



HADMÉRNÖK

Kiemelt közlemények

HALMI LAJOS: *Szívfrekvencia-variabilitás monitorozása légi járművek fedélzetén*

PAPP ISTVÁN, BÉKÉSI BERTOLD, KÁROLY KRISZTIÁN: *Pilóta nélküli légi járművek rajirányítási és rakétavezérlési vizsgálata komplex légi műveletek során*

BIRÓ GABRIELLA: *A katonai és civil infrastruktúrák összefonódása az orosz-ukrán háború kiberműveleteiben*

21. évf. (2026)
2. szám

ISSN 1788-1919 (elektronikus)



LUDOVIKA
EGYETEMI KIADÓ

Hadmérnök

Katonai műszaki tudományok online folyóirata

ISSN 1788-1919 (elektronikus)

A szerkesztőbizottság elnöke

Kovács László vezérőrnagy, egyetemi tanár

A szerkesztőbizottság elnökhelyettese

Munk Sándor ny. ezredes, professor emeritus

A szerkesztőbizottság tagjai

Alexandru Babos alezredes, egyetemi docens

Berek Tamás ezredes, egyetemi tanár

Bryson Payne egyetemi docens

Eleki Zoltán ezredes

Földi László ezredes, egyetemi tanár

Haig Zsolt ezredes, egyetemi tanár

Horváth Attila ny. ezredes, egyetemi tanár

Kállai Attila alezredes, egyetemi docens

Lukács László ny. alezredes, egyetemi tanár

Pohl Árpád ny. dandártábornok,
egyetemi docens

Josef Procházka ny. alezredes, egyetemi docens

Szászi Gábor ezredes

Taksás Balázs őrnagy, egyetemi docens

Turcsányi Károly ny. ezredes, egyetemi tanár

Ujházy László ezredes, egyetemi docens

Szerkesztőség

Főszerkesztő

Farkas Tibor egyetemi docens

Szerkesztőségi tagok

Biró Gabriella, tanársegéd

Kovács László vezérőrnagy, egyetemi tanár

Németh József Lajos egyetemi docens

Nemzeti Közszerológiai 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 Közszerológiai 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, Resofszi Ágnes



Tartalom

Védeleminformatika

BÁNYÁSZ-VÁCZI KINCŐSŐ BORÓKA, RAJKI ZOLTÁN: <i>A bölcsészet-, társadalomtudományi és pedagógiai szakokon tanuló hallgatók perspektívái a mesterséges intelligencia lehetőségeiről és kockázatairól, 2. rész</i>	5
BIRÓ GABRIELLA: <i>A katonai és civil infrastruktúrák összefonódása az orosz–ukrán háború kiberműveleteiben</i>	27
GÁBOR FAZEKAS: <i>Multispectral Reconnaissance of Operational Areas</i>	45
ISTVÁN PARÁDA: <i>Cybersecurity Failures in Enterprise MDM Platforms</i>	61

Környezetbiztonság

TAMÁS STADLER: <i>Military-related Heavy Metal Pollution in Soil</i>	75
--	----

Katonai műszaki infrastruktúra

FÖLDES TIBOR: <i>Védett létesítmények fizikai védelme</i>	87
---	----

Katonai logisztika

SZAJKÓ GYULA, LÉVAI ZSOLT: <i>A közúti infrastruktúrák katonai megfelelőségi vizsgálata a logisztikai felderítés végrehajtásakor, 1. rész</i>	103
---	-----

Haditechnika

GÁBOR FARKAS: <i>Augmentation of Training Data for AI-based Drone Detection System.</i>	119
HALMI LAJOS: <i>Szívfrekvencia-variabilitás monitorozása légi járművek fedélzetén</i> . .	137
PAPP ISTVÁN, BÉKÉSI BERTOLD, KÁROLY KRISZTIÁN: <i>Pilóta nélküli légi járművek rajirányítási és rakétavezérlési vizsgálata komplex légi műveletek során</i>	149

Bányász-Váczi Kincső Boróka,¹ Rajki Zoltán²

A bölcsészet-, társadalomtudományi és pedagógiai szakokon tanuló hallgatók perspektívái a mesterséges intelligencia lehetőségeiről és kockázatairól, 2. rész

Perspectives of Students in the Humanities, Social Sciences, and Education on the Opportunities and Risks Associated with Artificial Intelligence, Part 2

Absztrakt

A tanulmány egy kétrészes cikksorozat második része. Az első rész elméleti keretet és átfogó szakirodalmi áttekintést adott, míg a jelen írás 1027 bölcsészettudományi, társadalomtudományi és pedagógiai képzésben részt vevő hallgató kérdőíves vizsgálatának eredményeit elemzi. A kutatás célja annak feltárása volt, hogy a hallgatók miként értékelik a mesterséges intelligencia jövőbeli szerepét a mindennapi életben és a munkaerőpiacon, milyen kockázatokat azonosítanak, valamint milyen jelentőséget tulajdonítanak az MI-kompetenciáknak saját karrierjük szempontjából. A válaszadók többsége számottevő társadalmi hatással számol, ugyanakkor a karrierre gyakorolt hatás megítélése differenciált. A hallgatók 42,5%-a nem vár érdemi befolyást pályájára, 30,4%

¹ Nemzeti Közszerológati Egyetem Nemeskürty István Tanárképző Kar, e-mail: vaczi.kincso.boroka@uni-nke.hu

² PPKE BTK Szociológiai Intézet, e-mail: zoltan.rajki@btk.ppke.hu

pozitív, 27,2% negatív következményekkel számol. Az MI-technológiák ismeretét 70,3% fontosnak vagy elengedhetetlennek tartja. A kockázátészlelés különösen erős a vizuális manipuláció, az álhírek terjesztése, az adatvédelem és a magánélet védelme esetében, a nők és a levelező tagozatos hallgatók több dimenzióban magasabb kockázati értékeket adtak. A rendszeres MI-használók nagyobb arányban várnak pozitív karrierhatást (39,5%), mint a nem használók (26,2%), miközben a nem használók körében gyakoribb a semleges álláspont (47,1%). Az MI-használattól teljesen elzárkózók 64,8%-a nem tartja fontosnak az MI-eszközök ismeretét. Az eredmények alapján a karrierpercepció a használati tapasztalat, a kockázátészlelés és a demográfiai jellemzők együttes hatásaként értelmezhető. A 68,1%-os nem használói arány arra utal, hogy az MI felsőoktatási integrációja korlátozott, ami célzott kompetenciafejlesztést indokol, különösen a humán és pedagógiai képzési területeken.

Kulcsszavak: mesterséges intelligencia, felsőoktatás, munkaerőpiac, attitűdvizsgálat, kvantitatív elemzés

Abstract

This study constitutes the second part of a two-part research series. The first part provided a theoretical framework and a comprehensive literature review, while the present paper analyses the results of a questionnaire survey conducted among 1,027 students enrolled in humanities, social sciences, and teacher education programmes. The aim of the study was to explore how students evaluate the future role of artificial intelligence in everyday life and in the labour market, which risks they identify, and how important they consider AI-related competencies for their future careers. The majority of respondents anticipate substantial societal impact; however, perceptions of career-related effects are differentiated. While 42.5% do not expect AI to significantly influence their career paths, 30.4% foresee positive and 27.2% negative consequences. Overall, 70.3% regard knowledge of AI technologies as important or indispensable for their future careers. Risk perception is particularly high in relation to visual manipulation, misinformation, data security, and privacy protection. Female students and part-time students report higher levels of perceived risk across several dimensions. Regular AI users are more likely to expect positive career effects (39.5%) compared to non-users (26.2%), whereas neutral evaluations are more prevalent among non-users (47.1%). Among those who completely reject AI use, 64.8% do not consider AI-related knowledge important for their careers. The findings suggest that career perceptions related to AI are shaped by the combined influence of usage experience, risk perception, and demographic characteristics. The high proportion of non-users (68.1%) indicates that AI integration in higher education remains limited, highlighting the need for targeted competence development, particularly in humanities and teacher education programmes.

Keywords: artificial intelligence, higher education, labour market, attitude analysis, quantitative analysis

A vizsgálat bemutatása

A jelen tanulmány egy kétrészes cikksorozat második része. Az első rész a releváns nemzetközi és hazai szakirodalom szisztematikus feldolgozására, valamint az elméleti keretek meghatározására irányul,³ míg a jelen írás 1027 hallgató bevonásával végzett kvantitatív vizsgálat eredményeit ismerteti. Az elemzés a bölcsészettudományi, társadalomtudományi és pedagógusképzésben részt vevő hallgatók mesterséges intelligenciával (MI) kapcsolatos attitűdjeit, jövőorientációját és használati hajlandóságát vizsgálta.

A vizsgálat célja annak feltárása volt, hogy a bölcsészettudományi, társadalomtudományi és pedagógusképzésben tanuló hallgatók miként értékelik az MI jövőbeli karrierjükre és mindennapi életükre gyakorolt hatását. A kutatás azonosította azokat a területeket, amelyeket a válaszadók az MI alkalmazásával összefüggésben kockázatosnak tartanak, továbbá felmérte, milyen jelentőséget tulajdonítanak az MI-alapú alkalmazásokban való jártasságnak. Az elemzés kiterjedt a nemek, a képzési területek és a képzési formák közötti különbségek vizsgálatára, valamint arra, hogy eltérés mutatkozik-e az MI jövőbeli hatásainak megítélésében az aktív és nem aktív felhasználók, illetve a technológiára nyitott és attól elzárkózó hallgatók között.

A kutatási célkitűzésekkel összhangban az alábbi kutatási kérdésekre kerestük a választ az elemzés során:

- Milyen jövőképek van az egyetemi bölcsészettudományi, társadalomtudományi és pedagógia szakos hallgatóknak az MI-vel kapcsolatban a munkaerőpiacon?
- Melyek azok a területek, amelyeket kockázatosnak találnak az oktatásban és a mindennapok MI-használata során?
- Mennyire felkészültek a jövő munkaerőpiaci kihívásaira a megkérdezett hallgatók?
- Összefügg-e az MI használata vagy az arra való nyitottság a karrierrel kapcsolatos várakozásokkal és az MI-ismeretek fontosságának megítélésével?

A kutatási kérdésekhez kapcsolódóan a következő hipotéziseket fogalmaztuk meg:

- H1: Az MI használatára nyitottabb hallgatók kevésbé érzékelik az MI kockázatait.
- H2: Az MI-eszközöket rendszeresen használó hallgatók kevésbé érzékelik annak kockázatait.
- H3: Az MI-eszközöket rendszeresen használó hallgatók pozitívabbnak ítélik az MI szerepét jövőbeli karrierjük szempontjából.
- H4: Azok a hallgatók, akik magasabb szintű kockázatot érzékelnek az MI-vel kapcsolatban, kevésbé optimisták az MI jövőbeli karrierjükre gyakorolt szerepét illetően.
- H5: Azok a hallgatók, akik elzárkóznak az MI használatától, kevésbé tartják relevánsnak az MI-eszközök ismeretét jövőbeli karrierjük szempontjából.

A hipotézisrendszert három, egymással összefüggő dimenzió mentén alakítottuk ki, az MI-hez kapcsolódó attitűd és használati nyitottság, a kockázatesztelés, valamint a karrierrelevancia és a foglalkoztathatósággal összefüggő optimizmus mentén. Az első két hipotézisünk arra irányult, hogy kimutatható-e alacsonyabb kockázatesztelés azok

körében, akik nyitottabb attitűddel viszonyulnak a technológiához, illetve rendszeres használónak tekinthetők. E feltevések összhangban állnak azzal a szakirodalmi megközelítéssel, amely az elfogadás és a kockázatesztelés között negatív irányú kapcsolatot azonosít,³ ugyanakkor figyelembe veszi a nyitottság és a kockázattudatosság együttes jelenlétének lehetőségét is.⁴

A további hipotézisek a használat, illetve a kockázatesztelés és a karrieroptimizmus közötti kapcsolat empirikus megerősítésére irányultak. A kiinduló feltételezésünk szerint a rendszeres MI-használat, valamint az MI-hez kapcsolódó kompetenciák fontosságának elismerése pozitív összefüggést mutathat a karrierrel kapcsolatos bizalommal,⁵ míg a magasabb szintű kockázatesztelés az optimizmus csökkenésével és a bizonytalanságérzet erősödésével járhat együtt.⁶ A vizsgálat empirikus célja e dimenziók közötti összefüggések tesztelése, valamint a hallgatói attitűdök és jövőbeli várakozások strukturált feltárása volt.

Mintavételi eljárás

A mintavétel során azokat a felsőoktatási intézményeket kerestük fel intézeti és tanszéki szinten, ahol bölcsészettudományi, társadalomtudományi, illetve pedagógiai képzési területeken alap-, mester- vagy PhD-képzés zajlik nappali vagy levelező tagozaton. A hallgatókat e-mailen keresztül (például tanszéki levelezőlistákon) és Facebookon (például hivatalos hallgatói csoportokon) keresztül értük el. Az online kérdőívet a Survio.com platformon tettük közzé 2023. szeptember 14. és 2023. október 14. között. A saját készítésű kérdőív 27 kérdést tartalmazott, köztük nyílt végű, zárt végű egy- és többválaszos, valamint Likert-skálára épülő kérdéseket.

A publikáció és az adatgyűjtés közötti időtáv elsősorban a szakirodalom szisztematikus feldolgozásának időigényéből adódik. A kutatás célja az empirikus eredmények elméleti beágyazása volt a nemzetközi MI-kutatások kontextusába, ami a gyorsan bővülő szakirodalom kritikai áttekintését és integrálását igényelte. A tanulmány kétrészes felépítése szintén hozzájárult az időhorizonthoz, mivel az empirikus elemzés az első, elméleti rész publikálását követte, amelynek leadása 2025 év elején történt.

A kérdőívet 1201 fő töltötte ki. Néhány felsőfokú szakképzésben részt vevő hallgató kivételével a kitöltők egyetemen vagy főiskolán tanultak, közülük azonban 1027 fő tartozott a kutatásban vizsgált képzési területekhez, vagyis a bölcsészettudományi, társadalomtudományi és pedagógiai szakokon tanuló hallgatók körébe. A tanulmány további részében kizárólag az ő adataikat elemezzük ($n = 1027$). A kutatás szempontjából releváns kitöltők 53,8%-a a Pázmány Péter Katolikus Egyetem Bölcsészeti- és Társadalomtudományi Karán (PPKE BTK), 13,5%-a a Kodolányi János Egyetemen, 8,4%-a a Gál Ferenc Egyetemen, míg 24,3%-uk egyéb felsőoktatási intézményekben

³ MUSYAFFI et al. 2024.

⁴ LI-CASTULO-XU 2025.

⁵ BAVADHARANI-ROSHAN-KALAIVANI 2025.

⁶ LIANG-ZHAI 2025.

tanult.⁷ A minta 83,2%-a alapképzésben, 11,1%-a mesterképzésben, 4,5%-a osztatlan képzésben, míg 1,3%-a PhD-képzésben végezte tanulmányait. A kitöltők több mint 10%-a tanult modern nyelvi szakokon (11,3%), kommunikáció és médiatudomány szakon (13,4%), politika és nemzetközi tanulmányok szakon (11,3%), szociológia szakon (11,5%), pszichológia szakon (11,1%), illetve pedagógia, tanító, tanár vagy óvopedagógus szakokon (19,8%). Képzési területekre lebontva a hallgatók 34,5%-a bölcsészettudományi, 43,7%-a társadalomtudományi és 21,1%-a pedagógiai képzési területen végezte tanulmányait. A kitöltők 79%-a nő, míg 21%-a férfi volt. A mintánk életkori megoszlását illetően több mint a fele (54,3%) 18–22 év közötti volt, 20%-ot tett ki a 23–30 év közöttiek, illetve 25,7%-ot a 31 és a felettiek aránya. A kérdőívet kitöltők 37,3%-a nem dolgozott, 29,8%-a részmunkaidőben, míg 32,9%-a teljes munkaidőben dolgozott az egyetemi tanulmányai alatt.

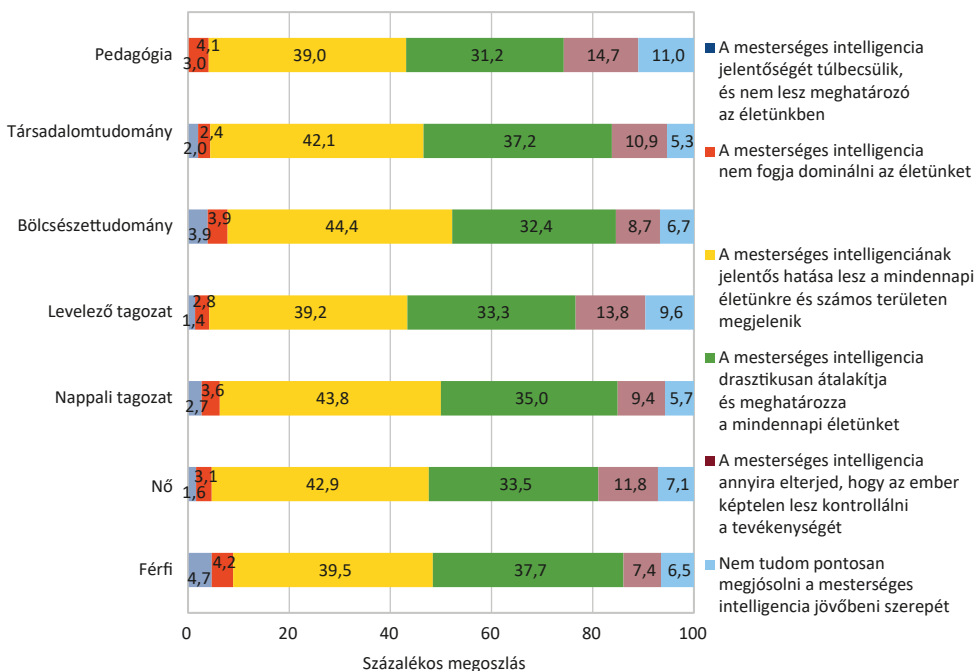
Az adatfelvétel nem valószínűségi mintavételi eljárással zajlott. A minta intézményileg koncentrált, a válaszadók 53,8%-a egyetlen intézmény (PPKE BTK) hallgatója. Emellett a nemi összetétel erősen torzított (nők: 79%), ami a nemek szerinti összehasonlítások értelmezésekor óvatosságot indokol. Mindezek az eredmények általánosíthatóságát korlátozzák; a feltárt összefüggések inkább jelzésértékűek, mint reprezentatív érvényűek. A jelentős elemszám ($n = 1027$) lehetővé teszi a statisztikai tesztek alkalmazását, de nem pótolja a valószínűségi mintavételt. Az adatfeldolgozást az IBM SPSS 20.0 szoftverrel végeztük, az ábrák elkészítéséhez pedig a Microsoft Excel programot használtuk.

A kérdőív három tematikus blokkra épült. Az első blokk az MI mindennapi életben és a munkaerőpiacon betöltött jövőbeli szerepének megítélését vizsgálta két nominális kérdéssel: az MI általános társadalmi hatásának megítélése hat válaszlehetőséggel (a drasztikus átalakulástól a túlértékelt technológia percepciójáig), illetve a karrierre gyakorolt várható hatás három kategóriával (pozitív/semleges/negatív). Az MI-ismeretek karrierrelevanciáját négy szintű ordinális skálán mértük (elengedhetetlen – fontos, de nem elengedhetetlen – nem fontos, de előnyös – egyáltalán nem fontos). A második blokk a kockázatszűrés hét területen vizsgálta ötfokozatú Likert-skálán (1 = egyáltalán nem kockázatos, 5 = nagyon kockázatos): adatvédelem, magánélet védelme, döntéshozatali elfogultság, munkahelyek elvesztése, álhírek terjesztése, kép- és videószerkesztő programokkal való visszaélés, illetve az esélyegyenlőtlenség fokozódása. A harmadik blokk az MI-használat intenzitását kilenc alkalmazási területen mérte ötfokozatú skálán (nem hallott róla – rendszeresen használja), amelyből két-értékű rendszeres használói indikátort képeztünk. A nyitottságot négy kontextusban vizsgáltuk három kategóriás skálán (nem használja és nem is használná – nem használja, de szívesen használná – használja): tanulás, munkahelyi feladatok, szórakozás és kommunikáció. A kockázatszűrés kumulatív mutatóját az egyes dimenziókban magas értéket (4–5) kapott területek összeszámolásával képeztük (0–7 skála).

⁷ A mintában a további legalább 1%-ot képviselő felsőoktatási intézmények: Debreceni Egyetem: 2,9%, ELTE: 5%, Károli Gáspár Református Egyetem: 4,4%, Miskolci Egyetem: 3,1%, Nyíregyházi Egyetem: 1,7%, Pannon Egyetem: 1,7%, illetve a Pécsi Tudományegyetem: 2,9%.

A mesterséges intelligencia jövőbeli szerepe a mindennapi életben és a karrierben

A kutatás három kérdés mentén vizsgálta, hogy a bölcsészettudományi, társadalomtudományi és pedagógiai képzési területen tanuló hallgatók miként ítélik meg a mesterséges intelligencián alapuló alkalmazások jövőbeli térnyerését a mindennapi életben, azok karrierre gyakorolt hatását, valamint az MI-eszközök ismeretének jelentőségét saját pályáútjuk szempontjából. Az elemzés három dimenzióra fókuszált, a mindennapi életre gyakorolt várható hatásra, a karrierrelevanciára és a kompetenciaszintű felkészültség fontosságára, egységes értelmezési keretben vizsgálva a hallgatói percepciókat. A válaszadók többsége számottevő társadalmi átalakulást prognosztizál.



1. ábra: Szerinted mennyire kap fontos szerepet a mesterséges intelligencia a jövőben a mindennapi életünk során?, N = 1027 (%)

Forrás: a szerzők szerkesztése

A hallgatók 34,4%-a drasztikus változást vár, 42,2% több területre kiterjedő jelentős hatással számol, míg 10,9% szerint az MI elterjedése a kontroll elvesztésének kockázatát hordozza, továbbá csekély vagy elhanyagolható hatást mindössze 5,5% valószínűsít. A minta alapján a hallgatók többsége – a nemzetközi kutatásokban megfigyelttel párhuzamosan – a mesterséges intelligencia jelentős társadalmi hatásával számol, miközben a technológia elterjedéséhez kapcsolódó kockázatokat is tudatosítja.⁸

⁸ YAROVENKO et al. 2024; NKEDISHU–OKONTA 2024.

