor a jelszó tartalmát nézzük, hogy a jelszó kis- és nagybetűket, számokat és speciális karaktereket, valamint értelmes szót tartalmaz, szignifikáns különbség van. Láthatjuk, hogy a válaszadók Magyarországon szignifikánsan összetettebb jelszavakat használnak a jelszó tartalmát illetően. Az értelmes szót tartalmazó jelszó esetében pedig elmondható, hogy Szerbiában szignifikánsan többen használnak olyan jelszót, amely értelmes szót tartalmaz.

Összefoglalás

Az eddigi szakirodalmi áttekintések alapján, amelyek vizsgálták a két ország informatikai oktatási tananyagát, azt lehet mondani, hogy Magyarország előnyben van Szerbiához képest. Láthatjuk, hogy a két ország informatikai oktatási tananyaga között különbség található. Magyarországon több informatikai óraszám van, mint Szerbiában, valamint a tantervben is van különbség. Ezenkívül Szerbiában azoknak a középiskolásoknak, akik nem az IT-, valamint a digitális ágazatokhoz tartoznak, csak az első évben kötelező a számítástechnika és informatika tantárgy. Magyarországon az információbiztonság-tudatosság fejlesztésére nagyobb hangsúly kerül, mint Szerbiában. Szerbiában továbbá még mindig kevés tanfolyam és képzés foglalkozik a lakosság digitális kompetenciáival. Ez a felmérés eredménye alapján is látható, amit az okoseszköz-használók körében végeztünk Magyarországon és Szerbiában. Ez alapján

[32] Lásd Interpret the key results for Mann-Whitney Test [é. n.].

elmondható, hogy Magyarországon szignifikánsan összetettebb jelszavakat használnak a jelszó tartalmát illetően, amely így biztonságosabb azonos hosszúság esetén brute force támadáskor. Szerbiában szignifikánsan többen használnak olyan jelszót, amely értelmes szót tartalmaz, így a Szerbiában élők nagyobb veszélynek vannak kitéve, mint a Magyarországon élők. Szerbia az elmúlt évek során több lépést is tett annak érdekében, hogy próbálja javítani az oktatási rendszert, de ez még mindig nem elegendő, és további javításokra lenne szükség.

A cikk a 2024. október 15-i II. Alverad-Bánki Nemzetközi Kiberbiztonsági Konferencián elhangzott előadás kivonata.

Felhasznált irodalom

Bak Gerda – Kelemen-Erdős Anikó (2022): Információbiztonság-tudatosság az Y generáció szemszögéből, kvalitatív megközelítés alapján. *Hadmérnök,* 17(3), 81–95. Online: https://doi.org/10.32567/hm.2022.3.6

Busa Attila József (2023): A digitális információbiztonság alapja: A megfelelő kibertudatosság. *Hírvillám,* 25–43. Online: https://comconf.hu/kiadvany/Nemzetk%C3%B6zi%20Katonai%20Inform%C3%A1ci%C3%B3biztons%C3%A1gi%20Konferencia_2023.pdf

Eduline (2020): Informatika helyett jön a digitális kultúra óra – a diákok már ötödikben robotokat programozhatnak. *Eduline,* 2020. július 16. Online: https://eduline.hu/kozoktatas/20200716_digitalis_kultura_ora

Farkas Csaba – Lénárd András – Siegler Gábor (2020): *Útmutató a digitális kultúra tantárgy tanításhoz a 2020-ban kiadott Nemzeti alaptanterv és kerettantervek alapján.* NAT. Online: www.oktatas2030.hu/wp-content/uploads/2020/10/utmutato-a-digitalis-kultura-tantargy-tanitasahoz.pdf

Horváth Regina (2019): Az okoseszközök világának kockázatai a GDPR tükrében, avagy mennyire vagyunk biztonságban? *Acta Universitatis Szegediensis: Forum: Publicationes Discipulorum Iurisprudentiae,* (2), 131–160. Online: https://acta.bibl.u-szeged.hu/70864/1/forum_discipulorum_2019_131-160.pdf

Ilić, Silvia (2020) *Upotreba informacionih tehnologija u nastavi – stavovi i mišljenja nastavnika i učenika.* Doktori disszertáció. Univerzitet u Novom Sadu Prirodno-Matematički Fakultet. Online: https://nardus.mpn.gov.rs/bitstream/id/68509/Disertacija.pdf

Interpret the Key Results for Mann-Whitney Test [é. n.]. Online: https://support.minitab.com/en-us/minitab/help-and-how-to/statistics/nonparametrics/how-to/mann-whitney-test/interpret-the-results/key-results/

Informatika postaje obavezan predmet od prvog razreda osnovnih škola u Srbiji. Online: https://startit.rs/informatika-postaje-obavezan-predmet-od-prvog-razreda-osnovnih-skola-u-srbiji/

Информатика и Рачунарство – 7. разред. Online: https://osstanojemiljkovic.nasaskola.rs/files/Vladimir%20Kne%C5%BEevi%C4%87/Plan%20Informatika%20i%20Ra%C4%8Dunarstvo%20-%20Kne%C5%BEevi%C4%87%20Vladimir%20VII%20razred.pdf

Информатика и рачунарство обавезан предмет за ученике петог разреда. Online: https://prosveta.gov.rs/vesti/informatika-i-racunarstvo-obavezan-predmet-za-ucenike-petog-razreda/

Годишњи програм информатика и рачунарство – 5. разред. Online: https://osstanojemiljkovic.nasaskola.rs/files/Vladimir%20Kne%C5%BEevi%C4%87/Plan%20Informatika%20i%20Ra%C4%8Dunarstvo%20-%20Kne%C5%BEevi%C4%87%20Vladimir%20V%20razred.pdf

Годишњи програм информатика и рачунарство – 6. разред. Online: https://osstanojemiljkovic.nasaskola.rs/files/Vladimir%20Kne%C5%BEevi%C4%87/Plan%20Informatika%20i%20Ra%C4%8Dunarstvo%20-%20Kne%C5%BEevi%C4%87%20Vladimir%20VI%20razred.pdf

Годишњи програм информатика и рачунарство – 8. разред. Online: https://osstanojemiljkovic.nasaskola.rs/files/Vladimir%20Kne%C5%BEevi%C4%87/Plan%20Informatika%20i%20Ra%C4%8Dunarstvo%20-%20Kne%C5%BEevi%C4%87%20Vladimir%20VIII%20razred.pdf

Kerti András – Koller Marco (2021): Az okoseszközök applikációi által gyűjtött metaadatokkal való visszaélések kockázati szemléletmód általi, felhasználói szintű lehetséges visszaszorítása. ***Hadmérnök,*** 16(4), 145–156. Online: https://doi.org/10.32567/hm.2021.4.11

Kerettanterv az általános iskola 5–8. évfolyama számára. Online: https://www.oktatas.hu/kozneveles/kerettantervek/2020_nat/kerettanterv_alt_isk_5_8/

Kerettanterv a gimnáziumok 9–12. évfolyama számára. Online: https://www.oktatas.hu/kozneveles/kerettantervek/2020_nat/kerettanterv_gimn_9_12_evf

Kőrösné Mikis Márta (2009): ***Az Informatika helyzete és fejlesztési feladatai.*** Oktatási Hivatal. Online: https://ofi.oh.gov.hu/tudastar/tantargyak-helyzete/informatika-helyzete

Mandić Dorottya (2023): Az okoseszközök veszélyei. ***Biztonságtudományi Szemle,*** 5(3), 37–45. Online: https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/ho me/article/view/369/289

Mandić Dorottya – Kiss Gábor (2023): Az okoseszközök és vírusvédelem használata Magyarországon és Szerbiában. In Kiss Gábor (szerk.): ***30th Anniversary Conference of the Safety and Security Enineering Education: A biztonságtechnikai mérnök képzés 30 évi jubileumi konferenciája.*** Budapest: Óbudai Egyetem, 64–75.

Mandić, Dorottya – Kiss, Gábor – Rajnai, Zoltán (2024): Password Usage among Users of Smart Devices in Hungary and Serbia. In Szakál, Anikó (szerk.): ***SACI 2024: 18th IEEE International Symposium on Applied Computational Intelligence and Informatics: Proceedings.*** New York: Institute of Electrical and Electronics Engineers (IEEE), 309–313. Online: https://doi.org/10.1109/SACI60582.2024.10619863

Matović, Marijana (2021): ***Programi digitalnih kompetencija u Republici Srbiji.*** Fakultet političkih nauka, Univerzitet u Beogradu. Online: www.osce.org/files/f/documents/d/7/495181.pdf

Jogi források

2012/2015. (XII. 29.) Korm. határozat az internetről és a digitális fejlesztésekről szóló nemzeti konzultáció eredményei alapján a Kormány által végrehajtandó Digitális Jólét Programjáról

Zakon o osnovama sistema obrazovanja i vaspitanja. Online: www.paragraf.rs/propisi/zakon_o_osnovama_sistema_obrazovanja_i_vaspitanja.html

HADMÉRNÖK
VÉDELEMINFORMATIKA

19. évfolyam (2024) 4. szám 153–165.
DOI: 10.32567/hm.2024.4.11

István Oláh,[1] Sándor Magyar[2]

Security and Operational Controls for a Public Cloud Service in a Financial Institution

Abstract

Today, cloud computing services are growing very fast. One of the main reasons for this is the increasing competition and innovation in the market, the increased demand for resources in IT systems and the demand for more complex knowledge-based solutions. Deploying a server and performing the associated tasks on your own infrastructure can often take weeks or months, while the same process takes only a few minutes with a cloud service provider. The use of cloud services has become commonplace for anyone using mobile devices, and for financial institutions, this technology is becoming inevitable in the short term. If an organisation carefully selects a service provider on the basis of legal, technical and information security criteria, and then monitors its operations on an ongoing basis, there is no reason why a financial institution should not use public cloud services, according to the criteria examined. It is important to stress, however, that our analysis did not cover all possible risk factors.

Keywords: public cloud services, information security, financial controls, audit method, physical controls, logical controls

Introduction

Today, IT services based on cloud technology are rapidly expanding. One of the reasons for this is the new demand for resources in IT ecosystems, systems with more complex knowledge, resulting from accelerating market competition and innovation. Getting a server up and running, and setting up the associated tasks, can take weeks or months on a dedicated infrastructure. The same in the cloud can be provided by

[1] E-mail: olah.istvan.gyorgy@uni-nke.hu
[2] E-mail: magyar.sandor@uni-nke.hu

a cloud service provider in minutes. For the processes and operations of a company, financial institution, or public administration, the IT systems must be available according to the SLAs[3] to access the services provided, and these can be delivered in the cloud. This expectation is reflected in the CER,[4] NIS2,[5] and DORA[6] specifications, which came into force in January 2023. Gartner's *The Cloud Strategy Cookbook*[7] outlines several key information security ideas:

- What are the security, governance, compliance, and data requirements?
- Does it contain personally identifiable information and security requirements?
- Is a vendor involved?
- Does it have special integration or location requirements?

In 2015, ENISA[8] published *Secure Use of Cloud Computing in the Finance Sector*.[9] In 2021, it has already clearly recommended the use of a specification in practice in its publication on healthcare systems,[10] based on NIST[11] and BSI[12] – C5.[13]

In many cases, the choice between a terrestrial and/or a cloud-based IT system is no longer a decision for the operations of financial institutions. The reason is that software vendors are developing new solutions in their own data centres less and less frequently, and are also migrating existing systems to cloud versions, resulting in the fact that in a few years, they will no longer support the non-cloud case.

The present study sets out the following research objectives:

RO1: Examination of the utilisation of public cloud services in a financial institution.

RO2: Analysis of physical security requirements from the perspective of a financial institution in the context of public cloud services.

Consequently, the research study has identified the following research questions to be addressed:

RQ1: Can a public cloud be audited in compliance with domestic regulations for a financial institution?

RQ2: Can a cloud service provider's data centre be considered part of a financial institution's operational environment? If so, how?

[3] SLA – Service Level Agreement.
[4] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.
[5] Directive (EU) 2022/2555 OF the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS2 Directive).
[6] Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.
[7] Gartner 2021.
[8] ENISA – European Union Agency for Cybersecurity.
[9] Naydenov et al. 2015: 11.
[10] ENISA 2021.
[11] NIST – National Institute of Standards and Technology.
[12] BSI – Federal Office for Information Security in Germany.
[13] C5 – Cloud computing C5 criteria catalogue.

Cloud services

The cloud is a technology and the services associated with it. In practice, they are still often confused, because, for example, a "cloud" can be on the ground.

Cloud services are not defined in legislation. There are several arguments for and against the need for separate regulation, for example:

- NO, because the cloud (all components) or part of it can be in your machine room
- NO, because the primary concern for the data is consistent protection
- NO, because everything can be regulated in the related contracts
- YES, because it is in the public interest to regulate part of the mandatory content of contracts
- YES, because the immediacy of physical controls has been partially removed
- YES, because of the level of risk justified by the non-operational risk of larger cloud service providers
- YES, because the cloud has become the operational space for civil and military cyberspace

The authors' position on this is that no specific regulation is necessary, because it is irrelevant to the data where it can be located in an IT ecosystem,

- user, server on host
- on the network
- on storage
- the above on a virtual version
- on tape
- on disk
- on portable storage media
- on a mobile device
- anywhere
- in the cloud

because its protection must be consistent and proportionate to the risks.

In practice, the definitions provided in the National Institute of Standards and Technology (NIST) document 800-145 are utilised.[14] The common characteristics of services are:

- the ability to use the service as needed at that time, sometimes on a self-service basis
- access to the network is essential
- shared use of resources among users
- tracking of required operational capacities, payment of dynamic resources, and charges proportional to the services utilised

[14] Mell–Grance 2011.

Taking into consideration the ownership, the nature and content of the services provided, and the geographical location, the following cases may exist according to NIST:

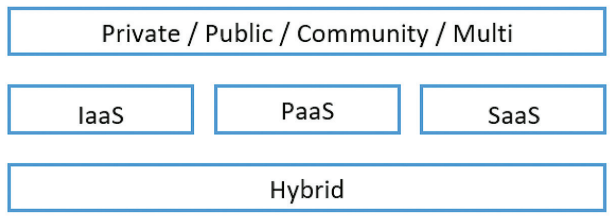


Figure 1: Categorisation of cloud services
Source: compiled by the authors

- Private is when an organisation uses the cloud as a technology in a private manner
- Public refers to service is typically available to everyone via the Internet, free of charge and/or for a service fee
- Community describes a service that is typically available to a specific group of people over the Internet, free of charge and/or for a fee
- IaaS[15] is when the basic infrastructure is utilised
- PaaS[16] when a service includes an operating system and/or running environment
- SaaS[17] when everything is provided by the service provider by outsourcing data and users
- Multi refers to the scenario where multiple service provider solutions are used in an integrated manner
- Hybrid describes a service provider's solution is deployed with some or all of the resources being hosted on the customer's infrastructure

Responsibility aspects

The management of information security risks in terms of services between the service provider and the service recipient should be clearly defined in terms of responsibilities at the IT ecosystem levels. The Hungarian National Bank Recommendation[18] guides a financial institution in this regard:

[15] IaaS –Infrastructure as a Service.
[16] PaaS – Platform as a Service.
[17] SaaS – Software as a Service.
[18] Recommendation No. 4/2019 (IV. 1.) of the National Bank of Hungary.

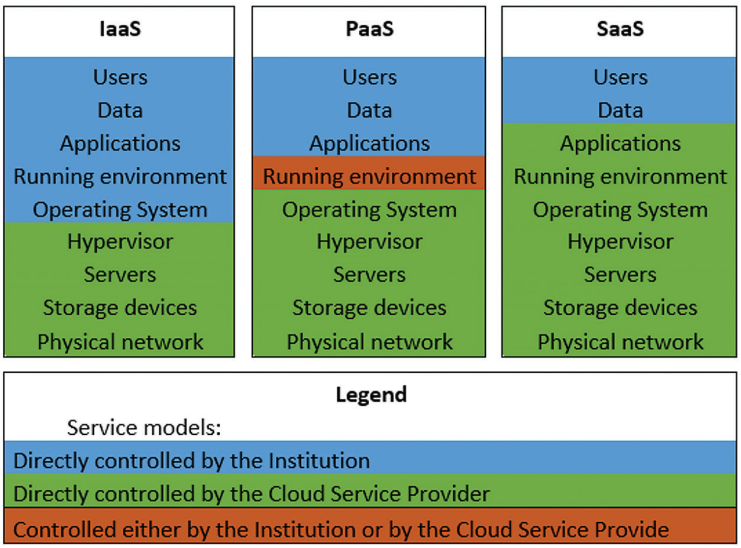


Figure 2: Service models and direct operators of controls over elements
Source: Recommendation No. 4/2019 (IV. 1.) of the National Bank of Hungary

It is important to emphasise that the client of the public cloud service, i.e. the financial institution, is always responsible for the handling of users and the confidentiality, integrity, and availability of data.

A service used can now be practically anything. Cloud technology can be used for wrong purposes without significant expertise, for example by cybercriminals.

Matching the control logic of a public cloud service to its legal logic in five steps

In our country, several financial institutions are covered by the Act CLXVI of 2012 on the identification, designation and protection of critical systems and facilities (hereinafter: LRTV),[19] because finance is one of the sectors listed in its annex. In this context, the Act L of 2013 on the information security of state and municipal bodies (hereinafter: IBTV)[20] is applicable to these organisations under Section 2(c). The information security requirements of the IBTV are established in an implementing decree of the Ministry of the Interior; in 2024, the MK decree on the new security classification and information security conventions in the context of NIS2 was published.[21]

At the time of writing, both regulations were in force. The Act CCXXXVII of 2013 on Credit Institutions and Financial Enterprises (hereinafter: HPT)[22] is one of the foundational pieces of legislation relating to financial activities. According to Article 67/A

[19] Act CLXVI of 2012.
[20] Act L of 2013.
[21] Decree No. 7 of 2024 (VI. 24.) of the Cabinet Office of the Prime Minister.
[22] Act CCXXXVII of 2013.

of the HPT, IT systems in operation must possess a continuous certificate of secrecy. The Act CIII of 2023 on the Digital State and Certain Rules for the Provision of Digital Services (hereinafter: DÁPTV),[23] a financial institution is also an organisation obliged to provide digital services. In this context, Section 81(1)(d) of the Act establishes the basis for the requirements regarding information security compliance. Both the HPT and the DÁPTV require compliance with the same government regulation.[24] It has been stated in several analyses, and conference presentations, that financial institutions to which the DORA requirements apply are not subject to NIS2. This correlation exists as long as a credit institution provides its services to an entity subject to DORA under a law of a country's jurisdiction that is founded on NIS2.

Based on the provisions of the NIS2, the Cybersecurity Act, the Act also defines several services, such as data centre services and cloud services, which are included in the Digital Infrastructure sector. A credit institution may have customers that DORA does not cover, and therefore the Act XXIII of 2023 on Cybersecurity Certification and Cybersecurity Supervision (hereinafter: Cyber-certification Act).[25] For this reason, the implementing regulation will also apply to a credit institution if it is a financial institution. The controls in the new regulation are defined based on NIST-800-53 Rev. 5.[26]

Audit of legal logic requirements

In the light of international and national laws and regulations, the question arises as to whether a credit institution's IT systems can be audited against the required logical controls.

This question has been posed to the audience and co-presenters at several professional conferences in the recent past. The typical answer received back was no. We believe the answer to this question is yes, but in several steps. The steps can be taken for any public cloud provider, an example is given for Microsoft Azure.

Selecting and assembling a test control

As a first step, it is necessary to select a logical control based on BM Decree 41/2015 (15. VII.)[27] (hereinafter: BM Decree) and MK Decree 7/2024 (24. VI.) (hereinafter: MK Decree), for example, the lock of the work section, which must be aligned with the NIST identifier.

[23] Act CIII of 2023.
[24] Government Decree 42/2015 (III. 12.).
[25] Act XXIII of 2023.
[26] NIST Computer Security Resource Center 2020.
[27] Decree 41/2015. (VII.15.) of the Minister of Interior.

Table 1: NIST assembly of regulatory control

BM Decree			
Locking the session	3.3.10.10	3.3.10.10.2 Covering the screen: When locking a session, the information previously visible on the screen should be obscured by a publicly visible image (or blank screen) or by the login interface, which may include the name of the person locking the session.	
MK Decree			**NIST**
Lock device, Screen lock	2.83	The organisation concerned shall hide the information on the display when locking the device. The organisation shall display static or dynamic images on the device display during the lock period. During device locking, the organisation shall ensure that the information on the display is not visible. In this way, the organisation prevents access by unauthorised persons.	AC- 11 (1)

Source: compiled by the authors

NIST control documentation

The second step is to identify the control in the audit documents published by the cloud service provider.

Table 2: AC-11 (1) control

NIST			
AC-11 (1)	Device Lock, Pattern-hiding Displays	Conceal, via the device lock, information previously visible on the display with a publicly viewable image.	The pattern-hiding display can include static or dynamic images, such as patterns used with screen savers, photographic images, solid colours, clock, battery life indicator, or a blank screen with the caveat that controlled unclassified information is not displayed.

Source: NIST Special Publication 800-53

Examining the possibility of control

In a third step, it is suggested to examine the possibility of establishing control AC-11 (1) in the example, based on several compliance documents audited by third parties. It is very important to note that control as an option does not imply the implementation of control as required by the organisation.

This is stated in the documentation:

"AC-11 Session Lock. The information system:

(a) Prevents further access to the system by initiating a session lock after [FedRAMP Assignment: fifteen (15) minutes] of inactivity or upon receiving a request from a user; and

(b) Retains the session lock until the user re-establishes access using established identification and authentication procedures."

Definition of control parameters at the organisational level

In the fourth step, it is necessary to define the control parameters of the organisation. This can be done in a related policy or an Information System, Information Security System Plan. In the case of a session lock control, it is the time parameter that must be specified. This can be any value, which may be as long as 15 minutes, set by the cloud service provider. The principle of proportionality of risk should be applied to this definition. Accordingly, several values may be prescribed for a single cloud service provider based on the risk level of the IT system. In the practical examples examined, this conscious value setting is often not performed and the time parameter set by the service provider is typically used. In any case, it is recommended that the parameters of the controls for service users should be defined, if possible, based on a risk analysis. The defined values can and should be recorded in the system security system plan, for example, in an OVI[28] table. If necessary, the table can be extended with additional controls specific to the cloud service.

Validation of the required control parameters

In the fifth step, the parameters required by the security domains in the design of a cloud service need to be set according to the related and approved documentation. This can also be accomplished through individually accessible administrator service web interfaces. For an IT system, many information security controls must be established in a public cloud service. This may require thousands of parameters to be configured. To facilitate this, service providers typically offer an API.[29] A simple script can be created to set the required security parameters in an automated manner. In this case, it is recommended that a six-eyes check is integrated into the organisation's internal processes before executing the settings, as the use of this procedure in itself poses a significant information security risk.

Continuous monitoring of controls

APIs provided by service providers also allow an organisation to export the parameters of the services it uses. Building on this capability, simple scripts can be created to

[28] See: https://nki.gov.hu/hatosag/hirek/ovi-urlap-4-60/
[29] API – application programming interface.

provide an automated way to continuously monitor the information security control parameters of IT ecosystem elements in the cloud. One example of this is to compare the read parameter with the required parameter and reporting discrepancies. Another possibility is to monitor the deviation from the previously read value. Many more examples of verification could be described, but the emphasis is on treating any discrepancy found during verification as an information security incident. These incidents are always investigated in a documented manner by the organisations according to their respective procedures, thus creating secondary control over the cloud service providers. It is recommended that the logs of a cloud service provider's administrative activities be reviewed before engaging a service. It is necessary to determine for which activities and which log entries should be generated by the organisation. In practice, it is advisable to do this before the contract is concluded because, in this case the specification can be taken into account when choosing a service provider. The logs generated by operational systems in a public cloud should be continuously scanned by an analytical SIEM,[30] SOAR[31] or any analytical system, thus reducing the risk of exposure to the cloud service provider.

Mapping a public cloud service to regulatory-based physical controls

When using a public cloud service, except in the hybrid case, the user must accept, in fully or in part, that the server rooms or data centres will be located outside the physical space under their direct control. It does not follow that it is not necessary to analyse the physical controls. It is recommended that a public cloud service provider's data centre is subject to the physical controls of the relying organisation, even though the data centres are not located in its facilities.

The legislation described for the examination of logical controls includes the IBTV. The second paragraph of the third section typically applies to a financial institution. According to this, IT systems may have components within the European Union. This is a geolocation constraint that should be tested for compliance at the outset of a cloud service provider selection process and non-compliant providers should be excluded. Typically, the leading cloud providers in Europe and the U.S. can meet this requirement. It is recommended that cloud service contracts should specify the countries and localities in which the service provider will deliver services to the customer. It is also advisable to stipulate in the contracts that the customer has the right to control the physical facilities directly or indirectly. If these are included in the contracts, a significant step will be taken to ensure that a cloud service user can view the service provider's premises as they would as a private facility.

[30] Security Information and Event Management.
[31] Security Orchestration, Automation, and Response.

Audit of legal physical requirements

Most physical controls can be checked similarly using the five-step method described in the previous chapter. For completeness, a specific procedure and/or additional control is recommended. An example of each is provided.

Continuous monitoring of controls with specific additions

A public cloud service operating area is usually not managed or controlled by the user. It is recommended that specific additions beyond the five steps outlined in the case of logical controls are included in the related contracts.

Chapter 3.1.5 of the BM Decree provides for the management of security incidents. According to 3.1.5.6.1.1, "everyone who is in contact with the electronic information system or the object in which it is located is required to report the occurrence of a security incident or if an indication or emergency is detected".

Chapter 3.2.1 of the BM Decree prescribes controls for physical and environmental protection, for example: "3.2.1.4.1 The covered entity: 3.2.1.4.1.1. Shall ensure physical access to authorized personnel only at entry and exit points defined by the covered entity."

The technical, human, and other skills needed to do this are covered in the five-step methodology already described for logic checks. This does not imply that the user organisation meets the requirements in Sections 3.1.5 and 3.2.1, as the information on the controls is available from the cloud service provider in the course of day-to-day operations. For this reason, specific clauses for such cases need to be included in the service contracts, as they are usually not included in the service providers' blanket contract designs. In our case, the physical locations of the services used:

- access rules
- for the management of rights in the monitoring systems
- the incident reporting process and contact details
- the means of monitoring the above

be specified in the service contract.

It is also included as a control requirement in the MK Decree in point 11.6:

"The organization shall ensure that digital and analog media are protected and controlled by appropriate security measures during transportation outside the controlled area." Examples of digital media include floppy disks, magnetic tapes, external/removable hard disks, flash drives, CDs, and DVDs. Examples of analog media include paper and microfilm.

"The organization must ensure accountability of the media during transport outside controlled areas." This may include restricting transport activities to authorised persons and monitoring transport activities.

"The organization should document activities related to the transport of media." The organisation concerned should have the flexibility to define the methods of

record-keeping for different types of media transfers, based on the risk assessment of the EIR.

Additional physical controls

If you use a cloud service, you may need to implement additional controls, as data centres are not directly supervised. An example of this are the requirements found in BM Decree 3.3.8.5.2, and in MK Decree 11.6, which can be used as a logical control to facilitate activities in the physical space.

