HADMÉRNÖK

Kiemelt közlemények

17. évf. (2022)
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: Bujdosó Hajnalka, Gergely Zsuzsánna, Resofszki Ágnes

Tartalom

Védeleminformatika

Fórum

HADMÉRNÖK
BIZTONSÁGTECHNIKA

17. évfolyam (2022) 4. szám 5–16.
DOI: 10.32567/hm.2022.4.1

Bak Gerda,[1] Kovács Tibor,[2] Őszi Arnold[3]

A biometrikus azonosítás megítélése – 1. rész

Assessment of Biometric Identification – Part 1

Dr. Kovács Tibor emlékére ajánljuk

A technológiai fejlődés és a biztonság iránti igény növekedésének következtében egyre több helyen találkozhatunk a biometrikus azonosítás különböző módjaival; jelen van az okostelefonokban, illetve számos vállalkozás is alkalmazza, felismerve annak előnyeit.

Jelen tanulmány azt hivatott felmérni, hogy a felhasználók körében a biometrikus azonosításról milyen vélemények alakultak ki, illetve miként vélekednek ezekről a módszerekről. A kutatás jelentősége abban rejlik, hogy 2006-ban és 2014-ben az Óbudai Egyetem keretein belül már lezajlott két hasonló céllal megfogalmazott kutatás, amelyet a jelen kutatás során igyekeztünk folytatni, valamint továbbvinni.

Az első rész a felmérés azon részét hivatott bemutatni, amely a megkérdezettek biometrikus azonosítási rendszerek ismertségével és használatával foglalkozik. Az eredmények alapján elmondható, hogy a biometrikus azonosítás kapcsán a felhasználók ismeretei bővítésre szorulnak, mivel még mindig sokan csak használják ezeket a technológiákat a hozzá tartozó tudásanyag és tudatosság nélkül.

Kulcsszavak: **biometrikus azonosítás, megítélés, elfogadottság, 2006, 2014, 2021**

Nowadays, biometric identification is becoming more and more common, as it is present in smartphones and is also used by many businesses that recognise its benefits.

[1] Óbudai Egyetem Biztonságtudományi Doktori Iskola, e-mail: bak.gerda@uni-obuda.hu
[2] Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, e-mail: kovacs.tibor@bgk.uni-obuda.hu
[3] Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, e-mail: oszi.arnold@bgk.uni-obuda.hu

This study aims to assess the perceptions and opinions of users on biometric identification. The significance of the research lies in the fact that two studies with similar aims were conducted in 2006 and 2014, also at Óbuda University, which we tried to continue and further develop in the present research.

The first part presents the part of the survey dealing with respondents' awareness and use of biometric identification systems. Based on the results, it can be said that the users' knowledge of biometric identification needs to be expanded, as many people still simply use these technologies without the corresponding knowledge and awareness.

Keywords: **biometric identification, perception, acceptance, 2006, 2014, 2021**

1. Bevezetés

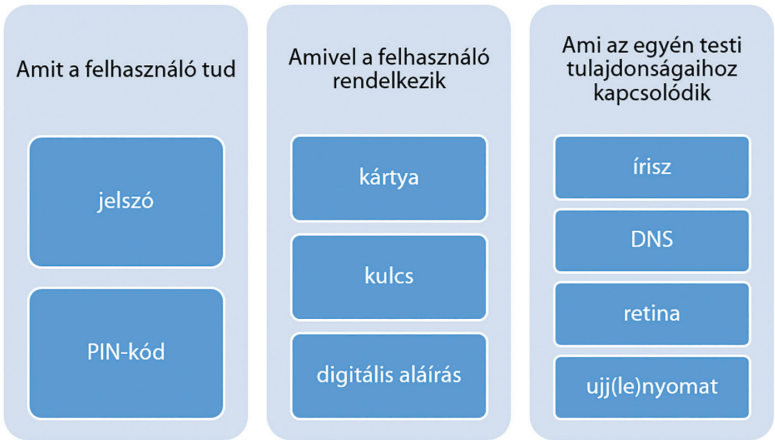
A biometrikus azonosítás iránti igény az elmúlt években megsokszorozódott, amit mi sem bizonyít jobban, mint a rendszer elterjedtsége, sokrétű felhasználtsága és a biometrikus rendszerek piaci részesedése. A Statista[4] adatai alapján a digitális személyazonosítási rendszerek piaci értéke a következő évek során a kétszeresére nő, ami közel 50 milliárd dollárt jelent világszerte, továbbá a biometrikus rendszerekre költött összeg 2025-re globálisan elérheti a 68,6 milliárd dollárt is.

Azonban a biometrikus rendszerek adta kényelemnek számos kockázata is van: az egyes szenzorok megtéveszthetők, az egyén biometrikus adatait tároló adatbázis vagy akár a hálózat célpontja lehet a támadóknak.[5] Az IBM[6] online felméréséből kiderül, hogy bár a megkérdezettek számára fontos a kényelem a különböző applikációkba és alkalmazásokba történő bejelentkezés során, a biztonságot fontosabbnak ítélik meg. Az is kiderült, hogy a megkérdezettek 67%-ának nem okoz gondot valamilyen biometrikus azonosítási módot alkalmazni, 44%-uk az ujjnyomatot mint azonosítási módot tekinti a legbiztonságosabbnak, illetve a pénzügyi alkalmazások kapcsán tekintik igazán lényegesnek a biztonságot, a közösségi média applikációinak esetében pedig a kényelmes, gyors bejelentkezés a fő szempont.

A felhasználók azonban hajlamosak egyszerű, könnyen megjegyezhető jelszavakat, PIN-kódokat használni, amelyeket viszonylag ritkán változtatnak meg, ezzel is növelve a kockázatot.[7]

A digitális technológia fejlődésével és használatával számos információ keletkezik, valamint tárolódik a számítógépeken, telefonokon vagy akár az interneten egyetlen nap leforgása alatt is. Ezeket a tartalmakat pedig érdemes, sőt ajánlott gondosan őrizni, jelszavakkal, azonosítókkal védeni. A jelenlegi technológiát tekintve három azonosítási, hitelesítési módot különböztetünk meg, illetve létezik egy negyedik is, azonban az csak az ötvözete az első két módnak, ezt mutatja be a következő, 1. ábra.

[4] Liu 2021.
[5] Földesi 2015; Rui–Yan 2019; Dargan–Kumar 2020.
[6] IBM 2021.
[7] Shen–Chen–Guan 2018.



1. ábra: Az egyén azonosítási módjainak típusai
Forrás: a szerzők szerkesztése Datta et al. 2020 és Szűcs–Őszi–Kovács 2020 alapján

Jelen kutatás a következőkben a felsorolás utolsó, vagyis az egyén fizikai sajátosságaival foglalkozó azonosítási módokra terjed ki.

2. Biometrikus azonosítás

A biometrikus azonosítás az emberek automatikus hitelesítését jelenti fiziológiai vagy viselkedésbeli jellemzőik vagy tulajdonságaik alapján.[8] A viselkedésbeli jellemzők egyik jelentős hátránya, hogy az idő előrehaladtával változhatnak (mutálódik a hang, változik az aláírás képe, dinamikája), ezzel szemben a fizikai tulajdonságaink, mint az ujj(le)nyomat, nem, mint ahogy a DNS-ünk sem.[9] Azonban a fiziológiai jellemzőknek is van néhány hátránya. Először is, másolhatók: az ujjlenyomatok és a kézgeometria könnyen újraalkotható;[10] másodszor, a fiziológiai jellemzők külső hatásra könnyen torzulnak vagy megváltoznak (például a hegek vagy zúzódások megváltoztatják az ujjlenyomatokat, az arc különböző pózai összezavarhatják az arcfelismerő rendszert);[11] harmadszor, a fiziológiai jellemzők mindig speciális hardveres támogatást igényelnek. Másrészt az okostelefonokban rendelkezésre álló különféle szenzorok, például az érintőképernyő és a mozgásérzékelők képesek átfogó információk hatékony gyűjtésére. Ezért a viselkedésbeli biometria az okostelefon-hitelesítés egyik kutatási fókuszpontjává vált.[12]

A biometrikus rendszerek kapcsán a szakirodalom különbséget tesz az unimodális és a multimodális rendszerek között: míg az unimodális rendszer egyetlen biometrikus tulajdonság alapján hitelesíti, értékeli a felhasználót, addig a multimodális kettő vagy több biometrikus jellemző alapján végzi el ugyanezt, ezzel is növelve a rendszer

[8] Flynn–Jain–Ross 2008; Hazai 2019.
[9] Sarhan–Alhassan–Elmougy 2016.
[10] Tamviruzzaman et al. 2009.
[11] Jain–Ross–Prabhakar 2004.
[12] Shen–Chen–Guan 2018. 9.

megbízhatóságát és pontosságát.[13] Az unimodális rendszerek hátránya lehet a nem megfelelő állapotban tartott érzékelő, aminek következtében a szenzor deformált vagy zajos adatokat eredményezhet, illetve a megkülönböztethetőség is gondot okozhat a rendszernek: a felhasználó nem megfelelő módon lép interakcióba a szenzorral (nem jól tartja az ujját az érzékelőhöz, túl közel vagy távol áll stb.), vagy a felhasználók körének növekedésével előforduló hasonló karakterisztikájú egyének átfedéseket okozhatnak, ami ronthatja a rendszer pontosságát.[14]

A fenti problémák mellett az unimodális biometrikus rendszerek további hátrányokkal is küzdenek, ezek a problémák pedig magasabb hamis elutasítási arányhoz (*false reject rate,* FRR) és hamis elfogadási arányhoz (*false accept rate,* FAR) vezetnek.[15] A biometrikus azonosító rendszerek pontosságának, teljesítményének értékelésére az előbb említett két mutatón kívül még létezik az egyenlő hibaarány (*equal-error rate,* ERR), ami azt a pontot jelöli, ahol az FRR és FAR értéke egyenlő.[16]

3. Módszertan

A kutatáshoz kérdőíves vizsgálati módot alkalmaztunk, amelynek adatbegyűjtési időszaka 2021. október 23. – 2021. december 12. közé esett, hólabda módszerrel. A kérdőívet online és papír formában is terjesztettük, ami 209 kitöltést eredményezett. Az adatok nem tekinthetők reprezentatívnak, elemzésük IBM SPSS 26 programmal történt.

A kérdőív két fő részből tevődött össze: az általános demográfiai részből és a biometrikus azonosítással kapcsolatos részből. A kérdések zárt formában, illetve Likert-skála segítségével voltak megválaszolhatók.

A kutatás legelején négy fő kérdés fogalmazódott meg, amelyek a következőkben láthatók. A negyedik, egyben utolsó kutatási kérdésre a tanulmány második részében kapnak helyet az eredmények.

Kutatási kérdések:

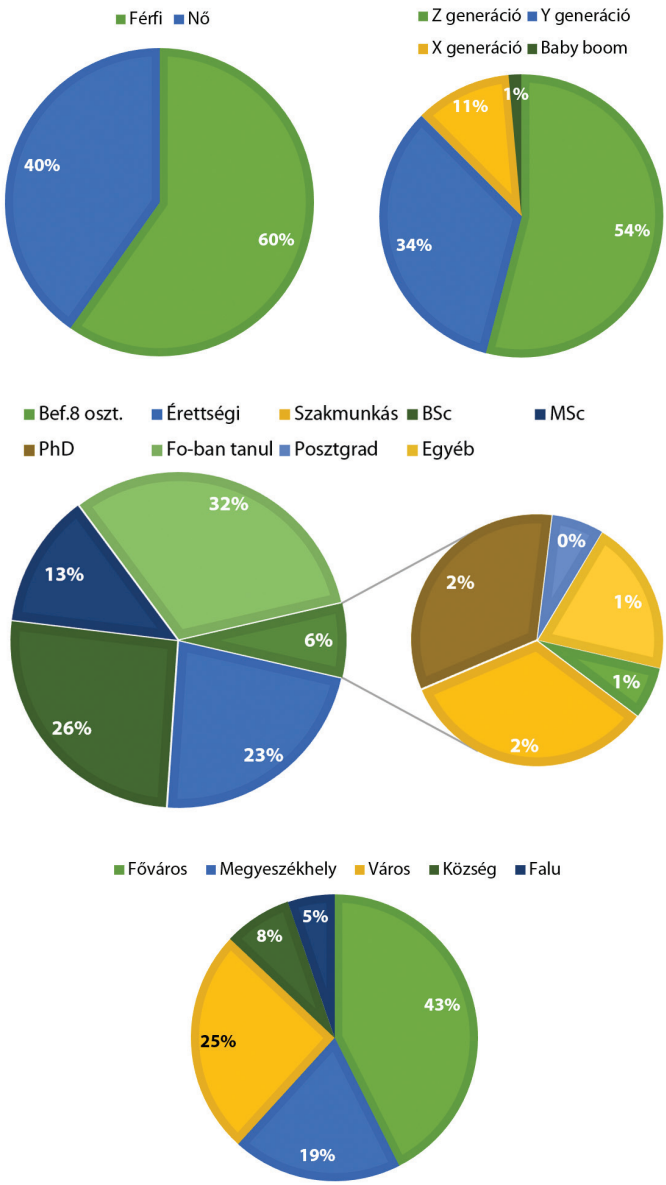
- Mely biometrikus azonosítási rendszereket használják a hétköznapokban az okostelefonjaikon?
- Mennyire elfogadottak ezek a rendszerek a hétköznapokban?
- Van-e különbség a biometrikus azonosítási rendszerek megítélésében a nemek tekintetében?
- Miként vélekednek az emberek a biometrikus azonosítási rendszerekről?

3.1. Minta bemutatása

A kérdőív kitöltőiről nemek szerinti bontásban elmondható, hogy a férfiak nagyobb arányban (60%), főként Z generációs fiatalok (54%) töltötték ki, akik jelenleg is a felsőoktatásban tanulnak (Fo.-ban tanul) (32%), illetve többségében a fővárosban (43%)

[13] Ammour–Bouden–Boubchir 2018.
[14] Gad et al. 2015.
[15] Kovács–Földesi 2021; Devi–Sujatha 2017.
[16] Fejes 2018.

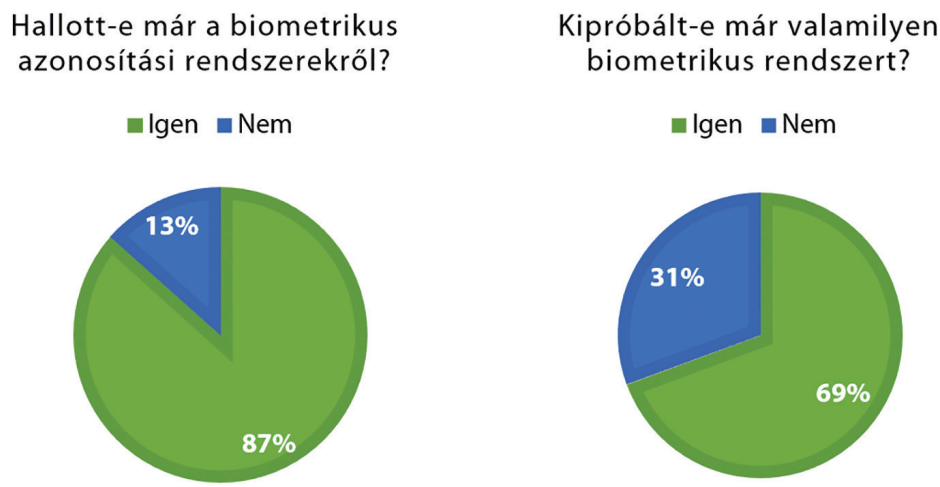
laknak. A kitöltők leíró statisztikai jellemzőit a 2. ábra foglalja össze. A kitöltők között legkisebb arányban a baby boom generáció képviselte magát. A képzettséget tekintve a befejezett 8 osztállyal rendelkezők, a posztgraduális képzést végzettek, a szakmunkásban tanultak, valamint az egyéb képzést végzők szerepeltek alacsony arányban. A lakhelyet tekintve pedig a faluban és községben élőkhöz jutott el kis arányban a kérdőív.



2. ábra: A kérdőív kitöltőinek leíró statisztikája (n = 209)
Forrás: a szerzők szerkesztése a minta adatai alapján

4. Eredmények

A kérdőív első felében megkérdeztük, hogy a kitöltők hallottak-e már róla, illetve kipróbáltak-e már valamilyen biometrikus azonosítási rendszert. Az alábbi, 3. ábra ennek a két kérdésnek az eredményeit mutatja be. Ahogy az látható, a kitöltők 87%-a hallott már erről, illetve 69%-uk ki is próbált már legalább egy biometrikus azonosítási módot.



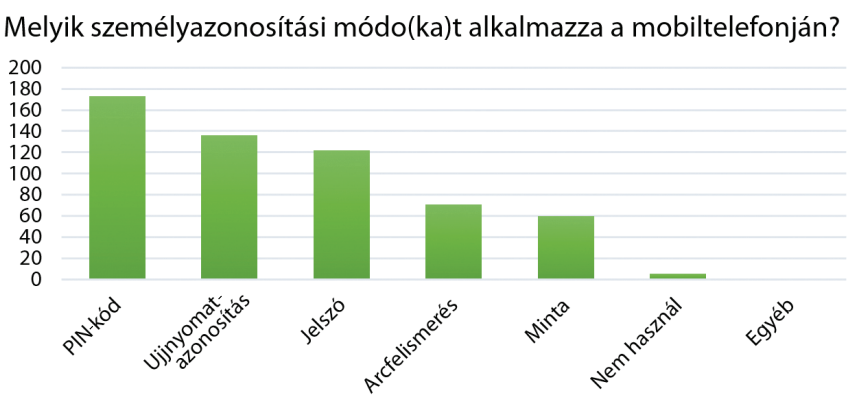
3. ábra: A kitöltők megoszlása aszerint, hogy hallottak-e róla, illetve kipróbáltak-e már valamilyen biometrikus azonosítási módszert (n = 209)

Forrás: a szerzők szerkesztése a minta adatai alapján

Az előbb ábrázolt eredmények két szempontból is jelentősek, illetve érdekesek. Egyrészt érdekesek, mivel a kérdőív további részében, amikor arra kerestük a választ, hogy a megkérdezettek milyen azonosítási módokról hallottak, akkor a kitöltők kivétel nélkül minimum egy azonosítási formát jelöltek az előre megadott opciók közül. Továbbá arra is kerestük a választ, hogy a mobiltelefonjukon milyen azonosítási módo(ka)t alkalmaznak: néhány (5 db) válaszadó kivételével mindegyik alkalmaz valamit. A 4. és 5. ábra az előbb tárgyalt két kérdésre adott válaszokat mutatja be. Mind a két kérdés esetén több válasz megjelölése is lehetséges volt. Ahogy azt az ábra is mutatja, a legismertebb azonosítási módszer az ujjnyomat-azonosítás, amelyet 208 kitöltő ismer, ezt követi a PIN-kód 204 és a jelszó 203 jelöléssel. Az előre felsorolt azonosítási módok közül a legkevésbé ismert a DNS-azonosítás, 92 fő nyilatkozta a módszer ismeretét. A válaszokat tekintve az *egyéb* opciót is jelölhették a kitöltők, ahol megnevezhettek további, számukra ismert módozatokat is. Az egyebek között az írisz-, retinavizsgálat, vénaszkenner fordultak elő többnyire, de említették az aláírást és a mozgáselemzést is.

4. ábra: A válaszadók által ismert személyazonosítási módok (n = 209)
Forrás: a szerzők szerkesztése a minta adatai alapján

A válaszadók által a mobiltelefonokon alkalmazott azonosítási módokat ábrázolja az 5. ábra, itt is több válaszadási lehetőség volt. Látható, hogy a leggyakoribb azonosítási módszer a megkérdezettek körében a PIN-kód 173 válaszadóval, ezt követi 136 jelöléssel az ujjnyomatos feloldás, illetve 122 jelöléssel a jelszó. A legkevésbé előnyben részesített mobiltelefon-feloldási mód a minta, amelyet 60 válaszadó alkalmaz, továbbá 5 kitöltő úgy nyilatkozott, hogy nem használ semmilyen feloldási módot, vagyis bárki feloldhatja a mobiltelefonját. Az általunk előre megadott azonosítási módok mellett a kitöltőknek természetesen lehetőségük volt megnevezni egyéb azonosítási módot is, amennyiben azt alkalmazzák az okostelefonjukon; egy válaszadó jelezte, hogy ő egy általunk nem nevesített módszert is használ, méghozzá a QR-kódos azonosítást.

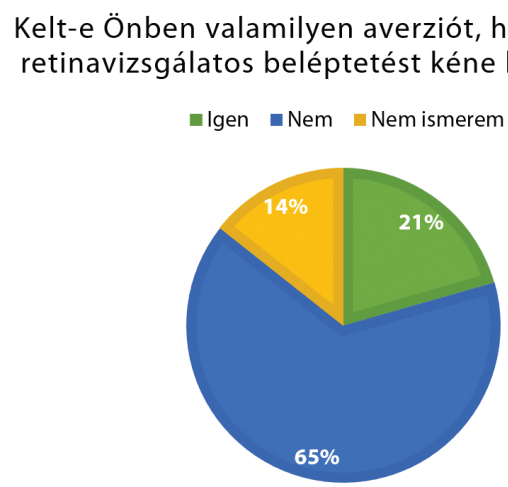


5. ábra: A válaszadók által személyazonosításra használt mobiltelefon-feloldási módok (n = 209)
Forrás: a szerzők szerkesztése a minta adatai alapján

A kérdőív biometrikus azonosítási rendszerek elfogadottságát vizsgáló része előtt négy olyan kérdést tettünk fel a kitöltőknek, amelyek egyrészt átvezetésül szolgálnak a mélyebb kérdésekhez, másrészt a segítségükkel általános képet kaphatunk a felhasználók biometrikus azonosítási módszerekkel szembeni véleményéről és hozzáállásáról. Az említett kérdések esetében, az első kivételével, ötfokozatú Likert-skálán kellett a válaszadóknak jelölniük a válaszukat. A négy kérdés a következő:

- Keltene-e önben valamilyen averziót, ha írisz- vagy retinavizsgálatos beléptetést kellene használnia?
- Általában mennyire tartja korszerűnek a biometrikus azonosításon alapuló beléptetési lehetőséget?
- Ön szerint mennyire könnyű/egyszerű egy biometrikus rendszer használata?
- Mennyire találja gyorsnak a biometrikus azonosítási folyamatot?

A fentebb említett kérdések közül az elsőre – azaz, hogy kelt-e bennük bármilyen kellemetlen, rossz érzést az írisz- vagy retinavizsgálatos beléptetési módszer alkalmazása – adott válaszokat szemlélteti a 6. ábra. Az eredmények alapján elmondható, hogy a megkérdezettek több mint a felét (65%) nem töltené el rossz érzés, ha az írisz- vagy retinavizsgálatos beléptetési módszert kellene használniuk. Ezzel szemben 21%-ot zavarna, valamint 14% a saját elmondása alapján nem ismeri a fent nevezett módszert.

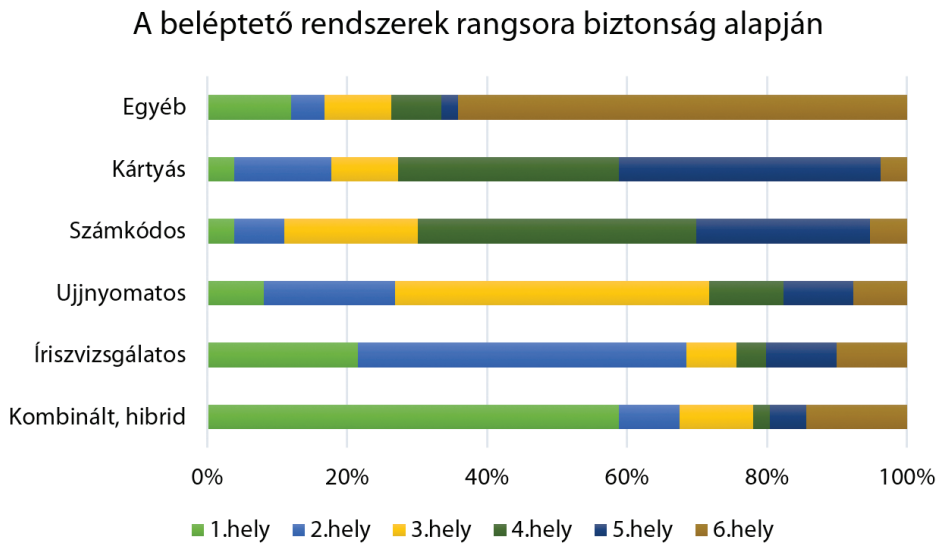


6. ábra: Írisz- vagy retinavizsgálatos beléptetéssel szembeni averzió megjelenése a válaszadók körében (n = 209)

Forrás: a szerzők szerkesztése a minta adatai alapján

A kérdőív során arra kértük a kitöltőket, hogy rangsorolják az egyes biometrikus azonosítási módokat aszerint, hogy melyiket tartják a legbiztonságosabbnak és melyiket a legkevésbé. A 7. ábra ennek eredményeit mutatja be. Az eredmények értelmében elmondható, hogy a megkérdezettek közel 60%-a (58,85%) a kombinált, hibrid módszereket ítéli meg a legbiztonságosabbnak, ezt követi az íriszvizsgálat 46,89%-kal,

az ujjnyomatos 44,98%-kal, a legkevésbé biztonságosnak az egyéb beléptetési módot jelölték 64,11%-kal.



7. ábra: Az egyes biometrikus beléptetési rendszerek megítélése biztonság szempontjából (n = 209)
Forrás: a szerzők szerkesztése a minta adatai alapján

5. Következtetések

A jelen kutatási részt tekintve az látható, hogy a felhasználók sokrétűen és elterjedten használják a biometrikus azonosítási rendszereket. Az eredmények tükrében elmondható, hogy az általunk megkérdezettek körében is nagy elfogadottságnak örvendenek a biometrikus azonosítási módok, különös tekintettel az okostelefonokon. Hayiel Hino az online vásárlás kapcsán vizsgálta, hogy mely tényezők befolyásolják a biometrikus azonosítás elfogadottságát, és arra a következtetésre jutott, hogy többek között az észlelt adatvédelem mértéke, a társadalmi befolyás és a technológiával való ismeretség (tapasztalat) jelentősek. A megkérdezettek szinte mindegyike kettő vagy több azonosítási módról hallott, illetve használja is. A különböző beléptető rendszerek, valamint az azokról alkotott biztonsági megítélés is a többség esetében megfelelő.[17] Lauren Norfolk és Michael O'Regan kutatása hasonló eredményeket hozott; a szerzőpáros az ujj(le)nyomat használatának elfogadottságát vizsgálta a zenei fesztiválokon, ahol a válaszadók majdnem 71%-a vélekedett úgy, hogy szívesen használná, 68,5%-uk az arcfelismerőt is komfortosnak tekinti.[18] Michele Cornacchia,

[17] Hino 2015.
[18] Norfolk–O'Regan 2020.

Filomena Papa és Bartolomeo Sapio szintén speciális közönséget vizsgálva jutott hasonló eredményekre; kutatásuk a hangazonosító rendszerek alkalmazásának elfogadottságát mérte a Milánó-Linatei nemzetközi repülőtéren, ahol a megkérdezettek szintén pozitívan viszonyultak a rendszerhez, elfogadhatónak tartották a használatát.[19]

6. Összefoglalás

A kutatás eredményei alapján elmondható, hogy bár a különféle biometrikus azonosítási módszerek rendkívül elterjedtek, a felhasználók egy része csak használja azokat, a használat mögül pedig hiányzik a kellő tudatosság. Ezt támasztja alá az is, hogy a válaszadók nagy része a saját mobiltelefonja feloldásához is biometrikus azonosítási módot használ (ujjnyomat-azonosítás, arcfelismerés), mégis, közülük sokan azt nyilatkozták, hogy még nem próbáltak ki egyetlen biometrikus azonosítási rendszert sem. Az eredmények másik érdekességét az adja, hogy a biometrikus rendszerek biztonság szerinti rangsorolásánál helyesen jelölték a kitöltők, hogy a kombinált, hibrid rendszerek számítanak a legbiztonságosabbnak, megelőzve az ujjnyomatos, illetve a kártyás módokat, amelyek megtéveszthetőbbek, illetve a kártya sérülékenyebb és el is tulajdonítható. Ez viszont azt feltételezi, hogy bizonyos információkkal, tudással rendelkeznek a témában, még ha akadnak is hiányosságok, illetve az egyes kifejezések kapcsán is érdemes lenne rendet tenni.

Az eredmények alapján megállapítható, hogy az általunk megkérdezettek igénylik és használják is a különféle azonosítási módokat, amelyek révén növelhetik adataik, személyük és mobiltelefonjuk biztonságát. Azonban a biometrikus azonosítási módok általánosítása területén hatalmas eltérések találhatók. Az azonosítási módok megítélése pozitív, nyitottak a használatukra, ám az egyének a biometrikus adataik rögzítése kapcsán már negatívabban vélekednek.

Felhasznált irodalom

Ammour, Basma – Bouden, Toufik – Boubchir, Larbi (2018): Face-Iris Multimodal Biometric System Based on Hybrid Level Fusion. In *2018 41st International Conference on Telecommunications and Signal Processing (TSP)*. IEEE. 1–5. Online: https://doi.org/10.1109/TSP.2018.8441279

Cornacchia, Michele – Papa, Filomena – Sapio, Bartolomeo (2020): User Acceptance of Voice Biometrics in Managing the Physical Access to a Secure Area of an International Airport. *Technology Analysis & Strategic Management,* 32. évf. 10. sz. 1236–1250. Online: https://doi.org/10.1080/09537325.2020.1758655

Dargan, Shaveta – Kumar, Munish (2020): A Comprehensive Survey on the Biometric Recognition Systems Based on Physiological and Behavioral Modalities. *Expert Systems with Applications,* 143. évf. 113114. Online: https://doi.org/10.1016/j.eswa.2019.113114

[19] Cornacchia–Papa–Sapio 2020.

Datta, Priyanka – Bhardwaj, Shanu – Panda, S. N. – Tanwar, Sarvesh – Badotra, Sumit (2020): Survey of Security and Privacy Issues on Biometric System. In *Handbook of Computer Networks and Cyber Security.* Cham, Springer. 763–776. Online: https://doi.org/10.1007/978-3-030-22277-2_30

Devi, R. Subathra – Sujatha, Pothula (2017): A Study on Biometric and Multi-Modal Biometric System Modules, Applications, Techniques and Challenges. In *2017 Conference on Emerging Devices and Smart Systems (ICEDSS).* IEEE. 267–271. Online: https://doi.org/10.1109/ICEDSS.2017.8073691

Fejes Attila (2018): Beszéd alapján történő személyazonosítás új kihívásai a kriminalisztikában. *Magyar Rendészet,* 18. évf. 2. sz. 117–126.

Flynn, Patrick J. – Jain, Anil K. – Ross, Arun A. (2008): Introduction to Biometrics. In *Handbook of Biometrics.* Boston, MA, Springer, 2008, 1–22.

Földesi Krisztina (2015): Paradigmaváltás a biztonságtechnikában — miért alkalmazzunk biometrikus rendszert? *Magyar Rendészet,* 15. évf. 3. sz. 37–48.

Gad, Ramadan – El-Sayed, Ayman – El-Fishawy, Nawal – Zorkany, M. (2015): Multi-Biometric Systems: A State of the Art Survey and Research Directions. *(IJACSA) International Journal of Advanced Computer Science and Applications,* 6. évf. 6. sz. 128–138. Online: https://doi.org/10.14569/IJACSA.2015.060618

Hazai Lászlóné (2019): Módszerek, technikák a biometrikus arcfelismerésben, -azonosításban. *Belügyi Szemle,* 67. évf. 1. sz. 118–126. Online: https://doi.org/10.38146/BSZ.2019.1.9

Hino, Hayiel (2015): Assessing Factors Affecting Consumers' Intention to Adopt Biometric Authentication Technology in E-shopping. *Journal of Internet Commerce,* 14. évf. 1. sz. 1–20. Online: https://doi.org/10.1080/15332861.2015.1006517

IBM (2018): IBM Security: Future of Identity Study. *IBM*, 2021. december 10. Online: www.ibm.com/downloads/cas/PL9VJ9KV

Jain, Anil K. – Ross, Arun – Prabhakar, Salil (2004): An Introduction to Biometric Recognition. *IEEE Transactions on Circuits and Systems for Video Technology,* 14. évf. 1. sz. 4–20. Online: https://doi.org/10.1109/TCSVT.2003.818349

Kovács Tibor – Földesi Krisztina (2021): Összehasonlító kutatáselemzés a biometrikus személyazonosító-beléptető rendszerek, eljárások 2006. és 2014. évi társadalmi averzív reakcióinak vizsgálatára. *SecureInfo,* 2021. december 10. Online: www.securinfo.hu/wp-content/uploads/2015/06/20150602_osszehasonlito_elemzes_a_biometrikus_szemelyazonosito_rendszerek.pdf

Liu, Shanhong (2021): Biometric Technologies – Statistics & Facts. *Statista,* 2021. október 30. Online: www.statista.com/topics/4989/biometric-technologies/#dossierKeyfigures

Norfolk, Lauren – O'Regan, Michael (2020): Biometric Technologies at Music Festivals: An Extended Technology Acceptance Model. *Journal of Convention & Event Tourism,* 22. évf. 1. sz. 36–60. Online: https://doi.org/10.1080/15470148.2020.1811184

Rui, Zhang – Yan, Zheng (2019): A Survey on Biometric Authentication: Toward Secure and Privacy-Preserving Identification. *IEEE Access,* 7. évf. 5994–6009. Online: https://doi.org/10.1109/ACCESS.2018.2889996

Sarhan, Shahenda – Alhassan, Shaaban – Elmougy, Samir (2016): Multimodal Biometric Systems: A Comparative Study. *Arabian Journal for Science and Engineering,* 42. évf. 2. sz. 443–457. Online: https://doi.org/10.1007/s13369-016-2241-0

Shen, Chao – Chen, Yufei – Guan, Xiaohong (2018): Performance Evaluation of Implicit Smartphones Authentication via Sensor-Behavior Analysis. *Information Sciences,* 430–431. évf. 538–553. Online: https://doi.org/10.1016/j.ins.2017.11.058

Szűcs, Kata Rebeka – Őszi, Arnold – Kovács, Tibor (2020): Mobile Biometrics and their Risks. *Hadmérnök,* 15. évf. 4. sz. 15–28. Online: https://doi.org/10.32567/hm.2020.4.2

Tanviruzzaman, Mohammad – Ahamed, Sheikh Iqbal – Hasan, Chowdhury Sharif – O'Brien, Casey (2009): ePet: When Cellular Phone Learns to Recognize Its Owner. In *SafeConfig '09: Proceedings of the 2nd ACM Workshop on Assurable and Usable Security Configuration.* ACM. 13–18. Online: https://doi.org/10.1145/1655062.1655066

HADMÉRNÖK
HADITECHNIKA
17. évfolyam (2022) 4. szám 17–28.
DOI: 10.32567/hm.2022.4.2

Gajdács László[1]

Pilóta nélküli légi jármű érzékelésének lehetséges megoldásai

Possible Solutions for Unmanned Aircraft Vehicle Detection

Napjainkban a drónok kiemelt figyelmet kapnak világszerte. Egyre növekvő számban jelennek meg a különböző típusok polgári, kereskedelmi, valamint közszolgálati felhasználásban is. Egyre szélesebb körű felhasználása viszont számos kihívást jelent a hatósági szerveknek. A drónok integrálása a légi közlekedésbe jelenleg is zajlik. Kellő odafigyelést és éberséget követel az egyéb „hagyományos" légi járművet vezető hajózó állománytól is, hiszen ezek az eszközök sokszor váratlanul jelennek meg az égbolton, és jelenlétük a legtöbb esetben alig észrevehető. A cikkben összegyűjtöm azokat a fizikai alapokon nyugvó műszaki megoldásokat, amelyek segítségével információt kaphatunk a pilóta nélküli légi járművek jelenlétéről, hollétéről, illetve nyomon követhetjük tevékenységüket.

Kulcsszavak: **drón, detektálás, radar, felderítés, elektromágneses jel**

Nowadays, drones are getting a lot of attention worldwide. They are becoming more and more common in various types of civil, commercial and public service use.

Their increasing use poses a number of challenges for public authorities. The integration of drones into air transport is still in the particular focus of attention, as it is currently being implemented. It also requires a high level of attention and vigilance on the part of the crews of other "conventional" aircraft, as they often appear unexpectedly in the sky and in most cases their presence is hardly noticeable. In this article, I will collect technical solutions based on physical sub-systems that can be used to obtain information on the presence and whereabouts of unmanned aerial vehicles and to monitor their activities.

Keywords: **drone, detection, radar, reconnaissance, electromagnetic signal**

[1] Tanársegéd, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Repülőfedélzeti Rendszerek Tanszék; doktori hallgató, e-mail: gajdacs.laszlo@uni-nke.hu

1. Bevezetés

A pilóta nélküli légi járművek használata nem új keletű. A történelem folyamán különböző céllal készültek ilyen repülőgépek, de alapvetően katonai feladatok végrehajtására tervezték őket.

E területtel ismerkedve számos rövidítéssel találkozhatunk, amelyek a hosszú évek folyamán alakultak ki velük kapcsolatosan, például:

- UAV – *unmanned aerial vehicle*: pilóta nélküli légi jármű;
- UAS – *unmanned aircraft system*: pilóta nélküli légijármű-rendszer;
- RPA – *remotely piloted aircraft*: távirányítható légi jármű;
- RPAS – *remotely piloted system*: távirányítható légijármű-rendszer stb.[2]

„Hagyományos" – pilótával vezetett – légi járművek felderítéséhez és mozgásuk nyomon követéséhez régóta használnak műszaki megoldásokat úgy a polgári, mint a katonai repülésben. Azonban a pilóta nélküli légi járművek felderítésének megvalósítása és annak hatékony alkalmazása még várat magára. Ennek oka részben az, hogy ezek a tárgyak méretükből adódóan nehezen észrevehetők, érzékelhetők. Alkalmazásukkal párhuzamosan szeretnénk információval rendelkezni aktuális pozíciójukról, illetve hogy milyen irányba szeretnék tevékenységüket folytatni. A repülésben ez nélkülözhetetlen, nélküle mintha vakon repülnénk, nem látva és nem érzékelve a környezetünkben jelen lévőket. Ezekre az információkra szüksége van egyrészt a légi irányításért felelős szervezetnek, de leginkább a légtérben közlekedő repülőgépek hajózó állományának, illetve a drónokat üzemeltető személynek is.

Szükséges „látni" a repülőeszközöket, és „láthatónak" is lenni a levegőben az egyéb légi közlekedők számára. Ha e két feltételnek meg tudnánk feleltetni a drónokat, akkor megjelenésük a légtérben sokkal kevesebb kockázattal járna.

A repülőgépek jelenlétének érzékelése, nyomon követése különböző módokon lehetséges. Lehetőség van a légi járművek által kibocsátott hang, hő alapján érzékelni azokat, és helyzeti információt kapni jelenlétükről, például a hagyományos RADAR[3]- és/vagy LiDAR[4]-technológiák segítségével.[5]

Ebben a cikkben a különböző, már létező műszaki rendszerek pilóta által vezetett légi járművek érzékelésének lehetséges műszaki megoldásait foglalom össze, amelyek megoldást nyújthatnak a pilóta nélküli légi járművek érzékelésére is.

2. Légi járművek detektálásának módjai

Különböző műszaki rendszerek különféle mozgó célok érzékelésére szolgálnak, annak függvényében, hogy a légi jármű milyen információkat bocsát ki magából és/vagy

[2] Ujjady–Major 2021.
[3] Radio direction and ranging.
[4] Light detection and ranging.
[5] Makkay 2014a.

ver vissza, és ezeket milyen módon képes az adott „érzékelő rendszer" feldolgozni. A dinamikusan mozgó célokat az alábbi módokon van lehetőségünk felderíteni és adott esetben figyelemmel kísérni:

- elektroakusztikai méréssel, iránymméréssel;
- elektromágneses hullámtartomány érzékelésével, ezen belül:
  - az eszköz által kisugárzott rádiójelek érzékelésével (passzív);
  - radarrendszerekkel való érzékeléssel (aktív);
- elektrooptikai rendszerekkel való érzékeléssel.[67]

3. Elektroakusztikai eljárás légi járművek felderítésére

A műszaki berendezések, rendszerek által keltett zajfajták az ember érzékszerveivel sok esetben észlelhetők. A különböző hangtípusok felismerése az emberi agy képességén alapul. A hangok azonosítása alapvetően függ a hang kibocsátásának helyétől, annak irányától és az érzékelés helyének távolságától, továbbá a hang intenzitásától vagy frekvenciájától, valamint az érzékelő eszköz érzékenységétől.

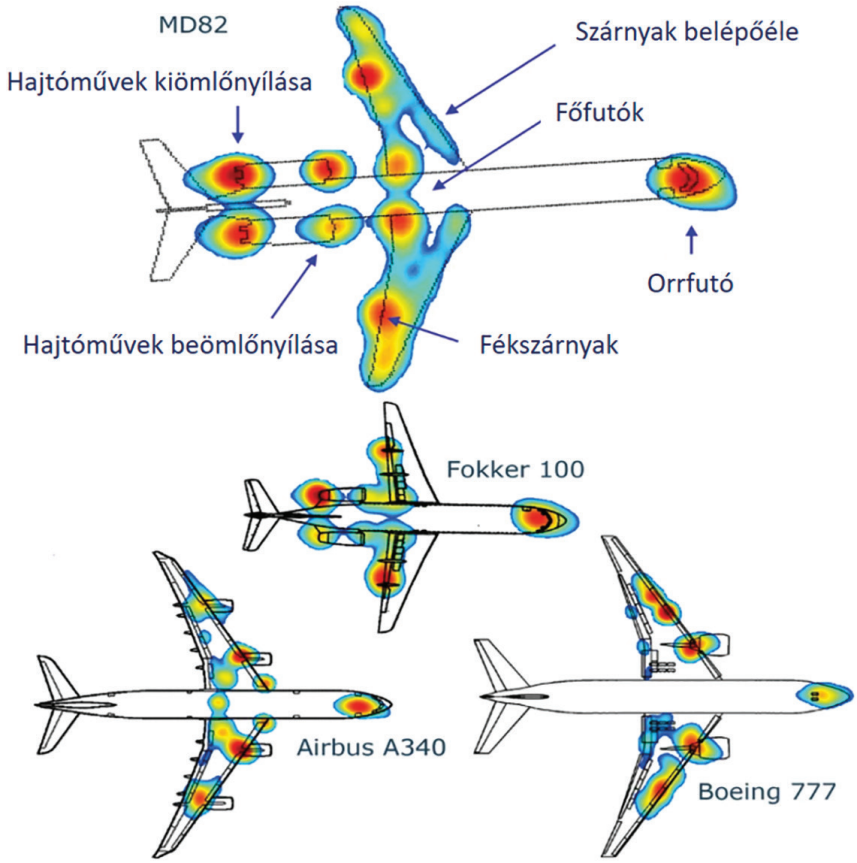
A kültérben végzett akusztikus felderítésnek mindig van negatív velejárója, nevezetesen a különféle környezeti terhelésből adódó zajok jelenléte. Azonban ez különböző méréstechnikai módszerekkel kiszűrhető, de legalábbis negatív hatásuk csökkenthető.

Légi járművek által keltett zajforrások az alábbi tényezőkből származtathatók:

- hajtómű- vagy motorzaj – az energiaátalakítás folyamán keletkezik;
- hajtóművek légcsavarjai által keltett zaj – a légcsavar adott lapátja metszi az előtte haladó lapát által gerjesztett örvényrendszert, aminek következtében közepes és magas hangtartományú zajok jönnek létre. A zaj intenzitása alapvetően függ a légcsavar vagy forgószárny fordulatszámától, kialakításától és méretétől;
- repülőgép sárkányszerkezete és a levegő aerodinamikai kapcsolatából keletkezett zaj – amely keletkezhet például a szárnynak a törzsön való elhelyezéséből adódóan;
- fedélzeti rendszerek, illetve egyes berendezések működéséből adódóan keletkezett zaj.

Akusztikai felderítéssel egy mozgó légi jármű által keltett zaj intenzitása és annak forrása határozható meg. A mérés hangképeit összevetve korábban eltárolt hangmintákkal meghatározható egy légi jármű típusa és iránya. Az 1. ábrán különböző repülőgéptípusok környezetében keltett zajforrások láthatók.

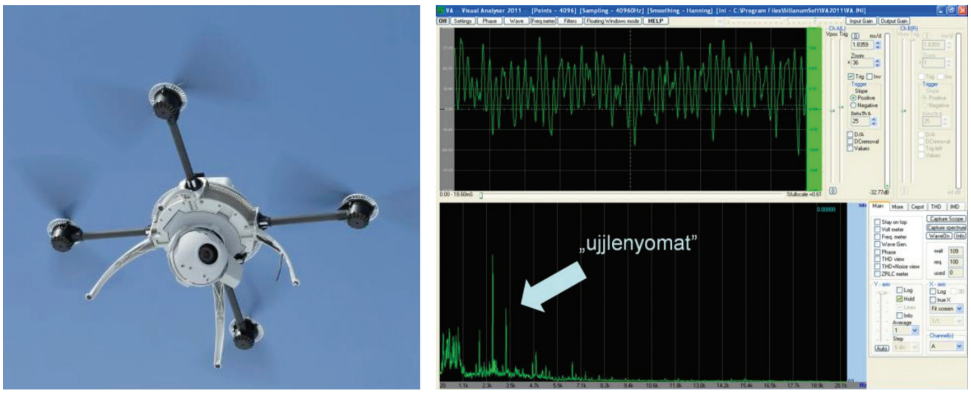
6 Makkay 2015.
7 Gajdács–Palik–Dudás 2021.



1. ábra: Repülőgépek környezetében keletkező zajforrások
Forrás: Merino-Martínez 2019.

A repülőgépek által keltett zaj több négyzetkilométer területet érint a repülőterek környezetében. A légi járművek működéséből keletkezett zaj a második legnagyobb környezeti zajforrás a közlekedési utak zaját követően. A különböző repülőgépek szerkezeti méretükből, repülési magasságukból adódóan különböző területet képesek lefedni, ami egyben azt is jelenti, hogy akusztikai érzékelés módszerével ezek viszonylag jól detektálhatók. Ellenben a drónok – alapvetően a kereskedelmi forgalomban elérhető típusok – méretükből adódóan nehezebben érzékelhetők az előbbi módszerrel.

A forgószárnyas kialakítású drónoknak jellegzetes hangja (zaja) van, így felderítésük akusztikai módszerrel kivitelezhető, azonban e módszer hatékonysága és eredményessége – hogy milyen távolságból érzékeljük az általuk kibocsátott zajt – nem feltétlen biztosít kielégítő megoldást detektálásra. Alapvetően a légcsavarlapátok forgásából adódó turbulens légáramlatokból származik, ami megfelelő méréstechnikai eszközökkel, illetve rendszerekkel érzékelhető. Így meghatározható az úgynevezett „*ujjlenyomatuk*" is (2. ábra).



2. ábra: Négyrotoros quadcopter hangképe
Forrás: Makkay 2014a.

Számos kutatás igazolja, hogy mérettől függetlenül a drónok által keletkezett hangminták elektroakusztikus módszerrel való mérése alkalmas a felderítésükre és azonosításukra.

3.1. Iránymérés alkalmazása légi járművek felderítésére

Mint ismeretes, a repülőgépek működésük, repülésük folyamán kiemelt zajforrásnak tekinthetők. Amennyiben a detektálni kívánt légi jármű hangforrása ismertté válik, szükséges lehet az érzékelés pontjához viszonyított irányának és a további mozgásának felderítése, hiszen csak ekkor jelenthetjük ki, hogy megvalósul az érintett légi jármű figyelemmel kísérése, nyomon követése.

3. ábra: Repülőgép zajforrásainak monitorozása, nyomon követése
Forrás: Makkay 2014a.

A repülőterek környezetében használatos különböző mérő/ellenőrző akusztikai állomások számos információt képesek biztosítani (3. ábra), például siklópályaadatokat, emelkedéssel és süllyedéssel kapcsolatos információkat. Így e mérőrendszerek alkalmazásával már nemcsak a hangforrás koordinátái lehetnek ismertek, hanem a légi jármű mozgásáról is információt kapunk.

A hangalapú felderítés legfőbb jellemzői:

- a nem, vagy csak csekély radarvisszaverő felülettel rendelkező légi járművek felderítésére is alkalmas megoldást kínál ez a mérési módszer;
- önállóan és egyéb felderítési módszerekkel ötvözve is képes repülőgépek érzékelésére és/vagy nyomon követésére is egyben.[8]

4. Elektromágneses hullámtartományú érzékelés

4.1. Az eszköz által kisugárzott rádiójel alapján való érzékelés

A drón és a távirányítást megvalósító adó (RC-távirányító) közötti kommunikáció rádiófrekvenciás kapcsolattal valósul meg. E rádiófrekvenciás jel (RF) érzékelésével, majd folyamatos mérésével a drón helyzeti koordinátája, illetve az őt irányító kezelő személy pontos pozíciója is meghatározható. Ennek megvalósítását a 4. ábra szemlélteti vázlatos formában.

4. ábra: UAV érzékelésének rendszermodellje
Forrás: a szerző szerkesztése Nemer et al. 2021. alapján

Az érzékelő rendszer egy vevőegységen keresztül észleli az adó–vevő (távirányító–gép) közötti kapcsolatot biztosító rádiófrekvenciás jelek alsó és felső határát, illetve megkezdődik azok kisugárzási forrásának felderítése. A begyűjtött adatok számítógépes

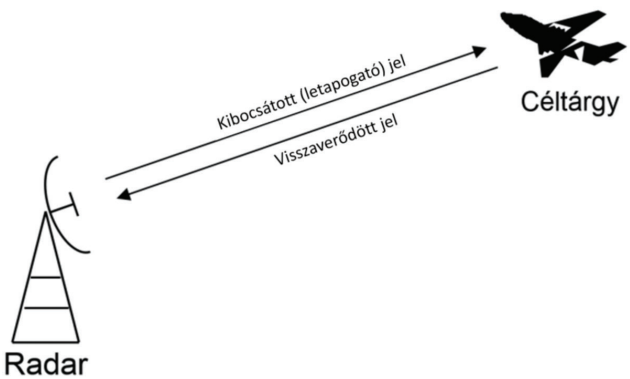
[8] Makkay 2014a.

feldolgozását követően megtörténik a drón helyzeti koordinátáinak azonosítása, illetve további szinteken megvalósulhat a légi jármű azonosítása, egyben a felhasznált és rendelkezésre álló adatok tárolása.[9]

4.2. Radarrendszerekkel történő érzékelés

Mozgó (repülő) tárgyak detektálására a hagyományos radarrendszerek is alkalmasak. Működésük a rádiólokátor által kisugárzott rádióhullámok visszaverődésének érzékelése alapján különféle tárgyak helyét tudja megállapítani.

Az 5. ábrán látható, hogy egy „céltárgy" (keresendő mozgó cél) felületéről visszaverődve a rendszer összegyűjti (felfogja) ezen információcsomagot, illetve az energia egy bizonyos részét.



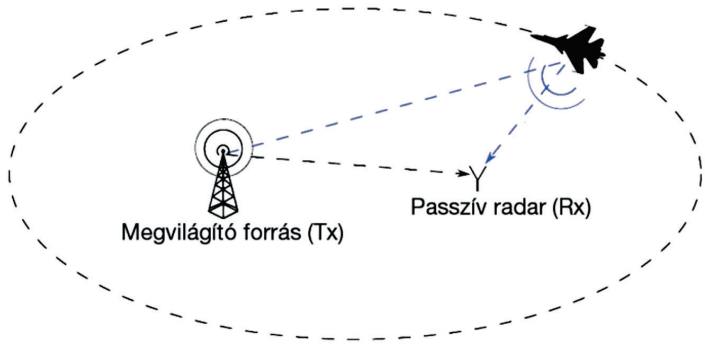
5. ábra: A radarmérés elvi vázlata
Forrás: a szerző szerkesztése Seller et al. 2019. alapján

A rendszer működése folyamán időmérésre visszavezethető távolságmérés valósul meg. A kibocsátott jel és a vett jel (visszavert jel) között bizonyos idő eltelik, aminek segítségével meghatározható a keresendő céltárgy távolsága. A visszavert vagy felfogott jel egy indikátoron megjeleníthető, így információval szolgál az érzékelt céltárgy hollétéről és mozgásáról. A rendszer működése folyamán további kiegészítő információkat is kaphatunk a céltárgyról visszavert jel alapos vizsgálatával a jel különböző összetevőiről (a jel amplitúdójának, fázisának és frekvenciájának mérésével).[10] A visszavert jel további vizsgálatával, elemzésével lehetőség adódik még több információ megszerzésére a céltárgyról, ami lehetőséget teremt annak kategorizálására, illetve osztályozására. Az aktív radarrendszer legfontosabb tulajdonsága, hogy az elektromágneses jel kisugárzását a radar maga kelti egy adóberendezés segítségével.

Azonban a módszernek hátrányai is vannak, ami hozzájárult a passzívradar-koncepció (*passive coherent location,* PCL) létrejöttéhez a 20. század második felében.

[9] Nemer et al. 2021.
[10] Krajnc 2019.

Ellentétben az aktív rendszerrel a passzív rendszer nem sugároz ki a céltárgy felderítéséhez szükséges megvilágító jelet, hanem a tárgy környezetében meglévő jelforrásokat használja fel a céltárgy detektálásához. Az úgynevezett megvilágító jelek valamilyen műsorszóró vagy telekommunikációs adótól származnak. Ezeket az adókat nevezzük a passzívradar-rendszerek megvilágító forrásainak, amelyet a 6. ábra szemléltet.



6. ábra: Passzívradar-rendszer elvi vázlata
Forrás: Seller et al. 2019.

A passzív radar vevőberendezésébe a „megvilágító források" *(illuminator of opportunity)* jelei több irányból érkezhetnek, közvetlenül (úgynevezett referenciacsatornán keresztül), illetve a céltárgyról visszaverődve (úgynevezett felderítő csatornán keresztül). A források helye és elrendezése miatt az egyes jelkomponensek eltérő időben érkeznek a vevőegységbe. Egy repülő céltárgyat számos adók különböző frekvenciákon megvilágítanak, például VHF-sávú FM[11]-, UHF-sávú DAB[12]- és DVB-T[13]-adók, műholdas jelek stb. Így a közvetlen vagy közvetett jelcsomagok mérésével megvalósulhat a képalkotás, amely többek között a céltárgy méretéről és alakjáról ad számunkra információt.

A passzívradar-rendszer előnyei:

- nem igényel adóberendezést;
- kisebb energiaigény szükséges a rendszer működéséhez;
- nem terheli a környezetet elektromágneses sugárzással;
- harcászati szempontból, a passzív radarok felderítése elektromágneses eljárásokkal nehézkes.[14]

4.3. Elektrooptikai rendszerek alkalmazása légi járművek felderítésére

A légtérben közlekedő légi járművek érzékelésének másik módja, az úgynevezett elektrooptikai rendszerek alkalmazása. A hagyományos radartechnológia – amely alapvetően a céltárgy felületéről visszaverődő rádióhullámok mérésén alapul – eredményes

[11] analóg–televízióműsor-szóró – frekvenciasávok: 47–862 MHz.
[12] digitális–földfelszíni rádióműsor-szóró – frekvenciasávok: 47–1467 MHz.
[13] digitális–földfelszíni televízióműsor-szóró – frekvenciasávok: 174–862 MHz.
[14] Seller et al. 2019.

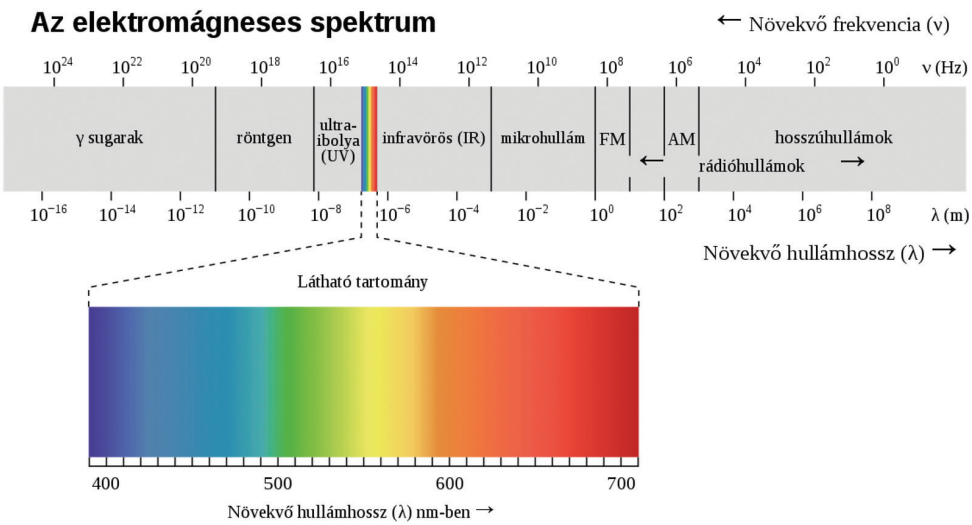
különböző légi járművek detektálására, ami nagyban függ a visszaverő felület nagyságától, anyagától és annak geometriájától.

Azonban a pilóta nélküli légi járművek érzékelése a hagyományos radartechnológiával számos kihívást jelent, hiszen ezek a repülőgépek kis méretükből adódóan egyrészt kevesebb visszaverődésre alkalmas felülettel rendelkeznek, másrészt pedig az építésükhöz felhasznált szerkezeti anyagok (különböző alapanyagú és összetételű műanyagok, kompozitok) csak minimálisan alkalmasak a radarhullámok visszatükrözésére.

Napjainkban az egyre több drón jelenléte miatt azonban fontos lenne, hogy azok a környezetünkben láthatóak is legyenek. Lehetséges megoldás a különféle elektrooptikai szenzorok alkalmazása. Ezek a megfigyelt célterületről vagy annak közvetlen környezetéről nyújtanak információt, az emberi szem számára látható és nem látható frekvenciatartományban, és az adatok analizálása és feldolgozása során használják fel őket.[15]

4.4. Látható spektrum

A látható spektrum vagy más néven látható fény az emberi szem számára érzékelhető elektromágneses frekvenciatartomány. Ebben a 380 és 750 nm-es tartományból érkező elektromágneses sugárzást képes érzékelni az ember a látáshoz szükséges érzékszerveivel (7. ábra). Ez azt is jelenti egyben, hogy ha e tartományon kívülre eső spektrumokat szeretnénk érzékelni, ahhoz speciális műszereket, átalakítókat, illetve képalkotó rendszereket kell alkalmaznunk.



7. ábra: Elektromágneses spektrum felosztása
Forrás: Wikipédia

[15] Makkay 2014b.

A láthatófény-tartomány képfelderítésére alkalmas megoldást kínál a PAL-optika[16]-rendszer.

A képfelderítés folyamán a következő szinteket különböztetjük meg: érzékelés, felismerés és azonosítás. Ebben a sorrendben követik egymást a nem felcserélhető átmenetek. A képfelderítés és -feldolgozás folyamatának lényege, hogy a rétegek között a látószöget időnként csökkenteni szükséges. Ha az észlelés sikeres volt, akkor folyamatosan elkezdjük szűkíteni a látószöget, fókuszálva az optikai rendszerrel abba az irányba, ahol az éppen detektálni kívánt vagy keresendő céltárgy, például repülőgép látható (érzékelhető). Így haladunk a képalkotás adta információk birtokában az érzékelésen keresztül a felismerésen túl az azonosításig.

A láthatófény-tartományban a mesterséges világítás, környezeti fényviszonyok szolgáltatják azt az energiát, amellyel érzékelhetünk (láthatunk) különféle tárgyakat. Azonban ennek felhasználható mértékét – hogy mennyire könnyen vagyunk képesek észlelni a környezetünkben – nagyban befolyásolja számos időjárási körülmény, állapot, mint például felhő, köd, csapadék. Ezek a tényezők mindenképpen hatással vannak a felderítés hatótávolságára.[17]

4.5. Infravörös tartomány

Nemcsak a láthatófény-tartományban érzékelhetők a testek a környezetünkben, hanem infravörös tartományban is, amelyre igaz, hogy emberi érzékszerveinkkel nem észlelhető. Minden test kibocsát magából infravörös sugárzást (hősugárzást), amennyiben a test hőmérséklete magasabb az abszolút nulla foknál. Ez az energiatartalom vagy ennek változása azonban mérhető. Az elektromágneses spektrum infravörös sugárzásának hullámhossztartománya 1 nm és 1 mm között érzékelhető (például rövid, közepes és távoli hullámhosszú infravörös tartományok stb.).

A hő mint energiaforrás átadása megvalósulhat hővezetés, hőáramlás és hősugárzás formájában. Egy testből kisugárzott hő értékének hőkamerával való mérése folyamán nem lehet egyértelműen különválasztani a hőenergiát mint mérendő fizikai jelenséget, mivel abban reflektált, emittált és transzmittált sugárzások összegét mérjük egy időben.

Különböző méretű és különféle hőintenzitású céltárgyak közel azonos képet adnak a megfigyelő számára.

Erre kínál elektrooptikai műszaki megoldást a HGH Infrared System (franciaországi székhelyű vállalat) a Spynel hőérzékelők családjával, amely lehetőséget biztosít drónok érzékelésére, illetve nyomon követésére (8. ábra).

[16] Dr. Greguss Pál professzor a NASA (National Aeronautics and Space Administration – Nemzetközi Repülési és Űrhajózási Hivatal) által is elismert találmánya.

[17] Makkay 2014b.

8. ábra: Drónok érzékelése Spynel hőkamerával
Forrás: HGH Infrared company 2022.

A különböző típusú infrakamerák különböző hullámhosszú infravörös tartományban képesek működni – közepes (3,0–5,0 µm) és távoli (8,0–14,0 µm) hullámhosszú infravörös tartományban – így képesek eltérő típusú és méretű pilóta nélküli légi járművek érzékelésére több kilométeres távolságból úgy nappal, mint éjszaka. Továbbá a rendszer különlegességének számít, hogy több célpont megfigyelésére is alkalmas, így akár drónraj egy időben való megjelenését is tudja érzékelni, illetve azt nyomon követni.[18]

5. Összegzés

Mozgó tárgyak, nevezetesen légi járművek érzékelésére gyűjtöttük össze azokat a fizikai elveken nyugvó műszaki megoldásokat, amelyek külön-külön vagy együttes alkalmazásával detektálni, illetve nyomon követni tudjuk ezeket az eszközöket. A hatékony megoldást a több csatornából érkező valós idejű adatok jelenthetik, amelyeket vélhetően a különféle érzékelési módok együttes alkalmazásával érhetünk el.

[18] Lásd: https://hgh-infrared.com/about-us/

Felhasznált irodalom

Gajdács László – Palik Mátyás – Dudás Zoltán (2021): Drónok és hagyományos légi járművek közös légtérben történő alkalmazásának repülésbiztonsági kockázatai. *Repüléstudományi Közlemények,* 33. évf. 1. sz. 157–170. Online: https://doi.org/10.32560/rk.2021.1.12

Krajnc Zoltán (2019): *Hadtudományi Lexikon.* Budapest, Dialóg Campus Kiadó.

Makkay Imre (2014a): Elektroakusztikai eljárások légijárművek felderítésére. *Repüléstudományi Közlemények,* 26. évf. 2. sz. 351–359. Online: https://folyoirat.ludovika.hu/index.php/reptudkoz/article/view/4627/3788

Makkay Imre (2014b): Elektrooptikai eszközök légijárművek felderítésére. *Repüléstudományi Közlemények,* 26. évf. 3. sz. 15–27. Online: www.repulestudomany.hu/folyoirat/2014_3/2014-3-02-0177_Makkay_Imre.pdf

Makkay Imre (2015): Drónok harca. *Repüléstudományi Közlemények,* 27. évf. 1. sz. 61–72. Online: www.repulestudomany.hu/folyoirat/2015_1/2015-1-05-0192-Makkay_Imre.pdf

Merino-Martínez, R. et al. (2019): A Review of Acoustic Imaging Methods Using Phased Microphone Arrays. *CEAS Aeronautical Journal,* 10. évf. 197–230. Online: https://doi.org/10.1007/s13272-019-00383-4

Nemer, Ibrahim – Sheltami, Tarek – Ahmad, Irfan – Ul-Haque Yasar, Ansar – Abdeen, Mohammad A. R. (2021): RF-Based UAV Detection and Identification Using Hierarchical Learning Approach. *Sensors,* 21. évf. 6. sz. Online: https://doi.org/10.3390/s21061947

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

Ujjady András – Major Gábor (2021): A civil drónszabályozáson innen, a katonain túl. *Repüléstudományi Közlemények,* 33. évf. 2. sz. 167–180. Online: https://doi.org/10.32560/rk.2021.2.12

HADMÉRNÖK
HADITECHNIKA

17. évfolyam (2022) 4. szám 29–45.
DOI: 10.32567/hm.2022.4.3

Hegedűs Ernő,[1] Vég Róbert László[2]

Mérnökök a magyar haditechnika fejlesztéstörténetében – Dr. Lipták Pál

– Új technikatörténeti kutatási eredmények az első hazai harckocsi és helikopter fejlesztőjéről

Engineers in the History of Hungarian Military Research and Development – Paul Lipták

– New Results of Technical Research on the Developer of the First Hungarian Tank and Helicopter

Dr. Lipták Pál (1874–1926) mérnök, gyártulajdonos és parlamenti képviselő volt, illetve egyetemi tanársegéd, majd a műszaki tudományok egyik első doktori fokozatosa. Építőmérnökként kutatásaival jelentősen hozzájárult a vasbeton szerkezetek technológiájának fejlődéséhez. Nevéhez fűződik az első magyar harckocsi szabadalma, terve és prototípusa. Lőszergyárában készült a világ egyik első helikopterének prototípusa is.

Kulcsszavak: **harckocsi, lőszergyártás, helikopter, haditechnikai fejlesztés**

Paul Lipták (1874–1926) was an engineer, a factory owner and an Assistant Professor. He was one of the first doctoral graduates in engineering. As an architect, his research contributed significantly to the development of reinforced concrete structure technology. He is credited with the patent, construction and prototype

[1] PhD, adjunktus, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar, e-mail: hegedus.erno@uni-nke.hu
[2] PhD, egyetemi docens, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar, e-mail: vegh.robert@uni-nke.hu

of the first Hungarian tank. One of the first helicopters in the world was also made in his ammunition factory.

Keywords: **tank, ammunition product, helicopter, military technology research and development**

1. Bevezetés

Dr. Lipták Pál (1874–1926) mérnök, építési vállalkozó, elsősorban eredményes építészként ismert, azonban tevékenysége a magyar haditechnika-fejlesztés történetében is igen jelentősnek mondható.

Dr. Lipták Pál mérnök a magyar haditechnikai fejlesztés korai időszakának kevéssé ismert, de fontos szereplője. Gyártulajdonos és parlamenti képviselő, illetve egyetemi tanársegéd, majd a műszaki tudományok egyik első doktori fokozatosa. Építőmérnökként kutatásaival jelentősen hozzájárult a vasbeton szerkezetek technológiájának fejlődéséhez. Az első világháború alatt lőszergyárat működtetett. Nevéhez fűződik az első magyar harckocsi terve, amely forgó toronnyal és beépített géppuskával rendelkezett.[3] Lőszergyárában készült a világ egyik első helikopterének prototípusa is. Lőszergyára részt vett a jelentős vegyipari és technológiai hátteret igénylő vegyiharclőszer-programban is. Hadiipari tevékenysége során nemcsak a bécsújhelyi repülőkísérleti intézettel (Osztrák–Magyar Monarchia Fischamendi Repülőkísérleti Intézete, K.u.K. Fliegerarsenal Flugzeugwerk, Fischamend) – a Monarchia egyik legfontosabb haditechnikai kutatás-fejlesztést végző intézetével – folytatott fejlesztési együttműködést, hanem részt vett olyan hadiipar-fejlesztési programokban is, mint a Hindenburg-program. Jelentős volt a szerepe a műszaki szakképzés hazai szervezésében is, mivel Pestszentlőrincen ipari iskolát hozott létre. Nevét ma a Lipták-telep őrzi Pestszentlőrincen.