A kontrollvesztéstől való félelem kisebbségi álláspontként jelenik meg, ami megfelel a korábbi empirikus eredményeknek.⁹

A nemek között következetes eltérések (χ^2 , $p = 0,034$) azonosíthatók, ahogyan ezt az 1. ábra is szemlélteti. A férfi hallgatók nagyobb arányban számítanak drasztikus hatásra (37,7% vs. 33,5%), illetve gyakrabban tekintik túlértékeltnek az MI jelentőségét (4,7% vs. 1,6%), miközben körükben alacsonyabb a kontrollvesztéstől való félelem (7,4% vs. 11,8%). A női hallgatók ezzel szemben erőteljesebb aggodalmat jeleznek a társadalmi következményekkel kapcsolatban, ami egybeesik azokkal a kutatásokkal, amelyek nemi különbségeket mutatnak ki az MI-hez kapcsolódó kockázatesztelés és optimizmus terén.¹⁰ A levelező hallgatók (χ^2 , $p = 0,026$) körében magasabb a kontrollvesztési forgatókönyv elfogadottsága (13,8% vs. 9,4%). Képzési terület szerint a bölcsészhallgatók (χ^2 , $p = 0,045$) inkább mérsékeltebb hatást valószínűsítene, míg a pedagógiai képzésben (χ^2 , $p = 0,001$) részt vevők körében felülreprezentált a bizonytalanság és a kontrollvesztéstől való félelem, ami a nem technikai diszciplínák hallgatóira jellemző kritikusabb attitűdöt tükrözi.¹¹

A karrierre gyakorolt hatás megítélése differenciált képet mutat. A válaszadók 42,5%-a nem vár érdemi befolyást jövőbeli pályájára, 30,4% pozitív, 27,2% negatív következményekkel számol. A pozitív várakozások aránya enyhén meghaladja a negatív percepciókat, ugyanakkor a relatív többség semleges álláspontot képvisel. A nemi különbségek ezen a területen is markánsak (χ^2 , $p = 0,001$). A férfi hallgatók 40,5%-a számít kedvező karrierhatásra, a nőknél ez az arány 27,7%, miközben a negatív következmények feltételezése a nőknél magasabb (29,1% vs. 20,0%). A társadalomtudományi képzésben tanulók körében a pozitív várakozások aránya szintén erősebb. A nemzetközi szakirodalom hasonló tendenciát jelez az általános MI-attitűdök tekintetében, bár a karrierre vonatkozó konkrét percepciók vizsgálata ritkább, így a jelen eredmények ezen a dimenzión belül részletesebb empirikus képet nyújtanak.¹²

Az MI-kompetenciák jelentőségét a hallgatók 70,3%-a tartja lényegesnek a jövőbeli karrier szempontjából. Ez azt jelzi, hogy a technológiai felkészültség stratégiai értékét azok is elismerik, akik a közvetlen karrierhatást nem tekintik meghatározónak. A megállapítás illeszkedik ahhoz a szemlélethez, amely az MI-készségeket horizontális munkaerőpiaci kompetenciaként értelmezi.¹³ A férfi hallgatók 34,9%-a minősíti elengedhetetlennek az MI-ismereteket, míg a nőknél ez 18,8%, ugyanakkor a nők nagyobb arányban sorolják a kompetenciát a fontos, de nem nélkülözhetetlen kategóriába (50,9% vs. 37,7%). Ez a különbség a férfi hallgatók körében gyakrabban dokumentált technológiai optimizmus irányába mutat (χ^2 , $p < 0,001$).¹⁴ A társadalomtudományi képzésben tanulók (χ^2 , $p < 0,001$) 26,9%-a tekinti elengedhetetlennek az MI-ismereteket, más területeken ez az arány 18,5%, miközben körükben alacsonyabb azok aránya, akik egyáltalán nem tartják fontosnak (3,1% vs. 7,3%). Bár a szakirodalom

⁹ GHOTBI-HO 2021.

¹⁰ HRUŠKA-ROUBÍK 2025; CACHERO-TOMÁS-PUJOL 2025; STÖHR-OU-MALSTRÖM 2024; AŞIKSOY 2024.

¹¹ GHERHEŞ-OBRAĐ 2018; STÖHR-OU-MALSTRÖM 2024.

¹² STÖHR-OU-MALSTRÖM 2024; MØGELVANG-GRASSINI 2025; CACHERO-TOMÁS-PUJOL 2025.

¹³ VÁZQUEZ-PARRA et al. 2024.

¹⁴ STÖHR-OU-MALSTRÖM 2024; CACHERO-TOMÁS-PUJOL 2025.

rendszerint a technikai diszciplínák hallgatóinál mutat kedvezőbb attitűdöt,¹⁵ a jelen eredmények arra utalnak, hogy a társadalmi és kommunikációs orientációjú szakmákban is hangsúlyos az MI-kompetenciák stratégiai szerepének felismerése. A pedagógiai képzésben részt vevők körében 11,9% tartja elengedhetetlennek az MI-ismereteket, más területeken ez 25,0%, és magasabb azok aránya is, akik szerint az MI egyáltalán nem fontos (8,7% vs. 4,6%), vagy csupán előnyt jelent (28,4% vs. 23,1%). Mivel a pedagógushallgatók karrierrelevancia-percepcióját a nemzetközi szakirodalom korlátozottan tárgyalja, ez az eltérés empirikusan újszerűnek tekinthető, és további vizsgálatot indokol a szakmai identitás, a technológiai önhatékonyság és a jövőbeli szerepfelfogás összefüggésében.

Kockázati tényezők és a mesterséges intelligencián alapuló alkalmazások

A következő kérdésben azt vizsgáltuk meg, hogy az egyetemi hallgatók mennyire tartják kockázatosnak a mesterséges intelligencián alapuló alkalmazásokat a szakirodalom által leggyakrabban említett területeken (2. ábra). A kitöltőknek ötfokozatú skálán kellett megadniuk a választ, amelyben 1 a legkevésbé, míg az 5 a leginkább kockázatosnak vélt értéket jelentette. A vizsgált területek az esélyegyenlőtlenség fokozódása, a kép- és videószerkesztő programokkal való visszaélés, az álhírek terjedése, a munkahelyek elvesztése, a döntéshozatali elfogultság, a magánélet védelme és az adatvédelem voltak.

1. táblázat: Kockázati tényezők értékelésének átlaga (1 = legkevésbé kockázatos, 5 = leginkább kockázatos), N = 1027

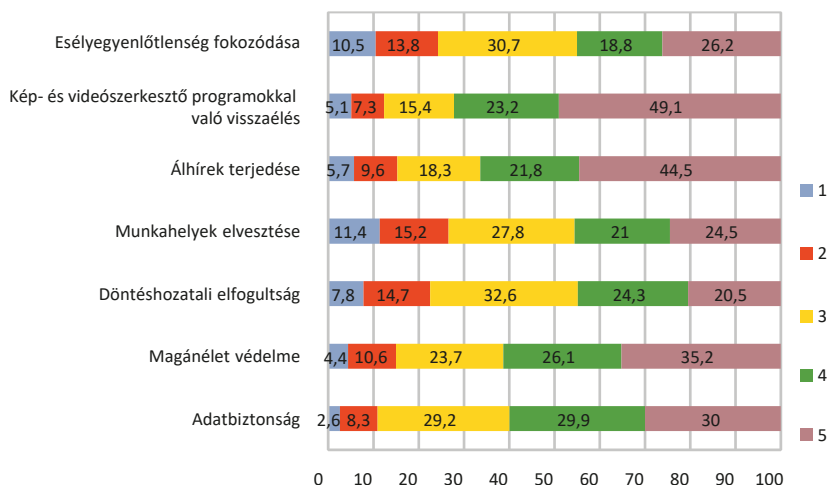
Kockázati terület	Átlag
Kép- és videószerkesztéssel való visszaélés	4,04
Álhírek terjesztése	3,90
Magánélet védelme	3,77
Adatvédelem	3,76
Esélyegyenlőtlenség fokozódása	3,36
Döntéshozatali elfogultság	3,35
Munkahelyek elvesztése	3,32

Forrás: a szerzők szerkesztése

Az eredmények differenciált, ugyanakkor összességében magas szintű kockázatesztelést jeleznek (1. táblázat). A legjelentősebb veszélyként a kép- és videószerkesztő programokkal való visszaélést azonosították (átlag: 4,04), amelyet a válaszadók 72,3%-a magas kockázatúnak minősített, és 49,1% a legmagasabb értéket jelölte meg. Hasonlóan erős aggodalom kapcsolódik az álhírek terjesztéséhez (átlag: 3,90), ahol 66,3% adott 4-es vagy 5-ös értéket. A dezinformációval és manipulációval összefüggő

¹⁵ CHOUDHARY–NIROULA–PANT 2025; DOLENC–BRUMEN 2024.

kockázatok kiemelt kezelése egybeesik azokkal a nemzetközi eredményekkel, amelyek a hallgatók fokozott érzékenységet mutatják ezen a területen.¹⁶ A magánélet védelme (átlag: 3,77) és az adatvédelem (átlag: 3,76) szintén hangsúlyos dimenzióként jelenik meg, mindkét esetben a válaszadók mintegy 60%-a jelölt magas értéket. Az adatkezelés feletti kontroll és a kiberbiztonsági fenyegetések kiemelt státusza megfelel azoknak a kutatási eredményeknek, amelyek az MI legkritikusabb kockázatai közé sorolják e területeket.¹⁷



2. ábra: Mennyire tartod kockázatosnak a mesterséges intelligencián alapuló alkalmazásokat az alábbi területeken? (1 – legkevésbé, 5 – leginkább), N = 1027 (%)

Forrás: a szerzők szerkesztése

Az alacsonyabb átlagértékek a munkahelyek elvesztése (3,32), a döntéshozatali elfogultság (3,35) és az esélyegyenlőtlenség fokozódása (3,36) esetében jelentek meg, ugyanakkor e dimenziókban a vélemények erősen megosztottak, ami a társadalmi és munkaerőpiaci következmények eltérő értelmezésére utal. A nemzetközi szakirodalom ebben a kérdésben nem egységes, egyes vizsgálatok szerint a hallgatók nem tekintik az MI-t súlyos munkaerőpiaci fenyegetésnek,¹⁸ míg más kutatások a torzítás, a méltányosság és a munkahelyek kiváltásának problémáját jelentős kockázatként azonosítják.¹⁹

A tagozat szerinti bontás alapján a levelező hallgatók több területen magasabb kockázatesztelést mutattak, különösen az adatvédelem (3,90 vs. 3,69, $p = 0,028$), a magánélet védelme (3,95 vs. 3,68, $p < ,001$), az álhírek terjesztése (4,00 vs. 3,84, $p = 0,006$) és a kép- és videószerkesztéssel való visszaélés (4,16 vs. 3,97, $p = 0,007$)

¹⁶ PONCE ROJO et al. 2025; VOLYNETS–TRACH 2025.

¹⁷ BRAUNER et al. 2023; LÜNICH–KELLER–MARCINKOWSKI 2024.

¹⁸ YAROVENKO et al. 2024.

¹⁹ TEIXEIRA et al. 2022.

esetében. A nappali és levelező hallgatók közötti különbségek felvetik az élethelyzeti, munkaerőpiaci vagy tapasztalati tényezők lehetséges szerepét. Nemi bontásban három területen rajzolódik ki szignifikáns eltérés, az adatvédelem (3,80 vs. 3,62, χ^2 lineáris trend, $p = 0,028$), a munkahelyek elvesztése (3,38 vs. 3,12; χ^2 lineáris trend, $p = 0,009$) és az esélyegyenlőtlenség fokozódása (3,50 vs. 2,85, $p < 0,001$) esetében, mindhárom dimenzióban a nők észlelnek magasabb kockázatot. Ez a tendencia megfelel azoknak a nemzetközi eredményeknek, amelyek a női hallgatók körében erősebb adatvédelmi és strukturális kockázatérzékenységet dokumentálnak.²⁰ Képzési terület szerint a pedagógia szakos hallgatók 42%-a jelölte a legmagasabb kockázati szintet a magánélet védelme esetében, ami meghaladja más területek arányát (33,3%), és fokozott adatvédelmi érzékenységre utal. Ez a minta összecseng azokkal a megfigyelésekkel, amelyek az oktatási profilú hallgatók körében erősebb átláthatósági és felhasználóvédelmi elvárásokat azonosítanak.²¹

A hét vizsgált tényező közül a hallgatók átlagosan 3,95 területet minősítettek jelentős kockázatúnak. A válaszadók 14,0%-a mind a hét dimenziót magas kockázatúnak tartotta, 11,3% hatot, 16,2% ötöt, 18,8% négyet, míg 6,7% egyetlen területet sem jelölt meg. Az eloszlás azt jelzi, hogy a többség több dimenzióban is azonosít kockázatot, ugyanakkor a percepció intenzitása differenciált. Szignifikáns eltérés mutatkozott nem és tagozat szerint. A nők átlagosan több területet ítélték jelentős kockázatúnak, mint a férfiak (4,05 vs. 3,58, Mann–Whitney U $p = 0,002$), és felülreprezentáltak a 6–7 dimenziót megjelölők körében. A levelező hallgatók átlagosan 4,12 területet tartottak kockázatosnak, míg a nappali tagozatosok 3,86-ot (Mann–Whitney U $p = 0,01$). A nemek közötti különbség egybeesik azokkal a nemzetközi eredményekkel, amelyek a nők körében következetesen magasabb MI-kockázatészlelést mutatnak ki, különösen adatvédelmi és társadalmi sérülékenységi dimenziókban.²² A tagozati eltérésre a szakirodalom nem kínál közvetlen összehasonlítási alapot, így a levelező hallgatók magasabb kumulatív kockázatpercepciója további empirikus vizsgálatot indokol. Az eredmények azt mutatják, hogy az MI-vel kapcsolatos kockázatészlelés több, egymással összefüggő dimenzióban strukturált módon jelenik meg, és nem korlátozódik egyetlen kiemelt területre.

A mesterségesintelligencia-használat gyakorisága és a kockázatészlelés

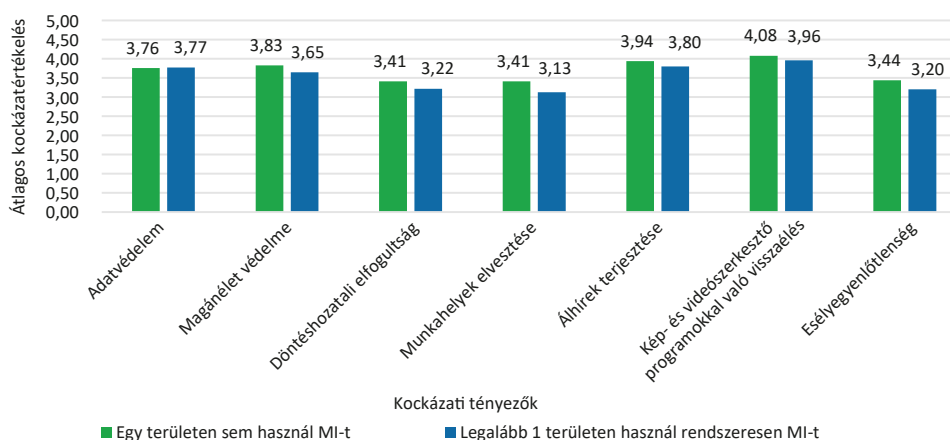
A kockázati területeket követően megvizsgáltuk, hogy az MI-alapú alkalmazások használatának intenzitása összefügg-e a kockázatok megítélésével. Az első hipotézisünk szerint az MI-eszközöket rendszeresen használók kevésbé látják azok kockázatát. A kérdőívünkben 9 használati területre (chatbotok, kép- és videószerkesztő eszközök, virtuális asszisztensek, hangfelismerő rendszerek, oktatási alkalmazások, játékok, sport, zeneszerzés és irodalmi művek megalkotása) kérdeztünk rá. Az MI-eszközök

²⁰ AŞIKSOY 2024; CACHERO–TOMÁS–PUJOL 2025; HRUŠKA–ROUBÍK 2025.

²¹ AŞIKSOY 2024.

²² BORWEIN et al. 2026; HRUŠKA–ROUBÍK 2025; CACHERO–TOMÁS–PUJOL 2025.

használata erősen feladatfüggő, így bárkit, aki a 9 terület közül egy területen bejelölte azt a válaszlehetőséget, hogy rendszeresen használ MI-eszközt/eszközöket, akkor őt a rendszeres használók közé soroltuk. A kilenc vizsgált terület alapján a hallgatók 68,1%-a egyetlen területen sem használ rendszeresen MI-alapú alkalmazást, 19,1% egy, 8,2% két, 3,6% három területen aktív, míg négy vagy több terület rendszeres használata marginális. Az adatok tehát alacsony általános használati intenzitást jeleznek, a minta 31,9%-a tekinthető legalább egy területen rendszeres használónak. E körben felülreprezentáltak a nappali tagozatos hallgatók (34,5%) és a társadalomtudományi képzési területen tanulók (36,7%), míg alulreprezentáltak a levelező tagozatosok (27,0%) és a pedagógiai képzésben részt vevők (10,1%). A mintázat értelmezhető a digitális tőke, a technológiai önhatékonyság és a diszciplináris szocializáció különbségeinek kontextusában.²³



3. ábra: A kockázati tényezők megítélése a rendszeres és nem rendszeres MI-használók körében, $N = 1027$

Forrás: a szerzők szerkesztése

A Spearman korrelációs elemzés az előző fejezetben azonosított hét kockázati tényező mindegyike esetében szignifikáns ($p < 0,01$) gyenge negatív kapcsolatot mutatott a használati intenzitás és a kockázatesztelés között (lásd 3. ábra). Minél több területen alkalmaz valaki MI-alapú eszközöket, annál alacsonyabb kockázati értékeket ad. A legerősebb összefüggés a magánélet védelme ($\rho = -0,171$), a munkahelyek elvesztése ($\rho = -0,142$) és a kép- és videószerkesztő eszközökkel való visszaélés ($\rho = -0,114$) esetében jelent meg, míg az álhírek terjesztésénél a kapcsolat nagyon gyenge ($\rho = -0,087$).

A rendszeres használók – akik legalább egy területen rendszeresen használták – hat területen alacsonyabb kockázati értékeket adtak. Négy dimenzióban a különbség

²³ PARK et al. 2022.

szignifikáns (Mann–Whitney U, $p < 0,05$): a magánélet védelme (3,65 vs. 3,83), a döntéshozatali elfogultság (3,22 vs. 3,41), a munkahelyek elvesztése (3,13 vs. 3,41) és az esélyegyenlőtlenség fokozódása (3,20 vs. 3,44) esetében. A használati intenzitás folytonos mutatója és az egyes kockázati dimenziók között gyenge, de szignifikáns negatív összefüggések mutatkoztak (Spearman $\rho = 0,071$ és $-0,171$ között; $p < 0,01$), ami konzisztens, alacsony erősségű kapcsolatot jelez. A kumulatív kockázatesztelés alapján a nem rendszeres használók átlagosan 4,07 területet, a rendszeres használók 3,71 területet minősítettek jelentős kockázatúnak, a különbség szignifikáns ($\rho = -0,143$, $p < 0,001$). Az eredmények azt mutatják, hogy a nagyobb használati tapasztalat mérsékelt kockázatcsökkenéssel járhat együtt, különösen a magánélet dimenziójában, ami a nemzetközi szakirodalomban leírt *risk blindness* jelenséggel hozható párhuzamba.²⁴ Hasonló irányú összefüggéseket jeleznek azok a kutatások is, amelyek az MI-t gyakran használók körében magasabb bizalmi szintet és erősebb haszonpercepciót azonosítanak, valamint hangsúlyozzák az adatvédelmi aggodalmak mediáló szerepét.²⁵

A korrelációk gyengesége ugyanakkor arra utal, hogy a használat önmagában nem determinálja a kockázatesztelést. Az attitűdök formálásában valószínűsíthetően szerepet játszik az MI-műveltség, az etikai és technológiai tudatosság, valamint a médiakitettség. A szakirodalom szerint az MI-műveltség dimenziói szignifikánsan befolyásolják az attitűdöt és az észlelt viselkedési kontrollt,²⁶ és érdemben hozzájárulnak a használati szándék magyarázatához.²⁷ Emellett egyes vizsgálatok arra mutatnak rá, hogy az észlelt kockázat nem minden esetben befolyásolja közvetlenül a használat fenntartását,²⁸ ami a használat-kockázat kapcsolat kontextusfüggő jellegét erősíti meg.²⁹

Mindezekre tekintettel megállapítható, hogy első hipotézisünk részben igazolódott. A rendszeres MI-használat következetesen, de csekély mértékben alacsonyabb kockázateszteléssel társul. A kapott eredmények nem erős oksági hatásra, hanem egy gyenge, stabil familiaritási effektus jelenlétére utalnak, amely további magyarázó változók bevonását indokolja.

A rendszeres mesterségesintelligencia-használat és a jövőbeli karrier megítélése

Ezt követően azt vizsgáltuk, hogy a rendszeres MI-használat összefügg-e a karrierre gyakorolt hatás megítélésével. A hipotézis szerint a rendszeres használók pozitívabb munkaerőpiaci várakozásokat fogalmaznak meg. A vizsgálat során a mesterséges intelligencia munkaerőpiaci hatásának megítélését elemeztük az MI-t használók és nem használók körében, aszerint, hogy a technológiának pozitív hatást és új lehetőségeket,

²⁴ SAID et al. 2023; MOON 2024.

²⁵ ZHANG et al. 2025; LI et al. 2025; BASCH et al. 2025.

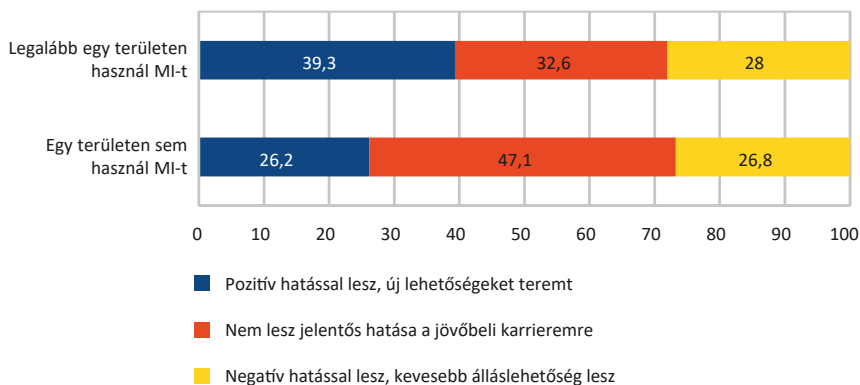
²⁶ ZHANG et al. 2025.

²⁷ WANG et al. 2024.

²⁸ SUMMARYANTO–RICADONNA–SUSANTI 2026.

²⁹ LIU–CHEN 2025; DOROTIC–STAGNO–WARLOP 2023.

negatív hatást és az álláslehetőségek csökkenését tulajdonítanak, vagy úgy vélik, hogy az nem lesz jelentős hatással a jövőbeli karrierjükre. Az adatok (4. ábra) alapján a rendszeres MI-használók közel 40%-a számít kedvező hatásra, míg a nem használók körében ez az arány 26,2%.



4. ábra: Az MI munkaerőpiaci hatásának megítélése az MI-t használók és nem használók körében, $N = 1027$ (%)

Forrás: a szerzők szerkesztése

Ezzel szemben a nem használók 47,1%-a úgy véli, hogy az MI nem befolyásolja érdemben karrierjét, a használók körében ez 32,6%. A negatív következményekkel számoló aránya ugyanakkor hasonló a két csoportban (28,0% vs. 26,8%). A kapcsolat szignifikáns (χ^2 -próba, $p = 0,001$), ami megerősíti a hipotézist, és arra utal, hogy a használati tapasztalat pozitív irányba mozdítja el a karrierpercepciót. A minta összhangban áll azokkal az empirikus eredményekkel, amelyek szerint az MI-vel kapcsolatos ismereteikben jártasabb hallgatók nagyobb karrierbizalommal rendelkeznek, és több szakmai fejlődési lehetőséget látnak maguk előtt.³⁰ Hasonló következtetésekre jutnak azok a vizsgálatok is, amelyek az MI-hez kapcsolódó tudatosságot és kompetenciát a karrierbizalom, valamint az MI-hez kötődő pályák iránti nyitottság meghatározó tényezőjeként azonosítják.³¹ A rendszeres használók körében megfigyelhető magasabb pozitív arány értelmezhető familiaritási és kontrollérzeti effektusként, mivel a nagyobb tapasztalat csökkentheti a bizonytalanságot és erősítheti az észlelt kompetenciát, ami kedvezőbb jövőképet eredményez.³²

Figyelemre méltó, hogy a negatív várakozások aránya nem tér el érdemben a két csoport között. Ez arra utal, hogy a használat elsősorban a semleges attitűdöket tolja el pozitív irányba, miközben a strukturális munkaerőpiaci bizonytalanságokkal kapcsolatos aggodalmak nem kizárólag a használati intenzitás függvényében alakulnak.

³⁰ SANTOS-JAÉN et al. 2025.