Table 3: NIST assembly of regulatory control

BM Decree			NIST
Cryptographic protection	3.3.8.5.2	Cryptographic mechanisms should be in place to protect the confidentiality and integrity of information stored on digital media during transport outside controlled areas.	MP-5
MK Decree			
Transport of data media	11.6	1. The organisation must ensure that digital and analogue media are protected and controlled by appropriate security measures during transportation outside the controlled area. Examples of digital media include floppy disks, magnetic tapes, external/removable hard disks, flash drives, CDs, and DVDs. Examples of analogue media include paper and microfilm. 2. The organisation must ensure accountability of the media during transport outside controlled areas. This may include restricting transport activities to authorised persons and monitoring transport activities. 3. The organisation should document activities related to the transport of media. The organisation concerned should have the flexibility to determine the methods of record-keeping for different types of media transfers, based on the EIR risk assessment.	

Source: compiled by the authors

Microsoft's premises are considered to be an area not controlled by the user. Digital media for backup and archiving purposes are also produced here and handled during transport. According to the documentation available for the five-step methodology described in the Logical controls test, the service provider platform is capable of encryption. It does this by default using a self-generated and self-managed cryptographic procedure. For a financial institution, it is necessary to consider whether these are sufficient to adequately manage industry secrets, GDPR,[32] and corporate confidentiality. We think not, because in this case all data is still available to a cloud service provider in an interpretable manner, so additional controls need to be applied. To this end, it is proposed to develop a separate HSM[33] solution used and managed

[32] GDPR – General Data Protection Regulation.
[33] HSM – Hardware Security Module.

exclusively by the user organisation. To enhance the information security for use, the following is proposed:

- If possible, do not generate keys on the service provider's devices, because residual information must be considered.
- Key management should be controlled and restricted.
- All activities in the key management processes should be performed by the user organisation.
- Stored keys should not be directly accessible by the cloud service provider.

There are several options for setting up an HSM with cloud service providers on a software-based solution, which can be interpreted as a SaaS. Its development can be completed quickly with the associated process flows without integration issues. In our experience, this solution is suitable for a financial institution. If required, it is also possible to develop a custom hardware-based HSM, but then all external and internal APIs must be developed and kept up to date by the customer organisation, which can be managed by a specially trained staff.

Discussion

Cloud services are now commonplace for anyone using a mobile device. In the case of financial institutions, it will become unavoidable in the short term. If an organisation selects a service provider based on legal, technical, and information security criteria and continuously monitors its operations, there is no obstacle for a financial institution to use a public cloud service based on the criteria examined in this article.

It is also important to emphasise that not all possible risks have been considered in this analysis. For this reason, we recommend that all organisations should draw up a list of information security controls for analysis in proportion to the risks associated with other aspects. Based on the criteria you have compiled, analyse the use of any public cloud service, the outcome of which may be that you do not use the service or use it differently.

Drawing on the conducted studies, our results are as follows:

R1: We have determined that by applying our five-step examination method proportionally to risk, a financial institution can audit a public cloud service, except for certain physical controls.

R2: We have found that, from the perspective of protected data, security must be implemented uniformly regardless of storage and processing location. Therefore, a public cloud provider's data centre must be subject to at least the same controls as a financial institution's own data centre. Given that a financial institution cannot directly control the physical space of a public cloud provider, compensatory controls, such as data encryption, ensure adequate protection.

This article is an excerpt from a presentation given at the II. Alverad-Bánki International Cybersecurity Conference on October 15, 2024.

References

European Union Agency for Cybersecurity (ENISA) (2021): *Cloud Security for Healthcare Services.* Online: www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Cloud%20Security%20for%20Healthcare%20Services.pdf

Gartner (2021): *The Cloud Strategy Cookbook.* Online: www.gartner.com/smarterwithgartner/the-cloud-strategy-cookbook

Mell, Peter – Grance, Tim (2011): NIST SP 800-145, *The NIST Definition of Cloud Computing.* Gaithersburg, MD, USA: National Institute of Standards and Technology. Online: https://doi.org/10.6028/NIST.SP.800-145

Naydenov, Rossen – Liveri, Dimitra – Dupre, Lionel – Chalvatzi, Eftychia (2015): *Secure Use of Cloud Computing in the Finance Sector.* ENISA. Online: https://doi.org/10.2824/199301

NIST Computer Security Resource Center (2020): *NIST SP 800-53 Rev. 5 Security and Privacy Controls for Information Systems and Organizations.* Online: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

Recommendation No. 4/2019 (IV. 1.) of the National Bank of Hungary on the use of community and public cloud services. Online: www.mnb.hu/letoltes/4-2019-felho.pdf

Legal sources

Act CLXVI of 2012 on the Identification, Designation and Protection of Critical Systems and Facilities

Act L of 2013 on the Information Security of State and Municipal Bodies

Act CCXXXVII of 2013 on Credit Institutions and Financial Enterprises

Act XXIII of 2023 on Cybersecurity Certification and Cybersecurity Supervision

Act CIII of 2023 on the Digital State and Certain Rules for the Provision of Digital Services

Decree No. 7 of 2024 (VI. 24.) of the Cabinet Office of the Prime Minister on the requirements for security classification and the specific security measures to be applied for each security class

Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC

Government Decree 42/2015 (III. 12.) on the protection of IT systems of financial institutions, insurance and reinsurance undertakings, investment ventures and commodity exchange service providers

Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011

Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)

HADMÉRNÖK
VÉDELEMINFORMATIKA

19. évfolyam (2024) 4. szám 167–182.
DOI: 10.32567/hm.2024.4.12

Paráda István,[1] Tóth András[2]

A NATO katonai légi szállítási képességek kibervédelmi aspektusai

Cybersecurity Challenges for NATO Military Air Transport Operations

Absztrakt

A légi közlekedési ágazat egyre nagyobb mértékben támaszkodik a technológiára, ami aggodalomra ad okot az államilag támogatott kibertámadásokkal kapcsolatban, ami a katonai és polgári légi közlekedés számára is kihívást jelent a kiberbiztonság terén. Ez a cikk a NATO katonai légi teherszállítási képességeit elemzi. A kutatás a releváns polgári légi közlekedési kibertámadásokat vizsgálja mint esettanulmányok, a NATO katonai légi szállítás potenciális kiberfenyegetései tükrében. Mindezeket összegezve a szerzők következtetéseket vonnak le azok hatásairól. Ezután elemző-értékelő módszerrel meghatározzák a kibertéri eszközök kategóriáit, amelyek kulcsfontosságúak a légi közlekedési informatikai infrastruktúra védelméhez, és katonai vonatkozásban kiemelik az IT-OT és Platform közötti különbségeket, átfedéseket. Ezenfelül mind a polgári, mind a NATO katonai légi közlekedési rendszereinek kibertámadásokkal szembeni hatékony védelme módjainak átfogó bemutatására törekednek, ami nélkülözhetetlen a biztonságos légi közlekedési rendszer biztosítása és a fejlődő kiberfenyegetések kezelése miatt.

Kulcsszavak: NATO katonai légi teherszállítási képességek, polgári légi közlekedési kibertámadások, Boeing, Airbus, kiberbiztonsági kihívások, IT-OT-Platform

[1] Informatikai műveleti tiszt, NATO Támogatási és Beszerzési Ügynökség, e-mail: paradaistvan@gmail.com
[2] Egyetemi docens, Nemzeti Közszolgálati Egyetem, e-mail: toth.hir.andras@uni-nke.hu

Abstract

The aviation industry's increasing reliance on technology has led to concerns about state-sponsored cyberattacks, which pose cybersecurity challenges for both military and civil aviation. This paper analyses NATO's military air cargo capabilities. It examines relevant civil aviation cyberattacks as case studies in light of potential cyber threats to NATO military aviation. Summarising these findings, the authors conclude their implications. They then use an analytical-evaluative method to identify categories of cyberspace assets that are key to protecting aviation IT infrastructure and highlight the differences and overlaps between IT-OT and Platforms in a military context. In addition, a comprehensive presentation of ways to effectively defend civil and NATO military aviation systems against cyberattacks will be presented, which is essential to ensure a secure aviation system and address evolving cyber threats.

Keywords: NATO military air cargo capabilities, civil aviation cyberattacks, Boeing, Airbus, cybersecurity challenges, IT-OT-Platform

Bevezetés

Ahogy a technológia egyre inkább integrálódik a légi közlekedési ágazatba, az olyan iparági és katonai szereplők számára, mint a NATO, elengedhetetlenné válik, hogy prioritást adjanak a kiberbiztonsági intézkedéseknek. Geopolitikai fronton az államilag támogatott kibertámadások egyre nagyobb aggodalmakat vetnek fel a lehetséges ártalmaik miatt. A digitális rendszerekre való fokozott támaszkodás azonban olyan kiberbiztonsági kihívásokat is jelent, amelyeket kezelni kell, különösképpen a katonai képességek szemszögéből vizsgálva.

A cikk legfontosabb kutatási kérdése, hogy a polgári légi közlekedésben az informatikai rendszerek és infrastruktúra kiberbiztonsági sebezhetőségeinek és fenyegetéseinek azonosítása, elemzése és kezelése milyen kihívásokat tartogat, különös tekintettel a NATO katonai légi szállítási képesség tükrében. A NATO katonai légi szállítási képességek részletes bemutatásának segítségével a kutatás célja az, hogy átfogó képet adjon a katonai légi szállításról és annak potenciális kiberbiztonsági sebezhetőségeiről. Az informatikai rendszerek integrációjának és a digitalizáció folyamatos térnyerésének köszönhetően a civil légi közlekedéshez hasonlóan a katonai légi közlekedési ágazat (és ezáltal a katonai légi szállítás) is egyre nagyobb kockázatnak van kitéve a kiberfenyegetésekkel szemben, ami nagymértékben befolyásolhatja a repülésbiztonságot és az üzemeltetést. E kiberfenyegetések kezelése érdekében a fejlett kiberbiztonsági protokollok és a személyzet folyamatos oktatása kulcsfontosságú lehet az informatikai infrastruktúra védelmében.

A kutatás során alkalmazott módszertanként elsődlegesen a nemzetközi és a kevésbé jellemző hazai releváns szakirodalmak és információt biztosító oldalak elméleti áttekintésével, feldolgozásával a NATO katonai légi szállítási képességének elemeit mutatjuk be. Mivel a NATO katonai légi szállítási képességek és a kiberbiztonság közötti kapcsolatot feltáró adatok és infomációk többnyire nem publikusak,

így elemzési módszertan, illetve esettanulmány a releváns polgári légi közlekedés és kibervédelem kapcsolatában jelenik meg a cikkben. Ezt követően vázoljuk a kiberbiztonság jelentőségét és kihívásait a katonai légi szállítási műveletekben, meghatározzuk a kibertéri eszközök kategóriáit, majd átfogó ajánlásokat teszünk a kockázatok lehetséges csökkentésére.

A NATO katonai légi szállítási képessége

A hatékony stratégiai légi szállítási képességek létfontosságúak annak biztosításához, hogy a NATO-szövetségesek és partnerek gyorsan be tudják vetni haderejüket és felszereléseiket, ahol szükség van rájuk. Ez az oka annak, hogy egyes NATO-szövetségesek és partnerek egyesítik erőforrásaikat annak érdekében, hogy a Szövetség profitálhasson a közösségből, az interoperabilitásból és a méretgazdaságosságból. Az erőforrások összevonása révén a NATO-országok a méretgazdaságosság előnyeit élvezik, és lehetőségük nyílik arra, hogy olyan eszközöket kollektíven szerezzenek meg, amelyek megvásárlása az egyes országok számára megfizethetetlenül költséges lenne.

Jelenleg három kezdeményezés létezik, amelyek célja a Szövetség és a részt vevő partnerországok stratégiai légi szállítási képességeinek biztosítása:

- a Stratégiai Légi Szállítási Megoldás (SALIS) kezdeményezés,
- a Stratégiai Légi Szállítási Képesség (SAC)
- és a Multinacionális Többfeladatú Tanker Szállítási (MRTT) Fleet (MMF).

Minden program sokoldalú és rugalmas képességeket kínál, beleértve a NATO-műveletek és -küldetések támogatását, orvosi segítség szállítását, polgári és katonai betegek evakuálását, polgári és katonai felszerelések szállítását, humanitárius segélynyújtást katasztrófák után és levegő-levegő utántöltés biztosítását. A NATO stratégiai légi szállítási kezdeményezései közé tartozik a szoros együttműködés más nemzetközi szervezetekkel, köztük az Európai Unióval (EU), az Egyesült Nemzetek Szervezetével (ENSZ) és az Afrikai Unióval (AU).[3]

SALIS

A Strategic Airlift International Solution (SALIS) kilenc ország támogatási partnersége, amely Antonov AN–124–100 típusú repülőgépeket bérelve garantált hozzáférést biztosít akár öt repülőgéphez – ezek közül három válság esetén néhány napon belül küldetésre készen áll, kettő a rendelkezésre állás függvényében – nemzeti, NATO- és EU-műveletek és -küldetések támogatására. A Támogatási Partnerség – amelyet a NATO Támogatási és Beszerzési Ügynökség (NSPA) kezel – egy többnemzetiségű együttműködési mechanizmus, amelyet két vagy több NATO-tagország kezdeményezésére hoztak létre, amelyek közös támogatási és szolgáltatási tevékenységeket kívánnak szervezni. 2021 októberében az NSPA ötéves szerződést írt alá a németországi

[3] NATO 2024a.

székhelyű Antonov Logistics Salis céggel. Ez felváltja a korábbi SALIS-szerződéseket, amelyek közül az utolsó 2021 decemberében járt le. A jelenlegi szerződés az AN–124-es[4] repülőgépeken kívül más nagy teherszállító repülőgépeken is rakománykapacitást biztosít, beleértve az IL–76-ot,[5] a készlet erejéig. E szerződés értelmében a SALIS-ban részt vevő országok garantált hozzáférést kapnak a stratégiai légi szállítási képességekhez a túlméretezett rakományok esetében, az éves repülési órakvóta alapján. A képességet napi szinten a Stratégiai Légiszállítási Képesség koordinálja, amely a hollandiai Eindhovenben található európai mozgáskoordinációs központtal (MCCE) közösen működik. Az NSPA kezeli a SALIS szerződést a részt vevő országok nevében, és támogatást nyújt a SALIS Támogatási Partnerségnek.[6]

SAC

A második kezdeményezés, amelynek célja a NATO-szövetségesek és partnerek számára a stratégiai légi szállításhoz való hozzáférés biztosítása, a Stratégiai Légiszállítási Képesség (SAC), amely három Boeing Globemaster III C–17[7] szállítórepülőgépet vásárolt a 12 NATO-szövetségesből álló csoport nevében. Az első C–17-est 2009 júliusában adták át, a második és a harmadik repülőgép 2009 szeptemberében és októberében követte. A légi járművet a Magyar Honvédség 47. Repülőbázisán Pápán a SAC hadműveleti ága, a katonai Heavy Airlift Wing (HAW) üzemelteti. A Stratégiai Légiszállítási Képesség (SAC) egy multinacionális kezdeményezésben részt vevő három katonai Boeing C–17 Globemaster III nagy hatótávolságú teherszállító repülőgépből álló egység, amely megfelel a stratégiai és taktikai légi szállítási követelményeknek. Minden tag nemzete a rendelkezésre álló repülési órák egy részét birtokolja, amit a nemzeti NATO-, ENSZ- és EU-vállalásaik teljesítésére használnak fel. A legújabb fejlemények közé tartozik, hogy a SAC-nemzetek C–17 repülőgép-kiképzési szimulátor üzembe helyezését teszik lehetővé a pápai repülőbázison. A szimulátor kezdeti működési képessége a tervek szerint 2025.[8] A HAW-t az összes részt vevő ország katonai személyzete működteti, és küldetései támogatják a nemzeti követelményeket. A műveletek közé tartozott a Nemzetközi Biztonsági Segítő Erők (Afganisztán), a Koszovói Erők (KFOR), a líbiai Unified Protector hadművelet támogatása, a Haitin és Pakisztánban nyújtott humanitárius segítség, az afrikai békefenntartás, valamint a lengyel hatóságoknak nyújtott segítség a szmolenszki légi katasztrófát követően Oroszországban. Két humanitárius

[4] Az Antonov An–124 Ruszlan (NATO-kódja: Condor) a kijevi Antonov tervezőirodában az 1970-es évek második felében Viktor Tolmacsov főkonstruktőr irányításával kifejlesztett, teljesen fémépítésű, félhéjszerkezetű, felsőszárnyas elrendezésű, behúzható futóművel rendelkező, kétáramú gázturbinás sugárhajtóművel, hermetikusan zárható kabinnal és nem hermetikus tehertérrel rendelkező, merevszárnyú teherszállító repülőgéptípus.

[5] Az Il–76 a Szovjetunióban, az Iljusin tervezőirodában az 1960-as évek végén kifejlesztett négyhajtóműves közepes teherszállító repülőgép.

[6] Hood 2009.

[7] A C–17 Globemaster III (beceneve: Moose = „Jávorszarvas") az amerikai McDonnell Douglas, majd később a Boeing Integrated Defence Systems által kifejlesztett, részben fém, részben kompozit anyagokból épített, félhéjszerkezetű, felsőszárnyas, behúzható futóművel, nagy kétáramúsági fokú gázturbinás sugárhajtóművekkel, hermetikusan zárható kabinnal és tehertérrel rendelkező, harcászati teherszállító feladatkörre kifejlesztett, a levegőben utántölthető, nagy hatótávolságú (stratégiai), merevszárnyú teherszállító repülőgéptípus.

[8] Szarvas 2008: 72–74.

SAC-repülést szerveztek a 2017-es Irma hurrikán után Barbadoson és Guadalupe-on elszenvedett áldozatok megsegítésére. A SAC emellett alapvető egyéni védőfelszereléseket szállított több tagjának a Covid–19 2020-as csúcspontja idején. 2021-ben a SAC járatokat küldött Afganisztánba, hogy evakuálják az embereket (a szövetséges és a partnerországok, valamint a NATO-hoz és a SAC-hoz kötődő afgánok személyzetét) az afgán kormány és az afgán nemzetvédelmi és biztonsági erők összeomlását követően. 2022-ben a SAC tűzoltó egységeket szállított Romániából Franciaországba, hogy segítsenek az erdőtüzek leküzdésében. A Törökországot 2023 februárjában sújtó pusztító földrengésekre válaszul a SAC kilenc küldetést hajtott végre, hogy Finnország, Hollandia, Románia, Svédország és az Egyesült Államok nevében 340 tonna sürgős felszerelést és személyzetet szállítson az országba.[9]

A HAW multinacionális repülőszemélyzete a C–17-es légi és szárazföldi küldetések teljes spektrumát biztosítja, beleértve a légi utántöltést, ejtőernyő-ledobást, rohamleszállást és minden időjárási körülmények közötti műveleteket, nappal vagy éjszaka alacsony és közepes fenyegetettségű környezetekben. A HAW több mint 30 000 órát repült, és kiemelkedően magas (> 80%) átlagos küldetési képességet ért el a SAC flottájában a NAM karbantartás támogatásával. A magas bevetési képességi arány azt jelenti, hogy a repülőgépek készen állnak a SAC nemzet küldetésének késedelem nélküli végrehajtására. A HAW minden kontinensre szállított rakományt, és szállított utasokat.[10]

A NATO Légiszállítási Program (NAMP) egy multinacionális szervezet a NATO támogatási és beszerzési programján belül. A NAMP kezeli és támogatja a C–17-es flottát, amelynek repülőgépei Magyarországon vannak bejegyezve. A NATO nemzetközi állománya a NAMP szervezeti struktúrán belül pénzügyi, logisztikai és adminisztratív szolgáltatásokat nyújt a Heavy Airlift Wing számára. A Heavy Airlift Wing felelős a küldetések végrehajtásáért az előre egyeztetett repült óraelosztásnak megfelelően. A multinacionális SAC Irányítóbizottság átfogó felelősséggel tartozik a program irányításáért és felügyeletéért, és meghatározza a követelményeket. A NATO Támogatási és Beszerzési Ügynökség (NSPA) Légiszállítási Programja (NAMP) kezeli és támogatja a SAC légi szállítási eszközeit, valamint adminisztratív támogatást nyújt a pápai légi bázison működő Heavy Airlift Wing számára.[11]

MRTT

A Multinacionális Többfeladatú Tanker Transport (MRTT) Fleet (MMF) stratégiai szállítási, légi utántöltési és egészségügyi evakuálási lehetőségeket biztosít a részt vevő országok számára. A program az egyetértési megállapodásban (Memorandum of Understanding) körvonalazott összevonási és megosztási koncepción alapul, amelyben a részt vevő országok összevonják a repülőgépeket és megosztják a költségeket, miközben kihasználják a méretgazdaságosság előnyeit. A 111 tonnás alapüzemanyag-kapacitás

[9] Nyitrai 2016: 80–81.
[10] Siposné 2019: 32–33.
[11] Szászi 2015: 221–223.

lehetővé teszi, hogy a repülőgépek kiválóan teljesítsenek a levegő-levegő utántöltési feladatokban anélkül, hogy további üzemanyagtartályokra lenne szükség. Ezenkívül körülbelül 2200 liter/perc maximális üzemanyag-áramlási sebességet tud biztosítani egy gém vagy egy tömlő és szívócső segítségével, és gyorsan meg tudja tölteni az összes, az MMF-országokban készleten lévő és a legtöbb NATO-n belül használt repülőgépet (F–16, F–35, C–17, Eurofighter, Tornado és Gripen).[12]

Az MRTT-flotta a NATO egyik jól látható projektje, amelynek célja a felszerelések, a képzés, a doktrínák és az eljárások egységességének kiaknázása a méretgazdaságosság és az interoperabilitás biztosítása érdekében. A flotta a NATO tulajdonában van, és a NATO Támogatási és Beszerzési Ügynöksége (NSPA) irányítja. Az NSPA MMF csapata az NSPA központjában található, Capellenben, Luxembourgban, de mások más helyekről is nyújtanak támogatást, például Eindhovenből, Köln-Wahnból, Bonnból és Getaféből. Az NSPA ezt a támogatást a részt vevő országoknak a Multinacionális Többfeladatú Tanker Szállítási Flottatámogató Partnerségen keresztül biztosítja.

A flottát a részt vevő országok katonáiból álló Multinacionális Többcélú Tanker Transport Unit (MMU) üzemelteti. Az egység székhelye a hollandiai Eindhovenben található Fő Operatív Bázison (MOB) és Kölnben, a Forward Operating Base-en (FOB) található.[13]

1. táblázat: A NATO légi szállítási képességek repülőgépeinek összehasonlítása

NATO légi szállítási képesség	**SAC**	**MRTT**	**SALIS**
Repülőgéptípus	Boeing Globemaster III C–17	Airbus A330–200	Antonov An–124–100
Hosszúság	53,04 m	59 m	68,96 m
Szárnyfesztávolság	51,74 m	62 m	73,3 m
Magasság	16,79 m	16,8 m	21,08 m
Maximális felszálló tömeg	265 352 kg	242 000 kg	405 000 kg
Teherszállítási/utaskapacitás	77 500 kg – 170 000 kg	253–277 utas	150 000 kg
Maximális sebesség	830 km/h	913 km/h	850 km/h

Forrás: a szerzők szerkesztése

A kiberbiztonság jelentősége és kihívásai a polgári és katonai légi szállítási műveletekben

A polgári légi közlekedési szektor elleni támadás az előző fejezetben is részletezett NATO katonai képességekre is hatással lesz, ezért átfogó választ igényel. A polgári és katonai légi közlekedési rendszerek kölcsönös függősége miatt a kibertámadás ellen egyik sem védekezhet elszigetelten. Az új fejlett technológiák és kommunikációs rendszerek fejlődésével a kézi folyamatok helyett a hatékonyabb automatizált

[12] NATO 2022: 1–2.
[13] Oppelaar 2023: 25–31.

folyamatok, kommunikáció és tárolás irányvonal a meghatározó. Ezek a technológiai fejlesztések növelik a légi forgalmi irányító rendszer kapacitását és javítják a biztonságot. A következő polgári képességek azonban szintén jelentős kibervédelmi aggályokat vetnek fel, és ha összekapcsolódnak, hatással lesznek a NATO műveleti képességeire.

A mai digitális korban a katonai műveletek nagymértékben támaszkodnak fejlett technológiákra és hálózati rendszerekre. Az előző fejezetben említett katonai légi szállítási képességek döntő szerepet játszanak a globális mobilitásban és az erőkivetítésben, lehetővé téve a személyzet, a felszerelés és a készletek gyors mozgását. Ahogy a katonai légi szállítási képességek technológiailag fejlettebbé válnak, a kiberfenyegetésekkel szemben is sebezhetőbbek. A fejlődő kiberfenyegetettségi környezet jelentős kockázatokat hordoz a katonai légi szállítási képességekre nézve. Látható tehát, hogy a kockázatkezelés egyre inkább tudományos alapokra helyeződve nyújt segítséget, különösen az informatikai rendszerek,[14] ezáltal a légi szállítási képességek sebezhetőségének kezelése terén. Az ellenfelek, az államilag támogatott szereplőktől a hacktivistákig, igyekeznek kihasználni a hálózati rendszerekben rejlő sebezhetőségeket. A katonai légi szállítási képességek elleni sikeres kibertámadásnak messzemenő következményei lehetnek, beleértve a stratégiai szállítási műveletek megzavarását, az érzékeny információk ellopását, a küldetéstervezési rendszerek kompromittálását vagy a repülőgépek repülési irányításának szabotálását. Ezért a robusztus kibervédelem fenntartása elengedhetetlen a katonai légi szállítási műveletek biztonságának és ellenálló képességének biztosításához. A jelenlegi konfliktusok és jövőbeli válságok valószínűleg tartalmaznak kiberelemeket. A NATO műveletei nagymértékben támaszkodnak a számítógépes hálózatokra, ezért a kibertér figyelembevétele a biztonság kiépítése és fenntartása során alapvető követelmény. A kibertér saját területként való elismerésének következményei a Szövetség fókuszát az „információbiztosítás" helyett a „küldetésbiztosítás" felé helyezték át. A kibervédelmet túl gyakran a biztonság és a hadviselés önálló megközelítéseként értelmezik. Az ukrán válság megmutatta, hogy a kibervédelmet átfogóbb stratégiai és operatív koncepcióba kell integrálni.[15]

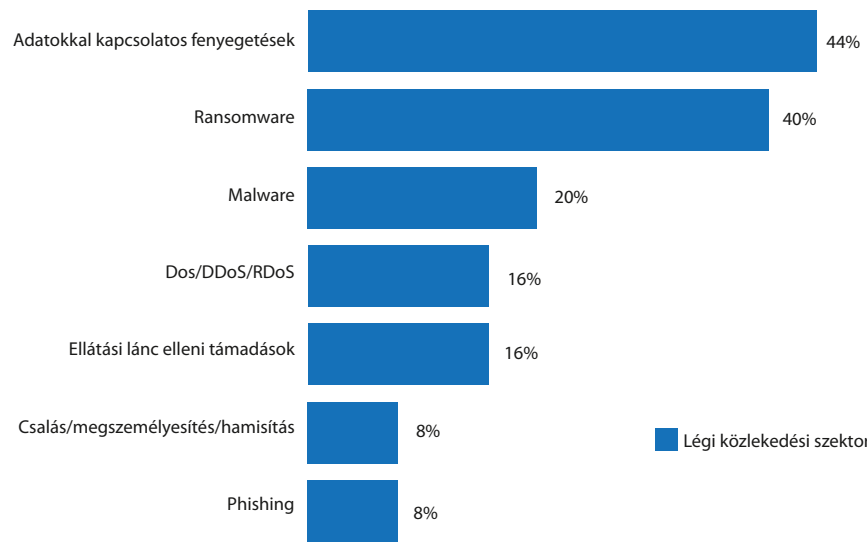
Polgári légi közlekedési kibertámadások kronológiája a NATO katonai légi szállítás potenciális kiberfenyegetései tükrében

A nemzeti légi közlekedési rendszerek kiberfenyegetésekkel szembeni védelme az állam előjoga és felelőssége. Nemzetközi dimenziója azonban megköveteli olyan iránymutatások és eljárások kidolgozását és végrehajtását, amelyek elősegíthetik a globális légi közlekedési rendszer zökkenőmentes rugalmasságát. A globális légi közlekedési rendszer az információs és kommunikációs technológia egyik legösszetettebb és legintegráltabb rendszere a világon. Kritikus infrastruktúraként potenciális kibertámadási célpont. A repülést fenyegető kiberalapú fenyegetések fejlődnek, és számuk növekszik, és ezek a fenyegetések számos forrásból származhatnak, beleértve a bűnözői és terrorista csoportokat, külföldi nemzeteket, bennfenteseket és másokat. Meg kell

[14] Megyeri–Farkas 2017.
[15] Bhargava 2024: 90–93.