Jelen publikáció számos tekintetben bővíteni törekszik Dr. Lipták Pál mérnök és gyártulajdonos szakmai életrajzát, helyenként pontosítva egyes, személyével és tevékenységével kapcsolatos korábbi kutatási eredményeket (például a világ első katonai helikopterének, a PKZ-2 első felszállásának helyszínét, amelyet Lipták Pál gyárában gyártottak, és ott is szállt fel). De új kutatási eredmény például a Lipták Pál gyárában megvalósított hulladékvas-újrafelhasználás – az első hazai hulladékvas-üzemű März-kemence – logisztikai és kohászati hátterének elsőként történő ismertetése is. Lipták cégének nemzetközi ipari és kutatás-fejlesztési együttműködéseit is ismertetjük. Összességében jelen publikáció célja, hogy a magyar haditechnikai fejlesztéstörténet jeles személyiségének, Dr. Lipták Pálnak a munkásságát az új technikatörténeti kutatási eredmények tükrében a korábbinál komplexebb módon mutassa be, teljesebb képet tárva a szakmai közönség elé.

[3] Bombay–Gyarmati–Turcsányi 1999.

2. Dr. Lipták Pál életrajza és szakmai munkássága a gyáralapításig

Dr. Lipták Pál 1874. április 13-án született Békéscsabán és 1926. május 15-én halt meg Balatonfüreden.[4] Békéscsabán járt iskolába, de édesapja korai halála miatt a gimnáziumot nem fejezhette be. Édesapja szakmáját, az ácsmesterséget tanulta ki. 1889-től a Vaskapu szabályozásának munkálataihoz került, ahol három évig dolgozott.

Tehetségével hamar kitűnt, és 16 évesen már több száz munkást irányított. A munkával párhuzamosan elvégezte a hiányzó középiskolai osztályokat Kecskeméten, és beiratkozott a budapesti József Nádor Műegyetemre, ahol 1901-ben építész oklevelet szerzett. Az oklevél megszerzését követően az egyetem középítési tanszékén dolgozott mint tanársegéd. A Magyar Mérnök és Építész Egylet 1905-ben pályázatot írt ki egy múzeumépület megtervezésére. Lipták Pál múltba visszanyúló stílusjegyeket tartalmazó tervével megnyerte a kiírást, az aranyérem mellé kapott pénzjutalmat pedig európai tanulmányútra fordította. Útja során megismerkedett a vasbeton felhasználási lehetőségeivel, amelynek hazai képviselőjévé vált, és amiből később doktori értekezését írta. 1906-ban szerezte meg az országban másodikként a műszaki doktori címet. Értekezésének címe az *Adalék a vasbetonszerkezet elméletéhez* volt, amely óriási feltűnést keltett és új korszakot jelentett a vasbeton-építkezések fejlődésében.[5] Az egyetemen tanári állást ajánlottak neki, de ő megvált az egyetemtől, és 1908-ban Budapesten műhelyt létesített, ahol vasszerkezeteket készített és magasépítkezéseken dolgozott. A manapság használatos vasbeton épületszerkezetet 1892-ben szabadalmaztatták Franciaországban. Lipták gyárában jelentős középületekhez készültek ilyen szerkezetek: például az Igazságügyi Minisztérium, több bíróság és takarékpénztár épülete, gyárak üzemcsarnokai, laktanyák és telefonközpontok Budapesten. Első munkája a Goldberger Textilgyár és a Goldberger-ház megtervezése és kivitelezése (1909) volt. Ezt követte a Budaörsi úti IV. Károly király laktanya (1909).[6] Nevéhez köthető a MÁVAG (Magyar Királyi Államvasutak Gépgyára) víztoronnyal is rendelkező munkáskolóniájának építése.

A Lipták és társa a legnagyobb építőipari cégek egyike volt az 1910-es évek elején. Ebből a vállalkozásból fejlődött ki 1910-ben a Dr. Lipták és Társa Építési és Vasipari Részvénytársaság, amelynek vezetője volt 1919-ig.

Az 1910-es évek végén Lipták Pál jelentős területet vásárolt meg ipari beruházása számára: martinacélgyárat és hengerművet (korabeli kifejezéssel: hengerdét) létesített. A cég Pestszentlőrincen, a lajosmizsei vasút melletti telken épült fel, amely a legnagyobb építőipari cégek egyike lett. Munkásai számára Lipták lakótelepet épített (ez a mai Lipták-telep). Lipták Pál az Apponyi Albert (ma Hengersor) utcában építette fel gyáregységét.

„1911 tavaszától így épült meg a vasszerkezeti csarnokot követően a hídszerkezeti műhely, a vasöntöde egytonnás kapacitású kupolóval, a korszerű acélmű 15 tonnás rekuperatív rendszerű Martin-kemencével, a hozzátartozó négy egységből álló gázgenerátor-teleppel, majd az 1913 februárjától üzemelő acélmű mellett a finomhengermű, a központi erőtelep – szénrakodóval

[4] Körösvidék 1926; Békésmegyei Közlöny 1926.
[5] Grósz 1995. 56.
[6] Bencze–Remport 2001. 162.

és víztisztító művel kiegészítve. […] A Lipták-gyár – 1913-tól Dr. Lipták és Társa Építési- és Vasipari Részvénytársaság […] a fővárosi építkezésein kívül – elsősorban közúti és vasúti vas- és vasbeton-szerkezetű hidak, raktárházi elektromos felvonók és elevátorok, bányafelvonók és egyéb berendezések, elektromos markolók, emelők, szénrakodók, különféle daruk, vasúti fordítókorongok, egy sor fővárosi középítkezéshez gyártott és szállított szerkezetek, hengerművi berendezések gyártásával és szerelésével foglalkozott. A cég 1913-ban 651 főnyi munkás-létszámával a hazai vas-, fém- és gépipari vállalatok között a hatodik helyet foglalta el."[7]

A budapesti építkezések mellett köz- és vasúti vonatkozású járműgyártásokat is végeztek.

A Dr. Lipták és Társa Építési és Vasipari Rt. üzeme 1914 márciusában vált teljessé, amikor megnyitották az acélöntőt és hengerművet is. Elsősorban épületek, hidak vasbeton szerkezetének előállításával foglalkozott, például a szolnoki Tisza-híd fűződik a nevéhez. Az 1913-ban elkezdett Pesti Hazai Takarékpénztár Gizella (ma Vörösmarty) téri palotájánál az összes vas- és vasbetonmunkálatot a cég kivitelezte, az épület 1915 júniusában lett kész. Ezt követően a dunakeszi vasúti szerelőműhely építésére kapott megbízást. Rövid idő alatt jelentős vagyonra tett szert, és büszke volt arra, hogy Budapesten ő fizette a második legtöbb adót. Cége nevéhez fűződik a méltán híres Párisi Udvar kivitelezése Budapest belvárosában. A vállalat a háború alatt haditermelésre állt át.

A Lipták-féle cég a Hofherr mezőgazdasági gépgyár (Hofherr–Schrantz–Clayton–Shuttleworth vagy HSCS-gyár) szomszédságában települt. A két nagy kiterjedésű iparvállalat összegzett gyártókapacitása olyan jelentős nyersanyag- és termékszállításokat generált, hogy kiszolgálása érdekében önálló iparvasutat építettek a Lipták-gyártól Soroksárig – egyes szakaszain a lajosmizsei vasút, illetve az úgynevezett Burma-vasút része volt, helyenként csatlakozott a Cséry Lajos hulladékgazdálkodó vállalkozó szomszédos birtokán futó iparvasúthoz is. (A Burma-vasút két vasútvonalat jelent Budapesten; a Kis-Burma és Nagy-Burma nevű összekötő vágányokat, amelyeket teherszállításra használtak. A Cséry-iparvasút 1897-ben csatlakozott a fővasúti kapcsolathoz: a Soroksár–Szemeretelep [Nagy-Burma] vasúthoz.) Budapest egyik legjelentősebb ipari övezete jött létre ezáltal Pestszentlőrincen, amelyet a Hofherr- és a Lipták-gyárak képeztek, és amely jelentős szerephez jutott az első világháború ipari termelésében. „A Lipták gyár emlékét őrzi a telepelnevezés, egykori igazgatósági épületében sok-sok évtizede közgazdasági szakközépiskolát találunk, területén még ma is működik a Lőrinci Hengerművi. A Havanna lakótelep helyén az I. világháború alatt fallal körülvett lőszergyárat hoztak létre. A gyár épületeit a 20-as években lakásokká alakították át."[8] A lőszergyár átalakított épületeiből született lakások alkották az Állami Lakótelepet. A Lőrinci Hengerművet (Dunaferr Lőrinci Hengerművi Kft.) a 2010-es évek elején zárták be.

[7] Bencze–Remport 2001. 163.
[8] Heilauf é. n.

3. Haditermelés és haditechnikai fejlesztések a Dr. Lipták és Társa Építési és Vasipari Részvénytársaságnál az első világháború alatt

Lipták gyára az I. világháborúban – számos más hadiipari termék mellett – elsősorban lőszert gyártott. 1913-ban az üzem munkásainak létszáma 650 fő volt, azonban ez a létszám a háború során a gyár kibővítésével jelentősen megugrott.

„1915 januárjában elkészültek és utána rövidesen megindult a legkülönfélébb tüzérségi lövedékek, gránátok és srapnelek, repülőbombák és gyújtótestek gyártása, s igen rövid idő alatt a vállalat a Monarchia egyik legjelentősebb muníció-ellátójává lépett elő. Emellett még a gyár felkészültségének megfelelően gyártottak tüzérségi lőszerkocsikat, páncélozott kocsikat, sokféle egyéb hadfelszerelési cikket. Itt említhető meg, hogy a háború vége felé bekapcsolódtak a repülőgépgyártásba."[9]

A vállalat kibővült egy darugyárral, egy durvahengerművel és egy vasöntődével, majd a borsodszendrői szénbányával és egy lőszergyárral. A cég létszáma az utolsó háborús években meghaladta az 5200 főt.

A pestszentlőrinci Dr. Lipták és Társa Építési és Vasipari Rt. mellé 1916-ban létesített Lipták-lőszergyár részt vett a légi bombák alkatrészeinek gyártásában is: bombatesteket és bombagyújtókat gyártottak.[10] 1916-ban a Lipták-gyár az enzesfeldi lőszergyárral közösen megalapította a Magyar Lőszergyár Rt.-t, amelynek gyártelepét Pestszentlőrincen építették fel. A Magyar Lőszergyár részben a Dr. Lipták és Társa alapítása volt, és ugyanúgy Pestszentlőrincen helyezkedett el, a Lipták és Társa Rt. szomszédságában. Tervezésénél minden óvintézkedést megtettek a balesetek elkerülésére. A munkafolyamatokat elkülönítették, a veszélyes anyagokat a gyár területétől távol helyezték el és őrizték. Az esetleges tűz gyors eloltásához a telepet behálózó vízvezetéket terveztek, víztornyot építettek. A legmodernebb alacsony nyomású gőzfűtő berendezéssel látták el az üzemépületeket, hogy a szikrák keletkezését ezúton is kiküszöböljék. Az üzemnek közvetlen összeköttetése volt a lajosmizsei vasútvonallal, a vágányok a Reviczky utcán keresztül érték el a lőszergyárat, ahol négy ágra szakadtak, és a mai Margó Tivadar utca vonalán egészen a Baross utcáig körülölelték a telepet. Az egyes épületek között a szállítás megkönnyítésére keskeny nyomtávú sínpárokat fektettek le, amelyek az épületeken is keresztülfutottak. Rajtuk kézi erővel mozgatták a csilléket.

A háború alatt a lőszergyár átállt a folyamatos munkára, éjjel-nappal üzemelt, a gépek sohasem álltak le. 1914-ről 1915-re a gyárberendezés értéke megduplázódott, 1915-ről 1916-ra pedig megtriplázódott. A Lipták-gyárból az előirányzott tervek szerint naponta 2500–2500 db 7,5 cm-es,[11] 2300–2300 db 10,4 cm-es gránátnak és gránátsrapnelnek, valamint 1000 darab 15 cm-es gránátnak kellett volna kikerülnie.[12]

[9] Bencze–Remport 2001. 164.
[10] Kelemen 2018.
[11] A korabeli osztrák és német haditechnikai és katonai gyakorlattal egyezően, az eredeti leírásokban szereplő megfogalmazást tiszteletben tartva a [cm] az alkalmazott mértékegység, amely ilyen módon eltér az SI-szabványtól.
[12] *Hadiipar Pestszentlőrincen.* é. n.

A Hindenburg-program a gazdaság maximális kihasználását vette tervbe a hadi-termelés számára.[13] A Hindenburg-program 1916 végén indult meg, és a Monarchia napi összes tüzérségi lőszertermelését 20 000 db 7,5 cm, 72 000 db 8 cm, 45 000 db 10 cm, 4600 db 10,4 cm, 7300 db 15 cm-es gránátban, srapnelben és gránátsrapnelben határozta meg. Ez olyan hatalmas mennyiséget jelentett, hogy azt végül nem tudták elérni. (Még 1917 májusában sem, amikor a legintenzívebb volt a termelés, ugyanis az ebben a hónapban összeszerelt 2 600 000 darab tüzérségi lőszer is több mint 1 millióval maradt el a Hindenburg-program által előirányzottól.) Mégis, a Monarchia a háború alatt összesen 72 000 000 tüzérségi lőszert gyártott, ez lényegében megegyezett az olasz és orosz termeléssel.[14] 1916-ra nyolc lőszergyár működött a Monarchia területén: Wöllersdorf, Gebruder Böhler, Munitionswerke Enzesfeld, Skoda-Werke, Weiss Manfréd Csepel, Lipták és Társa Pestszentlőrinc, Dynamit-Nobel Pozsony, A. Z. D. Komárom. Utóbbi négy Magyarország területén volt. Amikor 1916-ban a Lipták-gyár az enzesfeldi lőszergyárral közösen megalapította a Magyar Lőszergyár Rt.-t, az a Hindenburg-program kapacitásbővítési törekvéseinek egyik legjelentősebb lépése volt.

A cég emellett az első világháború alatt katonai felszerelések széles körének gyártását vette át, és harckocsi-, valamint helikopterfejlesztési kísérleteket és prototípusgyártást is végzett. A gyár irodaépületében Lipták Pál egy lakást is kialakított maga számára, hogy folyamatosan jelen lehessen. 1916-ban és 1917-ben jelentősen kibővítették az üzemet (például srapnelüzem), ekkor építették az Apponyi utca sarkán a tiszti- és munkáséttermet is. A gyár munkásainak száma 1917-ben 5300-ra emelkedett. A sztrájkhelyzet a háború előre haladásával mind jobban elmérgesedett. 1918 nyarán már a termelés csökkenésére is erőteljesen reagált a karhatalom. A katonai parancsnok tizedelést akart elrendelni, ha nem fokozódik a termelés.

A Lipták Pál gyárában megvalósított termelés fontos iparszervezési aspektusa a hulladékvas-újrafelhasználás kohászati technológiája és e folyamat logisztikai szervezése. A Lipták-gépgyár, öntöde- és hengermű számára a szomszédos Cséry hulladékgazdálkodó-telep szeméthasznosító műve szállította a roncsvasat, szerződés alapján. A Cséry hulladékgazdálkodó-telep a Lipták-gyár fontos alapanyag-beszállítója volt. Működését az Ecseri úttól Pestszentlőrincig futó szemétszállító-vasút biztosította. A századfordulót megelőzően a főváros szerződést kötött ifj. Cséry József vállalkozóval. Cséry a család pestszentlőrinci birtokán alapította meg a Cséry-féle Szemétfuvarozási és Feldolgozási Gyár Rt.-t 1872-ben, és egy, a főváros közigazgatási határán kívül kialakított szeméttelepre szállította a fővárosi szemetet.[15] A telephely Kispest határában, a mai Vass Gereben utca – Nádasdy utca – Nagykőrösi út által határolt területen terült el, a Lipták- és Hofherr-gyárak nyugati oldalán, és fokozatosan töltötték fel a mai Pestszentimre irányába a Nagy-Burma vasútig. A hulladékot fajta szerint osztályozták, a hasznosítható anyagokat külön válogatták, feldolgozták. Cséry 1893-ban szabadalmat jegyeztetett be komposztgyár felállítására a telepen.[16] A szeméttelepet

[13] Dombrády et al. 2017.
[14] *Hadiipar Pestszentlőrincen.* é. n.
[15] Utóda Cséry Lajos (1855–1924) birtokos, vállalkozó. Lásd Tomory Lajos Múzeum é. n.
[16] Cséry szabadalmat jelentett be: a szerves hulladékból adalékanyagok hozzáadásával termőföldet állítottak elő, amelyet kertészeteknek és szőlészeteknek adtak el.

guberálók serege lepte el: egyesek kokszolódott szén, mások *fémhulladék után kutattak,* mindkettőt jó áron értékesítették.[17] A legjelentősebb ócskavas-felvásárló a szomszédos Lipták-vasgyár volt. Cséry és Lipták üzleti kapcsolatban álltak: a Cséry-hulladéktelepen különválogatott ócskavas kohászati felhasználására a Lipták-gyár beszállítói szerződést kötött a szemétfeldolgozó üzemmel. A korrodált ócskavas – részben adalékanyagként, részben nyersanyagként – jelentős szerephez jutott a jó minőségű acélgyártás kohászati folyamataiban.[18] A Lipták-gyár mérnöke úgy módosította a kohászati folyamatokat, hogy az ócskavas jelentősebb mennyisége legyen felhasználható. Király Endre, a Lipták-gyár vezető kohómérnöke megtervezte és üzembe helyezte az első März-kemencét Magyarországon, és kidolgozta az eljárást, amely lehetővé teszi az említett kemencét *kizárólag hulladékvassal üzemeltetni*. A hulladékvas-feldolgozásra tehát nemcsak az acélgyártás adalékanyagaként, hanem önállóan is sor került a Lipták-gyárban – ami fokozta az együttműködést az ócskavasforrásként működő Cséry-hulladékművekkel. Emellett Dr. Lipták Pálnak saját tulajdonú bányái is voltak, ahonnan vasúton szállították gyárába a nyersanyagokat, érceket, szenet stb. Ezeket egészítették ki a Cséry hulladékgazdálkodó telepről származó anyagok. A főváros hulladékának szállítására az Ecseri úti és a Kispest-Pestlőrinci Cséry-telepek között iparvágány is kiépült, amelyen Cséry 1891-től gőzvontatással szállíttatta a szemetet az Ecseri úttól a feldolgozó telepig, majd 1897-től a szemétlerakóig – ez volt a Cséry-vasút. Az Ecseri útról indulva a mai Nagykőrösi út vonalán, majd a Hofherr Albert utcánál balra fordulva az Ipacsfa utca vonalában haladt és a Kettős-Körös utcánál érte el a Pestszentlőrinc–Soroksár szárnyvonalat (a Nagy-Burma vasutat). A Lipták-gyár által alkalmazott nyersanyag-takarékos hulladékvas-felhasználási eljárásnak különösen a nyersanyaghiányos háborús évek során volt szerepe.

3.1. Vegyilőszer-gyártás a Lipták Vasgyárnál

„A Lipták-gyár nemcsak hagyományos lőszert gyártott, hanem a Monarchiában elsőként 1915-től vegyi fegyvert is."[19] A harci gázokat a 7,5, 8 és 10, illetve 15 cm-es repeszgránátok hüvelyébe töltötték. A töltőgázt kezdetben Németországból hozták be. A sorozatgyártás a Lipták-gyárban 1917-ben indult meg a német LOST és KLARK anyagokkal, majd tavasszal az újpesti Chinoin-gyár is beszállt a termelésbe, itt saját fejlesztésű gázokat is használtak (a brómtartalmú „C" és „B" anyagot). Érdemi gyártást

[17] A szén üzletágra létrejött a Pestszentlőrinci Kokszтermelő Vállalat.

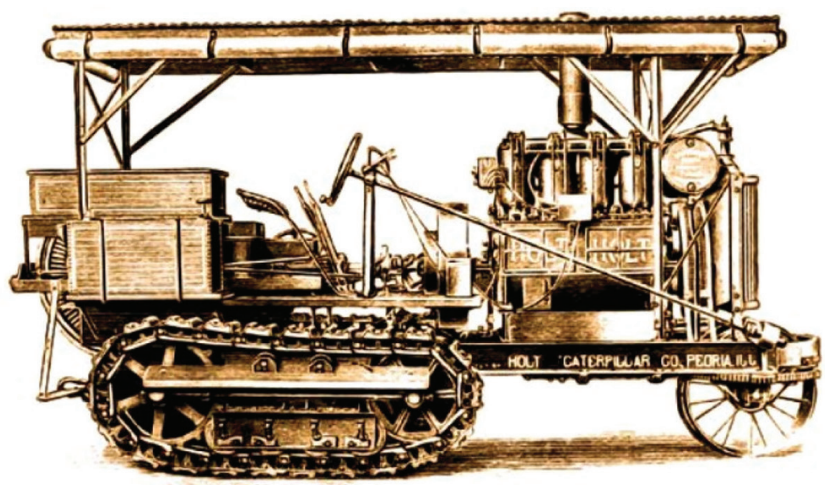
[18] Az ócskavas szerepe az acélgyártásban: 1. A Siemens–Martin-eljárást Pierre-Émile Martin francia mérnök szabadalmaztatta 1864-ben. Az eljárás nevében a Siemens nevet a Carl Wilhelm Siemens által szabadalmaztatott, és itt felhasznált váltakozó lángjárású regeneratív tüzelési rendszer magyarázza. A módszer lehetővé teszi folyékony nyersvas és *ócskavas* felhasználását is, de akár szilárd betéttel is lehetett indulni. 2. A Linz-Donawitz-(LD-) konverter oxigénbefúvásos acélgyártási módszer: Az oxigénbefúvás felülről történik. Az acélgyártás során megbillentik a meleg, legalább 1000 °C-os konvertert, és – *ha fémhulladékkal is dolgoznak* – beadagolják a *vashulladékot* és a nyersvasat úgy, hogy az *elfedje a hulladékot*. A konvertert függőleges helyzetbe állítják, leengedik az oxigénlándzsát, és először távolabbról megkezdik a fúvatást. Ezt követően salakképzőnek égetett meszet (CaO) adagolnak. A lándzsát fokozatosan lejjebb engedik, a fürdő hőmérséklete a végbemenő hőtermelő reakciók hatására megemelkedik. Folyamatosan képződik a salak, összetétele a folyamatoknak megfelelően alakul. Ha a hőmérséklet túl magas, acélhulladékot adagolnak.

[19] *Hadiipar Pestszentlőrincen*. é. n.

ez a két üzem produkált, 1918-ig megközelítően 1 millió 370 ezer gázlőszert. A termelés nagy részét az újpesti vegyületek tették ki. Hetenként átlag 20–25 000 lövedék készült el, de ez nagyban függött a német gázszállításoktól is. KLARK-ot, amelyet kék kereszttel jelöltek, mindkét üzemben töltöttek a lőszerekbe, míg LOST-ot (mustárgáz), a sárga kereszttel jelöltet, egyedül Pestszentlőrincen. Utóbbiból mintegy 200 000 darab készült. A kék keresztes anyag ingerlő hatású volt, a légzőszerveket károsító arzénvegyületeket tartalmazott. A sárga keresztes hólyaghúzó hatással bírt. A színtelen, szagtalan klórvegyületek áthatoltak a ruházaton is, velük érintkezve a bőrön néhány óra múlva hólyagos elváltozások jelentek meg.

3.2. Harckocsifejlesztés a Lipták Vasgyárnál

Az első világháborút megelőző években az Osztrák–Magyar Monarchia hadseregének gépesítése érdekében több eszköz fejlesztése is zajlott. A hadsereg ekkor világelső volt a mai harckocsik elődeinek tervezésében, de főként anyagi korlátok miatt ezt nem tudta kellőképpen kihasználni.[20] Dr. Lipták Pál 1913-ban nyújtotta be a Magyar Királyi Honvédelmi Minisztériumhoz a Lipták Vasgyár mérnökeinek harckocsitervét. A harckocsi alapját egy, a vasgyár területén működő Holt-típusú emelődaru alkotta. Az eredeti Holt Caterpillar traktor lánctalpas futóművét 1910-ben szabadalmaztatták.[21] Benjamin Holt (1849–1920) amerikai gyáriparos a 19. század végén, 1883-ban fivéreivel a kaliforniai Stocktonban gépgyárat alapított. A Holt Manufacturing Company névvel bejegyzett cég az Illinois állambeli Peoriában is létrehozott egy gyártó üzemet.



1. ábra: Holt Caterpillar traktor, amely a Lipták harckocsi alapját képezte
Forrás: Réz 2012. 38.

[20] Hajdú–Sárhidai 2005. 13–15.
[21] Varga 2008; Farkas 2017.

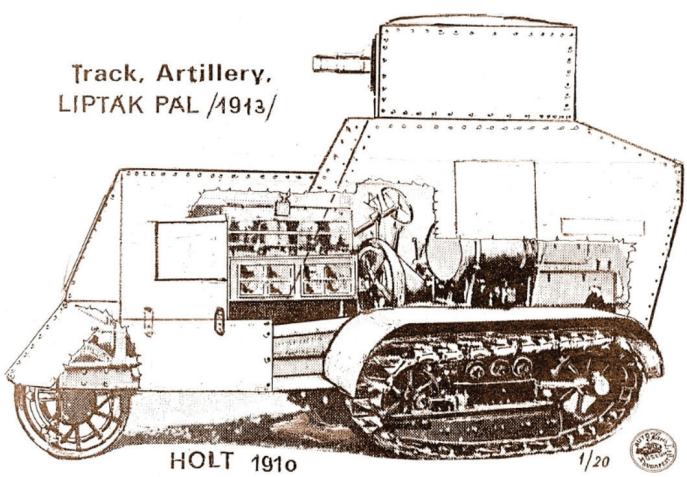
A Lipták-harckocsi fejlesztéséhez alkalmazott Holt Caterpillar 1910 M. traktor jó minőségű lánctalpas járműalvázat biztosított a kísérletekhez. A neves gyáralapító 1906-ban szabadalmaztatta világhírű korszakalkotó találmányát, a lánctalpas traktort. (A lánctalpelvet az angol George Cayley találta fel még 1825-ben.) Magyarországon a legelső Holt Caterpillar Company cég által forgalmazott lánctalpas traktor 1912-ben Somogy megyében, Dr. Steiner Leó berzencei birtokán mutatkozott be. A későbbiekben mintegy 30 hazai földbirtokos, többek között gróf Bethlen István Maros-Torda megyei mezősámsondi birtokán (Trianon óta Romániához tartozik) és Festetics Tasziló (Keszthely) gazdaságában szántottak a 60 lóerős benzintraktorral. A tengerentúli gépgyárnak 1913-ban már magyarországi vezérképviselete is volt. (Budapest, V., Hold utca 15.)

1. táblázat: A Holt Caterpillar traktor főbb műszaki adatai (1912. évi típus)

Motor típusa	**4 hengeres, 4 ütemű folyadékhűtéses benzin-petróleum motor**
Motorteljesítmény	60 LE 500 1/min fordulatszámnál
Szélesség	2040 mm
Hosszúság	5570 mm
Magasság	3050 mm
Nyomtáv	1940 mm
Tömeg	9200 kg

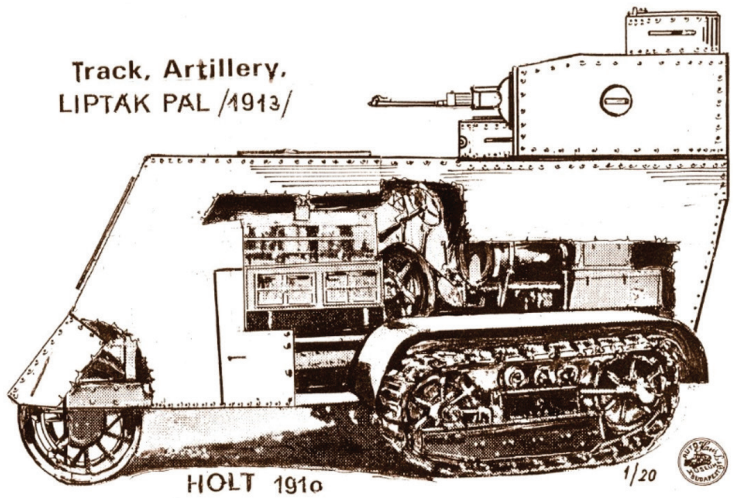
Forrás: Varga 2008.

Lipták már 1913-ban megkezdte egy harcjármű tervezését erre az alvázra. Dr. Lipták Pál 1913-ban – a XXXII.DRP/1914. számú szabadalomként – nyújtotta be a szabadalmi hivatalhoz, illetve a M. Kir. Honvédelmi Minisztériumhoz a Lipták Vasgyár mérnökeinek harckocsitervét – ami akkor világelsőséget jelentett a harckocsifejlesztés területén.



2. ábra: A Lipták-féle első harckocsi vázlatos rajza
Forrás: Hajdú–Sárhidai 2005.

A Lipták-féle első harckocsi ennek a Holt Caterpillar traktornak acéllemezzel való beborításával készült, amelyet egy forgó toronyban elhelyezett géppuskával láttak el. 1915 tavaszán ki is próbálták, de a hadvezetés nem támogatta a konstrukciót. (A páncélzatkonstrukció egyik gyenge pontja a szegecselt lemezkonstrukció volt, mivel sikeres ellenséges találat esetén a szegecsek repeszként viselkednek a küzdőtérben.)



3. ábra: A Lipták-féle harckocsi második változatának vázlatos rajza
Forrás: Hajdú–Sárhidai 2005.

A második változatot 1915-ben tervezték meg, lépcsős testtel és géppuskafegyverzettel rendelkezett, és a Szakács-féle lángvetőt kapta fegyverként a toronyba, viszont ez a változat sem került gyártásba.

Lipták terve nem volt irreális: Holt Caterpillar alvázra az amerikaiak is építettek harckocsit 1916–17-ben. A traktortípust tüzérségi vontatóként is alkalmazták.

„A honvédség 1913 elején 1912-es típusú Holt-Caterpillar vontatókat rendelt a budapesti vezérképviselettől. A megrendelt vontatók gyorsan megérkeztek, és azok már 1913 tavaszán a honvéd tüzérség rendelkezésére álltak. A darabszámra következtetni lehet arról, hogy a közös hadsereg gépkocsizóosztaga (Automobil Abteilung) egy speciális tanfolyamon 24 főt képzett ki a lánctalpas vontató vezetési és kezelési ismereteire. Mozgósítás esetén a 30,5 cm-es mozsarak vontatórészlegéhez (Gelande dienst) kellett bevonulniuk. A Holt vontatók első háborús alkalmazására 1914 nyarán és őszén a nyugati hadszíntéren került sor. A Holt-Caterpillar vontatót 1917-ig elvileg akadálytalanul importálhatta Magyarország, de az amerikaiak hadüzenete miatt behozatala megszűnt. Az 1919-es év eseményeivel végleg lezárult a Holt-Caterpillar vontató katonai célra való alkalmazása hazánkban. A proletárdiktatúrát leverő, megszálló (román)

csapatok 37356 vasúti kocsi rakományban minden fellelhető gépalkatrészt és hadianyagot, köztük a lánctalpas Holt-vontatókat is elszállították az országból."[22]

3.3. Helikopterfejlesztés a Lipták Vasgyárnál

„A háború második felében a pestszentlőrinci Lipták-gyárban felállították a repülőosztályt, ahol repülőgépeket gyártottak."[23] Ezen a bázison kezdték meg a helikopter-prototípus gyártását 1917-ben.

Az első világháború alatt, 1916-ban, Petróczy István, az Osztrák–Magyar Monarchia hadseregének őrnagya (később repülő ezredes), azt a javaslatot terjesztette be a felső katonai vezetésnek, hogy a megfigyelésre használt, ám az ellenségnek könnyű célpontot jelentő léggömböket váltsák fel helikopterekkel.[24] 1916-ban a közös hadügyminisztérium a kötött tüzérségi megfigyelő ballonok felváltására alkalmas, motorral hajtott helikopterek készítését rendelte el. A Monarchia repülőcsapatainak legfontosabb fejlesztő intézete Wiener Neustadtban települt K. u. K. Fliegerarsenal (Repülőszertár) néven. Ennek részét képezte a fischamendi aerodinamikai laboratórium és a Légcsavar Kísérleti Intézet is. Itt számos magyar szakember dolgozott, a legismertebbek Petróczy István őrnagy (parancsnok 1917–1918), Kármán Tódor fizikus, tartalékos főhadnagy, továbbá Wilhelm Zurovecz tartalékos hadnagy, mérnök, illetve Asbóth Oszkár tartalékos főhadnagy, üzemvezető, Bier Henrik gépészmérnök és még sokan mások. Nevükhöz fűződik a PKZ-1 és PKZ-2 (Petróczy–Kármán–Zurovecz 1 és 2) kötött helikopter tervezése és megépítése, a Budapesti MÁG (Magyar Általános Gépgyár Rt.) és a Dr. Lipták és Társai Rt. gyárakban 1917–1918-ban.

1917 nyarán Petróczy István őrnagy, repülőkísérleti intézetvezető a gépek tervezésével Dr. Kármán Tódor professzor, tartalékos főhadnagy (fizikus) aerodinamikust bízta meg, míg a helikopter-prototípus gyártási munkálatokkal a budapesti Magyar Állami Gépgyárat és a Dr. Lipták és Társai Gépgyár Rt.-t.

Az Osztrák–Magyar Monarchia bécsújhelyi repülőkísérleti intézete 1917-ben Kármán Tódort kérte fel az első katonai kötött helikopter kifejlesztésére, aki fejlesztőcsoportjával két prototípust hozott létre: a PKZ-1 és PKZ-2 típusokat.

A PKZ-1 elektromotoros meghajtású kötött helikopter volt. A mátyásföldi MÁG 1917-ben kezdte az építést, és 1918 márciusában fejezte be, működése nem bizonyította az elektromos hajtás létjogosultságát. A villanymotor 195 kg tömegű, 140 kW (190 LE) teljesítményű volt 6000 f/min mellett. A légcsavarok 3,8 m és 4,2 m átmérőjűek voltak, négytollú forgószárnnyal. Fordulatszámukat reduktorral 800 1/min értéken állították be. A tömege 650 kg volt. A futómű helyén 4 felfújt ballon volt, és 3 kábel tartotta fix állapotban lebegés közben. Az első próbarepülések 1918 márciusában voltak a mátyásföldi hangárban. Ekkor 0,5 m magasságba emelték 750 f/min légcsavar érték mellett. 4 felszállás volt, az utolsónál az elektromotor leégett.

[22] Varga 2008.
[23] *Hadiipar Pestszentlőrincen.* é. n.
[24] Szabó szerk. 1991. 150–151.

A PKZ-2 robbanómotoros, kötött katonai megfigyelő-helikopter volt, a Dr. Lipták és Társai Rt. cég építette Pestszentlőrincen. 50 méteres magassági és 30 perces időtartamú világrekordot repült 1918-ban. 3 db francia 88 kW-os (120 LE-s) LeRhone 9 hengeres forgómotorral épült. A helikopter tömege 140 kg tüzelőanyaggal 1400 kg volt. A 2 db 6 m átmérőjű koaxiális, egymással ellentétesen forgó 2 tollú légcsavart Asbóth Oszkár tervezte meg és készítette el. Ezeket kúpáttételekkel, csőtengellyel hajtották, így fordulatszámuk 600 f/min volt.

Az eleve kötött üzemmódra tervezett helikoptert repülés során 3 kötéllel eresztették fel, a köteleket csörlővel tartották feszes állapotban. Korábbi kutatások 2005-ben és 2010-ben még Mátyásföldet jelölték meg az első helikopter felszállási helyszíneként, azonban a 2016-ban és 2021-ben közreadott helytörténeti kutatások már bebizonyították, hogy Pestszentlőrincen került sor a PKZ-2 helikopter első felszállására 1918. április 2-án, a Lipták-gyártelep északi részén, a mai Vaslemez és Reviczky utca sarkánál lévő sík területen.[25] Összesen 36 sikeres repülést végeztek el, ennek során a légcsavarok fölé felszerelték az 1,3 m átmérőjű és 1,5 m magas megfigyelőkosarat.

A felemelkedést két, egymással szemben forgó Asbóth-féle emelőlégcsavar biztosította. A helikopterek helyben lebegésének stabilizálását köteles kipányvázással biztosították.

A helikopter sárkányszerkezete acélcső-rács szerkezetű volt, a futómű egy nagy és 3 kis ballon volt, a középrész és a 3 motortartó konzol alatt.

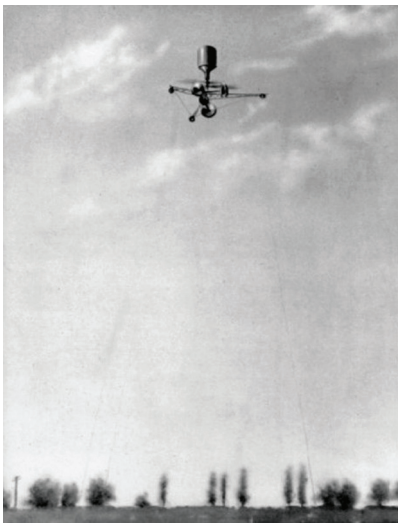
2. táblázat: PKZ-2 helikopter főbb adatai

Rotorátmérő	6,0 m
Rotorfelület	2 x 28 m^2
Tüzelőanyag- (benzin-) tömeg	140 kg
Max. felszálló tömeg	1400 kg
Repülési magasság max.	50 m
Repülési idő	1 h lebegés
Személyzet	1 fő megfigyelő

Forrás: Pokorádi 2009. 3–18.

A megfigyelőkosaras példány 1918. június végén egy kísérleti repülés alatt, 50 m magasban az oldalszél hatására, illetve a túlzottan magas súlypont miatt lengésbe jött, és nem tudták idejében lehúzni a kötelekkel, ezért lezuhant és megsemmisült.

[25] A PKZ-1 és PKZ-2 kötött helikopter, lásd Hajdú–Sárhidai 2005. 22–24; Hajdú 2010. 204–205. Azonban fotók és dokumentumok alapján Heilauf Zsuzsa helytörténeti kutató, muzeológus és múzeumvezető, illetve munkatársainak kutatásai pontosan meghatározták a PKZ-2 kísérleti repülések helyszínét a Lipták-gyár mellett. *Hadiipar Pestszentlőrincen.* é. n., illetve Pápai–Heilauf 2016. 58.



4. ábra: A megfigyelőkosaras PKZ-2 kötött helikopter 50 méter magasságban repül 1918 tavaszán Pestszentlőrincen, a Lipták-gyár mellett
Forrás: wikimedia.org/wikipedia/commons/6/60/A_PKZ-helikopter_50_méter_magasságban.jpg

A háborús helyzet rohamos romlása, majd az 1919-es kommün és a trianoni békeszerződés repülést tiltó passzusai miatt a magyar helikopterprogramot 1927-ig nem folytatták.

4. Lipták Pál életútja az első világháború után, szerepe a műszaki szakképzés szervezésében és a politikában, illetve a helikopterkísérletek utóélete

Az első világháború vége felé a kormány már nem volt képes finanszírozni a hadianyag-utánpótlás költségeit, de Lipták gyárai továbbra is szállítottak anyagot. 1917-ben Lipták kivált a cégből, és egy új magasépítési vállalkozásba kezdett, amely terület nem volt idegen a számára, mivel a korábbi években több épület (banképületek, igazságügyi palota) építését végezte. Az első világháború után a korábbi szállításokat nem fizették ki, és Lipták vagyonának, bányáinak jelentős része az országhatáron kívülre került, ezért a vállalata megszűnt.

1919-ben a gyár megkezdte a béketermelésre való áttérést, ezért munkásainak túlnyomó részét elbocsátotta. A román megszálló csapatok a raktáron lévő mintegy 250 000 darab készre szerelt tüzérségi lövedéket magukkal vitték, továbbá 168 munkagépet és 39 motort tulajdonítottak el. Amit pedig nem tudtak elvinni, azt annyira összetörték, hogy teljesen hasznavehetetlen legyen. Lényegében teljesen kifosztották a lőszergyárat is, 83 gépet és 26 villanymotort vittek haza magukkal. A román rablóhadjárat 2,5 millió korona összegű kárt jelentett, és ehhez jött még, hogy a termelés folytatása érdekében 2 millió korona költséggel más gépeket kellett átalakítani. Az üzem ezt követően bekapcsolódott a jóvátételi szállításokba: Lengyelország részére szállítandó mozdonyok javítására, készítésére rendezkedett be. 1919 decemberében

620, 1920-ban 1329, 1921-ben pedig 900 munkása volt. 1927-ben a Ganz és Társa-Danubius cégcsoport felvásárolta a vállalatot.

A korábban nagy kiterjedésű vállalat egy kisebb része hengerműként egészen a nyolcvanas évekig működött a pestszentlőrinci Hengersor utcában – ám jelentős részét lebontották, helyén ma a Havanna lakótelep áll.

Lipták Pál az első nemzetgyűlési választáskor a fővárosi XVI. kerület mandátumával jutott be a nemzetgyűlésbe, amelynek egyik vezető egyénisége és tagja volt 1920-tól 1922-ig. Tagja volt a nemzetgyűlés kivándorlási, közgazdasági, közlekedési és pénzügyi bizottságának. 1922-ben Emich Gusztáv kereskedelmi miniszterségé alatt államtitkári tisztséget vállalt a kereskedelmi minisztériumban, amelyet a következő két miniszter vezetése alatt is megtartott.[26] 1921-ben a szendrői bányáira alapozva megalapította a Borsod Szendrői Kőszénbánya Rt.-t. A háború alatt felhalmozott vagyona a húszas évek elején nagyobbrészt elenyészett, de még 1926-ban is megvoltak a kőszénbányái, Tokajban három gőzfűrész tulajdonosa, továbbá igazgatósági tagja volt a Közgazdasági Hitelbanknak.

Lipták egészsége 1926-ban megrendült, Balatonfüredre vonult vissza, majd 52 évesen elhunyt. 1926. május 15-én halt meg a balatonfüredi szanatóriumban. Síremléke a Fiumei Úti Nemzeti Sírkertben található. Emlékét a Lipták-telep őrzi Pestszentlőrincen. Lipták nevéhez kötődik továbbá egy villa Zuglóban, a Hermina út 3. alatt, amelyet Lipták Pál tervezett, és az épületet cége kivitelezte.

Lipták Pál nem élhette meg a magyar helikopterprogram folytatását, amelyet az 1919-es kommün és a trianoni békeszerződés repülést tiltó passzusai miatt 1927-ig nem folytathattak. A magyar helikopterprogramot Asbóth Oszkár folytatta, aki a PKZ-helikopter-fejlesztések időszakában szintén Fischamendben dolgozott, a Légcsavarkísérleti Intézetet vezette. A PKZ-1 és -2 helikopter-emelőlégcsavart (helikopterrotort, koaxiális rotort) a fischamendi légcsavargyártásért felelős Asbóth tervezte és gyártotta le. A háború után hazatérve Asbóth 1927–1930 között AH1-4 típusjelzéssel tökéletesítette az 1918-as PKZ-2 típust.

5. ábra: Asbóth helikoptere 1928-ban az Ecseri úti Cséry-vasút indulóállomás mellett repült, és a PKZ-2 kötött helikopter javított változatának volt tekinthető
Forrás: Fortepan, képszám: 200923, adományozó: Fortepan

[26] Vidor 1921. 86.; *Magyar Politikai Lexikon. Politikai Magyarország 2. kötet (1929–1935)*. 262.

A PKZ-2 túlzottan magas súlypontját egy, a légcsavar alatt elhelyezett pilótaüléssel javította Asbóth, míg a kormányzást az áramlásba helyezett kormánylapátokkal oldotta meg (részleges eredményre jutva). A PKZ-2 továbbfejlesztésének tekinthető AH-1-4 Asbóth-féle kötött helikopterek (az AH-1-AH-4 típusok együttvéve) 1927–1930 között összesen 182 repülést végeztek, 29 órát és 7,5 percet voltak a levegőben. 1930-ban az AH-4-et kipróbálta egy léghajózással foglalkozó angol repülőtiszt is. A helikoptert – a PKZ-2-höz hasonlóan – 1928-ban még kötelekkel stabilizálták. A merev légcsavar és a kormánylapos irányítási rendszer működött ugyan, de lényegében nem vált be, nem oldotta meg a helikopter hatékony kormányzásának kérdéseit (amihez csuklós, kollektív és egyéni rotorlapát-szögállítású helikopterrotor szükséges). Asbóth helikopterkísérleteivel tapasztalatokat gyűjtött, amelyből a hazai repülőszakma elméleti síkon haszonnal építkezhetett a továbbiakban (akár annak hiányosságaiból is).

A Lipták-gyár megszűnése után a Hengersor utcában 1934-ben Pestszentlőrinc első érettségit adó középiskoláját nyitották meg. A Pestszentlőrinci Magyar Királyi Állami Fiú Felsőkereskedelmi Iskola Pestszentlőrinc legrégebben nyílt középiskolája volt. Az új tanintézmény működését a Lipták-gyár igazgatósági épületének északi szárnyában kezdte el. Az épületben egy ideig polgári iskola, általános iskola és gimnázium működött. 1949-ben közgazdasági gimnázium, 1950-ben közgazdasági középiskola lett. 1952-ben ipari tagozatú közgazdasági technikummá alakult (más területek mellett ipari képzési irányú osztályokkal), és bekapcsolódott a felnőttek esti oktatásába is (dolgozók esti tagozata).[27] A közgazdasági technikumot közgazdasági szakközépiskolává szervezte át, és 2 általános irányú /ipari/, gép-, gyorsíró idegen nyelvi és gép-, gyorsíró általános ügyviteli szakközépiskolai osztály megnyitását engedélyezték. 1993-tól tagja lett a Csepel Térségi Integrált Szakképző Központnak. Jelenleg a Pestszentlőrinci Közgazdasági és Informatikai Szakközépiskola működik benne.

5. Összegzés

Dr. Lipták Pál gyára az egyik legjelentősebb magyar hadiüzem volt az első világháborúban. Eredményei jelentősek voltak a lőszergyártás és a merőben új területnek mondható vegyifegyver-gyártás területén is. Lipták 1918-as PKZ-2 helikopterrel folytatott helikopter-fejlesztései, „kísérletei a maguk korában a világ legjobb eredményeinek számítottak" Dr. Pokorádi László professzor szerint.[28] Harckocsifejlesztései szintén úttörő jellegűek voltak – még ha nem is vezettek eredményre. Lipták helikopterkísérletei viszont nem vesztek kárba, hiszen Asbóth Oszkár a Lipták-gyárhoz közel eső Cséry-telepen 1930-ra – bizonyos fokig – tökéletesítette a PKZ-2-t és eredményes repüléseket folytatott. Lipták Pál hadiüzemét egyszerre jellemezte a termelékenység és az innováció. Lipták Pál mérnök és gyáros vasbeton szerkezetekkel kapcsolatos tudományos munkássága, illetve építészeti hagyatéka és hadiipari

[27] A V.K.M június 15-én kelt /1934. V. a 2. sz. rendeletével alapította meg. Pestszentlőrinci Közgazdasági és Informatikai Szakközépiskola. Lásd: https://docplayer.hu/10875206-Pedagogiai-program-pestszentlorinci-kozgazdasagi-es-informatikai-szakkozepiskola.html

[28] Pokorádi 2009.

munkássága összességében a jelentős szakmai személyiségek közé sorolja őt a magyar haditechnika-fejlesztés történetében.

A Lipták-gyárban készültek az alábbi, kiemelt fontosságú ipari termékek:

- a világ egyik első helikopterének, a PKZ-2-nek a prototípusa;
- az első magyar harckocsi szabadalma, terve és prototípusa;
- hagyományos és vegyi lőszerek széles köre nagy darabszámban;
- vasbeton-építészettel kapcsolatos innovatív megoldások (amelyek Lipták külföldi tanulmányútjának tapasztalatain és doktori értekezésének kutatási eredményein alapultak).

Dr. Lipták Pál gyárában az alábbi korszerű technológiákat és magas fejlettségi szintű szaktevékenységeket honosította meg:

- együttműködés a Monarchia haditechnikai kutatás-fejlesztést végző intézetével;
- hulladék-újrahasznosításon alapuló korszerű acélgyártási technológia bevezetése (üzembe helyezte az első hazai März-kemencét és kidolgozta az eljárást annak kizárólag hulladékvassal üzemeltetésére);
- részvétel a hadiipar lőszergyártó teljesítményét fokozó Hindenburg-programban;
- közös gyár alapítása az enzesfeldi lőszergyárral (a Hindenburg-program részeként).

Személye, a nevéhez kötődő első magyar harckocsi-szabadalom és -prototípus, illetve a hadiipari gyárában folytatott helikopterkísérletek és prototípusgyártás igazán megérdemelnének egy emléktáblát.

Felhasznált irodalom

Bencze Géza – Remport Zoltán (2001): A Lipták-féle cég tündöklése és bukása. In *Ezer év innováció Magyarországon. Tanulmányok a természettudományok, a technika és az orvoslás történetéből.* Budapest, Műszaki és Természettudományi Egyesületek Szövetsége Tudomány- és Technikatörténeti Bizottsága. 161–166.

Bombay László – Gyarmati József – Turcsányi Károly (1999): *Harckocsik 1916-tól napjainkig*. Budapest, Zrínyi Kiadó.

Cséry Lajos – Lipták Pál. Tomory Lajos Múzeum hivatalos oldala. Online: http://muzeum18ker.hu/muzeumpedagogia/vetelkedok/csery-lajos-liptak-pal/

Dombrády Lóránd – Germuska Pál – Kovács Vilmos – Kovács Géza Péter (2017): *A magyar hadiipar története – A kezdetektől napjainkig 1880–2015*. Budapest, Zrínyi Kiadó.

Dr. Lipták Pál 1984–1926. (1926) *Körösvidék,* 7. évf. 110. sz. 1926. május 16.

Dr. Lipták Pál meghalt. (1926) *Békésmegyei Közlöny,* 53. évf. 110. sz. 1926. május 18.

Farkas Zoltán (2017): Lánctalpas futóművek. *Haditechnika,* 51. évf. 5. sz. 64–68. Online: https://doi.org/10.23713/HT.51.5.14

Grósz Mihály (1995): *Csabai életrajzok*. Békéscsaba.

Hadiipar Pestszentlőrincen. (é. n.). A Tomory Lajos Múzeum hivatalos honlapja. Online: http://muzeum18ker.hu/ipar/

Hajdú Ferenc (2010): Dr. Lipták Pál szerepe a XVIII. kerület kialakulásában és a haditechnikai fejlesztésekben. In *Mérlegen a Múlt. Írások Budapest XVIII. kerületének történetéből.* Budapest.
Hajdú Ferenc – Sárhidai Gyula (2005): *A Magyar Királyi Honvéd Haditechnikai Intézettől a HM Technológiai Hivataláig 1920–2005.* Budapest, HM Technológiai Hivatal.
Heilauf Zsuzsanna (é. n.): *Múltunk őrzői: érdekes épületek, közterületek a XVIII. kerületben*. Online: http://muzeum18ker.hu/heilauf-zsuzsanna/
Kelemen Ferenc (2018): A magyar hadiipar szerepe a kiegyezéstől 1918-ig. *Nagyhaboru. blog,* 2018. január 11. Online: https://nagyhaboru.blog.hu/2018/01/11/a_magyar_hadiipar_szerepe_a_kiegyezestol_1918-ig
Magyar Politikai Lexikon. Politikai Magyarország 2. kötet (1929–1935). Budapest, Magyar Lap- és Könyvkiadó Részvénytársaság kő- és könyvnyomdája.
Pápai Tamás László – Heilauf Zsuzsanna (2016): *Sorsfordulók – Pestszentlőrinc és Soroksárpéteri az első világháborúban*. Budapest, Tomory Lajos Múzeum. Online: http://muzeum18ker.hu/wp-content/uploads/2016/10/teljesk%C3%B-6tetnetre-1.pdf
Pokorádi László (2009): A helikopteres repülés első 100 éve. In *Debreceni Szemle 1.* 3–18.
Réz Gyula (2012): Az első Caterpillar traktorok Magyarországon. *Mezőgazdasági technika,* 2012. június. 38–39. Online: http://technika.gmgi.hu/uploads/termek_273/az_elso_caterpillar_traktorok_magyarorszagon_12_06.pdf
Szabó József szerk. (1991): *Repülési Lexikon 1. kötet*. Budapest, Akadémiai Kiadó.
Varga A. József szerk. (2008): *A magyar harc- és gépjármű-fejlesztések története*. Budapest, Maróti Könyvkiadó.
V.K.M június 15-én kelt /1934. V. a 2. sz. rendelete
Vidor Gyula (1921): *Nemzetgyűlési almanach 1920–1922. A nemzetgyűlés tagjainak életrajzi adatai.* Budapest, Magyar Lap- és Könyvkiadó Részvénytársaság kő- és könyvnyomdája.

HADMÉRNÖK
KATONAI LOGISZTIKA ÉS KÖZLEKEDÉS

17. évfolyam (2022) 4. szám 47–61.
DOI: 10.32567/hm.2022.4.4

Szajkó Gyula,[1] Fábos Róbert[2]

A pilóta nélküli légi járművek alkalmazhatósága a vasút- és közúthálózatok logisztikai felderítésében – 1. rész

Applicability of Unmanned Aerial Vehicles in Logistic Reconnaissance of Road and Railway Networks – Part 1

A béketámogató műveletek logisztikai támogatásának tervezési, szervezési folyamatainál fontos szerepet töltenek be a hadszíntér felderítéséből származó információk. A logisztikai felderítés magában foglalhatja a logisztikai támogatás szempontjából fontos körletekről, objektumokról, létesítményekről, közlekedési hálózatokról szóló információk feltérképezését és a megszerzett adatok rendszerezését. Ezek közül kiemelhetők a közlekedési hálózatok értékeléséből származó adatok, amelyek meghatározó jelentőséggel bírnak az erők mozgatásának, átcsoportosításának tervezésekor és végrehajtásakor. A közlekedési hálózatokat figyelembe véve a közúti és a vasúti infrastrukturális elemek főként az erők szárazföldi szállításakor válnak fontos tényezővé, amikor nagy létszámú személyi állományt és eszközt szükséges mozgatni. A hozzájuk kapcsolódó információk gyűjtésére többféle módszer áll rendelkezésre, a pilóta nélküli légi járművek alkalmazása csak az egyik ilyen lehetőség, mégis fontos lehet a logisztikai felderítést végző személyek vagy csoportok számára, mivel segítségével elérhetővé válhat az út- és vasúthálózatok helyszíni szemrevételezésének gyorsabb és pontosabb végrehajtása. Napjainkban a pilóta nélküli légi járművek típusai és felhasználásuk lehetőségei széles spektrumot ölelnek

[1] Tanársegéd, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Hadtáp, Pénzügyi és Katonai Közlekedési Tanszék; doktori hallgató, Katonai Műszaki Doktori Iskola, e-mail: szajko.gyula@uni-nke.hu
[2] Adjunktus, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Hadtáp, Pénzügyi és Katonai Közlekedési Tanszék, e-mail: fabos.robert@uni-nke.hu

fel. Ezeket célszerű megvizsgálni és elemezni: mely eszközök lehetnek alkalmasak logisztikai felderítés végrehajtására. A tanulmányban a szerzők célja, hogy – a teljességre törekvés igénye nélkül – bemutassák (csoportosítások alapján) a pilóta nélküli légijármű-típusokat, majd elemezzék gyakorlati tapasztalatok alapján a logisztikai felderítéshez kapcsolódó alkalmazhatóságukat.

Kulcsszavak: *logisztikai felderítés, pilóta nélküli légi járművek, vasút- és úthálózatok, szemrevételezés, béketámogató műveletek, logisztikai támogatás*

Information that derives from theatre reconnaissance plays an important role in planning and organising the process of logistic support of peace support operations. Logistic reconnaissance may contain information about areas, infrastructures, transportation networks and systematisation of these data which is very important for (the) logistic support. Data from the evaluation of transportation networks, which have crucial importance when movement and deployment tasks of forces are planned and conducted, can be highlighted. Considering transportation networks, road and railway infrastructure elements become important factors during land movement of forces when a significant amount of personnel and equipment are to be moved. There are different methods of gaining such information. The application of Unmanned Aerial Vehicles is one of the possible solutions, however, it can be important for personnel carrying out reconnaissance, because with the help of it inspection of road and railway networks can become quicker and more accurate. Nowadays, there are a wide range of types and applications of Unmanned Aerial Vehicles. It should be analysed which of them are (the most) suitable for conducting logistic reconnaissance. Without attempting to be comprehensive, the objectives of the authors of this article are to present the different types of Unmanned Aerial Vehicles and analyse their applicability for logistic reconnaissance based on practical experience.

Keywords: *logistic reconnaissance, Unmanned Aerial Vehicle, road and railway networks, visual inspection, peace support operation, logistic support*

1. Bevezetés

A Magyar Honvédség (MH) az elmúlt 25 évben különböző béketámogató műveletekben vett és vesz részt a jövőben a NATO, ENSZ, valamint az EBESZ szervezetek tagjaként. A feladatok végrehajtásakor fontos szempont, hogy az erőforrások a megfelelő időben, a megfelelő helyen, a megfelelő minőségben és mennyiségben az optimálishoz közeli költségráfordítással váljanak elérhetővé a küldetések teljes ciklusában. Ezt sikeres logisztikai művelettervezéssel lehet megvalósítani, amelyen keresztül kivitelezhető a műveletek támogatására kiépített ellátási láncok hatékony működtetése. A művelettervezési folyamatoknál a hadszíntéri logisztikai felderítésből származó adatok meghatározó jelentőségűek, mivel a közlekedési hálózatokról, logisztikai bázisokról, objektumokról, a javító kapacitásokról vagy a befogadó nemzeti támogatás keretében nyújtható szolgáltatásokról megszerzett információkkal nagymértékben lehet növelni az erők támogatásának sikerességét.

Ezért is fontos, hogy a logisztikai felderítés kitérjen minden olyan tényezőre, amely hatással lehet a logisztikai támogatás eredményességére. A logisztikai felderítési feladatok közül kiemelkedik a közlekedési hálózatok hadszíntéri értékelése, amely kifejezetten az erők mozgatásának, átcsoportosításának tervezésekor és szervezésekor jelentkezik kulcsfontosságú tényezőként. A személyek és eszközök a honi területről a kijelölt hadszíntérre történő mozgatásakor kombinált (légi, vízi, közúti és vasúti) szállítási módszert is alkalmazhatnak a művelettervezést végző törzsek. A közlekedési hálózatokat figyelembe véve az út- és vasúthálózatok főként az erők szárazföldön történő szállításakor válnak fontos részelemeivé az ellátási láncnak, amikor nagy létszámú személyi állományt és eszközt szükséges egyik pontról a másikra mozgatni. A közlekedési hálózatokhoz kapcsolódó információgyűjtő folyamatok végzésére többféle módszer is rendelkezésre áll a felderítést végző csoportok számára. Az egyik a logisztikai szemrevételezéssel (helyszíni szemlék teljesítésével), míg a másik lehetőség az informatikai hálózat(ok) felhasználásával beszerzett adatokkal hozzájárulni a közlekedési támogatási feladatok hatékony végrehajtásához, ezen keresztül a műveleti célkitűzések eléréséhez.[3] Azonban a helyszíni szemlék teljesítéséről elmondható, hogy a logisztikai felderítés egyik legfontosabb kulcseleme, amely nem pótolható semmilyen más felderítési módszerrel, ezért amikor lehetőség van rá, ezt kell alkalmazni a begyűjtött adatok pontossága és naprakészsége érdekében.[4] A helyszíni szemlék végrehajtásához érdemes tehát minden olyan eszközt igénybe venni, amely segítheti az információk gyors és precíz begyűjtését. A pilóta nélküli légi járművek alkalmazása az egyik ilyen lehetőség, segítségével egyszerűsíteni lehetne a vasúti és közúti hálózatok hadszíntéri értékelését. Napjainkban a drónok típusai és azok felhasználásának területei széles spektrumot ölelnek fel, amelyeket célszerű megvizsgálni és elemezni, következtetéseket levonni, hogy mely eszközök lehetnek leginkább megfelelőek a logisztikai felderítés eredményes teljesítéséhez.

A kétrészes tanulmányban célunk, hogy – a teljességre törekvés igénye nélkül – a tanulmány első részében bemutassuk a pilóta nélküli légijármű-típusokat, majd a második részben egy végrehajtott drónrepülésen keresztül, a készített fotók kiértékelésével elemezzük a logisztikai felderítéshez kapcsolódó alkalmazhatóságukat. Ehhez fel kívánjuk használni az út- és vasúthálózatok helyszíni katonai értékeléséhez használható szemrevételezési szempontokat tartalmazó listákat,[5] amelyek támpontot adnak a beszerzendő információk azonosításában és rendszeresítésében, így segítve a javaslatok pontosabb megfogalmazását.

1.1. Pilóta nélküli légi járművek osztályozása

Az eszközök csoportosítása elsősorban azért fontos a tanulmány szempontjából, mert segíti a javaslatok jobb meghatározását arra vonatkozóan, hogy mely járműveket célszerű használni a közlekedési hálózatok logisztikai felderítéséhez.

[3] *Magyar Honvédség Összhaderőnemi Támogatási Doktrína.* 2015.
[4] Magyar Honvédség 2015. 122.
[5] Szajkó 2019; Szajkó–Lévai 2021. 1.

Meghatározásával kapcsolatban többféle definíció létezik (különösen eltérő felhasználásai miatt), de általánosan elfogadott, hogy a pilóta nélküli légi járművek tulajdonképpen olyan repülőeszközök, amelyeket úgy terveztek, és úgy tartanak üzemben, hogy annak vezetését, irányítását nem a fedélzeten tartózkodó személy végzi.[6] Ezek a légi eszközök az ember fedélzeti jelenléte nélkül, autonóm módon képesek repülni.[7] A működésükhöz szükséges információkat a környezetükből gyűjtik, szenzorok segítségével érzékelik pozíciójukat, és egy döntési folyamat eredményeként működésüket, helyzetüket, mozgásukat a háromdimenziós térben korrigálják.[8] Ezt figyelembe véve az eszközök katonai alkalmazásával kapcsolatban már a 19. század végén is található írásos feljegyzés.[9] Az osztrák hadsereg 1849. augusztus 22-ei Velence ellen végrehajtott támadásánál például gyúlékony, robbanó anyagokkal megrakott, személyzet nélküli ballonokkal bombázták a várost. A későbbi időszakokban a kutatók, gyártók egyre nagyobb figyelmet fordítottak fejlesztésükre, így megjelentek az 1900-as évek elején a légi torpedók, majd a célrepülőgépek, ezt követően a második világháborúban a robotrepülőgépek, később a hidegháború ideje alatt a UAV[10]-k, amelyek már valóban automatizált pilóta nélküli légi járművekként funkcionáltak (és főként légi műveletekben robbanóanyagok célba juttatására, a légi erők kiképzésére és felderítési feladatokra használták).[11]

Az Amerikai Egyesült Államok fejlesztései közül kiemelhetők a vietnámi háború idején előállított UAV-k. Ezek a légi indíttatású járművek főként felderítési feladatokat hajtottak végre (például az ellenséges erők mozgásainak megfigyelését, objektumok, létesítmények azonosítását, elektronikai jelfelderítést, passzív zavarást vagy röplapszórást, megtévesztést) elérve akár a 18 000 méteres magasságtartományt is.[12] A vietnámi háború után az izraeli fejlesztések bemutatták, mennyire sokoldalúan lehet harcászati célokra felhasználni a UAV-ket. A Hermes 450 elnevezésű pilóta nélküli légi járművet már úgy tervezték, hogy fegyverekkel is fel lehessen szerelni, képes legyen 20 órát a levegőben repülni (200 km-es hatótávolsággal), amelyet az izraeli haderő alkalmazott is a Szudán elleni légi csapások végrehajtásakor.[13] A továbbfejlesztett Hermes 900-at már hőkamerával és célmegjelölővel is ellátták, valamint alkalmassá tették a fel- és leszállások automatikus végrehajtására is, elkerülve ezáltal a költséges indító platformok használatát. A felhasznált könnyű anyagok ellenére jelenleg a felszálló tömege 1180 kg, a törzse 8,3 m hosszú, míg szárnyfesztávolsága 15 m (1. ábra).[14]

6 Sándor–Boros 2017. 50.
7 Békési 2013a.
8 Szegedi–Békési 2015.
9 Monash University é. n.
10 *Unmanned aerial vehicle.*
11 Palik 2013.
12 Palik 2013. 37.
13 Elbit Hermes 450: Unmanned Aerial Vehicle (UAV). 2003.
14 Palik 2013. 43.

1. ábra: Hermes 900 repülés közben
Forrás: www.airforce-technology.com/projects/hermes-900/

A terjedelmes kialakítású UAV-k mellett az izraeli haderő törekedett arra, hogy szárazföldi gyalogsági egységeinek támogatására rendszeresítsenek kisebb méretű légi járműveket is. A kézi indítású harctéri felderítő eszközzel az alegységek képesek nagy felbontású, valós idejű képet készíteni a vizsgált területekről, amelyet ráadásul éjjel és rossz látási viszonyok között is lehet alkalmazni. A többcélú felhasználási lehetőségek kialakításával Izrael a világ legnagyobb UAV-exportőrévé vált.[15]

Napjainkban számos ország hadereje fejleszt vagy vásárol drónokat, hogy ezzel is támogassák a különböző műveletek sikeres végrehajtását. Az Amerikai Egyesült Államok és a NATO például a balkáni, afganisztáni vagy az iraki műveletekben is használt UAV-ket a felderítési feladatok teljesítéséhez, illetve a célpontok megsemmisítéséhez. Az eszközöket azonban nemcsak a védelmi iparban alkalmazzák, jelenleg számos példa mutatja, hogy polgári célú felhasználásai is egyre elterjedtebbé válnak. A UAV-ket használják például a városi közlekedésben forgalomszámláláshoz, a különféle csomagok (orvosi eszközök, postai küldemények) szállításához,[16] különböző adatok begyűjtéséhez (például a környezeti emisszió és a levegő összetételének mérésére)[17] vagy a mezőgazdaságban a korai gyom és vízháztartási problémák felmérésére, a vízhiány, tápanyaghiány meghatározására, a termésbecslésre, vadkárbecslést támogató, döntéshozó műveletek alkalmazására, valamint permetezésre.[18]

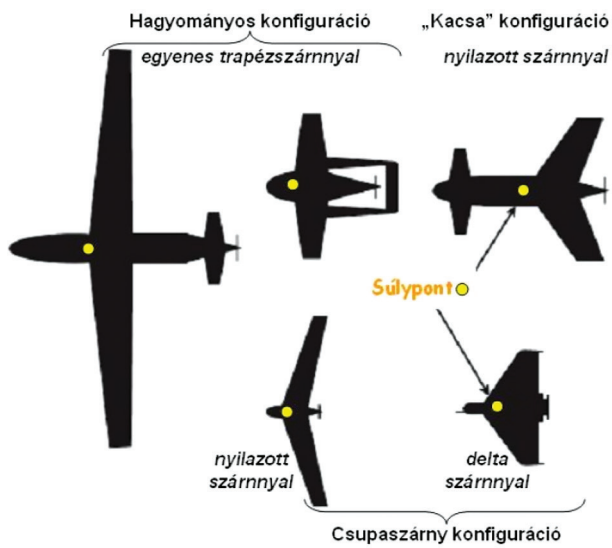
A változatos felhasználási lehetőségek egyben magukban hordozzák, hogy különböző típusú és kialakítású UAV-k találhatók a kereskedelemben, ennek megfelelően az osztályozásuk is különböző szempontok szerint valósítható meg, amit célszerű röviden ismertetni, mert segítséget nyújthatnak rendszerezésükben, összehasonlításukban és a javaslatok meghatározásában.