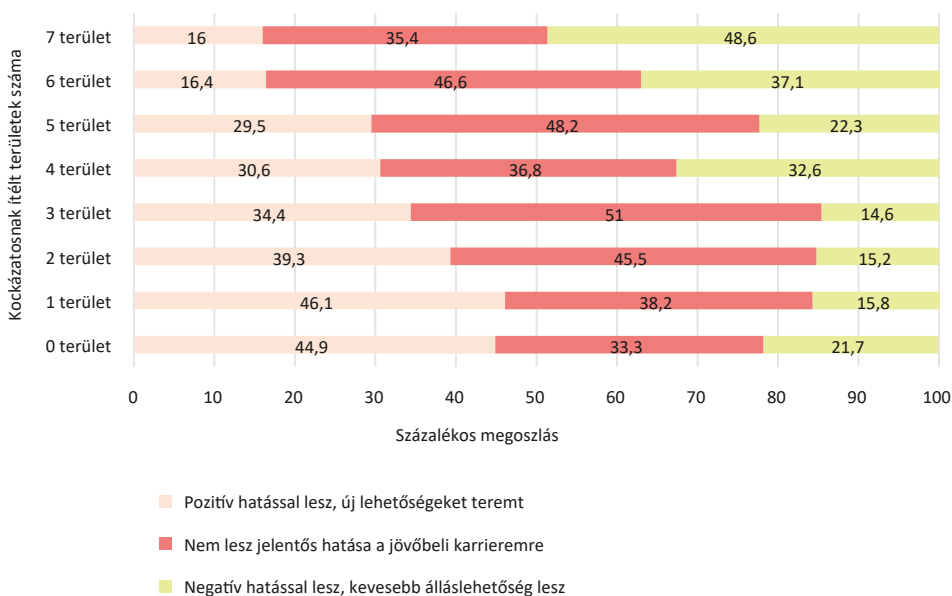
³¹ BAVADHARANI-ROSHAN-KALAIVANI 2025.

³² BARRERA-JIMENEZ et al. 2025; DE LOYOLA et al. 2024.

Az eredmények tehát nem a negatív percepciók eltűnését, hanem a pozitív értelmezési keret megerősödését jelzik a rendszeres használók körében.

A mesterséges intelligenciával kapcsolatos kockázateszlelés és a karrierpercepció összefüggése

Az MI-használat és a jövőbeli karriermegítélés-vizsgálat után elemzésünk arra fókuszált, hogy a kockázateszlelés intenzitása miként kapcsolódik az MI jövőbeli karrierhatásának megítéléséhez (lásd 5. ábra). A teljes mintában a hallgatók 30,4%-a pozitív, 42,5%-a semleges, 27,2%-a negatív hatást tulajdonít az MI-nek saját pályája szempontjából. A kockázatosnak ítélt területek száma és a karrierhatás megítélése között gyenge, de szignifikáns pozitív összefüggés mutatkozott ($\rho = 0,249$; $p < ,001$). A kódolás logikájából következően ez azt jelenti, hogy minél több dimenzióban észlel valaki jelentős kockázatot, annál inkább a semleges vagy negatív karriermegítélés irányába mozdul el.



5. ábra: Az MI karrierhatásának megítélése a kockázatosnak ítélt területek száma szerint, $N = 1027$ (%)

Forrás: a szerzők szerkesztése

A kategorikus bontás egyértelmű tendenciát jelez, tehát azok körében, akik egyetlen területet sem, vagy csak egyet tartanak kockázatosnak, a pozitív karriermegítélés aránya 45% körüli. Ezzel szemben a hat vagy hét területet jelentős kockázatúnak minősítők esetében a pozitív arány 16% körülre csökken, miközben a negatív percepció 21,7%-ról 48,6%-ra emelkedik. A kapcsolat különösen a magas kockázati szinteken válik markánsná, ami arra utal, hogy a multidimenzionális kockázattudatosság erőteljesebben formálja a jövőképet, mint az izolált aggodalmak.

Az eredmények megerősítik a hipotézist, miszerint a kockázatesztelés növekedése pesszimistább karriervárakozásokkal társul. Ez megfelel azoknak a vizsgálatoknak, amelyek a kockázattudatosság és a foglalkoztatási bizonytalanság percepciója között pozitív kapcsolatot azonosítottak,³³ ugyanakkor a korreláció mérsékelt erőssége azt jelzi, hogy a kockázatesztelés önmagában nem határozza meg a karrierattitűdöt. A nemzetközi szakirodalom alapján a negatív hatást mérsékelheti a hasznosságészlelés, az önhatékonyosság és a tanulási orientáció.³⁴ Ennek megfelelően a hallgatók egy része magas kockázattudatosság mellett is képes pozitív karrieroptimizmust fenntartani, amennyiben az MI-t adaptív erőforrásként értelmezi. Az eredmények alapján a kapcsolatos MI-attitűd többtényezős konstrukcióként ragadható meg, amelyben a kockázatesztelés fontos, de nem kizárólagos magyarázó tényező.

A mesterségesintelligencia-eszközök használata iránti nyitottság vizsgálata a jövőbeli karrier szempontjából

Utolsó elemzésünkben azt vizsgáltuk, hogy az MI-alapú alkalmazások használata iránti nyitottság miként függ össze az MI-eszközök ismeretének jövőbeli karrier szempontjából tulajdonított jelentőségével. A hipotézisünk szerint az MI-használattól teljesen elzárkózó hallgatók kevésbé tekintik fontosnak e kompetenciák elsajátítását. A nyitottság mérésére két indikátort alkalmaztunk. Az első négy általános területre terjedt ki, tanulás, munkahelyi feladatok, szórakozás és kommunikáció, ahol a nyitottság a tényleges használatot és a használati hajlandóságot egyaránt magában foglalta. A második mutató kilenc specifikus oktatási és tanulási kontextust vizsgált, a nyelvtanulástól és fordítástól kezdve a szemináriumi anyaggyűjtésen és prezentációkészítésen át a virtuális tanárok és szakdolgozatírás támogatásáig. Az MI-ismeretek relevanciáját négy szintű ordinális változóval mértük, „elengedhetetlen”, „fontos, de nem elengedhetetlen”, „nem fontos, de előnyös”, illetve „egyáltalán nem fontos” kategóriák mentén. A változók nem normális eloszlása miatt nem paraméteres eljárásokat alkalmaztunk.

A négy területet aggregáló nyitottsági mutató és a karrierrelevancia között a Spearman-korreláció gyenge-közepes, de szignifikáns negatív kapcsolatot jelzett ($\rho = -0,287$; $p < ,001$). A kódolás irányából következően ez azt mutatja, hogy a nagyobb nyitottság magasabb fontosság tulajdonításával jár együtt. A Kruskal-Wallis ($p < 0,001$) és a khi-négyzet-tesztek ($\chi^2 < 0,001$) szintén szignifikáns különbségeket jeleztek a nyitottsági szintek között. A kategorikus bontás egyértelmű tendenciát rajzol ki, a teljesen elzárkózók 64,8%-a nem tartja fontosnak az MI-eszközök ismeretét, 35,1% „nem fontos”, 29,7% „egyáltalán nem fontos” választ jelölt, míg a legnyitottabb csoportban ez az arány 19,3%-ra csökken. Ezzel párhuzamosan az „elengedhetetlen” kategória aránya 18,9%-ról 32,7%-ra emelkedik. A mintázat jelzi, hogy az elzárkózó attitűd alacsonyabb stratégiai értéktulajdonítással társul. Következésképpen hipotézisünk megerősítést nyert, a nagyobb nyitottság magasabb

³³ LIANG-ZHAI 2025.

³⁴ MUSYAFFI et al. 2024.

kompetenciafontosság-percepcióval társul. A kapcsolat heterogén jellege ugyanakkor arra utal, hogy a nyitottság és a stratégiai értéktulajdonítás közötti összefüggést további tényezők, így az MI-önhatékonyság, az MI-műveltség és a diszciplináris identitás is alakíthatják, ami indokolja e változók bevonását a későbbi kutatásokba.

Az eredmények összhangban vannak azokkal a kutatásokkal, amelyek a technológiai nyitottságot és használati hajlandóságot a kompetenciák fontosságának erősebb percepciójával kapcsolják össze,³⁵ míg az információkerülés és technológiai elzárkózás alacsonyabb stratégiai jelentőségtulajdonítással jár együtt.³⁶ A kapcsolat erőssége mérsékelt, ami arra utal, hogy a karrierorientált fontosságészlelés nem vezethető vissza kizárólag a használati attitűdre. A szakirodalom szerint az attitűdök és a tényleges kompetenciák közötti kapcsolat gyakran gyenge,³⁷ és a karrierbizalom az MI-vel kapcsolatos tudatossággal, valamint a felkészültség szintjével is összefügg.³⁸

Diszkusszió

Az öt hipotézis tesztelése differenciált, többdimenziós mintázatot rajzolt ki (lásd 2. táblázat), amely az MI-vel kapcsolatos attitűdök strukturális összetettségét erősíti meg:

- H1 hipotézisünk részben igazolódott; az MI-re nyitottabb hallgatók alacsonyabb kockázateszlelést mutatnak, különösen az oktatási kontextusban ($\rho = -0,287$; $p < 0,001$). A kapcsolat azonban gyenge-közepes erősségű, ami arra utal, hogy a nyitottság önmagában nem determinálja a kockázatpercepciót.
- H2 hipotézisünk megerősítést nyert, a rendszeres MI-használók több kockázati dimenzióban alacsonyabb értékeket adtak ($\rho \approx -0,09$ és $-0,17$ között; $p < 0,05$). Ugyanakkor az összefüggések gyengésege familiaritási, nem pedig erős attitűdformáló hatásra utal.
- H3 hipotézisünket szintén igazoltuk, a rendszeres használók nagyobb arányban számítanak pozitív karrierhatásra (39,5% vs. 26,2%; $p < 0,05$). A nem használók körében a semleges álláspont dominanciája (47,1%) inkább bizonytalanságot, mint kifejezett pesszimizmust jelez.
- H4 hipotézisünket egyértelműen alátámasztottuk, a magasabb kockázateszlelés negatívabb karrierpercepcióval jár együtt ($\rho = 0,249$; $p < 0,001$). A hét területet jelentős kockázatúnak tartók körében a negatív megítélés aránya 48,6%-ra emelkedik, ami a multidimenzionális kockázattudatosság és a munkaerőpiaci aggodalmak összefonódását jelzi.
- H5 hipotézisünket a részletes (9 területet vizsgáló) nyitottsági mutató esetében megerősítettük ($\rho = -0,287$; $p < 0,001$); az elzárkózók 64,8%-a nem tartja fontosnak az MI-ismereteket. A 4 területet mérő aggregált mutató gyengébb kapcsolatot jelzett ($\rho = -0,101$), ami arra utal, hogy az elzárkózás mögötti motivációk – például bizalmatlanság, érdektelenség vagy alacsony önhatékonyság – heterogének.

³⁵ BEWERSDORFF et al. 2025.

³⁶ OTERMANS-ROBERTS-BAINES 2025.

³⁷ IVANOVA-TARASOVA-TALOV 2025.

³⁸ BAVADHARANI-ROSHAN-KALAIVANI 2025.

2. táblázat: Összefoglaló táblázat a hipotézisek tesztelésének eredményeiről, $N = 1027$

Hipotézis	Tartalom	Eredmény	Eredmény
H1	Nyitottabb → alacsonyabb kockázatészlelés	Részben igazolt	$\rho = -0,287$; $p < 0,001$
H2	Rendszeres használó → alacsonyabb kockázat	Igazolt (gyenge)	$\rho \approx -0,09-0,17$; $p < 0,05$
H3	Rendszeres használó → pozitívabb karrierhatás	Igazolt	39,5% vs. 26,2%; $p = 0,001$
H4	Magasabb kockázat → negatívabb karrierpercepció	Igazolt	$\rho = 0,249$; $p < 0,001$
H5	Elzárkózó → MI-ismeretek kevésbé fontosak	Igazolt	64,8%; $\rho = -0,287$

Forrás: a szerzők szerkesztése

Kutatásunk eredményei azt jelzik, hogy az MI-vel kapcsolatos karrierattitűd nem redukálható egyetlen változóra, a használat, a kockázatészlelés és a kompetencia egymással összefüggő, de csak mérsékelt erősségű kapcsolatokat mutatnak. Ez a mintázat összhangban áll azokkal az elfogadáselméleti modellekkel, amelyek a technológiai attitűdöt többdimenziós, mediált konstrukcióként írják le, a gyenge, de konzisztens korrelációk pedig arra utalnak, hogy a hallgatók percepcióit valószínűleg további pszichológiai és kontextuális tényezők – például technológiai önhatékonyság, MI-műveltség, bizalom vagy médiakitettség – is formálják.

Vizsgálatunk értelmezésekor több módszertani korlátot is figyelembe kell venni. A nem valószínűségi mintavétel korlátozza az eredmények általánosíthatóságát, különösen az intézményi koncentráció és a nemi aránytalanság fényében. A keresztmetszeti adatfelvétel nem teszi lehetővé oksági következtetések levonását; a használat és az attitűd közötti irányultság nem dönthető el egyértelműen, az önbevallásos mérés torzítási kockázatot hordoz, különösen a használati intenzitás és a kompetenciafontosság esetében. Emellett a kockázatészlelés kumulatív operacionalizációja nem differenciálja az egyes dimenziók relatív súlyát, így a konstrukció belső szerkezete további finomítást igényelhet.

A jövőbeni kutatási irányokban indokolt a longitudinális design alkalmazása, amely képes feltárni az attitűdök időbeli változását és az oksági irányokat, strukturális egyenletmodellek segítségével vizsgálható lenne az önhatékonyság, a hasznosságészlelés és a technológiai bizalom mediáló szerepe. Objektív MI-kompetenciamérések bevonása csökkenthetné az önbevallás torzítását, míg kvalitatív módszerek – például interjúk – árnyalhatnák az elzárkózás mögötti motivációk megértését. Ezen túlmenően a diszciplináris összehasonlító vizsgálatok nagyban segíthetnék annak feltárását, hogy az MI-percepció mennyiben kontextusfüggő. Kutatásunk empirikus alapot nyújthat az MI-elfogadás hallgatói dimenzióinak továbbfejlesztett, többváltozós modelljeihez, ugyanakkor a feltárt összefüggések értelmezése csak a módszertani korlátok figyelembevételével tekinthető megalapozottnak.

Felhasznált irodalom

- AŞIKSOY, Gülsüm (2024): An Investigation of University Students' Attitudes Towards Artificial Intelligence Ethics. *International Journal of Engineering Pedagogy*, 14(8), 153–169. Online: <https://doi.org/10.3991/ijep.v14i8.50769>
- BÁNYÁSZ-VÁCZI Kincső Boróka – RAJKI Zoltán (2025): A bölcsészet-, társadalomtudományi és pedagógiai szakokon tanuló hallgatók perspektívái a mesterséges intelligencia lehetőségeiről és kockázatairól, 1. rész: Szakirodalmi áttekintés. *Hadmérnök*, 20(1), 187–201. Online: <https://doi.org/10.32567/hm.2025.1.10>
- BARRERA-JIMENEZ, Felipe et al. (2025): Invulnerability Bias in Perceptions of Artificial Intelligence's Future Impact on Employment. *Scientific Reports*, 15(1). Online: <https://doi.org/10.1038/s41598-025-14698-2>
- BASCH, Corey et al. (2025): Artificial Intelligence in Higher Education: Student Knowledge, Attitudes, and Ethical Perceptions in the United States. *SDGs Studies Review*, 6. Online: <https://doi.org/10.37497/sdgs.v6i1studies.34>
- BAVADHARANI, K. – ROSHAN, K. – KALAIVANI, N. (2025): Artificial Intelligence Awareness and its Influence on Career Decision-Making Among University Students. *ASET Journal Management Science*, 4(2), 325–333. Online: <https://doi.org/10.47059/ajms/v4i2/33>
- BEWERSDORFF, Arne et al. (2025): AI Advocates and Cautious Critics: How AI Attitudes, AI Interest, Use of AI, and AI Literacy Build University Students' AI Self-Efficacy. *Computers and Education: Artificial Intelligence*, 8. Online: <https://doi.org/10.1016/j.caeai.2024.100340>
- BORWEIN, Sophie et al. (2026): Explaining Women's Skepticism Toward Artificial Intelligence: The Role of Risk Orientation and Risk Exposure. *PNAS Nexus*, 5(1). Online: <https://doi.org/10.1093/pnasnexus/pgaf399>
- BRAUNER, Philipp et al. (2023): What Does the Public Think About Artificial Intelligence? – A Criticality Map to Understand Bias in the Public Perception of AI. *Frontiers in Computer Science*, 5. Online: <https://doi.org/10.3389/fcomp.2023.1113903>
- CACHERO, Cristina – TOMÁS, David – PUJOL, Francisco A. (2025): Gender Bias in Self-Perception of AI Knowledge, Impact, and Support among Higher Education Students: An Observational Study. *ACM Transactions on Computing Education*, 25(2), 1–26. Online: <https://doi.org/10.1145/3721295>
- CHOUDHARY, Satyanarayan – NIROULA, Arjun Kumar – PANT, Ganesh Datt (2025): Beyond Discipline: Quantifying the Impact of Prior AI Experience and Digital Literacy on Student Acceptance of Educational AI. *Nepal Journal Multidisciplinary Research*, 8(2), 186–195. Online: <https://doi.org/10.3126/njmr.v8i2.78027>
- DE LOYOLA, Rhyann et al. (2024): Sentiment Analysis of AI's Impact on Labor Market: Opportunities and Threats. *Philippine Journal of Science Engineering Technology*, 1(1), 48–54.
- DOLENC, Kosta – BRUMEN, Mihaela (2024): Exploring Social and Computer Science Students' Perceptions of AI Integration in (Foreign) Language Instruction. *Computers and Education: Artificial Intelligence*, 7. Online: <https://doi.org/10.1016/j.caeai.2024.100285>

- DOROTIC, Matilda – STAGNO, Emanuela – WARLOP, Luk (2023): AI on The Street: Context-Dependent Responses to Artificial Intelligence. *International Journal of Research in Marketing*, 41(1), 113–137. Online: <https://doi.org/10.1016/j.ijres-mar.2023.08.010>
- GHERHEȘ, Vasile – OBRAD, Ciprian (2018): Technical and Humanities Students' Perspectives on the Development and Sustainability of Artificial Intelligence (AI). *Sustainability*, 10(9). Online: <https://doi.org/10.3390/su10093066>
- GHOTBI, N. – HO, Manh-Tung (2021): Moral Awareness of College Students Regarding Artificial Intelligence. *Asian Bioethics Review*, 13, 421–433. Online: <https://doi.org/10.1007/s41649-021-00182-2>
- HRUŠKA, Adam – ROUBÍK, Hynek (2025): Fear of the Future in the Context of the Emergence of Generative Artificial Intelligence Among Young Adults: The Case of Czechia. *Advances in Distributed Computing and Artificial Intelligence Journal*, 14. Online: <https://doi.org/10.14201/adcaij.32644>
- IVANOVA, A. E. – TARASOVA, K. V. – TALOV, D. P. (2025): Between Interest and Skill: How Students Perceive and Use AI (Между интересом и умением: как студенты воспринимают и применяют ИИ). *Vysshee Obrazovanie V Rossii Higher Education in Russia*, 34(8–9), 9–32. Online: <https://doi.org/10.31992/0869-3617-2025-34-8-9-9-32>
- LI, Yifu – CASTULO, Nilo Jayoma – XU, Xiaoyuan (2025): Embracing or Rejecting AI? A Mixed-Method Study on Undergraduate Students' Perceptions of Artificial Intelligence at a Private University in China. *Frontiers in Education*, 10. Online: <https://doi.org/10.3389/feduc.2025.1505856>
- LIANG, Yanlong – ZHAI, Yun (2025): The Impact of Artificial Intelligence Impact Awareness on College Students' Employment Risk Perception: A Moderated Mediation Model. *Acta Psychologica*, 261. Online: <https://doi.org/10.1016/j.actpsy.2025.105808>
- LIU, Xuan – CHEN, Yuci (2025): The Impact of Artificial Intelligence Usage on Employee Career Commitment: The Moderating Role of Artificial Intelligence Awareness. *American Journal of Applied Psychology*, 14(3), 101–112. Online: <https://doi.org/10.11648/j.ajap.20251403.14>
- LÜNICH, Marco – KELLER, Birte – MARCINKOWSKI, Frank (2024): Diverging Perceptions of Artificial Intelligence in Higher Education: A Comparison of Student and Public Assessments on Risks and Damages of Academic Performance Prediction in Germany. *Computers and Education: Artificial Intelligence*, 7. Online: <https://doi.org/10.1016/j.caeai.2024.100305>
- MØGELVANG, Anja – GRASSINI, Simone (2025): Validating the AI Attitude Scale (AIAS-4) and Exploring Attitudinal Differences in a Large Sample of Norwegian University Students. *Discover Education*, 4. Online: <https://doi.org/10.1007/s44217-025-00657-6>
- MOON, Su-Ji (2024): Effects of Perception of Potential Risk in Generative AI on Attitudes and Intention to Use. *International Journal on Advanced Science Engineering Information Technology*, 14(5), 1748–1755. Online: <https://doi.org/10.18517/ijaseit.14.5.20445>

- MUSYAFFI, Ayatulloh Michael et al. (2024): Improving Students' Openness to Artificial Intelligence Through Risk Awareness and Digital Literacy: Evidence From a Developing Country. *Social Sciences Humanities Open*, 10. Online: <https://doi.org/10.1016/j.ssaho.2024.101168>
- NKEDISHU, Victor Chukwubueze – OKONTA, Vinella (2024): Unpacking Optimism versus Concern: Tertiary Students' Multidimensional Views on the Rise of Artificial Intelligence (AI). *International Research Journal of Multidisciplinary Scope*, 5(4), 362–377. Online: <https://doi.org/10.47857/irjms.2024.05i04.01261>
- OTERMANS, Pauldy C. J. – ROBERTS, Charlotte – BAINES, Stephanie (2025): Unveiling AI Perceptions: How Student Attitudes Towards AI Shape AI Awareness, Usage, and Conceptions. *International Journal of Technology in Education*, 8(1), 88–103. Online: <https://doi.org/10.46328/ijte.995>
- PARK, Yong Jin et al. (2022): Digital Assistants: Inequalities and Social Context of Access, Use, and Perceptual Understanding. *Poetics*, 93. Online: <https://doi.org/10.1016/j.poetic.2022.101689>
- PONCE ROJO, Antonio et al. (2025): From Digital Natives to AI Natives: Emerging Competencies and Media and Information Literacy in Higher Education. *Education Sciences*, 15(9). Online: <https://doi.org/10.3390/educsci15091134>
- SAID, Nadia et al. (2023): An Artificial Intelligence Perspective: How Knowledge and Confidence Shape Risk and Benefit Perception. *Computers in Human Behavior*, 149. Online: <https://doi.org/10.1016/j.chb.2023.107855>
- SANTOS-JAÉN, José Manuel et al. (2025): University Students' Perceptions of the Impact of Artificial Intelligence in the Business Sector on Their Educational and Professional Development. *Education and Information Technologies*, 30(17), 24395–24428. Online: <https://doi.org/10.1007/s10639-025-13712-4>
- STÖHR, Christian – OU, Amy Wanyu – MALMSTRÖM, Hans (2024): Perceptions and Usage of AI Chatbots Among Students in Higher Education Across Genders, Academic Levels and Fields of Study. *Computers and Education: Artificial Intelligence*, 7. Online: <https://doi.org/10.1016/j.caeai.2024.100259>
- SUMARYANTO, Sumaryanto – RICADONNA, Nadia Adriane – SUSANTI, Nani Irma (2026): How Perceived Risk Shapes User Satisfaction and Continuance Intention Toward AI-Based Applications in Higher Education ? *International Journal of Business, Law, and Education*, 7(1), 55–66. Online: <https://doi.org/10.56442/ijble.v7i1.1333>
- TEIXEIRA, Sónia et al. (2022): An Exploratory Diagnosis of Artificial Intelligence Risks for a Responsible Governance. *Proceedings of the 15th International Conference on Theory and Practice of Electronic Governance*, ACM, 25–31. Online: <http://dx.doi.org/10.1145/3560107.3560298>
- VÁZQUEZ-PARRA, José Carlos et al. (2024): Importance of University Students' Perception of Adoption and Training in Artificial Intelligence Tools. *Societies*, 14(8). Online: <https://doi.org/10.3390/soc14080141>
- VOLYNETS, Viktoriia – TRACH, Yuliia (2025): Ethical Awareness of Youth about Artificial Intelligence: Education, Risks, Regulation (Етична обізнаність молоді щодо штучного інтелекту: освіта, ризики, регулювання). *Digital Platform Information Technologies in Sociocultural Sphere*, 8(2), 289–298. Online: <https://doi.org/10.31866/2617-796x.8.2.2025.347871>

- WANG, Chengliang et al. (2024): Factors Influencing University Students' Behavioral Intention to Use Generative Artificial Intelligence: Integrating the Theory of Planned Behavior and AI Literacy. *International Journal of Human-Computer Interaction*, 41(11), 6649–6671. Online: <https://doi.org/10.1080/10447318.2024.2383033>
- YAROVENKO, Hanna et al. (2024): The Future of Artificial Intelligence: Fear, Hope or Indifference? *Human Technology*, 20(3), 611–639. Online: <https://doi.org/10.14254/1795-6889.2024.20-3.10>
- ZHANG, Xiaoxuan et al. (2025): Integrating AI Literacy with the TPB-TAM Framework to Explore Chinese University Students' Adoption of Generative AI. *Behavioral Science*, 15(10). Online: <https://doi.org/10.3390/bs15101398>

Biró Gabriella¹

A katonai és civil infrastruktúrák összefonódása az orosz–ukrán háború kiberműveleteiben

The Co-mingling of Military and Civilian Infrastructure in the Cyber Operations of the Russia–Ukraine War

Absztrakt

A 21. századi fegyveres konfliktusokban a kibertér domináns hadszínterré vált, ahol a kinetikus csapások és a kiberműveletek szoros szimbiózisban, valós időben támogatják egymást. Jelen tanulmány az orosz–ukrán háború tapasztalataira építve elemzi a katonai és a polgári kritikus infrastruktúrák technológiai és funkcionális összefonódását. A szerző rámutat, hogy a kettős felhasználású rendszerek – különösen az energiaellátás és a távközlés – elleni támadások során elmosódik a határ a katonai és civil célpontok között, ami súlyos társadalmi következményekkel és nemzetközi tovagyrúzó hatásokkal jár. A cikk konkrét esettanulmányokon keresztül (Viasat, Kyivstar, energetikai hálózatok elleni támadások) vizsgálja a hibrid hadviselés gyakorlatát, bizonyítva, hogy a civil rendszerek megbénítása a modern hadműveletek szerves részévé vált. Az elemzés kiemelt figyelmet szentel a védekezés paradigmaváltásának: bemutatja, hogyan váltak a globális technológiai magánvállalatok és a civil társadalom Ukrajna digitális védelmének kulcsszereplőivé. A tanulmány konklúziója szerint a jövőbeni nemzeti ellenálló képesség már nem garantálható kizárólag állami monopóliumként, a hatékony védelem alapfeltétele a civil szféra, a magánszektor és a védelmi szervek integrált, bizalmi alapú együttműködése.