érteni, hogy az információs rendszerek közötti növekvő összekapcsolhatóság egyre nagyobb lehetőségeket kínál a kibertámadások számára. Azt is meg kell jegyezni, hogy a polgári és katonai repülés felhasználói és érdekelt felei közötti kölcsönös függőségek növelik a köztük lévő bizalom szükségességét, mivel a légi forgalmi irányítási rendszer képessége a kibertámadások elleni védekezésre csak annyira jó, mint a leggyengébb láncszem a légi közlekedésben. A légi forgalmi irányítási rendszer elleni esetleges kibertámadás nemcsak a polgári és katonai repülések biztonságos lebonyolítását és irányítását akadályozná, hanem alááshatja a Szövetség és tagállamai általános biztonsági és ellenálló képességébe vetett bizalmat is.[16]

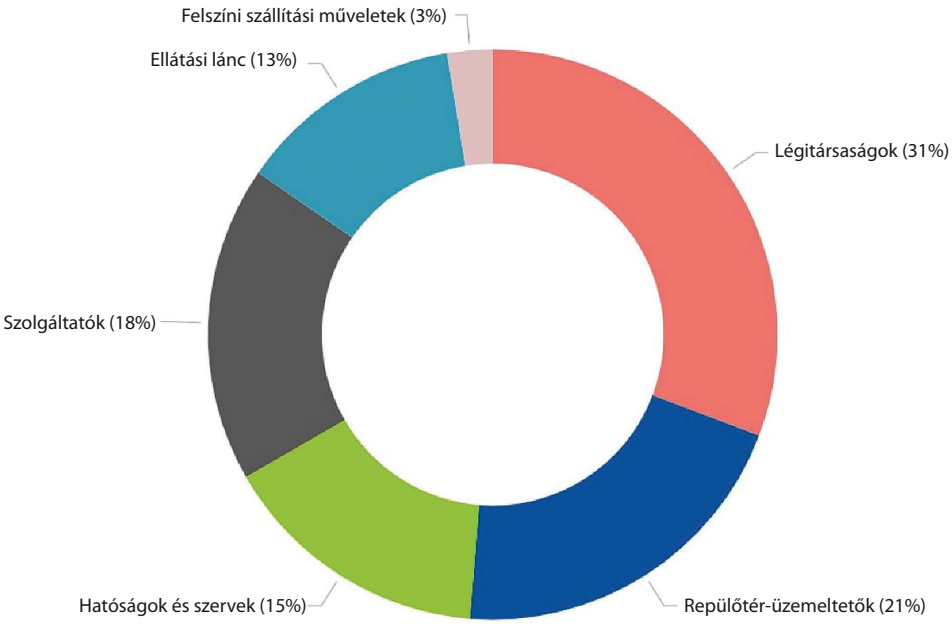
Az ENISA és az Eurocontrol adatai szerint a légtérhasználók/légitársaságok a támadások elsődleges célpontjai. Az ENISA és az EU repülésbiztonsági ügynöksége által az OSINT-en keresztül gyűjtött adatok szerint a légi közlekedési ágazat legfőbb kiberfenyegetéseit az adatokkal kapcsolatos fenyegetések (45%), a ransomware (36%) és a rosszindulatú programok (23%) jelentik. A légi közlekedési szektorban előforduló zsarolóprogram-esetek többségében a támadást adatokkal kapcsolatos fenyegetések követik, mint például az adatok kiszűrése és kiszivárogtatása, így ebben a két kategóriában jelentős az átfedés.[17]



1. ábra: Légi közlekedés elsődleges kiberfenyegetései 2022
Forrás: Theocharidou et al. 2022

Az Eurocontrol jelentése szerint 2022 januárja és júniusa között a legfontosabb célpontok a légtérhasználók, a repülőterek, az eredeti gyártók/ellátási lánc, a légi navigációs szolgáltatók és a polgári légi közlekedési hatóságok.[18]

[16] Elochukwu 2022: 3–5.
[17] Theocharidou 2022: 27–29.
[18] Illing–Dawn 2023.



2. ábra: Az ENISA fenyegetési tájképe: Légi közlekedési kibertámadási célpontok ágazati jelentés
Forrás: Theocharidou et al. 2022

A 2. és 3. táblázat a releváns polgári légi közlekedési iparhoz köthető kibertámadásokat mutatja be,[19] amelyek a NATO katonai légi szállítási képességek eszközparkját figyelembe véve szoros kapcsolatban állnak a NATO katonai légi szállítás potenciális kiberfenyegetéseivel.

2. táblázat: Boeing-kibertámadások kronológiája

Boeinggel kapcsolatos kibertámadások	
Időpont	**Leírás**
2018	A Boeing céget 2018 márciusában sújtotta WannaCry vírus általi informatikai támadás. A Microsoft Windows XP szoftverének sebezhetőségeit kihasználva a WannaCry néven ismert kibertámadás globális szinten jelentős zavarokat okozott. Számos számítógépet támadott meg. Célja az volt, hogy megakadályozza a felhasználók számára az adatok elérését, amíg nem teljesítik a váltságdíjat, gyakran kriptovalutában (Gates 2018).

[19] Hunorfi–Paráda–Farkas 2024.

Boeinggel kapcsolatos kibertámadások	
Időpont	**Leírás**
2019	2019-ben egy spamkampány a Boeing 737 Max legfrissebb balesetét aknázta ki a kártékony szoftverek ellen. A 360 Threat Intelligence Center szakértői egy spamkampányt észleltek, amely arra törekedett, hogy kihasználja a Boeing 737 Max két balesetét. A kampány mögött kétes szereplők „info@isgec[.]com" fiókkal küldtek e-maileket, amelyek témája „Fwd: Airlines plane crash Boeing 737 Max 8". A leveleket állítólag egy „Joshua Berlinger" nevű magánnyomozó küldte, és arra próbálták ösztönözni a címzettet, hogy nyissa meg a mellékelt JAR-fájlt. A kutatók felfedezték, hogy ennek a kampánynak az a célja, hogy a „H-WORM" Remote Access Trojan (RAT) vírust egy káros JAR-fájl mellékletén keresztül juttassa el a címzett számítógépére (Anomali Threat Research 2019).
2021	A 2020 végén kirobbant SolarWinds-kibertámadás hatással volt a Boeingra is. A támadók az IT-szolgáltató, a SolarWinds szoftverfrissítéseit manipulálták, hogy hozzáférjenek a cégek rendszereihez. Az ilyen típusú támadás során a Boeing, mint a legnagyobb felhasználó, veszélybe került (Robin 2023).
2022	2022. november 2-án több Jeppesen-szolgáltatás is leállásra kényszerült. A Jeppesen a Boeing teljes tulajdonában áll, élen jár a légi navigációs szolgáltatások terén. Navigációs adatbázisokat, repüléstervezési alkalmazásokat kínál EFB-khez, valamint portfóliójába tartozik a NOTAM-kezelés is (Thurber 2022; Klint 2022; Britton 2022).
2023	2023. október 27-én a Boeing neve feltűnt a LockBit weboldalán, ahol november 2-ig adtak határidőt a cégnek a kapcsolatfelvételre és a tárgyalások megindítására, hogy elkerüljék a nyilvánosságra kerülő adatokat, amelyek súlyos károkat okozhatnak. A csoportnak jelentős mennyiségű érzékeny adatot sikerült megszereznie. Rövid időre a Boeing lekerült a LockBit áldozatai közül, de november 7-én újra felbukkant, amikor a csoport jelezte, hogy a cég figyelmen kívül hagyta figyelmeztetéseiket. November 10-én a LockBit közzétette weboldalán az összes olyan adatot, amely a Boeingtól származik, köztük IT-menedzsmentszoftverek biztonsági mentései és monitoring-, valamint auditeszközök naplói. Egy hackercsoport körülbelül 50 GB nyers adatot szivárogtatott ki a Boeingtől, miután az nem volt hajlandó kifizetni. A szivárgás során talált Citrix eszközök biztonsági másolatai arra utalnak, hogy a LockBit kihasználhatta a Citrix Bleed sebezhetőséget (CVE-2023-4966), ennek bizonyítékát október 24-én fedezték fel (Ilascu 2023; Raj 2023).

Forrás: a szerzők szerkesztése

3. táblázat: Airbus-kibertámadások kronológiája

Airbusszal kapcsolatos kibertámadások	
Időpont	**Leírás**
2019	Az Airbus 2019-ben bejelentette, hogy egy „adatvédelmi incidens" történt, amely során támadók hozzáfértek egyes rendszereihez, és nem hivatalos hozzáférést szereztek érzékeny információkhoz (Duvelleroy 2019).
2023	2023-ban az Airbus adatszivárgást vizsgált, amely állítólag több ezer beszállítót érint. A kiberbiztonsági incidens vizsgálata azért volt szükségszerű, mert a hírek szerint egy hacker a cég 3200 szállítójáról tett közzé információkat a sötét weben. Egy „USDoD" becenevet használó fenyegetőző a BreachForums-on közzétette, hogy hozzáférést kapott egy Airbus internetes portálhoz, miután feltörték egy török légitársaság alkalmazottjának fiókját. A Hudson Rock jelentése szerint a hacker azt állította, hogy több ezer Airbus-eladóról rendelkezik adatokkal, köztük nevekkel, címekkel, telefonszámokkal és e-mail-címekkel (Antoniuk 2023).

Forrás: a szerzők szerkesztése

Következtetésként megállapítjuk, hogy mivel a NATO katonai légi szállítási képességek eszközparkját az adott polgári légi közlekedési ipari szereplők biztosítják, nagymértékben fennáll a lehetősége, hogy esetenként (minden technikai körülmény és paraméter együtt állásának teljesülése során) a kibertámadások és fenyegetések befolyásolják a NATO katonai légi szállítási képességeinek műveleteit.

A NATO légi közlekedési képességei és rendszerei kibertéri eszközeinek csoportosítása és kibertámadásokkal szembeni hatékony védelmének módja

A 2023-as vilniusi NATO-csúcstalálkozón a szövetségesek új koncepciót hagytak jóvá a kibervédelemnek a NATO általános elrettentő képességéhez és védelmi helyzetéhez való hozzájárulásának fokozására. A vilniusi csúcstalálkozón a szövetségesek megismételték és megerősítették a kibervédelmi ígéretet, és ambiciózusabb célok mellett kötelezték el magukat a nemzeti kibervédelem prioritásként való megerősítésére, beleértve a kritikus infrastruktúrákat is.[20] A 2024-es washingtoni NATO-csúcstalálkozón a szövetségesek megállapodtak abban, hogy létrehozzák a NATO Integrált Kibervédelmi Központot a hálózatvédelem, a helyzetfelismerés és a kibertér mint műveleti terület megvalósítása érdekében.[21]

A csúcstalálkozón elfogadott kibervédelmi intézkedések felismerték, hogy a manapság használt fegyverek és küldetésrendszerek többségét az internet előtti világra tervezték. Az implicit feltételezés az volt, hogy rendszereink alapvetően megengedő kibertérkörnyezetben működnek. Sok rendszerünket évtizedekkel ezelőtt tervezték, és egyáltalán nem meglepő, hogy senki sem tudta megjósolni a kibertértartomány robbanásszerű növekedését és jelentőségét. Amikor a rendszertervezők a fegyverrendszerek információbiztonságának valamilyen formáját fontolgatták, a mérnökök általában azt feltételezték, hogy a határhálózat védelme távol tartja az ellenfeleket, így a fegyverrendszer által látott környezet továbbra is megengedő és védett lesz a hálózati védelemben. Ezek az implicit feltételezések hamisnak bizonyultak. A NATO légi közlekedési képességei és rendszerei már nem biztonságosak, mivel a kibertámadások üteme naponta növekszik a katonai, kormányzati és polgári szektorban.[22]

Mivel minden modern fegyverrendszer (például a NATO légi korai figyelmeztető és szövetségi földi megfigyelőrendszerei, valamint a továbbfejlesztett légi és földi örökölt rendszerek) egyszerre létezik mind a fizikai (légi, szárazföldi és tengeri), mind a kibertér területén, a kibertámadások közvetlenül érintik a hadviselési rendszereket. Számos hozzáférési pont létezik, amelyeken keresztül az ellenfelek megtámadhatják ezeket a rendszereket a kibertéren keresztül. Bármilyen fizikai kapcsolat, amely adatokat továbbít, vagy bármilyen antenna, amely integrált processzorral rendelkezik, potenciális út a támadó számára. Nyilvánvaló példák közé tartoznak a karbantartási és logisztikai rendszerek, a rádiók és az adatkapcsolatok, valamint más rendszerek,

[20] NATO 2023.
[21] NATO 2024b.
[22] Kalivoda–DeFazio 2017.

amelyek összekötik a kezelőket és a platformokat (például repülőgépek vagy fegyverek). Természetesen ezek a dolgok még bonyolultabbak, hiszen ezek a sérülékenységek nem statikusak, hanem folyamatosan változnak. Minden szoftverfrissítés, minden új képesség és minden új berendezés új sebezhetőséget jelenthet. A bonyolultság további növelése érdekében számos kritikus küldetésfüggőség a katonai befolyáson kívül esik, amelyek a kereskedelmi rendszerekkel kapcsolatosak. Mivel a sérülékenységek skálája rendkívül széles, először is meg kell határoznunk, mi a legfontosabb.

Mielőtt meghatározzuk, hogyan kell a NATO-nak megvédenie légi közlekedési képességeit és rendszereit, a kibertéri eszközöket a következő három nagy területre kategorizáltuk:

- Hagyományos IT: magában foglalja az IP-alapú hálózatokat, beleértve a NATO kombinált légi műveleti központjait és egyéb személyzeti és logisztikai rendszereket. Ezek főleg irodai és adminisztratív célú rendszerek IT-támogatását foglalják magukba, amelyek közvetetten kapcsolódnak a NATO kombinált katonai légi műveleteihez, vagy általánosságban bármilyen katonai művelethez.
- Működési technológia OT: számítógéppel vezérelt fizikai folyamatok vagy más típusú vezérlőrendszerek, valamint IP-alapú specifikus szoftverek vagy hálózati rendszerek. Ezek főként a katonai műveleti célú rendszerek üzemeltetését, IT-támogatását foglalják magukba, amelyek az előző kategóriához képest már közvetlenül kapcsolódnak a katonai műveletek végrehajtásához, azok speciális leszűkült tartományi értelmezéséhez, valamint azok sikeres végrehajtásához.
- Platformok: tartalmazza a repülőgépeket, hajókat, tankokat és minden más fegyverrendszert, amelyet a Szövetség és tagjai üzemeltetnek.

Míg a kibervédelmi szakértők jól ismerik a hagyományos IT-rendszerek védelmét, és kezdenek az OT védelmére összpontosítani, a platformok védelmével kapcsolatos munkát még vizsgálni kell. Ezt szem előtt tartva, a NATO légi közlekedési képességei és rendszerei kibertámadásokkal szembeni hatékony védelmének legjobb módja a mélyreható védelem, az ellenálló képesség és a fejlett védelmi intézkedések kombinációja. Mindegyik megközelítés szükséges, és egyik sem elegendő önmagában. Ezért a NATO-nak és tagjainak a maximális hatékonyság érdekében össze kell kapcsolniuk ezeket egy koherens egésszé.[23]

- A mélyreható védelem számos IT-rendszerrel kapcsolatos megoldást jelent, amelyeken az ellenfélnek át kell jutnia, ez biztosítja a kezdeti védelmet, és blokkolja a legtöbb kevésbé kifinomult támadást. A jó mélyreható védekezésnek több összetevője van. Az első egy határvédelem, amely távol tartja a képzetlen támadók alacsony szintű támadásait. A jó védelem számos konfigurált határolással rendelkezik, hogy megakadályozza az oldalirányú mozgást, a privilégiumok fokozódását és az érzékeny adatok kiszűrését. A sebezhetőségkezelés a vállalatokon belül is része a mélyreható védelemnek, és a védőknek nemcsak a sebezhetőségeket kell kizárniuk, hanem le kell állítaniuk a szükségtelen folyamatokat és alkalmazásokat is, hogy megszüntessék a támadási felület nagy részét. Ennek megvalósításához hatékony és biztonságos rendszertervezésre

[23] Bryant 2016: 10–13.

van szükség, amely figyelembe veszi a kibervédelmi szempontokat a tervezési folyamat során.

- Az ellenálló képesség megakadályozza, hogy az ellenfelek elérjék céljaikat, amikor megtámadják a NATO és a tagállamok rendszereit. A NATO és tagállamai légi közlekedési rendszereinek védelmében az ellenálló képességhez flexibilitásra, a támadási felületek csökkentésére és a kibertámadásokra való dinamikus reagálásra lesz szükség. A rugalmas globális légi közlekedési rendszerhez többletkapacitásra lesz szükség a flexibilitásból következő redundanciák biztosításához. Ezenkívül heterogén rendszernek kell lennie, védhető területekre bontva. Ahhoz, hogy dinamikusan reagálhassanak a kibertámadásokra, a globális légi közlekedési rendszer védelmezőinek jobb helyzetfelismerést kell kialakítaniuk saját hálózatukkal kapcsolatban, és fejleszteniük kell hírszerzési képességeiket, hogy megértsék, mit terveznek a potenciális ellenfelek.
- A fejlett védelmi intézkedések az ellenfelek megtalálásával és legyőzésével megnehezítik a támadó számára, hogy elég sokáig a rendszerben maradjon és ezáltal károkat okozzon. Fontos megjegyezni, hogy ezek nem mindig jelentenek valós idejű megfigyelést és manőverezést, hanem időszakos ellenőrzésekre is támaszkodhatnak bizonyos típusú rendszerek esetében, ahol a valós idejű megfigyelés nem praktikus vagy nem követelmény. A fejlett védelmi intézkedések három összetevőből állnak: manőverező erők, érzékelők és eszközök. A manőverező erők az aktív védelem sikeres végrehajtásához szükséges képzett személyzet. Nemcsak a hagyományos informatikai rendszereket kell érteniük, hanem ismerniük kell az OT- és platformrendszereket is. Ennek a manőverező erőnek a fejlesztésére szükség van, de el kell látni őket a rejtett kibertámadók megtalálásához szükséges érzékelőkkel is. Ezeknek az érzékelőknek túl kell lépniük a szabványos behatolásérzékelő rendszereken. Amint egy támadást észlelnek, a manőverező erőknek szükségük lesz a megfelelő eszközökre, hogy képesek legyenek legyőzni a betolakodót.

Végül figyelembe kell venni a repülésbiztonságot és azokat a folyamatokat, amelyek biztosítják a repüléstechnikai termékek, alkatrészek és berendezések légi alkalmasságát. A fent felsorolt katonai és polgári rendszerekhez hasonlóan a légi alkalmassági bizonyítványokhoz használt berendezéseket is kibertámadások érik. Ezért az ebben a dokumentumban javasolt kibervédelmi intézkedéseknek a légi alkalmassági folyamatokra is vonatkozniuk kell.[24]

Összegzés

A polgári légi közlekedés működési környezetének jelenlegi változásai erősen integrált és kölcsönösen függő számítógépes és digitális hálózatokat eredményeznek mind a repülőgépek fedélzetén, mind a légi forgalmi irányító létesítményekben, ami belső

[24] Bryant 2015: 90.

biztonsági réseket okoz. A NATO-nak ezért meg kell védenie légi közlekedési képességeit és rendszereit a kibertámadásoktól a mélységi védelem, az ellenálló képesség és a fejlett védelmi intézkedések kombinációjával. Továbbá, mivel a polgári légi közlekedési rendszerek elleni támadás a katonai repülést is érinti, átfogó megoldásra van szükség.

Ahogy a NATO az „információbiztosításról" a „küldetésbiztosításra" helyezi a hangsúlyt, tagjainak fontolóra kell venniük kibertéri eszközeik besorolását hagyományos információs technológia, operatív információs technológia vagy platformok kategóriájába, hogy jobban megvédjék őket a kibertámadásoktól, ahogyan azt a jelen dokumentum javasolja.

Jelenleg nincs közös jövőkép, stratégia, cél, szabvány, megvalósítási modell vagy nemzetközi politika, amely meghatározná a légi közlekedés kibervédelmét. A biztonságos légi közlekedési rendszer biztosítása és a fejlődő kiberfenyegetéssel való szembenézés az összes érdekelt fél közös felelőssége, beleértve a kormányokat, a légitársaságokat, a repülőtereket és a gyártókat.

A következő generációs és továbbfejlesztett örökölt rendszerek csak fokozzák a jövőbeli kibervédelmi problémákat, mivel egyre inkább hálózatfüggővé válnak. Ezért kulcsfontosságú lesz, hogy a kibervédelmi tesztelés része legyen a NATO és tagállamai légi alkalmassági tanúsítási folyamatának.

A katonai légi szállítási képességek nélkülözhetetlen szerepet játszanak a globális katonai műveletekben, és ezeknek a képességeknek a kiberfenyegetésekkel szembeni védelme rendkívül fontos. Egy holisztikus kibervédelmi stratégia megvalósításával, amely magában foglalja az átfogó kockázatértékelést, a biztonságos hálózati architektúrát, a biztonságos kommunikációs csatornákat, a hozzáférés-ellenőrzési mechanizmusokat, az incidensreagálási tervezést, a képzési és figyelemfelkeltő programokat, az ellátási lánc biztonsági intézkedéseit, valamint a folyamatos ellenőrzést és auditálást, a katonai erők jobban tudják biztosítani légi szállítási képességeik rugalmasságát és hatékonyságát. Ezeknek a kiberbiztonsági intézkedéseknek a folyamatos adaptálása és fejlesztése elengedhetetlen az újonnan megjelenő kiberfenyegetések leküzdése és az erős védelem fenntartása érdekében a gyorsan változó digitális környezetben.

A polgári és katonai légi közlekedési rendszerek kölcsönös függősége miatt a kibertámadás ellen egyik sem védekezhet elszigetelten. A polgári légi közlekedési szektor elleni támadás a NATO katonai képességeire is hatással lesz, ezért átfogó választ igényel. A polgári képességek szintén jelentős kibervédelmi aggályokat vetnek fel, és ha összekapcsolódnak, hatással lesznek a NATO műveleti képességeire.

A cikk a 2024. október 15-i II. Alverad-Bánki Nemzetközi Kiberbiztonsági Konferencián elhangzott előadás kivonata.

Felhasznált irodalom

Anomali Threat Research (2019): Weekly Threat Briefing: Spam Campaign Uses Recent Boeing 737 Max Crashes to Push Malware. *Anomali,* 2019. március 19. Online: https://www.anomali.com/blog/weekly-threat-briefing-spam-campaign-uses-recent-boeing-737-max-crashes-to-push-malware

ANTONIUK, Daryna (2023): Airbus Investigates Data Leak Allegedly Involving Thousands of Suppliers. *The Record,* 2023. szeptember 12. Online: https://therecord.media/airbus-data-leak-suppliers-breachedforums

BHARGAVA, Amit Kumar (2024): Cybersecurity in Aerospace: A Military Perspective. *Blue Yonder,* 1(1). Online: https://journals.capsindia.org/index.php/byj/article/view/48

BRITTON, Niki (2022): 'Cyber Incident' Affected Flight Planning. Boeing Subsidiary Jeppesen Apparently Targeted. *AOPA,* 2022. november 9. Online: www.aopa.org/news-and-media/all-news/2022/november/09/cyber-incident-affected-flight-planning

BRYANT, William D. (2015): Resiliency in Future Cyber Combat. *Strategic Studies Quarterly,* Winter, 87–107. Online: www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-09_Issue-4/Bryant.pdf

BRYANT, William D. (2016): Mission Assurance through Integrated Cyber Defense. *Air & Space Power Journal,* 30(4), 5–17. Online: www.airuniversity.af.edu/Portals/10/ASPJ_Spanish/Journals/Volume-29_Issue-3/2017_3_04_bryant_s_eng.pdf

DUVELLEROY, Matthieu (2019): Airbus Statement on Cyber Incident. *Airbus,* 2019. január 30. Online: www.airbus.com/en/newsroom/press-releases/2019-01-airbus-statement-on-cyber-incident

GATES, Dominic (2018): Boeing Hit by WannaCry Virus, But Says Sttack Caused Little Damage. *The Seattle Times,* 2018. március 28. Online: www.seattletimes.com/business/boeing-aerospace/boeing-hit-by-wannacry-virus-fears-it-could-cripple-some-jet-production/

HOOD, James D. (2009): *NATO Strategic Airlift: Capability or Continued US Reliance?* Maxwell Air Force Base, Air Command and Staff College Air University. Online: https://apps.dtic.mil/sti/tr/pdf/ADA539589.pdf

HUNORFI, Péter – PARÁDA István – FARKAS Tibor (2024). Kiberbiztonsági kihívások a légi közlekedésben. *Hadmérnök,* 19(1), 101–120. Online: https://doi.org/10.32567/hm.2024.1.6

ILASCU, Ionut (2023): LockBit Ransomware Leaks Gigabytes of Boeing Data. *Bleeping Computer,* 2023. november 12. Online: www.bleepingcomputer.com/news/security/lockbit-ransomware-leaks-gigabytes-of-boeing-data/

ILLING, Dawn (2023): The Cyber Threat Landscape Of The Aviation Sector. *Skyradar,* 2023. március 28. Online: www.skyradar.com/blog/the-cyber-threat-landscape-of-the-aviation-sector

KALIVODA, Michal – DEFAZIO, Alexander (2017): Defending NATO's Aviation Capabilities from Cyber Attack. *JAPCC,* 2017. január. Online: www.japcc.org/articles/defending-natos-aviation-capabilities-from-cyber-attack/

KLINT, Matthew (2022): Breaking: Boeing's Jeppesen Subsidiary Hit with Potential Ransomware Attack. *Live and Let's Fly,* 2022. november 3. Online: https://live-andletsfly.com/boeing-jeppesen-ransomware-attack/

MEGYERI Lajos – FARKAS Tibor (2017): Kockázatkezelés, tudomány vagy kuruzslás? *Hadmérnök,* 12(3), 198–209. Online: https://real.mtak.hu/64731/1/1.Farkas_Hadm%C3%A9rn%C3%B6k2017.pdf

NATO (2022): *Multi Role Tanker Transport Capability (MRTT-C) Factsheet.* Online: www.nato.int/nato_static_fl2014/assets/pdf/2022/9/pdf/2209-factsheet-mrtt.pdf