[15] Palik 2013. 44.
[16] Gupta et al. 2021. 345.
[17] Szabolcsi 2020. 135.
[18] Balázs é. n.

A felosztásuk történhet:[19]

- a felépítés (merev- és forgószárnyas, valamint hibrid járművek);
- a felhasználás módja (egyszeri és többszöri);
- a meghajtás (dugattyús, gázturbinás és elektromotoros);
- az irányítás módszere (távirányítású, programvezérelt és kombinált vezérlésű);
- az indítás módja (földi- és légi indítású);
- visszatérés módja (leszállással, ejtőernyővel, elfogó hálóval);
- repülési jellemzők (sebesség, magasság, hatósugár, repülési időtartam) alapján is.

A felépítés szerint megkülönböztetett UAV-k közül a merevszárnyú légi járművekről elmondható, hogy vezérlése kevésbé bonyolult, mint a forgószárnyas változatoknak, ráadásul nagyobb repülési sebességgel, magassággal és időtartammal is rendelkeznek.[20] A vízszintesen felszálló repülőgépek a stabilizátor elrendezésétől függően lehetnek hátsó-, első és stabilizátor nélküli, úgynevezett „csupaszárny konstrukciójúak.[21] Általában a vízszintesen felszálló UAV-k meghajtását biztosító légcsavarok toló vagy vonó kialakításúak lehetnek. Ennek a típusnak egyik nagy előnye, hogy a felderítési feladatok végzésére kialakított eszköz törzsében könnyebben elhelyezhetők az előre, oldalra és/vagy lefelé kitekintést biztosító optikai, valamint infrakamerák.[22] A merevszárnyú UAV-k között található hagyományos szárny–törzs–vezérsík konfigurációk, canard elrendezésű eszközök, csupaszárnyjárművek vagy deltaszárny-repülőgépek is (2. ábra).



2. ábra: A toló légcsavaros légi járművek konfigurációi
Forrás: Austin 2010. Figure 3.7 és Békési 2013a. 71.

[19] Békési–Békési 2013a; Békési 2013. 68.
[20] Palik 2007. 20.
[21] Békési 2013b.
[22] Békési 2011.

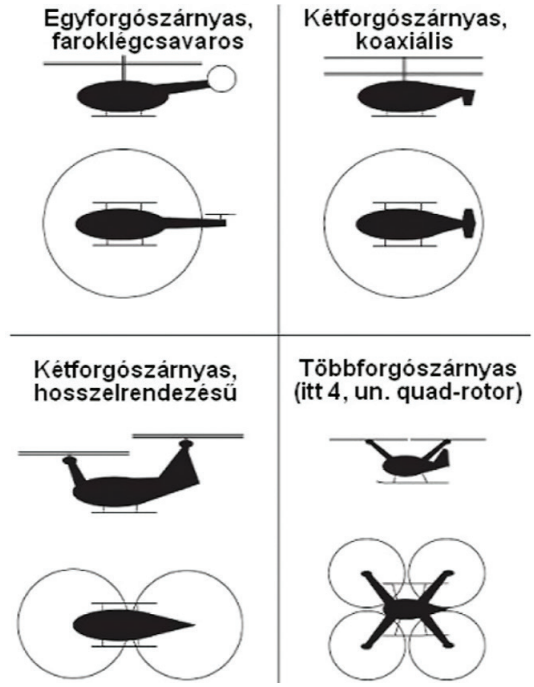
Ezek közül a hagyományos kialakítású a leggyakoribb megoldás, itt a törzsben helyezik el a hasznos teher nagy részét, ahol a hosszstabilitási tulajdonságokat a felhajtóerőt termelő szárny aerodinamikai centrumának tengelye előtti elhelyezésével biztosítják.[23] A 3. ábrán egy Seeker 400 UAS[24] látható, amely toló légcsavaros, szárny–törzs–vezérsík-konfigurációjú és automata fel- és leszállási képességekkel rendelkezik.

3. ábra: Seeker 400 UAS
Forrás: www.deneldynamics.co.za/album/UAVs/37

A canard típusú légi járműveknél a szárny előtt helyezkedik el a vízszintes vezérsík, így a fel- és leszálláskor részt vesz a felhajtóerő termelésében, ezáltal kevesebb úthossz és sebesség szükséges az emelkedéshez, illetve a landoláshoz. A csupaszárny-repülőgépek viszont nem rendelkeznek vízszintes vezérsíkkal, a csűrő kormánylapok mellé itt általában a magasságiakat is beépíthetik a szárnyon; egyik nagy előnye, hogy ezzel csökkenthető a homlokellenállás,[25] és a nagy fesztávolság kialakításával jó vitorlázó képesség biztosítható. A deltaszárny alkalmazásának fő jellemzője, hogy háromszög alakúak és 15°-os szárnynyilazási szögnél nagyobb szögben készülnek.[26] Előnyei közé tartozik, hogy erősebbre és merevebbre építhető, mint az előzőekben említett „társaik". Hátránya, hogy a támadási szöget a farok távolsága korlátozza, vagyis nehezebben tudja ellensúlyozni a szárnyak által okozott orrlefelé irányuló mozgást.

A forgószárnyas UAV-ket a helikopterekhez hasonlóan többféle megoldással is tervezik, amit a 4. ábra szemléltet.

[23] Békési 2013a. 71.
[24] *Unmanned aerial system,* pilóta nélküli légijármű-rendszer.
[25] A homlokellenállás két részből tevődik össze. Az egyik összetevő a határrétegen belüli súrlódásból, a másik pedig a nyomáskülönbségből ered. Rohács 2012. 71.
[26] Békési 2013a. 75.



4. ábra: Függőlegesen felszálló repülőgépek forgószárny elrendezései
Forrás: Austin 2010. Figure 3.9 és Békési 2013a. 76.

Az egyforgószárnyas járművekről elmondható, hogy vezérlése viszonylag nehézkes, ráadásul a faroklégcsavar fokozottan sérülékeny, könnyen ütközhet a talajjal a fel- és leszálláskor.[27] A kétforgószárnyas helikoptereknél kedvező tulajdonság, hogy a hossszelrendezés alapján ellentétes irányba forgó forgószárnyakkal nagyobb tömeg is emelhető, ennek ellenére kivitelezése – a pilóta nélküli légi járműveknél – még csak tervezési fázisban van.[28] A koaxális kétforgószárnyas UAV-k előnye, hogy a függőlegesen elhelyezett ellentétes irányban forgó szárnyak kialakításával nincs szükség faroklégcsavarra, és ezzel az elrendezéssel egyben optimális energiafelhasználás is biztosítható. Az úgynevezett Quad rotoros járművek a legnépszerűbb UAV-típusok között vannak napjainkban. A két-két egymással szemben forgó forgószárnyak fordulatszámainak módosításával érhető el az eszköz térbeli helyzetváltoztatása. Ennek megfelelően nincs szükség bonyolult rudazatrendszerre és a hozzá kapcsolódó vezérlő automatára, amelyek a legtöbb helikopternél biztosítják – a forgószárnylapátok beállítási szögének állításával – a vonóerő irányának és nagyságának változtatását.[29] Hátránya ugyanakkor, hogy kifejezetten érzékeny a széllökésekre és irányíthatatlanná válik, ha a fogószárnyak közül bármelyik is meghibásodik.

[27] Békési–Békési 2013b.
[28] Békési 2013a. 77.
[29] Békési 2013a. 79.

A hibrid hajtások kedvező tulajdonsága, hogy az eszközök képesek a forgószárnyakat függőleges és vízszintes üzemmódban is használni, így a jármű – a helikopterekhez hasonlóan – képes kisebb helyen felszállni, és a forgószárnyainak vízszintes helyzetbe állításával – a repülőgépeknél jellemző – gyorsabb utazó sebességet is elérni. Az egyik kifejlesztett megoldásnál az eszköz légcsavarja és motorja egyszerre fordul el, majd képez az emelőerőből vonóerőt, míg a másik típusnál már a szárnyak is el tudnak mozdulni a légcsavarral és motorral együtt. Közös jellemzőjük (az előnyökön kívül), hogy fajlagos teherbírásuk kisebb, és drágább áron lehet beszerezni a piacokon, mint a hasonló „egyfunkciós" drónokat.[30]

A felhasználás célja szerint megkülönböztethetünk egyszeri és többszörös felhasználású eszközöket. Az egyszeri felhasználású járművek két alkategóriába sorolhatók: csapásmérő UAV-k és célrepülőtestek. A csapásmérő UAV-k általában önállóan derítik fel, azonosítják, és szükség szerint magukkal együtt semmisítik meg a megfigyelés alá vont célokat. A célrepülőtestek csoportjába azok az eszközök tartoznak, amelyeket a kiképzéseken, gyakorlatokon a különböző fegyvernemek (tüzéregységek, repülőcsapatok) célok imitálására használnak. A többszöri felhasználású UAV-k csoportjába pedig valamennyi légi jármű beletartozik, amelyekkel megoldható a – földi és navigációs eszközeivel – a repülőtestek visszavezetése és leszállítása.[31]

A meghajtás módja alapján a UAV-k lehetnek dugattyús, gázturbinás és elektromos elv szerint működők. A dugattyús motorral hajtott járművek általában egy- vagy többhengeres (kettő, négy) változatban vonó, illetve toló légcsavarral készülnek. Előnyük, hogy kevésbé zajosak, megbízhatók, és kevés kiegészítő berendezés szükséges működésükhöz.[32] A gázturbinás hajtóművek többféle kialakítással készülhetnek, ezek lehetnek:[33]

- sugárhajtóművek:
- egyáramú sugárhajtóművek;
- kétáramú sugárhajtóművek;
- turbólégcsavaros hajtóművek;
- légcsavar-ventillátoros hajtóművek.

Általában ezek a légi járművek már képesek a sztratoszférában repülni és hadműveleti-hadászati felderítést, valamint zavarást is végrehajtani. Ennek megfelelően a repülőgépeket úgy tervezik, hogy a felderítésüket gátolva a visszaverő felületük csekély legyen, valamint optimális üzemanyag-felhasználással és minimális hőkibocsátással rendelkezzenek. Az elektromos UAV-k meghajtását biztosító akkumulátorok és az elektromotorok hatásfokának emelkedésével egyre inkább alkalmazott erőforrássá vált ez a típus napjainkban, háttérbe szorítva az előzőekben említett eszközöket. Az elektromos légcsavarral működő légi járműveket kis magasságon – harcászati szintű felderítésekre – használják (katonai alkalmazását tekintve), mivel képes 1–1,5 órát

30 Békési 2013a. 81.
31 Békési 2013a. 86.
32 Békési et al 2012.
33 Sánta 2008.

a levegőben maradni, megtenni akár 50–70 kilométert, ráadásul kis méretű és csöndes, ami nehezíti az eszközök felderítését, észlelését.[34]

Az irányítás módja szerint az UAV-k lehetnek távirányítású, programvezérelt vagy kombinált vezérlésű légi járművek. A távirányítású repülőgépeknél a fel- és leszállás, valamint a levegőben történő repülés csak „emberi" segítséggel, távirányítással valósítható meg. Ennek megfelelően a biztonságos üzemeltetéshez elengedhetetlen, hogy az eszköz vizuálisan látható legyen, vagy rendelkezzen olyan rádiólokációs, optikai berendezéssel, amellyel a jármű folyamatosan nyomon követhető, és a repülési jellemzőkről megfelelő mennyiségű adat biztosítható az operátor részére.[35] A programvezérlésű UAV-k már a teljes működésüket önállóan hajtják végre a fedélzeti számítógép memóriájába táplált adatok segítségével. A repülés pontos teljesítéséhez a járműveket különböző fedélzeti, kis magasságú és navigációs rendszerekkel látják el, amelyek a felszállás után azonnal aktiválódnak.[36] Rendszerint felderítő és csapásmérő feladatok végrehajtására alkalmazzák ezeket az eszközöket. A kombinált irányítású UAV-knél ötvözik a távirányítású és a programvezérelt módszereket. A rendszert általában úgy alkalmazzák, hogy a légi járművet a földi ellenőrző pontig irányítják (távirányítással), majd a fedélzeti számítógépnek küldött utolsó parancs feldolgozását követően az eszköz átáll a programozott repülésre és teljesíti a részére előzetesen meghatározott feladatokat (például a harcmező felderítését). A kombinált vezérlés egyik nagy előnye, hogy a földi ellenőrző állomás paraméterei nincsenek hatással a hatótávolságra, ráadásul a kritikusnak tekinthető fel- és leszállási manőverek távirányítással megoldhatók, ami szintén növeli a rendszer biztonságát.

A UAV-k indítását figyelembe véve különböző módszereket is alkalmazhatnak a felhasználók, attól függően, hogy milyen szerkezeti kialakítással és felszálló tömeggel rendelkeznek a pilóta nélküli légi járművek. Ezek alapján a UAV-k lehetnek földi és légi indítású repülőeszközök. A földi indításúak közül a kis súlykategóriába tartozó gépeket (max. 10 kg) általában emberi kéz segítségével hozzák működésbe. Hátránya, hogy az indításukhoz (a levegőbe juttatás pillanatában) két ember is szükséges, és a merevszárnyúaknál a dobástechnikát is indokolt elsajátítani a működtetőknek. Előnyük ugyanakkor, hogy bárhol elindíthatók terepen, ahová a felhasználók gyalog is el tudnak jutni. A közepes tömegű UAV-k indításához már általában indítókatapultot használnak, amely lehet:[37]

- elasztikus (gumiköteles);
- pneumatikus és hidraulikus
- vagy rakétaindítási elv szerinti meghajtású.

Az elasztikus katapultnál az elindításhoz szükséges energiát a kötél előfeszítésével állítják elő, amely emberi erővel vagy csörlő segítségével is megvalósítható.

[34] Békési 2013a. 89.
[35] Forbes 2017.
[36] Békési 2013a. 91.
[37] Békési 2013a. 93.

Az indítókatapultos megoldásoknál a kinetikus energiát szolgáltathatja egy kompresszor vagy egy akkumulátor is (5. ábra).

5. ábra: Hermes 450 indítása pneumatikus meghajtással
Forrás: HERMES450-robonic-launcher.jpg (400×182) (defense-update.com)

A rendszer előnye, hogy a UAV-k felszállási helye csak az indítóállvány terepjáró képességétől függ, hátránya, hogy az előállítási költségek magasak lehetnek és nagyobb tömeg felett már nem biztonságos a használatuk sem. Ezt a problémát oldja fel a segédhajtómű (gyorsító rakéta) alkalmazása. A rakétaindítással a légi jármű már nem igényel más energiaforrást és bármely helyzetből képessé válik a felszállásra. A rakéta kiégése után leválik a UAV-ről, hogy az eszköz a saját hajtóműve segítségével folytassa tovább repülését.[38] Katonai alkalmazását tekintve hátrányként említhető, hogy a felszállást hang- és fényhatás kíséri, amely könnyen felderíthető, ráadásul a rakéták üzemeltetése, tárolása, illetve szállítása is kockázatokat, veszélyeket jelenthet a felhasználó számára. A légi indítású UAV-k rendszerint repülőgép vagy helikopter fedélzetéről indulnak. Általában ezeket az eszközöket nagy hatótávolságú felderítési feladatokra használják, és főként nagy repülési magasságon és sebességgel hajtanak végre.[39] Ennek megfelelően a UAV-k előre programozottan teljesítik repülésüket, hogy a felderítéskor megszerzett információkat valós időben tudják továbbítani a földi ellenőrző állomásra.

A visszatérés alapján is meg lehet különböztetni a pilóta nélküli repülőeszközöket, aminek azért lehet fontos szerepe a kiválasztásban, mert általánosságban elmondható, hogy a UAV-k legtöbbször a visszatéréskor (leszálláskor) „szenvednek el" szerkezeti

[38] Békési 2013a. 95.
[39] Békési 2013a. 96.

sérüléseket. A visszatérés szerint a UAV-k leszállhatnak a saját futóművük, az ejtőernyő és elfogóháló segítségével is (6–7. ábra).

6. ábra: Ejtőernyővel landoló UAV
Forrás: https://manta-air.com/uav_safety_and_recovery_systems/

7. ábra: Elfogóhálóval visszatérő UAV
Forrás: https://upload.wikimedia.org/wikipedia/commons/b/ba/Iowa_drone.jpg

A futóművel visszatérő repülőeszközöknél a fel- és leszállást távirányítással oldják meg, mivel a teljes automatizálás még nem minden légi járműnél érhető el. A landolást figyelembe véve többféle kialakítással készülhetnek a UAV-k, amelyek lehetnek hasra, kerékre, csúszó- vagy rúgóstalpra leszálló eszközök. Az utóbbi a kerekes megoldás továbbfejlesztett változata, amelynél kevesebb kockázattal jár az eszköz felborulása (landoláskor) akár előkészítetlen terepen is. A UAV-k csúszótalpra történő biztonságos leszállása, viszont általában csak egyenes, füves vagy homokos területen hajtható végre. A kerekekkel felszerelt légi járműveknél a leszálláshoz szükséges „úthossz" csökkentését pedig a kerekek fékezésével és elfogóhorog alkalmazásával érik el az irányítók. A kerekes és csúszótalpas eszközöknél rendszerint hidraulikus rugóstagot is használnak annak érdekében, hogy a talajtól származó ütközési energia ne tegyen kárt a járműben.[40] A sérülések csökkentését lehet elérni továbbá az ejtőernyők alkalmazásával. Általában a kis és közepes tömegű UAV-kre szerelnek fel ejtőernyőt: a meghatározott leszálló terület fölé érkezésekor (programozva vagy távirányítással) a magasság, sebesség és irány beállítása után az eszköz „kinyitja" az ejtőernyőjét, hogy a földet érése biztonságosan végrehajtható legyen. Az újabb fejlesztésekre már légzsákokat is felszerelnek, hogy a leszálláskor jelentkező ütközés hatása kisebb mértékű legyen. Talán legfontosabb előnyeinek egyike, hogy nem igényel leszállópályát, ugyanakkor a landolás pontos koordinátái nehezen behatárolhatók, így csak szárazföldön használhatók egyelőre (a jelenlegi fejlesztéseket figyelembe véve) eredményesen. Az elfogóháló viszont ezt a hiányosságot szüntetheti meg, amelyet főként hajókon alkalmaznak kis felszálló-tömeggel rendelkező UAV-k landolásához. Hátránya, hogy az eszköz elfogóhálóval történő biztonságos leszállítása pontos navigációt és szélmentes időjárást igényel.

[40] Békési 2013a. 98.

A repülési jellemzők alapján a UAV-ket be lehet sorolni kategóriákba a repülési magasságuk, a sebességük, a hatósugaruk és a repülési időtartamuk szerint is. A könnyebb áttekinthetőség érdekében táblázatba foglaltuk össze a repülési jellemzők szerint megkülönböztetett pilóta nélküli repülőeszközöket (1. táblázat).

1. táblázat: Repülési jellemzők alapján csoportosított UAV-k

Típus	**Repülési magasság**		**Üzemidő**	**Hatótávolság**	**Repülési sebesség**
MAV[41]	alacsony magasság	maximum néhány 10 méter	néhány perc	néhány 100 méter	Kis sebességű 0–350 km/h repülési sebességű
LASE[42]		néhány 10–100 méteres magasság	néhányszor 10 perc	néhány km	
LALE[43]		néhány 100 méteres magasság	néhányszor 30 perc	néhány 10 km	
MALE[44]	közepes néhány km-es magasságig		néhány órás időtartam	több száz km	Kis sebességű 0–350 km/h repülési sebességű /Nagy sebességű 350–1000 km/h repülési sebességű
HALE[45]	nagy magasságban 10–30 km között		néhányszor 10 óra	több ezer km	

Forrás: Szajkó Gyula szerkesztése Sándor–Boros 2017. 51. alapján

Látható, hogy a lehetséges feladatoktól függően többféle UAV-k közül választhatnak a felhasználók, ez a fajta csoportosítás lehetőséget ad javaslatok megfogalmazására a logisztikai felderítéshez használható pilóta nélküli repülőeszközökre vonatkozóan is. Természetesen célszerű megvizsgálni milyen feladatok kapcsolódhatnak a logisztikai felderítéshez, azon belül – az erők szárazföldi mozgatásában kulcsfontossággal bíró – vasút- és közúthálózatok értékeléséhez. A következő részben ismertetjük ezért röviden a UAV-k lehetséges katonai alkalmazását, a logisztikai felderítéshez kapcsolódó feladatokat, valamint a vasút- és úthálózatok értékeléséhez használható szemrevételezési szempontokat tartalmazó listákat. Ezt követően bemutatjuk (gyakorlati tapasztalat alapján) a pilóta nélküli repülőeszközzel szerzett információk (elkészített képek, fotók) feldolgozhatóságát, hogy javaslatot fogalmazzunk meg a közlekedési hálózatok értékeléséhez használható UAV-típusok felhasználására vonatkozóan.

(folytatjuk)

41 *Micro air vehicle*: mikro pilóta nélküli repülőeszközök.
42 *Low altitude, short endurance*: kis repülési magasságú rövid repülési időtartamú.
43 *Low altitude, long endurance:* kis repülési magasságú, hosszú repülési időtartamú.
44 *Medium altitude, long endurance:* közepes repülési magasságú, hosszú repülési időtartamú.
45 *High altitude, long endurance:* nagy repülési magasságú, hosszú repülési időtartamú.

Felhasznált irodalom

A Global Defence Technology Company (2022): *UAVs.* Online: www.deneldynamics.co.za/album/UAVs/37

Austin, Reg (2010): *Unmanned Aircraft Systems UAVS Design, Development and Deployment.* John Wiley & Sons Ltd. Online: https://doi.org/10.1002/9780470664797

Balázs Viktor (é. n.): *Nemzeti Agrárgazdasági Kamara, Mezőgazdasági termelés, Drón, Monitoring, Adatgyűjtés.* Online: https://bit.ly/3B2AGSz

Békési Bertold (2011): UAV-k sárkányszerkezeti megoldásai. *Szolnoki Tudományos Közlemények,* 15. Szolnok. 1–11.

Békési Bertold et al. (2012): *Pilóta nélküli légijárművek: kategorizálás, fedélzeti hardver besorolás.* Kutatási jelentés. Szolnok.

Békési Bertold (2013a): Pilóta nélküli légijárművek jellemzése, osztályozásuk. In Palik Mátyás szerk.: *Pilóta nélküli repülés profiknak és amatőröknek.* Budapest, Nemzeti Közszolgálati Egyetem. 65–110. Online: www.repulestudomany.hu/kiadvanyok/UAV_handbook_Secon_edition.pdf

Békési Bertold (2013b): Pilóta nélküli légijármű típusok sárkányszerkezeti megoldásai. In Pokorádi László szerk.: *Műszaki tudomány az északkelet-magyarországi régióban 2013 konferencia előadásai*. Debrecen, Debreceni Akadémiai Bizottság Műszaki Szakbizottság. 122–132.

Békési Bertold – Békési László (2013a): Merevszárnyú pilóta nélküli légijárművek (UAV-k). *Szolnoki Tudományos Közlemények,* 17. Szolnok. 7–34.

Békési László – Békési Bertold (2013b): Forgószárnyas pilóta nélküli légijárművek. *Economica,* 6. évf. 2. sz. 88–98. Online: https://doi.org/10.47282/ECONOMICA/2013/6/2/4421

Elbit Hermes 450: Unmanned Aerial Vehicle (UAV). 2003. Online: www.militaryfactory.com/aircraft/detail.php?aircraft_id=824

Forbes (2017): *What Are The Differences Between Drones, UAVs, And RPVs?* Online: www.forbes.com/sites/quora/2017/08/15/what-are-the-differences-between-drones-uavs-and-rpvs/?sh=34bbf65f7b21

Magyar Honvédség Összhaderőnemi Logisztikai Támogatási Doktrína. (2015) (3. kiadás). Budapest, Magyar Honvédség.

Monash University (é. n.): *Remote Piloted Aerial Vehicles: An Anthology.* Online: www.ctie.monash.edu/hargrave/rpav_home.html

Gupta, Anunay – Afrin, Tanzina – Scully, Evan – Yodo, Nita (2021): Advances of UAVs toward Future Transportation: The State-of-the-Art, Challenges, and Opportunities. *Future Transportation,* 2. évf. 1. sz. 326–350. Online: https://doi.org/10.3390/futuretransp1020019

Manta Air (2020): *UAV Safety & Recovery: A safe flight ends with a safe landing.* Online: https://manta-air.com/uav_safety_and_recovery_systems/

Palik Mátyás (2007): *Pilóta nélküli légijármű rendszerek légi felderítésre történő alkalmazásának lehetőségei a légierő haderőnem repülőcsapatai katonai műveleteiben.* PhD-értekezés. Budapest. Online: http://hdl.handle.net/20.500.12944/12060

Palik Mátyás (2013): A pilóta nélküli repülés rövid története. In Palik Mátyás szerk.: *Pilóta nélküli repülés profiknak és amatőröknek.* Budapest, Nemzeti Közszolgálati Egyetem. 25–60.

Rohács József szerk. (2012): *Aerodinamika.* BME Közlekedésmérnöki és Járműmérnöki Kar, 2012. Online: www.vrht.bme.hu/letoltes/Tanszeki_letoltheto_anyagok/Oktatok_anyagai/Jankovics_Istvan_anyagai/Aerodinamika/Rohacs_Gausz_Aerodinamika.pdf

Sándor Zsolt – Boros Péter (2017): Pilóta nélküli légi járművek okozta kihívások a légiforgalmi irányításban. *Közlekedéstudományi Szemle,* 67. évf. 6. sz. 49–58. Online: http://real.mtak.hu/70631/7/49_PDFsam_KTSZ_2017_06_print%20v%C3%A9gleges.pdf

Sánta Imre (2008): *Repülőgép-hajtóművek elmélete I. (Gázturbinás hajtóművek).* Előadásvázlat. Budapest.

Szabolcsi Róbert (2020): Multirotoros pilóta nélküli légijárművek háromdimenziós repülési pályáinak számítógépes tervezése és szimulációja. *Hadtudomány*, 30. évf. 4. sz. 133–150. Online: https://doi.org/10.17047/HADTUD.2020.30.4.133

Szajkó Gyula (2019): Az út és úthálózatok értékelése a hadszíntéri logisztikai felderítés végrehajtásakor. *Hadmérnök,* 14. évf. 4. sz. 61–77. Online: https://doi.org/10.32567/hm.2019.4.4

Szajkó Gyula – Lévai Zsolt (2021): A vasúthálózatok értékelése a hadszíntéri logisztikai felderítés végrehajtásakor. *Hadtudományi Szemle,* 14. évf. 1. sz. 27–52. Online: https://doi.org/10.32563/hsz.2021.1.3

Szegedi Péter – Békési Bertold (2015): *Az UAV-on alkalmazható szenzorok.* XIV. Természet-, Műszaki és Gazdaságtudományok Alkalmazása Nemzetközi Konferencia. Szombathely, Nyugat-magyarországi Egyetem. 175–182. Online: http://publicatio.nyme.hu/613/1/TTK_14_Nemzetkozi_Konf_Eloadasok_201500516.pdf

HADMÉRNÖK
KATONAI MŰSZAKI INFRASTRUKTÚRA

17. évfolyam (2022) 4. szám 63–73.
DOI: 10.32567/hm.2022.4.5

Ember István[1]

3D nyomtatott lyukasztó töltetek hatásvizsgálata[2]

Efficacy Trial of 3D Printed Shaped Charges

A kumulatív töltetek alkalmazása sok esetben kifejezetten fontos lehet a robbantástechnikában. Ezek az alkalmazási területek egyaránt lehetnek civil, ipari vagy katonai vonatkozásúak. A 3D nyomtatás jelentősége minden tekintetben kiemelkedő, alkalmazása komoly előnyöket hordozhat. A vizsgálat megmutatja, hogy ezek a töltetek hatékonyak lehetnek alacsony sűrűségű béléstestekkel is. A félgömb és kúp alkatelemek esetében egyértelműen meghatározható, hogy melyik képes hatékonyabban átütni a céltárgyakat a vizsgált paraméterek mellett. A több méretben felrobbantott kumulatív töltetek penetrációs képessége tekintetében leszögezhető, hogy ilyen vastagságú céltárgyakat kisebb töltet is képes lehet átütni. Ez további vizsgálatokat igényel.

Kulcsszavak: **kumulatív töltet, robbantás, vizsgálat, 3D nyomtatás**

The use of shaped charges may be vital in lots of cases in blasting technique. These fields of adaptation can be civilian, industrial, or military. The importance of 3D printing is significant in every aspect, the adaptation of the method may provide indicative benefits. The trial shown below indicates that these charges can be effective with low density liners. In the case of a semi-sphere and a cone part the outcome shows which of those types can produce the most effective penetration within the circle of test parameters. The shaped charges were blasted in multiple size, and it is absolutely certified that a smaller type may be effective too on the same target. This fact determines more tests in the future.

Keywords: **shaped charge, blasting, trial, 3D printing**

[1] Egyetemi tanársegéd, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Műveleti Támogató Tanszék; Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Hadtudományi Doktori Iskola, doktori hallgató, e-mail: Ember.Istvan@uni-nke.hu

[2] A cikk az Innovációs és Technológiai Minisztérium ÚNKP-21-3-II-NKE-26 kódszámú új nemzeti kiválóság programjának a nemzeti kutatási, fejlesztési és innovációs alapból finanszírozott szakmai támogatásával készült.

1. Bevezetés

A robbantástechnika alapvetően a gyorsan fejlődő területek közé tartozik, bár vannak elemei, amelyek akár évszázados múltra tekintenek vissza. Napjainkban nem is lehet kérdés, hogy a technológiai fejlődés meghatározó eszközei szintén részei lesznek ennek a fejlődési folyamatnak. A 3D nyomtatás manapság már viszonylag olcsón elérhető akár otthonainkban is, a széles körű használatot csupán az egyedi alkatrészek számítógépes tervezésének nehézségei akadályozzák, bár egyre egyszerűbb megoldásokat találhatunk erre a problémára.

Katonai vonatkozásban szintén van létjogosultága a robbantási feladatok ilyen irányú fejlesztésének, vizsgálatának. A kitűzött mérvadó kutatási irányok[3] közül több területen hozhat gyakorlatban is alkalmazható eredményt a 3D nyomtatás.

A kumulatív töltetek egyes robbantási feladatokban nélkülözhetetlen előnyöket hordoznak, méretezésük széles skálán lehetséges.[4] A bennük alkalmazott robbanóanyagok alapvetően brizáns és többnyire bináris[5] változatok lehetnek.

Jelen vizsgálatban egy ilyen, 3D nyomtatással készült töltetsorozat hatékonyságának vizsgálatát és annak eredményét mutatjuk be. Az eredmények vélhetően jó alapjai lesznek a további fejlesztési, méretezési folyamatoknak. Mivel egy első vizsgálati sorozatról van szó, a tölteteket és az alkalmazott céltárgyakat a vizsgált típusok szűkítése céljából állítottuk össze, ezzel optimalizálva az erőforrások felhasználását, valamint a nyomtatási és tervezési idővel történő gazdálkodást.

2. A kialakított töltetváltozatok

Több változatot alakítottam ki a kumulatív tölteteknél. Méretezésük során alapvető adatnak a béléstest belső átmérőjét vettem. Ez a méret határozta meg a későbbiekben az eltartást vagy fókusztávolságot, amely a kumulatív sugár kialakulásához biztosítja a szükséges teret. Ennek a méretnek a fontossága jelentős, mert a töltet hatékonyságát nagyban befolyásolhatja.

A méreti jellemzők mellett nem elengedhetetlen szempont a visszaáramlásgát kialakítása, amely szintén a fentebb említett kumulatív sugár tökéletesebb formálódását segítheti az által, hogy a céltárgyról visszaverődő anyagsugarat elvezeti.

Másik fontos kérdés a béléstest, amely minden kétséget kizáróan a legtöbbet nyomja a latban, ha egy kumulatív töltet hatékonyságát vizsgáljuk. Vitán felül áll, hogy a fémek alkalmazása, különös tekintettel a rézé, eredményezheti a legnagyobb átütést. A sűrűség ennél az alkatelemnél kifejezetten fontos, mert a céltárgy és a kumulatív sugár találkozáskor ideális folyadékokként viselkednek, ha a folyamatot fizikai leírással szeretnénk értelmezni. Történik ez annak ellenére, hogy a fémekből robbantásos roncsolással formált kumulatív sugár szilárd halmazállapotú.[6]

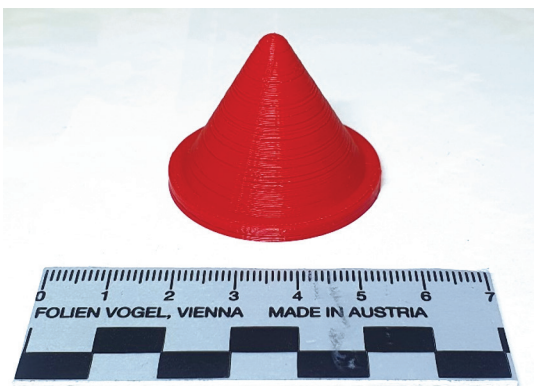
[3] Boda et al 2016.
[4] Lukács 2010.
[5] Kugyela 2020.
[6] Doig 1998. 1.

Jelen vizsgálatban azonban alacsony sűrűségű anyagból kialakított béléstestekkel szerelt tölteteket teszteltünk. Ez néhány esetben kifejezetten hasznos lehet, mégpedig akkor, ha csak egy meghatározott vastagságú anyagot kell kilyukasztani, és az anyag másik oldalán elvárt a jelentős hatáscsökkenés.

Éppen ezért a 3D nyomtatásban legelterjedtebb anyagot, a politejsavat[7] (PLA) választottam. Az anyag sűrűsége kellően alacsony[8] a fémekhez képest. Mivel a vizsgálat során összehasonlítási alapnak is meg kell jelennie, két geometriai forma mellett döntöttünk a béléstestek esetében. A kúp triviális választás volt, a területen jártas szakembereknek további magyarázatra nem szorul. A kúpszög esetében a 60^0-ot választottuk, amely hatékonyság szempontjából kiemelkedő és nyomtatástechnikai szempontból is könnyen kivitelezhető. Mindezek mellett hegyesebb kúpszög esetén a töltetház is megnyúlna, amely a plasztikus robbanóanyaggal történő feltöltés során nehezítené a készre szerelés mozzanatát. A félgömb tekintetében jelentős méretezést nem igényelt az elgondolás kialakítása, bár előfordulhat, hogy különböző magasságú gömbszelet alkalmazása módosíthatná a hatékonyságot.

A béléstestek esetében az anyag vastagságát 3 mm-ben határoztuk meg, annak ellenére, hogy egyes kutatási eredmények szerint[9] ennek a fele is kellő hatékonyságú. Mivel azonban más hasonló vizsgálatok ezt nem igazolták, maradtunk a kitűzött paraméternél.

Ezek mentén tehát három méretben készültek béléstestek: 40 mm, 35 mm és 30 mm. A forma tekintetében minden méretből készült kúp (1. ábra) és félgömb (2. ábra) változat is.



1. ábra: 30 mm-es kúp alakú béléstest
Forrás: a szerző szerkesztése

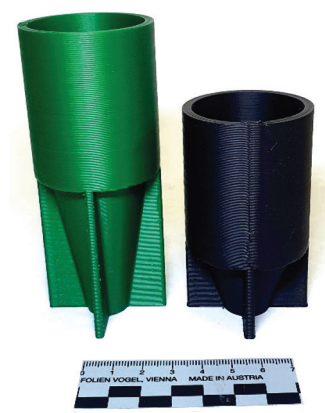
A béléstest forma esetében érdemes lehetőség lenne a dupla kúpos kialakítás, vagy a „trombita" forma tesztelése, de az erőforrások korlátozott száma miatt ezeket későbbre halasztottuk. További lehetőségként átgondoltuk a kúp csúcsa felé vékonyodó

[7] Angolul: *poly lactic acid.*
[8] A különböző gyártók technikai leírásai alapján a sűrűség változó lehet: 1,24–1,31 g/cm^3.
[9] Agu 2019.

béléstestek vizsgálatát is, de az előbb említett probléma okán egyelőre ezt is elhalasztottuk. Ez utóbbi lehetőség a kialakult kumulatív sugár hegye és magja közötti egyensúly megteremtésében játszhat fontos szerepet. A nagyobb balansz hatására az elvi hossz is megnő, amely az átütési képesség tekintetében szintén jelentős tényező. Más anyagok használatát is felvetettük, de ekkor a vizsgálati mátrix olyan szinten kiszélesedett volna, hogy már nemcsak az anyagi erőforrás nem tette volna lehetővé a végrehajtást, hanem további kutatók bevonása lett volna szükséges a folyamatba. Ez utóbbit a támogató projekt nem tette lehetővé, viszont reméljük a jövőben lesz lehetőség a területen további eredményeket elérni.

2. ábra: 40 mm-es félgömb alakú béléstest
Forrás: a szerző szerkesztése

A töltetház esetében a fenti béléstestek kialakítása volt a méretezés alapja. Az anyag itt is PLA volt. A nyomtatások során minden típusnál két eltartási távolsággal készültek ezek az alkatelemek, amelyek a béléstestek belső átmérőinek egyszeresei vagy kétszeresei voltak (3. ábra). A kialakítás tekintetében a fókusztávolságot a visszaáramlásgát, valamint a kialakított támasz biztosította.



3. ábra: Töltetházak egyforma átmérővel és különböző eltartással
Forrás: a szerző szerkesztése

A jelentős számú kombináció és az eredmények igazolása céljából minden változatot duplán vizsgáltam (1. táblázat).

1. táblázat: Vizsgált töltetek kombinációi

Fsz.	Béléstest átmérője (mm)	Fókusztávolság (D)	Béléstest forma	Béléstest anyag	Mennyiség (db)
1.	30	1	kúp	PLA	2
2.	30	2	kúp	PLA	2
3.	30	1	félgömb	PLA	2
4.	30	2	félgömb	PLA	2
5.	35	1	kúp	PLA	2
6.	35	2	kúp	PLA	2
7.	35	1	félgömb	PLA	2
8.	35	2	félgömb	PLA	2
9.	40	1	kúp	PLA	2
10.	40	2	kúp	PLA	2
11.	40	1	félgömb	PLA	2
12.	40	2	félgömb	PLA	2
Összesen					**24**

Forrás: a szerző szerkesztése

3. A vizsgálat körülményei

A vizsgálati feladatot Táborfalván, a Magyar Honvédség (MH) kijelölt robbantási területén hajtottuk végre, a MH 1. Honvéd Tűzszerész és Hadihajós Ezred (MH 1. HTHE) szakállományának segítségével, biztosításával.

A robbantási feladatot elektromos hálózat kialakításával hajtottuk végre, méretcsoportonként egy tűzben (3 robbantás, alkalmanként 8 töltet), soros hálózatba kötött rendszeresített villamos gyutacsok alkalmazásával. A robbantások során a tölteteket Semtex-H robbanóanyaggal töltöttük fel. A céltárgyakat és a rájuk helyezett tölteteket a talajban kialakított 300 x 300 mm alapterületű és 300 mm mély gödrökben helyeztük el. A gödröket egymástól a terep adottságainak figyelembevételével, de egymástól minimum 5 m távolságra alakítottuk ki.

A robbantási feladatot – mivel a hagyományos robbantási tevékenységtől nem tér el – a Mű/213 Robbantási utasítás vonatkozó rendszabályai alapján hajtottuk végre.

A kialakított töltetek paraméterei a 2. táblázat szerint alakultak. A kombinációk egyszerű, nyomon követhető kezelése és szerelése okán a típusokat egyedi elnevezéssel láttuk el, amely a béléstest belső átmérőjéből, a fókusztávolságból[10] és a béléstest formájából[11] tevődik össze.

[10] 1D = egy béléstest belső átmérőnyi eltartás; 2D = kettő béléstest belső átmérőnyi eltartás.
[11] K = kúp; FG = félgömb.

2. táblázat: Vizsgált töltetek paraméterei

Fsz.	Típus	Külső átmérő (mm)	Magasság (mm)	Töltetház tömege (g)	Béléstest tömege (g)	Robbanóanyag tömege (g)	Szerelt tömege (g)
1.	30-1D-K	46	80	40	8	70	118
2.	30-1D-K	46	80	40	8	70	118
3.	30-2D-K	46	110	53	8	71	132
4.	30-2D-K	46	110	56	8	71	135
5.	30-1D-FG	46	80	43	7	65	115
6.	30-1D-FG	46	80	43	7	65	115
7.	30-2D-FG	46	110	54	7	71	132
8.	30-2D-FG	46	110	56	7	70	133
9.	35-1D-K	51	90	51	9	100	160
10.	35-1D-K	51	90	51	9	100	160
11.	35-2D-K	51	125	67	9	101	177
12.	35-2D-K	51	125	67	9	102	178
13.	35-1D-FG	51	90	52	10	99	161
14.	35-1D-FG	51	90	52	10	98	160
15.	35-2D-FG	51	125	66	10	97	173
16.	35-2D-FG	51	125	66	10	96	172
17.	40-1D-K	60	100	66	13	160	239
18.	40-1D-K	60	100	66	13	161	240
19.	40-2D-K	60	140	90	13	162	265
20.	40-2D-K	60	140	92	13	162	267
21.	40-1D-FG	60	100	66	13	157	236
22.	40-1D-FG	60	100	66	13	156	235
23.	40-2D-FG	60	140	88	13	157	258
24.	40-2D-FG	60	140	92	13	158	263

Forrás: a szerző szerkesztése

A töltetek hatékonyságának vizsgálatához céltárgyakat alkalmaztunk (3. táblázat), amelyeket 4 mm vastag lemezekből alakítottunk ki. A lemezeket egyetlen táblából daraboltuk, hogy az eltérő anyagminőség ne befolyásolhassa az eredményeket. A kivágott lemezeket hegesztéssel rögzítettük egymáshoz és alapvetően kettő méretben, vastagságban készültek el. Ez utóbbira azért volt szükség, mert a legnagyobb változat esetén addigi tapasztalataink alapján biztosra vettük, hogy szükséges lehet a vastagabb változat.

3. táblázat: Vizsgált töltetek céltárgyai

Fsz.	Típus	Céltárgy
1.	30-1D-K	5 db 4 mm vastag és 50x50 mm-es egymásra hegesztett acéllemez Vastagsága: 20 mm
2.	30-2D-K	
3.	30-1D-FG	
4.	30-2D-FG	
5.	35-1D-K	
6.	35-2D-K	
7.	35-1D-FG	
8.	35-2D-FG	
9.	40-1D-K	6 db 4 mm vastag és 50x50 mm-es egymásra hegesztett acéllemez Vastagsága: 24 mm
10.	40-2D-K	
11.	40-1D-FG	
12.	40-2D-FG	

Forrás: a szerző szerkesztése

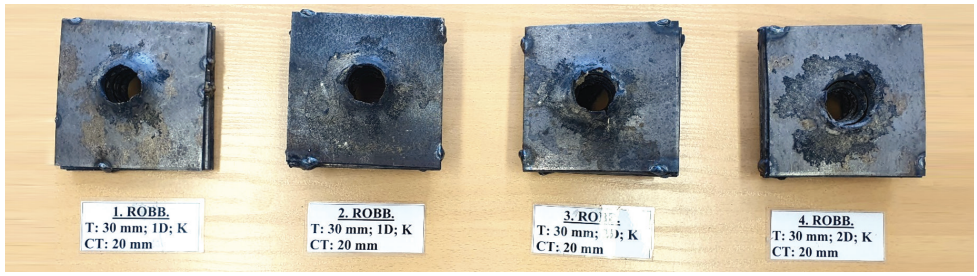
A céltárgyak ilyen kialakítása elviekben nem pótolja a homogén anyagon történő vizsgálatot, de a különböző töltetméretek teljesítményének egymáshoz viszonyítására alkalmas. A teljesítmény sok esetben még csökkenhet is a rétegződés miatt, hiszen a rétegek közé előfordulhat anyagbeáramlás átütéskor, ami csökkenti a kumulatív sugár hatékonyságát.

A töltetek elkészítésének folyamata:

- a töltetházak összeszerelése, az alkatelemek egymáshoz rögzítése pillanatragasztóval;
- a töltetek feltöltése plasztikus robbanóanyaggal;
- a feltöltött töltetekben a gyutacs helyének kialakítása formázó kupakkal;
- a töltetek tömegének ellenőrzése digitális mérleggel;
- a tölteteket rögzítése a céltárgyakhoz pillanatragasztóval;
- a rögzített töltetek behelyezése a robbantásra kialakított robbantó gödrökbe.

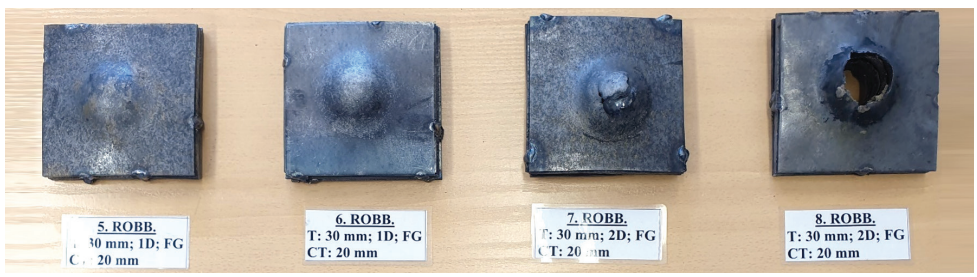
4. A vizsgálati eredmények

A 30 mm-es kúp alakú béléstestek alkalmazása esetében az eltartás 30 mm és 60 mm volt. A vizsgált töltetek mindkét eltartás esetében sikeresen átütötték a céltárgyakat. A kisebb eltartás esetében a felső lemezlapon nagyobb nyílás alakult ki, vélhetően a nagyobb visszaverődés miatt, és a kimeneti nyílás viszonylag egyenletes volt a jelentős kráterszerű megnyúlás ellenére. A nagyobb eltartás kisebb nyílást eredményezett a felső lemezen, és a kimeneti nyílás jobban szétnyílt, mint a kisebb eltartás esetében.



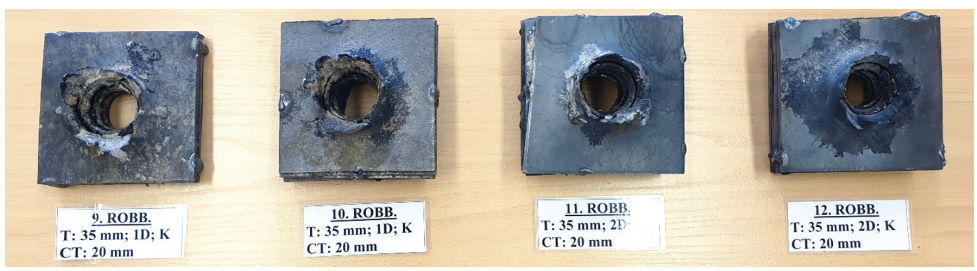
4. ábra: 30 mm-es kúp alakú béléstesttel szerelt töltetek céltárgyai robbantás után
Forrás: a szerző szerkesztése

A 30 mm-es félgömb alakú béléstesttel szerelt töltetek a kisebb, 30 mm-es fókusztávolság esetén nem értek el átütést. A kialakult üregben a lemezekből kiszakított korongok halmozódtak fel, préselődtek össze. A dupla eltartás esetén (60 mm) ez utóbbi jelenség szintén azonosítható volt, és egy esetben részleges átütést eredményezett, míg a másikban meggyőző, teljes átütés volt tapasztalható. Mindezek azt igazolják, hogy a 30 mm-es béléstestek vonatkozásában, a bemutatott paraméterek mentén a kúp változat bizonyult hatékonyabbnak.



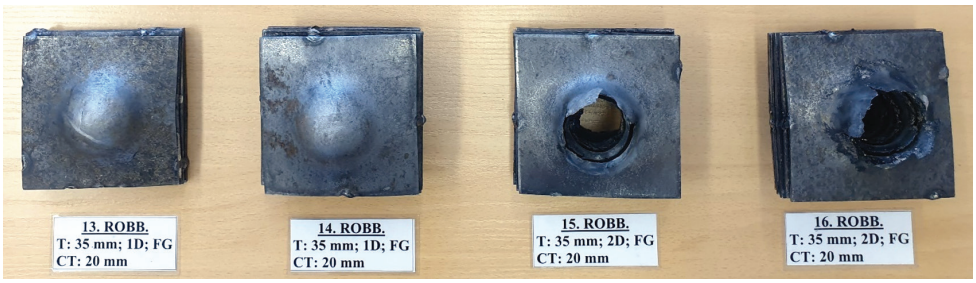
5. ábra: 30 mm-es félgömb alakú béléstesttel szerelt töltetek céltárgyai robbantás után
Forrás: a szerző szerkesztése

A 35 mm-es kúp alakú béléstestek mindkét eltartás (35 mm és 70 mm) esetében sikeresen átütötték a céltárgyakat. Mind a négy töltet homogén eredményt mutatott az átütésnél. A kilépő nyílások éles és jelentősen elnyúlt kráterszerű formát mutattak. A töltetek hatékonyságához kétség sem férhet.



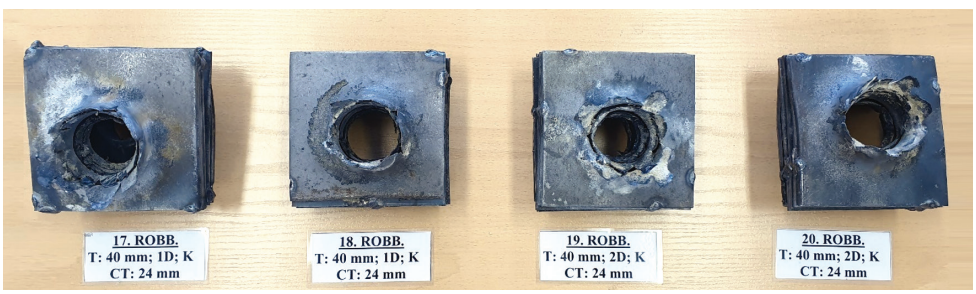
6. ábra: 35 mm-es kúp alakú béléstesttel szerelt töltetek céltárgyai robbantás után
Forrás: a szerző szerkesztése

A 35 mm-es félgömb alakú béléstesttel szerelt töltetek a kisebb, 35 mm-es fókusztávolság esetén nem értek el átütést. A kialakult üregben a lemezekből kiszakított korongok halmozódtak fel, préselődtek össze. A céltárgy alján jelentős deformitás tapasztalható, mint az előző, 30 mm-es változatnál. A nagyobb eltartás esetén (70 mm) teljes átütés tapasztalható, mind a két töltet homogén eredményt mutatott. Ez az utóbbi eredmény azt a látszatot kelti, hogy a félgömbből formált kumulatív sugár nagyobb hatékonyságot mutat nagyobb eltartással.



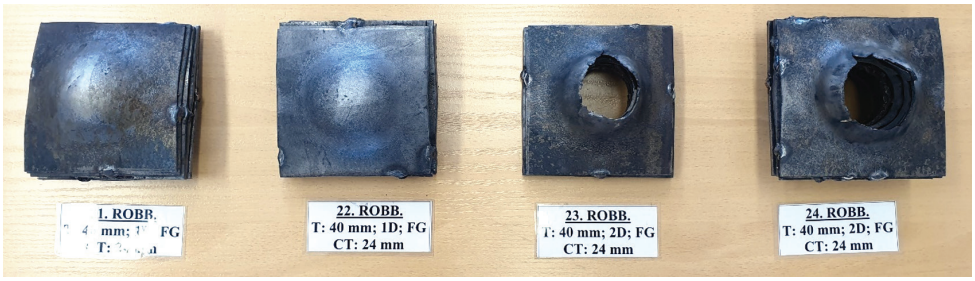
7. ábra: 35 mm-es félgömb alakú béléstesttel szerelt töltetek céltárgyai robbantás után
Forrás: a szerző szerkesztése

A 40 mm-es kúp alakú béléstestek mindkét eltartás (40 mm és 80 mm) esetében sikeresen átütötték az immár 24 mm vastag céltárgyakat. Mind a négy töltet homogén eredményt mutatott. A kilépő nyílás éles, magas peremű, alapvetően szétnyíló formát mutatott.



8. ábra: 40 mm-es kúp alakú béléstesttel szerelt töltetek céltárgyai robbantás után
Forrás: a szerző szerkesztése

A 40 mm-es félgömb alakú béléstesttel szerelt töltetek a kisebb, 40 mm-es fókusztávolság esetén ebben a méretben sem értek el átütést. A kialakult üregben a lemezekből kiszakított korongok itt is felhalmozódtak. A nagyobb eltartás esetén (80 mm) teljes átütés tapasztalható, mind a két töltet homogén eredményt mutatott, bár a kúp változathoz képest a kilépőnyílás pereme kevésbé jelzi a töltetben rejlő átütési tartalékot (nem széttartó).



9. ábra: 40 mm-es félgömb alakú béléstesttel szerelt töltetek céltárgyai robbantás után
Forrás: a szerző szerkesztése

A töltetek szempontjából kijelenthető, hogy a kúp béléstest hatékonysága a vizsgált fókusztávolságokon több mint kielégítő. Mind a 12 ilyen béléstesttel szerelt töltet eredményesen átütötte a céltárgyakat. A legkisebb változat esetén már látszott, hogy az eltartás jelentősége nő, ha a robbanóanyag-töltet tömege csökken.

A félgömb alakú béléstestek esetében az egy béléstest átmérőnyi eltartás nem elégséges az eredményes átütéshez, de ennek duplája esetén már jelentősen hatékonyabb a töltet és képes a megfelelő munkavégzésre. A legkisebb méret esetén az utóbbi tapasztalat nem volt minden kétséget kizáróan igazolható.

A céltárgyak tekintetében azok kialakítása az alapvető vizsgálati célnak megfelelt, bár a homogén lemezeken végzett kontrollvizsgálatok esetén előfordulhat majd eltérés.

További vizsgálatokat tartunk szükségesnek kisebb töltetekkel (25 mm, illetve 20 mm), valamint néhány tesztet visszaáramlásgát nélküli töltetekkel. Ez utóbbi igazolhatja vagy cáfolhatja az alkatelem szükségességét.

5. Összegzés

A vizsgált töltetek száma és típusa megfelelt az elvárásoknak. Sikerült végrehajtani a további kutatási irányok, méretezési megoldások közötti szűkítést, bár egyben új feladatok is adódtak, mivel a legkisebb változat is képes volt megbízhatóan átütni a céltárgyat. Ez a gyakorlatban létjogosultságot biztosít kisebb átmérővel szerelt változatok méretezésére és tervezésére. Ez utóbbi tekintetben legalább két további kisebb méretet tartunk szükségesnek.

A béléstestek közül sikerült egyértelmű választ kapni a további vizsgálandó irányra. A kúp forma hatékonysága kiemelkedő volt a félgömbhöz képest, bár ez nem azt jelenti, hogy a jövőben nem lehetne hatékonyabb töltetváltozatot kialakítani félgömb béléstesttel. Pusztán az jelenthető ki, hogy a félgömb béléstest teljesítménye a fenti paraméterek mentén elmarad a kúphoz képest.

A remek átütési eredmények azt jelzik előre, hogy van jövője ennek a kumulatívtöltet-típusnak a robbantástechnikában, civil és katonai vonalon egyaránt. Civil vonalon érdemes lehet majd jövőbeli vizsgálatra például jégrobbantás esetén a műtárgyak jégmentesítése egyes részfeladatainak támogatása. Hasonló eredményes felhasználási terület lehet a tűzszerész szakfeladatok során a különböző robbanótestek

hatástalanítása, úgymint hagyományos robbanótestek, improvizált[12] robbanótestek és az ABV-tűzszerészet[13] egyes feladatai.

Felhasznált irodalom

Agu, Henry Obediah (2019): *The Effect of 3D Printed Material Properties on Shaped Charge Liner Performance.* PhD-értekezés. United Kingdom, Cranfeld University. Online: https://dspace.lib.cranfield.ac.uk/handle/1826/15285

Berek Tamás (2016): ABV (CBRN) tűzszerészcsoport mint a biztonsági kihívásokra adott válaszlépés. *Bolyai Szemle,* 25. évf. 4. sz. 22–34. Online: https://bit.ly/3krgDaR

Boda József – Boldizsár Gábor – Kovács László – Orosz Zoltán – Padányi József – Resperger István – Szenes Zoltán (2016): A hadtudományi kutatási irányok, prioritások és témakörök. *Államtudományi Műhelytanulmányok*, 16. sz. 1–23. Online: www.med.u-szeged.hu/download.php?docID=90702

Doig, Alistair (1998): Some Metallurgical Aspects of Shaped Charge Liners. *Journal of Battlefield Technology,* 1. évf. 1. sz. 1–3.

Kovács Zoltán (2012): Fontos létesítmények IED elleni védelme. *Műszaki Katonai Közlöny,* 22. évf. ksz. 35–44. Online: https://mkk.uni-nke.hu/document/mkk-uni-nke-hu/2012_k_05%20IED%20elleni%20v%C3%A9delem%20-%20Kov%C3%A1cs_Z.pdf

Kugyela Lóránd (2020): A többkomponensű robbanóanyagok múltja, jelene és jövője. *Katonai Logisztika,* 28. évf. 4. sz. 58–75. Online: https://doi.org/10.30583/2020.4.058

Lukács László (1992): *A kumulatív hatás és a kumulatív töltetek méretezése*. *Jegyzet a Szárazföldi Haderőnemi Fakultás műszaki hallgatói számára.* Magyar Honvédség, Zrínyi Miklós Katonai Akadémia Műszaki Tanszék.

Lukács László (2010): A kumulatív töltetek és gyakorlati alkalmazásuk. *Műszaki Katonai Közlöny,* 20. évf. 1–4. 175–185.

[12] Kovács 2012.
[13] Berek 2016.

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG

17. évfolyam (2022) 4. szám 75–99.
DOI: 10.32567/hm.2022.4.6

László Bodnár,[1] Péter Debreceni[2]

Implementation of Wildfire Risk Evaluation Elements into the Hungarian Forest Fire Prevention System

Nowadays, wildfires are an increasing challenge for the defence sector. The fire risk of a given area depends only in part on human factors and the number of registered fires. A fire occurs when the moisture content of dead biomass drops to a level, where the fire can already spread between the individual pieces of fuel. Daily fire danger forecast examines the constant and changing components of the fire environment. This determines the flammability of the biomass; the rate of fire spread makes firefighting more difficult. The fire danger forecast identifies the fire hazard periods when fires can occur. Fire Risk Assessment Systems have been developed in many countries around the world. In addition to the daily fire risk, these include parameters describing the vulnerability of the areas affected by the fire. National risk assessments are available in many countries around the world using several methodologies. The Joint Research Centre of the European Commission has developed a community-wide approach to forest fire risk assessment, using scientific results and studying good practices. In this approach, the risk of a forest fire is made up of the effects of daily fire hazards and vulnerabilities. The risk of fire due to weather conditions is associated with ignition and the spread of fire. The authors examine in the paper the basic criteria to assess wildfire risk at the pan-European level. The authors analyse external and internal risk factors in an observation plot and examine how international recommendations can be utilised in Hungary.

Keywords: *wildfire risk evaluation, fire risk assessment, observation plot*

[1] Assistant Lecturer, University of Public Service, Faculty of Law Enforcement, Institute of Disaster Management, e-mail: bodnar.laszlo@uni-nke.hu

[2] Forest Engineer, National Food Chain Safety Office, System Management and Development Directorate, Department of Data Analysis, e-mail: debrecenip@nebih.gov.hu

1. Introduction

Wildfires have always been a part of our lives. The cavemen had already used fire, and during this time, humanity also recognised the harmful effects of fire. So wildfires have always been present in our lives, but climate change will pose an even greater challenge in some parts of the world, including Europe, in the future. Climate change is aggravating the situation, making countries more prone to wildfires and increasing the intensity of such events.[3] Year after year the fire seasons start earlier and end later, so it gives a greater opportunity to ignite the biomass.[4] Legislators have enacted legislation in order to prevent fires and fight against forest fires. In Hungary, the main legislation in connection with fires is Act CXXVIII of 2011 concerning disaster management and amending certain related acts (hereinafter referred to as Act on Disaster Management) and Act XXXI of 1996 on Fire Protection, Technical Rescue and Fire Services (hereinafter referred to as Fire Protection Act). The Act on Disaster Management is a comprehensive and complex legislation that includes the management of disaster management as well as the general order in the fields of industrial safety, civil protection and fire protection. It gives more importance to prevention activities compared to previous legislation. The Fire Protection Act specifically regulates the operation of fire departments. This legislation sets out in detail the procedures for the management and execution of firefighting, technical rescue and authority tasks in connection with fire protection. The importance of protection against wildfires is reflected in this law, but the relevant firefighting tasks are already set out in an implementing decree. At the international level, countries have different fire and forest fire regulations, so some organisations have already made recommendations to solve this problem.

National risk assessments are available in many countries around the world using several methodologies. The Joint Research Centre of the European Commission has developed a community-wide approach to forest fire risk assessment, using scientific results and studying good practices. In this approach, the risk of a forest fire is made up of the effects of daily fire hazards and vulnerabilities. The risk of fire due to weather conditions is associated with ignition and the spread of fire. Vulnerability can be characterised by ecological and socio-economic parameters. Socio-economic parameters are the environmental services and the human infrastructure. According to the European model, the factors influencing the occurrence and spread of wildfires can be interpreted as components of an internal and external system. Internal factors include biomass structure, forest health status and topographic parameters. External factors, such as climate change, land use, weather and human activity are not related to the parameters that describe the forest. The paper aims to examine how the elements of the European model can be adapted to the Hungarian fire risk assessment, and how the elements involved in the forest fire risk assessment can be reflected in the national and county-level Fire Protection Plans in Hungary. During

[3] European Commission 2021; Restás 2020
[4] Teknős 2019

our research, we study the elements of the model with the help of relevant literature and examine the possible operation of the model in a selected observation plot with high forest fire risk based on the fires that occurred between 2011 and 2020. As a result of the research, we make findings about the extension of the model and the limitations of the application.

2. Forest fire risk trends in Hungary and the European Union

One of the key elements of forest fire prevention activities is the registration of wildfire events that occur under natural conditions in Hungary, knowledge of the characteristics of wildfires and the course of the fire season. To achieve these goals, the forestry authority and disaster management have been working together for the past two decades to develop methodologies for data collection and analysis. They have also developed the professional and legal regulations and the development and operation of IT systems needed for daily operations. The Forest Fire Information System contains data on forest fires in Hungary. During data gathering, fires that typically damage property on the outlying property, grass vegetation and wooded areas, or affect crops, are registered as vegetation fires. This category also includes undergrowth burning in forests or wooded areas, as well as reed and peat fires or grass burning in pastures. A forest fire is defined as a fire in an open area that did not necessarily start in a forest and did not exclusively, but completely or partially, affect a forest or a wooded area. A fire is therefore considered to be a forest fire that affected a forest or other area covered with trees.[5]

In the last two decades, the risk of forest fire has increased significantly in the central and southern regions of Europe, but the number and extent of forest fires must also be expected to increase in the northern countries. Currently, 85% of burned areas in Europe are located in Southern Europe (Portugal, Spain, France, Italy and Greece) due to the higher risk of weather conditions typical of the Mediterranean region. In these five Mediterranean countries, an average of almost half a million hectares of land has burned annually over the past 20 years. In addition to the increase in the annual number of high and extreme fire-risk days, the impact of extreme fires will likely increase in large areas, with long-term effects. The forest fire season starts earlier and ends later, which puts an additional burden on disaster management agencies.

Based on the temporal distribution of forest fires in Hungary, there are two high-risk periods each year. Spring forest fires (February–May) accounted for 56.3% of all forest fire cases. In the last decade, only in the spring of 2013, so much precipitation fell that the spring fire season was practically missed. In the other years, March and the first half of April proved to be extremely high risk. Between 2011 and 2021, six springs had more than 50% of fires in these two months compared to the annual number of cases. At the beginning of the decade, the number of forest fires began to

[5] Camia et al. 2014

rise at the end of February, and, depending on the spring rainfall, we registered high numbers of fire cases until the middle or end of April. This trend seems to change by the end of the decade. In 2019 and 2020, the number of forest fires started to increase from the second week of February and we registered high numbers of fire cases until the end of April. In May and the first half of June, depending on the distribution of precipitation, the risk of fire decreases and we do not experience any outliers in the number of fire incidents.

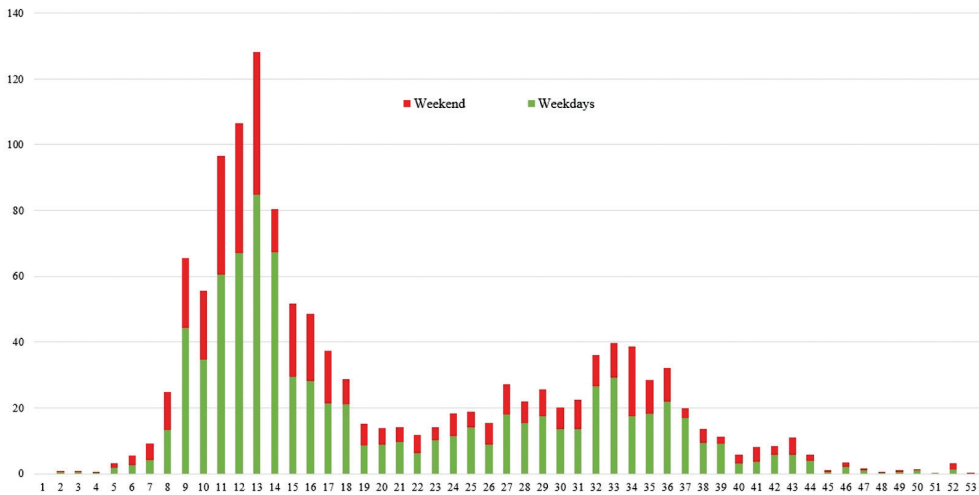


Figure 1: Average number of forest fires per week (2011–2021)
Source: Forest Fire Information System of Hungary.

Based on the number of fire events, the other fire-risk period of the year is in the month of July–September. In the second half of the decade, during periods without precipitation, forest fires also occurred in October. During the summer, when there is an increased risk of fire during heat waves, the number of fires does not reach the number of fires that occur in the spring, but the proportion of the area burned in one fire can be much higher. In recent years, during the increased risk of fire caused by the summer drought, many large-scale crown fires have occurred in the pine forests of the Great Plain and the wooded and shrubby areas of the northern part of the country. In the last decade, 35% of all forest fires started on weekends or holidays.

Between 2013–2021 a total of 9,789 forest fires occurred. Looking at the last 9 years, an increasing trend of fire incidents can be shown in Hungary, as shown in Figure 2.