Kulcsszavak: kibervédelem, kettős felhasználás, kritikus infrastruktúra, interdependencia

¹ Doktori hallgató, Nemzeti Köszolgálati Egyetem Katonai Műszaki Doktori Iskola; tanársegéd, Nemzeti Köszolgálati Egyetem ÁNTK Kiberbiztonsági és e-Közigazgatási Tanszék, e-mail: biro.gabriella@uni-nke.hu

Abstract

In 21st-century armed conflicts, cyberspace has become a dominant theater of war, where kinetic strikes and cyber operations support one another in close symbiosis and in real time. Building on the lessons learned from the Russia–Ukraine war, this study analyses the technological and functional interdependence of military and civilian critical infrastructure. The author points out that during attacks on dual-use systems – particularly energy supply and telecommunications – the line between military and civilian targets becomes blurred, leading to serious social consequences and international ripple effects. Through specific case studies (Viasat, Kyivstar, and attacks on energy grids), the article examines the practice of hybrid warfare, demonstrating that the disruption of civilian systems has become an integral part of modern military operations. The analysis devotes particular attention to the paradigm shift in defence: it illustrates how global private technology companies and civil society have become key players in Ukraine's digital defence. The study concludes that future national resilience can no longer be guaranteed solely through a state monopoly; rather, effective defence requires integrated, trust-based cooperation among the civil sector, the private sector, and defence agencies.

Keywords: cyber defence, dual-use, critical infrastructure, interdependence

Bevezetés

Problémafelvetés

A 21. századi konfliktusok természete alapvető átalakuláson ment keresztül; a hagyományos szárazföldi, vízi, légi és űrbéli hadszínterek mellé egyenrangú, sőt, sok esetben domináns tényezőként zárkózott fel a kibertér mint ötödik hadszíntér.² Ez a dimenzióváltás nagyon élesen megmutatkozik a jelenleg zajló orosz–ukrán háborúban, ahol a kinetikus csapások és a kiberműveletek szerves, valós idejű szimbiózisban valósulnak meg.³ A kiberműveletek így módon fel is erősíthetik a kinetikus támadások hatását és súlyosbíthatják a veszteségeket, például ha a védekező fél kommunikációjának akadályozásával megbénítják reagálóképességét.

A kinetikus és a kibertérben zajló támadások célpontjai általában a kritikus infrastruktúra elemei, amelyeket egymástól való függésük, fizikai interdependenciájuk gyakran még sérülékenyebbé tesz.⁴ Ezek a rendszerek azonban egy másik szempontból is összefüggenek: a katonai célpontokat és a polgári lakosságot kiszolgáló rendszereket sokszor ugyanaz az infrastruktúra látja el árammal és kommunikációs hálózatokkal. Ezért amikor az ilyen infrastruktúrák célkeresztbe kerülnek, a támadás következményei a hadsereget és a civil lakosságot egyaránt érintik. Ugyan az 1977-es, a genfi egyezményekhez fűzött I. Kiegészítő Jegyzőkönyv (AP I) 48. cikke (Alapvető szabály – Basic

² ORBÓK 2013.

³ MIRON–THORNTON 2024.

⁴ MUHA 2007.

Rule) kimondja, hogy a harcoló feleknek mindig meg kell különböztetniük a polgári lakosságot a harcosoktól és a polgári célpontokat a katonai célpontoktól, és műveleteiket csak katonai célpontok ellen irányíthatják a civil lakosság és célpontok védelme érdekében,⁵ a gyakorlatban mégsem ezt látjuk az orosz–ukrán háború során. Ennek nemzetközi jogi aspektusaival jelen cikk nem foglalkozik, azonban fontos megjegyezni, hogy a katonai parancsnokoknak tisztában kell lenniük a genfi egyezmény alapelveivel, amikor döntéseket hoznak a támadásokkal kapcsolatban, tehát a civil lakosságot is érintő következmények tudatos döntés eredményei. A kritikus infrastruktúra elemeit érintő kibertámadások meghatározásával és nemzetközi jogi megítélésével a *Tallinni Kézikönyv 2.0*⁶ foglalkozik behatóbban.

Jelen tanulmány célja annak részletes bemutatása, hogyan válnak a kettős felhasználású (*dual-use*) infrastruktúrák – mint a távközlés, az energiaellátás vagy a logisztikai hálózatok – a kiberműveletek elsődleges célpontjaivá akár önálló műveletek keretében, akár kinetikus műveletek támogató műveletei során. Az elemzés megmutatja, hogy ez az infrastrukturális interdependencia milyen komplex kihívások elé állítja a nemzeti ellenálló képességet, kiberrezilienciát. (A magyar nyelvre fordított európai uniós joganyagokban az angol *resilience* kifejezés fordítása „reziliencia”, azonban az angol szó köznapi értelemben ellenálló képességet jelent.) A kritikus feladatellátás biztonsága a jövőben már nem garantálható izolált védelmi stratégiákkal; ehelyett a polgári szféra, a katonai vezetés és a rendvédelmi szervek minden eddigénél szorosabb, integrált együttműködésére van szükség. A tanulmány arra a kutatási kérdésre keresi a választ, hogyan változtatja meg a kritikus infrastruktúrák technológiai és funkcionális interdependenciája a hadviselő felek célkiválasztási mechanizmusát, és ez milyen kényszerpályára állítja a nemzeti rezilienciaépítést a 21. századi hibrid konfliktusokban. A szerző hipotézise szerint a modern hadviselésben a kritikus infrastruktúrák fizikai és logikai összefonódása miatt a civil szféra veszteségei többé nem tekinthetők véletlenszerűnek, a hadviselés rendszerszintű, kalkulált velejárójává váltak. Bár a nemzetközi szakirodalom széleskörűen tárgyalja a kritikus infrastruktúrák militarizálódását, jelen tanulmány azzal kíván hozzájárulni a témakör vizsgálatához, hogy a nyugati elméleti modelleket ütközteti az orosz–ukrán háború regionális és doktrinális valóságával.

Elméleti és fogalmi keretek

A modern államok stabilitása a kritikus infrastruktúrák zavartalan működésén alapul. Ezen rendszerek – mint az energiaellátás, a közlekedés, az infokommunikáció vagy a pénzügyi szektor – kiesése súlyos gazdasági és társadalmi károkat, valamint a közbizalom megrendülését okozhatja. Ahhoz azonban, hogy megértsük a jelenlegi konfliktusok hibrid fenyegetéseit, elsőként tisztáznunk kell a kritikus infrastruktúrákhoz kapcsolódó definíciókat és elméleti megközelítéseket.

⁵ Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I), 8 June 1977 1977.

⁶ SCHMITT – NATO Cooperative Cyber Defence Centre of Excellence 2017.

Több gondosan megfogalmazott definíció is elérhető a kritikus infrastruktúrák,⁷ illetve az ahhoz kapcsolódó fogalmak meghatározására. Az Európai Unióban a 2022-ben kiadott CER irányelv⁸ így határozza meg a kritikus infrastruktúrát: „olyan eszköz, létesítmény, berendezés, hálózat vagy rendszer, vagy valamely eszköz, létesítmény, berendezés, hálózat vagy rendszer része, amely szükséges az alapvető szolgáltatás nyújtásához.” Az alapvető szolgáltatás meghatározása pedig a következő: „az alapvetően fontos társadalmi funkciók, a gazdasági tevékenységek, a népegészségügy és a biztonság vagy a környezet fenntartásához elengedhetetlen szolgáltatás.”

Hagyományos megközelítésben a civil és a katonai infrastruktúrák élesen elkülönülnek egymástól. A polgári infrastruktúra elsődleges célja a társadalmi és gazdasági jólét biztosítása, míg a katonai infrastruktúra a honvédelem operatív képességeit szolgálja ki. A nemzeti szabályozásokban (így a magyar⁹ és az európai uniós¹⁰ joganyagban is) a védelmi létesítmények általában nem részei a klasszikus kritikus infrastruktúra definíciónak, hanem önálló kategóriát képeznek (például honvédelmi célú létesítmények).

A katonai infrastruktúrák csak ott jelennek meg a nemzeti kritikusinfrastruktúra-rendszerekben, ahol funkcionális függőség mutatható ki: például, ha egy katonai bázis energiaellátása az országos hálózatról történik, vagy a logisztikai utánpótlás a közösségi közlekedési útvonalakra támaszkodik. Formálisan tehát létezik egy határvonal, a valóságban azonban ez a határ gyakran elmosódott. A 21. századi hálózatok legfőbb jellemzője az interdependencia. Egyetlen szektor sem működhet elszigetelten: a távközlés áramot igényel, az energiaszektor irányítása pedig távközlési hálózatokon zajlik. A kritikus infrastruktúrák interdependenciájának dimenzióit Bakos és Kovács vizsgálja részletesen.¹¹ Ebben a kontextusban jelenik meg a kettős felhasználás problematikája, amely a katonai műveletek egyik legnagyobb sérülékenységevé vált, és ezzel párhuzamosan katonai célponttá tette a civil lakosság által használt infrastruktúrát.

A szakirodalom gyakran *co-mingling* vagy *commingling* (összefonódás) néven hivatkozik arra a jelenségre, amikor a polgári és katonai adatforgalom, illetve funkciók fizikailag és logikailag nem választhatók szét. Az orosz–ukrán háború tapasztalatai alapján ez leginkább két területre összpontosul:

- energiahálózatok: a katonai létesítmények áramellátása ritkán független a lakossági hálózattól;
- távközlési rendszerek: a katonai kommunikáció (bár titkosított) gyakran ugyanazokon a gerinchálózatokon, optikai kábeleken és műholdas rendszereken fut keresztül, amelyeken a civil internetforgalom.

Mivel a kritikus infrastruktúrák jelentős része magántulajdonban vagy civil állami vállalatok kezében van, ezek védelme nem tekinthető tisztán katonai feladatnak.¹²

⁷ MUHA 2007; BOGNÁR–BONNYAI 2019.

⁸ Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve (2022. december 14.) a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről (EGT-vonatkozású szöveg) 2022.

⁹ 2024. évi LXXXIV. törvény a kritikus szervezetek ellenálló képességéről.

¹⁰ Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve.

¹¹ BAKOS–KOVÁCS 2025.

¹² MUHA 2007.

A jogi és operatív kereteket szükségszerűen úgy alakítják ki az egyes országok, hogy együttműködést feltételezzenek a polgári biztonsági, katasztrófavédelmi és honvédelmi területek közt. Ez a széttagoltság azonban lassítja az információáramlást és a reakcióidőt.

Ha a kritikus infrastruktúra kiberműveletek célpontjává válik, akkor ez az összefonódás többszörös kockázatot jelent:

- járulékos veszteség: egy katonai célpont (például vezetési pont) elleni kiber-támadás, amely a civil hálózaton keresztül történik, kommunikációs vagy energetikai szempontból megbéníthatja egy egész régió lakossági ellátását (kórházak, fűtés, távközlés);
- célponttévesztés: a kettős felhasználású eszközök miatt a támadó számára nehezen azonosítható, hogy egy adott szerver vagy hálózati csomópont kizárólag katonai célt szolgál-e, illetve ha bizonyítottan látja a katonai felhasználást, akkor esetleg nem törődik a civil veszteségekkel;
- védelmi aszimmetria: a katonai rendszerek általában megerősített védelemmel rendelkeznek, míg a hozzájuk kapcsolódó civil beszállítói hálózatok gyakran a „leggyengébb láncszemet” jelentik, könnyű behatolási pontot kínálva a támadóknak.

Az orosz–ukrán háború kiberdimenziója

Az orosz–ukrán háború műveleteinek elemzése során elengedhetetlen az orosz hadviselési koncepció megértése, amely a kiberműveleteket nem csupán támogató elemként, hanem a modern hadviselés szerves részeként kezeli.¹³ A műveletek dinamikája rávilágít arra, hogyan próbálta az orosz vezetés a digitális térben elért információs fölényt fizikai győzelemre váltani.

A kiberhadviselés természetéről szóló nemzetközi elméleti vitákban gyakori a stratégiai és az operacionális szintű kiberműveletek éles fogalmi szétválasztása. Míg a nyugati elméletirők egy része (például Thomas Rid¹⁴) a kiberfegyverek stratégiai, háborút eldöntő képességét szkeptikusan ítéli meg, addig az orosz hadviselési doktrína egyáltalán nem alkalmazza ezt a nyugati elemzési keretet. Ahogy arra a hazai hadtudományi szakirodalom (például Jójárt Krisztián¹⁵) és az orosz kibereszközöket vizsgáló nemzetközi kutatók (például Miron és Thornton¹⁶) is rámutatnak, az orosz és a posztszovjet katonai gondolkodásban – így a Valerij Geraszimov által is fémjelzett megközelítésben – az „információs küzdelem” (*информационное противоборство*) holisztikus fogalom. Ebből a perspektívából nézve irreleváns a stratégiai és operacionális hatások mesterséges szétválasztása: a kiberműveletek és a kinetikus csapások egyazon információs-pszichológiai cél alá rendelve, elválaszthatatlan szimbiózisban működnek. Jelen tanulmány esettanulmányai éppen azt bizonyítják, hogy a kettős felhasználású kritikus infrastruktúrák megbénítása (például a Viasat vagy a Kyivstar elleni csapások) a nyugati elméletek szerinti operacionális zavarkeltésen túlmutatva,

¹³ MIRON–THORNTON 2024.

¹⁴ RID 2013.

¹⁵ JÓJÁRT 2023.

¹⁶ MIRON–THORNTON 2024.

a társadalom működésének rendszerszintű megbénítását, ezáltal a védekezés stratégiai feltételeinek felszámolását célozza.

Az orosz katonai gondolkodásban az információs tér ellenőrzése kulcsfontosságú. A doktrína központi eleme a „káoszeremtés”, vagyis az ellenfél döntéshozatali ciklusának megbénítása. Ebben a koncepcióban a kibertámadások elsődleges célja az információs tér előkészítése a kinetikus műveletek támogatására: a célország társadalmi kohéziójának gyengítése, a bizalom aláásása és a védekező fél kommunikációs képességeinek kiiktatása még azelőtt, hogy az első lövés eldördülne.¹⁷

A 2022. február 24-i teljes körű orosz inváziót megelőző hónapokban, de különösen az utolsó hetekben a kibertevékenység jellege drasztikusan megváltozott. Míg korábban, 2014 után az orosz állami háttérű csoportok főként kémkedésre és adatszerzésre fókuszáltak, az 2022-es invázió előtt megjelentek a kifejezetten pusztításra tervezett, destruktív kódok (*wiperek*).¹⁸ Ukrajna és a világ többi része már 2017-ben találkozhatott a magát első ránézésre egyszerű zsarolóvírusnak álcázó NotPetya kártevővel, amely világszerte jelentős károkat okozott.¹⁹ 2022 januárjában jelent meg a WhisperGate, szintén zsarolóvírusnak álcázva magát, de valójában nem tartalmazott helyreállítási funkciót,²⁰ tehát a titkosított adat visszaszerzésére nem volt valószínűség. Közvetlenül az invázió előtt és alatt aktiválták a HermeticWiper és az IsaacWiper kódokat, amelyek ukrán kormányzati hálózatokat és pénzügyi rendszereket támadtak.²¹ Ezek a műveletek a felégetett föld taktikáját alkalmazták a digitális térben: céljuk a kritikus adatok megsemmisítése és a visszaállítás lehetetlenné tétele volt.

A destruktív vírusokkal párhuzamosan, a teljes körű orosz invázió előtti napokban (február 15-től kezdődően) és az első 48 órában Ukrajna történetének legintenzívebb elosztott szolgáltatásmegtagadás (*distributed denial of service, DDoS*) támadásai érték az országot.²² A célpontok tudatosan a civil szférából kerültek ki: a legnagyobb állami bankok, a védelmi minisztérium portáljai és a lakossági tájékoztatást szolgáló kormányzati weboldalak váltak elérhetetlenné. Ez a műveletsorozat szervesen illeszkedett az orosz hadászati elképzelésbe, amely a gyors siker feltételének tekinti az információs környezet destabilizálását. A banki szolgáltatások és kormányzati intézmények működésének akadozása a lakosság elbizonytalanítását, a pánikkeltést célozta, tehát pontosan a kritikus infrastruktúrák működésének/kiesésének társadalmi vetületére épült. A kormányzati kommunikációs csatornák elvágása (vagy azok megbízhatóságának megkérdőjelezése) megnehezítette a polgári védelem és a katonai vezetés koordinációját és gátolta a döntéshozatalt. A digitális vakság, a helyzetfelismerő képesség (*situational awareness*) elvesztése és a hátszárban eluralkodó káosz elméletben megkönnyítette volna az orosz előre nyomulást, előkészítve ezzel a kinetikus támadás sikerét és csökkentve a szervezett ellenállás esélyét.

¹⁷ HAIG 2018; KOVÁCS 2018.

¹⁸ *A Decade in the Trenches of Cyberwarfare* 2024.

¹⁹ KRASZNAV 2022.

²⁰ AMBRUS 2023.

²¹ ESET Research: *Ukraine hit by Destructive Attacks before and during the Russian Invasion with HermeticWiper and IsaacWiper* 2022.

²² *A Decade in the Trenches of Cyberwarfare* 2024.

Az orosz offenzíva nem ért el gyors sikert, de a kibertérben 2022 és 2023 közt nagyságrendi ugrás volt az orosz–ukrán háború során megfigyelt kibertámadások számában és a módszerek, célpontok is változatosabbak lettek.²³ A támadások adatait gyűjtő CyberPeace Institute pedig 2023 decemberével meg is szüntette az adatok publikálását,²⁴ de már 2023 során is látható volt, hogy nehezen birkóznak meg az egyre intenzívebb kibertevékenységek elemzésének feladatával.

Kutatási módszertan

Jelen tanulmány kutatási módszertana kvalitatív elemzésen alapul, keretében az elérhető szakirodalom, a technikai jelentések és a releváns események szisztematikus feldolgozása történt meg. A vizsgálat időbeli kereteit a 2022. február 24-én megindult orosz invázió kezdetétől napjainkig terjedő időszak határozza meg (néhány releváns korábbi esemény említésével), különös tekintettel a konfliktus azon szakaszaira, ahol a kiberműveletek és a kinetikus hadviselés koordinációja bizonyíthatóan megjelent.

Az elemzés esettanulmány-alapú megközelítést alkalmaz az elméleti megközelítések gyakorlati igazolására. A vizsgált incidensek – kiemelten a Viasat és a Kyivstar elleni támadások – kiválasztása során a célzott mintavétel elvét követtük, mivel ezek tekinthetők a leginkább reprezentatív példáknak a civil és katonai szféra összefonódásából fakadó kockázatok bemutatására. A Viasat-incidens a határokon átnyúló tovagyrúzó hatás (*spillover effect*), míg a Kyivstar-eset a társadalmi-katonai mély interdependencia miatt tekinthető paradigmateremtő példának – mindkettő alkalmas az elméleti hipotézis tesztelésére. Ezen esetek kiválasztását az is indokolta, hogy rajtuk keresztül szemléltethető legtisztábban a kettős felhasználású technológiák inherens sebezhetősége és a civil lakosságra gyakorolt súlyos következmények. Továbbá ezek az incidensek szolgáltatják a legkézzelfoghatóbb bizonyítékot arra, ahogyan egy lokális konfliktus kiberműveletei a fizikai határokon átnyúlva nemzetközi, tovagyrúzó hatásokat generálnak, veszélyeztetve ezzel harmadik felek kritikus infrastruktúráját is.

A kvalitatív kutatás adatgyűjtési protokollja a vizsgált jelenség – a zajló fegyveres konfliktus kiberdimenziója – dinamikus változó természete miatt nem néhány, adott időpillanatban lefuttatott keresésre épült. A felhasznált források gyűjtése folyamatos forrásmonitorozáson és longitudinális szakirodalom-követésen alapult a 2022. február 24-től napjainkig terjedő időszakban. A szakirodalmi és technikai források felkutatása és kiválasztása szakértői célzott mintavétellel történt. A feldolgozott források köre elsődlegesen a kurált, referált folyóiratokat indexáló tudományos adatbázisokban (például Scopus, Web of Science) megjelent, kiberbiztonsággal és hadtudománnyal foglalkozó lektorált cikkekre terjedt ki. Ezt a szisztematikus szakirodalom-gyűjtést tudományos keresőmotorok (elsősorban a Google Scholar) találatai, valamint akadémiai kutatói közösségi platformok (ResearchGate, Academia.edu) használata egészítette ki. A téma sajátosságaiból fakadóan az elemzés támaszkodott továbbá releváns technikai és iparági jelentésekre (eseménykezelő központok és nagyvállalatok

²³ Kiss 2024.