NATO (2023): *Vilnius Summit Communiqué*. Online: www.nato.int/24cps/ge/natohq/official_texts_217320.htm
NATO (2024a): *Strategic Airlift*. 2024. március 7. Online: www.nato.int/cps/en/natohq/topics_50107.htm
NATO (2024b): *Washington Summit Declaration.* 2024. július 10. Online: www.nato.int/cps/cn/natohq/official_texts_227678.htm
Nyitrai Mihály (2016): Eredmények a szövetséges stratégiai légi és tengeri szállítóképesség erősítése terén. *Hadtudományi Szemle,* 9(2), 73–94. Online: https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/14008
Oppelaar, Isaiah (2023): NATO's Multinational MRTT Unit An Update and Case Study for Future Defence Cooperation. *The Journal of the JAPCC,* 35, 25–31. Online: www.japcc.org/articles/natos-multinational-mrtt-unit/
Raj, Aaron (2023): Boeing Hack: Should the Airline Manufacturer Negotiate with Cybercriminals? *Tech Wire Asia,* 2023. november 6. Online: https://techwireasia.com/2023/11/boeing-hack-should-the-airline-manufacturer-negotiate-with-cybercriminals
Robin, Miriam (2023): Cyber Risk Disclosures in Crosshairs as SEC Charges SolarWinds with Fraud. *Intelligize,* 2023. november 16. Online: www.intelligize.com/cyber-risk-disclosures-in-crosshairs-as-sec-charges-solarwinds-with-fraud/
Siposné Kecskeméthy Klára (2019): A NATO biztonsági beruházási programja Magyarországon. *Honvédségi Szemle,* 147(2), 27–40. Online: https://real.mtak.hu/125189/
Szarvas László (2008): *Stratégiai Légi Szállítási képesség – egy új többnemzeti megoldás*. *Nemzet és Biztonság,* 1, 60–76. Online: www.nemzetesbiztonsag.hu/cikkek/szarvas_laszlo-strategiai_legi_szallitasi_kepesseg___egy_uj_tobbnemzeti_megoldas.pdf
Szászi Gábor (2015): A Magyar Honvédség légiszállító képességének változása napjainkig, a fejlesztés jövőbeni lehetpségei. *Economica,* 8(4/2), 216–227. Online: https://doi.org/10.47282/ECONOMICA/2015/8/4/2/4607
Theocharidou, Marianthi – Stanic, Zoran – Drougkas, Athanasios – De Sousa Figueiredo, Ricardo – Tsekmezoglou, Eleni – Naydenov, Rossen – Lella, Ifigeneia – Malatras, Apostolos szerk. (2022): *ENISA Threat Landscape: Transport Sector.* ENISA. Online: https://doi.org/10.2824/553997
Thurber, Matt (2022): Jeppesen Planning, Chart Products Suffer 'Technical Issues'. *AIN Online,* 2022. november 4. Online: www.ainonline.com/aviation-news/business-aviation/2022-11-04/jeppesen-planning-chart-products-suffer-technical-issues
Ukwandu, Elochukwu – Ben-Farah, Mohamed Amine – Hindy, Hanan – Bures, Miroslav – Atkinson, Robert– Tachtatzis, Christos – Andonovic, Ivan – Bellekens, Xavier (2022): Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends. *Information,* 13(3), 3–5. Online: https://doi.org/10.3390/info13030146

HADMÉRNÖK
VÉDELEMINFORMATIKA
19. évfolyam (2024) 4. szám 183–198.
DOI: 10.32567/hm.2024.4.13

Répás József,[1] Berek László,[2] Bak Gerda,[3]
Oláh Norbert,[4] Ujhegyi Péter[5]

HAIS-Q-tól a SAM-ig, a biztonságtudatosság mérésének modernizációja[6]

From HAIS-Q to SAM: Modernising Security Awareness Measurement

Absztrakt

A kiberbiztonság napjaink egyik legkritikusabb kihívása, amely folyamatos fejlődést és alkalmazkodást követel. A technológia exponenciális fejlődésével párhuzamosan a kibertámadások is egyre kifinomultabbá válnak, fokozva ezzel a veszélyt mind az egyénekre, mind a szervezetekre. Ebben a dinamikusan változó környezetben az információbiztonsági tudatosság kulcsfontosságú, amelynek mérése elengedhetetlen a hatékony védekezési stratégiák kialakításához és a fejlesztendő területek azonosításához.
A biztonságtudatosság mérésére számos eszköz áll rendelkezésre, amelyek közül kiemelkedik a HAIS-Q (Human Aspects of Information Security Questionnaire) modell. Jelen kutatásban egy új elméleti modellt, a SAM (Security Awareness Model) modellt mutatjuk be, amely a HAIS-Q modellre építve, de azt kibővítve és modernizálva közelíti meg a biztonságtudatosság mérését. A SAM hét fő dimenziót vizsgál: autentikáció, internetes szolgáltatások használata, információkezelés, eszközhasználat, incidensmenedzsment, szabályozás és tudatosság.

[1] Gábor Dénes Egyetem, e-mail: repas.jozsef@alverad.hu
[2] Óbudai Egyetem Egyetemi Könyvtár; Óbudai Egyetem Innováció Menedzsment Doktori Iskola, e-mail: berek.laszlo@uni-obuda.hu
[3] Óbudai Egyetem Biztonságtudományi Doktori Iskola, e-mail: bak.gerda@uni-obuda.hu
[4] Debreceni Egyetem Informatikai Kar Adattudomány és Vizualizáció Tanszék, e-mail: olah.norbert@inf.unideb.hu
[5] Óbudai Egyetem Biztonságtudományi Doktori Iskola, e-mail: ujhegyi.peter@uni-obuda.hu
[6] A cikk a TKP2021-NVA-05 számú projekt a Kulturális és Innovációs Minisztérium Nemzeti Kutatási Fejlesztési és Innovációs Alapból nyújtott támogatásával, a TKP 2021 pályázati program finanszírozásában valósult meg.

A SAM-modellre épülő kérdőív 120 kérdést tartalmaz, követve a KAB (Knowledge, Attitude, Behaviour) modellt. Ez a komplex mérőeszköz lehetővé teszi a biztonságtudatosság részletes és sokoldalú felmérését, hozzájárulva ezzel a hatékonyabb kiberbiztonsági stratégiák kialakításához.

Kulcsszavak: Security Awareness Model, kiberbiztonság, adatbiztonság, információbiztonsági tudatosság, kvantitatív mérés

Abstract

Cybersecurity is one of the most critical challenges of our time, requiring continuous evolution and adaptation. As technology evolves exponentially, cyberattacks has become more sophisticated, increasing the threat to individuals and organisations. In this dynamically changing environment, security awareness is crucial, and its measurement is essential to developing effective protection strategies and identifying areas for improvement.
Several tools are available to measure security awareness, most notably the HAISQ (Human Aspects of Information Security Questionnaire) model. The present research proposes a new SAM (Security Awareness Model), which builds on the HAISQ model and significantly extends and modernises its approach to measuring security awareness. The SAM examines seven main dimensions: authentication, use of internet services, information management, use of devices, incident management, regulation and human awareness.
The questionnaire based on the SAM model contains 120 questions, following the KAB (Knowledge, Attitude, Behaviour) model. This complex measurement allows a detailed and multifaceted security awareness assessment, contributing to the development of more effective cybersecurity strategies.

Keywords: Security Awareness Model, cybersecurity, security of data, security awareness, quantitative measurement

Bevezetés

Az infokommunikációs technológiák rohamos fejlődése napjainkban nem csupán a digitális jólét megteremtésével jár együtt, hanem egyúttal a polgári lakosság jólétét, kényelmét is elősegítheti. Az információtechnológia fejlődése az egyértelmű előnyei mellett azonban óriási kockázatot is hordoz, amennyiben nem tudatosan használják, így kiemelt figyelmet kell fordítani a lakosság digitális immunitásának erősítésére. Ahogy a digitális eszközök és rendszerek elterjedésével párhuzamosan növekszik a kibertámadások száma és kifinomultsága, új kihívások jelennek meg az egyének és a szervezetek életében. Számos kiberbűncselekmény által okozott kár mértéke, illetve a fejlődő technológia, a szabályozói oldal reaktív természete és a kiberbűnözők által használt újabbnál újabb megoldások is növelik a téma jelentőségét. Kiemelendő, hogy a kiberbűncselekmények okozta negatív hatások a vállalatok esetében az anyagi károkon túl fogyasztói elpártolást, reputációveszteséget és a versenytársak erősödését

is eredményezheti.[7] Így többek között az információbiztonsági tudatosítás egyre fontosabb feladattá válik hazai és világszinten,[8] és fokozott aktivitást igényel Magyarország állampolgárai és a társadalom különböző szereplői esetében is, annak érdekében, hogy a mindennapok részévé váló digitális eszközök és szolgáltatások biztonságos használata el legyen sajátítva. Sokszor azonban nem elegendő csupán az egyének információbiztonsági tudatosságát növelni, hanem a tudásukat is erősíteni szükséges a témában, illetve akár az információbiztonsági kultúra kialakítására, formálására is szükség lehet.[9] Bár a kutatók és a gyakorlati szakemberek folyamatos erőfeszítéseket tesznek ezen a területen, munkájukból gyakran hiányzik a „biztonságtudatosság" fogalmának egységes meghatározása,[10] illetve a különböző tanulmányok ellentmondásos megközelítést alkalmaznak abban a kérdésben, hogy szükséges-e különbséget tenni például a biztonságtudatosság és a biztonsági képzés között. Az Egyesült Államok Nemzeti Szabványügyi és Technológiai Intézete (NIST) által meghatározott biztonságtudatossági definíció a következőket mondja ki: „A tudatosság nem képzés. A tudatossági tréningek célja, hogy a figyelmet a biztonsági intézkedésekre és alkalmazásukra irányítsa. Emellett cél még, hogy az egyének felismerjék az informatikai biztonsággal kapcsolatos aggályokat, és ennek megfelelően reagáljanak."[11] A NIST SP 800-16 szerint a tudatosság megteremti a munkavállaló érzékenységét a számítógépes rendszerek fenyegetései és sebezhetőségei iránt, valamint annak felismerését, hogy az adatokat, az információkat és az azok feldolgozására szolgáló eszközöket védeni kell.[12] Az információbiztonsági tudatosság programok alapvető értéke, hogy a szervezeti kultúrát befolyásoló attitűdváltozást előidéző szemléletváltás révén megalapozzák a képzést. Jelen cikkünkben az információbiztonsági tudatosságot egy olyan adaptív folyamatként definiáljuk, amely reagál a környezeti és technológiai változásokra. A cél az, hogy növelje az egyének és szervezetek érzékenységét az információbiztonsági kockázatokkal kapcsolatban, miközben figyelembe veszi a folyamatosan változó környezet kihívásait és lehetőségeit. Az információbiztonsági tudatosság magában foglalja a releváns ismeretek, attitűdök, készségek és viselkedésformák folyamatos fejlesztését, lehetővé téve a résztvevők számára, hogy alkalmazkodjanak az új fenyegetésekhez és technológiai megoldásokhoz. Mivel a hagyományos, tisztán technológiai megközelítések már nem elegendők, valamint az információbiztonsági incidensek jelentős része emberi hibára vezethető vissza, egyre nagyobb hangsúlyt kap az emberi tényező szerepe, és a biztonságtudatosság mérése során kiemelt figyelmet kell fordítani az egyénekre.[13] Az emberi tényezők vizsgálata nemcsak a szervezeti biztonság szempontjából kulcsfontosságú, hanem abban is segít, hogy feltárjuk azokat az ok-okozati összefüggéseket, amelyek hozzájárulnak a biztonsági kockázatok kialakulásához. A biztonsági kockázatok beazonosítása és csökkentése rendszeres formális auditok segítségével minimalizálható, azonban ezek gyakran időigényesek

7 Modi et al. 2014; Jeong et al. 2019.
8 ENISA 2019.
9 Safa et al. 2015.
10 Hänsch et al. 2014.
11 Wilson et al. 1998.
12 Wilson et al. 1998.
13 Sangwan 2024; Rohan et al. 2021.

és drágák.[14] Ezenkívül külön figyelmet igényel az etikai és jogi félreértések elkerülése (például a behatolásvizsgálat során okozott kár).[15]

A cikk második fejezetében áttekintjük az elmúlt évek kutatásait, amelyek foglalkoztak a digitális transzformáció sikerességének feltételeivel és az információbiztonság szervezeti aspektusaival. Ezek a vizsgálatok rámutattak, hogy a technológiai fejlesztések mellett legalább olyan fontos a megfelelő szervezeti kultúra és viselkedési minták kialakítása. A harmadik fejezet a SAM elméleti modell bemutatására fókuszál, ismertetve annak alapvető felépítését és relevanciáját. Ezt követően a negyedik fejezet célja az elméleti modell dimenzióinak alátámasztása, amely szakirodalmi hivatkozások és korábbi kutatások eredményei alapján történik meg. Végül az összegzésben összefoglaljuk a főbb megállapításokat, kiemelve a SAM modell jelentőségét, valamint annak lehetséges alkalmazási területeit és jövőbeli kutatási irányait.

Tudományos megközelítés és a kapcsolódó modell

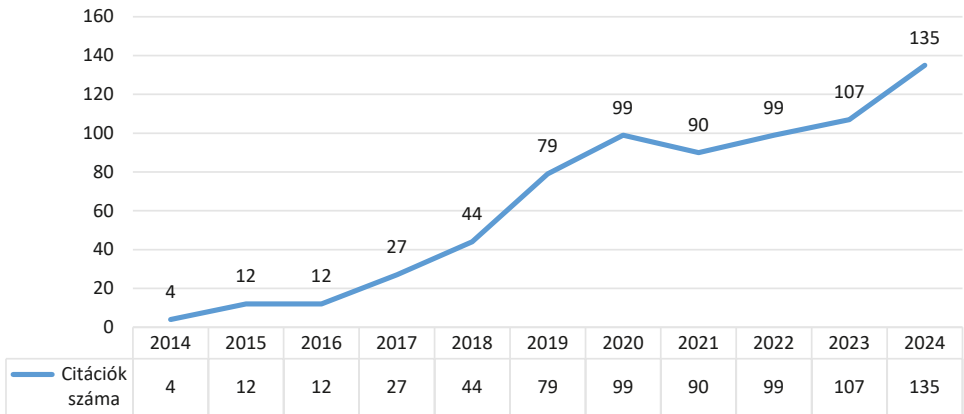
Az információbiztonsági tudatossági szint mérésére kiemelt figyelem irányult mind nemzetközi, mind hazai szinten az elmúlt évtizedekben. A 2010-es évek releváns kutatási eredményeinek szisztematikus áttekintése szerint a kutatócsoport fő iránya a kutatások során alkalmazott felmérések adatgyűjtési és kiértékelési módszerei, a célcsoportok megoszlása, illetve az azonosított biztonságtudatossági paraméterek és a témához kapcsolódó terminológiai változások feltérképezése volt.

A szakirodalmi kutatás során a Web of Science és a Scopus adatbázisokban indexelt, elmúlt 10 évben megjelent releváns publikációk közül a 100 legtöbb citációval rendelkezőt tekintettük át. Ennek során a cím és az absztrakt alapján, majd a teljes szöveg vizsgálatával tudtuk tanulmányozni a korábbi kutatások legfontosabb, témánk szempontjából releváns jellemzőit.[16]

Az adatgyűjtési módszerek vonatkozásában jól látható, hogy a kutatások túlnyomó része kérdőívet használt, a fellelt 37 publikációban mindössze 3 esetben alkalmaztak interjút.[17] Ezek a kutatások mindegyike céges környezetben vizsgálta a biztonságtudatosságot. A mintában szereplő többi, az egyén biztonságtudatosságára vonatkozó felmérés mindegyikében kérdőíves adatgyűjtés szerepelt. A vizsgált publikációkban a legtöbb esetben saját összeállítású, illetve korábbi kutatásokban használt kérdőívek részeiből felépített kérdőíveket alkalmaztak. A publikációk közül 6 esetben találtunk olyan kutatást, amelyben a HAIS-Q (Human Aspects of Information Security Questionnaire) kérdőívet használták.[18] További 4 publikációban hivatkoztak a HAIS-Q-ra. A szakirodalmi mintánkban nevesített kérdőívként egyedül a HAIS-Q szerepelt, és ezekben a kutatásokban egyenlő arányban voltak a kizárólag egyénre vonatkozó, illetve céges környezetben végzett felmérések.

[14] *National Data Guardian for Health and Care: Review of Data Security, Consent and Opt-Outs* 2016.
[15] Yeo 2013.
[16] Bak et al. 2024; Berek et al. 2024.
[17] Ali et al. 2020; Diesch et al. 2020; Kessler et al. 2020.
[18] Parsons et al. 2014; McCormac et al. 2017; Parsons et al. 2017.

Ezt követően a HAIS-Q három „alap" publikációja[19] idézettségének vizsgálata történt meg. A három publikáció citációinak száma a Scopus adatbázisban 734. Természetesen ez csak a Scopus által indexált tartalmakban található idézettséget mutatja, de ebből a kimutatásból jól látható, hogy a publikációk „minőségi szegmensében" a mai napig meghatározó felmérési módszerről beszélünk (1. ábra).



1. ábra: HAIS-Q citációk a Scopus adatbázisban, 2014–2024
Forrás: a szerzők szerkesztése

A három publikáció idézettségének időbeli megoszlásából jól látható, hogy szinte folyamatosan nő a hivatkozások száma. Az is beszédes adat, hogy az összes 734 idézőből 2024 során 135 publikációban hivatkoztak a három folyóiratcikk valamelyikére.

A Web of Science és a Scopus adatai mellett természetesen egy tágabb, nem feltétlen a legmagasabban jegyzett kiadványokban megjelenő publikációkat tartalmazó adatbázisban is lefolytattuk a keresést. A GoogleScholarban bár – adatszinten – szerepelnek azok a publikációk is, amelyeket a két nagy tudományos adatbázis indexel, de ezek mellett alacsonyabban rangsorolt folyóiratok, konferenciaközlemények is megtalálhatók. A GoogleScholar adatai alapján a három HAIS-Q cikk hivatkozásainak száma: 1489. Ezt követően HAIS-Q-ra vonatkozó keresést indítottunk a GoogleScholar felületén, amelynek eredménye 974 olyan publikáció volt, amelyben a „HAIS-Q" kifejezés szerepelt.

Látható, hogy a HAIS-Q széles körben hivatkozott eszköz, amely 7 területen, 63 elemmel vizsgálja a biztonságtudatosság kapcsán a felhasználói viselkedést, tudást és attitűdöt. A HAIS-Q áttekintését követően elmondható, hogy annak kérdései, témái nem feltétlen felelnek meg napjaink kiberbiztonsági kihívásainak, több hiányosságot azonosítottunk.

Ilyen hiányosság például az autentikáció területén az, hogy csak a jelszófaktoron alapuló hitelesítést vizsgálja, amely napjaink biometrikus és kétfaktoros megoldásaiban már kisebb súlyt reprezentál. Ezzel a témával az elmúlt években egyre több kutató

[19] Parsons et al. 2014; McCormac et al. 2017; Parsons et al. 2017.

foglalkozik különböző szempontból vizsgálva a kérdést.[20] Emellett a mesterséges intelligencia dinamikus fejlődése miatt egyre inkább részévé válik mindennapi életünknek, amely területtel értelemszerűen a HAIS-Q 2014-ben még nem foglalkozott. A mesterséges intelligencia az elmúlt években egyértelműen az egyik legforróbb téma volt, természetesen a technológia elfogadottságával, humán vonatkozásaival is sok kutatás foglalkozott.[21] A HAIS-Q kérdőív hiányosságai közé tartozik még a felhőbiztonság az IoT-eszközök szintjén, ami a biztonságtudatosság egyre fontosabb területe.

A kérdőív mindenképpen aktualizálásra, frissítésre szorult, azonban az alkalmazott modell nagyon jól használható a biztonságtudatossággal kapcsolatos felmérés során. A HAIS-Q kérdőív továbbfejlesztése során érdemes figyelembe venni a viselkedésváltozás elméleti megközelítéseit is, hiszen a biztonságtudatosság nem csupán a tudás meglététől, hanem az attitűdök és a viselkedésformák alakulásától is függ. Ebben nyújt hasznos keretet a KAB (Tudás, Attitűd, Viselkedés) modell, amely széles körben alkalmazott elméleti alap a viselkedésváltozás megértésére és előmozdítására. A modell azt hangsúlyozza, hogy a viselkedés megváltoztatásához szükség van a kapcsolódó tudás, attitűdök és készségek együttes fejlesztésére. A tudás magában foglalja a megfelelő információk és készségek elsajátítását, az attitűd a hozzáállás és meggyőződések módosítását, míg a viselkedés a kívánt cselekvések végrehajtására való képességet jelenti. A modell szerint e három tényező összehangolt fejlesztése kulcsfontosságú ahhoz, hogy a célzott viselkedésváltozás hosszú távon fenntartható legyen. A KAB modellt széles körben alkalmazzák az egészségügyi felvilágosítástól a szervezeti fejlesztésekig, mivel átfogó keretet nyújt a komplex emberi viselkedés megértéséhez és befolyásolásához.

A KAB modell szakirodalmi vizsgálata azt mutatja, hogy a modell alkalmazhatósága, megfelelősége szempontjából a kutatók eltérően értékelik: Hermawan et al. (2022) és An et al. (2022) szerint a tudás és viselkedés erősen kapcsolódik egymáshoz.[22] Egyes kutatások élesen bírálták a modellt, mert az az érzelmi és szituációs tényezőket nem veszi figyelembe: Kollmuss és Agyeman (2002) és Baranowski et al. (2003) kutatása szerint több olyan viselkedést befolyásoló tényező van, amelyet a KAB modell figyelmen kívül hagy.[23] A modell hatékonyságát csak akkor lehet megbízhatóan értékelni, ha a vizsgált változókat világosan meghatározzák, és azok kapcsolata a viselkedésváltozás folyamatával összefüggésbe állítható. A releváns eredmények elérése érdekében a modell használatakor figyelembe kell venni a viselkedést befolyásoló összetett tényezőket.

Modell

Az előző fejezetben áttekintett szakirodalom és az általa bemutatott empirikus kutatások feltárt összefüggései alkotják annak az elméleti modellnek az alapját, amely

[20] Srinivasan 2023; Mujeye 2021; Gokulkumari 2020; Buckley et al. 2019.
[21] Kaya et al. 2024; Stein et al. 2024; Kelly et al. 2023.
[22] Hermawan et al. 2022.
[23] Kollmuss–Agyeman 2002; Baranowski et al. 2003.

lehetővé teszi az információbiztonsági tudatosság komplex vizsgálatát, hidat teremtve a tudományos megállapítások és az aktuális gyakorlati alkalmazások között.

A modell célkitűzése az információbiztonsági tudatosság felmérése, amelynek alapját a KAB modell és a HAIS-Q modernizált dimenziói képezik. Az elméleti modellhez javasolt kérdőív a tudás, attitűd és viselkedés dimenzióinak felmérését valósítja meg, ahol az új állítások figyelembe veszik a legújabb információbiztonsági kihívásokat, például a kibertámadások egyre kifinomultabb fenyegetéseit és a hozzájuk kapcsolódó védelmi kontrollokat. Mivel a korszerűsített kérdőív nemcsak az egyén elméleti tudására fókuszál, hanem részletesen feltárja az attitűdöket, a kockázatészlelést és a tényleges biztonsági magatartásmintákat is, így lehetővé válik egy többdimenziós értékelés, amelynek segítségével azonosíthatók a kitöltő információbiztonsági tudatosságának erősségei és fejlesztendő területei.

Az általunk javasolt Security Awareness Measurement (SAM) az információbiztonsági tudatosság holisztikus mérési módszerére kifejlesztett 120 tételből álló eszköz, amelyet a 2. ábra mutat be. A SAM hét fókuszterületet értékel, nevezetesen a hitelesítési módszereket, az internetes alkalmazásokat és szolgáltatásokat, az információkezelést, az eszközöket, az incidensmenedzsmentet, a szabályozást és a tudatosságot. Egyes fókuszterületek további aldimenziókra oszthatók, amelyek tartalmazzák az új szempontokat (például az új autentikációs megoldásokat). Minden egyes fókuszterület esetén meg vannak adva állítások, ahol egy ilyen állítás a tudás, attitűd és viselkedés hármasát kérdezi le. A kérdőív összesen 40 állítást tartalmaz, így a tudás-, az attitűd- és viselkedéselemek 120 tételt adnak vissza. A SAM kérdőív elérhető az alábbi GitHub-linken.[24]

Az alábbi szakaszban áttekintést nyújtunk először az információbiztonsági kérdőívek evolúciójáról, majd a SAM fejlesztéséről, finomításáról és használatáról, amelyet az 1. és a 2. táblázatban foglalunk össze.

Az információbiztonsági tudatosság mérésére az évek során számos kérdőív készült, amelyek folyamatos fejlődésen mentek keresztül. A korai modellek még az egyéni biztonsági szokásokra fókuszáltak, míg az újabb kérdőívek egyre átfogóbb, strukturáltabb megközelítést alkalmaznak. A kontingenciaelmélet alapelvei a SAM esetében jelennek meg, amely figyelembe veszi a környezeti és technológiai változásokhoz való alkalmazkodás szükségességét.

A táblázatban felsorolt kérdőíveket azért választottuk ki, mert jelentős mérföldköveket jelentenek az információbiztonsági tudatosság kutatásában. A Kruger & Kearney által kidolgozott első modell megteremtette az alapokat, míg a HAIS-Q egy strukturáltabb, tudás–attitűd–viselkedés megközelítést alkalmazott. Az ISCA a szervezeti szintű biztonsági kultúra elemzésére fókuszált, a SeBIS pedig az egyéni biztonsági szokások mérése felé tett fontos lépést. A legújabb SAM modell a kontingenciaelmélet alkalmazásával biztosít egy adaptívabb és szélesebb körű mérési keretet.