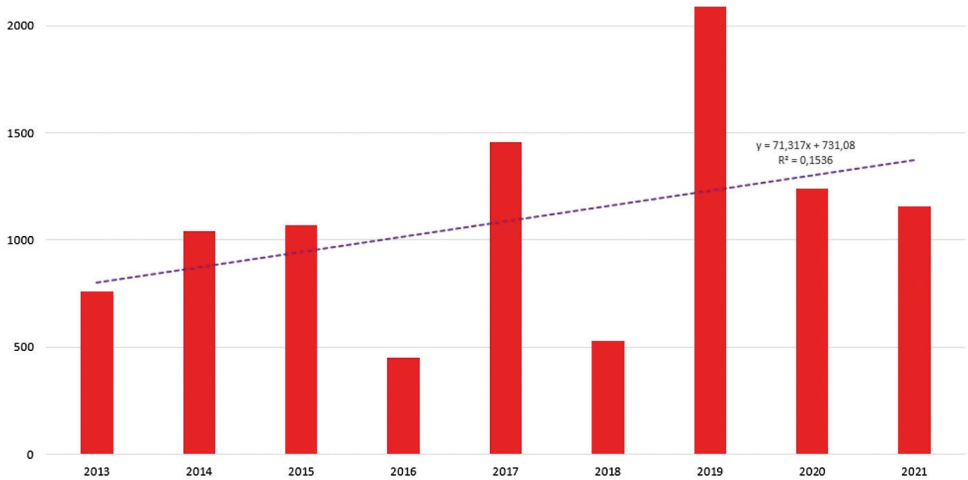


Figure 2: The number of forest fires in Hungary (2013–2021)
Source: Forest Fire Information System of Hungary.

From the data on forest fires that occurred between 2011 and 2021, a trend can be identified in the number of fires under 0.5 hectares, which shows a continuous increase in the last decade. These small fires require the intervention of the fire department at all times of the year, even in cases where the burning could be carried out safely by following the rules for lighting fires. In addition, a fire can become uncontrollable in the case of topography, biomass and meteorological conditions favourable to the spread of fire.

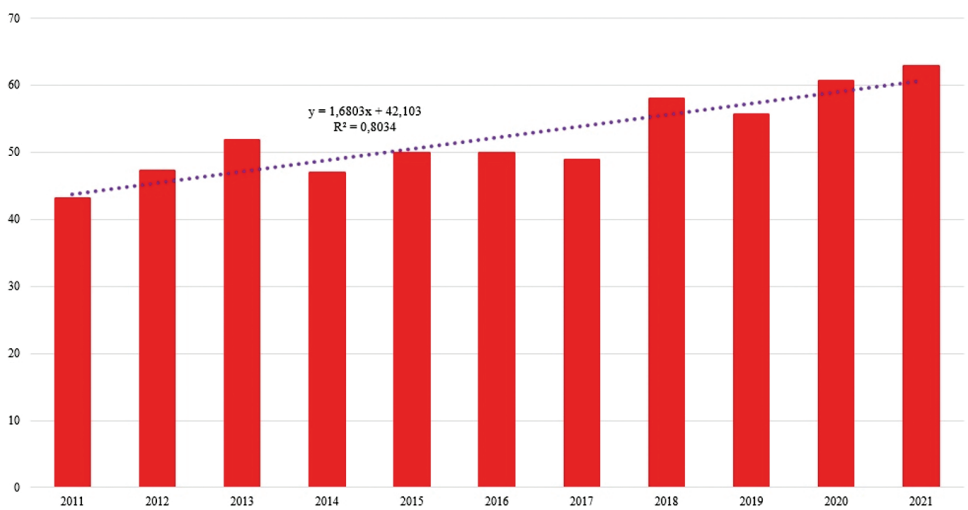


Figure 3: Proportion of forest fires under 0.5 hectares (2011–2021)
Source: Forest Fire Information System of Hungary.

The analysis of the fire incident data points out that a large number of smaller forest and vegetation fires separate in space and time occur every year. As a result of changing weather conditions, fires can have a significant impact on protected natural values, the maintenance of agricultural areas that provide livelihoods, and, in some cases, the condition of infrastructure. In periods of increased fire risk, several fires occurred at the same time in many cases, which can pose a great challenge to the personnel of the disaster management organisation and the forest managers and land users, and the use of their tools and resources. In the coming decade, more attention must be paid to the preparation, compliance with fire regulations and increasing the resilience of forest stands. Forest fire risk assessment is essential for the development of forest fire protection plans, for a better understanding of the factors that play a role in the origin of the fire, and for establishing the basis for official decisions that implement protection measures.

3. Forest fire risk evaluation in Hungary

Due to the mosaic landscape structure in Hungary, wildfires affect not only forest areas but also another wooded and agricultural land. The prevention of forest and vegetation fires, therefore, requires the continuous, well-thought-out, integrated cooperation of several specialist areas, economic organisations and authorities. Forecasting fire risk periods, early detection of fire, forest fire risk assessment, support of firefighting activities with IT systems, preparing and continuously updating of protection plans, public information, a support system for rural development, and education programs are the framework of modern forest and vegetation fire prevention activity. Forest fire prevention measures can be effective if they are planned by organisations with appropriate authority, infrastructure, and a team of professionals coordinate the activities and implement them according to plan. A scientific background is therefore essential for continuous development, the effective transfer of knowledge, and the development of new tools and methods. Domestic forest fire prevention tasks are included in the Forest Act and its executive decree, as well as in the ministerial decree on forest fire protection.

The fire hazard classification of forest areas is prepared by the forestry authority and updated every year. The classification is based on tree species data recorded in the forestry register. The classification is carried out at the forest section level. After the classification, each forest section will have its fire hazard indicator, on a three-level scale. The indicator expresses the quantity and combustibility of the combustible biomass in the forest section. The classification is based on the data registered by the forestry authority, and with its help, professional expectations can also be properly enforced.

Based on the classification at the forest section level, the forest manager must prepare a forest fire protection plan and is obliged to keep specific tools and work groups ready in case of a forest fire. Farmers with between 10 and 100 ha of fire-prone forest must prepare a simplified protection plan. Farmers in fire-prone areas larger than 100 hectares must prepare a complex forest fire protection plan. The

forest fire protection plan includes the risky forest areas in the farmer's territory and the prevention activities. The plan also includes a map system, which the forestry authority provides free of charge to forest managers. The classification is also available on the public forest map operated by the forestry authority on the World Wide Web. Hungary provides the use of forest maps as part of a web map service for the GIS system of disaster management.

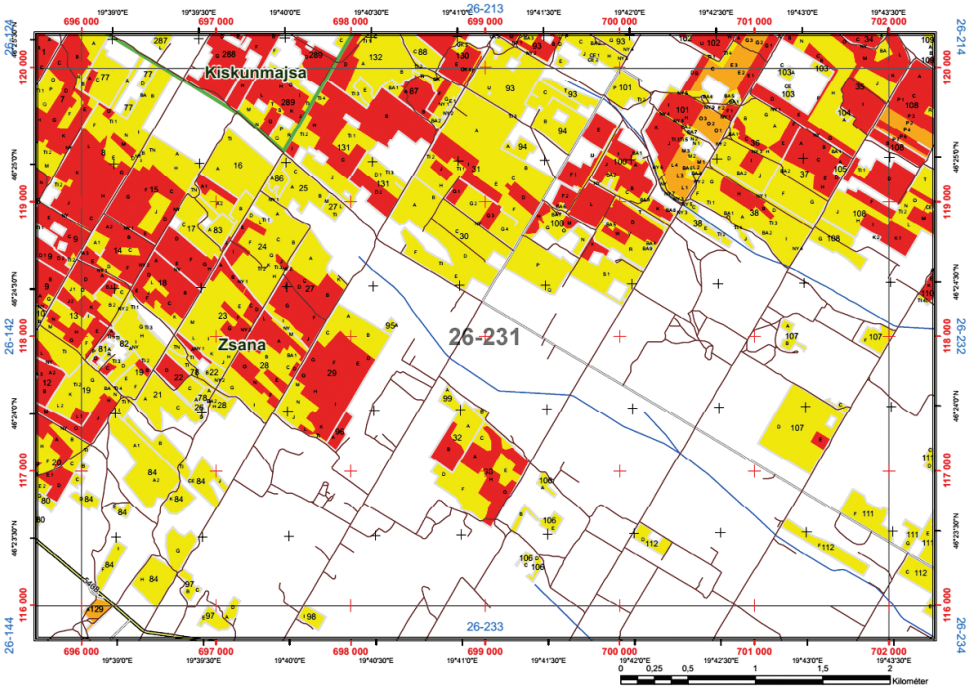


Figure 4: Fire hazard classification of forest land area
Source: Forest Fire Information System of Hungary.

In high-risk periods, the forest authority can order a fire ban in consultation with the fire service. The risk periods and the delimitation of the areas affected by fire risk must be displayed on the website of the forestry authority. The map is continuously available during the fire season on the websites of the relevant authorities[6] and cooperating organisations. The decision depends on three main parameters: meteorological conditions, the daily value of the Fire Weather Index (FWI) published by the JRC, and the frequency of fires. The assessment and analysis of forest fire risk are carried out every year from 1 February to 31 October. The forestry authority and the fire service will announce the increased risk of fire.

[6] Fire bans (http://erdotuz.hu/kezdolap/); BM Directorate General for Disaster Management (www.katasztrofavedelem.hu/).

The domestic forest fire risk assessment is based on the hazard classification of forest areas and the use of the FWI published by the JRC. In the next section, we will examine the approach the European Commission recommends for the Member States at the community level.

4. Forest fire risk evaluation in the European approach

In the Member States of the European Union, many approaches and methodologies are used to assess forest fire risk. Each method has been defined on a scale that varies from country to country (national, regional, local). In many cases, systems were created for different purposes. This has also caused some concepts related to fire risk to be used in different ways in some Member States. For this reason, it is difficult or impossible to compare the fire risk management measures of the member countries.[7] Different approaches not only take into account the frequency and effects of fires but also consider the level and to what extent each risk factor should be taken into account in decision-making processes (landscape management).

The Joint Research Centre of the European Union (JRC) wanted to create an approach that is simplified at the community level but can remain flexible to satisfy multiple needs and integrate new factors into the model later on. Of course, bearing in mind the limitation of the approach, the national and local fire risk assessment can be more accurate than the community-level model. The community approach defines wildfire risk as the product of the probability of a wildfire occurring and the damage it causes. Consequently, it examines three areas: fire ignition factors, fire behaviour, and the effect of fire on human life and equipment. In the following, we present the data sets that can be considered the basic criteria of the European forest fire risk assessment, which are illustrated in more detail in Figure 5.

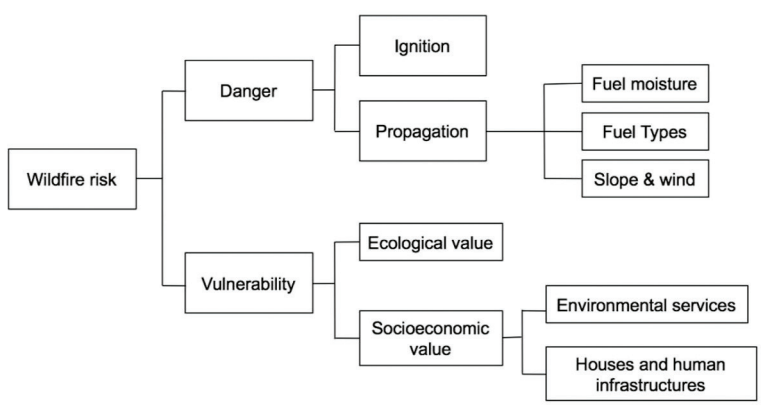


Figure 5: Basic components of wildfire risk assessment
Source: European Commission 2021: 10

[7] Hardy 2005

According to Figure 5, we can see that the two main components of wildfire risk are wildfire danger and vulnerability. Wildfire danger includes elements such as ignition, which is a natural chemical process, and propagation, which depends on fuel moisture, fuel types and other factors (slope, wind). So the fire propagation depends on several components, which is described in Richard Rothermel's surface fire spread model.[8]

$$R = Ir\zeta(1+\Phi w+\Phi s)/\rho b\ \varepsilon Qig$$

R = rate of spread
Ir = reaction intensity
ξ = propagating flux ratio
Q_w = wind factor
Q_s = slope factor
P_b = bulk density
ε = effective heating number
Q_{ig} = heat of pre-ignition

The essence of this is that if one factor of fire propagation is smaller but another factor is higher, we can get a similar fire propagation value.

The other element of wildfire danger is vulnerability. This includes ecological values and socio-economic values, such as environmental services and houses and human infrastructures.

In many cases, wildfire danger means the conditions under which a fire occurs or spreads. There are indicators such as the FWI that give a direct assessment of fire hazards due to weather conditions.[9] Wildfire danger includes factors such as wildfire ignition and wildfire propagation.

In connection with wildfire ignition, it can be determined that an increase in fire ignitions results in the occurrence of many fires at the same time. It allows a heavy fire spread and contributes to the development of large forest fires, which cause significant environmental damage. Biomass and weather conditions also affect the development and behaviour of fire.[10] It is also important to mention that the primary cause of fires in Europe is human negligence or intent.[11] It is 95% in the Mediterranean region and roughly 99% in Central Europe. The natural occurrence of fires is very small on the continent.

Wildfire propagation is another factor influencing wildfire danger. This includes the fuel moisture content, the types of fuel, and the slope and wind factors. Fuel moisture content is a basic element for wildfire spread because dry fuels burn easily and result in more intense wildfire propagation. Fuel moisture can be modelled via fuel moisture indexes derived from weather data. It was developed in Canada but

[8] Rothermel 1972
[9] Lee 2003
[10] Finney 2005
[11] Ganteaume et al. 2013

can also be used in European conditions.[12] The possibility of using indexes has already been analysed in Hungary.[13]

The fuel type is also a factor influencing the fire spread. In the case of fuel type, it is important how quickly the vegetation dries out, and the horizontal and vertical structure of the fuel. As a result of a European dataset, fuel types can be classified into 9 classes.

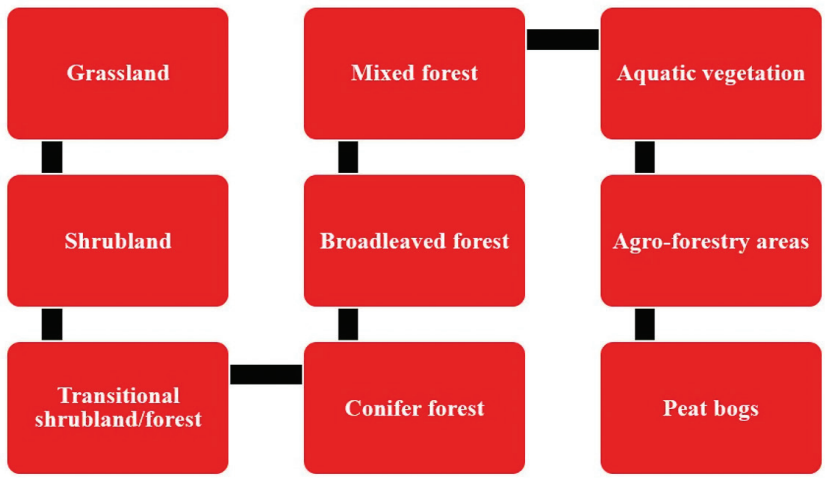


Figure 6: Fuel types in Europe organised into 9 groups
Source: Compiled by the authors based on European Commission 2021.

These 9 groups characterise the flammable fuel of the European continent. Fuel types have different combustion properties, which also affect the fire spread.[14] In this research, we do not examine it, due to space limitations.

In case of wildfire risk assessment analysis, the slope and wind factors are also essential. These affect the generation of wildfires, the fire spread, and the size of the burned areas, and these can be considered the abiotic factors of forest fires (non-living factors in the ecosystem). So the spread of wildfires also depends significantly on topographic conditions. The precipitation (rain) flows from the upper part of the hill towards the lower parts, so the moisture content of the flammable fuel and soil layer is potentially always higher in the valley. The lower part of the hill is also more windproof, and the effect of solar radiation is not as effective as on the hilltop, therefore, the precipitation cannot dry out quickly. The water conditions on the southern slopes are unfavourable, so the moisture content of the fuel is lower in this part. This provides better conditions for fire generation. Another significant factor is where the fire occurs on the terrain. Fires at the bottom of the slope develop faster than at the top of the slope. In these conditions flames bend, just as they do on plains in

[12] Van Wagner 1987
[13] Debreceni 2021
[14] MPI Feuerökologie und Biomassverbrennung AG 1994

case of wind. In this case, the pre-drying effect of convection and radiation increases towards the fuel in front of the frontline of fire. In contrast, fires occurred at the top of a slope move downhill slowly and slip slowly through the mountain ridge due to flame deflection.[15]

Wildfire vulnerability means ecological and socio-economic values. However, ecological values are difficult to measure, because they are often elusive, but their protection is essential for everybody. The Natura 2000 site network emphasises the special ecological values of a territory. National Designated Protected Areas must also be considered when assessing wildfire risk. The European Environment Agency (EEA) groups the designation types into three main categories such as:

a) designation types used to protect fauna, flora, habitats and landscapes
b) statutes under sectoral, particularly forestry, legislative and administrative acts providing adequate protection relevant for fauna, flora and habitat conservation
c) private statute providing durable protection for fauna, flora, or habitats[16]

Forest fires can have not only ecological but also socio-economic values that affect people's livelihoods, safety and health.[17] Socio-economic value is a practical approach to estimating the cost of damage caused by wildfires. There are a lot of costs involved during firefighting, but these include mainly the costs of fuel, mechanical depreciation, manpower and burnt areas. Most of the damage caused by forest fires is the burned areas.[18] Areas, in particular where houses meet or intermingle with the undeveloped wildland vegetation can also be considered a socio-economic value. It is referred to as the Wildland-Urban Interface (WUI) in international literature.[19] Research on WUI and the identification of areas have already begun in Hungary.[20] Socio-economic factors also include critical infrastructure elements. The JRC has collected European data on critical infrastructures from a range of sources and harmonised and stored them in a geographical database.[21]

The above-mentioned points set out the basic criteria for the European assessment of wildfire risk. The next step in the process is to implement the basic criteria and to test and validate the wildfire risk map at the European level.

In addition to the risk assessment dimension, it is also worthwhile to qualitatively examine the factors (hereinafter referred to as drivers) that play a role in the occurrence of forest fires and the increase in the number of fire incidents. In this approach, external and internal drivers play a role in the development of fire risk.

At the European level, cooperation in forest fire prevention is implemented by the Expert Group on Forest Fires of the Joint Research Centre. Its main role is to provide advice for the implementation and further development of the European Forest Fire

[15] Nagy 2013
[16] Nationally designated protected areas (www.eea.europa.eu/data-and-maps/indicators/nationally-designated-protected-areas).
[17] Vhiriri et al. 2021
[18] Bodnár 2017
[19] Radeloff et al. 2005
[20] Bodnár 2020; Bányai–Pántya 2020
[21] European Commission 2021: 10.

Information System and recommendations for improved forest fire prevention in the European and Mediterranean regions.[22]

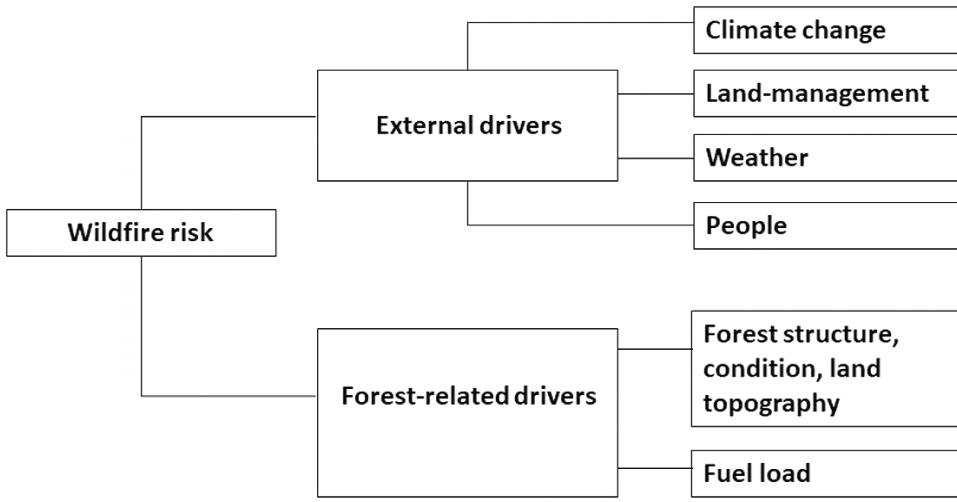


Figure 7: Forest fire drivers in risk evaluation
Source: Compiled by the authors based on European Commission 2021.

External factors such as climate change, land management, land use, weather and people affect wildfire risk. Rising temperatures and increased droughts are responsible for the higher risk of wildfires, as they make biomass more susceptible to ignition. Higher temperatures and more frequent droughts lead to more days with high fire danger, which partly explains the impact of climate change on wildfire risk. Rising temperatures and droughts also affect vegetation types, because changing environmental conditions stress existing vegetation types, thereby increasing their desiccation and susceptibility to forest fires.

At the same time, the changed climatic conditions extend the growing season, which in turn can lead to a change in species composition and an increase in combustible biomass, and thus to the risk of fire. Additionally, changing environmental conditions can affect species distribution, potentially making ecosystems more vulnerable to fire. Weather changes are of course closely related to climate. Decreasing rainfall and more frequent droughts are affecting areas of Europe that historically have rarely experienced forest fires.

Human actions often contribute to wildfires. Although fires can also be caused by natural causes (lightning, spontaneous combustion), European Forest Fire Information System[23] (EFFIS) data shows that the majority of fires in Europe are caused by humans, either accidentally, carelessly, or intentionally.

[22] For more information see https://effis.jrc.ec.europa.eu/
[23] For more information see https://effis.jrc.ec.europa.eu/

Land management and planning are the main links between forest-related factors and external activities. Fire management is also a form of land use. While the decline of rural areas can contribute to wildfires in some areas, in other cases urban sprawl has resulted that people are moving to fire-risk areas. On abandoned or only intermittently managed farmland, biomass also contributes to the increase of fire risk and the spread of fire in the absence of a human operator. Factors related to the forest and its biomass, such as its species composition, horizontal and vertical composition, as well as topography, all affect forest fire risk. Management decisions also affect the composition and quantity of combustible biomass. The risk of fire increases with the lack of cultivation work and improperly selected tree species in forest plantations. At the same time, forest fire risk is reduced by forest thinning and the creation and maintenance of the fire protection system, as well as the choice of resistant species suitable for the growing area for planting. Forest fire risk can be further reduced by forest fire prevention measures carried out during farming.

After reviewing the individual factors, in the next section, we will examine how the individual components can be transferred to the domestic system.

5. Investigating the possibility of implementation in the Hungarian forest fire risk assessment system

Risk modelling systems should be the result of an integrated framework of interconnected components associated with the firing process [24] [25] to provide an integrated view of fire likelihood and the consequences caused by them. Wildfire risk can be identified as the joint effect of:

- wildfire danger (also known as a fire hazard)
- wildfire vulnerability of people, ecosystems and goods exposed to wildfires

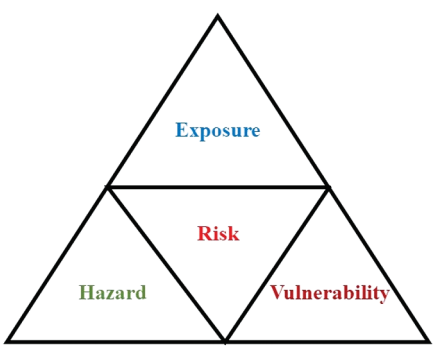


Figure 8: Forest fire risk scheme in European approach
Source: Compiled by the authors based on San-Miguel-Ayanz 2019.

[24] Chuvieco 2012
[25] Xi et al. 2019

This scheme is designed to be scale-independent and easily applicable to local, regional and global scales. The three main components are defined below.

Hazard: A dangerous phenomenon, substance, human activity, or condition that may cause loss of life, injury or other health impacts, property damage, loss of livelihoods and services, social and economic disruption, or environmental damage.

Exposure: People, property, systems, or other elements present in hazard zones that are thereby subject to potential losses.

Vulnerability: The characteristics and circumstances of a community, system, or asset that make it vulnerable to the adverse effects of a hazard.

The scheme was based on the quantitative analysis of "risk", based on the probability or possibility (P) of negative outcomes (damage, D):

Risk = Probability × Damage

The probability for a fire to start at a given location and time (P: fire danger/fire hazard) depends on the likelihood of ignition sources and local conditions to start and spread a fire (fire behaviour); namely, it depends on the fuel availability, type and pre-conditions of the fuel, the prevalent meteorological conditions, and on the presence of an event triggering the initial ignition. In Europe, the vast majority of wildfires are linked to human causes either deliberate or due to accident or negligence.[26] Therefore, P is not only a function of fuel and weather but prominently also of human behaviour P (fuel, weather, human).

Wildfire risk is assessed by considering the vulnerable areas where people, ecological and socio-economic values are exposed to fire danger. An aggregated wildfire risk index is proposed, which prioritises the risk for human lives, while also considering ecological and socio-economic aspects. This is done by ranking as high-risk areas those where people may be exposed to wildfires, and secondarily other areas where ecological and socio-economic aspects are at stake.

Figure 5 shows the main components of the pan-European forest fire risk assessment system. Appropriate basic data is required for the calculation and risk ranking of the individual components. In the European system, freely accessible databases produced by the JRC are used. The resolution of the data lines also corresponds to this. 250 m for components affecting fire behaviour, 0.25 degrees for FWI for fire ignition.

Table 1 shows which components must be included in the forest fire risk assessment model and which data sources are available in Hungary.

We have selected an observation area in which we can examine how certain parameters of the forest fire risk assessment behave under conditions in Hungary, and from which data source they can be obtained.

Our main observation plot is in South Hungary, in Bács-Kiskun County nearby the town Kiskőrös. The area belongs to the professional fire department of Kiskőrös, where a lot of wildfires occur each year. Approximately 20% more fires occur here each year than in other counties of the country, and several of these are large-scale wildfires, which are the biggest challenge for firefighters.[27]

[26] De Rigo et al. 2017
[27] Ronchi et al. 2021

Table 1: Datasets for the components of the wildfire risk assessment system

Wildfire risk component		Subcomponent	Values	Source
Fire danger or hazard	Ignition	Human cause	Historical fire data	Forest Fire Information System of Hungary
	Fire behaviour	Fuel moisture content	Dead fuel moisture content	Fire weather index
		Fuel types	Vegetation types	Corine Land Cover
		Climatic conditions	Wind, humidity, precipitation, temperature	Hungarian Meteorological Service
		Terrain	Slope, aspect	Topographical maps of Hungary
Vulnerability	People	People in WUI	Wildland-urban interface	OSM
	Ecological value	Ecological indicators	Irreplaceability score10 Protected area Potential burnable land	Protected area Natura2000 sites
	Socio-economic value	The monetary value of land cover and vegetation	Forest fire damage restoration costs	Corine Land Cover, restoration costs
		House, infrastructure	House, infrastructure	Local maps

Source: *Compiled by the authors based on San-Miguel-Ayanz 2019*

5.1. Wildfire danger

Wildfire danger is influenced by factors related to the probability of ignition and those affecting fire behaviour. It is therefore composed of the likelihood/possibility of having a fire ignition, and the behaviour (propagation and intensity) of a fire once it is ignited.

5.1.1. Wildfire ignitions

In Europe, the vast majority of ignitions are due to human causes (either deliberate, or accidental), exposing the critical role of the human factor in fire occurrence and fire conditions, either by increasing ignitions or by suppressing activities. Naturally

caused fires are normally a very small fraction of the total number of fires in Europe. The distribution of fire causes shows a similar picture in Hungary.

Based on the information obtained from the EFFIS, the most common cause of the fire is carelessness (96%). Cigarette butts thrown from a car, train, or bicycle, carelessly left campfires, carelessly done small garden and stubble burning, poorly organised barbecues and potlucks, or poorly executed slaughterhouse waste burning in forest areas are acts that can be categorised as careless negligence. The annual burning of lawns and shrubbery areas adjacent to forest areas to renew the vegetation can be classified as conscious carelessness (luxury). A natural cause or intentionality was indicated in 2–2% of the cases. For natural reasons, summer lightning can cause forest fires. In some cases, the origin of the fire can be traced back to some technical error (a broken electrical wire or a spark falling from the machine on the stubble).

Studying the high number of fire incidents and the cause of fire recorded on the data sheets, it is also necessary to draw attention to the fact that the fires were caused by breaking the fire lighting and fire use rules. According to the regulations in force, open burning of standing vegetation, stubble and waste generated in connection with plant cultivation is prohibited.

5.1.2. Fire behaviour

The fire behaviour is conceptually influenced by the fuel moisture content of both dead and live fuels, the different fuel types, slopes and wind patterns that will determine the propagation (rate of spread and spread direction) of a wildfire.

5.1.3. Fuel moisture

Fuel moisture content is a fundamental element for the availability of fuel for combustion, and as dry fuels burn easily, it is a fundamental element in providing favourable conditions for wildfire propagation.[28] The fuel moisture content, defined as the proportion of water contained in the vegetation about dry, fluctuates in time and space and is highly dependent on weather conditions. Fine fuel components may show a fast response to changing weather so that a windy, dry day might easily trigger a noticeable drop in their moisture content. On the other hand, thicker parts of the vegetation define quite a different fuel component: if thicker fuel requires more time (even several days or weeks) to dry under weather conditions facilitating the process, it conversely may preserve this dryness for a longer period, with higher latency to fast-changing weather. Even (not major) precipitation events may be unable to significantly increase a low fuel moisture content in thicker fuels, while a minor rainfall could easily saturate the moisture of finer fuels. Therefore, the behaviour of a wildfire is not only linked with the very recent weather conditions but also with the cumulative effect of the past weather.

[28] Yebra 2013

Common indices used for assessing vegetation moisture content of dead fuels are the three moisture indices which are components of the Canadian FWI system, Fine Fuel Moisture Code (FFMC), Duff Moisture Code (DMC), and Drought Code (DC), focusing respectively on fine, intermediate and thicker components of fuel. The dynamic nature of these indices, and their ability to keep the memory of past weather conditions, have been associated with their partial ability (especially for the components with longer time inertia) to correlate even with live fuel moisture.

For the risk assessment, we used the FWI which is a combination of the ISI index and the Buildup Index (BUI) which by combining DMC with DC, models the total amount of fuel available for consumption, providing a uniform numerical rating of the relative fire potential, by dynamically combining the information from four local meteorological variables such as temperature, wind speed, relative humidity and precipitation. The higher the FWI is, the more favourable the meteorological conditions would be to start a wildfire. The FWI uses information on the moisture content of dead fuels, as estimated from meteorological variables, and wind speed to determine the level of "fire danger" in different areas.[29] Long-term series of FWI data can be used as an explanatory variable in the assessment of wildfire danger at the pan-European level. The FWI has been proven suitable for European conditions[30] and is currently used in the EFFIS and widely adopted by many European countries as a best-harmonised approach to assess wildfire danger.[31] As detailed in the presentation of the domestic forest fire risk assessment system, the forestry authority also uses FWI in its daily work. We download the raster data for Hungary from the JRC database daily and evaluate the daily fire weather situation.

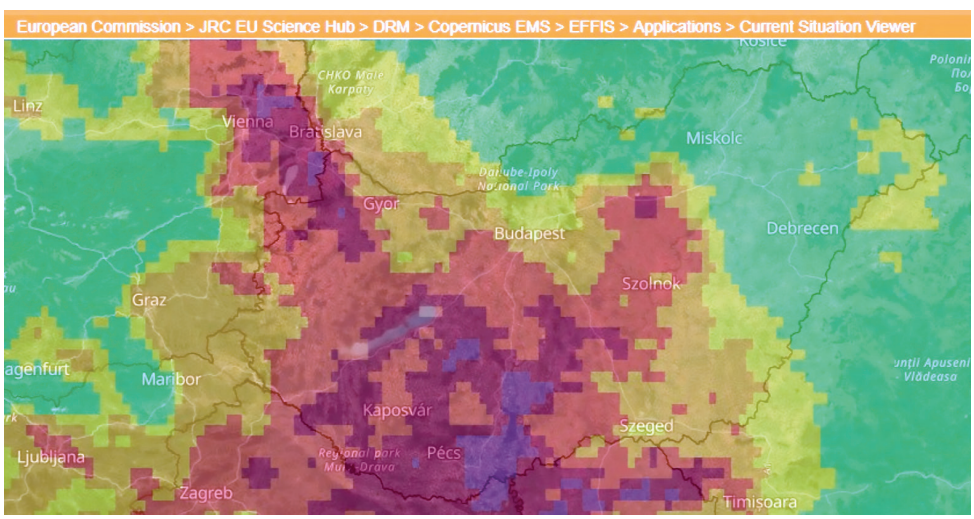


Figure 9: Fire Danger Forecast for Hungary
Source: European Commission s. a.

[29] Van Wagner 1987
[30] Viegas 1999
[31] San Miguel et al. 2017

5.1.4. Fuel–vegetation types

The type of fuel available to burn, which may include trees, shrubs, grasslands, etc., will directly influence wildfire propagation and is key to fire propagation risk assessment as it considers the changes and dynamics of vegetation due to fire.[32] Each type of vegetation fuel, with its physical and chemical-specific attributes and its phenology, affects wildfire behaviour (rate of spread, fire intensity and propagation) and the impacts of wildfires. Moreover, wildfire behaviour is highly dependent on the horizontal and vertical structure of the fuels and the interconnection among them, which may determine the horizontal and vertical progression of the firefront.

In Hungary, we use the Corine Land Cover (CLC) collections (2000, 2006, 2020, 2018) in the fire risk assessment. Based on the literature data, it is necessary to refine the resolution of the Corine database to make the estimation of the combustible material in the model more accurate. We prepared the CLC map for the sample area (Figure 8). Areas marked in red are high-risk areas based on the land cover map.

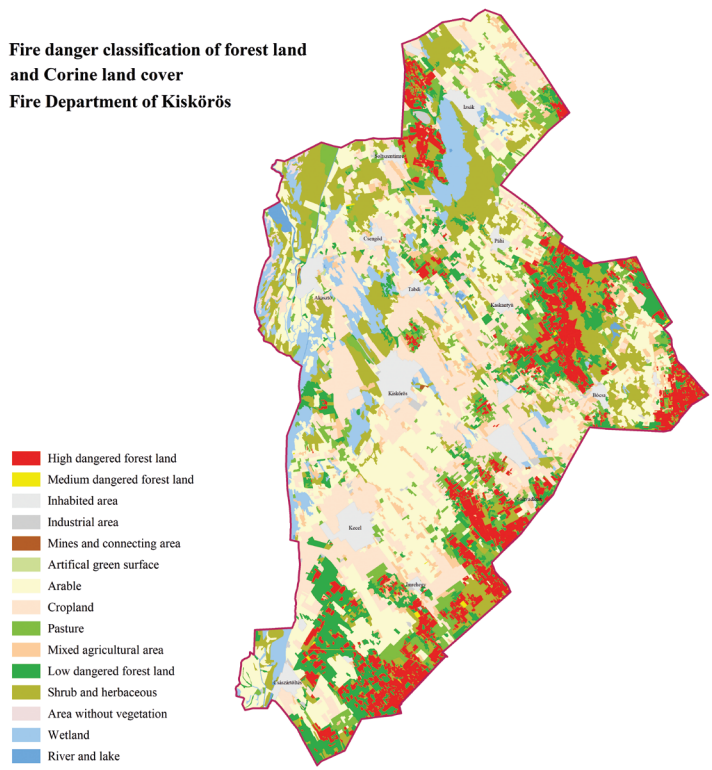


Figure 8: Fire danger classification of forest land and Corine Land Cover in the area of the Fire Department of Kiskőrös

Source: Compiled by the authors based on Corine Land Cover and Hungarian Forest GIS Database.

[32] Aragoneses–Chuvieco 2021

5.1.5. Slopes–Wind

The slope is the rate of change of elevation in the direction of the water flow line and it is especially important for the quantification of soil erosion, water flow velocity, or agricultural suitability. Angle, aspect and elevation is relevant for fire behaviour and wildfire propagation. For example, steep slopes (15°–20°) may affect wind direction and speed facilitating fire spread. In areas subject to frequent fire occurrence, even the local soil and vegetation composition may differ depending on the orography.[33] Associated with terrain characteristics, local wind conditions (direction, speed) could also affect wildfire propagation and intensity. Information on topography can be obtained from contour maps. Contour maps are available in Hungary from several sources. Contour maps made by digitising military maps can be obtained from the Lechner Knowledge Center. A land surface model created by the NASA space program using the radar interferometric process can be downloaded free of charge from the website of the U.S. Geological Survey (Shuttle Radar Topography Mission).[34] The model is also available for the Carpathian basin. Considering that the sample area is located on flat terrain, we did not examine the role of the slope separately in this research.

5.2. Vulnerability

The term "vulnerability" is intended to encompass people, ecosystems and goods exposed in vulnerable areas. This concise term includes the presence of assets within hazard zones,[35] and their susceptibility to suffering damage,[36] and within the risk framework, it is intended to be evaluated before the fire occurs. Defined as "the conditions determined by physical, social, economic and environmental factors or processes, which increase the susceptibility of an individual, a community, assets or systems to the impacts of hazards" by UNISDR, it has been recently included in fire risk systems, referring to the condition of assets that are exposed and subject to being damaged by wildfires. As anticipated, we consider three categories of vulnerability:

- people (focusing on the population exposed in the WUI by ecological indicators beyond economy and market)
- assets at the interface between nature and human activity (for example, forests, another woodland, and agricultural land) whose market value (e.g. timber, agriculture products) can be quantified monetarily

5.2.1. People

Populated areas are often close to wildlands, generating a human–nature interface. This may be observed where abandoned agricultural areas lead to an expanding wildland, or

[33] De Rigo et al. 2017
[34] For more information see www.usgs.gov
[35] United Nations 2009
[36] San Miguel et al. 2017

conversely where settlements enlarge over areas previously dominated by wildland. The evaluation of the 'social vulnerability'[37] is often focused on this interface, designated as the WUI. This interconnected patch interface enhances the potential ignition agents and with a lack of fuel management can easily increase the wildfire risk, especially in a fire-prone landscape, posing a major threat to the population living in the WUI. Ignitions are more frequent because of the accessibility of fuels to people, threatening also neighbouring locations in the WUI, because fires may spread in fuel-rich areas within or adjacent to the WUI. Consequently, the risk of fire near these areas may be especially high for the population.[38] Particular attention is given to the topic all over the world.[39]

We examined the fire statistics on wildfires from the last 10 years, especially in the observation plot. We distinguished the fires according to their distance from the residential area. The location of fires in residential areas is also very important, so we examined it in Table 1. The resilience of buildings is also important,[40] but we will not analyse it in this research. Using TopoXmap, we have created buffer zones around the boundary line of populated areas. We put fires in the WUI-1 zone that occurred 500 meters from the residential area. Additional zones were as follows: WUI-2 zone – 1,000 m; WUI-3 zone 1,500 m; – WUI-4 zone 2,000 m; and WUI-5 zone 2,500 m. After creating the buffer zones, a GIS topological test was performed to determine which WUI zone the starting point of each fire falls into. In Table 2, fires in WUI-1 and WUI-2 zones (red and orange hoops) are important for the analysis, because these fires pose a threat to the residential areas.

Table 2: Number of wildfires in the WUI zones in the observation plot

Year	Number of wildfires	WUI-1	WUI-2	WUI-3	WUI-4	WUI-5
2011	103	42	17	9	9	26
2012	278	114	42	25	21	76
2013	66	23	11	8	6	18
2014	78	35	5	5	9	24
2015	50	18	6	2	5	19
2016	69	24	10	12	4	19
2017	145	32	30	21	22	40
2018	45	8	9	10	5	13
2019	180	41	25	22	34	58
2020	85	26	11	8	15	25
	123	29	23	20	16	35

Source: Compiled by the authors based on the Forest Fire Information System of Hungary.

[37] Wigtil et al. 2016
[38] Pastor et al. 2020
[39] Kaim et al. 2018
[40] Érces–Ambrusz 2022

We performed GIS Spatial analyses with topoXmap in Figure 3, which presents fires that occurred in wildland areas of the settlements in the observation plot. The red colour indicates fires that occur within 500 meters from the residential area (WUI-1 zone) and the orange those that occur within 1 km (WUI-2 zone).

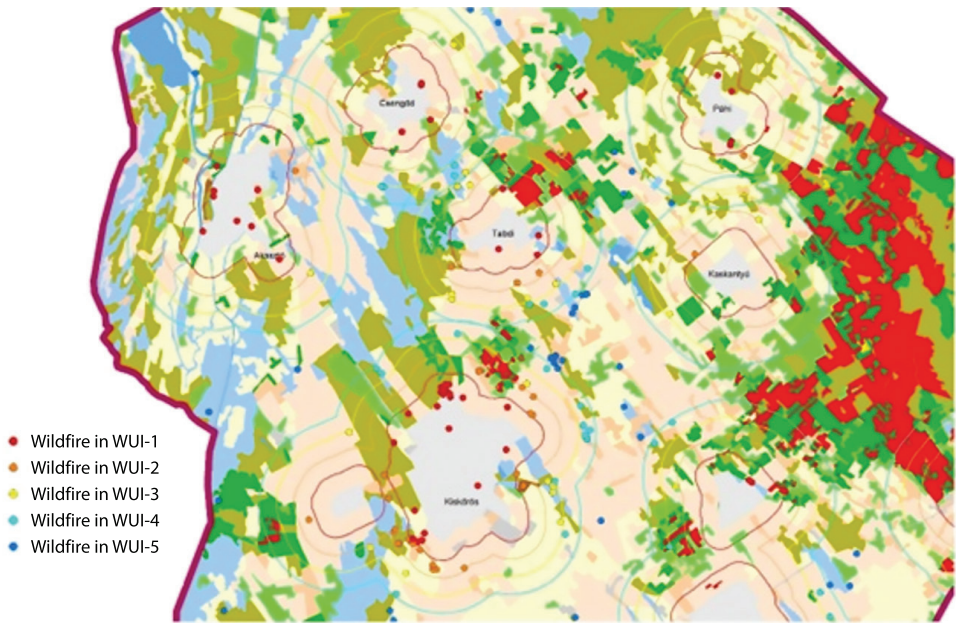


Figure 9: Wildfires (2011–2021) and WUI zones nearby Kiskőrös
Source: Compiled by the authors based on Corine Land Cover and Forest GIS Database.

5.2.2. Ecological value

Generally, the ecological impacts from a wildfire are mainly focused on the non-monetary values of ecosystem services, such as the negative impacts of fires on two major components: soils (soil loss, decreasing soil fertility, erosion) and vegetation cover. The protection of ecological assets is essential for all forms of life, including humans.

The vulnerability of an ecosystem's environmental value could be assessed through ecological indicators related to these three aspects at several temporal scales, such as short (immediately after the fire) and long-term (changes in vegetation structure and composition after a few decades including the vegetation response-ability). Ecological indicators may include the distribution of protected natural areas, and of areas of those ecosystems in which the recovery after wildfires may be compromised by weather conditions. Considering that ecological values are difficult to measure as they are often intangible, we suggest a qualitative approach to assess the ecological vulnerability within the wildfire risk framework. Therefore, to emphasise the special ecological values of the territory we use the Natura 2000 network.

Details of Hungarian Natura2000 are available on the website of the nature conservation authority (https://natura.2000.hu/).

5.2.3. Socio-economic value

Socio-economic damage caused by wildfires affects people's livelihood, safety and health. Vulnerable areas may be identified considering the presence and value of houses and infrastructure, the monetary value of the vegetation and wildlife that may burn, as well as the value of ecosystem services that would be lost after wildfires. Properties, infrastructures, economic services provided by the vegetation (wood, non-wood products, hunting revenues, fungi, etc.), agricultural products, carbon stocks, or recreational and tourist services can be associated with economic and social factors and be a part of the "tangible" values at stake (vulnerability) in the wildfire risk assessment.

In recent research, it was not possible to conduct a full-scale survey regarding socio-economic value. The built environment and infrastructure can currently be mapped based on the public Open Street Map data file. Methodology still needs to be developed to examine this factor in the domestic forest fire risk assessment.

6. Conclusions

A wildfire risk map was generated by JRC as a prototype index to summarise the combined effect of wildfire danger and vulnerability. An aggregated wildfire risk index is proposed, which prioritises the risk for human lives, while also considering ecological and socio-economic aspects. This is done by ranking as high-risk areas those where people may be exposed to wildfires, and secondarily other areas where ecological and socio-economic aspects are at stake. High risk may be expected where high wildfire danger affects the most critical areas for people, and secondarily for the other ecological and socio-economic aspects.

The method is also suitable for recalculating the fire risk for the entire country at certain intervals, even every year. In this way, changes due to sociological and economic reasons can also be followed. The fire risk assessment prepared by the JRC specifies the classification of a given area on a 12 km resolution raster map. Local data is required to prepare a higher-resolution fire risk assessment that also takes local specialties into account. Before preparing the assessment, it is necessary to define the goal that we want to achieve by preparing the risk maps. A forecasted risk estimate for the fire season helps the fire department and the forestry authority control. By increasing inspections, the public's attention can be drawn to the dangers that arise during the fire season. With targeted inspections, the authority can gather the areas that are particularly at risk. The maps based on the individual components can be used during firefighting. The land cover map and the relief map show important information about the possible spread of the fire. The component representing ecological values provides information on the damage caused and the difficulties of restoration.

The risk assessment prepared by the JRC classifies the regions of Hungary affected by forest fires (Northern Hungary, Great Plains) as high-risk areas. This fact shows that forest fire risk assessment and its usability should be considered an important issue shortly. By adapting the methodology, we can facilitate the clarification of the risk assessment prepared by the JRC, and we can give a new direction to the domestic risk assessment by incorporating new components.

The program was financed by the National Research Development and Innovation Office Fund and was implemented in the funding of the Thematic Program of Excellence 2020 application program number TKP2020-NKA-09.

References

Aragoneses, Elena – Chuvieco, Emilio (2021): Generation and Mapping of Fuel Types for Fire Risk Assessment. *Fire,* 4(3). Online: https://doi.org/10.3390/fire4030059

Bányai, Tamás – Pántya, Péter (2020): Településeken kívül eső lakott ingatlanok tűzoltói beavatkozásainak sajátosságai egy konkrét eset elemzésével [Particularities of Firefighter Intervention at Residential Buildings Outside of Settlements: A Case Study]. *Hadmérnök,* 15(2), 79–91. Online: https://doi.org/10.32567/hm.2020.2.6

Bodnár, László (2017): Case Study of "Hortobágy" and "Kunfehértó" Fires, Hungary: Disaster in Costs of their Elimination's View. *Ecoterra: Journal of Environmental Research and Protection,* 14(1), 40–46.

Bodnár, László (2020): Lakott területet érintő erdőtüzek vizsgálata, és a védekezés egyes lehetőségei [Examination of Forest Fires at Inhabited Areas and Certain Possibilities of Protection]. *Hadmérnök,* 15(1), 45–61. Online: https://doi.org/10.32567/hm.2020.1.4

Camia, Andrea – Durrant, Tracy – San-Miguel-Ayanz, Jesus (2014): *The European Fire Database. Technical Specifications and Data Submission.* JRC Science and Policy Reports, European Commission. Online: https://doi.org/10.2788/2175

Chuvieco, Emilio – Aguado, Inmaculada – Jurdao, Sara – Pettinari, M. Lucrecia – Yebra, Marta – Salas, Javier – Hantson, Stijn – de la Riva, Juan – Ibarra, Paloma – Rodrigues, Marcos et al. (2012): Integrating Geospatial Information into Fire Risk Assessment. *International Journal of Wildland Fire,* 23(5), 606–619. Online: https://doi.org/10.1071/WF12052

Debreceni, Péter (2021): Magyarországi vegetációtüzek keletkezési okainak vizsgálata és osztályozása [Study and Classification of the Causes of Wildfires in Hungary]. *Műszaki Katonai Közlöny,* 31(4), 111–128. Online: https://doi.org/10.32562/mkk.2021.4.8

De Rigo, Daniele – Libertà, Giorgio – Houston Durrant, Tracy – Artés Vivancos, Tomas – San-Miguel-Ayanz, Jesús (2017): *Forest Fire Danger Extremes in Europe under Climate Change: Variability and Uncertainty.* Luxembourg: Publications Office of the European Union. Online: https://doi.org/10.2760/13180

Érces, Gergő – Ambrusz, József (2022): Természeti csapásoknak ellenálló épületek. *Polgári Védelmi Szemle,* DAREnet projekt Különszám, 116–131.

European Commission (2021): *Land-based wildfire prevention. Principles and experiences on managing landscapes, forests and woodlands for safety and resilience in Europe.* Luxemburg: Publications Office of the European Union. Online: https://doi.org/10.2779/695867

European Commission (s. a.): *Copernicus. Emergency Management Service.* EFFIS. Online: https://effis.jrc.ec.europa.eu/apps/effis_current_situation/

Finney, Mark (2005): The Challenge of Quantitative Risk Analysis for Wildland Fire. *Forest Ecology and Management,* 211(1–2), 97–108. Online: https://doi.org/10.1016/j.foreco.2005.02.010

Ganteaume, Anne – Camia, Andrea – Jappiot, Marielle – San-Miguel-Ayanz, Jesús – Long-Fournel, Marlène – Lampin, Corinne (2013): A Review of the Main Driving Factors of Forest Fire Ignition over Europe. *Environmental Management,* 51(3), 651–662. Online: https://doi.org/10.1007/s00267-012-9961-z

Hardy, Colin (2005): Wildland Fire Hazard and Risk: Problems, Definitions, and Context. *Forest Ecology and Management,* 211(1–2), 73–82. Online: https://doi.org/10.1016/j.foreco.2005.01.029

Kaim, Dominik – Radeloff, Volker – Szwagrzyk, Marcin – Dobosz, Monika – Ostafin, Krzysztof (2018): Long-Term Changes of the Wildland–Urban Interface in the Polish Carpathians. *ISPRS International Journal of Geo-Information,* 7(4). Online: https://doi.org/10.3390/ijgi7040137

Lee, Byran (2003): *Fire Danger, Fire Risk, Fire Threat – Mapping Methods. EARSeL.* Ghent: International Workshop on Remote Sensing and GIS Applications to Forest Fire Management.

MPI Feuerökologie und Biomassverbrennung AG (1994): *Feuer in Umwelt.* Freiburg: Max Planck Institut.

Nagy, Dániel (2013): Erdőtűz megelőzési intézkedések erdővédelmi, tűzterjedési és ökonómiai paramétereinek kidolgozása [Development of Parameters for Forest Protection, Fire Spread and Economics of Forest Fire Prevention Measures]. Sopron: West Hungarian University.

Pastor, Elsa – Muñoz, Juan – Caballero, David – Àgueda, Alba – Dalmau, Ferran – Planas, Eulália (2020): Wildland–Urban Interface Fires in Spain: Summary of the Policy Framework and Recommendations for Improvement. *Fire Technology,* 56, 1831–1851. Online: https://doi.org/10.1007/s10694-019-00883-z

Radeloff, Volker – Hammer, Raphael – Stewart, Susanne (2005): The Wildland-Urban Interface in the United States. *Ecological Application,* 15(3), 799–805. Online: https://doi.org/10.1890/04-1413

Restás, Ágoston (2020): Az amazóniai, afrikai és ausztrál erdőtüzek tanulságai [Lessons of the Amazonian, African and Australian Wildfires]. *Védelem Katasztrófavédelmi Szemle,* 27(4), 23–26.

Rothermel, Richard (1972): *A Mathematical Model for Predicting Fire Spread in Wildland Fuels.* Ogden: Intermountain Forest and Range Experiment Station, U.S. Department of Agriculture.

Ronchi, Enrico – Wong, Stephen – Suzuki, Sayaka – Theodori, Maria – Wadhwani, Rahul – Vaiciulyte, Sandra – Gwynne, Steve – Rein, Guillermo et al. (2021): *Case Studies of Large Outdoor Fires Involving Evacuations.* Emergency Management & Evacuation (EME) Subgroup, Large Outdoor Fires & the Built Environment (LOF&BE) Working Group of the International Association for Fire Safety Science. Online: https://doi.org/10.5281/zenodo.4504853

San Miguel, Jesus – Chuvieco, Emilio – Handmer, John – Moffat, Andy – Montiel-Molina, Cristina – Sandahl, Leif – Viegas, Domingos (2017): Climatological Risk: Wildfires. In Poljanšek, Karmen – Marín Ferrer, Montserrat – De Groeve, Tom – Clark, Ian (eds.): *Science for Disaster Risk Management 2017: Knowing Better and Losing Less.* Luxembourg: Publications Office of the European Union, 294–305. Online: https://doi.org/10.2788/842809

San-Miguel-Ayanz, Jesús – Costa, Hugo – de Rigo, Daniele – Libertà, Giorgio – Artés Vivancos, Tomas – Durrant, Tracy – Nuijten, Daniel – Löffler, Peter et al. (2019): *Basic Criteria to Assess Wildfire Risk at the Pan-European Level.* Luxembourg: Publications Office of the European Union. Online: https://doi.org/10.2760/052345

Teknős, László: Current Issues in Disaster Management Aspects of Global Climate Change. In Földi, László – Hegedűs, Hajnalka (eds.): *Effects of Global Climate Change and Improvement of Adaptation Especially in the Public Service Area.* Budapest: Dialóg Campus, 145–162.

United Nations (2009): *UNISDR Terminology on Disaster Risk Reduction.* Geneva: United Nations International Strategy for Disaster Reduction. Online: https://purl.org/INRMM-MiD/c-13239301

Van Wagner, C. E. (1987): *Development and Structure of the Canadian Forest Fire Weather Index System.* Ottawa: Canadian Forestry Service.

Vhiriri, Eunice – Irwin, Yoland – Laubscher, Richard K. – Tandlich, Roman (2021): Short Communication: Quantitative Analysis on Gender Related Vulnerabilities and Fatalities in Disaster Situations in South Africa. *Védelem Tudomány,* 6(3), 565–592.

Viegas, D. Xavier – Bovio, Giovanni – Ferreira, Almerindo – Nosenzo, Antonio – Sol, Bernard (1999): Comparative Study of Various Methods of Fire Danger Evaluation in Southern Europe. *International Journal of Wildland Fire,* 9(4), 235–246. Online: https://doi.org/10.1071/WF00015

Wigtil, Gabriel – Hammer, Roger – Kline, Jeffrey – Mockrin, Miranda – Stewart, Susan – Roper, Daniel – Radeloff, Volker (2016): Places Where Wildfire Potential and Social Vulnerability Coincide in the Coterminous United States. *International Journal of Wildland Fire,* 25(8), 896–908. Online: https://doi.org/10.1071/WF15109

Xi, Dexen – Taylor, Stephen – Woolford, Douglas – Dean, C. B. (2019): Statistical Models of Key Components of Wildfire Risk. *Annual Review of Statistics and Its Application,* 6, 197–222. Online: https://doi.org/10.1146/annurev-statistics-031017-100450

Yebra, Marta – Dennison, Philip – Chuvieco, Emilio – Riaño, David – Zylstra, Philip – Hunt, Raymond – Danson, Mark – Qi, Yi – Jurdao, Sara (2013): A Global Review of Remote Sensing of Live Fuel Moisture Content for Fire Danger Assessment: Moving towards Operational Products. *Remote Sensing of Environment,* 136, 455–468. Online: https://doi.org/10.1016/j.rse.2013.05.029

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG

17. évfolyam (2022) 4. szám 101–112.
DOI: 10.32567/hm.2022.4.7

Dobor József,[1] Kiss Noémi,[2] Pátzay György[3]

Radioaktív izotópok egészségügyi használata és lehetséges kockázatainak összefoglalása

The Medical Use of Radioactive Isotopes and Summary of Potential Risks

Jelen cikk a radioaktív izotópok egészségügyben történő felhasználását és veszélyeit foglalja össze. A szerzők az egészségügyi felhasználás sokszínűségének bemutatásával szemléltetik a radioaktív izotópok alkalmazásának szükségességét, ismertetve a radioaktivitás veszélyeit. Ezek a veszélyek a biztonsági előírások be nem tartása esetén olyan eseményeket indíthatnak el, amelyek súlyos következményekkel járhatnak.

Már több mint száz éve tudatosan használják gyógyászati célzattal a radioaktív izotópokat, a velük kapcsolatos tudásanyag folyamatosan bővül, kutatások zajlanak, amelyek új lehetőségeket tárnak fel. A szén egyik instabil izotópja a szén-14 radioizotóp, amelyet az egészségügy mellett a kormeghatározásban is felhasználnak. A technécium-99m radioaktív izotópot a pajzsmirigybetegségek szcintillográfiás kimutatására használják.

Megítélésük meglehetősen ellentmondásos, ugyanis ellenőrzött körülmények között, számított mennyiségben, a sugárvédelem alapelveit betartva fontos segítői az emberiségnek, de ha egy balesetben kikerülnek a környezetbe, élő szervezet közelében káros hatásukat hosszú távon ki tudják fejteni. Napjainkra a radioaktív izotópok többsége gyakorlatilag nélkülözhetetlen, az 1900-as évek elejétől tudatosan, tervezetten szolgálják az emberiséget.

Kulcsszavak: **radioaktív izotópok, egészségügyi alkalmazás, radiológiai veszélyek**

[1] Habilitált egyetemi docens, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Katasztrófavédelmi Intézet Iparbiztonsági Tanszék, e-mail: dobor.jozsef@uni-nke.hu
[2] MA-hallgató, Nemzeti Közszolgálati Egyetem, e-mail: kissnnoemi@gmail.com
[3] Egyetemi tanár, Nemzeti Közszolgálati Egyetem, Rendészettudományi Kar Katasztrófavédelmi Intézet Iparbiztonsági Tanszék, e-mail: patzay.gyorgy@uni-nke.hu

This article summarises the use and dangers of radioactive isotopes in healthcare. The authors illustrate the need for the use of radioactive isotopes by presenting the diversity of medical uses, explaining the dangers of radioactivity. These hazards can trigger events with serious consequences if safety regulations are not respected. Radioactive isotopes have been consciously used for medical purposes for more than a hundred years, the body of knowledge related to them is constantly expanding, and research is taking place that reveals new possibilities. One of the unstable isotopes of carbon is the carbon-14 radioisotope, which is used not only in healthcare but also in age determination. The radioactive isotope technetium-99m is used for scintillographic detection of thyroid diseases. Their assessment is rather ambivalent, because under controlled conditions, in calculated quantities, and in compliance with the basic principles of radiation protection, they are important helpers to humanity, but if they are released into the environment in an accident, they can exert their harmful effects in the long term near a living organism. Nowadays, the majority of radioactive isotopes are practically indispensable, they have been consciously and deliberately serving humanity since the beginning of the 1900s.

Keywords: **radioactive isotopes, health applications, radiological hazards**

1. Bevezetés

Az ipari alkalmazás mellett napjainkban az egészségügyben alkalmazzák rendszerint a radioaktív izotópokat. Bár nagy kockázatokat hordoz magában, amennyiben ellenőrizetlenül kerül a környezetbe, veszélyeit az emberiség a biztonságos felhasználással előnnyé formálta. Az egészségügyben több céllal is alkalmazzák a radioaktivitást. A daganatos megbetegedések során a célzott sejtpusztítás mellett felhasználható a képalkotó diagnosztikában, továbbá tartós ízületi gyulladás kezelésére, fájdalomcsillapításra és pajzsmirigybetegségek gyógyítására is. A továbbiakban mindazon előnyök mellett, amelyekre az emberiség a radioaktív izotópok egészségügyi felhasználása által tett szert, bemutatjuk azokat a veszélyeket, amelyeket a radioaktivitás jelent.

A periódusos rendszerben található 118 elem közül mindössze 94 fordul elő a természetben. Jelenlegi tudásunk szerint 254 stabil izotóp létezik, és több mint 3000 radioaktív izotóp ismeretes, közülük körülbelül 84 található meg a természetben.[4]

2. A radioaktív izotópok felhasználása a képalkotó diagnosztikában

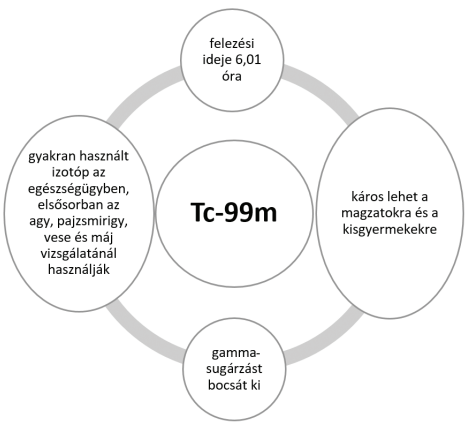
A radioaktív izotópok felhasználása a képalkotó vizsgálatok során hatalmas előnyt jelent egyes rendellenességek kimutatása során, megbetegedések feltérképezésében a korai stádiumban, továbbá támogatást nyújt az ezekre irányuló terápiák kialakításában. A velük történő vizsgálatok olyasforma csekély sugárterheléssel járnak, mint a röntgenvizsgálatokkal járó sugárterhelés. Az izotópdiagnosztikai eljárásokkal sokkal hamarabb feltérképezhető a szerv kóros állapota, így egy csontáttétes daganat akár fél évvel korábban feltárható ezzel

[4] International Atomic Energy Agency é. n.

a vizsgálati módszerrel, mint röntgenfelvétellel.[5] A vizsgálatok során az instabil izotópot szájon át, belélegezve vagy a leggyakrabban vénás úton juttatják be az emberi szervezetbe.[6]

A csontszcintigráfia[7] a leggyakrabban elvégzett izotópdiagnosztikai eljárás, amellyel megvizsgálható a csontok állapota. A daganatos megbetegedések esetében kimutatható vele, hogy a daganat adott-e csontáttétet, de nem megfelelően gyógyuló csonttörések esetében és az ok nélkül bekövetkező csontfájdalmak vizsgálására, valamint állapotfelmérésre is használható ízületi protézisek esetében. A csontszcintigráfia működési elve a foszfátok csontokba való beépülésének mérésén alapszik. A vizsgálatok során általában technécium radioizotóppal jelölik meg a szerves foszfátot, amelyet aztán a véráramba vénán keresztül juttatnak be. A gamma-sugárzó technécium izotóp eloszlását a szervezetben úgynevezett gamma-kamerák[8] segítségével figyelik meg, amellyel a csontok állapota határozható meg.[9]

Az 1. ábrán a technécium-99m radioaktív izotóp jellemzőit foglaltuk össze.



1. ábra: Technécium-99m radioaktív izotóp jellemzése
Forrás: a szerzők szerkesztése az International Atomic Energy Agency 2009a. alapján

A szív vérrel való ellátottsága és a szívizmok károsodása kimutatható a szívizom izotópos vizsgálatával, amelyre az egyik legalkalmasabb izotóp a technécium-99m.[10] A vizsgálat kétnapos, ugyanis terheléses és nyugalmi vizsgálatokból áll. A terheléses vizsgálat éhgyomorral zajlik, a vizsgálatot megelőzően semmilyen szívre ható gyógyszer nem alkalmazható. A vizsgált személy véráramába izotóppal jelzett értágító gyógyszert juttatnak. A nyugalmi vizsgálat ugyancsak éhgyomorral zajlik, azonban már bevehetők a szívműködést befolyásoló gyógyszerek, és értágító szer nélkül adják be az izotóppal jelzett anyagot. A vizsgálatok a radioaktív anyag beadását követően, másfél óra elteltével

5 Csinády 2018.
6 Rosenblatt–Zubizarreta 2017.
7 A rosszindulatú daganatok csontáttéteinek kimutatására szolgáló egyik legérzékenyebb képalkotó eljárás.
8 A nukleáris medicina esetében alkalmazott diagnosztikai eszköz, amellyel gamma-sugárzást kibocsátó nuklidok (pl. ^{131}I, ^{99m}Tc) szervezeten belüli eloszlása vizsgálható.
9 Halama et al. 2019.
10 International Atomic Energy Agency 2009a.

kezdődnek meg, és nagyjából húsz perc időtartamúak. A gamma-kamerával felvételeket készítenek, a vizsgálatok végeredményeit összehasonlítva alkotják meg a diagnózist.[11]

A vese működéséről általában a technécium-99m izotóppal alkotnak képet, amellyel feltárható a szerv károsodása, alaki és működési rendellenességei. A vizsgálat segítségével megállapítható, hogy a szerv mekkora része működőképes, valamint kimutatható a térfogatának nagysága. A vese funkciójának vizsgálata alkalmával a tisztítási hányados szerint elenyésző mennyiségű radioaktív izotóppal jelezhető a működése. A vizsgálat igazolhatja vagy kizárhatja a húgyutak elzáródását, megállapítható a reflux fennállása és annak mértéke, továbbá megállapítható, hogy a magas vérnyomást a veseartéria szűkülete okozza-e.[12] Az izotópokat a véráramba bejuttatva azonnal megkezdődnek a vizsgálatok, fél órás időtartamban gamma-kamerán keresztül figyelik meg a szerv működését. Amennyiben a vese megfelelően funkcionál, a radiofarmakon[13] négy óra alatt majdhogynem teljesen kikerül a páciens szervezetéből.[14]

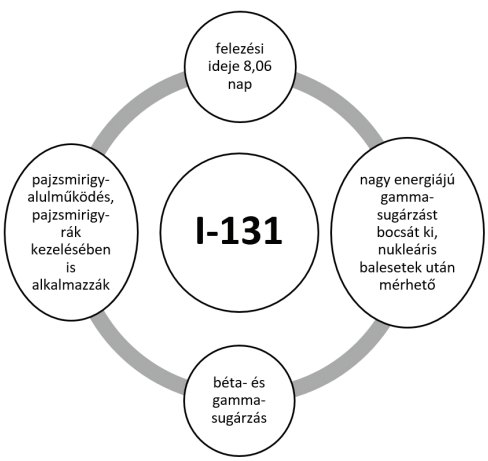
- Izotópos vizsgálattal a máj rosszindulatú megbetegedései is indikálhatóak, mint például az áttétes májdaganat, illetve a károsodás nagysága. Megállapíthatók vele májbetegségek, akárcsak a hepatitis vagy a májzsugor, továbbá a gócos májeltérések.[15] Szervátültetést követően a máj szövődményeinek jelzésére ugyancsak használható az izotópos vizsgálati eljárás. Ennek során technécium-99m izotópot használnak, amelynek a véráramba juttatása után 20-30 perccel készítenek felvételeket.[16] Az epe kivizsgálása során az epe működését, továbbá az esetleges elzáródásait figyelik meg. A vizsgálódások előtt a betegnek 4-6 órán át tilos étkeznie a pontos eredmények érdekében. Ha a vizsgált személy rendelkezik epehólyaggal, a vizsgálat folyamán az epe összehúzódásának elősegítéséért étcsokoládét kell fogyasztania.[17]
- Izotópok segítségével, kiegészítő jellegű módszerrel vizsgálható az agy stroke esetében, továbbá az agyi vérellátás aktuális állapota is meghatározható agyiér-betegségek gyanúja esetén. Adott esetben alkalmazzák az agyhalál kimutatására. Az izotópos vizsgálatot igénybe veszik mozgászavarok eredetének felmérésére és pszichiátriai elemzések esetében is. A technécium-99m izotóppal indikált hexametil-propilénamin-oxid a véráramba kerül, majd a radiofarmakon a véráramlással összegyűlik az agyszövetben.[18] A vizsgálatot megelőzően a betegek – a nyálmirigyeik képeken való megmutatkozásának redukálása érdekében – gyógyszert kapnak, ezen felül előfordul, hogy egy a vér áramlását növelő gyógyszert is be kell venniük. A véráramlás-fokozó szer generálhat szédülést, hányingert, ízérzékelési zavarokat, fejfájdalmakat és fülzúgást. A vizsgálatok nem éhgyomorra történnek, azonban az előtte levő napon tilos alkoholt és koffeint tartalmazó folyadékokat fogyasztani.[19]

[11] Halama et al. 2019.
[12] Varga 2002.
[13] Gyógyászatban használt radioaktív izotóp felhasználása specifikus anyag jelenlétében.
[14] Srivastava et al. 2012.
[15] Srivastava et al. 2012.
[16] International Atomic Energy Agency 2009a.
[17] Taylor et al. 2018.
[18] Györke é. n.
[19] Jodzio et al. 2002.