²⁴ *Cyber Attacks in Times of Conflict* [é. n.].

biztonsági jelentései, technikai elemzések), valamint elsődleges forrásokra (az érintettek Telegram- és blogbejegyzései). A kiberműveletekre vonatkozó források kiválasztásához és megbízhatóságának megítélésénél az ENISA (az Európai Unió Kiberbiztonsági Ügynöksége) fenyegetettségi térkép módszertanának szempontjait alkalmaztuk.²⁵ A tisztán kinetikus műveletekre fókuszáló forrásokat kizártam. Az azonosított források strukturálása, kódolása és rendszerezése egy dedikált referenciakezelő adatbázisban történt. A kutatás elméleti kereteit adó szakirodalom vizsgálatakor tudatosan nagy hangsúlyt kapott a magyar katonai és biztonságpolitikai szakirodalom, mivel a magyar kutatók nyelvi és regionális beágyazottságuk okán gyakran olyan primer orosz és ukrán forrásokat is feldolgoznak a konfliktus operatív szintű elemzésekor, amelyek az angol-szász elméleti irodalomban ritkábban jelennek meg.

Tekintettel a kutatás kvalitatív és esettanulmány-alapú jellegére, a vizsgálat megismételhetőségét és megbízhatóságát az analitikus transzparencia és a logikai konzisztencia garantálja. Az eredmények igazolhatóságát az események strukturált, előre rögzített analitikus mátrix – az interdependencia típusa, a járulékos kár és a további ürrítő hatás – mentén történő vizsgálata biztosítja. Ez a módszertani keret teszi lehetővé, hogy a vizsgált incidensek mint empirikus adatpontok, valamint a belőlük levont rendszerszintű, elméleti következtetések közötti összefüggés külső elemzők számára is egyértelműen visszakövethető és igazolható legyen bármilyen hiteles esetleírásból kiindulva.

Eredmények

Esettanulmányok: kritikus infrastruktúrák a célkeresztben

Az orosz–ukrán háború tapasztalatai azt mutatják, hogy a kinetikus hadműveletek sikeréhez ma már elengedhetetlen a hátszág kritikus rendszereinek megbénítása, mert a háború nem korlátozódik a frontvonalra. Az orosz támadók figyelme két szektor, az energia és a távközlés felé fordult, amelyek a modern információs társadalom és a hadsereg idegrendszerét és keringését jelentik, ezért stratégiai célpontok. Az energetikai hálózat elleni támadások, különösen az elosztóhálózatok és alállomások ipari vezérlőrendszerei (*industrial control systems* és *supervisory control and data acquisition*, ICS/SCADA) ellen azonnali, kaszkádszerű hatást váltanak ki. Áram nélkül megbénul a logisztika, leállnak a vízművek, és működésképtelenné válnak a kommunikációs tornyok. A távközlés és a kommunikációs csatornák elvágása pedig a védekező fél vakságát és süketségét eredményezi. Az orosz stratégia a fagyos tél taktikáját alkalmazta a kibertérben is: a polgári lakosság moráljának megtörése és a katonai vezetés kommunikációs csatornáinak elvágása egyszerre valósult meg ugyanazon infrastruktúrák támadásával.

A 2022-es teljes körű orosz invázió során látott kibertámadások nem voltak előzmény nélküliek, 2015 és 2016 során több nagyon súlyos kibertámadás is érte az ukrán villamosenergia-rendszert.²⁶ Az első nagyobb támadás során 2015. december 23-án

²⁵ European Union Agency for Cybersecurity 2025.

²⁶ KRASZNAV 2022.

mintegy 225 000 fogyasztó maradt ellátatlan a hideg ukrán télben.²⁷ A támadás egyértelműen Oroszországnak tulajdonítható, a közvetlenül karácsony előtti időzítés pedig erősen arra utal, hogy a lélektani hatás is szempont volt amellett, hogy az ünnepek alatt általában nehezebb a hibák elhárítása is. A vizsgált támadásokat és azok hatásait az 1. táblázat foglalja össze.

1. táblázat: A vizsgált incidensek összefoglalása

Vizsgált incidens	Elsődleges célpont	Érintett civil szféra	Interdependencia típusa	Tovagyűrűző hatás
Energetikai hálózatok elleni 2015-ös támadás	Ipari vezérlő-rendszerek (ICS/SCADA), elosztó-hálózatok	Lakossági áramellátás (több száz-ezer fogyasztó), fűtési kiesés	Fizikai és funkcionális (áramellátástól függő kritikus alrendszerek)	Szektorközi kaskádhatás (logisztika, vízművek, távközlési bázisállomások azonnali leállása)
Viasat KA-SAT (2022)	Viasat földi infrastruktúra, ukrán fegyveres erők C2 rendszere	Lakossági internetszolgáltatás, európai felhasználók	Technológiai (közös platform, kettős felhasználású műholdas hálózat)	Nemzetközi spillover (NATO-tagállam kritikus infrastruktúrája: német szélerőművek távvezérlésének elvesztése)
Kyivstar (2023)	Ukrán mobilszolgáltató maghálózata, katonai és polgári védelmi kommunikáció	Milliók mobil- és internetelérése, banki ATM-ek, légoltalmi szírnák	Szolgáltatói és logikai (azonos kereskedelmi hálózaton futó civil és védelmi adatforgalom)	Társadalmi-gazdasági sokk (pénzügyi tranzakciók és polgári védelmi rendszerek egyidejű megbénulása)

Forrás: a szerző szerkesztése

A Viasat KA-SAT-incidens

A Viasat KA-SAT-incidens a modern hadviselés történetének egyik legjelentősebb kiberbiztonsági eseménye 2022. február 24-én, az invázió megindulásának óráiban történt. A Viasat amerikai műholdas szolgáltató KA-SAT-műholdhoz kapcsolódó hálózata elleni támadás tökéletesen illusztrálja a kettős felhasználású technológiákból fakadó sebezhetőséget. Ez az eset tekinthető a civil–katonai összefonódás iskolapéldájának, ahol minden elméleti kockázat egyszerre vált kézzelfogható valósággá. Az offenzíva napján hajnalban, éppen akkor, amikor az orosz csapatok átlépték az ukrán határt, célzott kibertámadás érte a Viasat földi infrastruktúráját. A támadók egy menedzsmenthálózaton keresztül hibás *firmware* frissítést küldtek ki a felhasználói terminálokra (modemekre). A kártékony kód (amelyet később AcidRain néven azonosítottak) gyakorlatilag törölte a modemek memóriáját, használhatatlanná téve azokat és elvágyva a modemek által biztosított internetkapcsolatot.²⁸ A támadás elsődleges célpontja nem a civil lakosság volt, hanem az ukrán fegyveres erők. Ukrajna ugyanis – saját, dedikált katonai műholdas rendszer híján – nagymértékben támaszkodott a kereskedelmi

²⁷ GÖRGEY 2020.

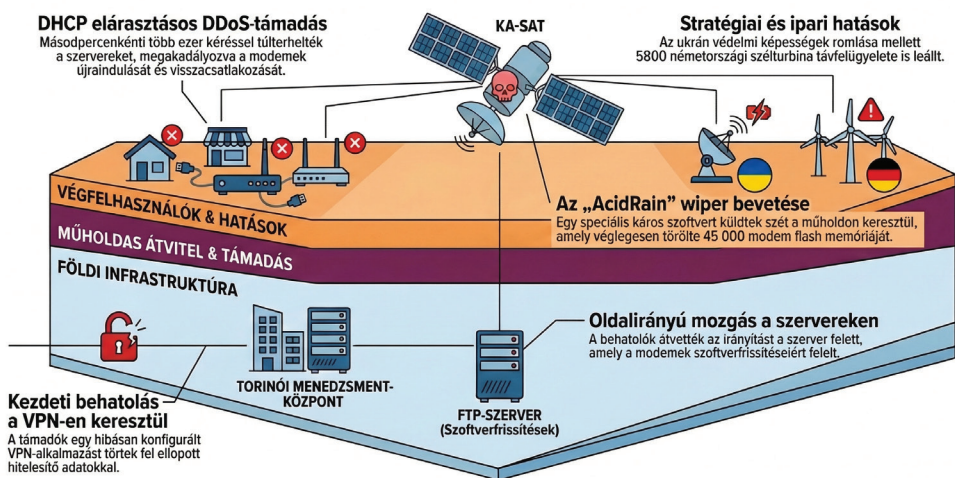
²⁸ BURGESS 2022.

Viasat hálózatra a katonai kommunikációban. A támadás következtében az invázió legkritikusabb első óráiban jelentős zavar keletkezett az ukrán parancsnoki és irányítási (C2) rendszerben, ami átmenetileg megnehezítette a védekező egységek koordinációját.

Amellett, hogy a támadás a katonai kommunikáción túl az ukrán civil lakosságot is jelentősen érintette, a Viasat-incidens rávilágított arra is, hogy a kibertérben nincsenek országhatárok. Mivel a KA-SAT-hálózat egész Európát lefedi, a támadás hatásai azonnal tovagyűrűztek, jelentős nemzetközi járulékos károkat okozva:

- civil felhasználók: Európa-szerte több tízezer lakossági internet-előfizető szolgáltatása szűnt meg hosszabb-rövidebb időre;
- kritikus infrastruktúra az EU-ban: a legmegdöbbentőbb hatás Németországban jelentkezett, ahol közel 5800 szélerőműű távvezérlése állt le.²⁹ Ezek a turbinák a Viasat hálózatán keresztül kommunikáltak a vezérlőközponttal. Bár az áramtermelés nem állt le, a rendszerek felügyelete megszűnt, ami rávilágított arra, hogy egy földrajzilag elkülöníthető konfliktus kiberműveletei hogyan veszélyeztethetik NATO-tagállamok kritikus infrastruktúráját is.

Ez az eset ékesen bizonyítja, hogy a katonai célú kibercsapások a közös technológiai platformok miatt elkerülhetetlenül érintik a civil szférát, a kibertér nemzetközi jellegéből adódóan potenciálisan globális biztonsági kockázatot teremtve. Az Európai Unió főképviselője közleményben ítélte el a Viasat elleni támadást, és kiemelte: „Az Ukrajnát célzó kibertámadások, beleértve a kritikus infrastruktúrát érintőket is, áttejedhetnek más országokra is, és rendszerszintű hatásokkal járhatnak, veszélyeztetve az európai polgárok biztonságát.”³⁰ Ez az eset empirikusan bizonyítja a kibertér területek feletti jellegét: egy lokális konfliktusban alkalmazott precíziós fegyver a közös technológiai platform miatt globálisan tovagyűrűző hatást váltott ki. A Viasat-incidens elemeit és hatásait az 1. ábra foglalja össze.



1. ábra: A Viasat-incidens elemei és hatásai

Forrás: a szerző szerkesztése a NotebookLM mesterséges intelligencia felhasználásával, a cikkben hivatkozott felhasznált irodalom alapján

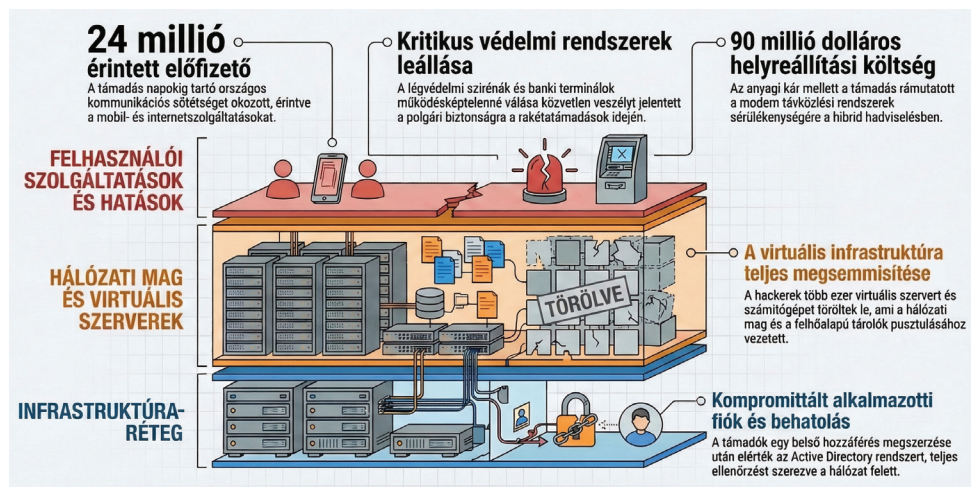
²⁹ Reuters 2022.

³⁰ European Council 2022.

A Kyivstar elleni támadás

2024. december 12-én történt egy másik nagyon jelentős, ukrán kommunikációs kritikus infrastruktúrát érintő támadás, amely a Kyivstar mobil- és internetszolgáltatását bénította meg napokra. A holland tulajdonú Kyivstar Ukrajna legnagyobb mobilszolgáltatója közel 24 millió előfizetéssel, így a szolgáltatáskiesés is több millió ügyfelet érintett Kijev és Szumi régióiban. A kommunikációs zavar nem csak lakossági ügyfelekre terjedt ki: a banki ATM-ek gyakran mobilhálózaton kommunikálnak (ha az elhelyezésük miatt nem praktikus vezetékes hálózatot kiépíteni), de a katasztrófavédelem kommunikációját és a két régió légoltalmazási-rendszereit is érintette a kiesés. A támadást technikai jellemzői alapján az ukrán eseménykezelő központ (CERT-UA) az orosz katonai hírszerzéshez, a GRU-hoz köthető Sandworm csoportnak tulajdonította. Egy szintén a Sandworm-egységhez köthető orosz hackercsoport pedig Telegram-közleményben vállalta magára a támadást. „A Kyivstar ellen azért indítottunk támadást, mert a vállalat kommunikációs szolgáltatásokat nyújt az ukrán fegyveres erőknek, valamint az ukrán kormányzati szerveknek és bűnüldöző szerveknek”, írták Telegram-csatornájukon.³¹ Mivel ez egy aktív információs hadviselési környezetben közzétett primer forrás, az abban foglalt állításokat a lehetséges stratégiai kommunikációs és dezinformációs célok miatt forráskritikával kell kezelni, azonban a közlés tartalma egybevág a más forrásokból ismert tényezőkkel (technikai attribúció, orosz hibrid hadműveletek módszertana).

A Kyivstar és a hozzá hasonló kibertámadások civil lakosság által elszenvedett következményei miatt a Nemzetközi Büntetőbíróság is vizsgálatot indított.³² A bizonyítékokat, amelyek a vizsgálat elindításához vezettek, a Berkeley Human Rights Center kutatói gyűjtötték össze és nyújtották be. Az ő nyilatkozataiból tudjuk, hogy legalább öt ügyben zajlik vizsgálat: három, az ukrán energetikai hálózatot ért kibertámadás, a NotPetya és a Viasat-incidens esetében merült fel a háborús bűncselekmények, azaz a genfi egyezmények megsértésének gyanúja.³³ A Kyivstar elleni támadás elemeit és következményeit a 2. ábra foglalja össze.



2. ábra: A Kyivstar-incidens elemei és hatásai

Forrás: a szerző szerkesztése a NotebookLM mesterséges intelligencia felhasználásával, a cikkben hivatkozott felhasznált irodalom alapján

³¹ GREENBERG 2023.

³² DEUTSCH-BERG-PEARSON 2024.

³³ VERBRUGGEN 2023.

Következtetések

A védekezés új modellje: a magánszektor és a civil társadalom stratégiai szerepe

Az orosz–ukrán háború egyik legmeghatározóbb tanulsága, hogy a modern kibervédelem már nem kizárólag állami monopólium. Ukrajna digitális túlélése nagymértékben a globális technológiai óriások (*big tech* cégek) példátlan szerepvállalásának és a civil társadalom mozgósításának köszönhető. Ez a jelenség új működési modellt teremtett, elmosva a határokat az állami és a magánszereplők között, és az együttműködés már nemcsak a kiberbűnözés elleni harcra terjed ki,³⁴ hanem kifejezetten védelmi célokat is szolgál. A 2022-es teljes körű orosz invázió kezdetén egyfajta digitális védőernyő jött létre Ukrajna felett, amelyet nem a NATO, hanem magánvállalatok tartottak. A nagy felhőszolgáltatók (Microsoft, Google, Amazon), valamint a kiberbiztonsági cégek, mint az ESET és a Mandiant, proaktívan léptek fel az orosz fenyegetésekkel szemben. A Microsoft alelnöke és elnöke, Brad Smith emellett blogbejegyzésben fejezte ki aggodalmát a civil célpontok elleni kibertámadások miatt is.³⁵

Az Amazon Web Services (AWS), a Microsoft Azure és a Google Cloud segítségével Ukrajna a háború első napjaiban végrehajtotta a kormányzati rendszerek „digitális evakuációját”. A fizikai szervertermek, amelyek rakétatalálatnak voltak kitéve, virtuálissá váltak: az állami adatvagyon (nyilvántartások, banki adatok) biztonságos, külföldi felhő-infrastruktúrákba költözött, garantálva az állam működőképességét. Míg korábban Ukrajna a magyar szabályozáshoz hasonlóan konzervatív módon tiltotta a nemzeti adatvagyon felhőbe költöztetését, a fizikai megsemmisülés fenyegetése miatt az ukránok újraértékelték a kockázatokat és kiadták a jogszabályt, amely lehetővé tette a felhő használatát.³⁶

Amikor a földi infrastruktúra a kinetikus támadások következtében sérült, a SpaceX Starlink műholdas rendszere biztosította a redundáns kommunikációt. Ez nemcsak a civil lakosság kapcsolattartását tette lehetővé, hanem a katonai egységek, tűzérési rendszerek és drónok irányításának gerincévé is vált, gyakorlatilag katonai képességgé konvertálva egy civil szolgáltatást.³⁷

A fentiek eredményeként a kormányzati és katonai műveletek támogatása egyre inkább privát kapacitásokra támaszkodik. A kettős felhasználású technológiák fogalma kiegészült a kapacitások „privatizálódásával”: a hadsereg olyan eszközöket használ, amelyeket nem ő birtokol, nem ő üzemeltet, és amelyek felett nincs teljes kontrollja. Ez a szimbiózis hatékony, de új függőségi viszonyokat és kockázatokat teremt, hiszen ezek a multinacionális cégek önálló geopolitikai aktorokká léptek elő, akiknek döntései (például szolgáltatás korlátozása egy adott régióban³⁸) közvetlen hatással vannak a katonai műveletek kimenetelére.

A technológiai óriások ezen szerepvállalása alátámasztja a civil–katonai viszonyokat vizsgáló korábbi nemzetközi kutatások (például Myriam Dunn Cavelty és Florian J.

³⁴ MOYNIHAN–WEBB–CLOONEY 2025.

³⁵ SMITH 2022.

³⁶ *Про хмарні послуги* [é. n.].

³⁷ BÍRÓ 2025a.

³⁸ ROULETTE – BRYAN-LOW – BALMFORTH 2025.

Egloff³⁹) azon megállapításait, miszerint a kibertérben a klasszikus állami erőszak-monopólium erodálódik. Kialakul a „digitális szuverenitás paradoxona”: az állam fizikai túlélése érdekében kénytelen védelmi funkcióinak és szuverenitásának egy részét önálló geopolitikai aktorokként fellépő magánvállalatokra delegálni. Bár ez a fejlődési irány megjósolható volt, a 2022. február 24. utáni események tökéletesen megmutatták, hogy a jelenség mennyire valós.

A technológia mellett az emberi tényező is átalakult. A kiberhadviselésben a frontvonal nem lövészárkokban, hanem szerverszobákban és nappalokban húzódik, a támadók és védekezők pedig gyakran civilek. A kritikus infrastruktúrák védelmében a magáncégek IT-szakemberei váltak az első védelmi vonallá. Amikor egy bankot vagy energiaszolgáltatót támadás ér, nem katonák, hanem civil mérnökök és rendszergazdák hárítják el a veszélyt. Ők azok, akik foltozzák a biztonsági réseket és helyreállítják a szolgáltatást, miközben munkájukkal közvetve kibervédelmi feladatot látnak el.

Egyedülálló jelenség az ukrán kormány által hivatalosan is támogatott, de önkéntes alapon szerveződő IT Army of Ukraine (ukrán IT hadsereg) létrejötte. Ez, a becslések szerint több százezer fős, globális hacktivisták közössége 2022 során koordinált DDoS-támadásokat intézett orosz célpontok ellen.⁴⁰ Bár rövid távon látványos sikereket tudtak felmutatni, és a kezdeményezés hatékony aszimmetrikus választ adott az orosz agresszióra, a jelenség súlyos etikai és jogi kérdéseket vet fel. Az IT Army of Ukraine-hez csatlakozó, Ukrajnán kívüli, nemzetközi önkéntesek az orosz rendszerek elleni támadásokkal valószínűleg bűncselekményt követnek el. Másfelől a nemzetközi hadijog (genfi egyezmények) értelmében a civilek védelmet élveznek, de ha közvetlenül részt vesznek a háborús cselekményekben (márpedig egy infrastruktúra elleni kibertámadás annak minősülhet), elveszíthetik védettségüket és legitim katonai célponttá válhatnak. Ugyanez fenyegeti azokat a civileket, akik az ukrán eVorog alkalmazás használatával segítik az orosz katonai célpontok azonosítását.⁴¹ Maga az eVorog szintén alapvetően civilek által használt komponensekből áll: a végfelhasználó mobiltelefonja, egy Telegram-csatorna és az ukrán elektronikus közszolgáltatásokhoz használt hitelesítési mechanizmus. Ezzel vissza is jutunk oda, hogy ha civil eszközöket használunk katonai célok megvalósítására, akkor a civil infrastruktúrák is katonai célponttá válnak.

A civil–katonai infrastruktúra kapcsolatának tanulságai a jövőre nézve

Az orosz–ukrán háború kiberdimenziója rámutatott a hagyományos védelmi doktrínák újragondolásának szükségességére. Korábban az állam szerepe kizárólagos vagy döntő volt a biztonság garantálásában, azonban a modern konfliktusokban – mint amilyen az orosz–ukrán háború is – ez a megközelítés már nem tartható. Az államnak ki kell alakítania a hatékony együttműködést a nem állami szférával (magánszektor, civil társadalom), mivel a biztonság szavatolása már nem tisztán állami feladat.⁴² Ugyanígy

³⁹ CAVELTY–EGLOFF 2019.

⁴⁰ SOESANTO 2022.

⁴¹ BIRÓ 2025b.

⁴² FARKAS–KELEMEN 2023.

a kritikus infrastruktúrák védelme is civil–katonai együttműködést igényel. A jövő konfliktusaiban a győzelem vagy vereség nem kizárólag a katonai képességeken múlik, hanem azon, hogy egy állam képes-e integrálni civil erőforrásait a védelmi rendszerbe. A konfliktus legfontosabb tanulságait az alábbi három pontban összegezhetjük:

- szervezeti és szabályozási paradigmaváltás;
- kiberreziliencia-építés és közös sérülékenységmentesítés;
- kritikus privát szereplők integrálása a védelmi tervezésbe.

A hibrid fenyegetések korában a polgári és katonai felelősségi körök szigorú szétválasztása biztonsági kockázatot jelent. A háború tapasztalatai alapján újra kell gondolni a védelmi struktúrákat. A védelem nem lehet kizárólag az állam feladata. Ukrajnában a decentralizáltan működő civil szervezetek (NGO-k) és szakmai közösségek sokszor gyorsabban reagáltak a kiberfenyegetésekre és az eszközhiányra, mint a központi bürokrácia. A jövő szabályozásának teret kell engednie az ellenőrzött, de rugalmas civil szakmai részvételnek. A békeidős jogszabályok gyakran akadályozzák az operatív együttműködést (például adatvédelmi korlátok a fenyegetési információk megosztásában). Olyan jogi keretekre van szükség, amelyek krízishelyzetben automatikusan lehetővé teszik a polgári infrastruktúra üzemeltetői és a honvédelmi szervek közötti közvetlen, kétirányú adatcserét.

Mivel a hadsereg a civil hálózatokon „utazik”, a katonai rendszerek biztonsága csak annyira erős, amennyire a civil infrastruktúra leggyengébb láncszeme. A felkészülés során fel kell térképezni a civil és katonai rendszerek közös metszeteit, leggyengébb láncszemeit (*single points of failure*). Nem elegendő a katonai hálózatot védeni; a hadsereg által használt polgári energiaszolgáltató vagy internetszolgáltató rendszerét is katonai szintű védelmi szabványokhoz kell közelíteni. A kettős felhasználású infrastruktúrák fejlesztésekor már a tervezési fázisban figyelembe kell venni a potenciális katonai felhasználásból eredő többletkockázatot.