[24] Lásd: https://github.com/ONorbert1991/SAM-kerdoiv

1. táblázat: Információbiztonsági tudatosság kérdőívek fejlődése

Kérdőív	Fejlesztés éve	Kulcsterületek	Felépítés	Újítások
Information Security Awareness Questionnaire (Kruger & Kearney)	2006	Politikai megfelelés, jelszókezelés, adathozzáférés, fenyegetések ismerete	Tudás, attitűd és viselkedés szerinti bontás	A biztonságtudatosság háromdimenziós megközelítése
Information Security Culture Assessment (ISCA) (Da Veiga & Eloff)	2010	Szervezeti információbiztonsági kultúra, munkavállalói viselkedés, szabályzatok betartása	Többdimenziós elemzés, szervezeti szintű megközelítés	Az információbiztonság kultúrájának átfogó vizsgálata szervezeti kontextusban
Human Aspects of Information Security Questionnaire (HAIS-Q) (Parsons et al.)	2014	Jelszóhasználat, e-mailek és adathalászat, internetes viselkedés, munkahelyi biztonság, mobilbiztonság	Tudás, attitűd és viselkedés alapú értékelés	Átfogó, strukturált mérési eszköz az egyéni biztonságtudatosságra
Security Behavior Intentions Scale (SeBIS) (Egelman & Peer)	2016	Jelszóbiztonság, szoftverfrissítések, eszközvédelem, biztonságtudatos viselkedés	Önbeszámolós kérdések skálázott válaszokkal	Magánszemélyek biztonsági viselkedési hajlandóságának mérése
Security Awareness Measurement (SAM)	2025	Hitelesítési módszerek, internetes alkalmazások és szolgáltatások, információkezelés, eszközök, incidensmenedzsment, szabályozás, tudatosság	40 állítás, mindegyik tudás, attitűd és viselkedés szerint bontva (összesen 120 tétel)	A kontingenciaelmélet alapján fejlesztett kérdőív, amely figyelembe veszi a technológiai és környezeti változásokat

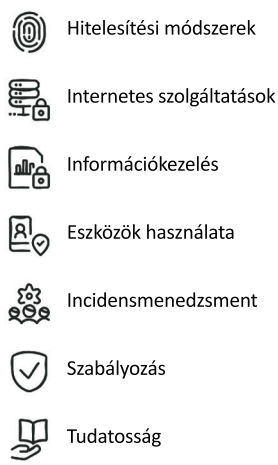
Forrás: a szerzők szerkesztése

2. táblázat: SAM modell fejlesztési lépései

Lépés	Leírás	Eredmény
Tudományos szakirodalom feldolgozása	Átfogó irodalomkutatás az információbiztonsági tudatosság mérésére alkalmazott módszerekről. A meglévő modellek, például a KAB (Knowledge, Attitude, Behaviour) vizsgálata	A mérési keretek, dimenziók és megközelítések azonosítása; a HAIS-Q alapjainak megértése
HAIS-Q modell beazonosítása	A HAIS-Q (Human Aspects of Information Security Questionnaire) vizsgálata és a KAB modellhez való illeszkedésének elemzése	A HAIS-Q hiányosságainak feltárása, például az új technológiákra való korlátozott alkalmazhatóság
HAIS-Q továbbfejlesztése	Az eredeti modell új dimenziókkal és kérdésekkel való kiegészítése. Az új területek közé tartozik a felhőalapú adattárolás biztonsága, a modern autentikációs megoldások és a szabályozási megfelelés	Az új SAM modell létrehozása, amely a HAIS-Q modernizált és bővített változata

Lépés	Leírás	Eredmény
Modernizálás keretének meghatározása	Az információbiztonsági kihívásokra való adaptáció főbb alapelveinek kialakítása, például a dinamikus technológiai változásokra való reagálás szükségessége	Az új kérdőív strukturális alapjai, amelyek igazodnak a mai környezet követelményeihez
Kontingenciaelmélet alkalmazása	A kérdőív alkalmazhatósága a kontingenciaelmélet alapján, amely hangsúlyozza a környezeti és technológiai változásokhoz való alkalmazkodás fontosságát	A kérdőív elméleti alapjainak megerősítése, amely rugalmas keretet biztosít a különböző szervezeti helyzetekhez való igazodáshoz

Forrás: a szerzők szerkesztése



2. ábra: A SAM fő dimenziói
Forrás: a szerzők szerkesztése

Az új területek adaptálását (például modern autentikációs megoldások, webes alkalmazásokkal kapcsolatos biztonsági elemek, tudatosság fejlesztése és kiterjesztése, illetve a napjaink szabályozási kérdésköre) az alábbi szempontok alapján alakítottuk ki.

Jelenleg az emberi tényezőkre jelentős nyomás helyeződik, ugyanis a hatékony információbiztonság nem csupán a technikai eszközökön múlik, hanem a felhasználók tudatosságán, szokásain és viselkedésén is, ami a KAB modellel továbbra is jól leképezhető.

Az autentikációs megoldások között a jelszavak relevanciája és szerepe továbbra is központi jelentőségű, bár a digitális világ egyre fejlettebb hitelesítési módszerei mellett gyakran vitatják hatékonyságukat.[25] A jelszavak napjainkban még mindig a rendszereink alapvető védelmi vonalát képezik, ugyanakkor a kizárólag jelszavakra támaszkodó védelem már nem elegendő a korszerű kiberfenyegetésekkel szemben. A HAIS-Q elsősorban az egyszerű jelszókezelési elvekre összpontosít, de nem veszi figyelembe a napjainkban egyre szélesebb körben alkalmazott többfaktoros hitelesítés (MFA) vagy jelszó nélküli autentikációs megoldások (például biometrikus azonosítás, hardveres

[25] Weber et al. 2008; Taneski et al. 2014; Wang et al. 2023.

tokenek) összetettségét.[26] A modern rendszerek esetében az autentikáció már nem csupán a jelszavak biztonságos megválasztásáról szól, hanem a hitelesítési folyamatok holisztikus megértéséről, valamint a felhasználók képességéről, hogy helyesen alkalmazzák az új technológiákat. Ezért az új megoldások, különösen a többfaktoros hitelesítés (MFA) alkalmazása, a biztonság új alappillérévé vált. Egyes elemzések azt mutatják, hogy a többfaktoros hitelesítés a fiókfeltörési támadások több mint 99,9%-át képes blokkolni.[27] Az MFA nemcsak technikai előnyt kínál, hanem rávilágít a felhasználók és a rendszerek közötti interakciók komplexitására is. Az ilyen megoldások hatékonysága azonban nagyban múlik azon, hogy a felhasználók megértik-e ezek működését, és elkötelezettek-e azok alkalmazása iránt (technológiai elfogadottság).[28]

A HAIS-Q internethasználatának dimenziója mér bizonyos böngészés közben felmerülő fenyegetéseket, azonban ezen a területen elkerülhetetlen, hogy a nyilvánvaló veszélyeken túl (mint az adathalász e-mailek) a preventív és a proaktív védekezési intézkedések is bekerüljenek az információbiztonsági tudatosság mérésébe. Ilyen intézkedések lehetnek a TLS- (Transport Layer Security) protokollt nem használó oldalakkal kapcsolatos óvatos felhasználói magatartás, a rosszindulatú bővítmények vagy a drive-by download támadások kockázatainak minimalizálása, a böngésző naprakészen tartása, a cookie-kezelési szabályok betartása vagy a privát böngészési lehetőségek alkalmazása. A webes biztonság aldimenzió hozzáadása a modellhez és külön vizsgálata kulcsfontosságú, mivel az internetes böngészés és a hozzá kapcsolódó kockázatok alapvető részei manapság a munkahelyi tevékenységeknek. A munkavállalók gyakran látogatnak külső weboldalakat információkeresés vagy üzleti kommunikáció céljából, és ezek az interakciók számos biztonsági fenyegetést hordozhatnak.[29] A kérdőív kapcsolódó állításaival megvizsgáljuk, az egyének képesek-e felismerni a nem biztonságos webhelyeket, tudják-e, milyen lépéseket kell tenniük, ha webes sérülékenységet látnak, és miért fontos a titkosítás az online vásárlások során.

Az internetes alkalmazások, különösen a felhőalapú szolgáltatások és kollaborációs platformok (Google Drive, Microsoft Teams, Slack stb.) használata napjaink egyik releváns kihívása. A digitalizáció rohamos térnyerése és a külső események (például Covid-járvány) tovább erősítették e platformok elterjedését és használatát. A HAIS-Q nem veszi figyelembe azokat a dinamikus és összetett adatmegosztási, jogosultságkezelési vagy incidenskezelési gyakorlatokat, amelyek ezeknél az alkalmazásoknál kiemelkedően fontosak. A felhő után a felhasználók mesterséges intelligencián alapuló alkalmazásokkal és rendszerekkel való kapcsolatát vizsgáljuk, kitérve arra, hogy tudatában vannak-e a potenciális biztonsági kockázatoknak, például az adatfeldolgozási torzításoknak vagy az automatizált döntések manipulálhatóságának. E hiányosságok különösen relevánsak a mai információbiztonsági környezetben, ahol a mesterséges intelligencia és a felhőalapú technológiák széles körben alkalmazott megoldásokká váltak. Az ezekhez kapcsolódó tudatosság hiánya jelentős kockázatok forrása lehet, ezért az új kérdőívbe feltétlenül integrálni kellett ezeket a területeket az elméleti modellben.

[26] Otta et al. 2023; Almadani et al. 2023.
[27] Hess et al. 2021.
[28] Ometov et al. 2018.
[29] Kashevnik et al. 2020.

A szabályozás dimenziójának integrálása az elméleti modellbe a GDPR, NIS2 és más globális adatvédelmi szabályozások megjelenésével áll összefüggésben.[30] Ezek az előírások nemcsak a személyes adatok felelős kezelését, hanem a szervezeti szinten alkalmazott biztonsági gyakorlatok harmonizálását is megkövetelik. Egy információbiztonsági tudatossági kérdőív számára a szabályozások értékelése azért kritikus, mert lehetővé teszi annak vizsgálatát, hogy az egyének és szervezetek mennyire értik és tartják be a vonatkozó jogi előírásokat, például az adattárolási vagy adatfeldolgozási folyamatokra vonatkozó szabályokat. E dimenzió figyelembevétele elősegíti a megfelelési kockázatok csökkentését, miközben megteremti a szabályozás és a gyakorlat közötti harmóniát.[31] A szabályozási ismeretek felmérésével a cél, hogy az elméleti modell a későbbi empirikus vizsgálatokkor megmutassa, hogy a felhasználók mennyire ismerik ezeket az előírásokat, illetve hogyan alkalmazzák őket a mindennapi munkafolyamatok során. Ez nemcsak a jogi megfelelőség biztosítása szempontjából fontos, hanem hozzájárul a szervezet reputációjának és biztonsági színvonalának fenntartásához is. A változó technológiai és a szabályozási környezethez való alkalmazkodás létfontosságú a versenyképesség és a hatékonyság érdekében, amely indokolja az aktuális jogi és üzleti követelményeken túl az általános megfelelőség és harmadik felek menedzselésének szabályozásait is.

A tudatosság dimenzió kiemelt szerepe abban rejlik, hogy a felhasználók biztonsági attitűdje és viselkedése alapvetően befolyásolja a szervezetek kockázatának alakulását.[32] A digitális világ gyors fejlődése megköveteli, hogy az alkalmazottak tisztában legyenek az információbiztonság alapelveivel és azzal, hogyan védekezhetnek a legújabb fenyegetések ellen. A humán faktornak ez a szerepe továbbra is meghatározó az információbiztonság területén, így elengedhetetlen a mérése, valamint a beépítése.[33] A biztonságtudatosságot holisztikus megközelítésben vizsgálva az emberi tűzfal *(human firewall)* fogalma kerül előtérbe. Az Awareness Continuum Management Model (ACM2) alkalmazásával látható, hogyan lehet az alkalmazottak viselkedését proaktívabbá és tudatosabbá tenni, ezzel minimalizálva az emberi hibából eredő kockázatokat.[34] Az elméleti modell kialakítása során ez a dimenzió szolgál arra, hogy a felhasználók mennyire értik a biztonságtudatos magatartás jelentőségét, és milyen mértékben képesek ezt a mindennapi helyzetekben alkalmazni. Az egyének és a szervezetek akkor működnek hatékonyan és megbízhatóan, ha képességeik és erőforrásaik alkalmazkodnak a környezet által támasztott igényekhez. Ennek megfelelően a tudatosság dimenziójának vizsgálata hozzájárul a szervezeti kiberreziliencia növeléséhez, miközben biztosítja, hogy a mérési eszköz a változó fenyegetési környezethez igazodva maradjon releváns.

Az új elméleti modellt lefedő kérdőívstruktúra tehát nemcsak az új technológiákhoz és kihívásokhoz igazodik, hanem figyelembe veszi a modern szervezeti környezetek dinamikáját és a humán tényezők folyamatos változását is. Ez a megközelítés lehetőséget nyújt arra, hogy az információbiztonságot átfogóbb módon mérjük és értékeljük.

[30] Bakare et al. 2024; Reis et al. 2024.
[31] Bamberger et al. 2010.
[32] Rohan et al. 2021.
[33] Sangwan 2024.
[34] Koza 2022.

Eredmények

Szakirodalmi áttekintésünk a mérésre használt módszerek feltérképezésén túl kiterjedt a kapcsolódó kutatások számának alakulására, tudományterületi és országok szerinti megoszlására, valamint a kulcsszavak változására és fejlődésére. Az eredmények alapján egyértelmű, hogy a biztonságtudatosság kutatása egyre fontosabbá válik, a kutatások specializálódnak, és a terület egyértelműen bővülni fog. A vizsgált kutatásokban foglalkoztak az emberi információbiztonsági tudatosság, viselkedés és szabálykövetési hajlandóság közötti összefüggésekkel, valamint a befolyásoló tényezőkkel. A kutatásokban megjelenő tényezőket emberi (ismeretek, tapasztalatok, attitűd, motivációk), környezeti (munkahelyi kultúra, normák, technológia, társadalmi elvárások), technológiai (biztonsági megoldások és eszközök) és oktatási/képzési (képzés, tréning) tényezőkre lehet csoportosítani. A HAIS-Q felmérésén alapuló, kibővített kérdőívünk ezeket a tényezőket figyelembe véve készült el.

A kérdőív bevezetése után a kontingenciaelmélet vált az eszköz működésének és relevanciájának elméleti magyarázatává, amely keretet biztosított a kérdőív alapelveinek és alkalmazkodási képességeinek értelmezéséhez. A kontingenciaelmélet segít megvilágítani, hogy ezek az új dimenziók és változtatások hogyan reflektálnak környezeti feltételekre és az aktuális technológiai elvárásokra.

A kontingenciaelmélet tehát keretet adott az új kérdőív indoklásához, és megmagyarázza, hogy miért van szükség a mérési eszköz folyamatos fejlesztésére és adaptálására. Az elmélet hangsúlyozza, hogy a hatékony mérési eszközöknek illeszkedniük kell a dinamikusan változó technológiai környezethez, és tükrözniük kell a releváns fenyegetéseket és alkalmazási területeket. Az új kérdőív ezen elvárások szerint lett kialakítva, amit a kontingenciaelmélet rendszerbe foglalva megmagyaráz.

Jövőbeli tervek

A SAM kérdőív fejlesztésének következő lépése az elméleti modell empirikus alátámasztása, amely jelenleg a meglévő kulcsszóelemzésre és a szakirodalomban elérhető empirikus adatok statisztikai vizsgálatára épül. A jelenlegi adatelemzés betekintést nyújt az információbiztonsági tudatosság dimenzióiba, azonban ezek megerősítéséhez további nagymintás vizsgálatok szükségesek. Ennek érdekében online kérdőíves felmérést tervezünk, amelyet egy közvélemény-kutató cég bevonásával szeretnénk megvalósítani, biztosítva a reprezentatív minta elérését. Az így gyűjtött adatok lehetővé teszik a SAM modell statisztikai validációját, különös tekintettel a dimenziók közötti összefüggésekre és azok prediktív erejére, megerősítve a kérdőív gyakorlati alkalmazhatóságát.

Összegzés

A kiberbiztonság napjainkban kiemelkedő fontosságú, hiszen nélkülözhetetlen a személyes adatok, üzleti információk és kritikus infrastruktúrák védelméhez, miközben a kibertámadások

egyre gyakoribbá és kifinomultabbá válnak. Ebben a környezetben a biztonságtudatosság segít az embereknek felismerni a potenciális fenyegetéseket és hatékony lépéseket tenni azok megelőzésére. Az egyre digitalizáltabb világban a felhasználók viselkedése és döntései alapvetően befolyásolják a rendszerek és adatok védelmét, ezért elengedhetetlen a tudatosság szintjének mérése. Ezáltal azonosíthatók azok a területek, ahol további képzésre vagy szabályozásra van szükség a kiberbiztonsági kultúra erősítése érdekében. Egy felkészült és tudatos társadalom pedig jelentősen csökkentheti a kibertámadások sikerességét, hozzájárulva a digitális biztonság fenntartásához.

A biztonságtudatosság mérésére számos eszköz létezik, amelyek közül kiválasztottuk a HAIS-Q modellt. Manapság azonban a HAIS-Q-nak számos hiányossága van, ami abból ered, hogy a dimenziói részben elavultak, ideértve az autentikációs megoldásokat, a webes biztonságot és az új internetes alkalmazások kihívásait. Emiatt egy rugalmasabb, környezetérzékeny kérdőívre van szükség, amely az információbiztonsági tudatosságot a jelenlegi technológiai és üzleti realitásokhoz igazítva méri.

Jelen kutatás egy új megközelítést, a SAM elméleti modellt javasolja. Ez a modell a HAIS-Q alapjaira épül, ugyanakkor jelentősen kibővített és modernizált dimenziókat kínál a biztonságtudatosság átfogó értékelésére. A SAM hét fő dimenzióra összpontosít: autentikáció, internetes szolgáltatások használata, információkezelés, eszközhasználat, incidensmenedzsment, szabályozás és tudatosság. A SAM modellhez kapcsolódó kérdőív 120 kérdést tartalmaz, amelyek a KAB (Knowledge, Attitude, Behavior) modellt követik. Ezzel a célunk egy komplex és sokoldalú mérőeszközt javasolni, amely az empirikus adatok beérkezése után lehetővé teszi a biztonságtudatosság mélyreható elemzését, ezzel hozzájárulva hatékonyabb kiberbiztonsági stratégiák kidolgozásához és megvalósításához.

A cikk a 2024. október 15-i II. Alverad-Bánki Nemzetközi Kiberbiztonsági Konferencián elhangzott előadás kivonata.

Felhasznált irodalom

Ali, Omar – Shrestha, Anup – Chatfield, Akemi – Murray, Peter (2020): Assessing Information Security Risks in the Cloud: A Case Study of Australian Local Government Authorities. *Government Information Quarterly,* 37(1). Online: https://doi.org/10.1016/j.giq.2019.101419

Almadani, Mwaheb S. – Alotaibi, Suhair – Alsobhi, Hada – Hussain, Omar K. – Hussain, Farookh K. (2023): Blockchain-Based Multi-Factor Authentication: A Systematic Literature Review. *Internet of Things,* 23. Online: https://doi.org/10.1016/j.iot.2023.100844

Bak, Gerda – Berek, László – Som, Zoltán – Ujhegyi, Péter – Répás, József (2024): On the Way to Updating the Measurement of Information Security Awareness: a Literature Analysis. *Interdisciplinary Description Of Complex Systems,* 22(3), 305–316. Online: https://doi.org/10.7906/indecs.22.3.6

Bakare, Seun S. – Adeniyi, Adekunle O. – Akpuokwe, Chidiogo U. – Eneh, Nkechi E. (2024): Data Privacy Laws and Compliance: A Comparative Review of the

EU GDPR and USA Regulations. *Computer Science & IT Research Journal,* 5(3), 528–543. Online: https://doi.org/10.51594/csitrj.v5i3.859

Bamberger, Kenneth A. (2010): Technologies of Compliance: Risk and Regulation in a Digital Age. *Texas Law Review,* 88(4), 669–739.

Baranowski, Tom – Cullen, Karen W. – Nicklas, Theresa – Thompson, Deborah – Baranowski, Janice (2003): Are Current Health Behavioral Change Models Helpful in Guiding Prevention of Weight Gain Efforts? *Obesity Research,* 11(S10), 23S–43S. Online: https://doi.org/10.1038/oby.2003.222

Berek László – Som Zoltán – Bak Gerda – Ujhegyi Péter – Répás József – Pető Richárd (2024): Az egyén információbiztonsági tudatossági szintjének megállapítására elterjedt mérési módszerek összefoglaló elemzése nemzetközi kutatások alapján. In Molnár György – Temesvári Zsolt – Wührl Tibor (szerk.): *XXXIX. Kandó Konferencia 2023.* Budapest: Óbudai Egyetem, 265–277.

Buckley, Gerard – Caulfield, Tristan – Becker, Ingolf (2024): GDPR and the Indefinable Effectiveness of Privacy Regulators: Can Performance Assessment be Improved? *Journal of Cybersecurity,* 10(1). Online: https://doi.org/10.1093/cybsec/tyae017

Buckley, Oliver – Nurse, Jason R. C. (2019): The Language of Biometrics: Analysing Public Perceptions. *Journal of Information Security and Applications,* 47, 112–119. Online: https://doi.org/10.1016/j.jisa.2019.05.001

Diesch, Rainer – Pfaff, Matthias – Krcmar, Helmut (2020): A Comprehensive Model of Information Security Factors for Decision-Makers. *Computers and Security,* 92. Online: https://doi.org/10.1016/j.cose.2020.101747

Egelman, Serge – Harbach, Marian – Peer, Eyal (2016): *Behavior Ever Follows Intention? A Validation of the Security Behavior Intentions Scale (SeBIS).* Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems, 5257–5261. Online: https://doi.org/10.1145/2858036.2858265

ENISA (2018): Cyberhead – Cybersecurity Higher Education Database. Online: www.enisa.europa.eu/topics/education/cyberhead#/

Gokulkumari, G. (2020): Analytical Outlook on Customer Awareness Towards Biometrics Mechanism of Unimodal and Multimodal in Online Transactions. *Multimedia Tools and Applications,* 79(41–42), 31691–31714. Online: https://doi.org/10.1007/s11042-020-09526-w

Hänsch, Norman – Benenson, Zinaida (2014): *Specifying IT Security Awareness.* 2014 25th International Workshop on Database and Expert Systems Applications (DEXA), 326–330. Online: https://doi.org/10.1109/DEXA.2014.71

Hermawan, Deni S. – Setiadi, Farisya – Oktaria, Dita (2022): *Measurement Level of Information Security Awareness for Employees Using KAB Model with Study Case at XYZ Agency.* 1st International Conference on Software Engineering and Information Technology (ICoSEIT) Bandung, Indonesia, 2022, 174–179. Online: https://doi.org/10.1109/ICoSEIT55604.2022.10029989

Hess, Elie – Tolbert, Matthew – Nascimento, Mattheus (2021): *Vulnerabilities of Multi-factor Authentication in Modern Computer Networks.* Worcester, UK: Worcester Polytechnic Institute.

Kashevnik, Alexey – Lashkov, Igor – Ponomarev, Andrew – Teslya, Nikolay – Gurtov, Andrei (2020): Cloud-Based Driver Monitoring System Using a Smart-

phone. *IEEE Sensors Journal,* 20(12), 6701–6715. Online: https://doi.org/10.1109/JSEN.2020.2975382

Kaya, Feridun – Aydin, Fatih – Schepman, Astrid – Rodway, Paul – Yetişensoy, Okan – Demir Kaya, Meva (2024): The Roles of Personality Traits, AI Anxiety, and Demographic Factors in Attitudes toward Artificial Intelligence. *International Journal of Human-Computer Interaction,* 40(2), 497–514. Online: https://doi.org/10.1080/10447318.2022.2151730

Kelly, Sage – Kaye, Sherrie-Anne – Oviedo-Trespalacios, Oscar (2023): What Factors Contribute to the Acceptance of Artificial Intelligence? A Systematic Review. *Telematics and Informatics,* 77. Online: https://doi.org/10.1016/j.tele.2022.101925

Kessler, Stacey R. – Pindek, Shani – Kleinman, Gary – Andel, Stephanie A. – Spector, Paul E. (2020): Information Security Climate and the Assessment of Information Security Risk Among Healthcare Employees. *Health Informatics Journal,* 26(1), 461–473. Online: https://doi.org/10.1177/1460458219832048

Kollmuss, Anja – Agyeman, Julian (2002): Mind the Gap: Why Do People Act Environmentally and What Are the Barriers to Pro-Environmental Behavior? *Environmental Education Research,* 8(3), 239–260. Online: https://doi.org/10.1080/13504620220145401

Koza, Erfan (2022): Information Security Awareness and Training as a Holistic Key Factor – How Can a Human Firewall Take on a Complementary Role in Information Security? In Ahram, Tareq – Karwowski, Waldemar (szerk.): *Human Factors in Cybersecurity.* New York: AHFE International, 49–57. Online: https://doi.org/10.54941/ahfe1002201

Kruger, H. A. – Kearney, W. D. (2006): A Prototype for Assessing Information Security Awareness. *Computers & Security,* 25(4), 289–296. Online: https://doi.org/10.1016/j.cose.2006.02.008

McCormac, Agata – Zwaans, Tara – Parsons, Kathryn – Calic, Dragana – Butavicius, Marcus – Pattinson, Malcolm (2017): Individual Differences and Information Security Awareness. *Computers in Human Behavior,* 69, 151–156. Online: https://doi.org/10.1016/j.chb.2016.11.065

Mujeye, Stephen (2021): *A Survey on Multi-Factor Authentication Methods for Mobile Devices.* Proceedings of the 2021 4th International Conference on Software Engineering and Information Management, 199–205. Online: https://doi.org/10.1145/3451471.3451503

National Data Guardian (2016): *National Data Guardian for Health and Care: Review of Data Security, Consent and Opt-Outs.* Online: www.gov.uk/government/publications/review-of-data-security-consent-and-opt-outs

Ometov, Aleksandr – Bezzateev, Sergey – Mäkitalo, Niko – Andreev, Sergey – Mikkonen, Tommi – Koucheryavy, Yevgeni (2018): Multi-Factor Authentication: A Survey. *Cryptography,* 2(1), 1. Online: https://doi.org/10.3390/cryptography2010001

Otta, Souma P. – Panda, Subhrakanta – Gupta, Maanak – Hota, Chittaranjan (2023): A Systematic Survey of Multi-Factor Authentication for Cloud Infrastructure. *Future Internet,* 15(4). Online: https://doi.org/10.3390/fi15040146

Parsons, Kathryn – McCormac, Agata – Butavicius, Marcus – Pattinson, Malcolm – Jerram, Cate (2014): Determining Employee Awareness Using the Human

Aspects of Information Security Questionnaire (HAIS-Q). *Computers and Security,* 42, 165–176. Online: https://doi.org/10.1016/j.cose.2013.12.003

Parsons, Kathryn – Calic, Dragana – Pattinson, Malcolm – Butavicius, Marcus – McCormac, Agata – Zwaans, Tara (2017): The Human Aspects of Information Security Questionnaire (HAIS-Q): Two Further Validation Studies. *Computers and Security,* 66, 40–51. Online: https://doi.org/10.1016/j.cose.2017.01.004

Reis, Oluwatosin – Eneh, Nkechi E. – Ehimuan, Benedicta – Anyanwu, Anthony – Olorunsogo, Temidayo – Abrahams, Temitayo O. (2024): Privacy Law Challenges in the Digital Age: A Global Review of Legislation and Enforcement. *International Journal of Applied Research in Social Sciences,* 6(1), 73–88. Online: https://doi.org/10.51594/ijarss.v6i1.733

Rohan, Rohani – Funilkul, Suree – Pal, Debajyoti – Chutimaskul, Wichian (2021): *Understanding of Human Factors in Cybersecurity: A Systematic Literature Review.* 2021 International Conference on Computational Performance Evaluation (ComPE), Shillong, India, 133–140. Online: https://doi.org/10.1109/ComPE53109.2021.9752358

Safa, Nader S. – Sookhak, Mehdi – Von Solms, Rossouw – Furnell, Steven – Ghani, Norjihan A. – Herawan, Tutut (2015): Information Security Conscious Care Behaviour Formation in Organizations. *Computers & Security,* 53, 65–78. Online: https://doi.org/10.1016/j.cose.2015.05.012

Sangwan, Aarti (2024): *Human Factors in Cybersecurity Awareness.* 2024 International Conference on Intelligent Systems for Cybersecurity (ISCS), Gurugram, India, 1–7. Online: https://doi.org/10.1109/ISCS61804.2024.10581139

Srinivasan, Srihari (2023): *Understanding User Perception of Biometric Privacy in the Era of Generative AI.* 4th International Conference on Communication, Computing and Industry 6.0 (C216) 2023, Bangalore, India, 01–06. Online: https://doi.org/10.1109/C2I659362.2023.10430931

Stein, Jan-Philipp – Messingschlager, Tanja – Gnambs, Timo – Hutmacher, Fabian – Appel, Markus (2024): Attitudes Towards AI: Measurement and Associations with Personality. *Scientific Reports,* 14(1). Online: https://doi.org/10.1038/s41598-024-53335-2

Taneski, Viktor – Heričko, Marjan – Brumen, Boštjan (2014): *Password Security – No Change in 35 Years?* 2014 37th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 1360–1365. Online: https://doi.org/10.1109/MIPRO.2014.6859779

Wang, Ding – Shan, Xuan – Dong, Qiying – Shen, Yaosheng – Jia, Chunfu (2023): *No Single Silver Bullet: Measuring the Accuracy of Password Strength Meters.* 32nd USENIX Security Symposium (USENIX Security 23), 947–964.