3. Pajzsmirigykezelés jód-131 alkalmazásával

- A gége előtt, kétoldalon pozicionáló pajzsmirigy a szervezet legnagyobb belső elválasztású mirigye. A pajzsmirigy révén termelt hormon, a thyroxin befolyásolja az anyagcserét és az energiafelhasználást. A pajzsmirigy hormontermeléséért az agyalapi mirigyből eredő TSH[20] felel.[21]
- A pajzsmirigy rendellenes működés esetében alulműködhet, illetőleg túlműködhet. A TSH hiánya esetén pajzsmirigy alulműködés alakulhat ki, amely különböző panaszokat idézhet elő, mint a fáradékonyság, a székrekedés, a hízás, a depresszió, de okozhatja a magzat nem megfelelő fejlődését is. Pajzsmirigy túlműködést sugallhat a foltokban történő hajhullás, az alvásminőség romlása, a szapora szívverés, a testtömeg hirtelen emelkedése vagy redukálódása, az izmok gyengeségének jelentkezése, a légzési nehézség vagy a kezek remegése is.[22] A pajzsmirigy alulműködése gyógyszerekkel, műtéttel, illetve radiojóddal[23] kezelhető. Abban az esetben, ha gyógyszerrel történő kezelés nem hoz eredményeket másfél év elteltével, illetve, ha nem áll fenn az alkalmazást kizáró ok, akkor a radiojóddal történő kezelés javasolt, mivel az ismételt gyógyszeres kezelés sikerességére csupán 25% esély áll fenn. A radiojódos kezelés célja a pajzsmirigy működési zavarának, valamint a pajzsmirigy mérete fokozódásának megszüntetése, továbbá a mirigy méretének redukálása.

A 2. ábrán a jód-131 radioaktív izotóp jellemzése látható.



2. ábra: Jód-131 radioaktív izotóp jellemzése
Forrás: a szerzők szerkesztése az International Atomic Energy Agency 2009b. alapján

[20] Thyreoid stimuláló, pajzsmirigyserkentő hormon.
[21] Melish 1990.
[22] Babai 2017.
[23] Radiojód: a nukleáris medicinában a jód-131 radioaktív izotóp rövid elnevezése.

4. Fájdalomcsillapítás izotópokkal

Fájdalomcsillapítás céljából ugyancsak felhasználják a radioaktív izotópokat, abban az esetben, ha a rosszindulatú daganatos megbetegedés előidézte csontfájdalmak már másfajta módszerrel nem enyhíthetők, még bódító hatású fájdalomcsillapítókkal sem. Ez esetben a béta-sugárzó ittrium-90, illetőleg a szamárium-153 izotópokat alkalmazzák. Pozitív tulajdonsága e fájdalomcsillapító eljárásmódnak, hogy csekélyebb mennyiségű mellékhatással jár, szemben egy bódító hatású fájdalomcsillapítóval, mindemellett, ha jelentkezik valamiféle mellékhatás, az hamarabb szűnik meg. Az izotópos fájdalomcsillapítással párhuzamosan továbbra is alkalmazhatóak az azt megelőzően szedett fájdalomcsillapítók. A kezelés több alkalommal ismételhető, 2-3 havonta, abban az esetben, ha az előző eljárás hatásosan csillapította a fájdalmat. A csontfájdalmakat a megnövekedett csontképződés idézi elő. Az eljárás alkalmával a radioizotópos szer a fokozott csontképződés helyén koncentrálódik. A kezelés – a szerzők véleménye szerint – azért megfelelőbb, mint a bódító hatású gyógyszerekkel való csillapítás, mert ott enyhíti a fájdalmakat, ahol a legszükségesebb, valamint csekélyebb eséllyel alakulhat ki a gyógyszerfüggőség.

4.1. Izotópos ízületi kezelés

Az emberek nagyjából három százalékát érinti a hosszú ideig fennálló ízületi gyulladás. Az érintetteknél leggyakrabban a térd ízületében jelentkezik fájdalommal járó, akár rokkantsághoz vezető gyulladásos állapot.[24]

A betegség okán sűrűn roncsolódik a porcszövet, ami az ínszalagok szakadását, károsodását is eredményezheti. Az ízület gyulladásos megbetegedésének fő jellemzője a fokozott ízületi folyadéktermelés. 1952 óta számtalan esetben alkalmazták műtéti beavatkozásokat elkerülve a radioaktív izotópos ízületi kezelést.[25] A kezelés alkalmával a beteg ízületburjánzását béta-sugárzás segítségével megfékezik. A radioaktív szert fecskendő segítségével juttatják be az ízület közelébe, amely rövid felezési idejének okán kis idő elteltével nem kimutatható a szervezetben. Az alkalmazás után jelentkezhetnek olyan mellékhatások ideiglenesen, mint az ízület gyulladása és felmelegedése. A beavatkozást előnyössé teszi, hogy nem jár olyan nagyságrendű fájdalommal, mint egy műtéti beavatkozás, azonban az alkalmazás sikerességének aránya elismerésre méltó. A kezeltek döntő többsége a kezelés sikerességét igazolja, fájdalmak csökkenéséről és jobb életminőségről számol be.

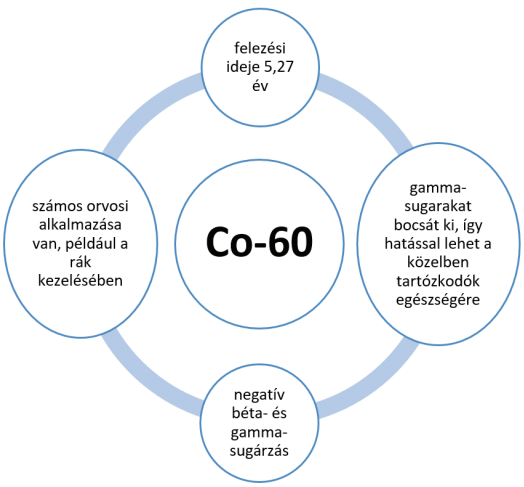
4.2. Daganatok gyógyítása

A daganatok kialakulására való hajlam lehet örökletes, azonban annak jelentkezéséhez nagyban hozzájárulhatunk rossz életmódunkkal is.[26] A környezeti hatások,

[24] Wallace et al. 2017.
[25] Szentesi et al. é. n.
[26] Varga 2012. 133.

az életmódból adódó gyakori stressz és az életkor, valamint az egyén más betegségei is rizikófaktort jelentenek.[27] Manapság az időben feltárt és kezelt betegségek körülbelül 60%-a meggyógyítható. A daganatok elpusztítására irányuló legkorábban alkalmazott és bevált gyógyászati módszer a műtéti beavatkozás. Ennek hátránya az esetlegesen felmerülő szövethiány, ez okból kifolyólag az orvostudomány fejlődésével fellendült a konzervatív, szerv- és szövetmegtartó gyógyító eljárások alkalmazása.

A kobalt-60 radioaktív izotópot jelen cikkünk csak érintőleg említi, de indokolt rövid bemutatása, ábra segítségével. A 3. ábrán a kobalt-60 radioaktív izotópot jellemeztük.



3. ábra: Kobalt-60 radioaktív izotóp jellemzése
Forrás: a szerzők szerkesztése az International Atomic Energy Agency 1990. alapján

Ezen eljárásokkal hasonló minőségű eredmények érhetőek el mindamellett, hogy a betegek életminősége nem romlik annyira, mint egy műtétet követően.[28] Rosszindulatú megbetegedések kezelése alkalmával az esetek nagyjából 50-60%-ában javasolt sugárkezelés is. A külső sugárterápia esetében kobaltágyúval külsőleg, gamma-sugárzással kezelik a szövetet. A kezelés eredményének érdekében kialakítanak olyan biztonsági zónákat, amelyek kis méretű és jól körülírt daganatoknál három-öt milliméteresek, nagy méretű daganatoknál pedig öt-tíz milliméteresek. A kezelés során az ép állapotban lévő szöveteket három-négy milliméter vastagságú ólommaszkkal árnyékolják.[29] A közelbesugárzás, avagy brachyterápia[30] alkalmával a beteget a szövet közti terébe, esetlegesen a testüregébe zárt sugárforrást juttatva gyógyítják. Belső sugárterápiás kezeléseknél gamma- és béta-sugárzó izotópot használnak, illetőleg neutronforrásokat. A közelbesugárzás során az egyike a leggyakrabban felhasznált béta-sugárzó izotópoknak a stroncium-90, gamma-sugárzó izotópok közül pedig

[27] World Health Organization 2020.
[28] Rosenblatt–Zubizarreta 2017.
[29] Kovács 2014. 464.
[30] A brachyterápia a sugárkezelés egyik típusa. A kezelés során eszközök közvetítésével radioaktív sugárforrást juttatnak a daganatba, vagy annak közelébe, ez végzi el a daganat roncsolását. Gyakran alkalmazott radioaktív izotópok: irídium-192, jód-125.

az irídium-192. A sugárforrást lehet ideiglenesen, implantátumként alkalmazni, ebben az esetben a tervezett dózis elérésével a betegből eltávolítják a sugárforrást, illetőleg léteznek állandó implantátumok, amelyeket nem távolítanak el. Ez utóbbi sugárforrásoknak sokkal rövidebb a felezési idejük.[31]

Előzőleg a jód-131 radioaktív izotópot is bemutattuk, ezért a jód egy másik izotópjának fontos alkalmazását foglaltuk össze a 4. ábrán, hangsúlyozva a jód radioaktív izotópjainak gyakorlati jelentőségét.

4. ábra: Jód-125 radioaktív izotóp jellemzése
Forrás: a szerzők szerkesztése az International Atomic Energy Agency 2006. alapján

5. A radioaktivitás veszélyei

A Föld lakosságának sugárterhelése 32%-ban mesterséges eredetű, 68%-ban pedig természetes eredetű sugárzásokból áll össze. Mesterséges eredetű források azok, amelyeket az ember hozott létre, ilyen például a röntgencső és az atomreaktor.[32] Természetes eredetű sugárforrás az űr és a földkéreg.[33] A radioaktív sugárzások okozzák leggyakrabban a sejtek örökítőanyagának károsodását. A nagyobb dózisban kapott radioaktív sugárzás a sejtek jelentős mértékű károsodását idézheti elő, amelynek hatása rövid idő elteltével jelentkezhet, akár halálos végkimenetelű is lehet napokon belül. Az ionizáló sugárzások késői hatásai évekkel később is felléphetnek, akár az utódoknál is, ilyen következmény lehet például a daganatok jelentkezése. Az ionizáló sugárzás használatbavételét igénylő munkafolyamatokat ellátó munkavállalók veszélyeztetettek a késői és a korai hatások tekintetében is. Determinisztikus hatások elsősorban

[31] Pesznyák–Sáfrány 2017.
[32] Országos Atomenergia Hivatal 2019.
[33] Országos Atomenergia Hivatal 2019.

egy-egy baleset bekövetkezése esetében alakulhatnak ki. A sztochasztikus hatás kialakulása függ a kapott dózistól, az időtartamtól, mindemellett a gyakoriságtól is.[34] Az ionizáló sugárzások bármilyen daganat jelentkezését előidézhetik, azonban léteznek olyan szövetek, amelyek az átlagosnál is érzékenyebbek a sugárzásokra. A felnőttek génállománya teherbíróbb, mint a gyermekeké, a fiatal korosztály hajlamosabb a sugárzásból eredő génmutációra, ezen okból kiindulva fontos izotópos kezeléseket követően a megfelelő és előírt távolságot megtartani a kisgyermekektől, a várandós nőktől és a kisgyermekeket szoptató édesanyáktól. A radioaktív sugárzás a fiatalok esetében gyakran vérképzési rendellenességet, leukémiát idéz elő.[35]

- A külső sugárterhelés elleni védelem többféle módszerrel megvalósítható, ilyen például a sugárforrástól való távolságtartás, a közelben tartózkodás időtartamának csökkentése és az árnyékolás. A belső sugárterhelés ellen védekezhetünk különféle védőöltözetekkel, valamint kisebb aktivitású nyílt sugárforrások esetében elkerülhető, amennyiben kellően ügyelünk rá, hogy szervezetünkbe ne kerüljön be. A már szervezetbe bejutott radioaktív izotóp károsító hatása minimalizálható azzal, ha ugyanazon kémiai elem stabil izotópjainak egyikét a szervezetbe juttatjuk, hígítva ezzel instabil izotópját.[36]

Olyan munkavállalók esetében, akik radioaktív források felhasználásával végzik munkatevékenységüket, elengedhetetlen, hogy a Munkahelyi Sugárvédelmi Szabályzatban rögzítetteket betartsák, valamint, hogy az előírt védőeszközöket alkalmazzák. A pajzsmirigy vizsgálatáról, gyógyításáról már volt szó az előzőekben, ezért ismertetjük a jód-123 radioaktív izotópot az 5. ábrán.

5. ábra: Jód-123 radioaktív izotóp jellemzése
Forrás: a szerzők szerkesztése az International Atomic Energy Agency 2009c. alapján

[34] Pátzay–Dobor 2016.
[35] Országos Atomenergia Hivatal 2019.
[36] Lásd: http://atomfizika.elte.hu/kornyfizlab/docs/ADM/index.html

Veszély esetén a lakosság a leghatékonyabban úgy tud védekezni a radioaktív sugárzások ellen a védekezésre rendelt erők megérkezéséig, ha minél hamarabb zárt és védett helyre vonul, valamint védőeszközöket alkalmaz. Elengedhetetlen az utasítások fegyelmezett betartása. Olyan, levegőben szálló radioaktív szennyeződések, mint a por, ellen védelmet jelenthet, ha a nyílászárókat eltömítik. A légzés időleges védelmét nyújthatja az arc többrétegű, vizes textíliákkal való fedése.[37]

6. Összegzés

Napjainkban az ipari alkalmazások után az egészségügyben használják a legtöbbször a radioaktív izotópokat. Az izotópok felhasználásának fontos szerepe van a képalkotó diagnosztikában, felhasználásuk hiányában az emberiséget érintő megbetegedések bizonyos számát csak a betegség előrehaladott állapotában lehetne kimutatni. Az izotópdiagnosztikai eljárások rengeteg rendellenesség és betegség korai diagnosztizálását teszik elérhetővé, mindemellett segítséget nyújtanak a terápiák pontos kialakításában is. Képalkotó vizsgálatok alkalmával radioaktív izotópot juttatnak a szervezetbe, amelyek anélkül vesznek részt a szervezetben lezajló folyamatokban, hogy azokat befolyásolnák. A radioaktív nyomjelző anyagokból kibocsátott sugárzás alapján lehet képet kapni speciális műszerek használatával az anyagok szervezetben való eloszlásáról, dúsulásáról, illetve kiürüléséről. A betegségek felismerése azok korai szakaszában elősegíti a gyógyulást. A rosszindulatú megbetegedések gyógyítása során napjainkban szükséges a radioaktív izotópok alkalmazása. Régen ezeket a betegségeket kockázatos műtétekkel gyógyították, amelyek számos esetben az életminőség romlását idézték elő. Az izotópok egészségügyi alkalmazása elősegíti, hogy a társadalom tagjai korszerű egészségügyi ellátásban részesüljenek. A csontáttétes daganatok gyógyítására is alkalmazhatóak az instabil izotópok, valamint a csontfájdalmak eredményes csillapítására is. A radionuklid-terápia alatt olyan szereket juttatnak az emberi szervezetbe, amelyek a daganatos szövetben megkötődnek, majd a kibocsátott radioaktív sugárzás célzott sejtpusztulást eredményez.[38] A radioaktív izotópok veszélyt jelenthetnek, de az előírások létrehozása, majd azok betartása által a kockázatok csökkenését értük el. Megfelelő és biztonságos megközelítéssel a radioaktív izotópok felhasználására szükség van.

A kutatások szerint több mint 3000 radioaktív izotóp ismeretes, és időben előre haladva a technológiai fejlettségi útvonalon egyre több alkalmazható a mindennapokban.

Felhasznált irodalom

Babai László (2017): *Pajzsmirigy.* Online: www.endokrinkozpont.hu/pajzsmirigy

Csinády Virág (2018): *Csontszcintigráfia szerepe a malignus tumorok staging és restaging vizsgálataiban.* Online: http://midra.uni-miskolc.hu/document/28804/24591.pdf

[37] Domokos 2011.
[38] Környei–Mikecz 2012.

Domokos Endre szerk. (2011): *Környezetmérnöki Tudástár.* 14. kötet. Sugárvédelem. Veszprém, Pannon Egyetem Környezetmérnöki Intézet. Online: https://tudastar.mk.uni-pannon.hu/anyagok/14-sugvedelem.pdf

Györke Tamás (é. n.): *Nukleáris Medicina.* Online: http://oftankonyv.reak.bme.hu/tiki-index.php?page=Nukle%C3%A1ris+medicina&structure=Orvosi_Gradu%C3%A1lis&no_bl=y

Halama, James R. – Chair, Daryl Graham – Harkness, Beth A. – Kappadath, S. Cheenu – Madsen, Mark T. – Massoth, Richard J. – Patton, James A. – White, Sharon L. – Williams, Lawrence E. – Wooten, Wesley W. (2019): *Acceptance Testing and Annual Physics Survey Recommendations for Gamma Camera, SPECT, and SPECT/CT Systems*. The Report of AAPM Task Group 177. Alexandria, American Association of Physicists in Medicine. Online: https://doi.org/10.37206/184

International Atomic Energy Agency (é. n.): *Radioisotopes.* Online: www.iaea.org/topics/nuclear-science/isotopes/radioisotopes

International Atomic Energy Agency (1990): *Guidelines for Industrial Radiation Sterilization Of Disposable Medical Products (Cobalt-60 Gamma Irradiation).* Vienna.

International Atomic Energy Agency (2006): *Production Techniques and Quality Control of Sealed Radioactive Sources of Palladium-103, Iodine-125, Iridium-192 and Ytterbium-169*. Vienna, (2006. június). Online: https://inis.iaea.org/collection/NCLCollectionStore/_Public/37/078/37078974.pdf?r=1&r=1

International Atomic Energy Agency (2009a): *Technetium-99m Radiopharmaceuticals: Status and Trends.* Vienna. Online: https://www-pub.iaea.org/MTCD/Publications/PDF/Pub1405_web.pdf

International Atomic Energy Agency (2009b): *Nuclear Medicine in Thyroid Cancer Management: A Practical Approach*. Vienna. Online: https://www-pub.iaea.org/MTCD/publications/PDF/te_1608_web.pdf

International Atomic Energy Agency (2009c): *Cyclotron Produced Radionuclides: Physical Characteristics and Production Methods.* Technical Reports Series No. 468. Vienna Online: https://www-pub.iaea.org/mtcd/publications/pdf/trs468_web.pdf

Jodzio, Krzysztof – Lass, Piotr – Nyka, Walenty – Gasecki, Dariusz – Bandurski, Tomasz – Scheffler, Justyna (2002): Cerebral Blood Flow Spect Imaging in Right Hemisphere-Damaged Patients With Hemispatial Neglect. A Pilot Study. *Nuclear Medicine Review – Central & Eastern Europe,* 5. évf. 1. sz. 49–51.

Kovács Árpád szerk. (2014): *Sugárterápia.* Budapest, Medicina Könyvkiadó Zrt. Online: http://tamop.etk.pte.hu/tamop412A/tananyag/sugarterapia/sugarterapia.pdf

Környei József – Mikecz Pál (2012): Radiokémia a gyógyítás szolgálatában. *Magyar Tudomány,* 173. évf. 2. sz. 141–145. Online: http://epa.oszk.hu/00600/00691/00098/pdf/mtud_2012_02_0141-0145.pdf

Melish, John S. (1990): Thyroid Disease. In Walker, H. K. – Hall, W. D. – Hurst, J. W. szerk.: *Clinical Methods: The History, Physical, and Laboratory Examinations.* 3rd edition. Boston, Butterworths; Chapter 135. Online: www.ncbi.nlm.nih.gov/books/NBK241/

Országos Atomenergia Hivatal (2019): *SV-18. sz. útmutató. Bővített fokozatú sugárvédelmi képzéseken és továbbképzéseken oktatandó témakörök.* Budapest, (2019. novem-

ber). Online: www.haea.gov.hu/web/v3/OAHPortal.nsf/BEA98D0C319A3C51C-1257F41003303E7/$File/SV_18_1.0.pdf
Pátzay György – Dobor József (2016): Ipari tevékenységekből eredő veszélyforrások és elhárításuk. Budapest, NKE Katasztrófavédelmi Intézet. Online: https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/10285
Pesznyák Csilla – Sáfrány Géza szerk. (2017): *Sugárbiológia*. Budapest, Typotex eKiadó.
Rosenblatt, Eduardo – Zubizarreta, Eduardo szerk. (2017): *Radiotherapy in Cancer Care: Facing the Global Challenge*. Vienna, International Atomic Energy Agency.
Srivastava, Mukesh – Gaikwad, Rajiv – Samad, A. – Sharma, Barkha – Srivastava, Ashish (2012): Diagnosis of Nephritis by Analysis of 99 Mtc-Dtpa Renal Scintigram Curve in a Dog. *Veterinary Practitioner,* 13. évf. 1. sz. 80–81. Online: www.researchgate.net/publication/289388237_Diagnosis_of_nephritis_by_analysis_of_99_MTC-DTPA_renal_scintigram_curve_in_a_dog
Szentesi Margit – Rajtár Mária – Géher Pál – Pellet Sándor – Balogh Ildikó (é. n.): Radiosynoviorthesis-módszertani útmutató (radiosynovectomia). Krónikus synovitisek kezelése beta sugárzó izotóppal. Online: www.nmc.dote.hu/nmszk/NMSZK_modszertan/10_7_radiosynovior.pdf
Taylor, Andrew T. – Brandon, David C. – de Palma, Diego – Blaufox, M. Donald – Durand, Emmanuel – Erbas, Belkis – Grant, Sandra F. – Hilson, Andrew J. W. – Morsing, Anni (2018): SNMMI Procedure Standard/EANM Practice Guideline for Diuretic Renal Scintigraphy in Adults With Suspected Upper Urinary Tract Obstruction 1.0. *Seminars in Nuclear Medicine,* 48. évf. 4. sz. 377–390. Online: https://doi.org/10.1053/j.semnuclmed.2018.02.010
Varga Gábor (2012): *Daganatok kórélettana*. Online: https://semmelweis.hu/oralbiologia/files/2012/12/12-Daganatok-Varga.pdf
Varga József szerk. (2002): *Nukleáris Medicina Tankönyv. 1977–2002.* Debreceni Egyetem Nukleáris Medicina Tanszék. Online: www.nmc.dote.hu/nmtk/index.html
Wallace, Ian J. – Worthington, Steven – Felson, David T. – Jurmain, Robert D. – Wren, Kimberly T. – Maijanen, Heli – Woods, Robert J. – Lieberman, Daniel E. (2017): Knee Osteoarthritis Has Doubled in Prevalence Since the Mid-20th Century. *PNAS,* 114. évf. 35. sz. 9332–9336. Online: https://doi.org/10.1073/pnas.1703856114
World Health Organization (2020): *Report on Cancer: Setting Priorities, Investing Wisely and Providing Care for All.* Geneva, (2020. február 3.). Online: www.who.int/publications/i/item/9789240001299

HADMÉRNÖK
VÉDELEMINFORMATIKA

17. évfolyam (2022) 4. szám 113–129.
DOI: 10.32567/hm.2022.4.8

Bihaly Barbara[1]

A felhőalapú szolgáltatások alkalmazása az amerikai haderőben, különös tekintettel a U.S. Army stratégiájára

The Use of Cloud-Based Services in the U.S. Military, Particularly in the Strategy of the U.S. Army

A rohamos technológiai fejlődésnek hála a kormányzati és a védelmi szerveknek is ideje modernizálni rendszereit. Ennek egyik lépése a felhőalapú szolgáltatások lehetőségeinek kiaknázása a kormányzati és rendvédelmi szférában. A cikk célja bemutatni a U.S. Army által kiadott két stratégiát a felhőalapú szolgáltatások alkalmazásáról.

Kulcsszavak: **felhőalapú szolgáltatások, Egyesült Államok, U.S. Army**

Thanks to rapid technological development, it is time for both government and defence agencies to modernise their systems. One step in this is to take advantage of the potential of cloud-based services in government and law enforcement. The purpose of this article is to present two strategies issued by the U.S. Army on the use of cloud-based services.

Keywords: **cloud computing, United States, U.S. Army**

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

1. Bevezetés

Az elmúlt évtizedekben rohamos technológiai fejlődésnek lehettünk tanúi, amellyel egyidejűleg exponenciálisan megnőtt a társadalom függősége az infokommunikációs rendszerektől. Ezek az új technológiák felgyorsítják a folyamatokat, költséghatékonyak és egyre szélesebb körben elérhetőek. Ugyanakkor megnőtt a biztonság iránti igény is, ez pedig felveti az egyes technológiák biztonságosságának és alkalmazhatóságának kérdéseit

Napjaink egyik kiemelkedő technológiai trendje a felhőalapú rendszerek térnyerése a piacon. A Microsoft jelentései már 2016-ban és 2017-ben is, a negyedéves eredménybeszámolókban rendre a felhőszolgáltatást emelték ki mint meghatározó húzóágazatot.[2]

A fő kérdés a felhőalapú rendszerekkel kapcsolatban, hogy mennyire biztonságosak és mennyire ellenőrizhetők? Elsődleges, hogy a megfelelő biztonság garantálható legyen a felhasználónak. Másrészről a hatóságoknak és védelmi szerveknek meg kell győződniük arról, hogy az adott rendszer megfelelőséget mutat az egyes, meghatározott biztonsági követelményeknek, ugyanakkor tisztában kell lennünk a fennmaradó biztonsági kockázatokkal is.[3]

Abban az esetben, ha ilyen új típusú rendszereket szeretnénk integrálni a meglévő (hon)védelmi rendszerekbe, akkor felvetődik a törvényes ellenőrzés problematikája is. Az informatikai rendszerekkel kapcsolatos biztonsági követelmény legpontosabb megfogalmazása a CIA- (*confidentiality* – bizalmasság, *integrity* – sértetlenség, *availability* – rendelkezésre állás) alapelv.[4]

Viszont, a rendkívül gyors ütemű technológiai fejlődéssel együtt jár az is, hogy a védelmi szféra, a haderők sem kerülhetik el a felhőalapú szolgáltatások alkalmazását.

A 2000-es években a világ egyik vezető hadereje, az amerikai haderő is felfedezte a felhőalapú szolgáltatásokban rejlő lehetőségeket. Egy 2016-ban kezdődő pilotprogrammal – hibrid felhőkörnyezettel – kezdték meg a felhőalapú rendszerek integrálását a könnyebb információmegosztás érdekében. Ez a hibrid felhőkörnyezet magában foglalta a helyszíni Védelmi Minisztériumi (Department of Defence, DoD) felhőkörnyezetek kombinációját, például a DoD-létesítményben elhelyezett milCloudot, valamint a kereskedelmi felhőszolgáltatókat és a nem helyszíni szövetségi felhőkörnyezeteket, például azokat, amelyeket más szövetségi ügynökségek üzemeltetnek.[5]

Habár a felhőalapú rendszereknek sok előnye van, felmerül, hogy milyen keretekben használhatók katonai célokra, és mennyi kockázatot rejtenek magukban, illetve kielégítik-e a CIA-alapelvet?

E felvetések okán jelen cikk célja bemutatni, milyen tervei, törekvései és szabályzói vannak az amerikai haderőnek a felhőalapú szolgáltatások integrálására, vizsgálva a kormányzati felhőstratégiákat, a haderő szintű felhőstratégiákat és a U.S. Army speciális terveit.

[2] Clarke 2016; Clarke 2017.
[3] Kovács 2021.
[4] Lásd: www.itbiztonsag.siteset.hu/index.php?m=996
[5] Vergun 2016.

2. Felhőalapú szolgáltatások katonai alkalmazásának alapjai

Korunk egyik legvitatottabb és legdivatosabb technológiai fejlesztése a felhőrendszer. A felhőalapú rendszerek lényege, hogy nem a saját IT-infrastruktúránkon található adatokkal, szoftverekkel vagy platformokon dolgozunk, hanem „valahol az interneten",[6] ugyanis a konkrét infrastruktúra helye a felhasználó számára többnyire nem, vagy nem pontosan ismert. A konkrét infrastruktúra akár országhatáron kívül is eshet, ha például külföldi szolgáltatót veszünk igénybe. Ez az országhatáron kívüliség további biztonsági kérdéseket vet fel, ha azt szeretnénk elérni, hogy egy rendvédelmi vagy nemzetbiztonsági szerv munkáját ültethessük át (részlegesen) felhőalapú rendszerekbe.

2.1. Felhőalapú rendszerek, szolgáltatások fogalma, típusai

Felhőalapú szolgáltatás lehet tárhely (például iCloud), szoftver (például Microsoft Office 365) vagy platform/infrastruktúra is (például Oracle Cloud Infrastructure). A NIST (National Institute of Standards and Technology, Nemzeti Szabványügyi és Technológiai Intézet) Információtechnológiai Laboratóriuma (Information Technology Laboratory) a következőképp rendszerezte a felhőalapú szolgáltatásokat tulajdonságaik alapján:

- igény szerinti önkiszolgálás *(on-demand self service);*
- jó hálózati hozzáférés *(broad network access);*
- teljes rugalmasság *(rapid elasticity);*
- mért szolgáltatások *(measured service).*[7]

Hasonló keretrendszert használ a Német Szövetségi Információbiztonsági Hivatal (Bundesamtes für Sicherheit in der Informationstechnik, BSI) is.[8] De léteznek olyan további kérdéses tulajdonságok is, mint például a rendelkezésre állás, a kiszolgálás gyorsasága, a megbízhatóság, a skálázhatóság, a teljesítmény, a biztonság, a karbantartás, a költség stb. Ezek alapján a felhasználó a saját igényeire és prioritásaira szabott szolgáltatást tud választani. Kovács azonban munkájában felhívja a figyelmet arra is, hogy a felhőalapú rendszerek csoportosításához szükség van a szolgáltatási és telepítési kategóriák ismeretére is, előnyeikkel, hátrányaikkal együtt.[9]

A szolgáltatási modellek lehetnek: szoftver mint szolgáltatás (*software as a service,* SaaS), platform mint szolgáltatás (*platform as a service,* PaaS) és infrastruktúra mint szolgáltatás (*infrastructure as a service,* IaaS). Ezeket a modelleket már többféleképpen próbálták kiegészíteni, továbbá megjelentek már a *desktop as a service* (DaaS) és PRaaS *(process as a service)* megoldások is.[10]

[6] Kovács 2021. 15.
[7] Lepenye 2011.
[8] Security Recommendations for Cloud Computing Providers (Minimum information security requirements) White Paper. 2011.
[9] Kovács 2021. 19.
[10] Kusnetzky 2009.

Telepítési modellek lehetnek: magán számítási felhő *(private cloud)*, közösségi számítási felhő *(community cloud)*, nyilvános számítási felhő *(public cloud),* hibrid számítási felhő *(hybrid cloud)*.

A felhasználó e modellek mátrixa alapján tudja igényeinek megfelelően kiválasztani, hogy milyen szolgáltatásra lenne szüksége.

2.2. Kormányzati felhőrendszerek

Az általános, technikai modellek mellett célja szerint beszélhetünk kormányzati *(gov-cloud)* és katonai *(mil-cloud)* felhőalapú rendszerekről.

Az Európai Hálózat- és Információbiztonsági Ügynökség (ENISA) a *Good Practice Guide for Securely Deploying Governmental Clouds* (Jó gyakorlati útmutató a kormányzati felhők biztonságos telepítéséhez)[11] című, 2013-ban kiadott dokumentumban megkísérli definiálni a gov-cloud-ot. A szakértők alapul vették a NIST által meghatározottakat, és kiemeltek három megoldást a gov-cloud-ra, mégpedig: a nyilvános számítási felhő, a magán számítási felhő és a közösségi számítási felhő.

A gov-cloudra általános definíció még nincs, de több szempontot is figyelembe vevő meghatározások már az ENISA említett dokumentumában is léteznek:

- „A gov-Cloud egy olyan környezet, ahol a futó szolgáltatások megfelelnek a kormányzati és EU szabályozásoknak az információbiztonság és az ellenálló képesség terén (ez a mi kérdésre ad választ).
- A gov-Cloud a közintézmények, kormányzatok által működtetett szolgáltatások futtatásának (magán vagy nyilvános felhőben) egy biztonságos és megbízható módja (ez a hogyan kérdésre ad választ).
- A gov-Cloud egy telepítési modell, amelyet arra építettek, hogy szolgáltatásokat nyújtsanak állami szervek (belső szolgáltatások nyújtása), polgárok és vállalkozások (külső szolgáltatások nyújtása a társadalom) számára (ez a kinek kérdésre ad választ)."[12]

A Technopedia meghatározása szerint,[13] az Egyesült Államokbeli szabályozások alapján, a gov-cloud megnevezés az összes felhőalapú számítástechnikai és virtualizációs termékre és megoldásra vonatkozik, amelyeket kifejezetten kormányzati szervezetek és intézmények számára fejlesztettek ki. A Gov-Cloud föderális kezdeményezés olyan felhőmegoldások kezelésére és tervezésére, amelyek megfelelnek az IT-szükségleteknek, valamint a szövetségi kormány stratégiai, pénzügyi és működési céljainak.

A Gov-Cloud program az Egyesült Államokban megkönnyíti a felhőalapú számítástechnikai megoldások megvalósítását formális szabványok és eljárások szerint, kiemelt hangsúlyt fektetve a biztonságra és az interoperabilitásra. Számos iránymutatást tettek közzé e program keretében, mint például a Federal Cloud Computing

[11] *Good Practice Guide for Securely Deploying Governmental Clouds.* 2013.
[12] *Good Practice Guide for Securely Deploying Governmental Clouds.* 2013.
[13] Lásd: www.techopedia.com/definition/28218/govcloud

Strategy,[14] a Federal CIO 25-Point Roadmap[15] terve és a NIST Cloud Computing Technology Roadmap.[16] Mindezek mellett, a GovCloudot olyan privát felhőszolgáltató, mint például az Amazon AWS is, márkatermékként kínálja.

A 2010-es évekre felismerték, hogy a szövetségi kormány információs technológiai (IT-) környezetét az alacsony eszközkihasználás, az erőforrások iránti töredezett kereslet, a duplikált rendszerek, a nehezen kezelhető környezetek és a hosszú beszerzési határidők jellemzik. Ezek a hiányosságok negatívan befolyásolják a szövetségi kormány azon képességét, hogy kiszolgálja az amerikai közvéleményt. A felhőalapú számítástechnika jelentős szerepet játszhat e hiányosságok kezelésében és a kormányzati szolgáltatások javításában. A számítási felhő modell jelentősen segítheti azokat az ügynökségeket, amelyek erőforráshiánnyal küzdenek. Tehát, a szövetségi kormány számára a felhőalapú számítástechnika óriási lehetőségeket rejt magában azáltal, hogy növeli a működési hatékonyságot és gyorsabban reagál a szükségletekre.

A fentieket alátámasztják a Federal Cloud Computing Strategy-ben megfogalmazott alábbi célitűzések is:

- a felhőalapú számítástechnika előnyeinek, szempontjainak és kompromisszumainak megfogalmazása;
- adjon döntési keretet és esetpéldákat, hogy támogassa az ügynökségeket a felhőalapú számítástechnikára való átállásban;
- a számítási felhő megvalósítási erőforrásainak kiemelése;
- határozza meg a szövetségi kormány tevékenységeit, szerepköreit és felelősségeit a felhő bevezetésének katalizálásával kapcsolatban.[17]

Ez a stratégia megfogalmazza azt is, hogy a digitalizálódó világban a kormány felelőssége az, hogy élen járjon az innovatív szolgáltatások amerikai néphez való eljuttatásában. Tekintettel arra, hogy minden ügynökség egyedi küldetési szükségletekkel, biztonsági követelményekkel és informatikai környezettel rendelkezik, a stratégia felszólítja az ügynökségeket, hogy a stratégia alapján dolgozzanak ki saját cselekvési tervet és beszerzési stratégiát összhangban a Cloud First Irányelvvel *(Cloud First Policy)*.[18]

A CIO 25-Point Roadmap egy 2010-ben kidolgozott cselekvési terv, amely bár nem oldotta meg az összes szövetségi informatikai kihívást, a legsürgetőbb, állandó kihívások közül sokra nyújtott megoldást. A CIO 25-Point Roadmap inkább a végrehajtásra összpontosított.

A szintén 2011-es NIST Cloud Computing programhoz szorosan kapcsolódik az USG Cloud Computing Technology Roadmap és az Egyesült Államok kormányának USG Cloud Computing Technology Roadmap dokumentuma 500-293. sz. speciális kiadványának első kiadása két kötetből áll. A NIST Cloud Computing program stratégiájával összhangban az ütemterv a felhőalapú számítástechnikával kapcsolatos stratégiai és műveleti célokra összpontosít.

[14] Kundra 2011.
[15] Kundra 2010.
[16] Hogan et al. 2011.
[17] Kundra 2011. 2.
[18] Kundra 2011. 33.

Az I. kötet, *Az USG felhőalapú számítástechnika további bevezetésének kiemelt követelményei,* keretet ad a vitának, és bemutatja az ütemtervet azon összefoglaló stratégiai követelmények tekintetében, amelyeknek az USG ügynökségei számára teljesíteniük kell a felhőalapú számítástechnika további bevezetéséhez. Az ütemterv stratégiai elemei „kiemelt prioritású műszaki területként" jellemezhetők, amelyek rövid és hosszú távon egyaránt lehetővé teszik a számítási felhőt.

A II. kötet tájékoztatást nyújt azoknak, akik aktívan dolgoznak a stratégiai és műveleti számítási felhőkezdeményezéseken, beleértve, de nem kizárólagosan, a kormányzati-felhő-használókat. Ez a kötet összefoglalja a 2010 novembere és 2011 szeptembere között a NIST Cloud Computing program és az USG Cloud Computing Technology ütemtervének kidolgozására irányuló közös erőfeszítések révén végzett munkát.[19]

A NIST-program megfogalmaz továbbá bizonyos standardokat az interoperabilitás, a mobilitás és a biztonság területein is a felhőalapú rendszerekkel kapcsolatban. A felhőalapú számítástechnika megvalósításának fő biztonsági céljai a NIST-program alapján a következők:

- Védje az ügyfelek adatait a jogosulatlan hozzáféréstől, nyilvánosságra hozataltól, módosítástól vagy megfigyeléstől. Ez magában foglalja az identitáskezelés támogatását, hogy az ügyfél képes legyen identitás- és hozzáférés-szabályozási irányelveket érvényesíteni a felhőszolgáltatásokhoz hozzáférő jogosult felhasználókon.
- Véd az ellátási láncot érő lehetséges fenyegetésektől. Ez jelenti a szolgáltató megbízhatóságát, valamint a használt hardver és szoftver megbízhatóságának biztosítását.
- Akadályozza az illetéktelen hozzáférést a felhőalapú számítástechnikai infrastruktúra erőforrásaihoz. Tehát a biztonsági tartományok megvalósítása a cél, amely révén a logikai elemek elválasztásával rendelkeznek a számítási erőforrások fölött, ezáltal biztosítva az alapértelmezett konfigurációk használatát.
- Felhőben telepített webalkalmazások tervezése egy internetes fenyegetésmodellhez, és a biztonság beágyazása a szoftverfejlesztési folyamatba.
- Végfelhasználói biztonsági rések csökkentése az internetre csatlakoztatott személyi számítástechnikai eszközök védelmét szolgáló intézkedések megtétele, biztonsági szoftverek, személyi tűzfalak és javítások, karbantartás révén.
- Állapítson meg bizalmi határokat a szolgáltató(k) és a fogyasztók között azért, hogy a biztonságért való felelősség egyértelmű legyen.
- Támogatja a hordozhatóságot, hogy az ügyfél szükség esetén a rendelkezésre állási, bizalmassági és integritási követelmények teljesítése érdekében intézkedhessen a felhőszolgáltatók megváltoztatásáról. Ez magában foglalja a fiók bezárásának lehetőségét egy adott napon és időpontban, valamint az adatok átmásolását egyik szolgáltatótól a másikhoz.[20]

A már említett Cloud First Irányelv célja volt felgyorsítani a tempót, amellyel a szövetségi kormány felismerte a felhőalapú rendszerek használhatóságának értékét azáltal,

[19] Hogan et al. 2011. 11–13.
[20] Hogan et al. 2011.

hogy megkövetelte az ügynökségektől, hogy értékeljék a biztonságos felhőalapú számítástechnikai lehetőségeket, mielőtt bármilyen új befektetést eszközölnének.[21]

Magyarországtól eltérően, az Egyesült Államok Szövetségi Kormánya tradicionálisan szerződésben áll magánszolgáltatókkal, akik megfelelnek a sajátos követelményrendszereknek és kiszolgálják a különböző ügynökségeket. A felhőszolgáltatások szempontjából a fő központi szolgáltató az Amazon Web Services (AWS).

Az AWS GovCloud (USA) elszigetelt AWS-régiókból áll, amelyek lehetővé teszik az egyesült államokbeli kormányzati szervek és ügyfelek érzékeny adatainak áthelyezését a felhőbe azáltal, hogy megfelelnek sajátos szabályozási és megfelelőségi követelményeiknek, ideértve a Szövetségi Kockázat- és Engedélykezelési Programot (FedRAMP), a Védelmi Minisztérium biztonsági követelményeinek útmutatóját (DoD SRG) és a Criminal Justice Information Services (CJIS) követelményeit.[22] A szolgáltatás specifikusan az Egyesült Államok szövetségi, állami és helyi szintű kormányzati szervei, valamint a vállalkozók, az oktatási intézmények és más egyesült államokbeli ügyfelek igényeire lett fejlesztve. Például, 2013 óta a CIA is használja az AWS szolgáltatásait (több egyéb multinacionális entitás szolgáltatásai mellett).[23]

3. Az amerikai haderő tervei és elképzelései a felhőalapú szolgáltatások alkalmazására

A kormányzat mellett a haderő szereplői is felismerték, hogy a felhőalapú rendszerek hatékonyabbá tehetnek bizonyos munkafolyamatokat.

A 2012 júliusában kiadott U.S. DoD Cloud Computing Strategy[24] olyan megközelítést vezet be, amellyel a minisztérium a duplikált, nehézkes és költséges alkalmazássilók jelenlegi állapotából egy agilis, biztonságos és költséghatékony végállapotba kerül, egy hatékony szolgáltatási környezet által, amely gyorsan reagál a változó küldetési igényekre. A DoD-szintű központosított felhőre való átállásának megközelítése a következő négy lépésből áll a stratégia szerint:

1. a felhőalapú szolgáltatások katonai célokra való alkalmazásának előmozdítása;
2. az adatközpontok konszolidációjának optimalizálása;
3. a DoD Enterprise Cloud Infrastructure létrehozása és
4. Deliver Cloud Services – kereskedelmi szolgáltatók igénybevétele és a DoD felhőszolgáltatások fejlesztésének és megvalósításának folytatása.

A DoD Cloud Computing Strategy külön megvalósításokat és adatcseréket határoz meg a kevésbé biztonságosnak tekintett Internet Protokoll Router Network (NIPRNet), a Secure Internet Protocol Router Network (SIPRNet) és a Top Secret Sensitive Compartmented Information (TS SCI) biztonsági tartományokhoz.[25]

[21] Lohrmann 2010.
[22] *What is AWS GovCloud (US)?* é. n.
[23] Fedscoop 2020.
[24] Az Amerikai Egyesült Államok Védelmi Minisztériumának Felhőstratégiája. 2018.
[25] Magar 2014. 16.

3.1. Haderőszintű tervek, elképzelések

Haderőszinten két fontos terv született a felhőrendszereket illetően. Az első a Joint Enterprise Defense Infrastructure (JEDI), a második a JEDI-t váltó, Joint Warfighter Cloud Capability (JWCC) program volt.

Mivel a számítógép-hálózatok kritikus szerepet játszanak a modern harctéren, továbbá tekintettel kell lennünk arra, hogy az Egyesült Államok jelenlegi katonai doktrínája a jövőben több domainben is (azaz szárazföldön, tengeren, levegőben, kibertérben vagy az űrben) vívandó háborúkra is felkészül, ezek a hálózatok még fontosabbá válnak. Lehetővé teszik az egységek számára a kommunikációt, az adatok feldolgozását, az információk megosztását és az erőfeszítések szinkronizálását ezekben a műveleti tartományokban. Az elmúlt, nagyjából két évtizedben a hagyományosabb számítógépes hálózatok helyét átvették a felhőalapú rendszerek. Ennek megfelelően az Egyesült Államok Védelmi Minisztériuma (DoD) 2019-ben szerződést kötött a Microsofttal a JEDI fejlesztésére, hogy ezeket a felhőképességeket eljuttassa a harcosokhoz.

A JEDI-nek az volt a célja, hogy a DoD komplex, darabokra bontott hálózatait egyetlen egységes felhőalapú vállalatra cserélje, hogy ezzel nagyobb megbízhatóságot és jobb információáramlást tegyen lehetővé a különböző rendszerek között. A felhőalapú szolgáltatás lehetővé tenné a DoD számára azt is, hogy számos új képességet hozzon be. A modern csatatéren elért siker attól függ, hogy a megfelelő információkat a megfelelő személyhez, a megfelelő időben eljuttathassuk. Bár számos egyéb technológia kötődik ehhez – mesterséges intelligencia, gépi tanulás, big data analitika –, a védelmi vállalat hatalmas mérete miatt szükség van a számítási felhőre.[26] Tehát a JEDI-t a meglévő, kereskedelmi forgalomban lévő technológia katonai megfeleltetésére szánták, miközben a méretgazdaságosságot is figyelembe veszi.

A programot 2021 júliusában törölték, arra hivatkozva, hogy a DoD-nak más típusú szükségletei lettek időközben, amelyekre a Joint All Domain Command and Control (JADC2) és a Artificial Intelligence and Data Acceleration (ADA) iniciatívák vetettek fényt. [27]

A JEDI-ről a JWCC-re való áttérés biztonságosabb és sokoldalúbb hálózatot biztosít a DoD számára. Tekintettel a számítógépes hálózatok fontosságára a modern harcokban, ez a lépés véleményem szerint szükséges volt.

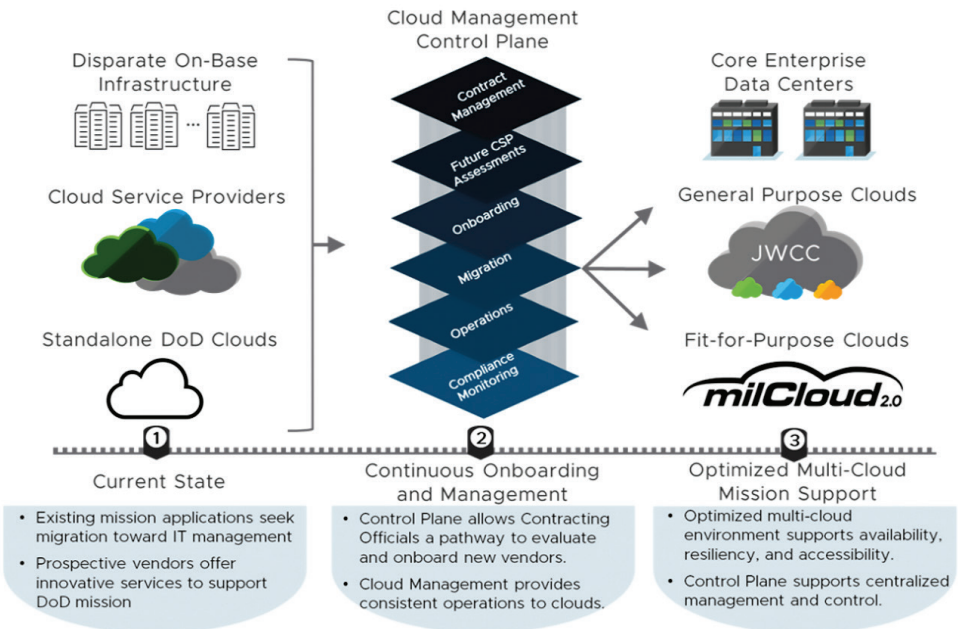
Végrehajtva a JWCC-ben megfogalmazottakat, egy többszállítós szervezeti felhő jön létre, amely a DoD-t minden biztonsági szinten lefedi. A JWCC lehetővé teszi a DoD számára, hogy megteremtse azokat a multicloud[28] előnyöket, amelyeket a multicloudot alapstratégiaként alkalmazó vállalati szervezetek nagy többsége realizált

[26] Mittal 2021.

[27] U.S. Department of Defense 2021.

[28] A multicloud, magyarul többfelhős környezet, amely több (kapcsolt) nyilvános felhőt jelent. Többfelhős telepítést használó vállalatok több nyilvános felhőt is használnak több felhőszolgáltatótól. Ahelyett, hogy egy vállalkozás egyetlen „szállítót" használna a felhőalapú tárhelyszolgáltatáshoz, tároláshoz és a teljes alkalmazásveremhez, a többfelhős konfigurációban többet használnak. A többfelhős környezetnek számos felhasználási módja van. A többfelhős telepítés több IaaS *(infrastructure-as-a-service)* szállítót is igénybe vehet, vagy használhat másik szállítót az IaaS-, PaaS- és SaaS-szolgáltatásokhoz. A többfelhő pusztán redundancia és rendszermentés célját szolgálhatja, vagy magában foglalhat különböző felhőszolgáltatókat a különböző szolgáltatásokhoz.

már.[29] A multicloud jobban illeszkedik a küldetésekhez az architektúrákon belül, szélesebb körű innovációkat kínál a jövőbeli küldetésekhez, jobb ellenálló képességet biztosít az egyetlen forrásból származó hibákkal szemben, és gazdasági előnyöket kínál versenyképes lehetőségekkel. A multicloud használatának masszív növekedése miatt az ipari szabványok és megoldások lehetővé teszik a multicloud környezetek egyszerű integrációját, hordozhatóságát, virtuális hálózatkezelését és irányítását



1. ábra: A többfelhős környezet előnyeinek maximalizálása
Forrás: https://blogs.vmware.com/industry-solutions/2021/10/19/how-jwcc-benefits-from-multi-cloud-adoption/

3.2. Haderőnemi szintű tervek, elképzelések

A hadsereg megváltoztatta az ICT-infrastruktúra korszerűsítésével kapcsolatos megközelítését a felhőalapú rendszerekre való átállással. Ez a megközelítés az IT-hardver-beszerzések és a fenntartás csökkentését helyezi előtérbe annak érdekében, hogy ezeket a képességeket szolgáltatásként a felhőszolgáltatóktól szerezzék be.

Haderőnemi szinten felhőalapú rendszereken dolgozik már az Egyesült Államok haderejének szárazföldi komponense (U.S. Army), az Amerikai Légierő és a Haditengerészet is.

Haderőnemi szinten a U.S. Army két fontos stratégiai dokumentumot készített a felhőalapú rendszerek implementálásáról a haderőben: Army Cloud Computing

[29] *What is JWCC?* é. n.

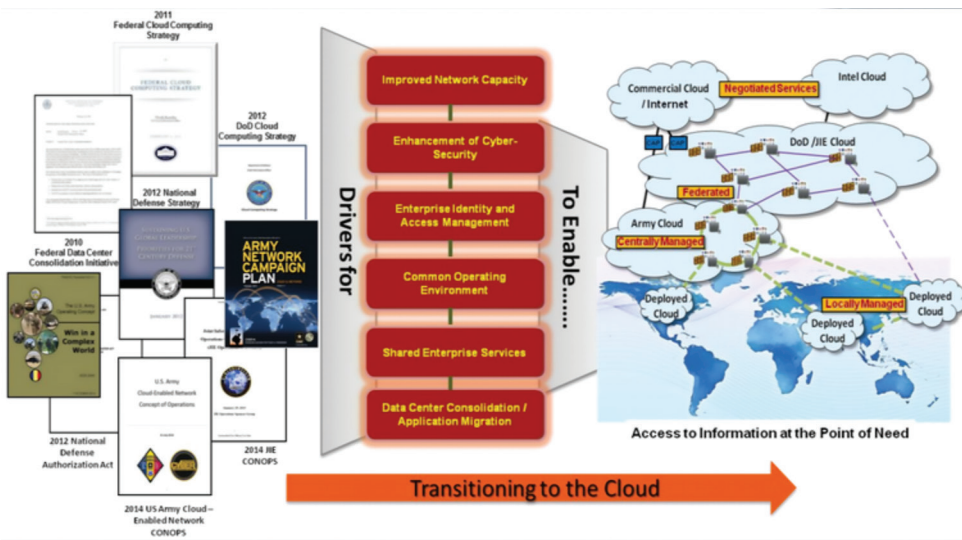
Strategy (a szárazföldi komponens stratégiája, 2015); Army Cloud Plan (a szárazföldi komponens stratégiája, 2020).

De a légierő (Air Cloud One) és a haditengerészet is használ felhőplatformokat (Navy Cloud, amelyet a 2021-es Navy Cloud Computing Policy szabályoz).

Az alábbiakban a fő fókuszt a U.S. Army két stratégiájára helyezi a cikk, mivel az ő példájukon keresztül lehet a legjobban bemutatni a stratégiai környezet fejlődését.

3.3. U.S. Army

Az Army Cloud Computing Strategy-t (ACCS)[30] 2015-ben adta ki a U.S. Army. Az Army Cloud Computing Strategy leírja a hadsereg vízióját és stratégiáját a felhőalapú hálózati képességek biztosítására, a küldetés és a hatékonyság javítása, az operatív információs technológia (IT) hatékonyságának növelése, valamint a hadsereg adatainak és infrastruktúrájának védelme érdekében. Az Army Cloud Computing Strategy kiterjeszti a különböző szövetségi, biztonsági és katonai irányelvekben és dokumentumokban meghatározott alapvonalat és koncepciókat, és beágyazódik a hadsereg hálózati kampánytervébe.



2. ábra: Felhőszámítási stratégiák kontextusa
Forrás: Army Cloud Computing Strategy 2015.

A 2. ábra a különböző megfelelő stratégiákat és dokumentumokat mutatja be, amelyek a hadsereg hadműveleti koncepcióját támogató felhőalapú képességek létrehozását segítik elő. Amint ezek a tevékenységek és kezdeményezések megvalósulnak, megvalósul a hadsereg hibridfelhő-képessége.

[30] U.S. Army (2015): *The Army Cloud Computing Strategy* (2015. március 26.).

Ennek érdekében a vezérkari főnökök és a DoD informatikai igazgatója egyesítették a szolgáltatás összetevőit és a DISA-t (Deployment of the Defense Information Systems Agency)[31] a JIE (DoD Joint Information Environment) létrehozásához és kezeléséhez. A JIE célja az egységes, biztonságos információs környezet létrehozása, amely lehetővé teszi a parancsnokok számára, hogy kapcsolódjanak, hozzáférjenek és megosszák a hatékony működéshez szükséges információkat. Ugyanis a felhőalapú képességek kulcsfontosságúak a JIE sikerében; lehetővé teszik az alkalmazások és az alapvető képességek konszolidálását biztonságos környezetben, valamint az egyetemes hozzáférhetőséget a DoD és a hadsereg között.[32]

A DoD CIO (Chief Information Officer)[33] és a DISA folyamatos együttműködését munkacsoportok biztosítják azért, hogy a DoD felhőstratégia és a kapcsolódó megvalósítási tervek és architektúrák összhangban legyenek a JIE-ben. A hadseregnek javítania kell a hatékonyságot és csökkentenie kell a költségeket, miközben meg kell őriznie az adatbiztonságot a jelenleg és az előrejelzések szerint használatban lévő nagyszámú szoftveralkalmazás és rendszer tárolásával és támogatásával kapcsolatban.

Ezért a speciális adatkommunikációs vezérlési eljárások (Advanced Data Communication Control Procedures, ADCCP) részeként a hadseregnek a hadsereg adatközpontjainak százait kell egységesítenie szabványosított adatközpontokká, telepítési feldolgozási csomópontokká és/vagy nem DoD felhőszolgáltató létesítményekké. A hadsereg parancsnokságának, a személyzetnek, a küldetési területeknek és a tartománymenedzsereknek kell eldönteniük, hogy fenntartsák vagy modernizálják alkalmazásaikat. A tartós alkalmazásoknak ezután át kell állniuk egy jóváhagyott tárhelykörnyezetbe.

A hadseregnek gondoskodnia kell arról is, hogy a meglévő missziós parancsnoki rendszerek, például a taktikai információs hálózat (Warfighter Information Network-Tactical, WIN-T), a széttagoltan települt szárazföldi csapatok (Distributed Common Ground System Army, DCGS-A), a jövőbeli parancsnokságok (Command Post of the Future, CPOF) és a modern tábori rendszerek (Advanced Field) képességei biztosítottak legyenek.[34]

A U.S. Army célja ezzel a stratégiával az volt, hogy megváltoztatja az ICT-infrastruktúra korszerűsítésével kapcsolatos megközelítését a felhőalapú megközelítésre való átállással. Ez a megközelítés az IT-hardver-beszerzések csökkentését és a fenntartást helyezi előtérbe annak érdekében, hogy ezeket a képességeket szolgáltatásként a felhőszolgáltatóktól szerezzék be.

A műveleti képességek átadásához és a kritikus működési funkciók támogatásához négy stratégiai követelmény és a hozzájuk kapcsolódó célkitűzések szükségesek:

[31] DISA: Védelmi Információs Rendszer Ügynökség, egy katonai, szövetségi civil és szerződő partnereikből álló Harci Támogatási Ügynökség. A DISA biztosítja a hálózatot, a számítástechnikai infrastruktúrát és a vállalati szolgáltatásokat az információmegosztás és a döntéshozatal támogatására a DoD-n és a szövetségi ügynökségeken belül.

[32] U.S. Army 2015. 5.

[33] DoD CIO: a Védelmi Minisztérium információs főtisztje, aki a védelmi miniszter fő vezérkari asszisztense és vezető informatikai tanácsadója. Ez a szerepkör számos nemzetbiztonsági és védelmi rendszer felügyeletét, információs erőforrások kezelését és a hatékonyság feltárását foglalja magában. Felelős az osztály információs vállalkozásával kapcsolatos minden ügyért. A cikk írásakor a pozíciót Dr. Kelly Fletcher töltötte be.

[34] U.S. Army 2015. 5.

- felhőirányítási és -kezelési gyakorlatok elfogadása;
- felhőalapú számítástechnikai képességek kategorizálása a hadsereg hálózatán belül;
- alkalmazások, rendszerek és adatok modernizálásának és migrációjának irányítása;
- felhőműveletek biztonságossá tétele és kezelése.[35]

Az ACCS-ban megfogalmazottak szerint a felhőalapú számítástechnika alkalmazásának másik kulcsfontosságú motivációja a felhőalapú számítástechnika bizonyított sikere a magánszektoron belül. Ez a siker olyan innovációknak és kulcsfontosságú technológiai áttöréseknek köszönhető, amelyek megkönnyítik:

- megfizethető, nagy sebességű sávszélesség széles körű elérhetővé tételét;
- kisebb, erősebb és olcsóbb számítógépes processzorok és végfelhasználói eszközök beszerzését;
- párhuzamos feldolgozási módszertanok kialakítását;
- gyors szoftvertelepítési ciklusok kialakítását;
- az adattárolási és -feldolgozási képességek továbbfejlesztett virtualizációját; így lehetővé téve több alkalmazás egyidejű futtatását megosztott fizikai erőforrásokon;
- továbbfejlesztett adatközpont automatizálását, amely jelentősen csökkenti a rendszeradminisztrációs munkaigényt;
- szinte univerzális szoftver-együttműködési szabványok megalkotását;
- új online piacterek létrehozását, ahol a szoftverplatform-szolgáltatók, eszközgyártók, alkalmazásfejlesztők és fogyasztók kapcsolatba léphetnek egymással.[36]

E fejlesztések elfogadása megteremtette a feltételeket az ADCCP számára, hogy az információk, adatok és alkalmazások gyűjtését, elérését, feldolgozását és terjesztését egyéni asztali számítógépekről, laptopokról vagy helyi szerverszobákról központilag kezelt távoli adatközpontokba helyezze át. Ugyanis úgy látták, hogy ha az adatközpont-konszolidációt felhőalapú számítástechnikával, az IT-képességek és -szolgáltatások vásárlására és eladására szolgáló segédprogram-alapú modellel kombinálják, az igény szerinti, fizetős szolgáltatások aggregálása és eljuttatása az ügyfelek számára vonzó és rendkívül versenyképes üzleti lehetőséggé válik. Ugyanakkor be kellett vezetni egy olyan módszeres folyamatot, amely figyelembe veszi a változó biztonsági és üzemeltetési aggályokat, és kockázati alapon végzett értékeléseken alapul. Mindezek a tényezők hozzájárulnak ahhoz, hogy a számítási felhő olyan opció legyen, amely jelentős költségmegtakarítást, IT-hatékonyságot és jobb képesség-szolgáltatást biztosít.

Tehát a U.S. Army Cloud Computing Strategy meghatározza a stratégiai irányt és útmutatást ad a U.S. Army számára a biztonságos működési környezet fenntartására, miközben átalakítja a hadsereg információtechnológiai infrastruktúráját, rendszereit, szoftvereit és alkalmazási platformjait, adatvagyonát, valamint a kapcsolódó műveleti

[35] U.S. Army 2015. 16.
[36] U.S. Army 2015. 6.

szintű folyamatokat és gyakorlatokat. Más néven a felhőalapú megoldásokra való átállás a U.S. Army-nak átfogó terve volt 2015-ben.

2020-ban a U.S. Army új stratégiát adott ki, az Army Cloud Plan-t, amely a 2018-as Nemzeti Védelmi Stratégia (National Defense Strategy, NDS) alá illeszkedik.

Az Army Cloud Plan stratégiai megközelítést kínál a változó digitális helyzetképhez, és támogatja az Army Data Plant (ADP) egy olyan „globálisan hozzáférhető, szabványokon alapuló környezet létrehozásához, ahol az adatok és információk láthatóak, hozzáférhetőek, érthetőek, megbízhatóak, interoperábilisak és biztonságosak a teljes életciklusukon keresztül".[37]

A 2018-as NDS-ben felismerték az új típusú biztonsági fenyegetéseket, ennek nyomán a U.S. Army új felhőstratégiája is igazodott ahhoz, hogy a U.S. Army folyamatai agilisabbá és hatékonyabbá válhassanak az információs hadviselésben.

Ennek értelmében az Army Cloud Plan stratégiai céljai a következők:

- az adatközpontú döntés felgyorsítása;
- a szoftver használati idejének csökkentése;
- optimalizálja a biztonsági akkreditációs folyamatot;
- alapvető kompetenciaként határozza meg a felhőtervezést, a szoftverfejlesztést és az adattervezést;
- szoftver tervezése a dinamikusan változó biztonsági környezethez való alkalmazkodáshoz (utalás történt tehát a gépi tanulás és a mesterséges intelligencia használatára);
- biztosítsa az IT-eszközök/-költségek átláthatóságát és elszámoltathatóságát.[38]

Látható, hogy az Army Cloud Plan a 2015-ös Army Cloud Computing Strategy-hez képest sokkal konkrétabb, kézzelfoghatóbb célkitűzéseket határozott meg, figyelembe véve a kialakult dinamikusan változó biztonsági környezetet.

Az alapvető elképzelés egy multicloud létrehozása a U.S. Army számára: egy minősített, egy nem minősített és egy nyilvános hálózatból.

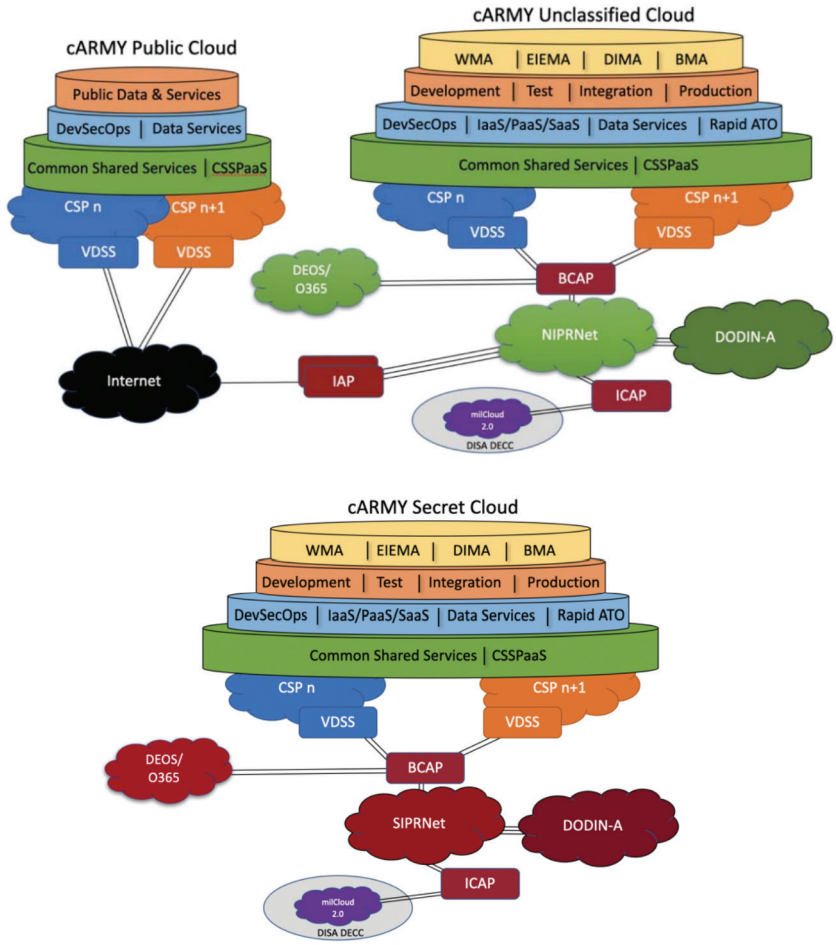
A terv felvázolja azokat a stratégiai célokat és ütemtervet, amelyek megvalósítják a U.S. Army felhőrendszerekről alkotott jövőképét. E terv értelmében a hadsereg többfelhős, több szállítós stratégiát valósít meg, kihasználva a legújabb kereskedelmi felhőszolgáltatásokat, beépített biztonsággal.

A U.S. Army honlapján található további információk szerint a jövőben folyamatosan fejleszti és frissíti a hadsereg felhőtervét, ahogy tapasztalatokat szerez a felhő használatával kapcsolatban. A felhőterv további lépései a következők:

- Közös megosztott szolgáltatások nyújtása, beleértve a kiberbiztonsági szolgáltatásokat is, hogy a hadsereg ügyfelei a cARMY[39]-felhőkörnyezetben működhessenek, operacionalizálhassák adataikat, és teljes mértékben kihasználhassák a felhőalapú számítástechnika előnyeit.

[37] U.S. Army 2020.
[38] U.S. Army 2020. 6.
[39] A cARMY közös megosztott szolgáltatás, amely lehetővé teszi az alkalmazások működését a tárhelykörnyezetben, és központilag az ECMA kezeli őket. A központosított közös megosztott szolgáltatások biztosítása csökkenti a költségeket és csökkenti a felhőbe való átvétel akadályait azáltal, hogy a környezetet minden alkalmazáshoz előkészíti.

- Tehetségkezelési terv kidolgozása és végrehajtása annak biztosítására, hogy a munkaerő rendelkezzen a szükséges adattudományi, szoftverfejlesztési és felhőtervezési készségekkel.[40]



3. ábra: Army Title 10 Enterprise Cloud Ecosystem
Forrás: https://api.army.mil/e2/c/downloads/2020/09/11/81bb912e/the-army-cloud-plan-2020-final2.pdf

2021-ben adták ki az *Army Enterprise Application/System Modernization and Migration to Commercial Cloud Statement of Objectives* (SOO)[41] című dokumentumot. Az Army Enterprise Cloud Management Agency (ECMA), egy helyszíni üzemeltető ügynökség adta ki, amely felügyeli a hadsereg összes felhőfolyamatát és tevékenységét.

[40] U.S. Army 2020.
[41] ECMA 2021.