A Starlink vagy a Microsoft szerepvállalása bizonyította, hogy a globális technológiai vállalatok *de facto* geopolitikai szereplőkké váltak. Az államoknak nem egyszerű beszállítóként, hanem stratégiai partnerként kell tekinteniük ezekre a cégekre. A védelmi tervezésbe be kell vonni a kritikus infrastruktúrát üzemeltető magáncégek képviselőit. A fenyegetésekről szóló hírszerzési információk (*threat intelligence*) megosztását ki kell terjeszteni a megbízható magánszereplőkre is, hiszen gyakran ők észlelik először a hálózataikon a rendellenes aktivitást, amely egy állami szintű támadás előjele lehet.

Az orosz–ukrán háború legátfogóbb tanulsága, hogy a civil infrastruktúrák sebezhetősége csökkenti az állam ellenálló képességét, mivel könnyű célpontot kínál az aszimmetrikus hadviseléshez. Ezzel szemben egy magas rezilienciájú, redundáns és a védelmi szektorral szorosan együttműködő civil infrastruktúra megnehezítheti a támadó dolgát. A jövőben a katonai erő nem értelmezhető a mögötte álló, ellenálló-képes digitális hátszázág nélkül.

Összegzés

Az orosz–ukrán háború elemzése rávilágított arra, hogy a 21. századi fegyveres konfliktusok természete visszafordíthatatlanul megváltozott. A tanulmányban bemutatott esettanulmányok és folyamatok igazolják, hogy a kinetikus és a kiberműveletek szinkronizációja a modern hadviselés alapmegközelítésévé vált. Ez a szoros összehangoltság a gyakorlatban megmutatta, hogy háborús helyzetben megszűnt az éles határvonal a civil és a katonai infrastruktúrák között, a civil szféra veszteségei pedig a hadviselés elkerülhetetlen következményévé váltak.

A technológiai fejlődés és a rendszerek mély integrációja miatt a katonai és civil infrastruktúrák szétválasztása ma már nem csupán elméleti, hanem súlyos gyakorlati nehézségekbe ütközik. A kettős felhasználású eszközök tömeges alkalmazása miatt a civil hálózatok (energia, távközlés) a hadműveletek szerves részévé és ezáltal legitimnek tekinthető célponttá váltak. Ebben a kontextusban a kritikus infrastruktúrák elleni támadások során a kiberműveletek stratégiai jelentősége megkérdőjelezhetetlen: képesek fizikai pusztítás nélkül is megbénítani egy állam védelmi képességeit és társadalmi működését.

A jövő kiberbiztonsági kihívásaira adható válasz kulcsa a szektorközi együttműködés. Az állami monopóliumra épülő védelem már nem elégséges; a nemzeti reziliencia csak a magánszektor, a technológiai szolgáltatók és a kormányzati szervek szoros, bizalmi alapú kooperációjával érhető el.

Végezetül, a hibrid fenyegetések komplexitása miatt felértékelődött a katasztrófavédelem szerepe. Mivel a kibertámadások a civil lakosságot is jelentősen érintő fizikai következményekkel járnak (például áramszünet, fűtés kiesés, ellátási láncok megszakadása), a katasztrófavédelem már nem csupán a természeti csapások kezelője, hanem a hibrid hadviselés okozta társadalmi sokkhatások első számú kezelője. A jövőben a kibervédelem és a polgári védelem (katasztrófavédelem) integrációja jelenti majd a nemzeti biztonság egyik legfontosabb pillérét.

Felhasznált irodalom

- A Decade in the Trenches of Cyberwarfare* (2024). Cyber Diia. Online: <https://nsarchive.gwu.edu/document/32135-30-cyber-diia-decade-trenches-cyberwarfare>
- AMBRUS Éva (2023): *Kiberhadviselési képességek a jelen tükrében*. Budapest: Nemzeti Közszolgálati Egyetem. Online: https://kmdi.uni-nke.hu/document/kdmi-uni-nke-hu/Ambrus_PhD_%C3%A9rtekez%C3%A9s.pdf
- BAKOS Tamás – KOVÁCS Ferenc (2025): Az interdependencia dimenziói és a kritikus szervezetek vizsgálata. *Hadtudomány*, 35(3), 106–119. Online: <https://doi.org/10.17047/HADTUD.2025.35.3.106>
- BÍRÓ Gabriella (2025a): Védelmi innováció az orosz–ukrán háború kiberműveleteiben. *Haditechnika*, 59(kisz.), 111–115.

- BÍRÓ Gabriella (2025b): Az ukrán eVorog chatbot és a Delta rendszer. *Haditechnika*, 59(5), 18–21. Online: <https://honvedelem.hu/kiadvanyok/haditechnika-2025-5.html>
- BOGNÁR Balázs – BONNYAI Tünde szerk. (2019): *Kritikus infrastruktúrák védelme I.* Budapest: Dialóg Campus. Online: https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/12450/595_kritikus_infrastrukturak_vedelme.pdf?sequence=1
- BURGESS, Matt (2022): A Mysterious Satellite Hack Has Victims Far Beyond Ukraine. *Wired*, 2022. március 23. Online: www.wired.com/story/viasat-internet-hack-ukraine-russia/
- CAVELTY, Myriam Dunn – EGLOFF, Florian J. (2019): The Politics of Cybersecurity: Balancing Different Roles of the State. *St Antony's International Review*, 15(1), 37–57. Online: https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Dunn_Cavelty_Egloff_2019%20STAIR%20Issue%2015.1.pdf
- Cyber Attacks in Times of Conflict* [é. n.]. CyberPeace Institute. Online: <https://cyber-conflicts.cyberpeaceinstitute.org/>
- DEUTSCH, Anthony – BERG, Stephanie van den – PEARSON, James (2024): ICC Probes Cyberattacks in Ukraine as Possible War Crimes, Sources Say. *Reuters*, 2024. június 14. Online: www.reuters.com/world/europe/icc-probes-cyberattacks-ukraine-possible-war-crimes-sources-2024-06-14/
- ESET Research: *Ukraine hit by Destructive Attacks before and during the Russian Invasion with HermeticWiper and IsaacWiper* (2022). ESET. Online: www.eset.com/us/about/newsroom/research/eset-research-ukraine-hit-by-destructive-attacks-before-and-during-the-russian-invasion-with-hermet/?srsltid=AfmBOopiPjnyDqcsp-R5AVqX3bBaryP8zUjiQOXcLzF2OPfEOCRU0-dhd
- European Council (2022): *Russian Cyber Operations Against Ukraine: Declaration by the High Representative on Behalf of the European Union*. Online: www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/
- European Union Agency for Cybersecurity (2025): *ENISA Cybersecurity Threat Landscape Methodology*. Luxembourg: Publications Office of the European Union. Online: <https://doi.org/10.2824/1888892>
- FARKAS Ádám – KELEMEN Roland (2023): *Nemzeti biztonság és kibertér*. Budapest: NMHH. Online: <https://mtmi.hu/files/7ddaa0c7-9a10-4123-af9c-e2d86c49cf30.pdf>
- GÖRGEY Péter (2020): Kibertámadások Ukrajnában: áramszünetek és tanulságok (I. rész). *Elektrotechnika*, 113(9–11), 9–11.
- GREENBERG, Andy (2023): Hacker Group Linked to Russian Military Claims Credit for Cyberattack on Ukrainian Telecom. *Wired*, 2023. december 13. Online: www.wired.com/story/ukraine-kyivstar-soltsepek-sandworm-gru/
- HAIG Zsolt (2018): *Információs műveletek a kibertérben*. Budapest: Dialóg Campus.
- JÓJÁRT Krisztián (2023): *Az orosz katonai gondolkodás 21. századi hadviselés-felfogásának értelmezése*. Budapest: Nemzeti Közszerológati Egyetem. Online: <https://doi.org/10.17625/NKE.2024.014>

- KISS Adrienn (2024): Az orosz–ukrán háború hatása a kritikus infrastruktúrákra – fókuszban az energiaszektor. *Hadmérnök*, 19(3), 183–200. Online: <https://doi.org/10.32567/hm.2024.3.11>
- KOVÁCS László (2018): *A kibertér védelme*. Budapest: Dialóg Campus. Online: www.uni-nke.hu/document/uni-nke-hu/Kov%C3%A1cs%20L%C3%A1szl%C3%B3.pdf
- KRASZNAY Csaba (2022): *Kiberbiztonság a XXI. században*. Budapest: Katonai Nemzetbiztonsági Szolgálat.
- MIRON, Marina – THORNTON, Rod (2024): The Use of Cyber Tools by the Russian Military: Lessons from the War against Ukraine and a Warning for NATO? *Applied Cybersecurity & Internet Governance*, 3(1), 147–169. Online: <https://doi.org/10.60097/ACIG/190142>
- MOYNIHAN, Harriet – WEBB, Philippa – CLOONEY, Amal (2025): *Legal Accountability for Malicious Cyber Operations*. Oxford Institute of Technology and Justice. Online: https://doi.org/10.35489/BSG-OITJ-PB-1_2025-01
- MUHA Lajos (2007): *A Magyar Köztársaság kritikus információs infrastruktúráinak védelme*. PhD-disszertáció. Budapest: Zrínyi Miklós Nemzetvédelmi Egyetem. Online: <https://real-phd.mtak.hu/74/1/1228916.pdf>
- ORBÓK Ákos (2013): A kibertér, mint hadszíntér. *Biztonságpolitika*, 2013, 101–108. Online: https://old.biztonsagpolitika.hu/documents/1375084295_Orbok_Akos_A_kibert%C3%A9r_mint_hadszinter_-_biztonsagpolitika.hu.pdf
- Reuters (2022): Satellite Outage Knocks out Thousands Of Enercon's Wind Turbines. *Reuters*, 2022. február 28. Online: www.reuters.com/business/energy/satellite-outage-knocks-out-control-enercon-wind-turbines-2022-02-28/
- RID, Thomas (2013): *Cyber War Will Not Take Place*. Oxford: Oxford University Press.
- ROULETTE, Joey – BRYAN-LOW, Cassell – BALMFORTH, Tom (2025): Musk Ordered Shutdown of Starlink Satellite Service as Ukraine Retook Territory from Russia. *Reuters*, 2025. július 25. Online: www.reuters.com/investigations/musk-ordered-shutdown-starlink-satellite-service-ukraine-retook-territory-russia-2025-07-25/
- SCHMITT, Michael N. szerk. (2017): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge – New York: Cambridge University Press. Online: <https://doi.org/10.1017/9781316822524>
- SMITH, Brad (2022): *Digital Technology and the War in Ukraine*. Microsoft on the Issues. Online: <https://blogs.microsoft.com/on-the-issues/2022/02/28/ukraine-russia-digital-war-cyberattacks/>
- SOESANTO, Stefan (2022): *The IT Army of Ukraine. Structure, Tasking, and Eco-System*. Zürich: Center for Security Studies (CSS). Online: <https://doi.org/10.3929/ethz-b-000552293>
- VERBRUGGEN, Yola (2023): Cybercrimes under Consideration by the ICC. *International Bar Association*, 2023. október 13. Online: www.ibanet.org/cybercrimes-under-consideration-by-the-ICC

Jogi források

2024. évi LXXXIV. törvény a kritikus szervezetek ellenálló képességéről
Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve (2022. december 14.)
a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon
kívül helyezéséről (EGT-vonatkozású szöveg). Online: <https://eur-lex.europa.eu/eli/dir/2022/2557/oj/hun>
Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to
the Protection of Victims of International Armed Conflicts (Protocol I), 8 June
1977. Online: <https://ihl-databases.icrc.org/en/ihl-treaties/api-1977>
Про хмарні послуги [é. n.]. Online: <https://zakon.rada.gov.ua/go/2075-20>

Gábor Fazekas¹ 

Multispectral Reconnaissance of Operational Areas²

Abstract

Multispectral and hyperspectral imaging offer complementary capabilities for remote reconnaissance by sampling reflected energy in several optical wavelength bands. This study evaluates their suitability for operational area monitoring, with an emphasis on light-weight, drone-borne sensors. A theoretical overview explains how spectral signatures arise from electronic transitions and molecular vibrations, leading to characteristic vegetation and soil reflectance patterns. Common vegetation and moisture indices are introduced, noting their sensitivity to chlorophyll content, water absorption and the limitations of MSI sensors lacking short-wave infrared bands. Remote-sensing platforms including handheld spectrometres, satellites and unmanned aerial vehicles are compared. UAVs equipped with multispectral cameras offer a favourable balance of spatial resolution, cost and ease of deployment. The DJI Mavic 3 Multispectral is selected for field experimentation due to its integrated four-band sensor (green, red, red-edge, near-infrared), sunlight sensor and RTK positioning. Other MSI cameras (MicaSense RedEdge-MX, Parrot Sequoia+) and representative hyperspectral cameras are briefly reviewed, highlighting tradeoffs in weight, spectral resolution and cost. A case study over a military training ground uses the M3M to acquire two flights – before and after a rain event – and processes the images using WebODM, QGIS and MATLAB. Vegetation indices map plant vigour and relative soil moisture, and change detection highlights vehicle tracks and wet areas. Results demonstrate that NDRE remains linear at high biomass and that simple red-edge metrics sensitively capture moisture changes despite the absence of SWIR. While the Mavic 3M lacks a blue band and SWIR band limits the calculation of some water related indices, its portability and affordability make it a valuable tool for rapid reconnaissance. The paper concludes by discussing future directions, including the integration of machine learning and additional sensors to enhance material identification and real-time processing. The index-based analysis is explicitly interpreted

¹ PhD student, Ludovika University of Public Service, Doctoral School of Military Engineering, e-mail: fazekas@gmail.com

² Supported by the DKÖP-NKE-24-06 Doctoral Excellence Scholarship Programme of the Ministry for National Research, Development and Innovation Fund.

as relative operational change detection rather than absolute biomass, reflectance or soil-moisture retrieval, because independent ground-reference measurements were not available during the field campaign.

Keywords: IMINT, CUAV, multispectral, hyperspectral imaging systems, image processing

Introduction

Remote sensing platforms have become indispensable for military and civil reconnaissance because they can monitor large areas without exposing human observers to danger. Multispectral (MSI) and hyperspectral (HSI) imaging systems capture reflected electromagnetic energy in a few or many optical wavelength bands, permitting analysts to infer material composition, vegetation health or land-use changes. In an operational context, the ability to detect footprints, vehicle tracks or the emergence of new objects relative to baseline imagery can provide early warning of adversary activities.³ In defence applications both the visible and thermal bands are widely used, but the application of narrow-band spectral processing in operational contexts remains an active area of research. The paper therefore moves in a deliberate sequence: it first reviews the physical background of spectral imaging, then compares the main sensing platforms and sensor categories, finally presents a drone-based case study to show how these principles translate into operational area monitoring in practice.

Physical background of spectral reconnaissance

Spectral imaging involves measuring the distribution of reflected or emitted electromagnetic energy as a function of wavelength. Multispectral imaging captures radiation in a limited number (e.g. 4–20) of broadbands using filters tailored to particular phenomena such as vegetation or water absorption. Hyperspectral imaging acquires hundreds of contiguous narrow bands ($\Delta\lambda \approx 1\text{--}10\text{ nm}$), effectively recording a full reflectance spectrum at each pixel. The key difference is therefore spectral resolution: HSI provides a quasi-continuous spectrum enabling subtle material identification, whereas MSI offers selected bands and is often sufficient when speed, cost and ease-of-use are paramount.⁴

The advantage of HSI is its ability to detect narrow absorption features associated with electronic transitions (e.g. chlorophyll absorption in the red) or molecular vibrations (e.g. water and hydroxyl bands in the short-wave infrared). However, hyperspectral instruments are heavier, more expensive and yield very large data volumes, which limits their use on small drones. Multispectral sensors, by contrast, use a handful of filters corresponding to specific phenomena (green, red, red-edge,

³ RAM et al. 2024.

⁴ RAM et al. 2024.

near-infrared), enabling lightweight and relatively inexpensive cameras that can be flown on compact drones such as the DJI Mavic 3 Multispectral (M3M). Their lower spectral resolution reduces the ability to unambiguously identify minerals or distinguish among similar vegetation types, but their simplicity and high spatial resolution make them attractive for operational reconnaissance tasks where rapid coverage is critical.⁵

Spectral signatures and material identification

Materials possess characteristic spectral signatures that arise from fundamental physical processes. In the visible and near-infrared (VNIR) region ($\approx 400\text{--}1,000\text{ nm}$) absorption is dominated by electronic transitions in pigments and minerals. For vegetation, the chlorophyll-a and chlorophyll-b molecules embedded in the thylakoid membranes of chloroplasts have strong absorption around $400\text{--}500\text{ nm}$ and $650\text{--}680\text{ nm}$ because of their molecular structure. The strong absorption in the red ($\approx 680\text{ nm}$) explains the low red reflectance of green leaves, while the decrease in absorption beyond 700 nm and the high internal scattering in leaf mesophyll cause a sharp rise in reflectance known as the red edge.⁶ Rocks and dry soils have weak absorption patterns because of metal ions and vibrations in their crystal structure, while water and hydroxyl groups absorb much more strongly in the short-wave infrared part of the spectrum at wavelengths longer than $1,000\text{ nm}$.⁷

Vegetation and soil spectral behaviour

The spectral behaviour of vegetation and soil can be explained by combining molecular absorption and canopy structure. Healthy leaves have low reflectance in the blue and red due to chlorophyll absorption, a steep red edge between $680\text{--}750\text{ nm}$ and high reflectance in the near-infrared due to multiple scattering within the spongy mesophyll. The position and slope of the red edge are sensitive to chlorophyll content, leaf structure and stress, which is why many sensors include a red-edge band.⁸ Dry soil exhibits relatively high reflectance across the visible and near-infrared, with gentle slopes and minimal absorption features; moisture darkens the soil and introduces absorption features around $1,450\text{ nm}$ and $1,950\text{ nm}$ (SWIR – Short Wave Infrared), so indices combining near-infrared and SWIR bands are often used to estimate soil water content.⁹

⁵ RAM et al. 2024.

⁶ GITELSON–MERZLYAK 1998.

⁷ TEIXEIRA et al. 2025.

⁸ DU et al. 2025.

⁹ TEIXEIRA et al. 2025.

Vegetation and moisture indices

Because multispectral sensors sample only a few bands, analysts often derive indices to enhance contrast between features of interest. The most widely used vegetation index is the Normalized Difference Vegetation Index (NDVI), defined as

$$NDVI = \frac{\rho_{NIR} - \rho_R}{\rho_{NIR} + \rho_R}$$

where ρ denotes reflectance, NIR is Near Infrared and R stands for Red. NDVI exploits the contrast between low red reflectance and high near-infrared reflectance. It correlates with vegetation vigour and is widely used for yield prediction, crop classification and irrigation management. The simplicity and general applicability of NDVI make it popular, but it saturates in dense vegetation and is sensitive to soil background and atmospheric effects. Other formulations, including soil-adjusted and red-edge-based indices, are often used to mitigate these limitations while preserving simple physical interpretation.¹⁰

For clarity, the notation used in the index equations refers to band-specific reflectance values rather than to wavelengths alone: ρ_{NIR} , ρ_R , ρ_{RE} , ρ_G and ρ_{SWIR} denote the measured reflectance in the near-infrared, red, red-edge, green and short-wave infrared bands, respectively. This distinction is important because the indices are calculated from reflectance values acquired in the corresponding spectral bands, not from the nominal band-centre wavelengths.

In unambiguous reflectance notation, the formulas can be written as: $NDVI = (\rho_{NIR} - \rho_R)/(\rho_{NIR} + \rho_R)$, $NDMI = (\rho_{NIR} - \rho_{SWIR})/(\rho_{NIR} + \rho_{SWIR})$, and $NDRE = (\rho_{NIR} - \rho_{RE})/(\rho_{NIR} + \rho_{RE})$.

Moisture indices combine bands sensitive to water absorption. The Normalized Difference Moisture Index (NDMI) uses near-infrared and SWIR reflectances

$$NDMI = \frac{\rho_{NIR} - \rho_{SWIR}}{\rho_{NIR} + \rho_{SWIR}}$$

to estimate vegetation or soil water content. The NDMI requires a SWIR band, so cameras lacking SWIR (e.g. M3M) cannot compute it directly. The Normalized Difference Water Index (NDWI) has multiple definitions; one common formulation uses green and NIR bands and is used to highlight open water.¹¹ Other indices, such as the Perpendicular Drought Index (PDI), calculate distances in the red-NIR reflectance space relative to a soil line to quantify soil moisture. Red-edge (RE) based indices like the Normalized Difference Red-Edge Index (NDRE)

$$NDRE = \frac{\rho_{NIR} - \rho_{RE}}{\rho_{NIR} + \rho_{RE}}$$

¹⁰ ROUSE et al. 1974.

¹¹ GAO 1996.

are sensitive to chlorophyll content and may complement NDVI when red-edge data are available.¹²

In this study, the NDWI calculation was used in a relative operational sense rather than as an absolute soil moisture retrieval method. Since the DJI Mavic 3 Multispectral does not include a SWIR band, SWIR-based moisture indices cannot be computed directly. Therefore, the green–NIR formulation of NDWI was applied

$$NDWI = \frac{\rho G - \rho NIR}{\rho G + \rho NIR}$$

where ρG and ρNIR denote the reflectance values measured in the green and near-infrared bands, respectively. This formulation is commonly used to enhance water-related spectral contrast, but in the present case it is interpreted as a relative indicator of surface wetness and post-rainfall changes. Without independent ground reference measurements, reflectance panel calibration or SWIR data, the resulting NDWI values should not be interpreted as absolute soil water content. Instead, they support the identification of spatial anomalies, wet areas and temporal changes when compared with a baseline acquisition. In operational reconnaissance, this relative interpretation is often sufficient, because the main objective is the rapid detection of disturbed surfaces, vehicle tracks and moisture-related changes rather than the quantitative retrieval of biophysical parameters.

Remote-sensing platforms and sensor selection

Ground truth measurements are essential for calibrating and validating airborne data. Handheld spectrometres measure reflectance spectra with fine spectral resolution and are often used to build spectral libraries or calibrate drone imagery. Their advantages include high spectral accuracy and flexible deployment, but they sample only a few points, so they cannot map large areas quickly. In operational reconnaissance, handheld spectrometres may be used to characterise materials in the field (e.g. soils, vegetation, camouflage fabrics) and to train classifiers that will later be applied to airborne imagery.¹³

Satellite remote sensing

Satellites provide consistent, large-scale coverage and free imagery. The Sentinel-2 mission of the European Space Agency (ESA) offers multispectral data at 10–60 m ground resolution with bands in the visible, red-edge and SWIR regions (Figure 1).¹⁴ Their long revisit history supports temporal monitoring, but spatial resolution generally remains

¹² GITELSON–MERZLYAK 1998.

¹³ RAM et al. 2024.

¹⁴ DRUSCH et al. 2012.

too coarse for routine detection of very small disturbances such as individual vehicle tracks when compared with centimetre-level UAV imagery.¹⁵



Figure 1: Sentinel-2 SWIR image of research operational area

Source: picture made by the author

UAVs and drone-based remote sensing

UAVs bridge the gap between ground measurements and satellites by providing high-resolution imagery (centimetre-level ground sampling distance) over user-defined areas. Drones can be flown below clouds and scheduled on demand, making them ideal for reconnaissance tasks. The choice of sensor depends on the mission: multispectral cameras like the DJI M3M, MicaSense RedEdge-MX or Parrot Sequoia capture a few targeted bands, while hyperspectral scanners such as the Headwall Micro-Hyperspec or Cubert ULTRIS provide dozens to hundreds of bands but are heavier and more expensive. In practice, MS cameras mounted on small quadcopters provide a good tradeoff between resolution, weight and cost.¹⁶

Representative multispectral cameras

- MicaSense RedEdge-MX: A widely used UAV multispectral sensor family in environmental and agricultural remote sensing. Published studies show that

¹⁵ DRUSCH et al. 2012.