Weber, James E. – Guster, Dennis – Safonov, Paul – Schmidt, Mark B. (2008): Weak Password Security: An Empirical Study. *Information Security Journal: A Global Perspective,* 17(1), 45–54. Online: https://doi.org/10.1080/10658980701824432

Wilson, Mark – Pitcher, S. I. – Tressler, J. D. – Ippolito, J. B. – de Zafra, D. E. (1998): *Information Technology Security Training Requirements: A Role- and Performance-Based Model.* National Institute of Standards and Technology Special Publication, 800–816. Online: https://doi.org/10.6028/NIST.SP.800-16

Yeo, John (2013): Using Penetration Testing to Enhance Your Company's Security. *Computer Fraud & Security,* (4), 17–20. Online: https://doi.org/10.1016/S1361-3723(13)70039-3

HADMÉRNÖK
VÉDELEMINFORMATIKA
19. évfolyam (2024) 4. szám 199–212.
DOI: 10.32567/hm.2024.4.14

Volarics József[1]

Lehetőségek a robbantással elkövetett terrorcselekmények helyszíni adatainak digitális rögzítésére és értékelésére

Possibilities for Digital Recording and Evaluation of On-Scene Data of a Terrorist Attack by Bombing

Absztrakt

Tanulmányom témája a robbantással elkövetett terrorcselekmények helyszíni adatainak digitális rögzítésére és értékelésére szolgáló eszközök és módszerek, valamint ezek integrált rendszerbe foglalásának lehetőségei.
A bevezető részben a NATO és a kriminológia által alkalmazott definíciók segítségével meghatározom a terrorizmus fogalmának saját szempontrendszerem szerinti lényegi elemeit, illetve röviden bemutatom a fizikai erőszak alkalmazásával elkövetett terrorista támadások során leggyakrabban alkalmazott módszereket. Összefoglalom a robbantással elkövetett terrorcselekmények sajátosságait, az ilyen cselekményeket követő elsődleges feladatokat, a szemle során beszerezhető adatok jelentőségét.
Részleteiben tárgyalom a szemle feladatait az alkalmazott robbanóeszköz vonatkozásában, így hatásának dokumentálása, az abból származó tárgytöredékek, anyagmaradványok összegyűjtése tekintetében. Bemutatom a vizuális adatok digitalizálásának alkalmazási lehetőségeit a helyszíni dokumentáció elkészítése során, kiemelve a 3D-technológiák előnyeit.
A robbanás okozta fizikai elváltozások tekintetében részletesen tárgyalom az épületkárok és a keletkezett kráter digitális értékelésének módszereit. Ismertetem a robbanóeszközből származó tárgytöredékek, illetve a robbanóanyagból származó anyagmaradványok detektálására alkalmas digitális eszközöket.

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola, e-mail: volaricsjozsef@gmail.com

Az összegzésben felvázolom a bemutatott technológiák integrált alkalmazásának lehetőségét, a rendszerként való alkalmazás előnyeit.

Kulcsszavak: terrorcselekmény, robbantás, helyszíni szemle, digitalizáció, 3D, detektálás, integrált rendszer

Abstract

The topic of my study is the equipment and methods for recording and evaluating on-scene data of terrorist attacks committed by improvised explosive devices (IEDs), and the possibilities of including them in an integrated system.
In the introduction, I define the essential elements of the concept of terrorism according to my criteria using the definitions used by NATO and criminology. I briefly present the methods most frequently used in terrorist attacks using physical force. I summarise the characteristics of terrorist attacks committed by IEDs, the primary tasks following perpetration, and the significance of the data that can be obtained during the investigation.
I discuss in detail the investigation tasks from the perspective of the explosive device used, such as documenting its effect and collecting object fragments and material residues. I present the possibilities of digitising visual data while preparing on-scene documentation with the advantages of 3D technology. I discuss in detail the methods of digital evaluation of building damage and the resulting crater about the physical effects caused by the explosion. I will describe the digital devices suitable for detecting the fragments from explosive devices and explosives residues.
In the summary, I will outline the possibility of integrated application of the presented technologies and the advantages of applying them as a system.

Keywords: terrorist attack, bombing, crime scene investigation, digitisation, 3D detection, integrated system

Bevezető

A nemzetközi terrorizmus jelensége komplex módon gyakorol hatást a biztonság szinte valamennyi dimenziójára,[2] meghatározó helyet foglal el az egyes állampolgárok, valamint közösségek biztonságát veszélyeztető,[3] illetve az aszimmetrikus és hibrid hadviseléssel összefüggésben jelentkező fenyegetések körében.[4] Napjaink terrorizmusa rendkívül összetett jelenség, e vonatkozásában az új típusú biztonsági kihívások közé sorolható, ami az érintett szervek részéről összehangolt fellépést igényel. Ez magában foglalja az egyes szervezetek szoros együttműködését, aminek

[2] Közvetlenül érinti a védelmi, politikai és közbiztonságot, de kihat a gazdasági vagy akár a környezetbiztonság területére is.
[3] Mátyás–Sallai 2015: 336.
[4] A napjaink poliarchikus nemzetközi környezetében jellemzők az aszimmetrikus, illetve hibrid konfliktusok. Ezek során az egyik leggyakoribb módszer a terrorista szervezetek támogatása, illetve alkalmazása a szemben álló fél gyengítésére. Hausner 2022: 121–122.

következtében a terrorizmus elleni küzdelem nem tekinthető más katonai vagy rendőri műveletektől elkülönülő területnek.[5]

Rendőri vonatkozásban a terrorelhárítási műveletek alapvető célja a terrorcselekmény megszakítása és felszámolása, a bizonyítási eszközök összegyűjtése, az elkövetők elfogása, valamint bíróság elé állítása.[6] A bűncselekmények helyszínén található bizonyítékok felkutatásának, illetve rögzítésének adekvát módszere a helyszíni szemle, amely során az eljáró bűnügyi technikai szervezeti egységek döntően a műszaki és természettudományok eredményeit (eszközeit, módszereit, eljárásait) alkalmazzák a bűnözés elleni harc céljaira.[7] Fontos körülmény, hogy az alkalmazott eszközök és módszerek kidolgozása és folyamatos fejlesztése is részben a bűnügyi technikai szakterület feladata.

Tanulmányomban a NATO és a kriminológia által alkalmazott definíciók segítségével meghatározom a terrorizmus fogalmának saját szempontrendszerem szerinti lényegi elemeit, illetve röviden bemutatom a fizikai erőszak alkalmazásával elkövetett terrorista támadások során leggyakrabban alkalmazott eszközöket, módszereket. Összefoglalom a robbantással elkövetett terrorcselekmények sajátosságait, az ilyen cselekményeket követő helyszíni szemle feladatait, a szemle során beszerezhető adatok jelentőségét.

Részleteiben tárgyalom a szemle feladatait az alkalmazott robbanóanyagok, illetve robbanóeszközök vonatkozásában, így azok hatásának dokumentálását, az azokból származó tárgytöredékek, anyagmaradványok felkutatását és összegyűjtését. Ismertetem a robbanóeszközökből származó tárgytöredékek, illetve a robbanóanyagból származó anyagmaradványok detektálására alkalmas digitális eszközöket és azok használatát. Bemutatom a vizuális adatok digitalizálásának lehetőségeit a helyszíni dokumentáció elkészítése során, kiemelve a 3D-technológiák alkalmazásának előnyeit. A robbanás okozta fizikai elváltozások tekintetében részletesen tárgyalom az épületkárok és a keletkezett kráterek digitális értékelésének eszközeit, illetve módszereit.

Az összegzésben felvázolom a bemutatott technológiák integrált alkalmazásának lehetőségét, a rendszerként történő alkalmazás előnyeit, alternatívát kínálva a büntetőeljárás szabályainak és a kriminalisztika ajánlásainak maradéktalanul megfelelő, a szükséges technikai eszközparkot, és az ezek működtetéséhez szükséges ismereteket, módszereket felvonultató eljárásrend kidolgozására.

A terrorizmus fogalmi meghatározása

A terrorizmus NATO szerinti definíciója: „Politikai, vallási, vagy ideológiai célkitűzések elérése érdekében kormányok és társadalmak kényszerítésére vagy megfékezésére tett kísérletben, az egyének vagy javak elleni erőszak törvénytelen alkalmazása, illetve azzal való fenyegetés."[8]

[5] Mumford 2016: 12.
[6] Beke 2022: 50.
[7] Illár 1984: 6.
[8] Kis-Benedek 2023.

A terrorizmus kriminológiai fogalma:

„A terrorizmus eltérő eszmerendszerekből merítő, sajátos logikának engedelmeskedő, változatos formákat öltő módszeres erőszak-alkalmazás, vagy ezzel való fenyegetés, melynek célja politikai törekvések elérése azáltal, hogy az áldozatban, a nézőközönségben, az államban, a társadalomban megalkuvó magatartás alakuljon ki. A meghirdetett cél általában politikai, ideológiai, vallási, etnikai stb. tartalmú radikális változás kikényszerítése, a cél elérésére alkalmazott cselekménysor. Az eszköz viszont jogi lényegét tekintve köztörvényes, erőszakos bűncselekmény."[9]

A NATO, illetve a kriminológiai fogalmak közös magatartási eleme az erőszak, vagy az azzal való fenyegetés. A ténylegesen erőszakkal járó támadások során a terroristák különböző módszereket vagy ezek kombinációját alkalmazzák.

A terrorista támadások leggyakoribb módszerei

Guy Fawkes és társai 1605. november 5-én akarták felrobbantani a parlamentet, I. Jakab angol királlyal együtt.[10] A módszer azóta is az egyik leggyakrabban alkalmazottak közé tartozik. A felhasznált anyagok sokfélék lehetnek, katonai és ipari robbanóanyagok, házi készítésű (például műtrágya alapú, vagy triaceton-triperoxid) robbanóanyagok, lőporkeverékek. A pusztító hatás növelésére a különböző improvizált robbanóeszközök (angolul: *improvised explosive device,* IED) repeszképző anyagokat tartalmazhatnak (például szegek, csavarok), illetve a töltet hatásfoka gázpalackokkal, benzinnel teli tárolóedényekkel növelhető. 2005. július 7-én négy öngyilkos merénylő hajtott végre összehangolt támadást Londonban. Három robbantás a metróban történt a reggeli csúcsforgalomban, míg a negyedik egy buszon a délelőtti órákban. A cselekmény 52 ember halálát okozta, a sebesültek száma 770 fő volt.[11]

ABV[12]-anyagokkal elkövetett támadásokra Európában nem került sor. Térségünkben az ABV-támadásokkal való fenyegetés a terrorista propaganda része, azonban a jövőben a terrorcselekmény elkövetésére alkalmas kémiai, biológiai fegyverek, radiológiai diszperziós eszközök kifejlesztése reális kockázatot jelenthet.[13] 1995. március 20-án az *AUM Shinrikyo* terrorista csoport tagjai hajtottak végre szarin alkalmazásával

[9] Gönczöl 2012.
[10] Schvéd 2020.
[11] *London bombings of 2005* [é. n.].
[12] A magyar katonai terminológiában használatos ABV, azaz atom, biológiai és vegyi kifejezéssel szemben a rendőrségi szakzsargonban az angol kémiai, biológiai, radiológiai és nukleáris (chemical, biological, radiological, and nuclear) szavakból származó CBRN rövidítés terjedt el. „A nukleáris terrorizmus egyik fenyegető eszközeként jelölik meg számos kiadványban a radiológiai diszperziós eszközöket (RDE). Az RDE-k alkalmasak akár hagyományos robbanóanyag, akár valamely fizikai hatás energiájának felhasználásával radioaktív anyagokat valamely intermedier közegbe diszpergálva környezetének jelentős sugárszennyezésére. A harctereken is veszélyeztető új elem (a nukleáris fegyverektől eltérő RDE) indukálta az NBC- (ABV-) fogalom újabb bővítését és áttérést a CBRN-weapons megnevezés használatára." Krajnc 2019: 8–9.
[13] A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának. Cselekvési terv a vegyi, biológiai, radiológiai és nukleáris biztonsági kockázatokkal szembeni felkészültség fokozásáról. 2017: 2

összehangolt támadást a tokiói metróhálózat öt vonalán. A támadásnak 19 halálos áldozata és több mint 5000 sérültje volt.[14]

A terrorcselekmények végrehajtása lőfegyverek alkalmazásával az elkövetők szempontjából tekintve az egyik leghatékonyabb módszer. Sorozatlövő kézifegyverekkel (például gépkarabélyokkal) felszerelt néhány fős csoport által egy tömegrendezvényen végrehajtott támadás katasztrofális következményekkel járhat. A 2015. november 13-án Párizsban végrehajtott támadások során, a Bataclan koncertteremben történt lövöldözés halálos áldozatainak száma 130 fő volt (ebből 91 fő a koncertteremben), a sebesültek száma meghaladta a 800 főt.[15] A Bataclan elleni támadást végrehajtó Omar Ismail Mostefai, Samy Amimour, illetve Foued Mohamed-Aggad gépkarabélyokkal és robbanó mellényekkel volt felszerelve.[16] A sorozatlövő kézifegyverekkel rendelkező terroristák eredményesen tudják felvenni a harcot a helyszínre általában elsőként érkező, többnyire öntöltő pisztolyokkal felszerelt rendőrökkel szemben. 2015. január 7-én a gépkarabélyokkal felfegyverzett Saïd és Chérif Kouachi Párizsban, a Charlie Hebdo szerkesztőségében végzett 11 áldozattal, további 11-et megsebesítettek. A helyszín elhagyását követően agyonlőttek egy időközben kiérkező rendőrtisztet.[17]

A késsel történő támadás az erőszakos terrorcselekmények legprimitívebb formájának tekinthető, a legolcsóbb és legkevesebb felkészülést igénylő módszer, azonban egyúttal a legkevésbé hatékony is, ezért több esetben más támadási formákkal (például gázolással) kombinálva alkalmazták. 2017. június 3-án három terrorista a London Bridge-en egy kisteherautóval a tömegbe hajtott, majd a járművet hátrahagyva a Borough Market városrészben késekkel támadtak az emberekre. A terrorcselekménynek 7 halálos áldozata, illetve 48 sebesültje volt.[18] A támadás elbeszélésének margójára kívánkozik az alábbi történet, amely egyben kiváló indikátora a módszer hatékonyságának. A három támadó a Black and Blue étteremben szembetalálta magát Roy Larnerrel. A 47 éves Larner, „B…….. meg, én Millwall (szurkoló) vagyok!" kiáltással, puszta kézzel támadt a három késes elkövetőre. Larner súlyosan megsérült, azonban fellépésének köszönhetően a vendégeknek lehetőségük nyílt a menekülésre. A férfit elnevezték a London Bridge Oroszlánjának, illetve petíció indult, hogy megkapja a György-kereszt kitüntetést.[19]

A gépjárművel elkövetett gázolásos támadás (angol kifejezéssel: *ramming*), hatékonyan alkalmazható gyalogosok ellen olyan területeken, ahol a tereptárgyak nem akadályozzák a gyors és folyamatos haladást. A módszer nem igényel komoly előkészületet, szervezést vagy jelentős anyagi eszközöket. 2017. augusztus 17-én Younes Abouyaaqoub, Barcelona La Rambla nevű sétálóutcáján egy bérelt kisteherautóval 80 km/h sebességgel belehajtott a tömegbe, majd gyalogosan elmenekült. A támadásnak 13 halálos áldozata volt, további 130 személy megsérült.[20]

[14] Tamási–Földi 2011: 69.
[15] *Forensics Crime Scene Investigation after Terrorist Attacks* 2022.
[16] Duquet et al. 2019: 44.
[17] Duquet et al. 2019: 39.
[18] Index 2017b.
[19] Index 2017a.
[20] Tálas–Szente-Varga 2017: 73.

A robbantással elkövetett terrorcselekmények sajátosságai

A robbantással elkövetett terrorcselekmények helyszíne többnyire valamilyen tömegrendezvény, vagy egyéb nyilvános, forgalmas hely. A támadás összehangolt akciók sorozatából is állhat, amelyek során az elkövetők különböző módszerek kombinációját is alkalmazhatják. Az egyes helyszíneken számolni kell a másodlagos robbanóeszközök jelenlétével is. Az ilyen típusú terrorcselekményeket követően kialakuló helyzet kezelése nagy erőket igénylő, rendkívül összetett feladat. Mint mindig, elsődleges az élet- és vagyonmentés, a sérültek és a túlélők evakuálása, ellátása, a keletkezett tüzek eloltása, a helyszínen tartózkodó fegyveres elkövetők semlegesítése, további robbanóeszközök felkutatása érdekében a helyszín átvizsgálása, a robbanás következtében fellépő veszélyhelyzetek (például sérült épületszerkezetek, közművek) kezelése stb. Mindezen körülmények a helyszíni szemle eredményességét negatívan befolyásolják.

Az egyik legfontosabb kérdés, hogy magányos elkövetőről vagy csoportról van-e szó, ez(ek) valamilyen szervezethez tartoznak-e. A robbantással elkövetett úgynevezett öngyilkos merényleteket végrehajtó személyek többnyire életüket veszítik. Más esetekben, például telepített, távirányított robbanóeszköz alkalmazásakor az elkövetők az elfogásukra irányuló intézkedés során a rendvédelmi szervek tagjaival folytatott tűzharc alkalmával halnak meg. Ilyen módon a szűkebb értelemben vett elkövető(k) kilétének, személyazonosságának megállapítása a holttest(ek) azonosításával történhet meg. Ugyanakkor ez esetben a nyomozó hatóságok nem számíthatnak az elkövető kihallgatásából származó információkra.

A helyszíni szemle során beszerezhető nagy fontosságú információhalmaz forrása az elkövetés eszközének, azaz a robbanóeszköznek, illetve a robbanóanyagnak a maradványai. Jelentőségük abban rejlik, hogy segíthetnek további két lényegi kérdés megválaszolásában:

- Ki készítette az eszközt?
- Honnan származnak az alkotóelemek?

Ezek az információk fontos elemei a terrorcselekmény felderítésének és a bizonyítási eljárásnak, továbbá hozzájárulhatnak további bűncselekmények megelőzéséhez akár a konkrét ügyhöz kötődően, akár jövőbeni hasonló eszközzel, anyagokkal vagy módon elkövetett cselekmények tekintetében.

A robbantással elkövetett terrorcselekmények helyszíni szemléjének specifikumai

A helyszíni szemle lefolytatását megelőzi a helyszín tűzszerész szolgálat általi átvizsgálása. Ennek során az el nem működött, illetve másodlagos robbanóeszközök, intakt robbanóanyagok felkutatására, összegyűjtésére és a helyszínről elszállítására kerül sor.

A helyszínen felkutatott és rögzített tárgytöredékek, anyagmaradványok és nyomok alapján történik az alkalmazott eszköz rekonstruálása. Ez magában foglalja az alábbiakat:[21]

- az eszköz típusának,
- a robbanótöltet fajtájának, nagyságának,
- a gyújtószerkezet típusának,
- az indítás módjának meghatározását.

E tekintetben a helyszíni szemle fő feladatai:

- A robbanóeszköz pusztító hatásának pontos, szakszerű dokumentálása:[22]
  - a nyomásváltozás (lökéshullám) okozta pusztítás (zúzó hatás);
  - a keletkezett kráter fizikai méretei, jellemzői;
  - elsődleges, azaz a robbanóeszközből származó, illetve másodlagos, a környezeti tárgyakból származó fragmentációs hatás.
- A robbanóeszköz maradványainak összegyűjtése. Improvizált robbanóeszközök esetén a robbanótölteten túl a fő szerkezeti elemek: gyújtószerkezet (katonai gyutacsok, bányászati detonátorok, harcanyagokból kinyert, illetve improvizált gyújtók), indítószerkezet (mechanikus, időzített, irányított – közvetlen, vezetékes, vagy rádióirányítású – szerkezetek). Kiegészítő szerkezeti elemek lehetnek repeszképző anyagok (szeg, csavar), áramforrások stb.[23]
- A robbanótöltetből származó anyagmaradványok összegyűjtése, mintavételezése. A robbanótöltet lehet katonai (katonai robbantástechnikában alkalmazott préselt vagy plasztikus, illetve fel nem robbant harcanyagokból kinyert), ipari, valamint házilag előállított (angolul: *home made explosives,* HME) robbanóanyag.[24] Az anyagmaradványok lehetnek makroszkopikus, szemmel látható (lőporkeverékek, házi előállítású elegyek, egyéb okból nem megfelelően működő robbanóanyagok maradványai), illetve kis mennyiségű, szabad szemmel nem látható anyagmaradványok (gőzök, szilárd felületeken abszorbeálódott részecskék stb.).[25]

E feladatok szakszerű végrehajtása tűzszerész[26] és vegyész szakértő[27] bevonásával végezhető el.[28]

[21] Lapat 2002: 34.
[22] Lapat 2002: 35–37.
[23] Kovács 2012: 39.
[24] Kovács 2012: 39.
[25] Lapat 2002: 38–39.
[26] Technical Working Group for Bombing Scene Investigation 2000: 27.
[27] Lapat 2002: 42.
[28] A tűzszerész szaktanácsadói minőségben segíti a nyomozó hatóság munkáját. Például egy robbantással elkövetett terrorcselekmény helyszínén közreműködik a robbanóeszköz maradványainak a felkutatásában.

A szemle vizuális adatainak digitális rögzítésére alkalmazható eszközök és eljárások

A büntetőeljárásról szóló 2017. évi XC. törvény 207. § (2) bekezdése szerint:

„A szemle alkalmával a bizonyítás szempontjából jelentős körülményeket részletesen rögzíteni kell, így különösen a szemletárgy felkutatásának, összegyűjtésének menetét, módját, helyét és állapotát. A tárgyi bizonyítási eszközök felkutatása, rögzítése és biztosítása során úgy kell eljárni, hogy az eljárási szabályok megtartása utólagosan is ellenőrizhető legyen. A szemle tárgyáról, ha lehetséges és szükséges, kép-, hang-, illetve kép- és hangfelvételt, rajzot vagy vázlatot kell készíteni, és azt a jegyzőkönyvhöz kell csatolni."[29]

A kriminalisztikai fénykép- és mozgóképfelvételek elkészítésére vonatkozó szakmai szabályokat és ajánlásokat módszertani útmutatók tartalmazzák.[30] Hazánkban az 1990-es évek második felében vezették be a kriminál technikai céllal alkalmazott digitális fényképezőgépeket. A digitális fényképezés, mozgóképrögzítés, mint a szemle vizuális adatainak rögzítésére alkalmazott technológia, az azóta eltelt időben egyeduralkodóvá vált. Itt szükséges megjegyezni, hogy a helyszínre elsőként kiérkező, az élet- és vagyonmentést, illetve egyéb elsődleges intézkedést végrehajtó szervezeti egységek (BM Országos Katasztrófavédelmi Főigazgatóság, Országos Mentőszolgálat, Rendőrség stb.) tagjai által viselt testkamerák,[31] illetve az esetlegesen alkalmazott drónok kameráinak felvételei a szemle megkezdése előtti állapotok, folyamatok tekintetében pótolhatatlan, releváns információk forrásai lehetnek.

A vizuális információk háromdimenziós rekonstrukciójának kriminalisztikai alkalmazása az elmúlt évtizedben jelent meg. E technológiák lehetőséget nyújtanak egy adott objektum tetszőleges nézetből való megtekintésére, ezáltal a dokumentáció olyan információkat is tartalmazhat, amelyek a kétdimenziós fényképfelvételekből nem nyerhetők ki.[32] További előnyt kínál a mérések, jelölések (például egyes tárgyi bizonyítási eszközök lokalizációja, lőirány stb.) elvégzésének lehetősége a 3D-modellben.

Kriminalisztikai célú térbeli rekonstrukció létrehozására a 3D optikai szkennerek és a fotogrammetriai eljárás alkalmazható eredményesen. A 3D optikai szkennerek fényt kibocsátva, majd a visszavert fényt érzékelve határozzák meg a környezet egyes pontjainak a szkennertől való távolságát, így egy mérési pontokból álló háromdimenziós pontfelhőt készítenek, amely térbeli modellé alakítható. Két fő típusuk a lézer- és a strukturáltfény-szkennerek.[33] A fotogrammetriai eljárás során a tárgyak térbeli helyzetének, illetve a környezet térbeli struktúrájának rekonstruálása egymással átfedésben lévő, kissé eltérő térbeli pozícióból készített fényképfelvételek alapján történik az erre szolgáló fotogrammetriai szoftverek alkalmazásával.[34]

[29] 2017. évi XC. törvény a büntetőeljárásról.
[30] Petrétei 2014: 25–33.
[31] Petrétei 2020.
[32] Ujvári–Metzger 2024: 90.
[33] Ujvári–Metzger 2024: 94–98.
[34] Ujvári–Metzger 2024: 99.

A Közösségi Kutatási és Fejlesztési Információs Szolgálat (angolul: Community Research and Development Information Service, CORDIS) 2012–2015 között folytatott Hyperion projektje során kifejlesztett 3D-technológia az optikai szkenner és a fotogrammetria kombinációját alkalmazza. A mérőegységet egy strukturált fényszkenner, egy sztereó fényképezőgép, valamint egy inerciális mérőegység (angolul: *inertial measurement unit,* IMU) modul alkotja. Utóbbi részegység a kamera pozíciójának, illetve tájolásának pontos rögzítését szolgálja, ezáltal biztosítva a térbeli rekonstrukció nagy pontosságát.[35]

A robbantásos cselekmények tekintetében a digitális 3D-modell lehetővé teszi a helyszín, az abban található objektumok, illetve a robbanás által okozott fizikai elváltozások összességében, összefüggésében való vizsgálatát, mégpedig a helyszíni szemlekori állapotnak megfelelő kondícióban, tetszőleges időben és alkalommal.

A robbanás okozta fizikai elváltozások digitális értékelésének lehetőségei

Az inverz robbanás analízis (angolul: *Inverse Explosion Analysis,* IEA) eszközökkel a robbanótöltet tömegének megállapítására irányuló számítások végezhetők a robbanás által okozott pusztítás alapján. E számítási modellek a robbanótöltet tömegének elsődleges becslésére alkalmasak. A számítások alapját a robbanás során bekövetkezett épületkárosodás, ablaktörés, a keletkezett kráter méretbeli sajátosságai képezhetik, míg a törmelék repülési távolsága kiegészítő információk forrásaként szolgálhat.[36]

Az épületkárok és ablaktörések esetében a módszer alapját a kár mértékének, a töltet tömegének, valamint az épület és a robbanás közötti távolságnak az összefüggései adják. Az eljárás lényege, hogy amennyiben egy struktúra, például ablak épen maradt, úgy a távolság és az alkalmazott robbanóanyag figyelembevételével maximum, ha pedig azt a robbanás teljesen megsemmisítette, minimum töltettömeg állapítható meg. A részlegesen sérült épületek esetében a módszer előzetesen meghatározott, a teljes megsemmisülés (amely a falazat legalább 75%-ának lerombolását jelenti) és az ép állapot között elhelyezkedő, tapasztalati úton megállapított kategóriákkal operálva, a távolság függvényében, ekvivalens TNT-tömegben adja meg az alkalmazott robbanóanyag mennyiségét. A módszer szórását, azaz a hibaszázalékot növelik az alábbi körülmények:

- A robbanás epicentrumának lokalizálása során fellépő nehézségek. Például nem keletkezett kráter, vagy a robbanás utáni tűz következtében megsemmisültek a nyomok.
- Az alkalmazott robbanóanyag működéséből eredő bizonytalanságok. Például különböző okokból nem megfelelően működő vagy változó összetételű HME-anyagok.
- A beépített területek esetén az épületek árnyékoló hatása és a töltet elhelyezési pontjához, illetve a robbanási hullám terjedésének irányához viszonyított tájolása.[37]

[35] European Commission 2016b: 9.
[36] European Commission 2016b: 13.
[37] van der Voort et al. 2015: 11–12.