A dokumentum leírja a hadsereg céljait és követelményeit, hogy vállalati szintű szerződést vagy megállapodást biztosítson a hadsereg alkalmazásai/rendszerei és adatok kereskedelmi felhőkörnyezetekbe történő modernizálására és migrálására.

Az Army Cloud Plan-nel összhangban, a hadsereg azon képessége, hogy hatékonyan használja a felhőalapú technológiákat, kritikus tényező az adatok operacionalizálására való törekvésben. Mint ilyen, a hadseregnek vállalati szintű képességre van szüksége az alkalmazások és adatok kereskedelmi felhőbe történő migrálásához.[42]

Ennek értelmében a hadsereg alkalmazásainak túlnyomó része a cARMY-ba, a hadsereg vállalati felhőkörnyezetébe költözik, amelyet az ECMA kezel. A cARMY jelenleg engedélyezett és működő közös megosztott szolgáltatásokat kínál az Amazon Web Servicesben (AWS) és a Microsoft Azure-ban, a közös, megosztott szolgáltatások fejlesztésére vonatkozó szerződésekkel/tervekkel.

A hadsereg a fentiek mellett figyelembe veszi a cARMY-ba való migráció alóli kivételeket, ha erre komoly üzleti indokok állnak fenn, például olyan szoftver mint szolgáltatás (SaaS) használata, amely nem elérhető a cARMY-ban, ugyanis a cARMY-ba vagy bármely kereskedelmi felhőbe való migráció előtt az akalmazásokat a Cloud Native Design[43] elvek alapján modernizálni kell, hogy kihasználhassák a kereskedelmi felhő előnyeit.[44]

4. Összegzés, következtetések

Az Egyesült Államok haderejében, és specifikusan a szárazföldi haderőben (U.S. Army) nem teljesen új keletű ötlet a felhőalapú szolgáltatások igénybevétele, illetve saját rendszerek építése erre a célra. A folyamatosan újuló stratégiák és tervek remekül körvonalazzák azt a szándékot, hogy a hadsereg lépést tudjon tartani a digitális korral.

A (kereskedelmi) felhőalapú megoldásra való áttérés a DoD digitális és szoftver-modernizációs törekvéseinek egyik pillére. Nem annyira a felhőről van szó, hanem arról, hogy a felhő mire képes. A vállalati kereskedelmi felhő ugródeszka olyan kritikus kezdeményezésekhez, mint a Joint All-Domain Command, Control Framework (JADC2).[45]

A felhőalapú számítási modellek alapvető jelentősége azonban a DoD számára a legkorszerűbb kapacitások támogatásában oda vezetett, hogy a Pentagon újraértékelte megközelítését, amivel a tervezés négy évvel korábban elkezdődött. Ez magában foglalta a felhőalapú szerződések és a kapcsolódó technológiai felvásárlások újraértékelését a JEDI-szerződéstől való elállás nyomán, és létrejött a JWCC, mert a DoD

[42] ECMA 2021. 3

[43] Cloud Native Desgin: a felhőalapú natív architektúra fokozza az IT Ops csapatok hatékonyságát, termelékenységét és együttműködési erőfeszítéseit azáltal, hogy a számítási felhő és a különböző felhőszolgáltatások kombinációját alkalmazza, hogy testreszabható moduláris infrastruktúrát hozzon létre nagyobb méretezhetőség mellett.

[44] ECMA 2021. 3.

[45] A JADC2 az Egyesült Államok Védelmi Minisztériumának (DoD) mozaikszava, a Joint All Domain Command and Control rövidítése, egy stratégiai háborús koncepció, amely összeköti az összes amerikai katonai szolgálat – hadsereg, haditengerészet, légierő, tengerészgyalogság – adatérzékelőit, lövészeket és kapcsolódó kommunikációs eszközöket és az űrerőt, és végül szövetséges partnereit egyetlen integrált „hálózati hálózatba". A stratégia 2022. január 3-án jelent meg.

szerint fontos lépést tartani a gyors technológiai változásokkal. Ezért az új szerződési feltételek biztosítják, hogy a DoD folyamatosan megkapja a kereskedelmi felhőpiac által kínált legjobb technológiai megoldásokat – mindhárom besorolási szinten.

Ezen elvek mentén a U.S. Army Cloud Computing Strategy meghatározza a stratégiai irányt és útmutatást ad a U.S. Army számára a biztonságos működési környezet fenntartására, miközben átalakítja a hadsereg információtechnológiai (IT-) infrastruktúráját, rendszereit, szoftvereit és alkalmazási platformjait, adatvagyonát, valamint a kapcsolódó műveleti szintű folyamatokat és gyakorlatokat. Ennek továbbfejlesztése az Army Cloud Plan, amely felvázolja a hadsereg vízióját arra vonatkozóan, hogy miként kívánja használni a felhőt annak biztosítására, hogy a hadsereg harci erői erősebbek, jobban felfegyverzettek és képzettebbek legyenek ellenfeleiknél az információs technológia használatában az információs harctéren.

Elmondható, hogy a stratégiai környezet a cArmy teljes körű használatára elég erős lábakon áll, amivel, ha a technikai kivitelezés sikeres, és sikerül operacionalizálni az adatokat és megfelelő beruházásokat tenni egy rugalmas információs ökoszisztémába, az amerikai haderő komoly előnyt szerezhet az információs térben.

A U.S. Army azon képessége, hogy elsajátítsa a számítási felhőt, fontos tényező abban, hogy a mesterséges intelligenciát és a gépi tanulást kiaknázzák a kibertéri hadviselésben. A hadseregnek kiemelten kell kezelnie pénzügyi és személyi erőforrásait, hogy céltudatosan folytathassa a fent felvázolt modernizációs erőfeszítéseket, illetve, hogy létrehozza, fenntartsa a digitális fölényt az ellenérdekelt felekkel szemben.

Felhasznált irodalom

Clarke, Steve (2016): *Fourth Quarter Results Highlight Microsoft Cloud Strength.* Online: https://news.microsoft.com/2016/07/19/microsoft-cloud-strength-highlights-fourth-quarter-results/

Clarke, Steve (2017): *Fourth Quarter Results Highlight Microsoft Cloud Strength.* Online: https://news.microsoft.com/2017/07/20/microsoft-cloud-strength-highlights-fourth-quarter-results-3/

ECMA (2021): *Army Enterprise Cloud Management Agency. Army Enterprise Application/System Modernization and Migration to Commercial Cloud Statement of Objectives (SOO)*. (2021. április). Online: https://bit.ly/3u0ZWoh

ENISA (2013): *Good Practice Guide for Securely Deploying Governmental Clouds*. Online: https://doi.org/10.2824/25181

Fedscoop (2020): *CIA Quietly Awards c2e Cloud Contract Possibly Worth Billions*. 2020. november 20. Online: www.fedscoop.com/cia-quietly-awards-billion-dollar-c2e-cloud-contract/

Hogan, Michael – Liu, Fang – Sokol, Annie – Tong, Jin (2011): *Nist Cloud Computing Standards Roadmap*. NIST Special Publication, 35. 6–42. Online: https://csrc.nist.rip/library/NIST%20SP%20500-291%20Cloud%20Computing%20Standards%20Roadmap,%202011-07-05.pdf

Kovács Zoltán (2021) *Az infokommunikációs rendszerek nemzetbiztonsági kihívásai.* Budapest, Ludovika Egyetemi Kiadó. Online: http://real.mtak.hu/128878/1/722_

az_infokommunkicios_rendszerek.pdfjsessionid513BA7B61ED404292AF714063F446241sequence1
Kundra, Vivek (2010): *25 Point Implementation Plan to Reform Federal Information Technology Management.* Online: https://apps.dtic.mil/sti/pdfs/ADA543512.pdf
Kundra, Vivek (2011): *Federal Cloud Computing Strategy*. 10–46. Online: https://acmait.com/pdf/Federal-Cloud-Computing-Strategy.pdf
Kusnetzky, Dan (2009): Fourth Type of Cloud Computing. *ZD Net,* 2009. október 5. Online: www.zdnet.com/blog/virtualization/fourth-type-of-cloud-computing/1346
Lepenye Tamás (2011): *Számítási felhő – egyszerűen.* Online: http://lepenyet.wordpress.com/2011/06/15/szmtsi-felho-egyszeruen/
Lohrmann, Daniel (2010): Cloud First Policy. What Does It Really Mean? *Government Technology,* 2010. december 19. Online: www.govtech.com/blogs/lohrmann-on-cybersecurity/cloud-first-policy—121910.html
Magar, Alan (2014): *Assessing the Use of Tactical Clouds to Enhance Warfighter Effectiveness*. Defence Research and Development Canada. Online: https://apps.dtic.mil/sti/pdfs/AD1016956.pdf
Mittal, Vikram (2021): The Next JEDI: The Joint Warfighter Cloud Capability. Forbes, 2021. július 10. Online: www.forbes.com/sites/vikrammittal/2021/07/10/the-next-jedi-the-joint-warfighter-cloud-capability/?sh=543463a88550
Security Recommendations for Cloud Computing Providers (Minimum information security requirements) White Paper. Federal Office for Information Security, 2011. június 22. Online: www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/CloudComputing/SecurityRecommendationsCloudComputingProviders.pdf?__blob=publicationFile&v=2
U.S. Army (2015): *The Army Cloud Computing Strategy* (2015. március 26.). Online: www.army.mil/standto/archive/2015/03/26/
U.S. Army (2020): *The Army Cloud Plan* (2020. október 9.). Online: www.army.mil/standto/archive/2020/10/09/
U.S. Department of Defense (2021): *Future of the Joint Enterprise Defense Infrastructure Cloud Contract.* (2021. július 6.). Online: www.defense.gov/News/Releases/release/article/2682992/future-of-the-joint-enterprise-defense-infrastructure-cloud-contract/
Vergun, David (2016): *The Army Aims for the Cloud.* U.S. Army, 2016. július 17. Online: www.army.mil/article/171548/the_army_aims_for_the_cloud
What is AWS GovCloud (US)? (é. n.). Online: https://docs.aws.amazon.com/govcloud-us/latest/UserGuide/whatis.html
What is JWCC? (é. n.). Online: www.oracle.com/industries/government/federal/jwcc/

HADMÉRNÖK
VÉDELEMINFORMATIKA

17. évfolyam (2022) 4. szám 131–151.
DOI: 10.32567/hm.2022.4.9

Lendvai Tünde[1]

Kiberbiztonsági körkép Tajvanról[2]

Cybersecurity Overview of Taiwan

A Tsai-adminisztráció kibervédelmi reformjai mentén Tajvan egy alapvetően defenzív berendezkedésű hatalomból mára jóval szélesebb körű, proaktív védelmi eszközkészlettel is rendelkező entitássá vált. A szerző azt elemzi, hogy milyen lehetőségeket nyújt, illetve milyen korlátok jelentkeztek az elrettentési koncepció mentén felépülő kibervédelmi stratégia alkalmazásával. A tanulmány azzal a konklúzióval zárul, hogy a jelenlegi tajvani vezetés stratégiai autonómia felépítésére törekszik a kibertérben, amely visszatükröződik a kiberdiplomáciai aktivitásban és a 2021–2024-es Nemzeti Kiberbiztonsági Programban előirányzott célokban. A minél ütőképesebb és széles körűbb – offenzív és defenzív – képességekkel rendelkező kibertéri erő kialakításával és folyamatos korszerűsítésével a diplomáciai erőfeszítések elérhetik, hogy Tajvan más védelmi szektorban is kimozduljon a kínai diplomáciai nyomás alól, vagy kiegyensúlyozottabb erőviszonyokon alapuló szoros-menti kapcsolatokat tartson fenn.

Kulcsszavak: **Tajvan, proaktív kibervédelem, kiberbiztonság, kiberelrettentés, kibervédelem, kiberdiplomácia**

Along the cyber defence reforms of the Tsai administration, Taiwan has evolved from a principally defensive power to a much broader entity with proactive defence capabilities. The academic problem studied by the author analyses the opportunities and constraints that Taiwan has encountered by applying a cyber defence strategy based on the concept of deterrence. The study concludes that the current Taiwanese leadership is seeking to build strategic autonomy in cyberspace, which is reflected in its cyber diplomacy activities and the goals envisaged in the National Cyber Security Program 2021–2024. By developing and continuously upgrading a cyber force with the most effective and extensive, both offensive and defensive, capabilities, diplomatic efforts could bring Taiwan out from Chinese diplomatic pressure in other defence sectors or maintain more balanced relations based on alignment of power.

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola, e-mail: tunde.lendvai@uni-nke.hu
[2] A tanulmány az Innovációs és Technológiai Minisztérium ÚNKP-21-3-I-NKE-124 kód-számú „új nemzeti kiválóság" programjának szakmai támogatásával készült.

Keywords: **Taiwan, proactive cyber defence, cybersecurity, cyber deterrence, cyber defence, cyber diplomacy**

1. Bevezetés

A 2000-es évektől kezdődően Tajvan (Kínai Köztársaság, a továbbiakban Tajvan) az IT-területen, különösen az információ- és kommunikációtechnológiai (IKT-) szektorban, lenyűgöző innováción ment keresztül, aminek eredményeképpen napjainkra globális viszonylatban szinte megkerülhetetlen gyártói és fejlesztői szerepkörbe került. Különösen érzékelhető a tajvani ellátási láncok jelentősége a chipgyártásban, ami a közeljövőben egyre komolyabb nehézségek árán tudja majd kiszolgálni a többek közt a hazánkban is stratégiai jelentőségű autóipar növekvő igényeit. A jelenlegi tajvani vezetés biztonságpolitikai alapvetése egy potenciális katonai megszállás esetére, hogy a Kínai Népköztársaság (a továbbiakban Kína) aszimmetrikus erőfölényét csak az ellátási láncokban betöltött szerepével és hadereje elrettentő képességének folyamatos fejlesztésével képes ellensúlyozni. Tsai Ing-wen (蔡英文), elnök asszony 2018-ban akképp írta le a *de facto* állam politikai szuverenitásának kulcsát, hogy Tajvannak „nélkülözhetetlenné és pótolhatatlanná kell válnia a világban" biztonságának garantálásához.[3] Az olyan bizalmi garanciákra érzékeny gazdasági szektorok, mint a microchipek, félvezetők (például TSMC vállalat, Taiwan Semiconductor Manufacturing Co.) és más IT-termékek meghatározó világpiaci gyártójaként a tajpeji döntéshozók számára a kibertér védelme ugyanolyan magas politikai prioritást élvez, mint a hagyományos hadszínterek.[4] A tanulmány kutatási célja, hogy átfogó jelleggel mutassa be, miként alakítja Tajvan kibervédelmi felfogását geostratégiai és biztonságpolitikai helyzete.

1.1. Kutatási kérdések és hipotézis

Tajvan biztonságpolitikáját regionális szinten két tényező befolyásolja. Az első az Egyesült Államok és Kína regionális szembenállása, a második a kelet-ázsiai biztonsági komplexumban tapasztalható militarizációs trendek, amelyek érvényesülnek a kibertérben is. A kelet-ázsiai régióban kialakult fegyverkezési verseny a folyamatos észak-koreai fegyverkísérletek okozta fenyegetésre és az USA elrettentését célzó kínai haderőfejlesztésből eredő biztonsági dilemmára vezethető vissza. A Kínai Népi Felszabadító Hadsereg (People's Liberation Army, PLA) képességeinek átalakítása a biztonsági komplexum legtöbb államát (különösen az ellentmondásos és konfliktussal terhelt szoros-menti kapcsolatokkal rendelkező Tajvant) védelmi stratégiája területvédelmi célú megreformálására és haderőfejlesztésre késztette.[5] Japánhoz hasonlóan, a tajvani

[3] Tajpej Képviseleti Iroda (Magyarország) 2018.
[4] Taiwan International Cooperation and Development Fund által szervezett 2022. június 21-i *Webinar on Digital Governance* című konferencián elhangzott előadások alapján.
[5] Bartók–Wagner 2020.

haderőfejlesztési program másik prioritása, a területvédelem mellett, a kiberbiztonsági készültségi szint emelése.[6]

A Tsai-elnökség (2016–2020; 2020–2024) fő védelempolitikai irányelve az „eltökélt védelem és több hadszínteret érintő elrettentés" *(resolute defence, multidomain deterrence)* megvalósítása. A koncepcióban megjelenő, úgynevezett első védelmi réteget *(the first layer of deterrent force)* a kibertérben kell megvalósítani, hiteles elrettentést megjelenítő kiberképességek adaptációjával. A kormányokon átívelő kibervédelmi reformok mentén Tajvan egy alapvetően defenzív berendezkedésű hatalomból mára már jóval szélesebb körű, aktív védelmi eszközkészlettel is rendelkező entitássá vált a kibertérben. A tanulmány első kutatási kérdése arra keresi a választ, hogy milyen lehetőségeket nyit, illetve milyen korlátok jelentkeztek Tajvan kiberdiplomáciai mozgásterében az elrettentési koncepció mentén felépülő kibervédelmi stratégia alkalmazásával párhuzamosan (KK1)? Ehhez kapcsolódóan azt a hipotézist állítottam fel, hogy Tajvan kiberdiplomáciai mozgásterének növelése érdekében arra törekszik, hogy további militarizálás nélkül, kooperatív eszközökkel növelje kiberbiztonsági szintjét, mivel stratégiai érdeke, hogy a régiós biztonsági dilemma ne terjedjen tovább a kibertérben (H1). 2021 novemberében Jyan Hong-wei (簡宏偉), az Ügyvezető Jüan (Kormány) Kiberbiztonsági Osztályának (Department of Cyber Security, 資通安全處) volt igazgatója, parlamenti meghallgatásán megközelítőleg napi 5 millió, kormányzati szektort érintő hálózati behatolási kísérletről számolt be, amelyek közel feléről feltételezik az attribúciót követően, hogy Kína területéről indult, vagy Kínához köthető infrastruktúrát használtak fel hozzá. A tajvani kibervédelmi szervek álláspontja szerint, az állami szektort érő, világszinten is kiemelkedő mennyiségű támadás összefüggésben van Tsai Ing-wen 2016-os és 2020-as újraválasztásával.[7] A kiemelkedő incidensszám összetételét tekintve főként dezinformációs kampányokról, kormányzati weboldalak és hírportálok eltorzításáról (úgynevezett *defacement* támadás) és szolgáltatásmegtagadó (DoS, DDos) támadásokról tettek jelentést a kibervédelmi szervek. E támadások időzítése, tartalma, TTP- *(tactics, techniques, practices)* elemzése arra engedte következtetni a tajvani szakembereket, hogy azok a *de facto* állam függetlenedését vagy a kínai szeparatizmust promulgáló kijelentésekre adott válaszreakciók.[8] Ugyanakkor az utóbbi öt évre visszamenően a tajvani szervek APT- *(advanced persistent treat)*[9] jelenlétre utaló bizonyítékokat találtak az állami szektor elleni sikeres támadások közt.[10] A kínai diplomácia következetesen tagadja állami érintettségét. Önálló, önérdek vezérelte kiberbűnözői tevékenységként tekint az incidensekre, más esetben felületesen elvégzett attribúción alapuló, a tajpeji vezetés vagy az Egyesült Államok által generált lejáratókampányokra figyelmezteti a nemzetközi közösséget.[11] Kérdéses, hogy a Taj-

6 Yau 2020.

7 AFP 2021; Strong 2021. A jelenlegi elnök a Kínai Népköztársaságtól való elhatárolódást és Tajpej függetlenedését szorgalmazza külpolitikájában, ellentétben a korábbi Koumintang-adminisztráció politikájával, amely az anyaországhoz való közeledést szorgalmazta. Az irányváltás fokozta a szoros-menti politikai ellentéteket és növelte az erődemonstrációs katonai aktivitást.

8 A tajvani *Webinar on Digital Governance* című (2022. június 21-i) konferencián elhangzott előadások alapján.

9 Az APT-k tevékenységét államilag támogatott hacker- vagy kiberbűnözői csoportok tevékenységéhez szokás kötni, a szofisztikált módszereik, jelentős infrastrukturális erőforrásaik és hosszan tartó hálózati jelenlétük miatt, amelyek főleg rendkívül érzékeny információk, minősített adatok megszerzésére vagy károsítására irányulnak.

10 Huang 2018.

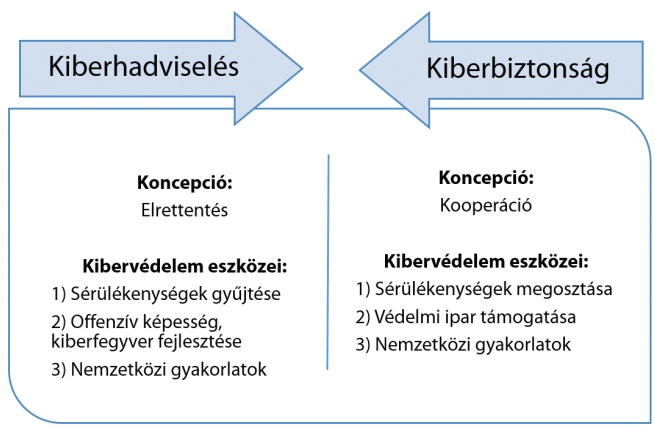
11 Yu–Blanchard 2018; Cheung–Ripley–Tsai 2021; Kínai Népköztársaság Külügyminisztériuma 2022.

vant érő kibertámadásokat lehet-e információs műveletekként (INFOOPS) értékelni (KK2). A tanulmány második hipotézise, hogy jelenleg a tajpeji külpolitikai fordulatra reagáló, a hibrid műveletek közé sorolható szürke zónás tevékenység tapasztalható a KNK részéről, amely nem minősül információs műveletnek (H2).

1.2. Módszertan

A kutatási módszereket tekintve a tanulmány deduktív megközelítést alkalmaz, esettanulmány feldolgozásán és dokumentációelemzésen alapuló kutatási stratégia mentén. Az elsődleges forrásból származó adatgyűjtés módszere szakértői interjú lefolytatásával valósult meg. A szerzőnek lehetősége nyílt kérdéseket feltenni az Ügyvezető Jüan Kiberbiztonsági Osztálya volt igazgatója részére, a magyarországi Tajpej Képviseleti Iroda közreműködésével, és részt venni a Taiwan International Cooperation and Development Fund (ICDF) International Human Resource Development Workshop programsorozata keretében, a 2022. június 21-i *Webinar on Digital Governance* című konferencián. Ezt kiegészítve, a másodlagos forrásokon alapuló adatgyűjtés sajtóhírek, publikus tajvani kormányzati jelentések és a vonatkozó szakirodalom feldolgozásával valósult meg.

2. A tajvani kibervédelmi stratégia témakörében rendelkezésre álló szakirodalom áttekintése



1. ábra: A nemzeti kibervédelem kiépítésének elrettentésen és kooperáción alapuló koncepciói
Forrás: a szerző szerkesztése Taddeo 2018 és Yau 2020 alapján

A tudományos probléma, amely a tajvani kiberképesség-fejlesztés kapcsán körvonalazódik, azt veti fel, hogy amennyiben egy állam – esetünkben *de facto* állam – kibertéri védelmét elrettentő koncepcióra alapozza abból a célból, hogy növelje kiberbiztonsági szintjét, ellentétes hatást érhet el a nemzetközi kapcsolatok realista szemléletmódja alapján. Az elrettentési koncepción alapuló nemzeti kibervédelem kiépítése során

kiberhadviselési eszközöket is felhasznál (lásd 1. ábra), amelyek más államokat késztethetnek ugyanerre, így biztonsági dilemma vagy fegyverkezési verseny alakulhat ki, csökkentve az adott régió és állam kiberbiztonsági szintjét. Az offenzív képességek – lehetnek akár magas vagy alacsony technológiai fejlettségi szinten – a politikai szándékot is figyelembe véve fenyegetettségérzetet kelthetnek a környező országokban, katonai és egyéb nemzetközi szövetségekben. A kelet-ázsiai biztonsági komplexum államainak védelempolitikai gondolkodásában rendkívül elterjedt az elrettentéskoncepció, amely célnak megfelelő kibertéri alkalmazhatósága számos kritikát vet fel elméleti oldalról.[12]

A kiberelrettentés-elmélet kritikusai szerint a kiberbiztonsági szintet valójában csökkenti és nem emeli a koncepció megvalósításának eszközkészlete. Először is, a nemzetközi vagy bilaterális gyakorlatokon (*red team* és *blue team* típusú szimulációk) való részvétel erődemonstrációvá válik a nemzetközi közösség számára. Másodszor, a malware-ek és más támadó programok fejlesztése, a célpontkiválasztás fényében kiberfegyverként értékelhetők, különösen, ha kontrollálhatatlanná válik terjedésük a hálózatokban. Harmadszor, az offenzív képességek fejlesztésének előfeltétele, hogy az állami aktor a felfedezett sérülékenységeket ne publikálja a gyártó vagy a nyilvánosság részére, hanem gyűjtse a későbbi kihasználás érdekében. Ez a gyakorlat végső soron csökkenti az adott állam kiberdiplomáciai mozgásterét, a piaci és állami szereplők közti bizalmat, valamint a szoftver- és hardvergyártók termékeibe vetett fogyasztói bizalmat, ami különösen fontos a világszinten kiemelkedő IKT-technológiai iparral rendelkező Tajvan számára.[13]

Tajvan esetében, a már említett kiemelkedő számú kormányzati és állami szerveket érintő incidensszám mellett, a kibertéri fenyegetések széles skálája fordul elő, amelyek a kognitív dimenziót célzó műveletektől kezdve a kritikus információs infrastruktúrát érő incidensig terjednek. E tényezők mellett a tajvani kiberbiztonsági stratégiai gondolkodást jelentős mértékben alakítja a kínai megszálláshoz kapcsolódó fenyegetettségpercepció. Ebben a kiberbiztonsági és biztonságpolitikai környezetben, 2018 szeptemberében a Nemzetbiztonsági Tanács közzétette első nemzeti kiberbiztonsági stratégiai jelentését, amely kiterjesztette a nemzetbiztonság értelmezését a kiberbiztonságra *(cybersecurity as national security)*. 2019-ben a tajpeji vezetés elérte a nemzeti biztonsági törvény módosítását, amellyel jogi felhatalmazást biztosított az állami szervek, köztük a hadvezetés részére, hogy offenzív képességekkel biztosítsák Tajvan kibertéri védelmét. A 2019-es Nemzeti Védelmi Jelentésében *(The 2019 National Defense Report)* a Tsai-elnökség offenzív és defenzív képességek adaptációjával kívánta felépíteni a hiteles kibertéri elrettentő erőt.[14] A szakértői interjú során megerősítették, hogy az e mögött álló kibervédelmi stratégiai elképzelés az, hogy a válaszcsapás lehetősége rettenti el a támadó aktorokat (például a támadó infrastruktúra ellehetetlenítésével), és egyelőre nem fogalmazódott meg politikai szándék egyéb alkalmazási célokra vonatkozóan, például a megelőző csapásmérés lehetőségével kapcsolatban. Ebben a nézőpontban a *passzív védelmi képességek,* vagyis a korai észlelési és detekciós képességek, a fejlett incidenskezelés

[12] Yau 2020. 11.
[13] Taddeo 2018.
[14] Yau 2020. 2.

annyira megnövelhetik a védelem áttöréséhez szükséges erőforrás-ráfordítást, hogy az már nem lesz összhangban az elérni kívánt eredmény nyújtotta előnyökkel. Ez eltérítheti a legtöbb kevésbé szofisztikált módszerekkel és szerényebb technológiai háttér-infrastruktúrával rendelkező támadó aktort, azonban nagy valószínűséggel az állami hátterű csoportokat nem. Elméletben az „ellentámadás" megindításának lehetősége, vagyis az *aktív kibervédelem* alkalmazása eltántoríthat egy állami szereplőt. Ilyen esetben a megtámadott fél, offenzív képességeit a támadó infrastruktúra vagy akár bármely más célpont ellen is bevetheti. Az ellentámadásnak pont a megfelelő mértékű, hálózati és kinetikus károkat kell okoznia (Stuxnet) kontrollált, például földrajzilag korlátozható kiterjedésben. Az elmélet alapján ez a károkozási képesség tántoríthatja el szándékától a potenciális állami hátterű támadókat, aminek hitelességét alá kell támasztani (például egy szimulációs gyakorlat alkalmával vagy éles demonstrációval).[15] A kibertéri elrettentéselmélet hatékony alkalmazhatósága több problémát is felvet. Egyrészt a válaszcsapás könnyen eszkalálhatja a konfliktust, vagy elmarasztaló reakciót válthat ki a nemzetközi közösségből, akár diplomáciai elszigeteltséghez is vezethet. Másrészt azon offenzív képességek, amelyek ilyen hatás kiváltására képesek, már túlmutathatnak a nemzetközi jogban bevett arányos fellépés és önvédelem esetpéldáin. Sokkal inkább értelmezhetők kiberfegyverként.[16]

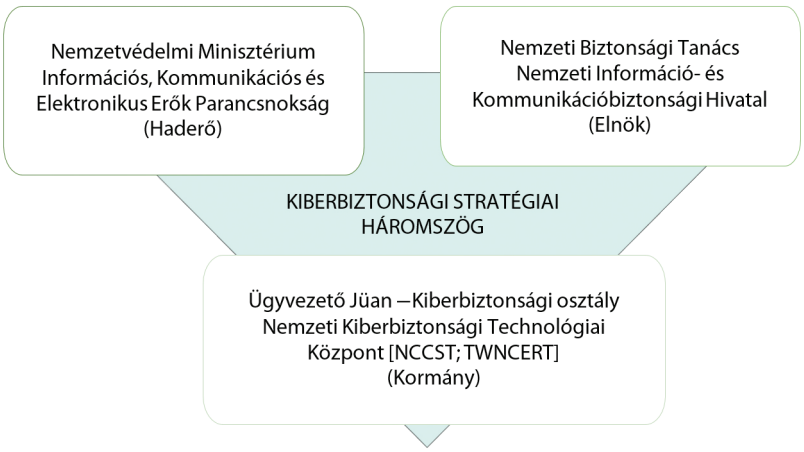
A szakirodalom alapján Tajvan és Kelet-Ázsia számára az alternatívát egy olyan együttműködésre építő stratégia jelenti, amelyben a hasonló fenyegetettségpercepcióval és kiberdiplomáciai célokkal rendelkező, közel azonos értékek mentén gondolkodó országok összehangoltan erősítik meg védelmi technológiai képességeiket. A kooperáció mélységétől függően a gyakorlati területek a kiberbiztonsági termékek fejlesztését, malware-elemzések és sérülékenységek publikálását és a felfedezett szoftveres sebezhetőségek kijavításával kapcsolatos információmegosztást foglalhatják magukban (lásd. 1. ábra). Ezek a lépések összességében emelik bármely ország vagy régió kiberbiztonsági szintjét és rezilienciáját.[17]

3. A kibervédelem szerkezeti felépítése és stratégiai háttere

A tajvani vezetés már 1999-ben megtapasztalta a kibertérből érkező fenyegetések lakosságra gyakorolt káros kognitív hatásait[18] és ezzel együtt felismerte az átfogó nemzeti kibervédelmi intézményrendszer és C3I-struktúra (*command, control, communications and intelligence*, parancsnokság, irányítás, kommunikáció és hírszerzés) kiépítésének szükségességét, az információs hálózatok folyamatos korszerűsítésének fontosságát.[19] Tajvanon a kibervédelmi keretrendszer és intézményi struktúra alapjait a 2000-es évektől kezdték kiépíteni, elsősorban a digitális információk védelmét célozva. A 2001-ben létrehozott Nemzeti Információs és Kommunikációs Munkacsoport

[15] Yau 2020. 7.
[16] Taddeo 2018.
[17] Yau 2019.
[18] 1999-ben számos kormányzati szerv weboldala szenvedett el defacement támadást azt követően, hogy Li Tenghui elnök „különleges államközi kapcsolatnak" nevezte a Tajvan és Kína közi viszonyt.
[19] Rawnsley 2005.

(National Information and Communication Task Force) feladata, hogy összefogja a minisztériumokon, kormányhivatalokon és egyéb állami szerveken belüli kiberbiztonsági részfeladatokat ellátó munkacsoportok tevékenységét.[20] Ezt az alapstruktúrát egészíti ki a Nemzeti Kiberbiztonsági Technológiai Központ (National Center for Cyber Security Technology) – amelyen belül a tajvani CERT (TWNCERT, kormányzati eseménykezelő központ) működik –, amely technológiai biztonsági szolgáltatásokat nyújt.[21]



2. ábra: A tajvani kiberbiztonsági szervek elhelyezkedése a védelmi szempontból releváns (elnök, kormány, hadsereg) államigazgatási területeken
Forrás: a szerző szerkesztése Huang 2018. 101. alapján

A stratégiai horderejű védelmi reformokat tekintve, Ma Ying-jeou (2008–2016, Kuomintang) elnöki ciklusa során, 2015-ben állítottak fel egy kiberhírszerzésre szakosodott szervezeti egységet a nemzetbiztonsági hivatalon belül. A Tsai-elnökség 2016-os beiktatását követő egyik első intézkedése volt a Nemzeti Információ- és Kommunikációbiztonsági Irodának a felállítása a Nemzeti Biztonsági Tanácson belül, amely az elnök közvetlen tanácsadó testülete. Ugyanebben az évben az Ügyvezető Yüan (a kormány) is felállította végrehajtó szervezetrendszerén belül a Kiberbiztonsági Osztályt, amelyhez tartozó munkacsoportok felelősek többek közt a kritikus információs infrastruktúra védelméért, a szabályozási és standardizálási előírások megalkotásáért és fejlesztéséért. 2017-ben a haderőszervezési reform keretében állították fel a tajvani hadsereg negyedik parancsnokságaként a Nemzetvédelmi Minisztérium irányítása alatt az Információs,

[20] Például az Oktatásügyi Minisztériumon belül működik a tudatosító képzésekért és tehetséggondozásért felelős csoport (Awareness Education and Talents Cultivation Group) az Igazságügyi és Belügyminisztériumok közös felügyelete alatt működik a kiberbűnözés felderítéséért és megelőzéséért felelős csoport (Cybercrime Protection and Control Group), míg a Nemzeti Kommunikációs Bizottság alatt az ún. Információs és kommunikációs ökoszisztéma és az internetes tartalom biztonsági csoport (Information and Communication Environment and Internet Content Security Group).

[21] Például általános tervezés és stratégiai elemzés (oktatás, jogi és szabályozási ügyek), incidensbejelentés és incidenskezelés (*monitoring, forensics* szolgáltatás is), adatelemzés, kutatás-fejlesztés, *penetration testing* (offenzív vizsgálatok) stb. A két szervezet tevékenységi köre magyar relációban a Nemzeti Infokommunikációs Szolgáltató Zrt. és a Nemzeti Kibervédelmi Intézet feladatköréhez hasonlítható.

Kommunikációs és Elektronikai Hadviselési Parancsnokságot, amely égisze alatt megkezdődhetett az offenzív kiberképességek kiépítése. Hsini Huang tajvani kiberbiztonsági szakember arról értekezett, hogy a kibervédelmi szervezetrendszer átalakítását érintő reformokban is megfigyelhető a Kuomintang-adminisztrációt jellemző, fenntartható Kína-kapcsolatok megtartása miatti óvatosabb, provokációt kerülő védelmi átszervezés. Ezzel szemben a jelenlegi elnökséget adó Demokratikus Progresszív Párt, a kiberbiztonsági környezet változását (növekvő incidensszám és APT-jelenlét) is kihasználva, képes volt keresztülvinni a katonai szervezetrendszert érintő reformokat. Emellett új stratégiai irányt hirdetett – amely a nemzeti biztonság részének tekinti a kiberteret, továbbá elrettentésre és offenzív technológiákra építi védelempolitikáját –, és a korábbiaktól eltérő megközelítést alkalmazva a hazai kiberbiztonsági iparág támogatásával kívánta korszerűsíteni a kiberbiztonsági infrastruktúrát. A Tsai-elnökség védelempolitikai elképzeléseihez illeszkedő szervezeti struktúrát „kiberbiztonsági stratégiai háromszög"-nek (lásd 2. ábra) nevezték el a szakirodalomban, mert integrálja a védelmi stratégiai tervezéshez és reagáláshoz szükséges három államigazgatási kulcsterületet: a hadvezetést, az elnöki tanácsadó testületet és a kormányzatot.[22]

A kibervédelmi fejlesztések politikai prioritásának kormányokon átívelő kontinuitása figyelhető meg abban, hogy 2001-től folyamatosan publikálták a négyéves ciklusra meghatározott kibervédelmi és kiberbiztonsági környezetet fejlesztő programokat. Két fejlesztési programot határoztak meg 2001–2004 és 2005–2008 között Nemzeti információs és kommunikációs infrastruktúra-biztonsági mechanizmusterv *(National Information and Communication Infrastructure Security Mechanism Plan)* néven. A 2005–2008 közötti fejlesztési időszakban kialakítottak egy nemzeti szinten működő kiberbiztonsági műveleti központot (Security Operation Center, SOC), amelynek feladata az incidensek megelőzése, detektálása és figyelmeztetések kiadása. Ezt követően – illeszkedve a nemzetközi trendekhez – a fejlesztési programokat új néven hirdették meg, a kiberbiztonság és kibervédelem szélesebb fogalmi értelmezése miatt, amely figyelembe veszi a pszichológiai hatások kiváltását az információs és kommunikációs technológiák felhasználásával. Ennek fényében négy további ciklusra vonatkozó Nemzeti Stratégiát adtak ki a Kiberbiztonság Fejlesztési Tervéről *(National Strategy for Cybersecurity Development Plan)*, amely legutóbbi, hatodik szakaszát a 2021–2024-es időszakra tervezték. A 2013–2016-as időszaktól kezdődően fokozatosan tovább bővült a nemzeti SOC rendszere, ami révén napjainkra kialakították az úgynevezett Nemzeti Közös Védelmi Rendszert (National Joint Defence System), amely ISAC- (Information Sharing and Analysis Center, információmegosztó és elemző központ) és CSIRT- (Computer Security Incident Response Team, számítógép-biztonsági incidenskezelő csoport) képességeket is integrál.[23] A reformsorozat növelte a nemzeti helyzetfelismerő képességet az úgynevezett domain szintű speciális nagyvárosi önkormányzati *(domain level)* és helyi önkormányzati, úgynevezett szolgáltató szinteken *(service provider level)* nyújtott felügyeleti szolgáltatások információinak becsatornázásával. A 2017–2020-as fejlesztési program egyik fő eleme a legmagasabb biztonsági osztályba sorolt állami szervek érettségi szintjének növelése és a hazai kiberbiztonsági piacot

[22] Huang 2018. 101–103.
[23] *Taiwan National Computer Emergency Response Team Annual Report 2021.* 2022.

támogató akcióterv megvalósítása volt. Emellett a teljes körű ISAC, SOC és CERT kiépítésének megkezdését irányozta elő a kritikus infrastruktúrában.[24]

A 2020-ban kiadott, 2021–2024-es Nemzeti Kiberbiztonsági Program (National Cyber Security Program) három fő célterületet határozott meg a víziójában a „biztonságos és ellenálló intelligens nemzet" *(smart country)* felépítéséhez:

- a kiberbiztonsági kutatás és képzés központjává válni az ázsiai és csendes-óceáni térségben;
- felépíteni egy proaktív védelmi alapokon nyugvó infrastruktúra-hálózatot;
- köz- és magánszféra közötti partnerség megteremtésével megfelelő ökoszisztémát létrehozni a kiberbiztonsági szint növelése érdekében.

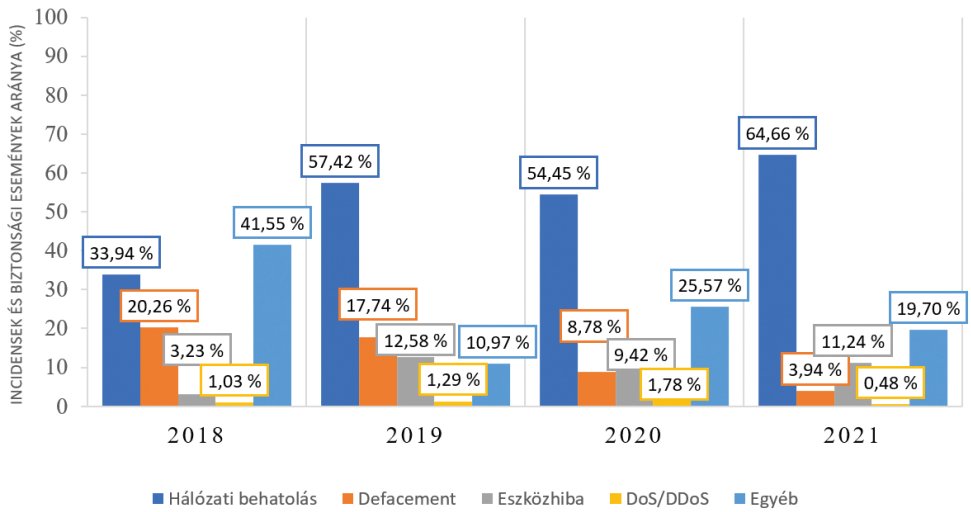
Az első célterülethez kapcsolódóan növelik a gyakorlati szakemberek számára elérhető tehetséggondozó lehetőségeket, és megnövelték a felsőoktatásban a kiberbiztonsági kutatási erőforrások és oktatók létszámának kvótáját, továbbá megnyitják a kormányzati szolgálati hálózat (Government Service Network, GSN) egy részét a gyakorlati oktatás részére. Emellett Kiberbiztonsági Kiválósági Központot (Cybersecurity Center of Excellence) hoznak létre az akadémiai kutatások és kritikai „jövőkutató" előrejelzések *(critical cybersecurity prospective research)* elvégzésére. A tervek szerint a központ csereprogramokat fog indítani és nemzetközi kutatókat is fogad majd. A második célterület a kritikus infrastruktúrák ellenállóképességének növelésére, valamint a kormányzati infrastruktúra felderítő képességei fejlesztéséhez fogalmaz meg intézkedéseket. Ilyen a kritikus infrastruktúra-szolgáltatók rendszeres auditálása és az egységes védelmi mechanizmus továbbfejlesztése (információmegosztás, értesítés az incidensekre adott válaszokról, kiberbiztonsági felügyelet). Fontos célkitűzés a CISO-k kinevezése és a biztonsági alapszint *(cyber security baseline)* kiépítése a létfontosságú infrastruktúra-szolgáltatóknál. A harmadik, magán- és állami szféra kooperációját növelő célterület főleg az infokommunikációs chipek gyártására fókuszál, valamint az 5G infrastruktúra biztonságának növelésére (Tajvan is biztonsági előírásokra vonatkozó megállapodást írt alá az Egyesült Államokkal: Joint Declaration on 5G Security).[25] Ennek keretében a kiszervezett szolgáltatások ellátási láncára vonatkozó kockázatkezelési rendszer megerősítését tűzte ki, és előrevetíti egy állami megfelelőségi tanúsítás *(compliance certificate)* kidolgozását az IoT-eszközök részére. Emellett fontos szegmens a lakosság tudatossági szintjének növelése a dezinformáció kiszűrése érdekében, amelyben célprogramokkal aktívan részt vesz a magánszféra, például a Google tajvani képviselete is.[26]

Arra a kérdésre, hogy védelempolitikai kérdésekben a tajvani vezetés mennyire tartja fontosnak a kibertér védelmét a haditengerészeti és légvédelemhez képest, a megkérdezett szakértő elmondta, hogy mindhárom domain egyforma fontosságú,

[24] Huang–Li 2018.
[25] Her 2021.
[26] Az információk alapjául a szakértői interjú és a Taiwan International Cooperation and Development Fund (ICDF) International Human Resource Development Workshop programsorozata keretében, a 2022. június 21-i *Webinar on Digital Governance* című konferencián elhangzottak szolgáltak. Lásd még a tajvani Nemzeti Kiberbiztonsági Technológiai Központ weboldalán megjelent összefoglalót: National Center for Cyber Security Technology 2022. (A program teljes szövege angol nyelven itt elérhető.)

mivel a biztonság és védelem értelmezését kiterjesztették a fizikai térről a kibertérre is, a támadások által kiváltható hatásokra tekintettel. Ebben a kérdésben Tajvanon konszenzus van a közvéleményben és a politikai diskurzusban.

4. Kibertéri fenyegetések



3. ábra: Kormányzati szervek által jelentett kiberbiztonsági incidensek százalékos megoszlása a TWNCERT éves jelentései alapján (2018–2020)

Forrás: a szerző szerkesztése a Taiwan National Computer Emergency Response Team Annual Report 2018–2021. alapján

A TWNCERT részére bejelentett biztonsági események és incidensek évenkénti megoszlásának százalékos arányát mutatja meg a 3. ábra.[27] Az éves részadatok 7709 db, 2022. január 31-én felügyelet alá tartozó intézménytől származtak, amelyek központi vagy helyi kormányzati szervek, kritikusinfrastruktúra-szolgáltatók, állami vállalatok és alapítványok. Az összesítő táblázat 2021-es „Hálózati behatolás" adatcsoportjára vonatkozik a sajtóhírekben megjelent, összességében 7709 intézményt érő, napi 5 milliós ártó szándékú esetszám, amelybe egyaránt beletartozik a sérülékenységeket kereső hálózati letapogatás *(scan)* és a támadás *(incidens),* valamint ez utóbbi sikeressége esetén az irányítás megszerzése *(control)*.[28] A CyCraft tajvani kiberbiztonsági

[27] Mivel a TWNCERT jelentéseiben használt címszavak pontos definíciói, a konkrét számadatok és háttérszámítások nem ismert, érzékeny információk, ezért csak korlátozott pontosságú megállapítások vonhatók le. Fontos megjegyezni továbbá a sajtóhírekben megjelent állami szerveket érő nagyszámú támadás – havi 30-40 millió hálózati behatolási kísérlet – kapcsán, hogy a tajvani kormányzati közleményekben a biztonsági eseményekre és incidensekre használt definíciók különbözhetnek az egyes nemzetközi szervek, az akadémiai és a civil szféra által használt munkadefinícióktól, emiatt a különféle forrásokban eltérőek lehetnek a vonatkozó számadatok.

[28] A Taiwan International Cooperation and Development Fund által szervezett 2022. június 21-i *Webinar on Digital Governance* című konferencián elhangzottak alapján.

vállalat, a *Taiwan News*-ra hivatkozva átlagosan heti 2644 támadásról (incidensről) írt blogbejegyzésében, így számításaik szerint 2020-ról 2021-re 38%-kal nőtt a tajvani állami szférában tapasztalt incidensek száma. A heti 925 támadásra tehető globális átlagtól való eltérés okát a CyCraft elemzői Tajvan egyedülálló geopolitikai helyzetére, csúcstechnológiás gazdaságára és kiforrott kommunikációs infrastruktúrájára vezetik vissza.[29] Tovább árnyalják az összképet a tajvani kormányzat által publikált, sikeres incidensek számára vonatkozó adatok, amelyek alapján 2019-ben 310 sikeres hálózati behatolás történt, 2020-ban 525 és 2021-ben 642 eset. A kihasznált sérülékenységek leggyakoribb eredői a gyenge jelszavakra, a *social engineering* technikákra és a frissítések hiányára *(unpatch)* vezethetők vissza.[30]

4.1. A dezinformáció esetpéldái

A 2021-es World Press Freedom Index Ázsián belül a másodikként (Dél-Korea mögött), világszinten negyvenhatodikként értékelte (180 vizsgált államból) a tajvani média diverzitását és a szólásszabadság biztosítottságát. 2020-as statisztika alapján a háztartások 99,99%-a rendelkezik digitális televízióval, továbbá 252 online és nyomtatott sajtószolgáltató, 32 hírügynökség, valamint 64 kábel- és 105 műholdas csatorna érhető el.[31] Ebben a médiakörnyezetben a kormányzati szereplők és a kiberbiztonsági szakértők egyaránt a dezinformáció mértékét tartják a Tajvant érő legsúlyosabb kihívásnak.[32] A dezinformáció elleni küzdelem részeként 2019-ben a Nemzetvédelmi Minisztérium politikai hadviselés elleni irodája (Political Warfare Bureau) bejelentette egy álhírekre adott válaszreakciókért felelős gyors reagálású csoport létrehozását, továbbá azt, hogy a Nemzeti Biztonsági Tanács big data elemzési technológiát alkalmazva elemzi a Kínai Kommunista Párt narratívájával egyező álhírek terjesztési taktikáit a megfelelőbb, technológiaalapú válaszlépések kidolgozásához. Ezzel párhuzamosan a kormányzat egyik új megközelítésében a köztisztviselők kreativitására bízta, hogy az „internet nyelvén", vagyis mémekkel reagáljanak az álhírekre, amely technikát a tajvani digitalizációért felelős miniszter, Audrey Teng egy 2019-es beszédében „a humorral a híresztelés ellen" ('humor over rumor', *meme engineering*) mechanizmusként írt le. A minisztériumokban olyan csoportokat alakítottak ki, amelyek feladata, hogy az álhírekre 1 órán belül reagáljanak, legfeljebb 20 szavas címet és 200 karakternyi szöveget tartalmazó tisztázó mémüzenet közzétételével a közösségimédia-felületeken. A kezdeményezés mögött olyan felmérés áll, amely alátámasztotta, hogy azon felhasználó, aki látta a tisztázó üzenetet, többé nem osztotta meg a kapcsolódó álhíreket, így gyors kiszűrés esetén rövid időn belül képesek visszaszorítani annak terjedését.[33] A módszer sikerének előfeltétele, hogy a lakosság magas digitalizáltsági mutatókkal és tudatossági szinttel

[29] CyCraft Technology Corp 2022.

[30] A Taiwan International Cooperation and Development Fund által szervezett 2022. június 21-i *Webinar on Digital Governance* című konferencián Jyan Hong-Wei (Végrehajtó Jüan Kiberbiztonsági osztályának volt igazgatója) *National Cyber Security Program of Taiwan* című előadása alapján.

[31] Tajvan Külügyminisztériuma 2022.

[32] A Taiwan International Cooperation and Development Fund által szervezett 2022. június 21-i *Webinar on Digital Governance* című konferencián elhangzottak alapján.

[33] Blanchette et al. 2021. 16–17.

rendelkezzen, továbbá a kormányzati kommunikációs csatornáknak széles elérési hálója legyen a társadalomban.

Az álhírek terjedéséről a tajpeji The DoubleThink Lab nevű kutatólabor végzett nagyszabású felmérést annak apropóján, hogy nagyszámú hamis vagy félrevezető információ jelent meg a tajvani médiában 2020-ban, ami a koronavírus okozta pandémia kiindulása mellett az elnökválasztás éve is volt. A támadók azt sugallták, hogy Tajvanon megbukott a demokrácia, és ezt a koronavírussal kapcsolatos hamis állításokra is visszavezették. Ezzel próbáltak megosztottságot generálni a lakosságban, csökkenteni a kormányzat iránti bizalmat, valamint megzavarni a politikai folyamatokat olyan eszközökkel, amelyek úgynevezett hír- és információs visszhangkamrákba[34] szorítják az egyes társadalmi csoportokat. A hamis vagy félrevezető információt tartalmazó közösségimédia-posztokon vizsgált indikátorok, amelyek a dezinformáció eredetét, célját, hatását, célközönségét és terjesztésének módját elemezték, összehangolt tevékenységre és pekingi narratívára vezethetők vissza. A The DoubleThink Lab elemzése feltárta, hogy a támadók szoros együttműködést kezdeményeztek célországbeli (nem csak Tajvan), valós online influencerekkel (véleményformálók), akiket arra próbáltak rávenni, hogy megosszák az álhíreket nagy elérésű platformjaikon. A kutatólabor összességében nagyszabású információs műveletként értékelte a 2020-as dezinformációs kampányt, amelyért állításuk szerint a Kínai Kommunista Párt tehető felelőssé. Megoldási javaslatukban jogi normák meghozatalát vagy módosítását és tartalomszabályozási intézkedéseket ajánlottak a tajpeji vezetés részére.[35] Fontos megjegyezni, hogy Magyarország és euroatlanti szövetségesei tágabban értelmezik az információs műveleteket a *Tallinn Manual* (*Tallinni kézikönyv,* a kiberháborúra alkalmazandó nemzetközi jog tallinni kézikönyve) alapján. A pszichológiai műveletek (PSYOPS) és a számítógép-hálózati műveletek mellett – amelyet a dezinformációs kampány érint – beletartoznak a fogalomba a képi és rádióelektronikai felderítés (IMINT, SIGINT) és az elektronikai hadviselés műveletei. Annak megállapításához, hogy Tajvant érik-e információs műveletek Kína részéről, komplexebb képet kell vizsgálni az euroatlanti katonai gondolkodásmód alapján.

Maradva a dezinformáció esetpéldáinál, a tajvani rendőrség csúcstechnológiás bűnözéselleni központja (High-tech Cybercrime Center)[36] 2020 és 2021 folyamán az alábbi két jelentős, állami hátterű dezinformációs támadásról számolt be. Az első eset 2021 áprilisában történt, amikor a Twitteren egy hamis állami dokumentumról készült fotó kezdett el terjedni, amely azt tartalmazta, hogy Tajvan nukleáris anyagokkal szennyezett vizet vesz át Japántól. Az álhíreket tartalmazó eredeti posztot közzé tevő fiókok lenyomozása után megállapították, hogy a felhasználó IP-címe kínai szolgáltatóhoz van regisztrálva, továbbá már korábban is használták támadások során. A második esetpéldában az összehangolt hiteltelen magatartás *(coordinated inauthentic behaviour)*

[34] Egy jelenség, amelyet a keresőmotorok és a közösségi hálózati oldalak üzemeltetői által működtetett hírválogatási algoritmusok (például a felhasználó által beállított szempontok vagy egyedi aktivitás) szűrőbeállításai okoznak. Emiatt a felhasználó a teljes médiakörnyezet helyett csak korlátozott, megszűrt híreket és hírforrást ér el közösségimédia-felületén vagy a keresőmotorokban, ami nem feltétlenül fedi a valóságot. GÁLIK 2019.

[35] Allen-Ebrahimian 2021.

[36] A központ és annak digitális igazságügyi laboratóriuma (digital forensics lab) rendelkezik ISO/IEC 17025 Windows Program Analysis Operating Procedures tanúsítvánnyal.

technikáját fedték fel 2021 szeptemberében egy tajvani kiberbiztonsági céget érintő dezinformációs kampányban. A támadás első hullámában egy japán hírmegosztási szolgáltatást nyújtó weboldalon keresztül jelenítettek meg álhíreket szeptember 17-én, amelyeket négy napig terjesztettek a tajvani közösségi médiában. Szeptember 25-én, a második hullám kezdetén a támadók által létrehozott felhasználó hamisnak nevezte a kiberbiztonsági cég hivatalos magyarázatát, két nappal később ugyanaz a japán weboldal a Kaspersky Lab japán kirendeltségének bejegyzésére hivatkozva újabb hamis információt közölt, amelyet a korábban is használt felhasználói fiókon keresztül terjeszteni kezdtek a közösségi médiában. Szeptember 30-án a Kaspersky Lab Japan közzétette hivatalos oldalán a helyesbítést, és elismerte, hogy a támadók megszemélyesítették. A támadók identitására többek közt a bejegyzésekben használt egyszerűsített kínai írásjegyek (ezeket Kínában használják hivatalosan, míg Tajvanon a régies, komplexebb írásjegyeket) is utaltak, a nyomozás végén a tajvani rendőrség két elkövető személyt azonosított.[37]

4.2. APT-jelenlét esetpéldái

Az egyértelmű politikai indíttatás miatt említésre méltó az Apple Daily tajvani hírszolgáltatót 2014-ben érő támadások sorozata, amely a szolgáltató hongkongi „esernyős forradalom" tüntetéssorozatról szóló, kínai kormányzatot elítélő hangvételű riportjaira adott válaszreakciók voltak.[38] Jelentős eseményként tartják számon a tajvani szakemberek a Közszolgálati Minisztériumot ért 2019. júniusi adatszivárogtatást, amely a közszolgálatot ellátók személyes adatait érintette.[39]

A tajvani kritikus információs infrastruktúrát 2020 májusában érte zsarolóvírus *(ransomware)* általi kibertámadás. A célpont a nemzeti olajvállalat – a CPC Corp – volt, amely az olajtermékek szállításáért és a cseppfolyósított földgáz (LNG) importjáért felelős. A tajvani hatóságok a támadási lánc első eseményét 2018 júliusára vezették vissza, amikor a támadók *malware-t* helyeztek el az áldozatok weboldalán. A támadók 2022. március végén kezdték meg a műveletet, ekkor a weboldal abnormális csatlakozást kezdeményezett az intranet irányába, majd négy nappal később a hackerek behatoltak a domainszerverre és nagyszámú csatlakozási kérést generáltak, ami riasztást váltott ki. Másnap a támadók két számítógépre helyeztek el programot *(backdoor)*, amely utat nyitott a rendszerbe történő behatoláshoz. Ezt a trójai típusú támadást tekinthetjük a behatolási pontnak *(intrusion point)*. Negyvenkét nappal később, a munka ünnepe miatti három napos hosszú hétvégét kihasználva, május 4-én a támadó átvette az irányítást a rendszergazda fiókja felett, és bejelentkezve az AD-szerverre, a csoportházirendek (GPO) segítségével szétterítette szervezeti szinten a zsarolóvírust,

[37] A Taiwan International Cooperation and Development Fund által szervezett 2022. június 21-i *Webinar on Digital Governance* című konferencián, Rufus Lin (Belügyminisztérium Nemzeti Rendészeti Ügynökség Információ Menedzsment Irodájának Igazgatója) *Fighting High Tech Crime Experience in Taiwan* című előadása alapján.

[38] Yang–Chung 2014.

[39] Huang 2018.

majd hajnalban aktiválta a programot, így az titkosította az adatokat.[40] Bár a támadás nem érintette a vállalat energiatermelését, egyes ügyfelek esetében megzavarta a vállalat által kiadott kártyákkal lebonyolított fizetési tranzakciókat.[41] A CyCraft Technology Corp elemzésében az APT10 tevékenységére utaló bizonyítékokat talált, amely több hátsó kaput, köztük a *CobaltStrike backdoor*-t kihasználva juttathatta be a rendszerbe a *ColdLock* zsarolóvírust. A vállalat malware-elemzésének eredményei alapján a ColdLock eltávolította az összes fizetési információt, a kapcsolattartó e-mail-címét és az RSA nyilvános kulcsot, amelyek mind információként szolgálhattak volna a titkosítás feloldásához.[42] 2020 májusában zsarolóvírus-támadás ért 10 másik kritikusinfrastruktúra-üzemeltető szervezetet is, köztük a Chunghwa Telecom-ot.

2020 augusztusában legalább 10 kormányzati intézményt ért támadásra derült fény: a *Waterbear malware* mintegy 6000 e-mail-címet kompromittált, így bizalmas információk és személyes adatok is érintettek voltak. A tajvani kiberbiztonsági nyomozó osztály attribúciója két kínai hátterű hackercsoport – az úgy nevezett Blacktech (APT10) és Taidoor csoportok – tevékenységére talált bizonyítékot. A nyomozóhivatal igazgatóhelyettese, Liu Chia-zung egy 2020-as interjúban elmondta, hogy a támadók céljaként, az adatlopás mellett, a bizalmas adatok kiszivárogtatása sem kizárható. A hálózati behatolás legkorábbi időpontját ebben az esetben is 2018-ra vezették vissza a szakemberek. A kampányban legalább négy tajvani technológiai cég is érintett volt, amelyek mind kormányzati beszállítók voltak.[43]

5. Nemzetközi együttműködések és gyakorlatok

Tajvan számos nemzetközi kooperációs platformon van jelen, sokrétű technikai jellegű tevékenységgel, így kiberdiplomáciai mozgásterének alapját is ezek a képességei adják, főként a Nemzeti Kiberbiztonsági Technológiai Központ, a TWNCERT és a kormányzati Kiberbiztonsági Osztály munkája nyomán. Tajvan nemzetközi kiberbiztonsági együttműködési lehetőségeinek egyik fő sarokköve az APCERT- (Asia Pacific Computer Emergency Response Team) tagság, amelyen keresztül nemzetközi szimuláción vett részt 2018 májusában (Data Breach via Malware on IoT),[44] 2019 júliusában (Catastrophic Silent Draining in Enterprise Network)[45] és 2020 márciusában (Banker doubles down on Mining).[46] Az együttműködés másik területe a technikai képzések megtartása az APCERT Képzési Munkacsoportjában (Training Working Group), amelyben Tajvan minden évben részt vett oktatóként a TWNCERT 2018–2021-es éves beszámolói alapján.[47]

[40] A Taiwan International Cooperation and Development Fund által szervezett 2022. június 21-i *Webinar on Digital Governance* című konferencián, Jyan Hong-wei (Végrehajtó Jüan Kiberbiztonsági osztályának volt igazgatója) *National Cyber Security Program of Taiwan* című előadása alapján.
[41] Lyngaas 2020.
[42] Cycraft Technologies Corp 2021.
[43] Lee 2020; CyCraft Technology Corp 2020.
[44] *Taiwan National Computer Emergency Response Team Annual Report 2018.* 2019. 8.
[45] *Taiwan National Computer Emergency Response Team Annual Report 2019.* 2020. 8.
[46] *Taiwan National Computer Emergency Response Team Annual Report 2020.* 2021. 9.
[47] *Taiwan National Computer Emergency Response Team Annual Report (A TWNCERT éves beszámolói.)* 2022.

Az államközi együttműködések kapcsán a megkérdezett szakértő kiemelte, hogy Tajvan minden évben megrendezi a Cyber Offensive and Defensive Exercise (CODE) gyakorlatot, amely kétévente (2019-ben és 2021-ben) egy alkalommal nemzetközi résztvevőket is fogad, általában a támadó fél szimulálásához. Az interjúalany azt is megerősítette, hogy Tajvan, az irányába mutatott nyitott és barátságos hozzáállású, bármely nemzetközi szervezettől és országtól érkező együttműködési lehetőségre nyitott. Jellemzően a közös védelem *(joint defence)* jegyében valósulnak meg az együttműködések, amelyben Tajvan szívesen megosztja a fenyegetésekről gyűjtött információit és az általuk szerzett tapasztalatokat, például a CODE-gyakorlatok alkalmával.

Egyes sajtóorgánumok szalagcímei „kiberháborús gyakorlatként" emlegették a 2019. novemberi négynapos 2019 CODE multinacionális, hálózatbiztonsági gyakorlatot, amelyet az Amerikai Intézettel (American Institute in Taiwan, az USA képviseleti szervezete) együtt szerveztek meg Tajvanon. A gyakorlat közös megtartása azért is jelentős diplomáciai előrelépésnek számított, mert Tajvan mégsem kapott meghívást az Egyesült Államok által szervezett 2018. tavaszi Cyber Storm nemzetközi gyakorlatra. A korábbi helyzetgyakorlatoktól eltérően a 2019-es CODE teljes körű szimuláció volt, amelyet pénzügyi kiberbiztonsági környezetre terveztek. A nemzetközi résztvevők a tajvani pénzügyi szervezetek szakembereivel alkottak integrált csapatokat, hogy fejlesszék mindkét szerepkör technikai és reagáló képességeit.[48] A TWNCERT 2019-es jelentése alapján a gyakorlaton részt vevők 4 támadó csapatot *(Red team)* alkottak, közülük egyet-egyet Malajzia (MyCERT) és a Cseh Köztársaság (NCISA) alkotott, kettőt pedig a tajvani kormányzati ügynökségek. A két védekező csapat *(Blue team)* 14 tajvani banki alkalmazottból állt.[49]

A 2020-as évben a TWNCERT részt vett az Iszlám Együttműködés Szervezete (OIC-CERT) által tartott gyakorlaton (Cyber Drill), valamint a CyberEx gyakorlaton, amelyet a Spanyol Nemzeti Kiberbiztonsági Intézet (INCIBE-CERT) vezetett.[50] Feltehetőleg a 2020. májusi CPC Corp energiavállalatot ért támadástapasztalat feldolgozásának jegyében, a 2020-as évhez hasonlóan, a TWNCERT 2021-es Cyber Offensive and Defensive Exercise (CODE 2021) nemzetközi gyakorlatán ismét energiaipari létfontosságú információs infrastruktúrát (CII) érő támadást szimuláltak. A CODE 2021-en 20 nemzetből érkeztek résztvevők, így összesen 31 állami és magánszervezet vett részt Red vs. Blue team felállásban. Az interjúalany hozzátette, hogy tíz különböző állam csatlakozott hivatalosan az eseményhez, az érkező szakemberek három támadó csapat felállítását tették lehetővé. A TWNCERT belföldi (úgynevezett Nemzeti Kiberbiztonsági Gyakorlat) helyzetgyakorlatokat is tartott a kormányzati szervek részére, amelyek közt a *social engineering* szimulációt és az incidensreagáló képességek fejlesztését célzó gyakorlatot nevesítették.[51]

Arra a kérdésre, hogy miként reagáltak a régió országai Tajvan offenzív kiberképességek kiépítésére irányuló erőfeszítéseire, a szakértő elmondta, hogy Tajvan nem offenzív képességként tekint a fejlesztésre, hanem proaktív védelemként, amellyel céljuk, hogy megállítsák a támadást annak folyamatában, vagy mielőtt kifejtené

[48] Department of Information Services, Executive Yuan 2019; BBC News 2019.
[49] National Center for Cyber Security Technology 2019. 7.
[50] *Taiwan National Computer Emergency Response Team Annual Report 2020.* 2021. 9.
[51] *Taiwan National Computer Emergency Response Team Annual Report 2021.* 2022. 7.

károkozó hatásait. Az utolsó interjúkérdés arra kereste a választ, hogy Tajvan miként látja szerepét a nemzetközi közösségben, milyen kiberdiplomáciai célkitűzései vannak. Az interjúalany elsősorban az ország kibertéri védelmét növelő eszközként tekint a kiberdiplomáciai lehetőségeikre. Ezt kiegészítve a konferencia házigazdája, a tajvani Nemzeti Chengchi Egyetem Közigazgatási Karának professzora úgy írta le Tajvan nemzetközi látásmódját, miszerint nagyon komolyan számol a kiberháború veszélyével és lehetőségével.

6. Összegzés és konklúzió

A szakértői interjún kapott válaszok alapján az a következtetés vonható le, hogy Tajvan a kibertérből érkező fenyegetéseket akképp igyekszik csökkenteni kiberdiplomáciai eszközökkel, hogy nemzetközi információmegosztáson (riasztási információk, *threat intel, forensics* és malware-elemzések megosztása) alapuló hálózatot épít régión belüli partnereivel és az USA-val. A Kínához fűződő speciális helyzete ellenére az utóbbi öt évben részt tudott venni nemzetközi kiberbiztonsági szimulációs gyakorlatokon, amelyek mellett az általa rendszeresen megszervezett CODE nemzetközi gyakorlatokon folyamatosan képes az állami szervek szakemberállományának technikai készségeit emelni. Tajvannak más irányba is bővítenie kell kiberdiplomáciai mozgásterét, amire a 2021–2024-es Nemzeti Kiberbiztonsági Program tudásmenedzsmentre vonatkozó célkitűzései alkalmasak lehetnek. A tervben előirányozottak sikeres megvalósítása regionális szintű (és világszínvonalú) tudásközponttá emelnék Tajvant, amiből a belföldi IKT-ipar és az akadémiai szféra is profitálna a tervezett Kiberbiztonsági Kiválósági Központon keresztül.

A belföldi kiberbiztonsági piac támogatása egyrészt a nemzeti infrastruktúra korszerűsítését szolgálja, másrészt a Nemzeti Kiberbiztonsági Programban körvonalazott állami megfelelőségi tanúsítvány bevezetése az IoT-eszközökre és a rendszeres állami auditok további bizalmi garanciákat adhatnak a tajvani félvezető- és chipgyártók fogyasztóinak, valamint az IKT-szektor piacának. Ezen intézkedések hatására erősít rá a Tajvan által képviselt diplomáciai szerepkör, amelyben a regionális kiberbiztonsági szintnövelés egyik előmozdítójaként kíván megjelenni, az információmegosztást és kooperációt promulgáló szereplőként. Tajvan emellett felhasználja a dezinformációs kampányok kezeléséből és a kormányzatot érő támadásokból származó tapasztalatát, és incidenskezelési kompetenciáját helyezi a kiberdiplomáciai kapcsolatok megindításának mérlegére.