¹⁶ SOUSA et al. 2022.

RedEdge systems can generate research-grade reflectance products, but they also emphasise that radiometric calibration remains a critical step for reliable quantitative analysis.¹⁷

- Parrot Sequoia (Figure 2): A lightweight four-band multispectral camera with a sunshine sensor, widely used in precision-agriculture and UAS radiometry studies. Published evaluations report useful geometric and radiometric consistency, while also noting that calibration and processing strategy strongly affect the final reflectance products.¹⁸
- DJI Mavic 3 Multispectral (Figure 2): The M3M integrates an RGB camera and a four-band multispectral module (560 ± 16 nm – green, 650 ± 16 nm – red, 730 ± 16 nm – red edge, 860 ± 26 nm – NIR) along with a sunlight sensor and RTK GNSS.¹⁹ A recent field study by Rand and Khan evaluated the M3M for cryospheric research and found that it successfully mapped the spatial distribution of red-snow algae using spectral indices and random-forest classification, assessed snowmelt timing and identified glacial surface features with 68% classification accuracy.²⁰ The authors emphasised the drone's low weight, low cost and ease of use, noting that the principal limitation is the absence of a blue band. The M3M therefore offers an attractive platform for operational reconnaissance and was selected for the case study in this paper.



Figure 2: DJI M3M and Parrot Sequoia multispectral cameras

Source: picture made by the author

¹⁷ DANIELS et al. 2023.

¹⁸ FRANZINI et al. 2019.

¹⁹ DE SOUZA SILVA et al. 2025.

²⁰ RAND-KHAN 2024.

Representative hyperspectral cameras

- Headwall Micro-Hyperspec: a representative push-broom UAV hyperspectral sensor. Such systems provide high spectral fidelity for material mapping, but payload, data rate and scanning requirements make deployment more demanding than with compact multispectral cameras.²¹
- Cubert ULTRIS: a representative snapshot hyperspectral camera. Snapshot systems capture all bands in a single exposure, which simplifies acquisition relative to line scanners, but they typically offer lower spatial sampling and remain costly for routine field deployment.²²
- Specim FX: a representative line-scan VNIR hyperspectral camera widely used in research and industrial settings. Its acquisition requires stable motion and synchronisation, making it better suited to larger airborne platforms than small quadcopters.²³

Platform tradeoffs in operational use

The choice between UAVs, handheld instruments and satellites involves tradeoffs among spatial resolution, spectral resolution, cost and coverage. UAV-mounted multispectral cameras achieve centimetre-level spatial resolution, enabling detection of small objects or footprints, but they measure only a few spectral bands. Hyperspectral sensors provide rich spectral information but are heavier and slower. Satellites cover large areas and include SWIR bands but have coarser spatial resolution and are subject to cloud cover. Handheld spectrometers provide high spectral resolution at point locations. Operational reconnaissance missions often employ UAV-borne multispectral sensors to obtain timely, high-resolution data and combine them with satellite data for broader situational awareness.²⁴

Radiometric and geometric considerations

All remote-sensing systems measure radiance, which must be corrected to reflectance to derive physical indices. Radiometric calibration typically uses a reflectance panel of known albedo and corrects for illumination variability. Geometric correction ensures that the multispectral images align across bands and between acquisition dates. Mismatches can introduce artefacts into indices. In this study, images were orthorectified and mosaicked using software such as WebODM, and the multispectral bands were registered in MATLAB to create a data cube on a smaller scale.²⁵

²¹ SOUSA et al. 2022.

²² SOUSA et al. 2022.

²³ SOUSA et al. 2022.

²⁴ DRUSCH et al. 2012.

²⁵ OLSSON et al. 2021.

Relative index-based assessment without absolute ground reference

The purpose of the index-based analysis in this study is not to derive absolute biophysical parameters, calibrated soil-moisture values or laboratory-grade reflectance spectra. No independent reflectance-panel observations, handheld spectrometre measurements or in-situ soil-moisture measurements were available during the field campaign. Therefore, the analysis is deliberately restricted to normalised spectral indices and relative temporal differences within the same sensor, flight area and processing workflow.

This limitation also reflects a common operational reconnaissance scenario: reference measurements are often unavailable, while rapid information about spatial anomalies, vehicle tracks, wet areas or vegetation disturbance is still required. Under these conditions, normalised indices such as NDVI, NDRE and NDWI are useful because they reduce the influence of absolute brightness differences and allow changes to be interpreted relative to a baseline acquisition. The resulting products should therefore be interpreted as operational change indicators, not as absolute environmental measurements.

Case study and processing workflow

The operational area selected for this case study was a closed military training ground in a temperate environment. Two flights were performed on the same day (10:00 and 13:00 local time) with a rain shower occurring between the flights, providing an opportunity to monitor changes in soil moisture and detect disturbances. A flight plan was created using a georeferenced KMZ file to ensure consistent coverage and overlap. The M3M's RTK module enabled centimetre-level positioning accuracy, reducing the need for ground control points.²⁶

The two acquisitions were consequently treated as a short-term baseline-and-follow-up pair. The morning flight served as the reference state, while the afternoon flight represented the post-rainfall state. Because the objective was rapid reconnaissance rather than absolute calibration, the evaluation focused on whether index differences could reveal spatially coherent changes that are consistent with observable surface disturbance and post-rainfall wetness patterns.

Flight execution and data processing

During each flight, the M3M captured multispectral (green, red, red edge, NIR) and RGB images at approximately 5 cm GSD (Ground Sampling Distance).²⁷ The integrated sunshine sensor recorded ambient irradiance for later radiometric correction.²⁸ After

²⁶ DE SOUZA SILVA et al. 2025.

²⁷ DE SOUZA SILVA et al. 2025.

²⁸ DE SOUZA SILVA et al. 2025.

data was downloaded, each band was separated into different directories. These separated images were imported into WebODM to generate an orthomosaic for each band and RGB, which was further processed with QGIS (Figure 3).²⁹



Figure 3: NIR orthofoto of operational area merged with satellite image

Source: compiled by the author

The multispectral bands were co-registered in MATLAB using cross-correlation and manual tie points to produce a four-band data cube. Vegetation indices and moisture proxies were computed on a per-pixel basis. Because the M3M lacks a SWIR band, the classical NDMI could not be calculated; instead, relative moisture was assessed via changes in red, red-edge and NIR reflectances.³⁰ The difference between the morning and afternoon mosaics provided a proxy for changes induced by rainfall, but meaningful comparison still depended on careful radiometric correction (Figure 4).³¹

Relative change detection workflow

The practical workflow consisted of the following steps:

1. Orthomosaics were generated separately for each spectral band.
2. Multispectral layers were brought onto a common spatial grid.
3. Relative radiometric normalisation was performed on post-rain data.
4. Normalised indices were calculated for each acquisition.
5. Pixel-by-pixel difference maps were produced between the morning and afternoon flights.
6. Spatial patterns in the difference maps were compared with visually identifiable surface features such as tracks, vegetation patches, bare soil and low-lying wet areas.

²⁹ GAAVWASE GBAGIR et al. 2023.

³⁰ TEIXEIRA et al. 2025.

³¹ OLSSON et al. 2021.

This procedure increases the scientific interpretability of the demonstration without claiming absolute validation. The comparison is internally consistent because it uses the same sensor, the same area and a short temporal separation. At the same time, the absence of independent reference measurements means that the output should be reported as relative change evidence. Where numerical reporting is required, the difference maps can be summarised over manually selected image-based regions of interest, for example by reporting mean, median and standard deviation values for disturbed ground, undisturbed vegetation and wet low-lying areas.

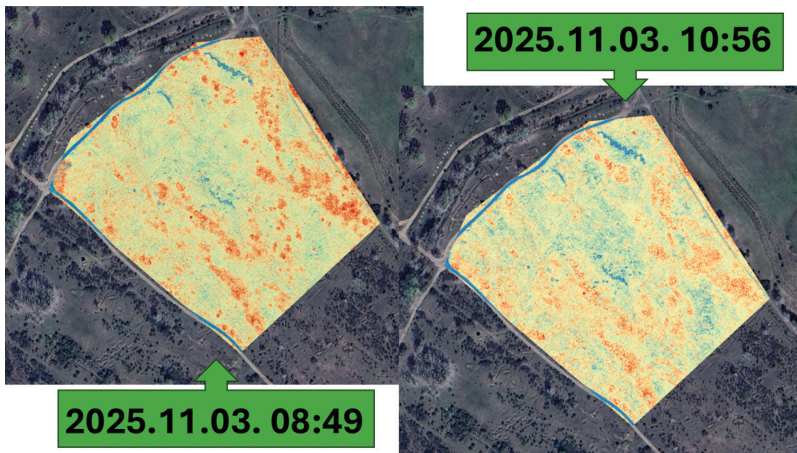


Figure 4: NDWI index of operational area calculated with QGIS before and after rain

Source: compiled by the author

Results and discussion

On the orthomosaic maps, several indices were calculated, analysed and compared between the two measurement sessions. To identify disturbances between flights, pixel-by-pixel subtraction was performed for all the NDVI, NDRE and NDWI maps created during the pre- and post-raining event. Areas where vehicles traversed the ground showed a decrease in NDVI, reflecting crushed vegetation and exposed soil. Conversely, some lower ground areas displayed increased NDWI due to soil darkening and slight increases in red-edge reflectance after the rain. The lack of SWIR limited the ability to quantify absolute soil moisture, but relative changes were evident. These results indicate that multispectral drones can support rapid change detection in operational areas, especially when baseline images are available for comparison.³²

Accordingly, the results are interpreted in comparative terms. A decrease in NDVI over track-like features is considered evidence of relative vegetation disturbance or exposed soil only when the change forms a coherent spatial pattern and differs

³² TEIXEIRA et al. 2025.

from nearby undisturbed vegetation. Similarly, increased NDWI-like response after rainfall is interpreted as a relative wetness-related signal rather than as an absolute soil-moisture estimate. This conservative interpretation directly follows from the lack of independent ground reference data.

To strengthen the quantitative part of the evaluation, the same difference maps can be evaluated with image-based reference regions. Reporting the distribution of ΔNDVI , ΔNDRE and ΔNDWI values for disturbed, undisturbed and wet areas would allow the reader to judge class separability even without external ground-truth measurements. Such statistics are suitable for supporting the operational conclusion because they test whether the observed changes are systematic rather than purely visual.

Spectral data cube analysis

Visualising the four-band data cube in MATLAB's Hyperspectral Viewer allowed exploration of spectral signatures at each pixel (Figure 5). Leafy vegetation showed the expected red absorption and high NIR reflectance.³³ Wet soil in the afternoon flight exhibited lower reflectance across all bands and a reduced red-edge slope.³⁴ Although only four bands were available, principal component analysis separated vegetation, dry soil and wet soil classes, illustrating that even limited spectral data can aid classification (Figure 6). The case study therefore demonstrates the practical value of the M3M for operational reconnaissance tasks.

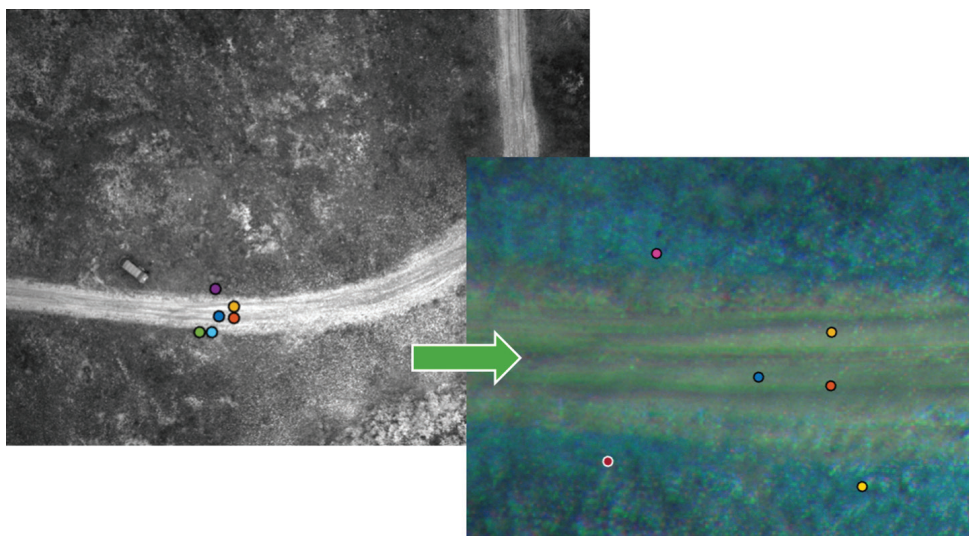


Figure 5: Sample points of spectral measurement on dirt road and vegetation at different points

Source: compiled by the author

³³ GITELSON–MERZLYAK 1998.

³⁴ TEIXEIRA et al. 2025.

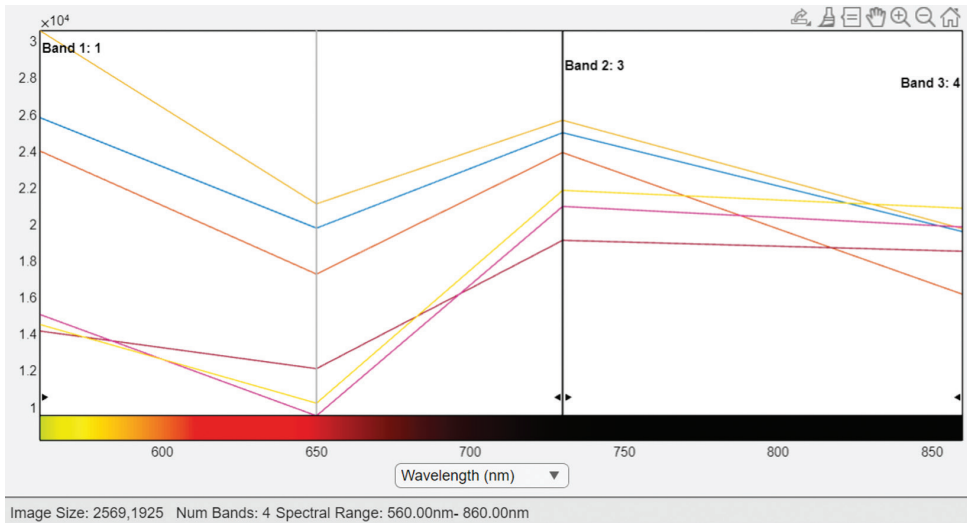


Figure 6: Spectrum of sample points, colour matched

Note: upper three curves connected to dirt road, bottom three curves for vegetation at different areas

Source: compiled by the author

Operational advantages and limitations of the M3M

The DJI Mavic 3 Multispectral provided several advantages for the mission: it is lightweight and easily transported to remote areas, integrates an RTK module for accurate geolocation, and captures both RGB and multispectral data.³⁵ Its bands coincide with those used in common vegetation indices, allowing the derivation of NDVI and NDRE. Its relatively low cost compared with professional systems (e.g. MicaSense RedEdge-MX) makes it accessible to a wider range of users. Nevertheless, there are certain limitations: the absence of a blue band precludes the calculation of some indices like EVI and ARVI. Without SWIR, moisture indices such as NDMI cannot be computed directly; this study used relative red-edge metrics instead. Radiometric calibration is essential to ensure comparability between flights, and changes in illumination (e.g. due to cloud cover) can introduce errors.³⁶ In addition, the limited number of spectral bands and the need for multiple flight lines over larger areas reduce flexibility compared with higher-end modular systems.³⁷

A further limitation of the present case study is the lack of independent absolute reference data. For this reason, statements about moisture and vegetation condition are formulated as relative indicators. The method is therefore most appropriate for rapid change detection, anomaly highlighting and prioritisation of field inspection,

³⁵ RAND-KHAN 2024.

³⁶ DANIELS et al. 2023.

³⁷ RAND-KHAN 2024.

while absolute soil-moisture retrieval or material identification would require reflectance-panel calibration, ground spectrometry or direct field measurements.

Future directions: From indices to artificial intelligence

While indices provide simple, interpretable metrics, emerging applications demand more sophisticated analysis. The next step is to apply convolutional neural networks (CNNs) or other machine learning algorithms to multispectral data to automatically detect changes and classify materials. Deep learning methods can exploit spatial and spectral patterns beyond simple band ratios.³⁸ EdgeAI hardware accelerators could enable on-board processing, reducing data transmission and enabling real-time alerts. However, the limited number of bands in multispectral cameras may restrict performance. Combining multispectral imagery with RGB, thermal or LiDAR data could improve accuracy.³⁹ Additionally, integrating SWIR or hyperspectral sensors would enable absolute soil moisture estimation and more robust material identification.⁴⁰ The inclusion of contextual information such as elevation, slope and historical imagery could further enhance change detection algorithms.

Conclusion

This paper presented a comprehensive overview of multispectral and hyperspectral reconnaissance of operational areas, focusing on drone-based imaging and the DJI Mavic 3 Multispectral. This paper summarises the physics of spectral signatures, reviewed vegetation and moisture indices and explained the tradeoffs among hand-held, drone and satellite platforms. Comparison was performed on commonly used multispectral and hyperspectral cameras and justified the choice of the M3M. A case study showed that the M3M can deliver high-resolution data suitable for vegetation monitoring and change detection, although the absence of SWIR limits absolute moisture estimation. Indices such as NDVI, NDRE and relative red-edge metrics provided useful proxies for vegetation health and soil moisture, and different maps revealed disturbances between flights. Future work should leverage machine learning to extract richer information from multispectral data and explore the integration of additional spectral bands or sensors. The main methodological contribution of the case study is therefore the demonstration of a practical relative index-based workflow for operational change detection under limited-reference field conditions. The results should not be interpreted as absolute soil-moisture or biomass estimates; rather, they show that coherent relative index differences can reveal surface disturbance and post-rainfall wetness patterns when a baseline acquisition is available.

³⁸ RAM et al. 2024.

³⁹ SOUSA et al. 2022.

⁴⁰ TEIXEIRA et al. 2025.

References

- DANIELS, Louis – EECKHOUT, Eline – WIEME, Jana – DEJAEGHER, Yves – AUDENAERT, Kris – MAES, Wouter H. (2023): Identifying the Optimal Radiometric Calibration Method for UAV-Based Multispectral Imaging. *Remote Sensing*, 15(11). Online: <https://doi.org/10.3390/rs15112909>
- DE SOUZA SILVA, Allef et al. (2025): High-resolution Suborbital Remote Sensing for Detecting Injuries Caused by *Saccharicoccus Sacchari* (Cockerell, 1895) (Hemiptera: Pseudococcidae) in Sugarcane. *Frontiers in Agronomy*, 7. Online: <https://doi.org/10.3389/fagro.2025.1630354>
- DRUSCH, Matthias et al. (2012): Sentinel-2: ESA's Optical High-Resolution Mission for GMES Operational Services. *Remote Sensing of Environment*, 120, 25–36. Online: <https://doi.org/10.1016/j.rse.2011.11.026>
- DU, Shanshan – ZHAO, Dianrun – GUAN, LinLin – QI, Mengjia – LIU, Xinjie – LIU, Liangyun (2025): PROSPECT-DP: A Coupled Leaf Optical Properties Model for Improving Leaf Spectra Simulation in the Red-Edge Domain by Excluding the ChlF Effect. *International Journal of Applied Earth Observation and Geoinformation*, 141. Online: <https://doi.org/10.1016/j.jag.2025.104651>
- FRANZINI, Marica – RONCHETTI, Giulia – SONA, Giovanna – CASELLA, Vittorio (2019): Geometric and Radiometric Consistency of Parrot Sequoia Multispectral Imagery for Precision Agriculture Applications. *Applied Sciences*, 9(24). Online: <https://doi.org/10.3390/app9245314>
- GAUVASE GBAGIR, Augustine-Moses – Ek, Kylli – COLPAERT, Alfred (2023): OpenDrone-Map: Multi-Platform Performance Analysis. *Geographies*, 3(3), 446–458. Online: <https://doi.org/10.3390/geographies3030023>
- GAO, Bo-cai (1996): NDWI – A Normalized Difference Water Index for Remote Sensing of Vegetation Liquid Water from Space. *Remote Sensing of Environment*, 58(3), 257–266. Online: [https://doi.org/10.1016/S0034-4257\(96\)00067-3](https://doi.org/10.1016/S0034-4257(96)00067-3)
- GITELSON, Anatoly A. – MERZLYAK, Mark N. (1998): Remote Sensing of Chlorophyll Concentration in Higher Plant Leaves. *Advances in Space Research*, 22(5), 689–692. Online: [https://doi.org/10.1016/S0273-1177\(97\)01133-2](https://doi.org/10.1016/S0273-1177(97)01133-2)
- OLSSON, Per-Ola – VIVEKAR, Ashish – ADLER, Karl – GARCIA MILLAN, Virginia E. – KOC, Alexander – ALAMRANI, Marwan – EKLUNDH, Lars (2021): Radiometric Correction of Multispectral UAS Images: Evaluating the Accuracy of the Parrot Sequoia Camera and Sunshine Sensor. *Remote Sensing*, 13(4). Online: <https://doi.org/10.3390/rs13040577>
- RAM, BILLY G. – ODUOR, PETER – IGATHINATHANE, CANNAYEN – HOWATT, KIRK – SUN, Xin (2024): A Systematic Review of Hyperspectral Imaging in Precision Agriculture: Analysis of its Current State and Future Prospects. *Computers and Electronics in Agriculture*, 222. Online: <https://doi.org/10.1016/j.compag.2024.109037>
- RAND, Colby F. – KHAN, Alia L. (2024): Applicability of Relatively Low-Cost Multispectral Uncrewed Aerial Systems for Surface Characterization of the Cryosphere. *Remote Sensing*, 16(19). Online: <https://doi.org/10.3390/rs16193662>

- ROUSE, J. W. Jr. – HAAS, R. H. – SCHELL, J. A. – DEERING, D. W. (1974): Monitoring Vegetation Systems in the Great Plains with ERTS. In *Third Earth Resources Technology Satellite-1 Symposium*. Volume 1, 309–317.
- SOUSA, Joaquim J. et al. (2022): UAV-Based Hyperspectral Monitoring Using Push-Broom and Snapshot Sensors: A Multisite Assessment for Precision Viticulture Applications. *Sensors*, 22(17). Online: <https://doi.org/10.3390/s22176574>
- TEIXEIRA, Ana C. et al. (2025): A Systematic Review on Soil Moisture Estimation Using Remote Sensing Data for Agricultural Applications. *Science of Remote Sensing*, 12. Online: <https://doi.org/10.1016/j.srs.2025.100328>

István Paráda¹

Cybersecurity Failures in Enterprise MDM Platforms

An Analytical Study of the Ivanti Case

Abstract

Mobile Device Management (MDM) platforms have evolved into critical components of enterprise security architectures, influencing device governance, access control and policy enforcement across corporate networks. As these systems increasingly operate as centralised control planes, they have become attractive targets for adversaries seeking scalable organisational compromise. The study develops a comprehensive analytical framework that integrates public Ivanti security incident data with vulnerability assessment documents and current MDM system design materials. Through qualitative incident analysis and architectural interpretation, the research identifies three primary factors that amplify the systemic impact of MDM compromise: excessive privilege concentration, identity adjacency and update trust dependencies. The findings demonstrate that the security significance of MDM systems extends beyond conventional endpoint management, as these platforms increasingly influence authentication processes, trust relationships and enterprise-wide security decisions. The study argues that MDM platforms should be governed as high-value control-plane assets requiring architectural risk management rather than solely operational security maintenance. The results contribute to the broader understanding of centralised management infrastructures and highlight the need for stronger segmentation, authentication controls, and trust-boundary protection mechanisms within modern enterprise environments.