A Hyperion projekt során a Holland Alkalmazott Tudományos Kutatóintézet (hollandul: Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek, TNO) által kifejlesztett IEA eszköz statisztikai módszert alkalmaz a három számítási mód (azaz a minimum- és maximumértékek, továbbá az adott mértékű károsodáshoz kötött érték) kombinálásával a töltettömeg megadásához.[38]

Az épületek árnyékoló hatása okozta számítási hibák kiküszöbölésére a folyadékok és gázok áramlásának szimulálására szolgáló számítási folyadékdinamikai (angolul: *computational fluid dynamics,* CFD) szoftverek használata kínál megoldást.[39]

A robbanótöltet tömege a robbanás során a talajban keletkező kráter mérete alapján is meghatározható. A folyamatot jelentősen befolyásolja a talajszerkezet, a robbanóanyag működése, illetve az a körülmény, ha a robbanás egy gépjármű alatt történik. Azonos tömegű töltetek robbanása során az agyagos talajokban nagyobb, a homokos talajokban kisebb, a vegyes talajokban közepes méretű kráterek képződnek. A talaj nedvességtartalmának növekedése nagyobb krátereket eredményez.[40] A HME-anyagokra jellemző változó, többnyire az optimális hatékonyság alatti működésből eredő hibák kiküszöbölésére az Egyesült Államok Hadseregének Hírszerző és Biztonsági Parancsnoksága Harci Eseményeket Elemző Részlegének (angolul: *Combat Incident Analysis Division,* CIAD) kutatásai alapján bevezették az effektív nettó robbanótömeg (angolul: *effective net explosive weight,* E-NEW) fogalmát, amely a krátert létrehozó robbanáshoz hatékonyan hozzájáruló robbanóanyag-mennyiséget jelöli.[41]

A kráterek elemzésére kifejlesztett, hazánkban is ismert szoftver a Caldera, amely elemzési és előrejelzési módban is alkalmazható. Elemzési módban a kráterméret (szélesség, illetve mélység), a talaj jellemzőinek (talajtípus, víztartalom és sűrűség), a robbanóanyag típusának megadása, illetve annak a körülménynek a rögzítése alapján, hogy a töltet felett volt-e a robbanás pillanatában gépjármű, a program megadja a robbanótöltet E-NEW értékét, illetve a töltet elhelyezésének mélységére vonatkozó adatokat. Előrejelzési módban a talaj tulajdonságai, az alkalmazott töltet jellemzői (robbanóanyag-típus, E-NEW érték), a töltet elhelyezési mélysége, valamint a gépjármű alatti működés körülményének figyelembevételével számolja ki a várható kráterméretet.[42]

Helyszíni detektálás és digitalizáció

A vizsgálatok tapasztalatai alapján a robbantással elkövetett cselekményeket követően a robbanóanyagból származó anyagmaradványok mérhető mennyiségben és koncentrációban találhatók meg a helyszínen.[43] E maradványok legnagyobb koncentrációja a robbanás epicentrumának környezetében a talajon, az érintett épületeken és a keletkezett törmeléken lokalizálható, de terjedésüket befolyásolja a szélirány, illetve

[38] European Commission 2016b: 13–14.
[39] van der Voort et al. 2015: 21.
[40] Collazo–Payne–Thomas 2014: 5.
[41] Collazo–Payne–Thomas 2014: 3.
[42] Collazo–Payne–Thomas 2014: 5.
[43] European Commission 2016b: 6.

a környező épületek elhelyezkedése is. Jelentőségük abban rejlik, hogy vizsgálatukkal meghatározható a bűncselekmény során alkalmazott robbanóanyag.[44]

Az anyagmaradványok helyszíni kimutatására és előzetes elemzésére a különböző kézi spektrométerek alkalmazhatók. Legelterjedtebbek a Raman és az IR- (infravörös) eszközök, mindkettő a rezgési spektroszkópia tárgykörébe tartozik, előbbi a fényszóródás, utóbbi a fényelnyelés elvét alkalmazza. A Hyperion projekt során mindkét technológiát tesztelték stand-off[45] detektorként, a kísérletek során Raman eszközzel 25 m,[46] IR spektrométerrel 10,2 m távolságból[47] hajtottak végre sikeres méréseket. A Raman spektroszkópiához kapcsolódó innovatív technológia a Raman-képalkotás (Raman Imaging). Az eljárással létrehozott színes képet alkotó pixelek mindegyike egy-egy Raman-spektrumnak felel meg, létrehozva a minta kémiai összetételének térbeli ábrázolását. Az eljárással megjeleníthető a molekulák térbeli eloszlása, illetve egyszerűsíthető a mintavételek végrehajtása.

A félvezetőt tartalmazó elektronikus eszközök felderítésére szolgálnak a Nonlinear Junction (NLJD) detektorok.[48] Ezekkel az eszközökkel a kikapcsolt vagy már üzemképtelen, lemerült eszközök is felkutathatók, így alkalmasak az IED eszközökből származó elektronikus alkatrészekből származó tárgytöredékek felkutatására is.[49]

Összegzés

A helyszín vizuális adatainak térbeli rekonstruálására a rendelkezésre álló 3D-technológiák, azaz a lézerszkenner, illetve fotogrammetriai eljárás, valamint ezek kombinációja alkalmazható. A digitális 3D-modell biztosítja a helyszín szemlekori állapotában való utólagos vizsgálatát bármely nézőpontban, lehetőséget nyújt mérések és jelölések alkalmazására, a helyszín és az ott található objektumok összességében és összefüggéseiben való értékelésére, következtetések levonására (például a robbanás epicentruma, azaz az IED lokalizációja, a pusztítás kiterjedése, a törmelék kiszóródásának iránya, távolsága stb.).

A Raman- és IR-spektrometria elvén működő stand-off detektorok segítségével a szemle statikus szakaszában biztonságos távolságból vizsgálhatók a hot spotok, illetve robbanóanyagok, robbanóanyag-maradványok. A szemle dinamikus szakaszában a robbanóanyagok, illetve azok maradványainak mintavételezését, vagy eredetben való biztosítását megelőzően kézi spektrométerekkel előzetes, helyszíni vizsgálatok végezhetők a robbanóanyag típusának megállapítására. A spektrometria nyújtotta lehetőségeket tovább bővíti a Raman képalkotó technológia, amely alkalmas a robbanóanyagokból származó anyagmaradványok térbeli eloszlásának képi ábrázolására.

[44] Rizzo et al. 2022: 1.
[45] A biztonságos távolságról, állványon elhelyezett eszközzel végrehajtott mérésre alkalmas detektortechnológiát jelölő angol kifejezés, amelynek jelenleg még nincs elfogadott magyar nyelvű megfelelője.
[46] European Commission 2016b: 7.
[47] European Commission 2016b: 14.
[48] E detektortípus megnevezésére az angol nyelvű rövidítést (NLJD) alkalmazzák a magyar nyelvű szakirodalomban is.
[49] European Commission 2016a: 4.

Az IED eszközök elektronikus alkatrészei (indító- és időzítő szerkezetek), illetve az ezekből származó tárgytöredékek felkutatása NLJD detektorokkal végezhető el.

Az IEA-szoftverek alkalmazásával a robbanás pusztító hatása (például a keletkezett kráter, illetve épületkárok) alapján számítások végezhetők a robbanótöltet tömegének megállapítására.

További lehetőségek rejlenek a nyomok, anyagmaradványok, tárgytöredékek lokalizációjára, rögzítésére, előzetes vizsgálatára vonatkozó adatoknak a felügyeleti lánc biztosításával a helyszín 3D-modelljébe integrálásában. A 2012–2015 között folytatott Hyperion (Hyperspectral imaging IED and explosives reconnaissance system),[50] illetve FORLAB (Forensic Laboratory for in-situ evidence analysis in a post blast scenario)[51] projektek során a különböző detektálási technikákkal végzett vizsgálatok helyét, illetve eredményét megközelítőleg valós időben integrálták a helyszín digitális térbeli modelljébe.

A cikk a 2024. október 15-i II. Alverad-Bánki Nemzetközi Kiberbiztonsági Konferencián elhangzott előadás kivonata.

Felhasznált irodalom

Beke József (2022): *A terrorelhárítás kialakulása és fejlődése Magyarországon a hidegháborúban a „C-79-es" akta tükrében.* PhD-disszertáció. Nemzeti Közszolgálati Egyetem Rendészettudományi Doktori Iskola. Online: https://doi.org/10.17625/NKE.2023.051

Collazo, Félix L. Santiago – Payne, Joshua E. – Thomas, Cameron D. (2014): *Evaluation and Optimization of the Random Forest Algorithm for Crater Analysis*. Engineering Research and Development Center of the U.S. Army Corps of Engineer and University of Puerto Rico at Mayagüez. Online: www.researchgate.net/publication/264810020_Evaluation_and_Optimization_of_the_Random_Forest_Algorithm_for_Crater_Analysis#fullTextFileContent

Duquet, Nils – Kbiltsetskhlashvili, Nino – Khan, Isthiaq – Woods, Eric (2019): *Armed To Kill. A Comprehensive Analysis of the Guns Used in Public Mass Shootings in Europe between 2009 and 2018.* Brussels: Flemish Peace Institute.

Európai Bizottság (2017): *A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának. Cselekvési terv a vegyi, biológiai, radiológiai és nukleáris biztonsági kockázatokkal szembeni felkészültség fokozásáról.* COM(2017) 610 final. Online: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52017DC0610&from=EN

European Commission (2016a): *Forensic Laboratory for in-situ evidence analysis in a post blast scenario. Final Report Summary – FORLAB (Forensic Laboratory for in-situ evidence analysis in a post blast scenario).* Online: https://cordis.europa.eu/project/id/285052/reporting

[50] European Commission 2016b: 4.
[51] European Commission 2016a: 4.

European Commission (2016b): *Hyperspectral Imaging IED and Explosives Reconnaissance System. Final Report Summary – HYPERION (Hyperspectral Imaging IED and Explosives Reconnaissance System).* Online: https://cordis.europa.eu/project/id/284585/reporting

Forensics Crime Scene Investigation after Terrorist Attacks (2022). Előadás. Saint Malo: Thematic course 2205.

Gönczöl Katalin – Kerezsi Klára – Korinek László – Lévay Miklós szerk. (2012): *Kriminológia – szakkriminológia.* Budapest: CompLex. Online: https://mersz.hu/hivatkozas/wk54_287

Hausner Gábor szerk. (2022): *Honvédelmi alapismeretek.* Budapest: Ludovika. Online: https://doi.org/10.1556/9789634549543

Illár Sándor szerk. (1984): *Kriminál technika.* Budapest: BM Könyvkiadó.

Index (2017a): Puszta kézzel ment neki a londoni terroristáknak a Millwall-szurkoló. *Index,* 2017. június 6. Online: https://index.hu/kulfold/2017/06/06/puszta_kezzel_ment_neki_a_londoni_terroristaknak_a_millwall-szurkolo/?token=ed4e9f51c-2f5ed8d877b6ae99c4dbb98

Index (2017b): Terrortámadás Londonban: gázolás, késelés, hét halott, 48 sérült. *Index,* 2017. június 4. Online: https://index.hu/kulfold/2017/06/03/gyalogosokat_gazolt_el_egy_furgon_a_london_bridge-en/

Kis-Benedek József (2023): *A terrorizmus megelőzése és felderítése.* Előadás. Budapest: Nemzeti Közszolgálati Egyetem.

Kovács Zoltán (2012): Az improvizált robbanóeszközök főbb típusai. *Műszaki Katonai Közlöny,* 22(2), 37–52. Online: https://mkk.uni-nke.hu/document/mkk-uni-nke-hu/2012_2_03%20IED-k%20főbb%20típusai%20-%20Kovács%20Z.pdf

Krajnc Zoltán főszerk. (2019): *Hadtudományi lexikon – Új kötet.* Budapest: Dialóg Campus.

Lapat Attila (2002): *Robbanóanyag-analitikai vizsgálati módszerek alkalmazása az igazságügyi szakértői munkában, szerepük a robbanóanyaggal elkövetett bűncselekmények felderítésében.* PhD-disszertáció. Zrínyi Miklós Nemzetvédelmi Egyetem. Online: http://hdl.handle.net/20.500.12944/11960

London bombings of 2005 [é. n.]. Online: www.btp.police.uk/police-forces/british-transport-police/areas/about-us/about-us/our-history/london-bombings-of-2005/

Mátyás Szabolcs – Sallai János (2015): Objektív és szubjektív biztonság néhány magyar nagyvárosban. In Hervainé Szabó Gyöngyvér (szerk): *A 21. század elejei államiság kérdőjelei.* Székesfehérvár: Kodolányi János Főiskola, 335–407.

Mumford, Andrew (2016): *The Role of Counter Terrorism in Hybrid Warfare. A report prepared for NATOs Centre of Excellence for Defence Against Terrorism (COE DAT).*

Petrétei Dávid (2014): Álló- és mozgókép készítése, helyszínvázlat, helyszínrajz. In Gárdonyi Gergely (szerk.): *Módszertani útmutató 1. bűnügyi technikusok részére.* Budapest: Nemzeti Közszolgálati Egyetem, 25–33. Online: https://rtk.uni-nke.hu/document/rtk-uni-nke-hu/Modszertani_utmutato_I_bunugyi_technikusok_reszere.pdf

Petrétei Dávid (2020): A kriminalisztikai fényképezés egyes aktuális kérdései. *Magyar Bűnüldöző,* 11(1–2), 12–22.

Rizzo, A. – Telloli, C. – Ubaldini, A. – Ottaviano, G. – Salvi, S. (2022): Fast Characterization of Compounds and Components of Explosives. *The European Physical Journal Plus,* 137. Online: https://doi.org/10.1140/epjp/s13360-022-02404-4

Schvéd Brigitta (2020): „Emlékezz, emlékezz november ötödikére…" – Az 1605. évi lőporos összeesküvés és a Guy Fawkes-nap történeti hagyománya. *Újkor,* 2020. november 5. Online: https://ujkor.hu/content/emlekezz-emlekezz-november-otodikere-az-1605-evi-loporos-osszeeskuves-es-guy-fawkes-nap-torteneti-hagyomanya

Tálas Péter – Szente-Varga Mónika (2017): A 2017. augusztusi spanyolországi terrortámadásokról. *Nemzet és Biztonság,* 10(5), 70–78. Online: http://real.mtak.hu/95605/1/nb_2017_05_06_talas_p-szente-varga_m_-_a_2017_augusztusi_spanyolorszagi _ terrortamadasokrol.pdf

Tamási Béla – Földi László (2011): A tokiói metróban végrehajtott szarin támadás katasztrófavédelmi aspektusai. *Hadmérnök,* 6(3), 68–78. Online: http://hadmernok.hu/2011_3_tamasi_foldi.pdf

Technical Working Group for Bombing Scene Investigation (2000): *A Guide for Explosion Bombing Scene Investigation Section A. Procuring Equipment and Tools.* Washington D.C.: U.S. Department of Justice, Office of Justice Programs National Institute of Justice. Online: www.ojp.gov/pdffiles1/nij/181869.pdf

Ujvári Zsolt – Metzger Máté (2024): A fotogrammetria kriminalisztikai alkalmazása – tudományosan megalapozott módszerek fényképezőgép segítségével történő 3D képrögzítéshez. *Rendőrségi Tanulmányok,* (Különszám), 78–220. Online: https://doi.org/10.53304/RT.2024.ksz.02

Van der Voort, M. M. – van Wees, R. M. M. – Brouwer, S. D. – van der Jagt-Deutekom, M. J. – Verreault, J. (2025): Forensic Analysis of Explosions: Inverse Calculation of the Charge Mass. *Forensic Science International,* 252, 11–21. Online: https://doi.org/10.1016/j.forsciint.2015.04.014

HADMÉRNÖK
FÓRUM
19. évfolyam (2024) 4. szám 213–232.
DOI: 10.32567/hm.2024.4.15

Zlatko Čović[1]

New Approaches in the Education of Software Engineers in the Field of Cybersecurity

Abstract

This paper presents innovative methodologies for cybersecurity education, with a focus on their application at Subotica Tech – College of Applied Sciences. The study highlights hackathon-based learning (HBL), challenge-based learning (CBL), and the integration of Artificial Intelligence (AI) tools to enhance teaching effectiveness. These approaches are incorporated into professional courses related to the development of web applications and integrated web systems, emphasising practical work and real-world scenarios to better prepare students for industry challenges. The primary objective of this paper is to introduce these novel educational approaches and provide a detailed description of their implementation, underscoring the importance of hands-on experience and student engagement in real-world systems and business environments. The results of the research on the impact of hackathon participation on final exam performance are presented. Additionally, the increasing use of AI tools in software engineering education is explored, with examples of their application. Finally, the paper outlines future research directions based on feedback from the current implementation of these methodologies.

Keywords: cybersecurity, software engineering, practical engineering education, hackathon, challenge-based tasks, AI

Introduction

In the rapidly evolving digital landscape, where technology plays an integral role in nearly every aspect of modern life, the importance of securing online systems cannot be overstated. Every day, huge amounts of information are exchanged through websites, applications, and other information systems. This information exchange is crucial to

[1] Subotica Tech – College of Applied Sciences, e-mail: chole@vts.su.ac.rs

the operation of modern digital systems, making secure data transfer essential. In addition to securing the exchanged data, it is equally important to ensure the safety and reliability of the systems themselves. As cyber threats continue to evolve, it is increasingly important for software and cybersecurity engineers to be well-versed in identifying potential security risks and vulnerabilities, while also possessing the knowledge and skills needed to address these security problems effectively.

Higher education should follow present trends and listen to the needs of industry, continuously adapting and improving curricula accordingly. In addition to the traditional model of engineering education, which includes theoretical lectures and practical laboratory exercises, it is essential to develop and implement new teaching methods that will contribute to the better development of key competencies in students, as well as enhance their competitiveness in the job market. Furthermore, it is crucial to find ways to integrate industry into the educational process, enabling students to directly engage in real-world challenges and market needs, thereby increasing the relevance and applicability of the knowledge acquired.

The importance of hands-on and practical methodologies in cybersecurity education has been extensively emphasised in recent research. For instance, authors analyse the educational value of Capture the Flag (CTF) challenges, demonstrating how they align technical knowledge areas like cryptography and network security with established curricular guidelines.[2] However, the authors highlight the need to incorporate non-technical aspects, such as social engineering, to address advanced cyber threats comprehensively. Similarly, authors in the study identify learning obstacles in CTF-based education, such as a steep learning curve for beginners, and propose varying difficulty levels and adequate support to enhance their effectiveness.[3]

Further, authors explore the role of serious games in enhancing cybersecurity skills. Their findings show that game-based learning can maintain student engagement while balancing educational objectives.[4] Additionally, authors in study advocate for using CTF competitions as an introductory tool for cybersecurity education, emphasising their potential to motivate students and providing practical exposure to key concepts.[5]

Beyond CTFs, authors investigate the integration of hackathons into online cybersecurity courses. Their study reveals that hackathons enhance collaboration and practical understanding, supporting teamwork and maintaining student engagement through real-world problem-solving.[6] These findings align closely with the methodologies implemented at Subotica Tech – College of Applied Sciences, where hackathon-based learning and challenge-based tasks are integrated into professional courses to prepare students for real-world challenges.

In the study by the authors Čović et al., the focus is on evaluating the effectiveness of the hackathon approach in the training of software engineers. This student-centred method employs a constructivist pedagogical framework. Throughout a hackathon, students work closely with programmers and other software development experts

[2] Švábenský et al. 2021.
[3] Chung–Cohen 2014.
[4] Vykopal et al. 2020.
[5] McDaniel et al. 2016.
[6] Obot Affia et al. 2022.

on collaborative projects. This approach enables students to acquire new knowledge, enhance their skills, and develop essential competencies.[7]

Another paper discusses the use of Challenge-Based Learning (CBL) in cybersecurity education, where challenges were based on students' interests in securing systems.[8] Students worked collaboratively to devise solutions, applying their knowledge in two cybersecurity competitions. Formative assessments revealed that while the benefits varied among students, skills in computer security, teaching, and interest in cybersecurity were enhanced. Despite the need for additional resources and flexible meeting schedules, the increased learning outcomes justified the effort.

As authors in Žagar et al. have shown, research in software engineering (SE) indicates that recent graduates are often unprepared for workplace challenges.[9] The authors presented two approaches used in SE courses at the University of Zagreb: a distributed project-based course where Croatian and Swedish students collaborate throughout the software development life cycle, solving technical and cultural problems, and an approach focused on self-constructing knowledge, presenting it to peers, and concluding with student discussions and a group project. Both approaches foster the development of soft skills, which are often underrepresented in SE education.

Authors in a study investigated challenges in teaching software engineering through a survey of 21 faculty and experts. Findings revealed that student engagement was the most significant challenge, with nearly half of respondents also reporting difficulties in designing practical activities.[10] Problem-based learning was the most used approach, followed by newer methods like gamification and role-playing, both shown to enhance engagement. Based on these insights, a conceptual model for improving student involvement is proposed, with future studies suggested to evaluate its impact in practice.

To ensure the security of web applications and information systems, developers must conduct appropriate tests. Raising awareness of potential vulnerabilities and threats is also crucial. The OWASP Top 10, developed by the OWASP Foundation, serves as a standard reference for developers, highlighting the most critical security risks for web applications.[11] This framework should also be incorporated into engineering education.

The primary goal of this paper is to introduce and evaluate innovative educational methodologies designed to enhance the training of software engineers in cybersecurity. Specifically, the study focuses on Subotica Tech – College of Applied Sciences, highlighting the integration of hackathon-based learning, challenge-based tasks, and AI tools. These methods emphasize real-world applicability through industry collaborations and advanced pedagogical techniques.

This paper is organised as follows. The first section provides an overview of engineering education at Subotica Tech – College of Applied Sciences, with a focus on cybersecurity education, including an introduction to the OWASP Top 10 web

7 Čović et al. 2022.
8 Cheung et al. 2011.
9 Žagar et al. 2008.
10 Ouhbi–Pombo 2020.
11 Čović 2024.

application security risks and vulnerabilities and OWASP API Security Top 10. The second offers a detailed description of the new approaches implemented in the education of software engineers, including Hackathon-based learning, challenge-based tasks, and the use of AI tools. The results of the research on the impact of hackathon participation on final exam performance are presented also in this section. Plans are discussed in the next section. In conclusion, the paper summarises the key points discussed throughout.

Engineering education at Subotica Tech

The Subotica College of Applied Sciences, established in 1960, is one of the most respected state higher education institutions in Serbia. For over half a century, the college has educated thousands of engineers in the field of technical and technological sciences, who now form the backbone of the skilled workforce in local and wider industry sectors.

The studies are organised at two levels: undergraduate applied studies (BSc) lasting three years and master applied studies (MSc) lasting two years. The undergraduate programmes offered include Electrical Engineering, Computer Science, Engineering Management, Mechanical Engineering, and Mechatronics. Currently, master's studies are available only in the field of Information Technology, with a focus on security.

At Subotica Tech – College of Applied Sciences, the focus of engineering education is on practical knowledge. In most professional courses, especially within the Informatics programme, teaching is delivered through a Project-Based Learning approach. During these courses, students, either individually or in teams, work on developing a software product (such as a web system, mobile application, or integrated information system), creating projects that include both software and hardware components, as well as managing and maintaining network systems. In addition to practical skills, students acquire theoretical knowledge in these areas, as well as in other foundational and advanced fields. In the final semester of undergraduate and master's studies, students complete a mandatory internship at one of the partner companies and conclude their studies with the preparation and defence of a final thesis.

The collaboration with companies at Subotica Tech involves organising student internships, expert lectures and workshops, joint projects, conference sponsorships, participation in competitions, student scholarships, and mentorship in student projects. All undergraduate and master's students are required to complete internships, often extending beyond the minimum duration.

Subotica Tech makes every effort to prepare future engineers with the necessary theoretical knowledge and practical skills across various engineering disciplines, including informatics. These skills can be further developed through internships and early work experience. The involvement of industry in both curricular and extracurricular activities significantly contributes to the development of key competencies and professional growth in engineering fields.

The College maintains close contact with industry to align study programmes with market needs. The programmes are not strictly tailored to specific job roles but

provide a broad foundation, enabling students to quickly adapt and pursue ongoing professional development. It is crucial that students acquire skills to approach problem-solving logically and apply algorithmic thinking and acquired knowledge to address challenges.

Additionally, new teaching methods are introduced in most professional courses, such as project-based learning, teamwork, hackathons, and challenge-based tasks. The aim is to engage students in real-world scenarios they will encounter in their professional careers.

Education in the field of cybersecurity

The experiences of students and professors gained through participation in various competitions, conferences, and hackathons, as well as strong industry relations, have contributed to the introduction of new methods in software engineering education. Security aspects of information systems have been studied for many years, but with the rise in risks and threats, the amount of coursework focused on cybersecurity has also increased.

Professional courses place a strong emphasis on various aspects of security. Many of these courses incorporate protection methods and techniques in laboratory exercises, employing diverse approaches to test information systems, web applications, mobile apps, and other software and network types.

According to the needs of cybersecurity experts, Subotica Tech participated in the ISSES (Information Security Services Education in Serbia) project under the Erasmus+ programme. The project brought together experts from higher education institutions and companies in the region to improve the higher education capacities in Information Security in the Republic of Serbia. As a result of the project, new courses and cutting-edge laboratories were developed, providing students with practical experience that can be directly applied in the information security industry. Subotica Tech also developed a new laboratory for information security, equipment for network and server room, and an MSC study programme in Information Technology with a focus on information security.

As part of the project, the Serbian Cybersecurity Challenge competition was organised five times to enable student teams to apply their acquired knowledge and gain new awareness in the field of information security. These efforts aim to enhance the competitiveness of students who graduate from participating higher education institutions in Serbia.[12]

It is essential to offer students opportunities to apply their knowledge. Assigning tasks in laboratory sessions and information security-related homework strengthens both their understanding and practical skills.

[12] Serbian Cybersecurity Challenge 2024.

Web application security risks and vulnerabilities

One of the most popular areas for developing various information systems today is the web. It is almost unimaginable for a system or application to lack a component that utilises data and resources from the internet. Therefore, significant attention is devoted to such systems.

Web application security, a critical aspect of information security, focuses on safeguarding web applications, websites, web systems, and web services. It extends the principles of application security, adapting them to address the unique challenges posed by web-based systems and the internet. One major issue in both developing and using web applications is the general lack of knowledge and awareness regarding potential threats. Developers often overlook the implementation of essential security techniques and methods, and they may neglect to perform necessary security assessments on their applications. One of the key aspects in creating secure web applications is the practical application of appropriate methods and technologies, based on theoretical knowledge. Additionally, it is essential to promptly identify security risks and threats and respond to them appropriately.

Categories of web application security risks that are listed in OWASP Top 10 document are:

- Broken Access Control
- Cryptographic Failures
- Injection
- Insecure Design
- Security Misconfiguration
- Vulnerable and Outdated Components
- Identification and Authentication Failures
- Software and Data Integrity Failures
- Security Logging and Monitoring Failures
- Server-Side Request Forgery[13]

The release of the OWASP Top 10:2025 is planned to be announced in the first half of 2025.[14] During their studies, students become familiar with most of the risk categories.