A kibervédelmi reformok és a kiberdiplomáciai aktivitás értékelése alapján az a konklúzió vonható le, hogy a Tsai-elnökség stratégiai autonómiára törekszik a kibertérben, amellyel célja, hogy ebben a védelmi ágazatban Kína ne tudja nemzetközileg elszigetelni, így akadályozva képességeinek korszerűsítését. Tajvan számára a kibertér védelme egyet jelent a szürke zónás és hibrid fenyegetések elleni felkészültséggel és a nemzetgazdasági húzóágazatok prosperálásával, míg a nemzetközi közösség számára Tajvan kibertéri biztonsága összefonódik a különböző gazdasági szektorokkal, például az elektronikai és autóipari ellátási láncokban betöltött szerepe okán. Ennélfogva Tajvan védelmi ipari fejlesztési lehetőségeit és korlátait figyelembe

véve, katonai szempontból a kibertér jelentheti azt az ágat, amelyben önerejére és, érdekegyezés alapján, a nemzetközi közösség segítségére is számíthat a területvédelemhez szükséges hiteles elrettentési képesség felépítésére. Ez is jól mutatja, hogy a tajvani védelempolitikai stratégia, „*Eltökélt védelem, több dimenzióra kiterjedő elrettentés*" koncepciójának első védelmi rétegeként miért a kibertér van megnevezve. A minél ütőképesebb és szélesebb körű – offenzív és defenzív – képességekkel rendelkező kibertéri erő kialakításával és folyamatos korszerűsítésével a diplomáciai erőfeszítések elérhetik, hogy Tajvan más védelmi szektorban is kimozduljon a kínai diplomáciai nyomás alól, vagy kiegyensúlyozottabb erőviszonyokon alapuló szoros-menti kapcsolatokat tartson fenn.

KK1:

A tanulmány első kutatási kérdése arra vonatkozott, hogy Tajvan elrettentési koncepció mentén felépülő kibervédelmi stratégiája milyen lehetőségeket nyit, és milyen korlátokat szab Tajpej kiberdiplomáciai mozgásterének. A tajvani IT-ipari termékek jelentősége, a kiberbiztonsági szakemberek incidenskezelési tapasztalata és szakértelme kiegészülve a proaktív védelmi képességekkel komoly nemzetközi figyelmet irányított Tajpejre. A tajvani diplomácia azt a tőkét, amelyet a technikai képességek nemzetközi gyakorlatokon való demonstrálásával, valamint a szaktudás szakmai fórumokon és képzéseken történő átadásával halmozott fel, kibertéri fenyegetettségekkel kapcsolatos hírszerzési és elemzési információkra tudta váltani, ám politikai, stratégiai értékű együttműködést még nem tudott megvalósítani regionális partnereivel vagy az USA-val, a bonyolult Kína-kapcsolatok miatt.

H1:

Ebben a kontextusban vizsgálva az első hipotézist, miszerint Tajvan kiberdiplomáciai mozgásterének növelése érdekében arra törekszik, hogy további militarizálás nélkül, kooperatív eszközökkel növelje kiberbiztonsági szintjét, mivel stratégiai érdeke, hogy a régiós biztonsági dilemma ne terjedjen tovább a kibertérben, csak részben tekinthető helytállónak. A kooperatív eszközök, mint amelyeket a 2021–2024-es Nemzeti Kiberbiztonsági Program tudásmenedzsment céljaiban, illetve az állami és magánszféra IKT-ipar, valamint kiberbiztonság területein megvalósuló kooperációjának előmozdítására tett intézkedésekben fektetett le, ugyanúgy hozzájárulnak a kiberdiplomáciai mozgástér bővítéséhez, mint a gyakorlati képességek a proaktív védelemi stratégia adaptációjával. Mindkét módszer szükséges a kibervédelmi stratégiai autonómia eléréséhez. Emellett lényeges az a politikai narratíva is, amelyre a szakértői interjú hívta fel a figyelmet, hogy Tajvan az offenzív képességeit proaktív védelemként definiálja, habár az magában hordozza a csapásmérés lehetőségét is. Összességében a kiberhadviselési képességek bármelyike indukálhatja a kelet-ázsiai biztonsági komplexumban a kibertér militarizálását, ami végső soron geopolitikai okok miatt csökkenti a kibertér biztonsági szintjét. Az északkelet-ázsiai biztonsági

szubkomplexum militarizációs trendjei és fenyegetettségpercepciói már jelenleg is érvényesülnek a kibertérben, így a folyamat öngerjesztővé válhat, ami kedvezőtlen a régió összes államára nézve, amelyek IT-ipari nagyhatalmak. Tajvan viszont akár előnyére is fordíthatja ezt a helyzetet, mivel gazdasági húzóágazatai – a félvezetők és a microchipek gyártása – alaptermékként szolgálnak például Kína IT-iparának. Ezt a gondolatmenetet támasztja alá Tsai Ing-wen elnök asszony niche piac (réspiac) erősítésére utaló beszédének részlete, miszerint Tajvannak „nélkülözhetetlenné és pótolhatatlanná kell válnia a világban" biztonságának garantálásához.

KK2:

A második kutatási kérdés arra kereste a választ, hogy értékelhető-e a Tajvant érő kibertámadások volumene és összetétele információs műveletekként. Tekintettel a kutatás azon korlátjára, miszerint az információs műveletek fogalmába beletartozó képi és rádióelektronikai felderítés, valamint elektronikai hadviselés esetpéldáiról, továbbá ezek súlyosságának mértékéről nem áll rendelkezésre részletes, publikus információ, nem lehet objektív választ alkotni. Mindazonáltal a dezinformációs kampányok okozta fenyegetés és az APT-jelenlét esetpéldái önmagukban nem tekinthetők információs műveleteknek, annak ellenére, hogy súlyosan érintik a pszichológiai dimenziót és állami hátterű, szofisztikált számítógép-hálózati műveletek voltak.

H2:

A kutatás fent említett korlátait figyelembe véve, a tanulmányban felsorakoztatott esetpéldák, valamint a kiemelkedően magas incidensszám összetevőinek elemzése részben alátámasztja a második hipotézist, amely a tajpeji politikai fordulatra reagáló, szürke zónás műveletek közé sorolja a KNK kibertéri aktivitását. Ezzel kapcsolatban az a kiegészítés tehető, hogy a szürke zónás műveletek volumene és az általuk generált konfliktus intenzitása igen magas, amit súlyosbít a PLA aktív katonai tevékenysége a tajvani szorosban és az ukrajnai háborúval kapcsolatos helytelen párhuzamok, amelyeket mindkét fél tagad.[52]

Tajvan kiberbiztonsági körképének megismerése nyomán Magyarország az alábbi ajánlások mentén profitálhat:

- A tajvani Nemzeti Közös Védelmi Rendszerhez hasonló nemzeti SOC-, CSIRT- és ISAC-képességeket integráló struktúra kialakításának megkezdése.
- A fentiekhez kapcsolódó tudás- és tapasztalatcsere érdekében, a diplomáciai érdekek vizsgálata mellett, megfontolandó a magyar nemzeti kiberbiztonsági szervezetek és a tajvani szervezetek közti technikai és akár más területen megvalósuló kooperáció előmozdítása, valamint az akadémiai, gyakorlati és kutatói tudásmenedzsment-lehetőségek és -kezdeményezések kiaknázása.

[52] Portfolio 2022.

- A tajvani Nemzeti Kiberbiztonsági Programban és fejlesztési tervekben megfogalmazott célok átültetése a magyar kiberbiztonsági struktúrába és környezetbe.
- A tajvani dezinformáció elleni kezdeményezések magyarországi megvalósíthatóságának vizsgálata és alkalmazása.

Felhasznált irodalom

AFP (2021): Taiwan Government Faces 5 Million Cyber Attacks Daily: Official. *The Guardian,* 2021. november 10. Online: https://guardian.ng/news/world/taiwan-government-faces-5-million-cyber-attacks-daily-official/

Allen-Ebrahimian, Bethany (2021): Report: Beijing Flooded Taiwan with Coronavirus Disinformation. *Axios China,* 2021. május 24. Online: www.axios.com/2021/05/24/report-beijing-taiwan-coronavirus-disinformation

Bartók András – Wagner Péter (2020): A kínai A2/AD és a válaszreakciók Kelet-Ázsiában (1). In *KKI-elemzések* E-2020/69. szám. Budapest, Külügyi és Külgazdasági Intézet. 3–12. Online: https://kki.hu/wp-content/uploads/2020/08/E-2020_69_kina-kelet_azsia.pdf

BBC News: US and Taiwan Hold First Joint Cyber-War Exercise. *BBC,* 2019. november 4. Online: www.bbc.com/news/technology-50289974

Blanchette, Jude – Livingston, Scott – Glaser, Bonnie – Kennedy, Scott (2021): Protecting Democracy in an Age of Disinformation: Lessons From Taiwan. *CSIS,* 2021. január 27. Online: https://apo.org.au/node/310698

Cheung, Eric – Ripley, Will – Tsai, Gladys (2021): How Taiwan Is Trying to Defend Against a Cyber ‚World War III'. *CNN Business,* 2021. július 23. Online: https://edition.cnn.com/2021/07/23/tech/taiwan-china-cybersecurity-intl-hnk/index.html

CyCraft Technology Corp (2020): *China Implicated in Prolonged Supply Chain Attack Targeting Taiwan Financial Sector,* 2022. február 22. Online: https://medium.com/cycraft/china-implicated-in-prolonged-supply-chain-attack-targeting-taiwan-financial-sector-264b6a1c3525

CyCraft Technologies Corp (2021): *China-Linked Threat Group Targets Taiwan Critical Infrastructure, Smokescreen Ransomware*. (2021. június 2.) Online: https://medium.com/cycraft/china-linked-threat-group-targets-taiwan-critical-infrastructure-smokescreen-ransomware-c2a155aa53d5

Department of Information Services, Executive Yuan (2019): *Taiwan and US Co-hosting Multinational Cybersecurity Exercise.* (2019. november 9.). Online: https://english.ey.gov.tw/Page/61BF20C3E89B856/0f357b66-7ed3-4123-98c6-b91097b82536

Gálik Mihály (2019): A hálózati hírmédia sajátosságai különös tekintettel a visszhangkamra- és a szűrőbuborék-jelenségre. *In Medias Res*, 2019. december 19. Online: https://media-tudomany.hu/2019/12/19/a-halozati-hirmedia-sajatossagai-kulonos-tekintettel-a-visszhangkamra-es-a-szurobuborek-jelensegre/

Her, Kelly (2021): Defending Cyberspace. *Taipei Times,* 2021. május 1. Online: https://taiwantoday.tw/news.php?unit=8&post=200638&unitname=Economics-Taiwan-Review&postname=Defending-Cyberspace

Huang, Hsini (2018): A Collaborative Battle in Cybersecurity? Threats and Opportunities for Taiwan. *Asia Policy, National Bureau of Asian Research,* 15. évf. 2. sz. 101–106. Online: https://doi.org/10.1353/asp.2020.0015

Huang, Hsini – Li, Tien-Shen (2018): A Centralised Cybersecurity Strategy for Taiwan. *Journal of Cyber Policy,* 3. évf. 3. sz. 344–362. Online: https://doi.org/10.1080/23738871.2018.1553987

Kínai Népköztársaság Külügyminisztériuma (2022): *Zhao Lijian szóvivő nyilatkozata a 2022. április 15-i rendes sajtótájékoztatón.* (2022. április 15.). Online: http://cy.china-embassy.gov.cn/eng/fyrth/202204/t20220415_10668556.htm

Lee, Yimou (2020): Taiwan Says China Behind Cyberattacks on Government Agencies, Emails. *Reuters,* 2020. augusztus 19. Online: www.reuters.com/article/us-taiwan-cyber-china-idUSKCN25F0JK

Lyngaas, Sean (2020): Taiwan's State-Owned Energy Company Suffers Ransomware Attack. *CyberScoop,* 2020. május 5. Online: www.cyberscoop.com/cpc-corp-ransomware-attack-taiwan-trend-micro/

Portfolio (2022): Dől a következő dominó? Menekül a tőke Tajvanból. *Portfolio,* 2022. március 8. Online: www.portfolio.hu/uzlet/20220309/dol-a-kovetkezo-domino-menekul-a-toke-tajvanbol

Rawnsley, Gary D. (2005): Old Wine in New Bottles: China–Taiwan Computer-Based 'Information Warfare' and Propaganda. *International Affairs,* 81. évf. 5. sz. 1061–1078. Online: https://doi.org/10.1111/j.1468-2346.2005.00502.x

Strong, Matthew (2021): Taiwan Government Departments Targeted by Hackers 5 Million Times per Day. *Taiwan News,* 2021. november 10. Online: www.taiwannews.com.tw/en/news/4340699

Taddeo, Mariarosaria (2018): How to Deter in Cyberspace? *Strategic Analysis.*

Taiwan National Center for Cyber Security Technology Annual Report 2019. 2020. Online: www.twncert.org.tw/Download/NCCST%20Annual%20Report%202019.pdf

Taiwan National Center for Cyber Security Technology (2022): *About NCCST: 6th Phase of National Cyber Security Program*, 2022. augusztus 30. Online: www.nccst.nat.gov.tw/About?lang=en

Taiwan National Computer Emergency Response Team Annual Report 2018. 2019. Online: www.twncert.org.tw/Download/TWNCERT%20Annual%20Report%202018.pdf

Taiwan National Computer Emergency Response Team Annual Report 2020. 2021. Online: www.twncert.org.tw/Download/TWNCERT%20Annual%20Report%202020.pdf

Taiwan National Computer Emergency Response Team Annual Report 2021. 2022. Online: www.twncert.org.tw/Download/TWNCERT%20Annual%20Report%202021.pdf

Tajpej Képviseleti Iroda (Magyarország) (2018): *Tsai elnök asszony ígérete egy erősebb Tajvan építésére nemzeti napi beszédében.* Taipei Representative Office in Hungary – Taiwan Today, 2018. november 9. Online: www.roc-taiwan.org/hu_hu/post/1919.html

Tajvan Külügyminisztériuma (2022): *Fact Focus. Mass Media.* Online: www.taiwan.gov.tw/content_11.php

Yang, Yuan-ting – Chung, Jake (2014): Apple Daily Slams Hack Attack. *Taipei Times,* 2014. június 19. Online: www.taipeitimes.com/News/front/archives/2014/06/19/2003593115

Yau, Hon-min (2019): A Critical Strategy for Taiwan's Cybersecurity: A Perspective From Critical Security Studies. *Journal of Cyber Policy,* 4. évf. 1. sz. 35–55. Online: https://doi.org/10.1080/23738871.2019.1604782

Yau, Hon-min (2020): *Evolving Toward a Balanced Cyber Strategy in East Asia: Cyber Deterrence or Cooperation? Issues & Studies,* 56. évf. 3. sz. Online: https://doi.org/10.1142/S1013251120400111

Yu, Jess Macy – Blanchard, Ben (2018): Chinese Cyber Attacks on Taiwan Government Becoming Harder to Detect. *Reuters,* 2018. június 15. Online: www.reuters.com/article/us-taiwan-china-cybersecurity-idUSKBN1JB17L

HADMÉRNÖK
VÉDELEMINFORMATIKA
17. évfolyam (2022) 4. szám 153–174.
DOI: 10.32567/hm.2022.4.10

István Paráda,[1] András Tóth[2]

Possible Scenario for Malware Exploit Investigation with Data-Driven Architecture[3]

In this article, the authors present a data-driven architecture-based malware exploit analysis as the next part of the Penetration Testing article series. The analysis contributes greatly to investigating malicious attacks, which are becoming increasingly sophisticated in cyberspace, thus posing a significant threat to the information and communication networks of state and non-state actors. To achieve their research objectives, the authors use analytical evaluation methods to define the principles, modular elements and procedures of the data-driven architecture to be applied, where decisions are made based on the available data. On this basis, they have presented an analytical process that can help the public and defence sectors to analyse this type of attack, thus facilitating recovery processes.

Keywords: **Metasploit, Metasploit Framework, vsFTPd, NMAP, TCP, FTP**

Thanks to increasingly sophisticated protection, logging and analysis techniques, we have much more information available to investigate an incident. There are a few basic reasons why there has recently been so much emphasis on data-driven information. First, technological advances in computing and networking capacity have made it possible to publish and transmit unprecedented amounts of data. Second, technological advances in artificial intelligence have helped us analyse these vast amounts of data in ways that were impossible before. These two factors lead to many cases where a machine can draw conclusions from the data and make (better) decisions based on the results.

In response to the volume and sophistication of malware, security experts rely on data-driven architecture analysis to detect malicious activities and software. Data-driven architectural analysis is the process of running binary patterns by experts to produce reports that summarise their real runtime behaviour. These reports can be

[1] PhD student, University of Public Service, e-mail: paradaistvan@gmail.com
[2] Associate Professor, University of Public Service, e-mail: toth.hir.andras@uni-nke.hu
[3] The research was financed by the National Research Development and Innovation Office Fund and was implemented in the funding of the Thematic Program of Excellence 2020 application program number TKP2020-NKA-09.

used to identify malware and determine attributes of threat types. They are crucially important in the government and defence sectors, where there are many critical information infrastructures, the loss of which could seriously compromise the functioning of the state or one of its critical infrastructures. Therefore, frameworks and procedures to prevent and deter malicious activities in these areas are of paramount importance.

In preparing this paper, the authors' main goal was to develop a framework to help investigate the increasingly sophisticated malicious attacks in cyberspace. For this purpose, the authors used analytical evaluation methods to define the principles, modular elements and procedures of the data-driven architecture to be applied. Data-driven means that decisions are made based on the available data.

This study develops a framework for malware detection and threat family identification using supervised machine learning techniques. The developed framework can support the work of professionals performing tasks in e-government, state and non-state actors' digitisation in cybersecurity incident detection and recovery. The results show the efficiency and portability of our solutions across a wide range of analyses and settings.

To achieve the best results, the authors chose Elasticsearch software, a real-time technology that allows working with all volumes with different APIs (from gigabytes to petabytes). Besides Kibana, many different solutions can take advantage of the open APIs offered by Elasticsearch and build visualisations on the resulting data, but Kibana is the only technology dedicated to this.

1. Data-driven architecture

Data can typically be anything. Accordingly, we can talk about business data, infrastructure data, accounting data, structured or unstructured data and personal data. For any organisation (public or non-public), extracting the value of data from huge data sets is a huge challenge, which helps to extract useful information from the data. This is typically challenging due to the following factors:

- Data complexity: Huge amounts of data, mostly from many different data sources and containing much useless information (noise).
- Data from various sources: Data can come from many sources that are not relevant to an organisation. For example, they can be legacy systems or databases, infrastructures, tools, or applications that are irrelevant to the organisation. These should be continuously monitored and validated.
- The volume of data is growing very fast: Managing it is a major challenge for all organisations. Therefore, particular attention must be paid to scaling the data management infrastructure to make it easier to determine which data should be retained.

In their paper, Wang et al. discussed data-driven architectures in 5G as the communication part of critical infrastructures. In the article, they formulated the following requirements that the architecture should meet:

- The architecture must monitor the applications used by users and the Quality of Service (QoS) status in real-time.
- The architecture must maintain a data mining system that can predict user preferences/expectations for the applications used.
- The architecture should manage communication resources based on the QoS state and predicted preferences/expectations to maintain a satisfactory Quality of Experience (QoE).[4]

Numerous features can be added to this in the design of public and defence communication systems. There, special attention must be paid to the management of sensitive data, so it is not enough to monitor and analyse user applications but also to pay special attention to solutions such as endpoint protection, encryption procedures, intrusion prevention and detection services. In principle, they are not only present in communication networks but must be applied to all systems using information and communication technologies (ICT). Accordingly, they should be applied to all areas of the public and defence sectors, such as smart cities,[5] power grid systems,[6] industrial control systems[7] and healthcare, among others.

The elements of the data-driven architecture that support the above requirements to be fully met are important. In the architecture case, data transport, data ingest, data storage at scale and data visualisation play a key role.

1.1. Data ingest

The data ingestion layer is responsible for receiving data, which includes commonly used transport protocols and data formats, while providing the ability to extract and transform data before final storage. From our perspective, data processing is the extraction, transformation, and loading of data, often referred to as the input pipeline, and essentially receives data from the transport layer to push it into a storage layer. It has these functions:

- In general, the ingestion layer has a pluggable architecture to facilitate integration with different data sources and destinations, using a set of plugins. Some of the plug-ins are designed to receive data from senders, which means that the data does not always come from the sender and can be delivered directly from a data source such as a file, a network or even a database.
- The data ingestion layer is used to prepare data, for example by analysing, formatting, correlating data with other data sources, and normalising and enriching data before storage. There are many improvements, but the most important is that it improves the quality of the data, providing better observations for visualisation.

4 Wang et al. 2017
5 Fang et al. 2021
6 Jia et al. 2018
7 Wang et al. 2018

- Data input and transformation consume computational resources. It is essential to take this into account, usually in terms of maximum data throughput per unit, and to plan the load by distributing the input over several data input instances. This is an essential aspect of real-time, or more precisely near real-time, visualisation.

1.2. Data shipping

The architecture must be able to transport any structured or unstructured data/event; in other words, it transports data from remote machines to a central location. This is usually done by a lightweight agent deployed on the same machine as the data sources or, in different aspects, on a remote machine:

- Lightweight because, ideally, it should not compete for resources with the actual process that produces the data; otherwise, it may reduce the expected performance of the process.
- There are many data transport technologies; some are tightly coupled to a specific technology; others are based on an extensible framework that is relatively adaptable to the data source.
- Data transport is not only about sending data over the wire but also about security and ensuring that the information is delivered to the right destination via an end-to-end secured pipeline.
- Another aspect of data transport is the management of data loading. Data transport must be done in proportion to the load the end destination can accommodate; this function is called backpressure management.

1.3. Storing data at scale

This ensures the basic, long-term preservation of data. In addition, it provides the essential functionality to search, analyse and discover insights into the data.

The storage layer generally provides:

- Scalability is the main aspect, with storage used for different data volumes, starting from gigabyte (GB), terabyte (TB) and petabyte (PB).
- A non-relational and highly distributed data store is usually used, allowing fast data access and analysis on large volumes and different data types, namely a NoSQL data store.
- For data visualisation, the repository must publish an application programming interface (API) for data analysis. Allowing the visualisation layer to perform statistical analysis, such as grouping data by a given dimension, would not scale.

1.4. Visualising data

In a data-driven architecture, the visualisation layer is one of the potential data consumers and mostly focuses on bringing key performance indicators (KPIs) to the stored data. It has the following basic functions:

- It should be lightweight and only display the result of the processing done in the storage layer.
- Allow the user to explore the data and quickly get out of the box.
- It brings a visual way to ask unexpected data questions, rather than having to perform a corresponding prompt.
- Modern data architectures need to meet accessibility needs.
- KPIs should be as fast as possible, and the visualisation layer should display data in near real-time.
- The visualisation framework should be extensible and allow users to customise existing tools or add new functionality depending on their needs.

2. Overview of the elastic stack

The Elastic stack, formerly called ELK from the acronym of three open-source projects: Elasticsearch, Logstash and Kibana, ensures the different layers needed to implement a data-driven architecture. The first is the ingestion layer with Beats and Logstash, the second is a distributed data store with Elasticsearch and the third is the visualisation with Kibana.

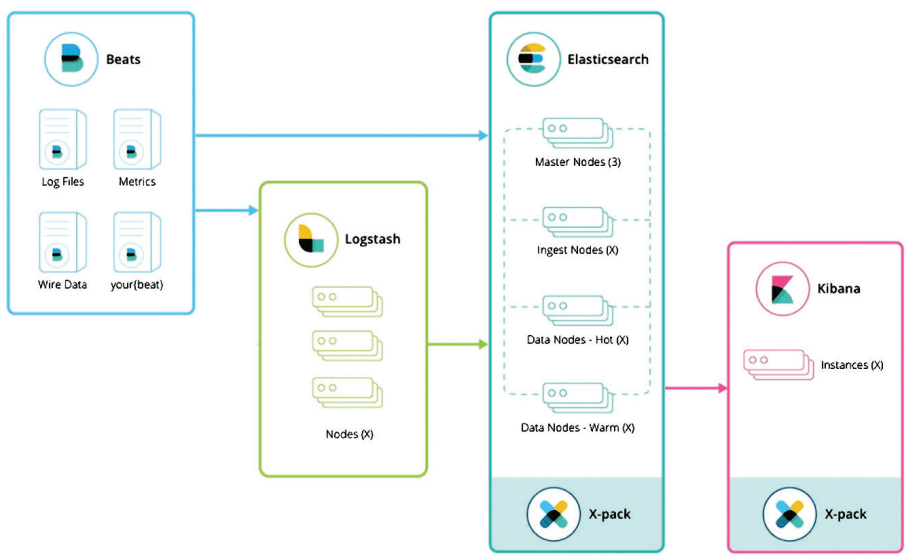


Figure 1: The elastic stack structure
Source: Azarmi 2017

2.1. Elasticsearch

Elasticsearch is a distributed and scalable data store from which Kibana pulls all aggregation results used in the visualisation. It is flexible and scalable by nature, so nodes can be added to the Elasticsearch cluster very easily, depending on the needs. Furthermore, Elasticsearch is a highly available technology, which means that:

First, data is replicated within the cluster, so at least one copy of the data is preserved in the event of a failure.

Secondly, due to its distributed nature, Elasticsearch can distribute the indexing and search load across the cluster nodes, ensuring service continuity and service level agreement (SLA) compliance.

Structured and unstructured data can be handled, and as the data is visualised in Kibana, it is noticeable that the data, or using Elasticsearch's vocabulary, documents are indexed in JavaScript Object Notation (JSON) documents. In addition, JSON makes it very practical to handle complex data structures as it supports nested documents, arrays, etc.

Elasticsearch is a developer-friendly solution that offers several REST APIs for interacting with data or cluster settings. Documentation for these APIs can be found at www.elastic.co/guide/en/elasticsearch/reference/current/docs.html.

In addition to these APIs, client APIs allow Elasticsearch to integrate with most technologies such as Java and Python.

Kibana generates the requests to the cluster for each visualisation. The final key aspect of Elasticsearch is that it is a real-time technology that allows working on volumes ranging from gigabytes to petabytes using a variety of APIs. In addition to Kibana, several other solutions can leverage the open APIs offered by Elasticsearch to build visualisations on top of data; but Kibana is the only technology dedicated to this.[8]

2.2. Beats

Beats is a lightweight data transporter that delivers data from various sources, such as applications, end devices, or networks. Beats is built on an open-source library that allows the beat to send data to Elasticsearch, as shown in the following image.

The diagram shows the following Beats:

- Packetbeat essentially looks for packets over the network wire for certain protocols such as MySQL and HTTP. It captures all the basic metrics used to monitor a given protocol. For example, HTTP receives the request and response, wraps them in a document, and indexes them in Elasticsearch.
- Filebeat is used to safely transport the contents of a file from point A to point B in a similar way to the tail command. This beat can be used with the new

[8] GoLinuxCloud 2020

ingest node (www.elastic.co/guide/en/elasticsearch/reference/master/ingest.html) to transfer data directly from the file to Elasticsearch, which processes it before indexing.

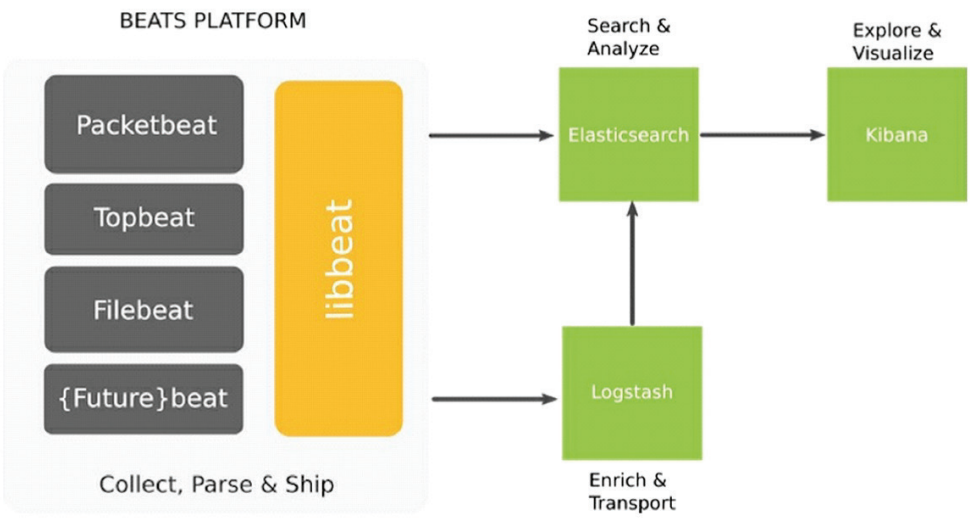


Figure 2: The Beats architecture
Source: Azarmi 2017

2.3. Ingestion pipeline without ingest

As shown in the previous figure, the data is first delivered by Beats, then sent to a message broker, after which it is processed by Logstash and indexed by Elasticsearch. The disadvantage of Beats is that it has some basic filtering functions, but these do not provide the level of transformation that Logstash can provide.

2.4. Ingestion pipeline with Ingest node

As shown in Figure 2, the architecture is reduced to two components using the filebeat and ingest node, and then the content is rendered in Kibana. To send machines or bapplication execution samples to Elasticsearch, we can use Topbeat, the first Metricbeat that allows us to do this. We also used this solution to transport our applied computer data and visualise it in Kibana during the test. A huge advantage of this solution is that this beat comes with pre-made templates that are standardised; accordingly, the templates received just need to be imported into Kibana for visualisation.

While Beats does offer some basic filtering features, they do not offer the level of conversion that Logstash does.

2.5. Logstash

Logstash is a data processor that uses a centralised data processing paradigm. It allows users to collect, enrich/transform and deliver data to destinations using more than 200 extensions, as shown in Figure 3.

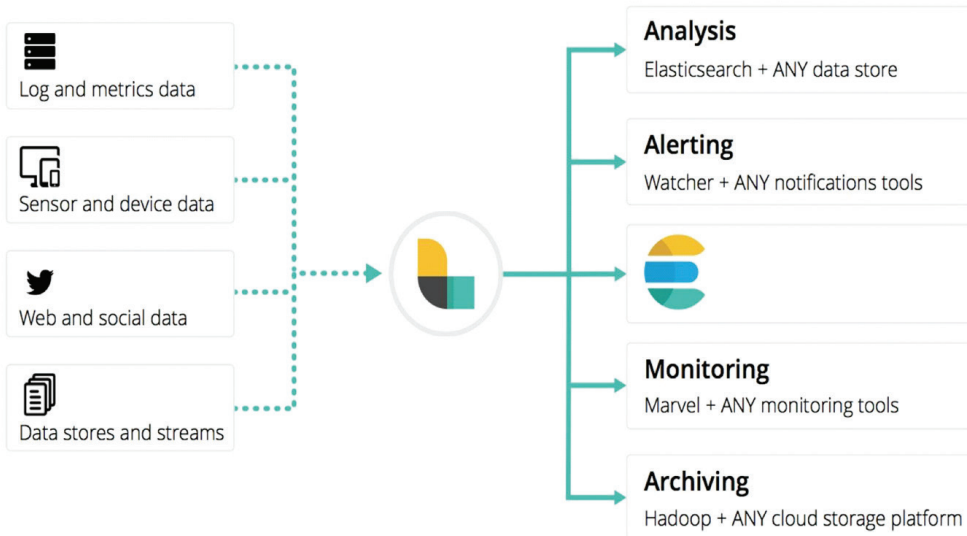


Figure 3: Logstash, the processing pipeline
Source: Azarmi 2017.

Logstash can collect data from several sources, one of which is Beats, as the out-of-the-box integration of Logstash is included in every Beat. However, in this case, the roles are separated clearly: Beats is responsible for delivering the data by default, while Logstash enables data processing before indexing. Consequently, Logstash should be used to prepare the data during the visualisation process.

2.6. Kibana

Kibana is where all the operations of the user interface take place. Most visualisation technologies handle the analytical processing, while Kibana is just a web application that displays the analytical processing done by Elasticsearch. It does not load data from Elasticsearch and then process it but leverages the power of Elasticsearch to do all the heavy lifting. This enables real-time visualisation at scale: as the data grows, the Elasticsearch cluster scales relatively to offer the best latency as a function of SLAs. In addition, Kibana provides visual performance for Elasticsearch aggregations, allowing time-series datasets or segmentation of data fields to be sliced as easily as possible. Kibana is equipped with time-based visualisation, even if the data can arrive

without a timestamp, and brings visualisation built for Elasticsearch aggregation framework visualisation.

3. Explore malware exploit by using Kibana

In investigations, it is important to determine when the attack occurred. Preliminary information on this can be provided by, for example, the Snort Network Intrusion Detection and Prevention System (NIDS), which can detect intrusion-based attacks. Snort is the world's foremost Open Source Intrusion Prevention System (IPS). Snort IPS uses several different rules in its analyses to help determine malicious network activity, and in its investigations, it can identify the unexpected packets that may be causing this malicious activity and send alerts to users immediately.

In the case of a malware exploit scan, it is very important to have an accurate timeframe, which can be achieved by narrowing down the timeframe. Therefore, the first step should definitely be to set an absolute time interval in Kibana to narrow the focus to the log data that is important to you. In this case, we get a graph showing a single entry. To see more detail, we need to restrict the time interval further to be examined and displayed. Once the time range has been reduced to what we need, we can then sort the events by their occurrence, and then analyse the details of each event by the time they occurred. Figure 4 shows how Kibana displays the total number of NIDS Alerts in the dashboard interface.

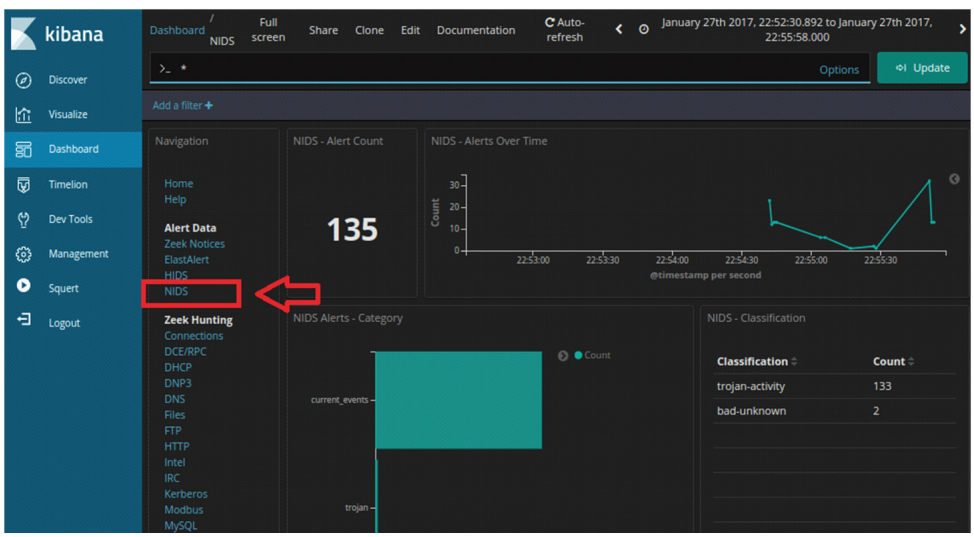


Figure 4: Total number of NIDS alerts in Kibana
Source: Compiled by the authors based on application Kibana.

Examining the details of the extended warning, we can get, amongst others, the following results:

- the date of the first detected NIDS alert in Kibana
- the IP address of the source in the alert
- destination IP address in the alert
- the destination port and service in the alert
- the classification of the alert
- the geographical name of the destination country

The visualisation of the above results in Kibana is illustrated in Figure 5, where the time of the first alert, the source and destination IP address and port are shown.

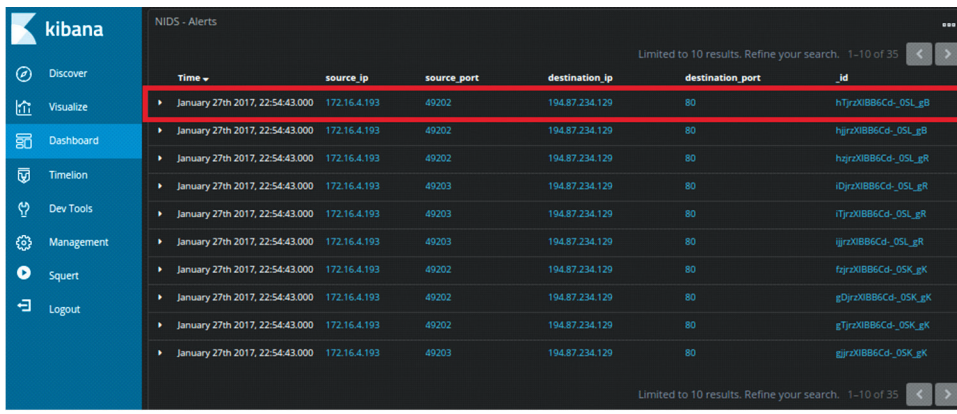


Figure 5: The results of NIDS alerts in Kibana
Source: Compiled by the authors based on application Kibana.

In the web browser of an internet-connected computer, we went to the link in the signature_info field of the alert. This led us to the Emerging Threats Snort alert rule for the exploit. A set of rules is shown. This is because signatures may change over time, or new and more specific rules may be developed. The most recent rule is at the top of the page.

Examining the details of the rule, we came to the following conclusions:

- the malware family for this event is Exploit_Kit_RIG
- the severity of the exploit is the signature severity, which is Major

We then defined what an Exploit Kit is. An Exploit Kit is a malware that aims to infect user devices or network elements with malicious software that uses multiple websites and redirects to achieve its goal. Exploit Kits often use a so-called drive-by method to initiate the attack process. In this type of attack, the user opens a site that appears to be secure, but which contains vulnerabilities that the attackers are aware of and can easily exploit. The vulnerabilities make it much easier for the

threat actors to operate, as they allow them to insert their malicious code into the HTML code of the website. The code is often inserted into an iFrame, which allows content from different web pages to be displayed on the same web page. In most cases, attackers create an invisible iFrame that links the browser to a malicious website. In addition, the HTML loaded into the browser from the website often contains JavaScript that sends the browser to another malicious website or downloads malware to the computer.[9]

3.1. Transcript CapME!

Clicking on the _id of the alert will switch to CapME! to examine the transcript of the event, which is shown in Figure 6.

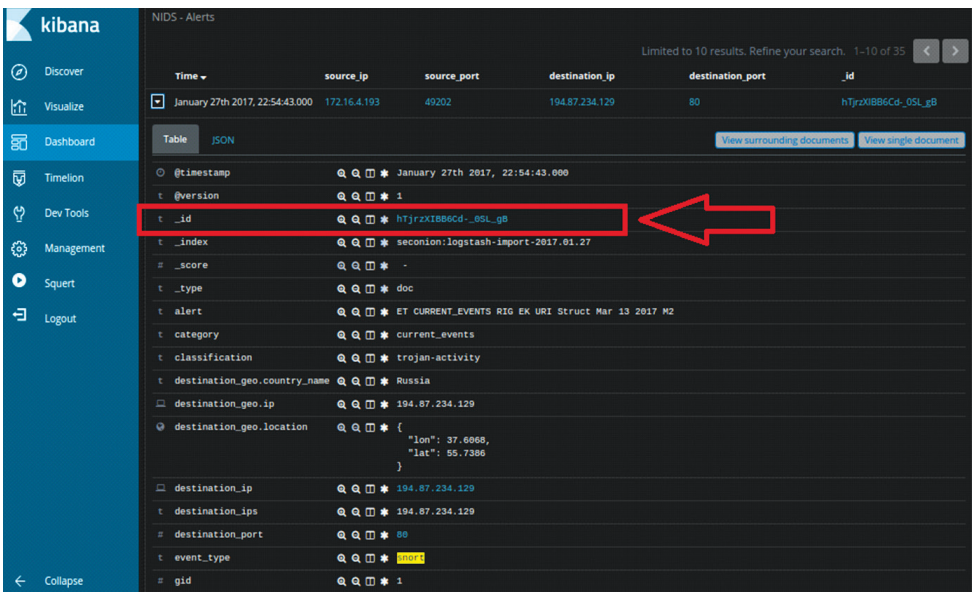


Figure 6: The CapME! window in Kibana

Source: Compiled by the authors based on application Kibana.

Further analysing the results shown in the CapME! window, the session transcript shows that the transactions between the source computer and the destinations reached by the source computer are highlighted in blue. The transcript also contains several valuable information, including a link to the pcap file associated with the alert. These results are shown in Figure 7.

[9] O'Driscoll 2019

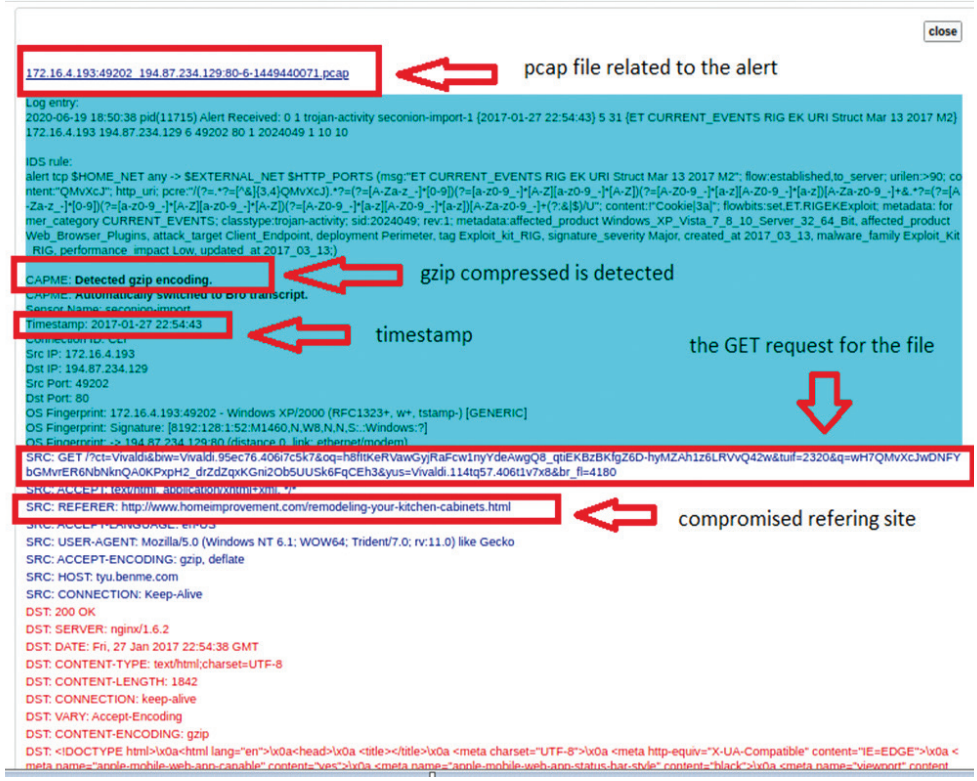


Figure 7: Results in the CapME! window

Source: Compiled by the authors based on application CapME!

We examined the first block of blue text, and we came to the following conclusions:

- The figure shows that this is a request to the target web server.
- It was observed that there are two URLs in this block.
- The first is tagged with SRC: REFERER.
- This indicates the web page that was first accessed by the source computer. However, the server redirected the browser's HTTP GET request to SRC:HOST, which indicated that something in the HTML had sent the source to this site, which indicated that this was most likely a drive-by attack.
- The user intends to connect to www.homeimprovement.com
- The browser refers the user to ty.benme.com URL
  - According to the referred URL, we checked what kind of content is requested by the source host from tybenme.com? We examined the DST server block of the transcript too.
  - The content is in gzip format, which could easily be a malware executable that, once downloaded, runs some malicious code on the host. Because of the compression of the file, its contents are obscured, so it is not easy to determine what is in the file.

CapME! allows checking in the HTTP dashboard section which web pages were visited during the period we are analysing. The HTTP Sites section of the dashboard provides the necessary information. In our case, the following website data were identified:

- www.bing.com
- p27dokhpz2n7nvgr.1jw2lx.top
- homeimprovement.com
- tyu.benme.com
- www.google-analytics.com
- api.blockcipher.com
- spotsbill.com
- fpdownload2.macromedia.com
- retrotip.visionurbana.com.ve

Some of the above websites were already known from earlier activities, not all of which were involved in the exploitation activities. Each URL was searched for on the Internet, and the URLs were enclosed in quotes in the search. In none of these cases were we directly linked to the website. The following conclusions were drawn from the investigations:

- These sites are likely part of the exploit campaign:
  - p27dokhpz2n7nvgr.1jw2lx.top
  - homeimprovement.com
  - tyu.benme.com
  - spotsbill.com
  - retrotip.visionurbana.com.ve
- The HTTP – MIME Types are in the Tag Cloud:
  - image/jpeg
  - text/plain
  - text/html
  - image/gif
  - image/png
  - application/javascript
  - application/x-shockwave-flash
  - text/json

4. Investigate the Exploit with Sguil

Sguil is a network security analyst tool. Sguil ensures access to real-time events, data and raw packets. In addition, Sguil helps with the Network Security Monitoring and event-driven analysis processes and procedures. The program is written in tcl/tk by Robert "Bamm" Visscher. Tcl is the Tool Command Language, an interpreted programming language. It was designed for fast software development.

Tk is a graphical part that draws the data on an analyst's screen. Sguil applies the following tools:

- Snort: this provides alert data, which is why it is very popular in the incident management field. The second copy of Snort collects full content data.
- The keepstats option of the Snort stream4 preprocessor: using this, Sguil receives TCP-based session data.
- Tcpflow: this regenerates the full content trace files to display the application data.
- P0f: it profiles traffic to identify operating system fingerprints.
- MySQL stores alert and packet data collected from Snort.[10]

Sguil can also help to analyse IDS alerts and gather additional information about the sequence of events related to the attack. Among other things, Sguil can help to identify the time when the event occurred, which in our case was:

- According to Sguil, the timestamps for the first and last of the alerts that occurred within about a second of each other are 22:54:42 to 22:55:28. The entire exploit occurred in less than a minute.

Other options include checking the field information in the packet header and the IDS signature rules associated with the alert to determine which malware caused the alert, which can be very helpful in future recovery processes. In our case, the following result was obtained:

- According to the IDS signature rule, Malware_family PseudoDarkLeech malware family triggered this alert.

During the rest of the analysis, event messages were checked for each alert ID associated with the attack, which returned the following results:

- According to the Event Messages in Sguil, the RIG EK Exploit exploit kit is involved in this attack.

Beyond labelling the attack as trojan activity, other information is provided regarding the type and name of the malware:

- ransomware
- Cerber

Based on the alerts so far, it appears that the basic vector of the attack was a visit to a malicious website.

[10] Bejtlich 2010

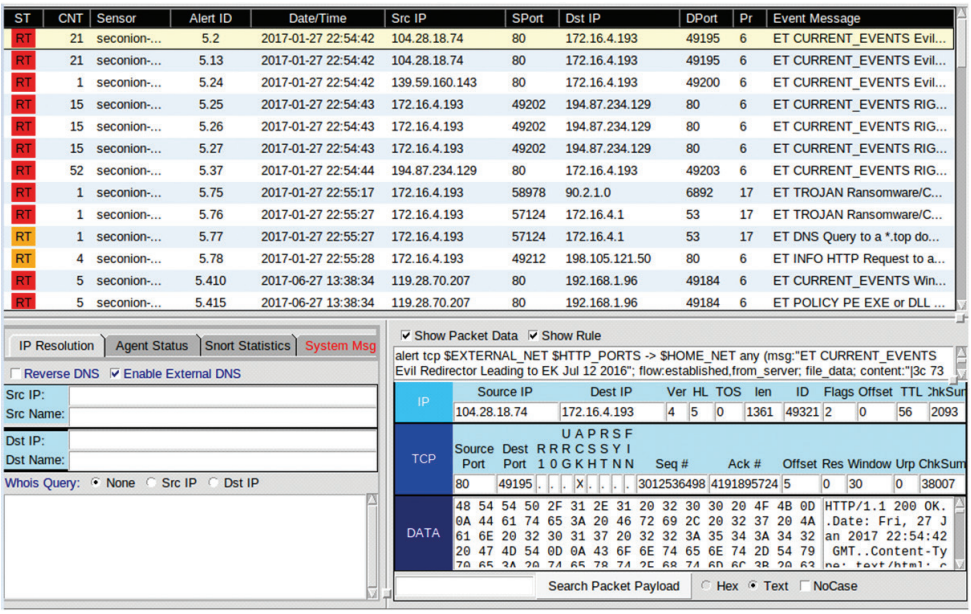


Figure 8: Listed IDS alerts is Sguil

Source: Compiled by the authors based on application Sguil.

4.1. Transcripts of events

After selecting the ID number of the alert shown in the picture above, it is possible to retrieve the Transcript, which can provide us with additional useful information. Examples include the sending and host websites, the browser or search engine used. The transcript may also show specific information such as the type of request, the file's name, format, or website address. For example, during our investigation, we were able to identify the following information from one of our alerts:

- HTTP/1.1 GET request kind of request was involved
- dle_js.js is files requested
- the referer website was www.homeimprovement.com/remodeling-your-kitch-en-cabinets.html and the host website was retrotip.visionbura.com.ve
- the content encoded by gzip

By examining a recent alert, we could identify much more detailed data, making it easier to identify indicators of compromise (IoC), analyse individual incidents, and even help improve the recovery process. These results were:

- 3 requests and 3 responses were involved in this alert
- GET /?ct=Vivaldi&biw=Vivaldi.95ec was the first request
- www.homeimprovement.com/remodeling-your-kitchen-cabinets.html was the referrer
- tyu.benme.com was the host server request to

- POST /?oq=CEh3h8…. Vivaldi was the second request
- tyu.benme.com was the host server request to
- the response was encoded by gzip
- GET /?biw=SeaMonkey.105…. was the third request
- http://tyu.benme.com/?biw…was the referrer
- application/x-shockwave-flash was the Content-Type of the third response
- CWS was the first three characters of the data in the response; the data starts after the last DST: entry; CWS is a file signature; file captions help identify the type of file representing different data types
- swf file was downloaded, Adobe Flashuses this type of file

5. Use Wireshark to investigate an attack

In the following analysis, Wireshark was used to examine the details of the attack. Wireshark is a network protocol analysis program that can capture packets from a network connection. In networking, a packet is a small segment of a larger message. Data transmitted over computer networks such as the Internet is divided into packets. The receiving computer or device then reassembles these packets. Wireshark is one of the most popular sniffer software that does three things:

- capture packets: listens to network connections in real-time and then collects the entire traffic stream
- filtering: this software has a slicing and dicing function for the captured information; if someone needs only specific information, it is available with filtering
- visualisation: it is possible to inspect and measure network packets; visualisation capability is available for complete conversations on the network[11]

In Sguil, we pivoted to select Wireshark from the menu for the chosen alarm ID. The pcap for the alert was opened in Wireshark. By default, Wireshark uses relative time per packet, which is not useful enough to isolate the exact time an event occurred. To make this more detailed, it is possible to select a time display format based on seconds, which makes it much easier to identify the exact time of the event. Several additional filtering options are available in Wireshark; in our analysis, we used the http.request display filter to filter only web requests, illustrated in Figure 9.

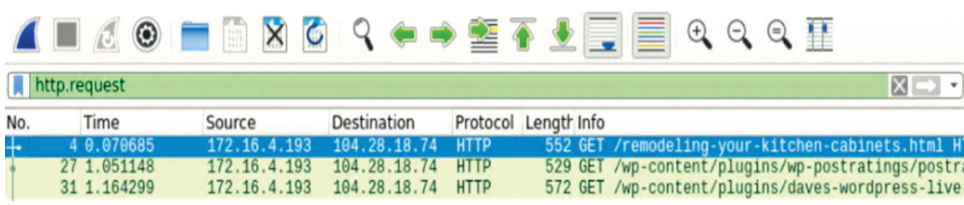


Figure 9: http.request requests in Wireshark
Source: Compiled by the authors based on application Wireshark.

[11] CompTIA 2020

We have selected the first package. In the packet details area, we expanded the Hypertext Transfer Protocol application layer data, which was used to determine to which website the web page of the search engine redirected the user. This is also an important piece of information for further analysis.

5.1. View HTTP objects

As shown above, several HTTP objects were involved in the attack, so their analysis is of paramount importance. To do this, it is possible to extract and save the remodeling. html page in Wireshark, which will provide us with a copy of the page we originally wanted to access. Afterward, in Sguil, we can check, among other things, which file the http request was for and which web page it pointed to. In the case we examined, the http request was for a JavaScript file named dle_js.js, and the host server was retrotip.visionurbana.com.ve.

In the application, the display filter function allows displaying information showing which specific requests are associated with the alert. For example, if we assign the Host column to the information displayed, the application will show us which page the infected website redirects us to. In our case, this is illustrated in Figure 10 where we can see that the Host address is tyu.benme.com. Such information can be the basis for further analysis and can therefore be of significant value.

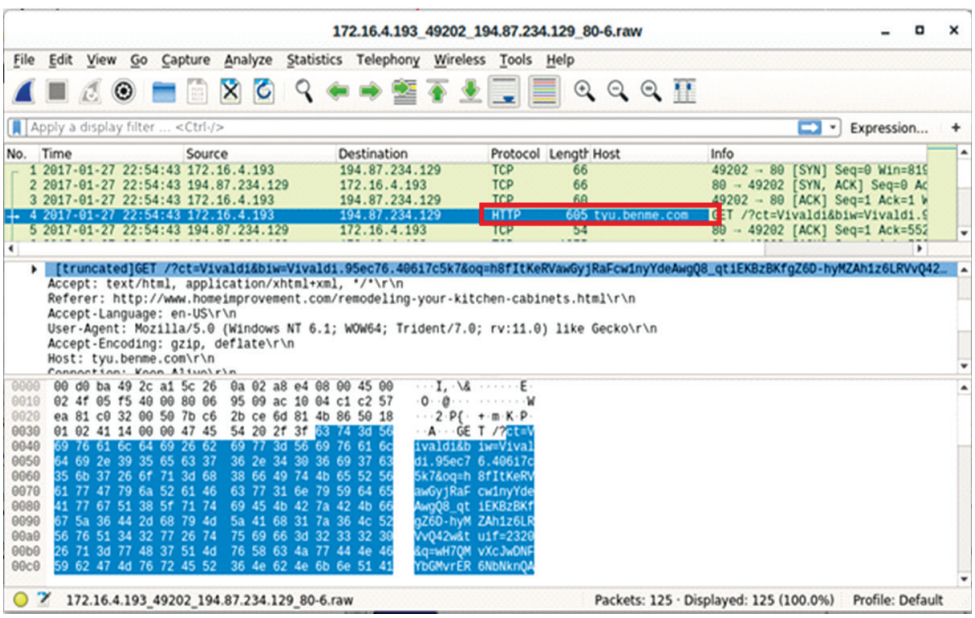


Figure 10: Redirected target address

Source: Compiled by the authors based on application Sguil.

6. Create a hash for an exported malware file

The investigation identified which website the user was trying to access, but the page redirected the user to another website, resulting in files being downloaded to the user's computer from a potentially malicious website. To determine whether a malicious file has been downloaded, it is possible to analyse the hash of the file. For this purpose, we primarily need the downloaded file and can analyse it using, for example, the VirusTotal website.

To generate the hash, it is needed first to export the files from the HTTP object list in Wireshark. In the case of our test, this was two text/html files and an application/x-shockwave-flash file, shown in Figure 11.

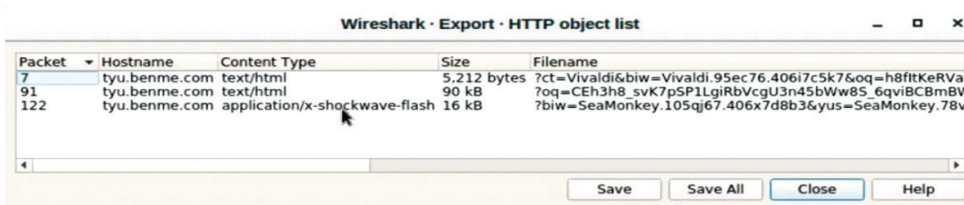


Figure 11: HTTP object list in Wireshark

Source: Compiled by the authors based on application Wireshark.

From the available files, a hash can be generated, which can then be entered into VirusTotal to see if this hash is present in its database for any previously discovered malicious code. VirusTotal is a website developed by Hispasec Sistemas in June 2004. VirusTotal makes fusions of many scan engines and antivirus software. The goal is to examine viruses missed on the host-based antivirus software. Files can be uploaded to the website or sent via email. In addition, there is suspect URL scan capability and VirusTotal dataset search. VirusTotal scans items with more than 70 antivirus and URL/domain blocklist services to extract signs from the examined content.

VirusTotal has got several file submission mechanisms and techniques. The web interface has the principal scanning priority among the publicly available submission methods. Uploaded files can be scripted in any programming language using the HTTP-based public API. These files are shared with the examining part and the sender as well. If somebody uploads a suspicious file or URL, that sender raises global IT security because VirusTotal is using it to develop their database with these kinds of data. Additional functions make the VirusTotal up to date, sharing based on database and community. For example, it allows users to comment on files and URLs and share their experiences with each other.

Some scanners identify everyday items as malicious. In these cases, the VirusTotal can separate and recognise the differences between malicious content and false positives. VirusTotal for dynamic analysis of malware uses the Cuckoo sandbox.

VirusTotal can provide the detection label information. Like the URL scanners cases, which separate malware sites, phishing sites, suspicious sites, etc.

The application shows us much information that can be useful for further analysis, such as MD5, SHA-1 and SHA-256 hash values, time of the first occurrence, time of last confirmation and analysis, file type and the names of infected files detected so far. For the analysed application/x-shockwave-flash file, the following results were obtained:

- MD5: f858070326067ba282d2a63969868e5a
- SHA-1: 97a8033303692f9b7618056e49a24470525f7290
- SHA-256: b3669ec83fb4bba5257da8c68b32dc15d1a08e9e8c22c7483698f-29de2839b5f
- File type: Flash
- File size: 15.88 KB (16261 bytes)
- First Seen in The Wild: 2017-01-27 22:39:08 UTC
- First Submission: 2017-01-27 22:41:40 UTC
- Last Submission: 2022-07-28 02:22:14 UTC
- Last Analysis 2022-06-22 10:43:06 UTC
- At the time of analysis, 22 different names for the malicious code were found by the application, and 30 out of 56 antivirus programs had rules to identify this hash as a malicious file.

Essentially, this provides us with all the information we need to prevent this type of malicious code from entering our systems in the future.

7. Examine exploit artefacts

Further examination of the HTML code extracted from Wireshark provides a wealth of additional useful information. For example, it is possible to determine which scripts in the header may contain malicious activities. In the header of the code we examined, there was a script section that loads the JavaScript file dle_js.js. In addition, the iFrame that loads the content from tyu.benme.com is defined in the HTML body. The script was the following:
<script type="text/javascript" src="//retrotip.visionurbana.com.ve/engine/classes/js/dle_js.js"*></script>*

Inspection of the dle_js.js file in a text editor of choice showed that Javascript document.write() writes the content to the web page, creating an iFrame that redirects to the tyu.benme.com URL. The iFrame was the following:
<iframe src="https://tyu.benme.com/?q=zn_QMvXcJwDQDofGMvrESLtEMUbQA-0KK2OH_76iyEoH9JHT1vrTUSkrttgWC&biw=Amaya.81lp85.406f4y5l9&o-q=elTX_fUlL7ABPAuy2EyALQZnlY0IU1IQ8fj630PWwUWZ0pDRqx29UToB-vdeW&yus=Amaya.110oz60.406a7e5q8&br_fl=4109&tuif=5364&ct=Amaya" *width=290 height=257 ></ifr' +'ame>*

The exploit kit we found is also an automated software to exploit known vulnerabilities in systems or programs. Attackers use them while victims are surfing on the

web. Meanwhile, in web surfing, the main purpose is for the victim to download and execute some variable of malware. Therefore, it is very difficult to determine the real fact of the attack because the exploit kits work in the background. Of course, avoiding unknown links and maintaining the software up to date can ensure a higher level of protection against an attack situation.[12]

An exploit kit is a package to hand over malware. If a victim's computer has a determined number of vulnerabilities, in that case, if the user reaches compromised URLs, it can happen when an exploit is delivered. For this purpose, the malware will be executed on that computer. A software vulnerability is a flaw in software that allows an attacker to take control of the system. These flaws can result from how the software is designed or coding errors. The attacker first determines whether a software vulnerability exists by scanning the system. From the scan, the attacker can find out what types of software are present on the system, whether they are up-to-date, and whether any software packages are vulnerable. If the attacker can find this out, he will have a better idea of the types of attacks he can launch against the system. A successful attack would result in the attacker being able to execute malicious commands on the target system.[13]

Known vulnerabilities are named in a reference list of Common Vulnerabilities and Exposures (CVE). The Common Vulnerabilities and Exposures (CVE) list is a dictionary that has created a common, standardised naming convention for system, network and software vulnerabilities to enable organisations to share information about new risks and establish baselines for assessing the effectiveness of cybersecurity tools and services. The CVE aims to facilitate sharing information on known vulnerabilities so that cybersecurity strategies can be updated to consider the latest security flaws and security issues. Common targets for exploits are popular software with many known vulnerabilities, such as Adobe Flash, Oracle Java and Internet Explorer.[14]

The first step is to make contact with the victim. For example, attackers often use spammed email, and social engineering lures to get individuals to click on a link to an exploit kit server. Another example is when the victim visits a compromised website and clicks on malicious advertising.

The remaining victims are redirected to an alternative landing page which is no longer the real URL. Code embedded into this landing page then proceeds to determine if the victim's device has any vulnerable browser-based applications that correspond to the exploits in the kit. If there are no vulnerabilities, the attack will be stopped. The website will send traffic to the exploit if the vulnerability is detected.[15]

The victims are subsequently redirected to the landing page of the exploit kit. It defines which vulnerabilities will be exploited during the attack. The mode of the exploit is carried out and is determined by the software. If web browsers are the target, the exploit will take the form of code embedded within the web page. The exploits are the first thing supplied to the victim's browser. These exploits will make use of previously known flaws.

[12] Qin et al. 2016
[13] JFrog 2021
[14] Horváth 2020
[15] Tutorialspoint 2022

Malware is executed on the victim's computer after successful exploitation. To the extent of the effect of the malware, there are many different scenarios. Exploit kits can be used to spread several types of malwares. In our case, we reached the homeimprovement.com URL, which had a malicious iFrame that redirected us to a malicious site. This site (tyu.benme.com) executed the malicious JavaScript ad and delivered the malicious Adobe Flash file.

8. Summary

Exploit Kits are digital weapons that are often used by cybercriminals. For example, EK automatically infected malware on the victim's computer without knowing facts by exploiting vulnerabilities.

In the malware exploitation scenario, the victim searched for a page on a search engine site and reached the URL of an infected website, which was identified as a compromised website according to the analysis of the detailed results. The exploit backend contacted the webserver to execute malicious JavaScript code. The EK backend then communicated with the web server and delivered the malicious JavaScript URL to the victim. As a result, ransomware malware was sent in a way the victim did not detect.

The data-driven analysis of the malware exploit contains several similar or identical process steps that could be used or researched in the event of a malware attack against a military network. The stages can provide useful data analysis techniques and methods that can help understand the behaviour of the malicious malware. In particular, malicious embedded URL encoders. It can also contribute to increasing the level of cybersecurity of the government or even military and increasing information and cyber awareness of government and defence sector personnel using external links from the Internet.

References

Azarmi, Bahaaldine (2017): *Learning Kibana 5.0.* Birmingham: Packt Publishing.

Bejtlich, Richard (2010): *The Tao of Network Security Monitoring. Beyond Intrusion Detection.* Boston: Addison-Wesley Professional.

CompTIA: What Is Wireshark and How Is It Used? *CompTIA,* 10 November 2020. Online: www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it

Fang, Yufei – Shan, Zhiguang – Wang, Wei (2021): Modeling and Key Technologies of a Data-Driven Smart City System. *IEEE Access,* 9, 91244–91258. Online: https://doi.org/10.1109/ACCESS.2021.3091716

GoLinuxCloud: *ELK Stack: Configure elasticsearch cluster setup CentOS/RHEL 7/8.* 2020. Online: www.golinuxcloud.com/setup-configure-elasticsearch-cluster-7-linux/

Horváth, Ingrid: Understanding Common Vulnerabilities and Exposures. *Invensis,* 17 September 2020. Online: www.invensislearning.com/blog/understanding-common-vulnerabilities-and-exposures/

JFrog: What is a Software Vulnerability? *JFrog,* 22 August 2021. Online: https://jfrog.com/knowledge-base/software-vulnerability/

Jia, Kunqi – Wang, Zhihua – Fan, Shuai – Xiao, Jucheng – He, Guangyu (2018): Data-Driven Architecture Design and Application of Power Grid Cyber Physical System. *Power System Technology,* 42(10), 3116–3127. Online: https://doi.org/10.13335/j.1000-3673.pst.2018.0876

O'Driscoll, Aimee: What is an exploit kit (with examples) and how do cybercriminals use them? *Comparitech,* 07 May 2019. Online: www.comparitech.com/blog/information-security/exploit-kits/

Qin, Feng – Liu, Dongxia – Sun, Bingda – Ruan, Liu – Ma, Zhanhong – Wang, Haiguang (2016): Identification of Alfalfa Leaf Diseases Using Image Recognition Technology. *Public Library of Science,* 11(12), 1–7. Online: https://doi.org/10.1371/journal.pone.0168274 ; DOI: https://doi.org/10.1371/journal.pone.0168274

Tutorialspoint: What is an Exploit Kit? (Stages, Process, How to Stay Safe). *Tutorialspoint,* 14 June 2022. Online: www.tutorialspoint.com/what-is-an-exploit-kit-stages-process-how-to-stay-safe

Wang, Ying – Li, Peilong – Jiao, Lei – Su, Zhou – Cheng, Nan – Shen, Xuemin Sh. – Zhang, Ping (2017): A Data-Driven Architecture for Personalized QoE Management in 5G Wireless Networks. *IEEE Wireless Communications,* 24(1), 102–110. Online: https://doi.org/10.1109/MWC.2016.1500184WC

Wang, Zhihua – Xiao, Jucheng – Jia, Kunqi – Gao, Feng – Tang, Yuanhe – He, Guangyu (2018): A Data-Driven Architecture Design of Stream Computing for the Dispatch and Control System of the Power Grid. *2nd IEEE Conference on Energy Internet and Energy System Integration (EI2),* 1–6. Online: https://doi.org/10.1109/EI2.2018.8582404

HADMÉRNÖK
FÓRUM
17. évfolyam (2022) 4. szám 175–194.
DOI: 10.32567/hm.2022.4.11

Molnár Dóra,[1] Szalkai Patrik[2]

Északi-sarki béke vagy háború?

Avagy mit mondanak az arktiszi stratégiák[3]

Arctic Peace or War?

Or What Arctic Strategies Say

Az Északi-sark térsége napjaink nemzetközi érdekütközéseinek egyik fontos régiójává kezd válni, ezért egyre több biztonságpolitikai kérdés merül fel vele kapcsolatban. A tanulmány az arktiszi államok speciális, az északi-sarki viszonyokat taglaló stratégiai dokumentumainak összehasonlító és elemző vizsgálata segítségével két fő kérdésre keresi és találja meg az igenlő választ. A hivatalos állami dokumentumok alapján igazolható egyrészt az, hogy az Arktisz egy önállóan értelmezendő és kezelendő régió, amelyre nem, vagy csak minimális mértékben hatnak más régiók konfliktusai. Másrészt az is egyértelmű, hogy Oroszország az arktiszi régióban sokkal inkább az együttműködés jeleit mutatja, sem mint agresszív szándékai volnának. Ez a békésnek mondható arktiszi légkör a nemzetközi szervezetek támogató tevékenysége nélkül természetesen nehezen lenne elképzelhető, az államok feletti szinttel azonban jelen tanulmány nem foglalkozik.