With the growing need for integrated systems using APIs, ensuring their security has become crucial. Students learn about API threats and protection methods from the OWASP Top 10 API Security Risks document and web portal. The OWASP API Security Top 10 project highlights key API security risks, helping developers and security professionals recognise and mitigate threats. It provides a Top 10 Risks document and a best practices portal, ensuring up-to-date guidance through collaboration with the security community.[15]

[13] OWASP Top 10 2024.
[14] OWASP Top 10 2024.
[15] OWASP API Security Top 10 2024.

New approaches in education

To allow students to participate in situations like real-life scenarios through the educational process, new teaching methods have been introduced in several specialised courses within the computer science programme, both during lectures and laboratory exercises.

The courses where new methods have been introduced include on the BSc level, Web Programming, Advanced Web Programming, and Integrated Web Systems. At the master's level, the course is Security in e-business systems. One of the innovations was also implemented in the education of students from Óbuda University in Budapest, who spent three months at Subotica Tech as part of the Erasmus exchange programme.

Hackathon-based learning (HBL)

A "hackathon" is a blend of "hack" and "marathon" referring to a 1- or 2-day brainstorming event where participants develop solutions for a specific challenge. Originally popular in the software industry, it typically involves developers working intensively to create software, applications, or hardware aimed at solving particular problems. This approach was first implemented in the introductory course Internet technologies, and after its successful integration, it has been organised annually in the course Web programming. Web programming is the first course where students must create a complex web project as a team, utilising various digital services and tools.

During hackathons, students can develop various key competencies such as collaboration, teamwork, negotiation, project management, time management, communication, and troubleshooting. Learning based on hackathons involves several activities and is carried out in multiple phases. Some of these phases can be categorised as "pre-hackathon" phases, as they aim to better prepare students for participating in a hackathon. At the beginning of the semester, since students are not yet familiar with the concept of HBL, each student is given a detailed description of the project task, which they will work on in teams of two. The document includes a detailed description of the functional requirements, as well as requirements for the implementation of security techniques and methods, and adherence to coding standards. All teams are provided with access parameters for the virtual web servers they will use during the project work.

Figure 1 illustrates the Hackathon-based learning process implemented at Subotica Tech, highlighting its structure and phases.

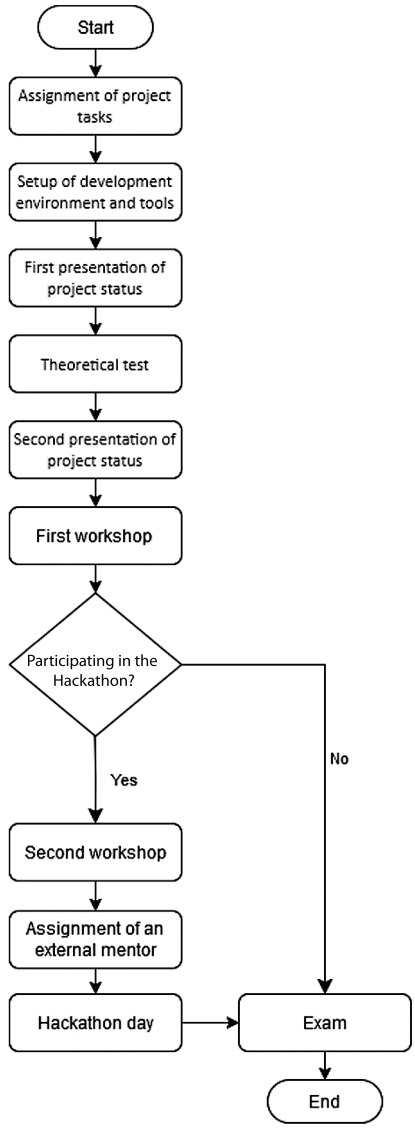


Figure 1: Phases of Hackathon-based Learning (HBL)
Source: compiled by the author

Students are required to use the *Trello* tool for project management, *Git* for version control of the code, and an appropriate hosting platform for repositories. Professors involved in the course are granted access to these services to monitor the overall progress of the project. The project work was supported and complemented by a series of lectures and lab exercises that were held throughout the entire semester. These sessions provided students with both theoretical knowledge and practical skills,

which were essential for the successful completion of their projects. In the first and second thirds of the semester, teams were required to publicly present the progress of their projects, allowing them to receive valuable feedback from both their peers and professors. These presentations were structured to not only assess the technical progress of the projects but also to foster a collaborative learning environment where students could share ideas, challenges, and solutions.

In the second third of the semester, an important milestone was reached: all students took a comprehensive theoretical test aimed at assessing the knowledge they had acquired up to that point. The test covered various aspects of the course material, including key concepts, methodologies, and tools relevant to the projects. The test results provided instructors with a clear understanding of each student's grasp of the subject matter, and helped in identifying areas that might require further attention.

In partnership with a local IT company, a workshop was organised for all students, with an additional session specifically for those who chose to participate in the hackathon. The workshops focused on the use of Git and included challenge-based tasks designed to enhance students' understanding of web application security.

After organised workshops, students were given the opportunity to participate in an additional, voluntary activity hackathon. While the hackathon required a significant amount of time and effort from the students, it was designed to further enhance their learning experience by providing an intensive, hands-on environment where they could apply their knowledge in real-world scenarios. This activity was expected to help students develop critical skills such as teamwork, problem-solving, and time management, while deepening their IT expertise.

The primary objective behind incorporating this hackathon activity was to stimulate the development of more polished and professional projects by the end of the semester. It was anticipated that the use of an HBL approach would encourage students to engage more deeply in their projects, enhance the quality of their work, and improve their overall IT competencies. By actively participating in such a dynamic and challenging environment, students were expected to gain valuable insights into the complexities of real-world problem-solving, making them better equipped to tackle similar challenges in their future careers.

Each team was paired with an external mentor-programmer from the local IT company. The mentors were given detailed descriptions of the project tasks and were responsible for identifying three additional functionalities that the teams were expected to implement during the hackathon. Teams and mentors communicated online during the first 24 hours. Mentors were also tasked with providing guidance on the use of specific classes or libraries if the additional functionalities required such resources.

After 24 hours of preparation and collaboration, the hackathon took place at Subotica Tech. The event lasted for a full 10 hours, during which teams had the opportunity to meet their mentors in person. The mentors played an active role in guiding teams through the process of developing and refining the additional functionalities assigned to them.

The following day, each team had the chance to publicly present their completed projects to the other teams, professors, and mentors. The presentations were an

important part of the process, allowing teams to showcase their work and demonstrate how their projects functioned as a whole. After each presentation, the mentors asked questions to gain a deeper understanding of the teams' approaches. The primary focus of the presentations was on the overall functionality, security and performance of the projects, rather than on a detailed analysis or review of the code itself.

When the day for project presentations was completed, both students and mentors received electronic surveys containing questions about the entire hackathon process. This practice was followed by each hackathon. The results from these surveys and feedback were used to assess participants' satisfaction with their involvement in the event, both from the students' and the companies' perspectives. Additionally, after certain hackathons, further evaluations were conducted to assess the impact of this learning method on the development of key competencies. The feedback collected helped to improve the organisation of future events.

The following day, students were required to defend their projects in front of professors, focusing specifically on the programming code level.

During the hackathon, students were required to apply appropriate security mechanisms and identify risks from all the categories listed in the OWASP Top 10 document. However, they focused most on the following risks:

- Server-Side Request Forgery
- Cryptographic Failures
- Injection
- Identification and Authentication Failures
- Broken Access Control

The surveys sent to participants after the last hackathon included 33 questions for students and 11 questions for mentors from the companies. When asked whether they would participate in another hackathon, 100% of the students responded positively. Furthermore, when asked about the importance of hackathons for companies, 100% of the mentors agreed that such events are very important for the companies as well.

The impact of hackathon participation on final exam performance

The most recent hackathon was organised for second-year computer science students as part of the Web Programming course during the summer semester of the 2023/2024 academic year. A total of 88 students were enrolled in the course of whom 64 successfully passed the final exam. For analysis, these students were divided into two groups:

- Experimental group: hackathon participants (14 students, all of whom passed the exam)
- Control group: non-hackathon participants who passed the exam (50 students)

To assess the impact of hackathon participation on academic performance, Welch's t-test was conducted to compare the final exam scores between the experimental and control groups. The grading scale ranges from 6 to 10 for students who passed.

Welch's t-test was selected due to its robustness in handling groups with unequal variances.

In this study, the null hypothesis (H_0) states that there is no significant difference in final exam performance between students who participated in the hackathon and those who did not:

$$H0: \mu_{hackathon} = \mu_{non-hackathon}$$

where $\mu_{\text{hackathon}}$ represents the mean exam score of hackathon participants, and $\mu_{\text{non-hackathon}}$ represents the mean exam score of non-participants.

The alternative hypothesis (H_1) posits that hackathon participation leads to significantly higher final exam performance:

$$H1: \mu_{hackathon} > \mu_{non-hackathon}$$

Table 1: Group Statistics

Group	Sample Size (n)	Mean Scaled Mark	Standard Deviation (σ)
Experimental Group (Hackathon)	14	9.86	0.53
Control Group (Non-Hackathon)	50	8.42	1.49

Source: compiled by the author

Table 2: T-Test Results

Statistical Test	Value
T-Statistic	5.66
P-Value	4.99×10^{-7}

Source: compiled by the author

The analysis of exam performance reveals a significant impact of hackathon participation on student outcomes. The average final exam score for hackathon participants was 9.86, notably higher than the 8.42 recorded for non-participants. Furthermore, score variability was lower among hackathon participants, with a standard deviation of 0.53 compared to 1.49 in the control group, indicating more consistent performance. Inferential statistics further support these findings, as the computed t-value of 5.66 suggests a substantial difference between the two groups. The extremely low p-value of 4.99×10^{-7} confirms that this difference is highly unlikely to have occurred by chance. Consequently, the null hypothesis is rejected, and it is concluded that hackathon participation had a statistically significant positive effect on final exam performance.

These findings suggest that students who engaged in hackathons not only achieve higher scores but also demonstrated greater performance stability. This highlights

the potential of hackathon-based learning as an effective educational strategy for improving student outcomes in web programming courses. Future research should investigate the broader applicability of this approach across different academic disciplines and assess its long-term impact on knowledge retention.

Challenge-based tasks

In cybersecurity education, challenge-based tasks are hands-on activities that engage students in identifying, analysing, and justifying security threats, simulating real-world cyber challenges to build practical skills and resilience against potential vulnerabilities. These types of tasks were first implemented in the course Security in E-Business Systems. Succeeding the successful initial implementation and student feedback, the tasks were slightly adjusted and integrated into the courses Web Programming, Advanced Web Programming and Integrated Web Systems.

Assigned to students toward the end of the semester, these tasks were introduced once they had acquired sufficient theoretical and practical knowledge. Covering all recognised categories of web application security risks, the assignments primarily focused on:

- Security logging and monitoring failures
- Cryptographic failures
- Injection
- Identification and authentication failures
- Security misconfiguration

The difficulty levels varied, and some challenges spanned multiple categories of web application security.

The tasks were designed as challenge-based assignments focused on web application security. Each task was assigned a specific timeframe for completion, after which students submitted their solutions. Their submissions included program code as well as a text file that documented their experiences, challenges faced, and, if necessary, a detailed explanation of their solution. For certain tasks, students were also required to identify potential security issues and vulnerabilities, discuss how these could be mitigated, and suggest the most suitable techniques or methods for prevention. Following the submissions, a discussion was held to explore different approaches to problem-solving and to address issues encountered. These tasks were highly practical, with created code or code snippets required to be submitted by students, giving them the characteristics of code-entry challenges. In the task description, the use of AI tools was not specified, but some students chose to use them while working on tasks.

The completion of each task involved several steps, each essential for successfully finishing the assignment. Figure 2 shows the steps of challenge-based task.

Following the initial implementation of these tasks, all participants completed a survey. Based on their feedback, some adjustments were made for the next round, with additional changes planned for future activities. The implemented updates include

anonymous logging of all attempts and testing, which provides useful material for discussion, and assigning some tasks to pairs of students for collaborative work.

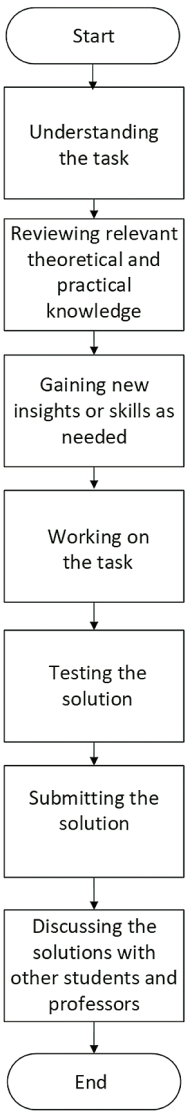


Figure 2: Steps of challenge-based task
Source: compiled by the author

During the discussion, the first focus was on analysing anonymous logs from the testing phase. The logs were reviewed to identify records that provided information indicating the correct approach to solving the problem, as well as those that demonstrated an incorrect approach or a misunderstanding of the task instructions. Following this,

a discussion of the submitted solutions took place. Interestingly, in some cases, parts of the final solutions did not differ from the information recorded during testing. Specifically, each attempt during testing received feedback from the task webpage on whether the solution was correct or not. If the response was negative, students were expected to continue working on solving the problem. The discussion and review of solutions provide a phase in which students gain new knowledge and insights into their weaknesses in a particular area. If none of the students could solve the task, the professor uploaded the solution to an internal platform. This was followed by a solution analysis, testing, and then a discussion.

The next use of this type of task is planned to be implemented in multiple iterations throughout a single semester. Each iteration will focus on a specific area covered during the coursework, with the final iteration encompassing content from the entire curriculum. Additionally, there is a plan to integrate challenge-based tasks with other new methods and to include them as part of a future research study.

The following text presents an example of a task that was given to the students.

"Visit the provided URL and analyse the HTML code of the form and the entire web page. Attempt to upload files and gather relevant information. Your objective is to locate and extract the secret word contained in the file named 'secret'. This file has no extension, and it is one level below the root directory. It is inaccessible via the browser and can only be reached through PHP code. Write PHP code to exploit the vulnerability in the web form and retrieve the contents of the 'secret' file. Once you find the secret string, decode the message to reveal the plaintext. For decoding, create a file named decode.php."

The output of this task is that students, by analysing the code of a web page, tested their knowledge of attributes essential for creating secure forms and gathered information obtained after successfully uploading files to the server.

Specifically, after a file was successfully uploaded to the server, the page displayed a message confirming that the file had been successfully uploaded. The web page with the form also displayed an image, and by analysing its URL, students could determine the directory name and its location relative to the root directory.

Next, students created a PHP script containing code that accessed the secret file, located one level below the root folder. They uploaded this file to the server via the web form. By analysing the location of the displayed image, they could attempt to directly open uploaded files in the browser. If the image was successfully displayed, this indicated that files uploaded via the form were accessible at that location. In this way, they managed to manually execute the PHP script, which reads the contents of the secret file.

The file's content was encoded, so students entered the obtained data into a separate script, *decode.php* and performed its decoding. They needed to recognise that Base64 encoding was used and apply the appropriate decoding function.

This task allowed students to identify security risks associated with such web forms and recognise vulnerabilities in the server-side code. Some key issues and security measures include:

- Restricting uploads to specific file types
- Disabling directory listing on the server
- Automatically renaming uploaded files using functions that generate unique names with additional parameters

After these initial tests of this type of task, a study is planned with an experimental and a control group to determine whether and to what extent these tasks contribute to better knowledge acquisition in web application security.

Artificial intelligence (AI) tools in education of software engineers

Incorporating Artificial Intelligence (AI) into the education of software engineers is transforming how students acquire knowledge and build practical skills. Today's learning environment extends beyond traditional resources, encompassing digital tools, online platforms, and a rapidly growing suite of AI technologies that enhance educational experience. By using AI, students can streamline and enhance their learning processes, accelerating development while working on assignments, homework, and projects.

AI tools provide students with real-time assistance, helping them debug code, optimise algorithms, and explore complex problem-solving approaches. Additionally, these tools allow students to test and analyse their projects more effectively by simulating various scenarios and identifying potential improvements. Many AI platforms also offer APIs, enabling students to integrate sophisticated AI functionalities into their applications, whether for machine learning models, natural language processing, or predictive analytics. This hands-on use of AI APIs deepens their understanding of both AI and software engineering principles, fostering skills directly applicable to the tech industry.

Moreover, by working with AI-driven tools, students are exposed to emerging trends and gain insights into ethical considerations, responsible AI use, and the impact of AI on society. In this way, AI not only supports their technical education but also prepares them to address broader issues in the field of software engineering. Integrating AI into their projects allows students to tackle real-world challenges, experiment with innovation, and develop a more versatile skill set that is critical for their future roles as software engineers.

Student tasks and AI

During the laboratory exercises in the courses Advanced Web Programming and Integrated Web Systems, students are given tasks that they need to solve during the class. The use of AI tools in solving some of the tasks is evident in the solutions that students submit to the internal service. Some students are noticeable for immediately forwarding the entire task text to AI and downloading the complete solution generated by the tool. However, most students approach the problem logically. The first thing they do is carefully review the task text to understand all the necessary

components, and then they start working on the program code. Some of them use AI tools when they need quick help with a minor issue or if they want to optimise a part of the code.

To encourage students who strictly use AI for generating solutions to read, analyse, and understand the problem in detail, they were given tasks containing illogical requirements that could affect the result and lead to a solution that functionally does not match the given problem. When these students received such solutions, they began to analyse the task text and try to solve the problem correctly.

As previously mentioned, it is important for students to be exposed to situations that are like real business environments. A new type of task was assigned to students in which they are placed in the role of project managers within an IT company primarily focused on developing software solutions.

Using AI tools and guidelines provided, students were tasked with creating a project description that would be randomly assigned to another student. The guidelines were of a technical nature: specifying which PHP classes to use, the database operations that needed to be implemented, security risks and threats, as well as a limited number of functional requirements.

Each student was required to record all input parameters provided to the AI tool, along with the responses. All conversations with the AI tool were to be documented. Based on the input parameters and the generated task description, students were also expected to request an estimation of the time required to complete the task. They had to take on the role of a project manager, using all available information about the task and the prior knowledge of their peers to estimate how long it would take to complete the task.

Once the proposed tasks and input parameters were uploaded to the internal service, the professor reviewed them and randomly assigned them to students. After completing the tasks, a group discussion was held to review all aspects of the task, with a focus on the estimated and actual time taken to complete it.

These activities have shown that incorporating AI tools into student tasks can enhance their problem-solving approach when structured thoughtfully. By designing assignments that require critical analysis, documentation, and estimation, students are encouraged to engage more deeply with the problem rather than relying solely on AI-generated solutions. This method helps bridge the gap between academic exercises and real-world software development challenges.

Integration of AI APIs in the development of tools for education

Multiple models developed by OpenAI are available, each designed to address specific purposes and use cases. Different approaches can be employed to interact with the API, with each tailored to distinct use cases.

The implementation of the AI API resulted in the creation of a web service to assist students in testing their knowledge in specific topics.

The model employed in this application is "GPT-4o Mini", which stands as the most advanced model within the category of smaller models. It is characterised by

its cost-effectiveness, speed, and efficiency. For this application, the "Chat Completion" method is utilised, as it best aligns with the specific requirements of the task. Essentially, this approach entails submitting a request to AI, which then generates and returns the corresponding output.

The application was developed using the Laravel PHP framework, along with Filament and Livewire. For data storage, the MySQL relational database management system is used.

The developed application is a web-based quiz platform where students can select the language in which they wish to receive questions, the difficulty level of the questions, and enter key terms related to the subject area for which the AI will generate the quiz. Each quiz consists of 10 questions of various types: true/false, multiple choice, and one correct choice. Data about the generated quizzes, entered key terms, and answers are stored anonymously in the database for future statistical analysis.

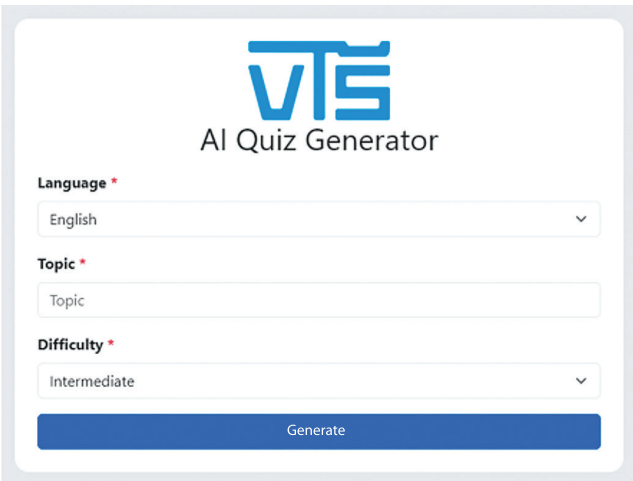


Figure 3: Index page of AQ Quiz Generator
Source: screenshot of web-based quiz platform

Future work

The plan for future research is to determine the extent to which the use of AI tools and challenge-based tasks contributes to better knowledge acquisition among students. The research would begin with an initial testing phase after which experimental and control groups would be formed. Members of the experimental group would have the opportunity to participate in challenge-based tasks and use the AI tool to test and improve their knowledge. The AI tool would offer predefined categories for generating quizzes, most likely based on material from the OWASP Top 10 and OWASP API Security Top 10 documents. After the period of using the tool and participating in challenge-based tasks, retesting would be conducted for both groups.

Another plan is to further involve companies in the future and deepen the collaboration in the field of implementing new methods in the education of software engineers. Companies would bring in their industry experience, thereby contributing to the increased awareness and knowledge of cyber threats and vulnerabilities. This approach would result in the development of experts who can quickly adapt to the demands of the labour market.

Future research will employ a structured framework involving experimental and control groups to evaluate the impact of these methodologies on student learning outcomes.

Additional studies will focus on the incorporation of more comprehensive empirical data, such as pre- and post-test results, to validate the effectiveness of AI tools and challenge-based learning tasks.

The plan for future research is to determine the extent to which AI tools and challenge-based tasks contribute to enhanced knowledge acquisition among students. The study will begin with an initial testing phase, followed by the formation of experimental and control groups. The experimental group will engage in challenge-based tasks while utilising AI tools to test and improve their knowledge. These tools will provide predefined quiz categories, likely based on materials from the OWASP Top 10 and OWASP API Security Top 10 documents. After a designated period of AI-assisted learning and participation in challenge-based tasks, both groups will undergo a retesting phase to assess knowledge retention and improvement.

Additionally, future research aims to strengthen collaboration with industry partners to integrate real-world cybersecurity challenges into educational practices. By involving companies, students will gain insights into industry-relevant security risks and best practices, ultimately developing expertise that aligns with the evolving demands of the job market.

To ensure a robust evaluation, the research will employ a structured framework with experimental and control groups, supported by empirical data such as pre- and post-test results. This approach will provide a clearer understanding of the effectiveness of AI-driven learning and challenge-based methodologies in improving student outcomes.

Conclusions

The innovative approaches outlined in this paper address critical gaps in cybersecurity education by integrating practical, real-world applications with theoretical instruction. By aligning academic curricula with industry demands, this study highlights the necessity of evolving educational practices to equip students with the skills needed to navigate the rapidly changing landscape of software engineering and cybersecurity.

In an era where secure data exchange is vital for modern systems, the demand for well-prepared software and cybersecurity engineers is greater than ever. Given the evolving nature of cyber threats, it is crucial that education in this field provides students not only with theoretical foundations but also with hands-on experience to identify and mitigate security risks effectively. Higher education must remain

dynamic, continuously adapting curricula to meet industry expectations and ensure graduates are prepared for real-world challenges.

This study explored the integration of innovative teaching methods in software engineering education, particularly in the context of cybersecurity. By embedding these methods into courses on web application and integrated web system development, the findings underscore the value of practical learning experiences in bridging the gap between academia and industry.

The results indicate that hackathon-based learning can be a highly effective strategy for improving student engagement and outcomes in web programming courses. Additionally, the integration of AI tools has proven to enhance the learning process, offering students new ways to tackle complex tasks and refine their problem-solving skills. The structured implementation of these approaches, combined with student feedback, reinforces the need for continuous evolution in educational methodologies to remain aligned with industry advancements.

Future research will further investigate the long-term impact of these strategies and their potential to shape the next generation of skilled software engineers. By refining and expanding these methods, we aim to develop an educational framework that not only enhances technical proficiency but also fosters adaptability and critical thinking – essential qualities in the ever-changing field of cybersecurity and software development.

This article is an excerpt from a presentation given at the II. Alverad-Bánki International Cybersecurity Conference on October 15, 2024.

References

Cheung, Ronald S. – Cohen, Joseph P. – Lo, Henry Z. – Elia, Fabio (2011): *Challenge Based Learning in Cybersecurity Education.* Proceedings of the International Conference on Security and Management (SAM) The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), Athens, 2011, 1–6.

Chung, Kevin – Cohen, Julian (2014): *Learning Obstacles in the Capture the Flag Model.* Proceedings of the 1st USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE).

Čović, Zlatko (2024): Threats and Vulnerabilities in Web Applications and How to Avoid Them. In Kovács, Tünde A. – Nyikes, Zoltán – Berek, Tamás – Daruka, Norbert – Tóth, László (eds.): *Critical Infrastructure Protection in the Light of the Armed Conflicts.* Cham: Springer Nature Switzerland, 93–103. Online: https://doi.org/10.1007/978-3-031-47990-8_9

Čović, Zlatko – Papp, Zoltán – Manojlović, Helena – Simon, János (2022): *Hackathon-based Teaching Method in the Training of Software Engineers*. Proceedings of the 12th International Conference on Applied Internet and Information Technologies AIIT, Zrenjanin, 2022, 108–116.

McDaniel, Lukas – Talvi, Erik – Hay, Brian (2016): *Capture the Flag as Cyber Security Introduction*. 2016 49th Hawaii International Conference on System Sciences (HICSS), Koloa, USA, 2016, 5479–5486. Online: https://doi.org/10.1109/HICSS.2016.677

Obot Affia, Abasi-amefon – Nolte, Alexander – Matulevičius, Raimundas (2022): *Integrating Hackathons into an Online Cybersecurity Course*. arXiv preprint arXiv:2202.06018. Online: https://doi.org/10.1145/3510456.3514151

Ouhbi, Sofia – Pombo, Nuno (2020): *Software Engineering Education: Challenges and Perspectives*. IEEE Global Engineering Education Conference (EDUCON), Porto, Portugal, 2020, 202–209. Online: https://doi.org/10.1109/EDUCON45650.2020.9125353

OWASP API Security Top 10 (2024). Online: https://owasp.org/API-Security/

OWASP Top 10 (2024). Online: https://owasp.org/www-project-top-ten/

Serbian Cybersecurity Challenge (2024). Online: https://sajberheroj.rs/en/scc/

Švábenský, Valdemar – Čeleda, Pavel – Vykopal, Jan – Brišáková, Silvia (2021): Cybersecurity Knowledge and Skills Taught in Capture the Flag Challenges. *Computers & Security,* 102. Online: https://doi.org/10.1016/j.cose.2020.102154

Švábenský, Valdemar – Vykopal, Jan – Cermak, Milan – Laštovička, Martin (2018): *Enhancing Cybersecurity Skills by Creating Serious Games.* Proceedings of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education, Larnaca, 2018, 194–199. Online: https://doi.org/10.1145/3197091.3197123

Žagar, Mario – Bosnić, Ivana – Orlić, Marin (2008): *Enhancing Software Engineering Education: A Creative Approach*. Proceedings of the 2008 International Workshop on Software Engineering in East and South Europe (SEESE '08), New York, 51–58. Online: https://doi.org/10.1145/1370868.1370878

Tartalom