Kulcsszavak: **Északi-sark, arktiszi államok, Oroszország, stratégia, béke, együttműködés**

The Arctic region is to become an important region of international conflict of interests today, raising more and more security policy issues. The study seeks and finds an affirmative answer to two main questions through a comparative analysis of the Arctic states' special strategic documents on Arctic relations. It can be justified on the one hand that the Arctic is a region to be interpreted and managed on its own, which is not or only minimally affected by conflicts in other regions. On the other hand, it is also clear that Russia has been showing signs of cooperation in

[1] Adjunktus, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Nemzetközi Biztonsági Tanulmányok Tanszék, e-mail: molnar.dora@uni-nke.hu
[2] Nemzetközi biztonság- és védelempolitikai mesterszakos hallgató, Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Nemzetközi Biztonsági Tanulmányok Tanszék e-mail: szpatrik141@gmail.com
[3] A kézirat lezárásának dátuma: 2021. december 1.

the Arctic region rather than aggressive intentions. This peaceful Arctic atmosphere would, of course, be difficult to imagine without the supportive work of international organisations, however, the supranational level is not addressed in this study.

Keywords: **Arctic region, Arctic states, Russia, strategy, peace, cooperation**

1. Bevezetés

Az Arktisz a történelem során mindig olyan terület volt, amelyet az emberiség meg akart ismerni, majd később meg is akart hódítani. Sokáig azonban egyrészt elérhetetlennek bizonyult, másrészt túl nagy stratégiai vagy gazdasági értéket sem tulajdonítottak neki az államok. Manapság ez a tendencia megváltozni látszik. Ha napjainkban az Arktisz térsége felmerül, leggyakrabban az erőforrások, a területi viták és a növekvő katonai jelenlét kontextusában lehet róla hallani. Bár az arktiszi katonai jelenlét az elmúlt évtizedekben folyamatosan nőtt, a világ más térségeihez képest az Arktisz még mindig békésnek mondható, és tudományos körökben is viszonylagos konszenzus van azzal kapcsolatban, hogy nem valószínű konfliktus a térségben.[4] Azonban a régió békéje ugyanúgy magyarázatra szorul, mint más régiók esetében az, hogy miért törnek ki konfliktusok. Egyfelől az Arktisz mint régió esetében olyan nagyhatalmak vannak viszonylag közel egymáshoz, akik egymás vetélytársai. A Bering-szoros két partján található az Amerikai Egyesült Államok és az Oroszországi Föderáció, és a két állam között mindössze 89 km távolság van. Továbbá az Arktisz az a régió, amelyre a legjobban hat napjaink égető kihívása, a klímaváltozás. A jég visszaszorulásával olyan gazdasági és katonai lehetőségek nyílnak meg a térség államai számára, amelyekről eddig álmodni sem mertek. Ennek következtében a verseny egyre erősödik a térségben. Számos területi vita van az államok között, és az érintettek jelentős összegeket költenek arra, hogy alátámasszák területi igényüket – ahogyan a hadseregük felkészítésére is, hogy sarkvidéki körülmények között is készek legyenek szükség esetén harcolni.[5]

Az Arktisz lehetne a 21. század vadnyugata, azonban mégsem ezt látjuk. Ennek okai közt szerepel egyrészt az, hogy az Arktisz egy önállóan értelmezendő és kezelendő régió, amelyre nem, vagy csak minimális mértékben hatnak más régiók konfliktusai. Másrészt Oroszország az arktiszi régióban nem agresszorként lép fel, hanem együttműködésre törekszik. Harmadrészt pedig az arktiszi politikai környezet formálásában jelentős szerepet játszanak a nemzetközi szervezetek.

Jelen tanulmány az állami szintre fókuszál (a második szintet, a nemzetközi szervezetek vonatkozásait nem elemzi). E körben az arktiszi államok vonatkozó stratégiai dokumentumait kell elemezni, kiemelve azon megállapításokat, hogy a vizsgált államok milyen szerepet tulajdonítanak az Arktisznak és miként vélekednek Oroszországról. Több ország esetében rendelkezésre áll a krími válság előtti és utáni stratégiai dokumentum; így e körben összehasonlító elemzés is végezhető (lásd az *Állami stratégiák* című részt).

[4] Grätz 2012; Käpylä–Mikkola 2013; Duxbury 2020.

[5] Az arktiszi nemzetközi szervezetekről lásd az Arctic Center, University of Lapland összefoglalását: www.arctic-centre.org/EN/arcticregion/international

Az Arktisz mint önálló régió létét egy külső konfliktus segítségével igazoljuk annak vizsgálata segítségével, hogy egy Arktiszon kívüli külső konfliktus milyen hatással van az államok közötti kapcsolatokra. Ez a régión kívüli konfliktus a krími válság. A választásunk azért erre a válságra esett, mert a konfliktusban egy arktiszi állam (Oroszország) is érintett, az Észak-atlanti Szerződés Szervezete (NATO) és annak tagországai – amelyek közül több arktiszi államként is definiálja magát – pedig hevesen ellenezték az orosz lépéseket és azokat a nemzetközi jogba ütköző cselekedeteknek minősítették. Ezért napjaink konfliktusai közül a krími válság az, amely a legnagyobb valószínűséggel befolyásolhatja az Arktiszt és annak biztonságpolitikai jövőjét.

A jövő számos újdonságot hoz a térségben, elsősorban a klímaváltozásnak köszönhetően. Erre már most készülnek az államok, és lépéseik, hozzáállásuk jól tükröződik a stratégiai dokumentumaikban. Ezért a továbbiakban az arktiszi államok vonatkozó stratégiáit vizsgáljuk meg a fenti két tétel igazolására.

2. Állami stratégiák

Az elemzés a nyolc arktiszi állam[6] arktiszi stratégiájának vizsgálatára irányul. A stratégiák elemzését az alábbi kérdésekre fókuszálva végezzük el:

- Az adott állam miként értékeli az Arktisz biztonsági helyzetét?
- Milyen fenyegetéseket észlel?
- Ezek a fenyegetések hogyan változnak 2014 után?
- A militarizáció mekkora szerepet kap a stratégiákban?

A stratégiák elemzése során minden esetben központi kérdésként vizsgáljuk, hogy az adott állam miként gondolkodik Oroszországról, ugyanakkor a további bilaterális kapcsolatokat nem elemezzük. Ennek oka egyrészt az, hogy mindegyik állam NATO-tagállam, így kizárható közöttük a katonai konfrontáció, másrészt pedig annak igazolásához vagy cáfolatához, hogy beszélhetünk-e különálló régióról az Arktisz kapcsán, az államok Oroszországgal ápolt kapcsolatának van döntő jelentősége.

2.1. Norvégia

Norvégia miniszterelnöke 2013 és 2021 között Erna Soldberg, a konzervatív párt elnöke volt. A *Norvégia Arktiszi Szakpolitikája* című dokumentumot már a krími válság után adták ki 2014 novemberében,[7] tehát az már tükrözi az ukrán válságot követő biztonságpolitikai változásokat. Norvégia militarizáló államnak tekinthető, bár stratégiájában konkrét stratégiai pillér nem foglalkozik a katonai szerepvállalás növelésének kérdésével. A stratégia külön nevesíti Oroszországot és vele összefüggésben a katonai szerepvállalás fontosságát, de hozzáteszi, hogy a cél az Oroszországgal

[6] A nyolc arktiszi állam a következő: Norvégia, Dánia, Svédország, Izland, Finnország, Kanada, Amerikai Egyesült Államok, Oroszországi Föderáció.

[7] Norway's Arctic Policy 2014.

való együttműködés. Ugyanakkor figyelemreméltó, hogy Norvégia növeli a katonai határállomások számát Norvégia és Oroszország között, valamint a fegyveres erők egyik fő feladataként nevesíti a norvég–orosz határ ellenőrzését. A militarizáló attitűdöt az is bizonyítja, hogy Norvégia 52 darab F-35-ös vadászgépet rendelt az Egyesült Államoktól.[8]

Norvégia azonban végső soron Oroszországgal szeretne együttműködni, bár megközelítésmódját még mindig az óvatosság jellemzi. Az együttműködésre való hajlandóságot az is mutatja, hogy 2011-ben a két országnak sikerült lezárni egy 44 éves területi vitát, amely még 1974-ben kezdődött a Barents-tengeren lévő határt illetően. Az érintett terület 175 000 km^2, és igen jelentős mind stratégiai, mind gazdasági szempontból. Stratégiailag azért fontos, mert ezen a területen keresztül érhető el Oroszország egyetlen egész évben jégmentes kikötője, Murmansk és ez a bejárata az Északi Tengeri Útnak is. Gazdaságilag pedig azért fontos, mert orosz számítások szerint 5,8 trillió m^3 kinyerhető gázkészlet és további 2,7 milliárd hordónyi olajkészlet található a térségben.[9]

2021-ben, továbbra is konzervatív irányítás alatt, Norvégia kiadta legfrissebb arktiszi stratégiáját, a *Norvég Kormány Arktiszi Szakpolitikáját*.[10] Ez a stratégia sokkal komorabb biztonsági helyzetet vázol fel, mint bármelyik kanadai, vagy akár a 2014-es norvég dokumentum. A stratégia kiemelt helyen foglalkozik Oroszországgal. Egyfelől kiemeli, hogy az elmúlt 30 évben az orosz–norvég kapcsolatok jelentősen fejlődtek számos területen, úgymint halászat, kutatás, környezetvédelem, kutató-mentő tevékenységek, nukleáris biztonság, egészség, oktatás, üzleti élet, energia, kultúra és az őslakosokat érintő ügyek, valamint négy bilaterális bizottság is létrejött a halászat, a nukleáris biztonság, a gazdasági kooperáció és a környezetvédelem terén. Azonban a stratégia azt is kiemeli, hogy a krími válság miatt Norvégia felfüggesztette a bilaterális katonai együttműködést Oroszországgal, a tengeri biztonság, a légtérvédelem és az északi stabilitást érintő ügyek kivételével. Az Összhaderőnemi Norvég Főparancsnokság és az Orosz Északi Flotta közötti közvetlen kapcsolat ugyanakkor megmaradt, és továbbra is együttműködik az orosz és a norvég parti őrség, a határőrség és a kutató-mentő műveletek résztvevői. Fenntartották továbbá a *Tengeri Incidensek Egyezmény*[11] mechanizmusait is, és tárgyalnak annak továbbfejlesztéséről.[12] Ez a tárgyalás idén, 2021-ben sikerrel zárult, a felek több kérdésben is megállapodtak. Ez a megállapodás a területi vizektől 12 tengeri mérfölddel távolabbi hajókat és katonai repülőket érinti, valamint egyéb átláthatóságot erősítő intézkedéseket is elfogadtak.[13] A stratégia ezenkívül kiemeli, hogy 2019-től orosz és norvég felső katonai vezetők között közvetlen kommunikációs csatornákat hoztak létre, majd az Oroszországgal történő katonai együttműködést

[8] Dennis 2019.
[9] Moe–Fjaertoft–Øverland 2011. 150.
[10] The Norwegian Government's Arctic Policy. 2021.
[11] A Tengeri Incidensek Egyezményt 1989-ben kötötte meg Norvégia és a Szovjetunió, célja a félreértések elkerülése azáltal, hogy protokollokat teremt az ütközések elkerülésére, távolságtartásra, hajók megfigyelésére. Az egyezmény továbbá betiltotta a támadások szimulálását és a hajóformációk zavarását. Lásd Łukasz–Frear–Raynova 2016.
[12] The Norwegian Government's Arctic Policy. 2021. 19.
[13] O'Dwyer 2021.

taglaló részt a stratégia azzal zárja, hogy „a jelen helyzetben kiemelten fontos tovább folytatni ezt a fajta érintkezést a védelem területén".[14]

A 2021-es stratégia azonban korántsem csak az Arktisz biztonságpolitikai elemzésével foglalkozik, hiszen az csak egy fejezet a nyolcból. A nemzetközi rendszert illetően kiemeli, hogy az Arktisz békés régió, ahol az államok hajlandóságot mutatnak az együttműködésre, és nézeteltéréseiket a nemzetközi jog elvei mentén oldják meg.[15]

Szemben a kanadai–orosz kapcsolatokkal, Norvégia esetében stratégiai szinten is megjelenik a 2014-es ukrán konfliktus okozta törés a két ország kapcsolatában. Ez esetben tehát azt láthatjuk, hogy egy külső konfliktus közvetlen hatással volt a régióra és annak biztonságára, amelyben két tényező is szerepet játszott. Egyfelől Norvégia és Oroszország egymással határos államok, ami magyarázatot adhat arra, hogy Norvégia miért reagált érzékenyebben a krími válságra, ugyanakkor – ahogyan a stratégia is kiemeli – még a válságot követően sem szűnt meg a két ország közötti katonai együttműködés, és a feleknek sikerült újabb megállapodást is kötniük (mint ahogyan azt a Tenger Incidensek Egyezmény kapcsán láttuk). Tehát a tanulmány elején szereplő állítást, miszerint a régió stabilitását nem, vagy csak kis mértékben befolyásolja külső konfliktus, a norvég–orosz katonai együttműködés gyengülése sem cáfolja meg, hanem éppen ellenkezőleg: erősíti, mivel bár a konfliktus hatása kimutatható volt, de a visszarendeződés jelei már most láthatóak.

2.2. Dánia

A 2011-es *Dán Királyság Stratégiája az Arktiszra 2011–2020* című dokumentum[16] a Lark Løkke Rasmussen miniszterelnök és Lene Espersen külügyminiszter és miniszterelnök-helyettes által vezetett kisebbségi kormányhoz köthető, amely a Liberális Szövetségből és a Konzervatív Néppártból állt. Dánia a stratégiája szerint szintén növeli katonai jelenlétét a térségben, és a hadsereggel kapcsolatban négy új kezdeményezést ír elő: egy összhaderőnemi arktiszi parancsnokság létrehozása, az arktiszi műveletek végrehajtásához szükséges képességek megteremtése az Arktiszi Reagáló Erő[17] létrehozásával, kockázatelemzések készítése a környező vizeken lévő forgalomnövekedéssel kapcsolatban és végül 2014-re egy átfogó elemzés készítése a katonaság jövőbeli feladatairól. Emellett a stratégia azt is rögzíti, hogy Dánia a szuverenitás érvényesítését a hadsereg elsődleges feladatának tekinti. A dán stratégiánál is ki kell emelni, hogy megemlíti az Oroszországgal való együttműködés fontosságát. A dán–orosz kooperáció kapcsán a stratégia felveti a tudományos együttműködésnek, az információcserének a fenntartható fejlődéssel összefüggésben, valamint a védelmi erők együttműködésének lehetőségét is. Ezzel Dánia újabb példa arra, hogy a militarizálás megfér a kooperációkereséssel. A 2011-es stratégia felülvizsgálata jelenleg is folyamatban van, és várhatóan még 2021-ben megjelenik a következő tíz évre vonatkozó dán dokumentum. 2018-ban a dán kormány *Védelmi Megállapodás*

[14] The Norwegian Government's Arctic Policy. 2021. 19.
[15] The Norwegian Government's Arctic Policy. 2021. 11.
[16] *Kingdom of Denmark Strategy for the Arctic 2011–2020.* 2011.
[17] Arctic Response Force.

2018–2023 címmel a többi ellenzéki párttal (Szociáldemokrata Párt, Dán Néppárt és a Szociál-Liberális Párt) egy teljes politikai spektrumot átfogó megállapodást kötött,[18] amely a dán haderő fejlesztési irányait határozza meg 2023-ig. A teljes dokumentum elemzése túlmutat a tanulmány keretein, ezért itt csak az Arktiszt érintő kérdésekre térünk ki. A megállapodás mindössze egyszer említi Oroszországot – mint a NATO keletről érkező kihívását – a globális biztonsági helyzet elemzéséről szóló részben. Az Arktisszal összefüggésben a dokumentum megjegyzi, hogy az a klímaváltozás által érintett olyan terület, ahol megnőtt az aktivitás, majd külön kitér a jövőbeli dán arktiszi katonai szerepvállalásra. A dokumentum szerint a jövőben geopolitikailag fel fog értékelődni a régió, azonban a dán cél az, hogy a régióban továbbra is békés viszonyok uralkodjanak.[19]

2.3. Svédország

A 2011-es svéd stratégia a Fredrik Reinfeldt liberális konzervatív koalíció (Mérsékelt Párt, Centralista Párt, Liberális Néppárt, Kereszténydemokraták) kisebbségi kormányához köthető. A *Svédország Arktiszi Stratégiája* szerint: „Svédországnak hangsúlyoznia kell azt a megközelítést, amely a biztonságot a legtágabb értelemben kezeli, és amely civil eszközöket használ katonaiak helyett."[20] A biztonságpolitikai helyzettel kapcsolatban kiemelte, hogy a kihívások elsősorban nem katonai jellegűek, hanem a klímaváltozás következtében inkább környezetiek. A stratégia bár számos ponton említi Oroszországot, nem mint fenyegetést, hanem mint egyet a többi arktiszi állam közül.

A 2020-ban kiadott *Svédország Arktiszi Stratégiája* című stratégia már a szociáldemokrata Stefan Löfven nevéhez kötődik.[21] A dokumentum a katonai erő alkalmazásával kapcsolatban úgy fogalmaz, hogy: „A kormány folytatja Svédország katonai képességeinek erősítését, hogy ütőképes legyen az ország északi területein és a szomszédos területeken." A megfogalmazáson enyhít egy másik kitétel, miszerint a kormány azon fog dolgozni, hogy az Arktisz továbbra is olyan régió maradjon, ahol jól működő nemzetközi együttműködés van, és az államok a nemzetközi jogot tiszteletben tartják, beleértve a tengeri jogot is. Eltér a 2011-es és 2020-as stratégia között a biztonsági kihívások értelmezése. Míg 2011-ben a svéd stratégia szerint a biztonsági kérdések a térségben nem katonai jellegűek, addig a 2020-as stratégia már a fegyverkezési verseny kockázatát látja a térségben, és a katonai szerepvállalás fontosságának növekedését hangsúlyozza. A 2020-as stratégia kiemeli, hogy bár a nyugati államok és Oroszország kapcsolata az utóbbi években romlott, az Arktiszi Tanács működését továbbra is a konstruktív lelkület és a kooperáció jellemzi, és jó az együttműködés Oroszországgal, különösen olyan területeken, mint a környezeti kérdések az Arktiszi Tanácsban, a Barents-kooperációban és bilaterális alapon is. Az orosz fegyverkezést a stratégia az orosz területek védelmének tulajdonítja, nem tekinti fenyegetésnek. A svéd stratégiában negyvenhétszer szerepel Oroszország neve, azonban egyetlen

[18] *Defence Agreement* 2018–2023. 2018.
[19] *Defence Agreement* 2018–2023. 2018. 10.
[20] *Sweden's Strategy for the Arctic Region.* 2011. 23.
[21] *Sweden's Strategy for the Arctic Region.* 2011.

egy esetben sem mint fenyegetés – még a militarizációval összefüggésben sem. Ezek a megállapítások egyértelműen igazolják, hogy az arktiszi régió képes függetlenül működni a világ többi részétől.

2.4. Izland

Izland tekintetében stratégiai dokumentum helyett egy határozat szolgál iránymutatásul. 2011-ben a Jóhanna Sigurðardóttir miniszterelnök által vezetett Szociál Demokrata Szövetség és a Bal-Zöld Mozgalom alkotta koalíció adta ki a *Parlamenti Határozat Izland Arktiszi Szakpolitikájáról* című dokumentumot.[22] A szakpolitika 12 elve közül az egyik (9.) kijelenti, hogy Izland a militarizáció minden formáját ellenzi, és a biztonságot csak civil eszközökkel szabad és kell garantálni. Mindez egyébként következik abból az évtizedekre visszanyúló izlandi megközelítésből, hogy Izland bár NATO-tagország lett, a szervezet katonai szárnyában csak megfigyelőként vesz részt.[23]

2.5. Finnország

Finnország esetében szintén jól kirajzolódik az ukrán válság előtti és utáni hozzáállásbeli különbség. 2013-ban a Jyrki Katainen miniszterelnök által vezetett jobbközép kormány kiadta a *Finnország Stratégiája az Arktisz régióra 2013* című dokumentumot,[24] amelyben a holisztikus megközelítés jegyében a gazdaságnak, az oktatásnak és a környezetnek tulajdonít nagyobb szerepet. Az arktiszi stabilitást illetően a hangsúlyt a felkészültségre kell helyezni, és fontos a szoros együttműködés a hatóságok, az ipar, a nem kormányzati szervezetek és a lakosság között. A stratégia kevés figyelmet fordít a biztonság katonai aspektusára. Rögzíti, hogy katonai konfliktus a régióban nem valószínű, és Oroszországról is csak a kooperáció kapcsán ejt szót. Más katonai kérdés fel sem merül ebben a stratégiában.

A Sanna Marin miniszterelnök és a Szociáldemokrata Párt által vezetett kormány 2021-ben adta ki az ország új stratégiai dokumentumát *Finnország Stratégiája az Arktisz Szakpolitikára* címmel.[25] Ez a dokumentum már egészen más szellemben íródott, amelyet jól mutat az is, hogy míg a 2013-as stratégia mindössze egy oldalt szentelt a biztonságpolitikai kérdéseknek, addig a 2021-es stratégia rögtön a célok ismertetését követően közel tíz oldalon keresztül elemzi az aktuális biztonsági helyzetet. A stratégia kiemelten foglalkozik Oroszországgal is, hangsúlyozva, hogy Oroszország közvetlenül befolyásolta a szomszédos régió biztonsági helyzetét Krím illegális annexiójával és rámutatva arra, hogy Oroszország növeli katonai jelenlétét az Arktiszon annak érdekében, hogy gazdasági érdekeit és az északi-tengeri útvonalat megvédje. Ennek az lett a következménye, hogy az Egyesült Államok, Kanada és az európai NATO-tagországok szintén növelték katonai jelenlétüket és a katonai válaszadási

[22] A Parliamentary Resolution on Iceland's Arctic Policy. 2011.
[23] *Iceland and NATO* é. n.
[24] *Finland's Strategy for the Arctic Region.* 2013.
[25] *Finland's Strategy for Arctic Policy.* 2021.

képességüket az északi területeken. Ez tipikusan a Herz által leírt biztonsági dilemma, amely során mintegy spirális folyamatként az egyik állam katonai lépései maguk után vonják a térség más államainak hasonló válaszlépéseit.[26] Ugyanakkor a stratégia azt is kiemeli, hogy a regionális együttműködés erősödött az előző stratégia kiadása óta, és cél, hogy a jövőben bilaterális alapon Oroszországgal is szorosabb legyen a kooperáció. A tekintetben nincs eltérés a 2013-as stratégiához képest, hogy az aktuális dokumentum sem fektet különösebb hangsúlyt a katonai kérdésekre, ugyanis a stratégia négy központi prioritásként a klímaváltozást, a lakosok jólétét és az őslakosok jogainak védelmét, az arktiszi szaktudást, valamint az infrastruktúra és logisztika kérdésköreit jelöli meg.[27]

Tehát bár a 2021-es stratégia észleli a biztonsági környezet 2014 óta bekövetkezett változását, ezt nem tekinti olyan mértékűnek, hogy fenyegetésként észlelje és a prioritások közé emelje, akár erőforrásokat is hozzárendelve.

2.6. Kanada

A krími válságot megelőző Arktiszt érintő kanadai stratégia a *Kanada Északi Stratégiája: Északunk, Örökségünk, Jövőnk* című dokumentum.[28] A stratégiát 2009-ben adták ki, amikor Kanada miniszterelnöke a konzervatív Stephen Harper volt. Az ő megfogalmazása szerint: „Az első és legfontosabb prioritása a mi északi stratégiánknak az arktiszi szuverenitásunk védelme."[29] Ez a gondolatmenet a stratégiában is megjelenik: négy pillére közül egy csak az arktiszi szuverenitás gyakorlásáról szól.[30] Ennek keretében foglalkozik a stratégia a katonai jelenlét növelésével, valamint az infrastruktúra és eszközpark fejlesztésével. Kiemeli a szárazföldi, tengeri és légi járőrözés fontosságát, valamint stratégiai feladatnak tekinti szárazföldön a Resolute-öbölben található Katonai Kiképző Központ létrehozását, a Kanadai Ranger-ek,[31] valamint tengeren mélytengeri kikötők, üzemanyag-létesítmények és új jégtörők szolgálatba állítását a parti őrség számára. Az ország más államokkal is együtt kíván működni, és Oroszországot sem tekinti fenyegetésnek. Oroszországot csak a közös kutatási együttműködés, a közös kisebbségjogi memorandum aláírása és az ilulissati deklaráció kapcsán említi meg.

A legfrissebb kanadai stratégia, amely az Arktisszal foglalkozik, a 2019-ben kiadott *Kanada Arktiszi és Északi Szakpolitikai Keretrendszere*[32] és a hozzá tartozó *Kanada Arktiszi és Északi Szakpolitikai Keretrendszer Nemzetközi Fejezete.*[33] Ezt a stratégiát már nem a korábbi konzervatív vezetés adta ki, hanem a Liberális Párt és a Justin Trudeau által fémjelzett adminisztráció. Nagy változás a tíz évvel korábbi dokumentumhoz

[26] Herz 1950. 157–180.
[27] Részletesen lásd a stratégiában: *Finland's Strategy for Arctic Policy.* 2021.
[28] *Canada's Northern Strategy: Our North, Our Heritage, Our future.* 2009.
[29] CBC News 2010.
[30] A további három pillér: a társadalmi és gazdasági fejlődés promótálása, környezeti örökség védelme, valamint az északi kormányzás fejlesztése és promótálása.
[31] Olyan, elsősorban őslakosokból álló tartalékos erő, akik lakhelyükön maradhatnak olyan távoli, északi régiókban, ahova a kanadai katonai erő nehezen, vagy egyáltalán nem tud eljutni.
[32] *Canada's Arctic and Northern Policy Framework.* 2019.
[33] *Canada's Arctic and Northern Policy Framework.* International Chapter. 2019.

képest a szuverenitás és a térség katonai megerősítésének háttérbe szorulása, amely helyét a 2019-es keretrendszerben az őslakosok és a kormány velük ápolt kapcsolata veszi át. A stratégia kiemeli, hogy „robusztus szabályok, normák és intézmények vannak, amelyek irányítják a nemzetközi ügyeket". Mindezt konkretizálva, az Arktiszi Tanácsot, az Arktiszi Parti Őrség Fórumot, az Arktiszi Gazdasági Tanácsot, számos ENSZ szervezetet, kiemelve a Nemzetközi Tengerészeti Szervezetet értve ezalatt. A jogi keretrendszert illetően az ENSZ Tengerjogi Egyezménye (UNCLOS) mellett a jogi kötőerővel bíró Arktiszt érintő nemzetközi megállapodásokat és a bilaterális megállapodásokat emeli ki a dokumentum. A stratégia csak korlátozottan foglalkozik a haderővel, és Oroszországot is csak egyszer említi az Inuit Sarkköri Tanács alapítása kapcsán, ott is csak lábjegyzetben.[34]

A stratégia nyolc célkitűzést rögzít, amelyek kivétel nélkül a békés és együttműködésen alapuló kapcsolatokat szorgalmazzák. Látható, hogy a biztonság katonai aspektusa kevés szerepet kap a stratégiában; helyette egy olyan civil megközelítést alkalmaz, amelyben a nemzetközi jog és az őslakosokkal való együttműködés élvez elsőbbséget.

A nemzetközi fejezet a stratégiában megfogalmazott célokat nemzetközi kontextusban vizsgálja. A rövid helyzetértékelést követően előbb az Arktiszi Tanács, majd a „robusztus" arktiszi nemzetközi rendszer többi tagjának szerepét vizsgálja meg. A stratégia kiemeli, hogy a régió geopolitikailag igen fontos, és jelentősége az arktiszi vizek klímaváltozás hatására bekövetkező könnyebb elérhetősége okán még tovább fog növekedni. A stratégia célul tűzi ki, hogy az amerikai–kanadai bilaterális találkozókat rendszeresítsék, és új alapokra helyezzék az orosz–kanadai kapcsolatokat is az őslakosok, a tudományos együttműködés, a környezetvédelem, a szállítás és a kutató-mentő tevékenységek kapcsán, hiszen közös érdekek, prioritások és kihívások vezérlik Kanadát és Oroszországot.[35]

Megállapíthatjuk, hogy míg a 2009-es kanadai stratégia erősen realista alapra építkezett, addig a tíz évvel későbbi stratégiát mintha maga Joseph Nye diktálta volna, olyan erősen érződik a más, liberálisabb politikai háttér és meggyőződés. Mindez visszatükröződik a két stratégia biztonságpolitikai megközelítésében is. A 2019-es, liberális megközelítés teljes mértékben tisztában van a térség geopolitikai jelentőségével és a klímaváltozás geopolitikára gyakorolt hatásával, amelyet nemcsak sejtet, hanem szövegszerűen is rögzít. Ugyanakkor ennek ellenére Kanada nem érzi úgy, hogy Oroszország rá nézve fenyegetést jelente, és elkötelezett az Oroszországgal való széles körű együttműködésre. E tekintetben tehát a krími válság nem befolyásolta Kanada biztonságpercepcióját a régió biztonságpolitikai kihívásait és elsősorban a lehetséges orosz fenyegetést illetően.

[34] *Canada's Arctic and Northern Policy Framework.* 2019. 15.
[35] *Canada's Arctic and Northern Policy Framework.* 2019.

2.7. Az Amerikai Egyesült Államok

Az Egyesült Államokban az adminisztrációváltás változásokat hozott az arktiszi szakpolitikával kapcsolatban is. A Bush- és az Obama-adminisztráció még nem fordított különösebb figyelmet a térségre, és elhanyagolta az infrastrukturális és katonai fejlesztéseket is.[36] A Védelmi Minisztérium 2011-ben kiadott jelentése még úgy fogalmazott, hogy nem valószínű fegyveres konfliktus a térségben az előrelátható jövőben és a már meglévő infrastruktúra megfelelő a rövid- és középtávú nemzetbiztonsági érdekeknek.[37] Az Obama-adminisztráció 2013-ban adta ki a *Nemzeti Stratégia az Arktiszi Régióhoz* című stratégiai dokumentumot.[38] A stratégia a régiót konfliktusmentes övezetnek tekinti, ahol a nemzetek felelősen együttműködnek a bizalom és a kooperáció jegyében. A stratégia Oroszországgal sem foglalkozik külön, mindössze az Arktiszi Tanáccsal kapcsolatban egy lábjegyzetben tesz róla említést. A stratégia – hasonlóan a fent elemzett dokumentumokhoz – kiemeli az éghajlatváltozás régiót érintő jelentős hatását és ennek következményeként az új kereskedelmi és gazdasági lehetőségek megnyílását. Ebben a gyorsan változó arktiszi környezetben az Egyesült Államok három fő célt kíván elérni: a saját nemzeti érdekeinek érvényesítését, a régió felelősségteljes kezelését és a nemzetközi együttműködés erősítését.[39]

A Trump-adminisztráció elsősorban biztonságpolitikai és gazdasági szempontból közelített a régió felé, így annak jelentősége elkezdett felértékelődni. Megkezdődött a jégtörő flotta felállítása,[40] kilátásba helyeztek szabad navigációs műveleteket[41] az Arktiszon, valamint felmerült a katonai jelenlét növelése és az infrastruktúra fejlesztése a Bering-tengeren.[42] 2019-ben a Védelmi miniszterhelyettesi Iroda[43] kiadta a *Védelmi Minisztérium Arktiszi Stratégiája* című dokumentumot,[44] amely a biztonsági környezetet komplexen ábrázolja. Egyfelől kiemeli, hogy az együttműködésnek már hagyománya van a térségben és az azonnali konfliktus kitörésének esélye alacsony, ugyanakkor felhívja a figyelmet számos olyan stratégiai tendenciára, amelyek veszélyeztethetik az Egyesült Államok érdekeit és ronthatják a régió stabilitását. A kulcsdinamikák, amelyek meghatározzák a régiót a következők:

- a fizikai környezet megváltozása;
- multilaterális együttműködés a közös érdekek és kihívások mentén;
- az arktiszi tengeri útvonalak státusza;
- növekvő katonai aktivitás;
- az arktiszi kormányzás manipulálása gazdasági erő által (Kína).

Kínával kapcsolatban a stratégia kiemeli, hogy bár nincs területi igénye a régióban, mégis részt akar venni az arktiszi kormányzásban, és az Egy Öv Egy Út kezdeményezés

[36] Holland 2014.
[37] U.S. Department of Defense 2011.
[38] Obama 2013.
[39] Obama 2013. 2.
[40] Trump 2020.
[41] Freedom of Navigation Operation (FONOP).
[42] Micallef 2020.
[43] Office of the Under Secretary of Defense.
[44] U.S. Office of the Under Secretary of Defense 2019.

részeként stratégiai gondolkodásának részét képezi a térség, összekötve az arktiszi stratégiáját a szélesebb stratégiai céljaival. (Nem véletlen, hogy 2018-ban Kína kiadta első arktiszi stratégiáját.) Az amerikai stratégia jelentős hangsúlyt fektet a haderő szerepére – nem meglepő módon, mivel azt a Védelmi Minisztérium adta ki. A dokumentum megjegyzi, hogy bár Kína „Arktisz közeli állam" jelzővel illeti magát, az Egyesült Államok nem ismeri el, hogy létezne ilyen kategória. A stratégia attól tart, hogy Kína alá fogja aknázni a régió nemzetközi normáit, és jelentős kockázata van annak, hogy a globálisan ismert ragadozó gazdasági viselkedése az Arktiszon is meg fog jelenni. Mégis, ami jelentős változás a 2013-as stratégiához és a legtöbb más északi állam arktiszi stratégiájához képest is, az az, hogy a dokumentum Oroszországot (Kína mellett) központi helyen kezeli. Azt az állítást, hogy a térségben növekszik a katonai aktivitás, elsősorban az orosz tevékenységekből vezeti le, és leszögezi, hogy Oroszország kihívást jelent a szabály alapú arktiszi régióra, mivel szabályozni akarja az északi-tengeri útvonalat. Az orosz (és kínai) kihívásra válaszul a stratégia az arktiszi gyakorlatok, képzések növelését és az infrastruktúra fejlesztését tűzte ki célul.[45]

A stratégia továbbá három pontban határozza meg az Egyesült Államok érdekeit a régióval kapcsolatban. Egyrészt az Arktiszt mint szülőföldet értelmezi, és úgy véli, hogy ezen a területen szuverén módon gyakorolhatja jogait – így joga van a területe megvédéséhez is. Továbbá az Arktiszra mint közös régióra tekint, ami azt is jelenti, hogy a régióban közös érdekek vannak a biztonságot és stabilitást illetően, az Egyesült Államoknak pedig késznek kell lennie, hogy az európai és indiai-csendes-óceáni erőegyensúly fenntartása érdekében az Arktiszon is képes legyen beavatkozni. Harmadrészt pedig abból indul ki, hogy az Arktisz a stratégiai versengés területe, ezért az Egyesült Államoknak az az érdeke, hogy továbbra is fent tudja tartani a globális erőkivetítési képességét, a hajózás és a repülés szabadságát, miközben korlátozza a kínai és az orosz törekvéseket, hogy stratégiai érdekeiket kényszerítő erővel érvényesítsék a régióban.

Ez a stratégia jelentősen eltér a többi vizsgált dokumentumtól. Hasonlóság ugyan, hogy felismeri: az Arktisz régióját a kooperáció és a nemzetközi jog alapú konfliktusmegoldás jellemzi, ahol az államok közötti fegyveres konfliktus esélye a jövőben is alacsony lesz; ugyanakkor más stratégiákkal ellentétben az amerikai dokumentum már globális perspektívából tekint a régióra, amit mi sem bizonyít jobban, mint a stratégia következő mondata: „Az északi-sarkvidéki fejlemények magukban hordozzák annak lehetőségét, hogy közvetlenül vagy közvetve korlátozzák az amerikai Védelmi Minisztérium globális erőkivetítési képességét, távolabbra tekintve pedig hatással legyenek a Kínával és Oroszországgal az indiai-, csendes-óceáni térségben, valamint az Európában folytatott versengéssel összefüggő amerikai stratégiai célokra."[46]

2.8. Oroszország

Oroszország szakpolitikáját a dokumentumok elérhetősége és a nyelvi korlátok miatt másodlagos források alapján dolgoztuk fel. Az orosz álláspontot jól tükrözi a 2008-as

[45] U.S. Office of the Under Secretary of Defense 2019. 6., 9.
[46] U.S. Office of the Under Secretary of Defense 2019. 6.

Az Orosz Föderáció Állami Szakpolitikájának Alapjai az Arktiszon[47] című stratégiában megfogalmazott vélemény az arktiszi kooperációról: „aktív interakciókat kell folytatni a szub-arktiszi államokkal a tengeri határokkal kapcsolatban a nemzetközi jog normáinak, a kölcsönös megállapodások és az Orosz Föderáció érdekeinek figyelembe vételével."[48] Az orosz álláspont lényege tehát az, hogy bár Oroszország nyitott a sarki államokkal való együttműködésre, azonban a lépéseit minden esetben az orosz érdekek fogják vezérelni. Ez akár jelenthet jövőbeli konfrontációt is, bár ennek lehetőségére nyíltan még maga Medvegyev elnök sem tért ki. Hogy melyek az Orosz Föderáció érdekei, azt maga a stratégia pontosan nevesíti:

- az Arktisz mint erőforrásbázis, amely megoldást nyújt Oroszország gazdasági és társadalmi problémáira;
- fenntartani a békét és az együttműködést az Arktiszon;
- az Arktisz egyedi ökológiai jellegzetességeinek fenntartása;
- az északi-tengeri útvonal mint egyedüli szállítási útvonal az Arktiszon.

Összehasonlítva a 2008-ban elfogadott 2020-ig érvényes alapelveket a 2020-ban elfogadott 2035-ig érvényes alapelvekkel megállapítható, hogy gazdasági szempontból nincs változás a két dokumentum között, és továbbra is központi stratégiai elem a béke és az együttműködés fenntartása. Ugyanakkor a 2020-as dokumentumban új elemként jelenik meg a szuverenitás biztosítása. A fogalom azonban nem mást takar, mint az előző stratégiai dokumentumban is már ismertetett célok összességét, így további katonai és civil modernizációra számíthatunk a jövőben is.[49] Oroszország szigorította a vizein áthaladó katonai és polgári hajókra vonatkozó előírásokat. 45 nappal a tervezett út előtt meg kell adni a hajó nevét, a hajózás célját, útvonalát és a hajózás időtartamát. Emellett a fedélzeten legalább egy orosz pilótának is tartózkodnia kell, és Oroszország fenntartja a jogot, hogy az északi tengeri útra való belépést bármikor megtagadja. Az új előírások oka részben a megnövekedett tengeri forgalom, de fontosabb az az orosz érdek, hogy Oroszország továbbra is képes legyen fenntartani a kereskedelmi hajózás feletti ellenőrzést.[50] Az orosz hadgyakorlatok továbbra is gyakoriak a térségben, 2018 óta a gyakorlatok során már éles lőszert is használnak.[51]

Az orosz stratégia kapcsán értelemszerűen nem az Oroszországról alkotott véleményt lehet vizsgálni, hanem az ország viszonyulását a többi arktiszi államhoz. Annak ellenére, hogy a tanulmányban Oroszországot kooperáló államként jellemezzük, nem lehet figyelmen kívül hagyni az elmúlt évek orosz törekvését az Arktisz (újra) militarizálására. 2007-ben Vlagyimir Putyin elrendelte a Jeges-tenger feletti járőrözést, aminek következtében stratégiai bombázók (Tu-95, Tu-160, Tu-22M3) jelentek meg a térségben.[52] A Kola-félszigeten állomásozó Északi Flotta jelentős fejlesztéseken esett át az elmúlt években elsősorban a tengeralattjáró-flotta tekintetében, a nukleáris elrettentés növelése céljából. 2008-ban Oroszország bejelentette, hogy ismét

[47] Medvedev 2008.
[48] Oroszról angolra fordította az Arctic Knowledge Hub, angolról magyarra pedig a szerzők.
[49] Klimenko 2020.
[50] Staalesen 2019.
[51] Nilsen 2019.
[52] Piffero Spohr 2013. 44.

hadihajók fognak járőrözni a Jeges-tengeren.[53] Oroszország emellett kifejlesztett egy arktiszi körülmények között is (-30 Celsius foktól 55 fokig) működőképes drónt, amely képes vízfelületen is landolni és onnan felszállni. Hivatalosan mentő szerepeket szánnak neki, azonban egy ilyen technológiának katonai implikációi is könnyen lehetnek.[54]

Mindezt figyelembe véve az orosz katonai építkezést nem lehet és nem szabad provokációnak értelmezni. Ennek főként geopolitikai okai vannak, és a gyakorlati tendencia sem ezt támasztja alá. Geopolitikai szempontból vizsgálva az országot, Oroszország legnagyobb előnye, amely megvédte 1812-ben Napóleontól, majd a második világháborúban Németországtól, a stratégiai mélysége. Egy európai államnak Oroszország legyőzéséhez mélyen be kellene hatolnia az ország területére. Ahogy a történelmi példák igazolják, saját korszakuk legerősebb hadseregei is belebuktak ebbe a vállalkozásba. A nyugati fenyegetés mellett számolni kellett a délivel is. A Kaukázus vonulatai mögött Oroszország területét nyílt síkságok uralják, többek közt Grúzia ezért is volt kiemelten fontos Oroszországnak 2008-ban, hiszen az amerikai befolyás megjelenése jelentősen megváltoztatta volna az orosz geopolitikai helyzetet. Amire viszont nem volt eddig példa, az az északi fenyegetés. Az Arktisz kiemelt szerepet élvez az orosz gazdaságban. Az Északi-sarkvidék adja az orosz földgáztermelés 91%-át, az ország feltárt földgázkészletének 80%-át, a tengerpart menti szénhidrogénkészleteinek 90%-át, valamint érclelőhelyének nagy részét.[55] Továbbá a térségben bányásznak sárgarezet, ónt, uránt és foszfátokat is. 2006-os adat szerint 25 bánya van az arktiszi területeken,[56] de a mai napig nyitnak új bányákat. A Roszatom például lítium bányákat tervez nyitni Szibériában 800 millió dollár értékben,[57] a Kola-félszigeten pedig gazdag apatit-,[58] alumínium-, vasérc-, csillámpala-, titán-, réz-, nikkel-, kobalt-, flogopit-[59] és vermikulit-[60] lelőhelyek találhatók.[61] Az észak felől érkező támadás eddig a technológia hiánya és az éghajlat miatt nem volt realitás. Ma azonban ez a tendencia megváltozni látszik, és a jég eltűnésével az orosz északi régiók is fenyegetettebbekké válnak. Egy, az Arktiszon kitörő fegyveres konfliktus éppen ezeket a létfontosságú gazdasági térségeket érintené először, ami jelentős csapás lenne az orosz gazdaságnak. Míg egy nyugatról jövő támadás során Oroszország (elméletileg) megteheti, hogy feladja a kevésbé fontos sztyeppéket, ezt északon nem teheti meg. Tehát Oroszország északi tevékenységét abból a szempontból is kell elemezni, hogy gazdaságilag az egyik legfontosabb területe egyre inkább kitetté válik.

Emellett az Arktisszal kapcsolatos orosz viselkedés is kooperáló állam képét mutatja. Valóban vannak területi vitái a térségben, de ezeket nem fegyverrel, unilaterális alapon kívánja megoldani, hanem a nemzetközi rendszer keretei között. Oroszország (elsőként) 2001-ben benyújtotta kérelmét az ENSZ Tengerjogi Egyezményére (UNCLOS)

[53] Piffero Spohr 2013. 44; Nowak 2008.
[54] Rescue Drone Taking off From Water Developed in Russia. 2021.
[55] Brzezinski 2020. 168.
[56] Glasby–Voytekhovsky 2010.
[57] Russia's Rosatom Plans to Launch Lithium Mines in Siberia, Arctic.
[58] Az apatitot műtrágya és mosószergyártáshoz használják.
[59] A flogopitot az autóiparban használt műanyagokhoz és azbeszt helyettesítésére használják fékeknél és váltóknál.
[60] A vermikulitot csíráztatáshoz, dugványozáshoz és magvetéshez használják.
[61] Glasby–Voytekhovsky 2010.

hivatkozva, utalva arra, hogy a Lomonoszov-hágó és az Alfa-Mengyelejev-hágó a szibériai talapzat része. A világszervezet az orosz kérelmet elutasította, mivel nem állt rendelkezésére elegendő adat az orosz igény alátámasztására.[62] 2013-ban Oroszország az Ohotszki-tenger kapcsán nyújtott be kérelmet, amelyet az illetékes bizottság[63] 2014-ben befogadott.[64] 2015-ben Oroszország ismét benyújtotta a 2001-es kérelmét, többévnyi kutatás eredményével kiegészítve,[65] amelyet azután 2021-ben kiegészített. Az új orosz területi igények már részben egybeesnek a kanadai és dán követelésekkel, ami előre vetíti a térségbeli konfliktusokat és a régió növekvő biztonságpolitikai jelentőségét.[66]

Az orosz fegyverkezést illetően gyakran hangsúlyozzák, hogy Oroszország rendelkezik a legnagyobb jégtörő flottával és nukleáris meghajtású jégtörőket is alkalmaz.[67] Bár tagadhatatlan, hogy katonai konvojok előtt is haladhatnak jégtörők, így kettős felhasználású eszköznek lehet tekinteni azokat, a jégtörő flotta feladata elsősorban mégsem ez. Oroszországban nagy hagyománya van a nukleáris jégtörő hajók építésének. Gyártásukat a Szovjetunióban 1957-ben kezdték meg, továbbá jelenleg Oroszország az egyetlen olyan ország, amely nukleáris jégtörő hajót üzemeltet. A jégtörő hajók építése és meghajtása is más, mint a többi hajóé, mivel jóval erősebb meghajtást igényelnek. Földrajzi adottságainál fogva számos orosz település egyszerűen rá van utalva a jégtörő flották nyújtotta képességre, mivel ezekre a településekre csak így juttatható el szállítmány, köztük az élelmiszer is. Azt, hogy miért van szükség ilyen jégtörőkre, talán a legjobban az 1983-as mentőakció mutatja be. 1983-ban az orosz jégtörő flotta 14 hajóból állt, ebből három nukleáris meghajtású volt (Lenin, Leonyid Brezsnyev és a Sibir). Az 1983-as ősz a vártánál is hidegebb volt, és több mint 20 tanker és teherhajó ragadt a jég fogságába. Mire a jégtörők, köztük több nukleáris meghajtású is, ki tudta szabadítani a hajókat, egyet már összetört a jég és elsüllyedt. E válság hatására számos változtatást vezettek be. A régebbi kisebb hajókat kivonták az Arktiszról, valamint kikötőfejlesztésbe kezdtek, hogy képesek legyenek nagyobb hajók befogadására. Több hajót állomásoztattak az arktiszi kikötőkben, hogy szükség esetén hamar el tudják kezdeni tevékenységüket. Megkezdték továbbá a LASH hajók[68] alkalmazását, amelyek bármelyik arktiszi kikötőben képesek ki- és berakodni.[69] Ez csak egy eset volt a sokból, azonban azt a következtetést le lehet vonni, hogy az orosz jégtörő flotta nagyságát részben a partvonal hossza, részben pedig a jég okozta kihívás indokolja, mintsem támadó szándék.

Államközi együttműködésekkel kapcsolatban kiemelendő, hogy 2015-ben a túlhalászat elkerülése érdekében Oroszország, az Egyesült Államok, Kanada, Dánia és Norvégia önként megállapodtak, hogy betiltják a kereskedelmi halászatot a Jeges-tengeren

[62] Heininen–Sergunin–Yarovoy 2014.
[63] Az ENSZ Kontinentális Talapzat Bizottsága (Commission on the Limits of Continental Shelf, CLCSÖ).
[64] Commission on the Limits of Continental Shelf 2014.
[65] *Russia Lays Claim to Vast Areas of Arctic.* 2015.
[66] *Russia Claims Continental Shelf in Artic Ocean.* 2021; Tranter 2021.
[67] Osborn 2021; Melino–Conley é. n.; Gady 2015.
[68] „A [LASH] a *Lighter Aboard Ship* angol kifejezés kezdőbetűiből képzett és a magyar hajózási szaknyelv által is használt kifejezés, mely a folyami-tengeri-folyami, ugyan végig vízi úton történő, de mégis kombinált áruszállítási mód megnevezésére szolgál." Lásd Hadházi é. n.
[69] Barr–Wilson 1985.

(a kizárólagos gazdasági övezeten belüli halászat kivételével).[70] Azóta az egyezmény új tagokkal bővült, mivel csatlakozott az Európai Unió, Kína, Japán és a Koreai Köztársaság is.[71] Ezt követően az Egyesült Államok, Kína, Japán, Oroszország, Kanada, Dánia, Norvégia, Izland, a Koreai Köztársaság és az Európai Unió közös kutatásban állapodtak meg a túlhalászat ellen, amelynek az előző megállapodás adta az alapját. Jelenleg pedig egy olyan testület létrehozása is tervben van, amely szabályozza az ellenőrizetlen halászatot, és eljár halászati viták esetén.[72]

2018-ban a Bering-szoroson áthaladó forgalom növekedése miatt az Egyesült Államok és Oroszország közösen tett javaslatot a Bering-szoroson és a Bering-tengeren áthaladó önkéntes hajózási útvonalak kialakítására, amelyet a Nemzetközi Tengerészeti Szervezet[73] elfogadott, és 2018-ban hatályba is léptetett.[74]

Végezetül az Arktisz a Föld azon kevés helyszíneinek egyike, ahol az Egyesült Államok és Oroszország vezérkari főnökei találkozhatnak. 2021 szeptemberében került sor Mark Milley, az amerikai Vezérkari Főnökök Egyesített Bizottságának elnöke és Valerij Geraszimov, az Orosz Fegyveres Erők Főparancsnoka határás megbeszélésére Finnországban.[75] Azonban nemcsak katonai vezetők találkoznak a térségben, hanem a félkatonai szervezetnek minősülő parti őrségek is. 2021-ben az Egyesült Államok Parti Őrsége és az orosz Tengeri Mentő Szolgálat megállapodott abban, hogy aktualizálják terveiket a nemzetközi tengeri szennyezés megakadályozása érdekében a Bering- és a Csukucs-tengeren. A megállapodást nem sokkal azután kötötték meg, hogy a parti őrség és az orosz határőrök közös járőrözést hajtottak végre a két ország tengeri határánál.[76] 2021 januárjában pedig az amerikai Polar Star hajó orosz repülőkkel hajtott végre kommunikációs gyakorlatokat és a jövőben továbbiakat is terveznek.[77]

3. Következtetések

Az Arktisz mint önálló régió létét, amelyre nem, vagy csak minimálisan hatnak más régiók konfliktusai, a fenti stratégiaelemzés igazolta. Megvizsgálva, hogy az államok stratégiai szinten milyen percepcióval rendelkeztek 2014 előtt és 2014 után, az az általános következtetés vonható le, hogy az arktiszi államok stratégiai szinten is érzékelték, hogy a globális biztonságpolitikai helyzet az elmúlt években jelentősen megváltozott. S bár régióspecifikus problémákról van szó, a legmeghatározóbb kérdés, amely az országokat foglalkoztatja, az éghajlatváltozás és az együttműködés fenntartása. Azt is meg kell jegyezni, hogy hatásként, még ha minimális mértékben is, de mind az állami szinten, mind az állam feletti szinten megfigyelhető volt az arktiszi integráció lassulása és néhány területet érintően visszaesése, leglátványosabban

[70] Hoag 2016.
[71] Európai Bizottság, Tengerügyi és Halászati Főigazgatóság 2021.
[72] Danilov 2021; Okuyama 2021.
[73] International Maritime Organization (IMO).
[74] Ham 2018; Fletcher et al. 2020.
[75] Liebermann–Kaufman 2021.
[76] Ez nem az első eset volt; már 2019-ben is hajtottak végre közös járőrözést. Lásd *Russian Border Guards, US Coast Guard Conduct Joint Patrolling in Bering Sea*. 2019.
[77] Schreiber 2021.

a katonai együttműködések terén. A kutatás eredményeit értékelve azonban a krími válság nem értékelhető olyan töréspontnak az Arktiszt érintően, amely megszakította volna a régióban zajló békés együttműködési folyamatokat.

Oroszország vonatkozásában a stratégiák elemzése alapján kijelenthető, hogy az ország az arktiszi régióban nem agresszorként lép fel, hanem együttműködésre törekszik. Oroszország számára kiemelten fontos az arktiszi régió mind gazdasági, mind biztonsági szempontból, és az ország ennek megfelelően cselekszik. A fő szempont a régió stabilitásának biztosítása a gazdasági potenciálok kiaknázása érdekében. Oroszország, bár növelte katonai képességeit a régióban, vitás ügyeinél mégsem alkalmazza a katonai erőt. A konfliktusoknál a tárgyalást részesíti előnyben, kiemelten követi a nemzetközi jog rendelkezéseit, és területi vitáknál aláveti magát a nemzetközi rezsim döntéseinek.

Mindezek alapján tehát bizakodhatunk, hogy a klímaváltozás nem várt, de minden bizonnyal rövidesen bekövetkező hatásai nem egy konfliktusokkal terhelt térség kialakulásához fognak vezetni az Arktiszt illetően, hanem az Északi-sarkvidék továbbra is olyan békés közeg marad, mint amilyen az elmúlt évszázadokban volt.

Felhasznált irodalom

A Parliamentary Resolution on Iceland's Arctic Policy. (2011. március 28.). Online: www.government.is/media/utanrikisraduneyti-media/media/nordurlandaskrifstofa/A-Parliamentary-Resolution-on-ICE-Arctic-Policy-approved-by-Althingi.pdf

Arctic Sovereignty a Priority: Harper. *CBC News,* 2010. augusztus 23. Online: www.cbc.ca/news/politics/arctic-sovereignty-a-priority-harper-1.951536

Barr, William – Wilson, Edward A. (1985): The Shipping Crisis in the Soviet Eastern Arctic at the Close of the 1983 Navigation Season. *Arctic,* 38. évf. 1. sz. 1–17. Online: https://doi.org/10.14430/arctic2101

Brzezinski, Zbigniew (2020): *Stratégiai vízió.* Budapest, Antall József Tuddásközpont.

Canada's Arctic and Northern Policy Framework. Goverment of Canada, 2019. Online: www.rcaanc-cirnac.gc.ca/DAM/DAM-CIRNAC-RCAANC/DAM-NTHAFF/STAGING/texte-text/nth-arctic_northern_policy_framework_1662642171557_eng.pdf

Canada's Northern Strategy: Our North, Our Heritage, Our Future (2009). Ottawa, Canada, Indian and Northern Affairs. Online: https://publications.gc.ca/collections/collection_2009/ainc-inac/R3-72-2008.pdf

Commission on the Limits of Continental Shelf: *Summary of Recommendations of the Commission on the Limits of the Continental Shelf in Regard of the Partial Revised Submission Made by the Russian Federation in Respect of the Sea of Okhotsk on 28 February 2013.* Subcommission established for the consideration of the Submission made by the Russian Federation (2014. február). Online: www.un.org/depts/los/clcs_new/submissions_files/rus01_rev13/rusrevrec.pdf

Danilov, Peter B. (2021): US, China and Russia Plan Joint Research in Order to Regulate Arctic Fishing. *High North News,* 2021. augusztus 2. Online: www.highnorthnews.com/en/us-china-and-russia-plan-joint-research-order-regulate-arctic-fishing

Defence Agreement 2018–2023 (2018). Danish Goverment. Online: www.fmn.dk/globalassets/fmn/dokumenter/forlig/-danish-defence-agreement-2018-2023-pdfa-2018.pdf

Dennis, Christopher (2019): US Officials Welcome Norway's New F-35 Capabilities in an Increasingly Competitive Northern Europe. *Stars and Stripes,* 2019. november 27. Online: www.stripes.com/theaters/europe/us-officials-welcome-norway-s-new-f-35-capabilities-in-an-increasingly-competitive-northern-europe-1.608872

Duxbury, Charles (2020): The 5 Most Important Races for the Arctic. *Politico,* 2020. január 1. Online: www.politico.eu/article/5-races-for-the-arctic-trade-resources-supremacy-tourism-salvation

Európai Bizottság, Tengerügyi és Halászati Főigazgatóság (2021): *Arctic: Agreement to prevent unregulated fishing enters into force* (2021. június 25.). Online: https://ec.europa.eu/oceans-and-fisheries/news/arctic-agreement-prevent-unregulated-fishing-enters-force-2021-06-25_hu

Finland's Strategy for Arctic Policy (2021). Finnish Government (2021. június 18.). Online: https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/163247/VN_2021_55.pdf?sequence=1&isAllowed=y

Finland's Strategy for the Arctic Region 2013. Prime Minister's Office Publication, 16/2013, (2013. augusztus 23.). Online: https://vnk.fi/documents/10616/1093242/J1613_Finland%E2%80%99s+Strategy+for+the+Arctic+Region.pdf/cf80d586-895a-4a32-8582-435f60400fd2

Fletcher, Sierra – Higman, Bretwood – Chartier, Alisha – Robertson, Tim (2020): *Adherence to Bering Strait Vessel Routing Measures in 2019.* Plymouth, (2020. április). Online: www.pewtrusts.org/-/media/assets/2020/04/200131nukaberingstraitroutingstudy.pdf

Gady, Franz-Stefan (2015): Russia and China in the Arctic: Is the US Facing an Icebreaker Gap? *The Diplomat,* 2015. szeptember 7. Online: https://thediplomat.com/2015/09/russia-and-china-in-the-arctic-is-the-us-facing-an-icebreaker-gap

Glasby, Geoff – Voytekhovsky, Jurij (2010): Arctic Russia: Minerals and Mineral Resources. *The Geological Society,* 2010. augusztus 8. Online: www.geolsoc.org.uk/Geoscientist/Archive/August-2010/Arctic-Russia-minerals-and-mineral-resources

Grätz, Jonas (2012): The Arctic: Thaw with Conflict Potential. *CSS Analysis in Security Policy,* 118. évf. 1–4. Online: https://doi.org/10.3929/ethz-a-007563656

Hadházi Dániel (é. n.): *LASH hajózás*. Online Vízügyi Szótár. Online: www.gwpszotar.hu/kifejezes/8047

Ham, Walter (2018): *U.S., Russia Propose Voluntary Bering Strait Shipping Routes*. U.S. Department of Defense (2018. január 25.). Online: www.defense.gov/News/News-Stories/Article/Article/1423960/us-russia-propose-voluntary-bering-strait-shipping-routes

Heininen, Lassi – Sergunin, Alexander – Yarovoy, Gleb (2014): *Russian Strategies in the Arctic: Avoiding a New Cold War*. Moszkva, Valdai Discussion Group. (2014. szeptember). Online: www.uarctic.org/media/857300/arctic_eng.pdf

Herz, John H. (1950): Idealist Internationalism and the Security Dilemma. *World Politics,* 2. évf. 2. sz. 157–180. Online: https://doi.org/10.2307/2009187

Hoag, Hannah (2016): Nations Negotiate Fishing in Arctic High Seas. *The New Humanitarian,* 2016. április 28. Online: https://deeply.thenewhumanitarian.org/arctic/articles/2016/04/28/nations-negotiate-fishing-in-arctic-high-seas

Holland, Andrew (2014): National Security in a Rapidly Changing Arctic: How a Lack of Attention to the Arctic is Harming America's Interests. *Georgetown Journal of International Affairs,* 15. évf. 1. sz. 79–88. Online: www.jstor.org/stable/43134266

Iceland and NATO (é. n.) Government of Iceland. Online: www.government.is/diplomatic-missions/permanent-delegation-of-iceland-to-nato/iceland-and-nato/

Käpylä, Juha – Mikkola, Harri (2013): *Arctic Conflict Potential – Towards an Extra-arctic Perspective.* FIA Briefing paper 138. Helsinki, 2013. szeptember 24. Online: www.fiia.fi/wp-content/uploads/2017/01/bp138.pdf

Kingdom of Denmark Strategy for the Arctic 2011–2020 (2011). Copenhagen, Ministry of Foregin Affairs. Online: http://library.arcticportal.org/1890/1/DENMARK.pdf

Klimenko, Ekaterina (2020): *Russia's new Arctic Policy Document Signals Continuity Rather than Change.* Stockholm International Peace Research Institute, (2020. április 06.). Online: www.sipri.org/commentary/essay/2020/russias-new-arctic-policy-document-signals-continuity-rather-change

Kulesa, Łukasz – Frear, Thomas – Raynova, Denitsa (2016): Existing Arrangements to Manage Incidents in the Euro-Atlantic Are. In *Managing Hazardous Incidents in the Euro-Atlantic Area: A New Plan of Action.* European Leadership Network, 2016. Online: www.europeanleadershipnetwork.org/wp-content/uploads/2017/10/ELN-Managing-Hazardous-Incidents-November-2016.pdf

Liebermann, Oren – Kaufman, Ellie (2021): Top US General Mark Milley Meets with His Russian Counterpart in Finland. *CNN,* 2021. szeptember 22. Online: https://edition.cnn.com/2021/09/22/politics/milley-russia-meeting-finland/index.html

Medvedev, Dimitrij (2008): *Basics of the State Policy of the Russian Federation in the Arctic for the Period till 2020 and for a Further Perspective.* Arctic Knowledge Hub. Online: www.arctis-search.com/Russian+Federation+Policy+for+the+Arctic+to+2020

Melino, Matthew – Conley, Heather A. (é. n.): The Ice Curtain: Russia's Arctic Military Presence. *CSIS.* Online: www.csis.org/features/ice-curtain-russias-arctic-military-presence

Micallef, Joseph V. (2020): President Trump's New Polar Strategy Is the First Step to Defending the Arctic. Military.com, 2020. augusztus 4. Online: www.military.com/daily-news/opinions/2020/08/04/president-trumps-new-polar-strategy-first-step-defending-arctic.html

Moe, Arild – Fjaertoft, Daniel – Øverland, Indra (2011): Space and Timing: Why Was the Barents Sea Delimitation Dispute Resolved in 2010? *Polar Geography,* 34. évf. 2 sz. 145–162. Online: https://doi.org/10.1080/1088937X.2011.597887

Nilsen, Thomas (2019): Russian Navy to Hold Live-Fire Exercise off Northern Norway. *The Independent Barents Observer,* 2019. augusztus 6. Online: https://thebarentsobserver.com/en/security/2019/08/russian-navy-announces-comprehensive-exercise-northern-norway

Norway's Arctic Policy (2014). Oslo, Norwegian Ministry of Foreign Affairs. Online www.regjeringen.no/globalassets/departementene/ud/vedlegg/nord/nordklo-den_en.pdf
Nowak, David (2008): Russian Warships to Patrol Arctic. *The Guardian,* 2008. július 15. Online: www.theguardian.com/world/2008/jul/15/russia.arctic
Obama, Barack (2013): *National Strategy for the Arctic Region*. U.S., 2013. május 10. Online: https://obamawhitehouse.archives.gov/sites/default/files/docs/nat_arctic_strategy.pdf
O'Dwyer, Gerald (2021): Norway and Russia Sharpen Transparency Pact on Warship, Aircraft Moves. *Defense News,* 2021. augusztus 20. Online: www.defense-news.com/global/europe/2021/08/20/norway-and-russia-sharpen-transparency-pact-on-warship-aircraft-moves
Okuyama, Miki (2021): International Research Planned to Manage Arctic Fish Stocks. *Nikkei Asia,* 2021. augusztus 1. Online: https://asia.nikkei.com/Politics/International-relations/International-research-planned-to-manage-Arctic-fish-stocks
Osborn, Kris (2021): Russia's Arctic Icebreakers Could Conduct Armed Military Missions. *The National Interest,* 2021. január 12. Online: https://nationalinterest.org/blog/buzz/russia's-arctic-icebreakers-could-conduct-armed-military-missions-176243
Piffero Spohr, Alexandre et al. (2013): The Militarization of the Arctic: Political, Economic and Climate Challenges. *Model United Nations Journal,* 1. évf. 11–70. Online: www.ufrgs.br/ufrgsmun/2013/wp-content/uploads/2013/10/The-Militarization-of-the-Arctic-Political-Economic-and-Climate-Changes.pdf
Rescue Drone Taking off From Water Developed in Russia. *Tass,* 2021. szeptember 28. Online: https://tass.com/economy/1343447
Russia Claims Continental Shelf in Artic Ocean. *The Moscow Times,* 2021. április 12. Online: www.themoscowtimes.com/2021/04/12/russia-claims-continental-shelf-in-arctic-ocean-a73566
Russia Lays Claim to Vast Areas of Arctic. *The Guardian,* 2015. augusztus 4. Online: www.theguardian.com/world/2015/aug/04/russia-lays-claim-to-vast-areas-of-arctic-seabed
Russian Border Guards, US Coast Guard Conduct Joint Patrolling in Bering Sea.*TASS,* 2019. június 11. Online: https://tass.com/society/1063239
Russia's Rosatom Plans to Launch Lithium Mines in Siberia, Arctic. *Engineering and Mining Journal,* 2021. augusztus 5. Online: www.e-mj.com/breaking-news/russias-rosatom-plans-to-launch-lithium-mines-in-siberia-arctic/
Schreiber, Melody (2021): U.S. And Russia Sign New Maritime Pollution Agreement, Conduct Joint Bering Sea Patrol. *Arctic Today,* 2021. február 11. Online: www.arctictoday.com/u-s-and-russia-sign-new-maritime-pollution-agreement-conduct-joint-bering-sea-patrol
Staalesen, Atle (2019): Russia Sets Out Stringent New Rules for Foreign Ships on the Northern Sea Route. *Arctic Today,* 2019. március 8. Online: www.arctictoday.com/russia-sets-out-stringent-new-rules-for-foreign-ships-on-the-northern-sea-route/
Sweden's Strategy for the Arctic Region (2011). Goverment Offices of Sweden, Stockholm. Online: www.government.se/contentassets/85de9103bbbe4373b55eddd7f71608da/swedens-strategy-for-the-arctic-region

The Norwegian Government's Arctic Policy (2021). Oslo, Norwegian Ministry of Foreign Affairs. Online: www.regjeringen.no/globalassets/departementene/ud/vedlegg/nord/arctic_strategy.pdf

Tranter, Emma (2021): 'You Cannot Claim Any More:' Russia Seeks Bigger Piece of Arctic. *CBC News*, 2021. április 11. Online: www.cbc.ca/news/canada/north/russia-arctic-ocean-canada-united-nations-continental-shelf-1.5983289

Trump, Donald J. (2020): *Memorandum on Safeguarding U.S. National Interests in the Arctic and Antarctic Regions*. 2020. június 9. Online: https://uaf.edu/caps/resources/policy-documents/us-memorandum-on-safeguarding-natl-interests-in-the-arctic-and-antarctic-regions-2020.pdf

U.S. Office of the Under Secretary of Defense (2019): *Report to Congress Department of Defense Arctic Strategy.* Virginia, 2019. június. Online: https://media.defense.gov/2019/Jun/06/2002141657/-1/-1/1/2019-DOD-ARCTIC-STRATEGY.PDF

U.S. Department of Defense (2011): *Report to Congress on Arctic Operations and the Northwest Passage.* 2011. május 25. Online: https://dod.defense.gov/Portals/1/Documents/pubs/Tab_A_Arctic_Report_Public.pdf

Tartalom