Keywords: Mobile Device Management, MDM security, Ivanti, enterprise security architecture, identity management

¹ Ludovika University of Public Service, e-mail: paradaistvan@gmail.com

Introduction

The introduction of mobile work solutions and remote work solutions has completely transformed how businesses establish their computer systems. The Mobile Device Management (MDM) system serves as the primary tool organisations use to enforce security regulations, manage device settings and ensure safe access to corporate networks.² MDM systems, which started as tools for inventory control and configuration enforcement, now manage devices and control user access while maintaining security.³ This expanded operational role has simultaneously increased the strategic value of MDM platforms as attack targets. Security breaches that target MDM systems have more harmful consequences because they enable attackers to access all parts of an organisation, whereas breaches targeting endpoint devices affect only specific devices. Control of an MDM system enables attackers to leverage centralised security systems to manipulate authentication processes and install harmful security settings, thereby disable protective controls across the organisation.⁴ The academic security literature fails to recognise MDM platforms as essential security elements because, according to researchers, they are secondary management tools. The recent series of high-impact vulnerabilities disclosed in Ivanti⁵ MDM products challenge this perception. Using the Ivanti incidents as an empirical case study, the paper seeks to extract generalisable insights into the architectural and governance factors that shape MDM security outcomes.

Research questions and methodology

The security risks associated with centralised administrative infrastructure have been studied extensively in the context of directory services and identity management systems. Researchers and practitioners have long recognised that Active Directory⁶ and similar directory services constitute high-value targets whose compromise yields organisation-wide consequences disproportionate to the effort required for initial access.⁷ The concept of "Tier 0" assets – systems whose compromise directly enables control over an entire identity domain – has become a foundational principle in enterprise security architecture and is reflected in Microsoft's widely adopted Enterprise Access Model.⁸

Within the MDM-specific literature, prior work has predominantly addressed device management from operational and compliance perspectives, with limited emphasis

² ENISA 2025.

³ SINGER–FRIEDMAN 2014.

⁴ CIPOLLA et al. 2025.

⁵ Ivanti is an IT software company that provides security, endpoint management and IT service management (ITSM) solutions.

⁶ Active Directory (AD) is a Microsoft-developed directory service that acts as a centralised database for managing users, computers, and security permissions within a Windows domain network.

⁷ ANDERSON 2020.

⁸ Microsoft 2023.

on architectural security implications.⁹ More recent studies emphasise the increasing complexity of identity architectures, particularly in distributed and cloud-based environments, where identity services act as central coordination mechanisms across multiple system layers.¹⁰ In this context, such systems are increasingly understood as components of the enterprise control plane rather than as isolated authentication services. Despite these developments, the existing literature has not systematically conceptualised Mobile Device Management platforms as identity-adjacent control planes. While prior work has addressed MDM technologies and vulnerability management practices, these analyses typically focus on operational implementation rather than on the structural mechanisms through which MDM architectures amplify systemic security risk.

This study builds on these foundations by specifically analysing how MDM architectures amplify security risks through privilege concentration, identity adjacency and update trust dependencies.

In light of the systemic nature of MDM-related risks and to evaluate the broader implications of the Ivanti breaches, this paper addresses three primary questions:

- RQ1: Why do MDM vulnerabilities consistently yield such a disproportionate impact on organisations?
- RQ2: Which specific architectural traits in modern MDM systems are responsible for magnifying these compromises?
- RQ3: What broader governance lessons can be extracted from the Ivanti case?

To address these questions, I use a qualitative methodology centred on structured document analysis. The empirical dataset consists of publicly available vulnerability disclosures, CVE records,¹¹ CISA alerts¹² and forensic incident reports published between 2023 and 2026. Rather than focusing on quantitative exploit frequency, the analysis examines how vulnerabilities interact with architectural trust relationships embedded within MDM platforms. I treat the Ivanti incidents as empirical points – not as isolated bugs, but as evidence of systemic privilege relationships that are inherently embedded in MDM platform designs.¹³ This approach is appropriate, given that the security impact of MDM compromise is driven less by exploit frequency than by systemic privilege relationships embedded in platform design. Vulnerabilities were selected based on the following criteria:

- relevance to MDM control plane components
- confirmed exploitability or documented real-world impact
- availability of technical documentation

⁹ YAMIN-KATT 2019.

¹⁰ KOVACEVIC et al. 2024.

¹¹ CVE Common Vulnerabilities and Exposures Records are standardised, unique identifiers and associated descriptions for publicly known cybersecurity vulnerabilities, designed to facilitate secure, consistent communication and tracking.

¹² CISA alerts are official, timely notifications from the Cybersecurity and Infrastructure Security Agency warning of new, high-impact cyber threats, vulnerabilities, or exploitation campaigns.

¹³ ISO/IEC 2022.

I categorised the vulnerabilities into three primary classes: authentication bypass, remote code execution and privilege escalation. I derived these categories inductively from the dataset and validated against established vulnerability taxonomies.

Fundamentals of Mobile Device Management security

Assessing the security implications of Mobile Device Management (MDM) platforms requires viewing them as centralised control infrastructures positioned between enterprise networks, managed devices and identity systems. An MDM system typically maintains persistent trust relationships with enrolled devices, possesses elevated administrative privileges, and exercises remote control capabilities over device configuration and software state. From a security perspective, this positioning creates a unique convergence of roles. MDM platforms simultaneously operate as policy enforcement points, configuration control systems, and, in many deployments, as intermediaries in authentication and access control workflows.¹⁴ As enterprises increasingly integrate MDM solutions with identity providers, conditional access engines and cloud services, the MDM layer becomes tightly coupled with identity assurance mechanisms. This architectural convergence introduces a critical dependency: device trust is commonly inferred from the device's MDM enrolment status. The MDM platform security breach results in two main consequences that impact both device management capabilities and subsequent security operations. Endpoint malware needs to evade detection on each device, but an MDM compromise enables attackers to use trusted administrative pathways while bypassing most standard endpoint security mechanisms. These characteristics indicate that MDM security cannot be adequately assessed through traditional endpoint threat models. Instead, MDM platforms should be understood as high-privilege control planes whose failure modes resemble those of directory services or identity providers rather than those of managed endpoints.¹⁵

The Ivanti MDM incidents as an empirical case study

The Ivanti Mobile Device Management system provides a representative empirical case for examining the systemic security risks associated with centralised device management infrastructures. Between 2023 and January 2026, multiple high-severity vulnerabilities were disclosed across Ivanti MDM products,¹⁶ which include Endpoint Manager Mobile Sentry¹⁷ and Avalanche.¹⁸ The disclosures encompass multiple types of security vulnerabilities, including authentication bypass, privilege escalation and

¹⁴ HOWELL et al. 2023.

¹⁵ AZODOLMOLKY 2013.

¹⁶ CISA 2024.

¹⁷ Ivanti Endpoint Manager Mobile Sentry (formerly part of MobileIron) is a secure, in-line gateway designed to manage and protect data traffic between mobile devices and corporate systems.

¹⁸ Ivanti Avalanche is a specialised mobile device management (MDM) system designed to manage, secure and update large fleets of rugged mobile computers, scanners and smart devices, frequently in logistics and supply chain environments.

pre-authentication remote code execution (in the following RCE)¹⁹ to demonstrate how MDM systems have developed over time.

Table 1 summarises the publicly disclosed Ivanti MDM vulnerabilities identified during this period, including their CVE identifiers, affected components and assessed severity levels. The dataset demonstrates that all authentication flaws, management interface weaknesses, and update system flaws produce excessive effects because MDM platforms function as central trust systems.

The first table shows that security vulnerabilities that allow remote attacks without authentication have become more common.²⁰ The initial security reports focused on post-authentication vulnerabilities and configuration-dependent weaknesses, whereas current reports indicate that organisations face security threats stemming from pre-authentication attack methods.

Table 1: Chronological overview of high-impact Ivanti MDM vulnerabilities (2023–2026)

Year	CVE ID(s)	Product / component	Type of vulnerability	CVSS ²¹
2023	CVE-2023-39335, CVE-2023-3933722	Ivanti Endpoint Manager Mobile (EPMM)	Enrolment impersonation/access misuse	CVSS 8.5 CVSS 6.8
2023	CVE-2023-3803523	Ivanti sentry	API24 authentication bypass	CVSS 9.8
2024	CVE-2024-2202625	EPMM	Local privilege escalation via crafted package	CVSS 6.7
2024	CVE-2023-46806, CVE-2023-4680726	EPMM	SQL injection ²⁷	CVSS 6.7
2024	CVE-2024-24996, CVE-2024-2920428	Ivanti Avalanche MDM	Heap overflow → possible RCE	CVSS 9.8
2025	CVE-2025-4427, CVE-2025-442829	EPMM	Auth bypass / RCE chain	CVSS 7.5 CVSS 8.8
2025	CVE-2025-2246230	Ivanti neurons for ITSM	Authentication bypass	CVSS 9.8
2026	CVE-2026-1281, CVE-2026-134031	EPMM	Pre-auth remote code execution (zero day)	CVSS 9.8

Source: compiled by the author based on NVD, CISA KEV Catalog and CVE Details (2023–2026)

¹⁹ Remote Code Execution (RCE) is a critical cybersecurity vulnerability that allows attackers to remotely run malicious code, commands, or software on a target computer or network, often resulting in a full system takeover. CVE Details 2026.

²¹ CVSS stands for Common Vulnerability Scoring System. It is an open industry standard used to assess and rate the severity of software and hardware security vulnerabilities, assigning them a numerical score from 0.0 to 10.0 based on factors like attack complexity, impact and exploitability.

²² Ivanti CVE-2023-39335, CVE-2023-39337 2026.

²³ NARANG 2023.

²⁴ An API (Application Programming Interface) is a set of rules and protocols that allow different software applications to communicate, share data and securely exchange functionality.

²⁵ NIST 2024.

²⁶ Computer Incident Response Center Luxembourg 2023.

²⁷ SQL injection (SQLi) is a security vulnerability in which attackers inject malicious SQL code into input fields to manipulate backend databases.

²⁸ ANDERSON 2025.

²⁹ SMITH 2025.

³⁰ Center for Cybersecurity Belgium 2025.

³¹ MOORE 2025.

The MDM platform has become more complex to operate, while its value as a target for attackers has increased due to its ability to deliver extensive attack paths.³² Importantly, the Ivanti incidents should not be interpreted solely as vendor-specific implementation failures. Instead, they reflect broader structural characteristics inherent in centralised enterprise mobility and endpoint management architectures. Similar security weaknesses exist across different enterprise mobile management systems, including both MDM and unified endpoint management platforms.³³ Ivanti, therefore, serves as a representative empirical example through which broader architectural characteristics of modern MDM platforms can be examined.

The empirical observations presented in this section establishes the foundation for the analytical findings discussed in the subsequent sections. By situating individual vulnerabilities within a temporal and architectural context, the analysis moves beyond incident reporting toward a systematic understanding of why MDM compromises produce organisation-wide security consequences.

Systematic analysis of the 2026 EPMM pre-authentication RCE incident (CVE-2026-1281) case

The practical validity of the proposed MDM threat model can be demonstrated through analysing the 2026 Ivanti Endpoint Manager Mobile (EPMM) zero day vulnerability chain (CVE-2026-1281). The analysed vulnerabilities were disclosed contemporaneously with the preparation of this manuscript. Accordingly, the study is based on publicly available information and should be interpreted as a contemporaneous analytical case study rather than a fully retrospective forensic analysis – the technical failure cascaded system-wide, affecting all services because it originated in the core MDM management plane. Public threat intelligence reports indicate that CVE-2026-1281 was actively exploited in combination with a second vulnerability (CVE-2026-1340), which enabled unauthenticated adversaries to execute arbitrary code on EPMM servers without the need of valid credentials or user interaction. The compromise provided attackers with administrative control over the centralised MDM infrastructure, thereby exposing enterprise-wide mobile device management functions to systemic manipulation. According to incident investigations published by the Palo Alto Networks Unit 42,³⁴ exploitation activities included the establishment of reverse shells, deployment of web shells, reconnaissance operations, and the downloading of additional malware payloads.

The attack sequence originated at the internet-facing management interface, which served as the most vulnerable trust boundary in the system architecture. By exploiting a pre-authentication remote code execution vulnerability, adversaries bypassed perimeter authentication mechanisms and obtained control over the management server. This effectively transformed the MDM platform from a defensive

³² SYYNIMAA 2022.

³³ CELIK 2025.

³⁴ Palo Alto Networks Unit 42 is a renowned global team of threat researchers, incident responders, and security consultants that provides proactive cyber risk management and emergency incident response.

management component into an entry point for the broader enterprise network. Following the initial breach, the attackers advanced to the second stage of the attack model by gaining administrative control of the MDM management server. At this stage, the adversary transitioned from an external attacker to an internally trusted administrative actor, inheriting the extensive privileges of a centralised MDM control plane. In the third phase of the attack chain, the adversaries used authorised MDM push-management functions to spread harmful configuration profiles across all devices in the enrolled device fleet. The enrolled devices executed the commands automatically because they had already established a trust connection with the management server. The compromised endpoints subsequently functioned as trusted proxies within the enterprise environment. The attackers used their ability to control device status, their access to valid session tokens, and their knowledge of enterprise network protocols to navigate the organisation's internal identity systems, including the VPN,³⁵ gateways, directory services and authentication systems.³⁶

The threat intelligence telemetry indicates that the exploitation campaign affected organisations across various sectors, including state and local government, healthcare, manufacturing, professional services and high-technology industries in the United States, Germany, Australia and Canada. The U.S. CISA³⁷ included CVE-2026-1281 in its KEV.³⁸ The catalogue was updated because attackers were currently exploiting the vulnerability, which had become a major security risk. The scale of potential exposure was also significant. Security telemetry identified more than 4,400 internet-accessible EPMM instances worldwide, demonstrating the platform's extensive deployment footprint and the large attack surface available to threat actors.

This case demonstrates that the organisational impact of MDM compromise is disproportionately high, not merely because of the underlying software vulnerability, but also because of the concentrated privilege structure and implicit trust relationships embedded in MDM platform architectures.³⁹ While the Ivanti case provides the empirical foundation for this analysis, the structural implications identified here apply broadly to modern enterprise MDM deployments and centralised endpoint management systems.

Vulnerability pattern analysis and threat modelling of MDM platforms

For analytical clarity, I introduce three core concepts that serve as the foundation for interpreting the security implications of Mobile Device Management (MDM) platforms. These concepts – privilege concentration, identity adjacency and update trust dependency – are not presented as entirely novel theoretical constructs, but

³⁵ A Virtual Private Network (VPN) is a service that creates a secure, encrypted "tunnel" between your device (computer, phone) and the internet.

³⁶ HOGAN-BURNEY – TSYGANSKIY 2025.

³⁷ Cybersecurity and Infrastructure Security Agency.

³⁸ Known Exploited Vulnerabilities.

³⁹ ROSE et al. 2020.

rather as an integrated framework tailored to the specific architectural characteristics of MDM systems.⁴⁰

Privilege concentration refers to the extent to which administrative authority and security-relevant control functions are centralised within a single system component. In the context of MDM platforms, this manifests as the aggregation of device management, policy enforcement, and configuration control within a unified management plane. Such concentration creates a structural condition in which the compromise of a single system element yields disproportionately high impact across the managed environment.

Identity adjacency describes the extent to which a system influences authentication processes or access control decisions without being formally classified as an identity provider. MDM systems increasingly operate in this intermediate space, as device compliance status, enrolment state, and configuration integrity are frequently used as implicit inputs into access control mechanisms. As a result, these systems acquire indirect authority over identity-related decisions, thereby expanding their security relevance beyond traditional device management roles.⁴¹

Update trust dependency captures the reliance of managed endpoints on a centralised authority for the delivery and execution of configuration changes, software updates and policy enforcement actions. This dependency is typically implemented through implicit trust relationships, where endpoints accept and execute instructions from the management server without independent validation. While this model enables efficient large-scale administration, it also creates a high-risk propagation channel in the event of control-plane compromise.⁴²

Using a consistent framework for interpretation helped me to make sense of the entire dataset. This structured approach enabled me to move from simply documenting incidents to generating more meaningful insights and analysis. During my analysis, I adopted an active stance, analysing vulnerabilities along with their impact on the MDM architecture. I found specific vulnerabilities, which included possible administrative takeover and granting unlimited control of the MDM system, as evidence of privilege centralisation. Moreover, I analysed vulnerabilities associated with authentication, device compliance validation, and access control using the notion of identity adjacency. Also, I classified vulnerabilities allowing unauthorised access to system configurations and updates as a sign of user trust in the system's update mechanisms. Adopting an interpretive model was critical in allowing me to analyse the whole dataset. The interpretive approach provided me with the opportunity to transition from mere documentation to deeper analysis.

While Table 1 presents a chronological overview of disclosed Ivanti vulnerabilities, the dataset also reveals several recurring structural patterns that are highly relevant for understanding systemic risk in Mobile Device Management architectures. Rather than representing isolated implementation defects, the vulnerabilities cluster around a limited number of architectural trust boundaries within MDM systems.⁴³

⁴⁰ TUHIN 2025.

⁴¹ ALPÁR et al. 2011.

⁴² CAPPOS et al. 2008.

⁴³ SALTZER-SCHROEDER 1975.

A qualitative classification of the vulnerabilities summarised in Table 1 identifies three dominant categories, as illustrated in Figure 1.

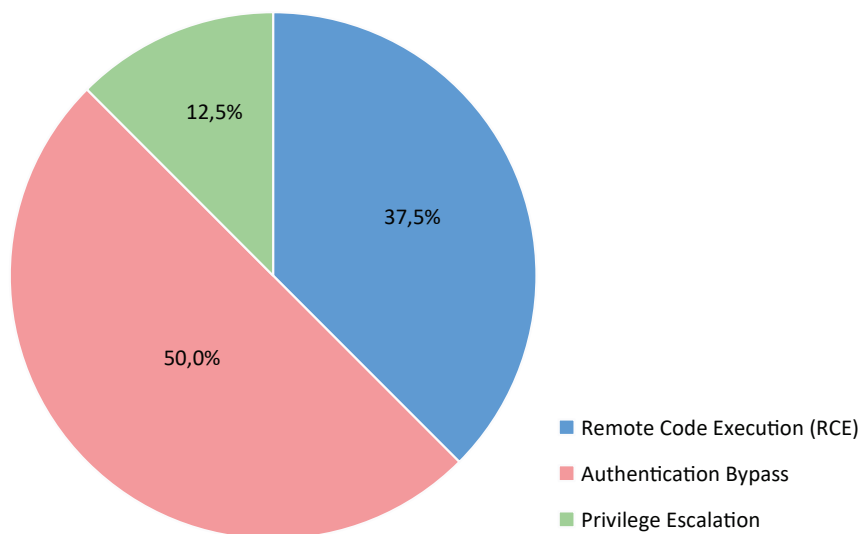


Figure 1: Distribution of incidents by vulnerability types in Ivanti MDM incidents (2023–2026)

Source: compiled by the author based on vulnerability data collected from MDM–Ivanti (2023–2026)

Authentication bypass vulnerabilities are among the most critical categories, as they allow attackers to circumvent the primary security boundary protecting administrative management functions. When such flaws occur in externally accessible interfaces, attackers may obtain control over the MDM platform without prior credentials. The process of exploiting privilege escalation vulnerabilities begins when attackers use their restricted access to elevate their privileges to full administrative rights. The RCE vulnerabilities in MDM systems pose major security risks because management servers handle privileged access while maintaining secure connections to all connected devices. Attackers who exploit these vulnerabilities gain complete access to the management server, including the ability to control device settings and network security protocols.⁴⁴

The distribution of vulnerabilities across MDM components highlights the concentration of risk within a small number of architectural interfaces.⁴⁵ The most frequently affected elements include:

- API management
- enrolment and device registration services
- administrative web interfaces
- update and package deployment mechanisms

⁴⁴ ELYASSA 2024.

⁴⁵ ANDERSON 2020.

These components represent the primary trust boundaries between external entities and the MDM control plane. Because many of these interfaces must remain accessible to devices across enterprise networks or the public internet, they inherently expand the platform's attack surface. An important trend in the dataset is the growing prevalence of pre-authentication vulnerabilities that enable attackers to exploit management interfaces without valid credentials. This shift significantly lowers the barrier to compromise and transforms the MDM platform into a viable initial access target rather than merely a post-compromise privilege escalation opportunity.

The architectural role of MDM platforms creates greater security risks because their system design enables common software vulnerabilities to have more severe effects than they do in standard enterprise environments.⁴⁶ While standard vulnerabilities usually affect a limited number of services or specific hosts, flaws in MDM control planes can have a cascading effect across the entire organisational infrastructure. The amplification effect affects all managed devices that experience operational failure due to a specific security vulnerability.⁴⁷ The system vulnerabilities turn off all authentication mechanisms that determine user access to protected resources in accordance with established security protocols. The adversary obtains access to software distribution pathways and compliance monitoring systems because the organisation's security system for system protection is compromised. Consequently, even moderately complex vulnerabilities can produce disproportionate organisational consequences when they occur within centralised device management systems.⁴⁸

Conclusion

The Ivanti incident research shows that organisations now protect their systems through centralised device control together with zero-trust security systems. Organisations now use MDM platforms as security systems to protect their devices, as they authenticate user identities through these platforms. The security standards that protect organisations through device management, along with identity management, now fail because attackers who breach MDM systems can gain complete control over device security and user authentication.⁴⁹ Through this analytical synthesis, I provide direct answers to the core research questions of this study:

- RQ1: Why do MDM vulnerabilities consistently yield such a disproportionate impact on organisations? The "Force Multiplier" effect in MDM systems results in all systems experiencing their most severe impact. Because the MDM server maintains an automated, pre-established trust relationship with the entire device fleet, a single compromise at the control plane level allows the

⁴⁶ BÁLINT-PETŐ 2025.

⁴⁷ ENISA Cyber Threats 2026.

⁴⁸ HAYES et al. 2020.

⁴⁹ WINDLEY 2005.

instantaneous propagation of malicious configurations without requiring the exploitation of individual devices.

- RQ2: Which specific architectural traits in modern MDM systems are responsible for magnifying these compromises? The magnification is primarily driven by privilege concentration and identity adjacency. Modern MDM systems are no longer peripheral tools; they are deeply integrated into the identity assurance chain. Using device enrolment status as a trust indicator creates a security vulnerability for the MDM platform, as it becomes the only security assessment method.
- RQ3: What broader governance lessons can be extracted from the Ivanti case? The Ivanti case demonstrates that MDM security must shift from a “patch management” focus to an architectural trust model. Governance must treat MDM platforms as Tier 0 assets⁵⁰ – equivalent to Active Directory or Identity Providers – consistent with findings in centralised command and control architectures where trusted information flows determine decision-making integrity⁵¹ requiring strict network segmentation, multi-factor authentication for all administrative interfaces, and the assumption that the management plane itself is a high-value target for pre-authentication attacks.
- The primary scientific contribution of this study lies in the analytical reframing of MDM platforms as identity-adjacent control planes. This research demonstrates that modern MDM systems operate across device, identity and policy layers concurrently, creating a concentration of privilege that traditional endpoint threat models fail to predict. By bridging the conceptual gap between identity-centric security and endpoint management, this study argues for applying high-assurance frameworks to all centralised management architectures.

The security of MDM systems will become increasingly important for organisations as they extend their mobile and remote work capabilities, according to the conclusion of this study. The Ivanti case study demonstrates that structural properties, including the exploitation of secure management pathways, determine the depth of security breaches in systems, not just software flaws. Future security approaches must adapt to view MDM platforms as essential, high-risk elements of the identity framework, and researchers need to explore multi-vendor resilience to develop systemic insights across different deployment models, particularly in the context of increasingly integrated, multi-domain system architectures.⁵²

⁵⁰ Tier 0 assets are the most critical IT systems, identities and components in an organisation – often called the “crown jewels” – that provide direct administrative control over Active Directory (AD) or cloud identity environments.

⁵¹ TÓTH 2025.

⁵² TÓTH-FARKAS 2023.

References

- ALPÁR, Gergely – HOEPMAN, Jaap-Henk – SILJEE, Johanneke (2011): The Identity Crisis: Security, Privacy and Usability Issues in Identity Management. *arXiv*. Online: <https://arxiv.org/abs/1101.0427>
- ANDERSON, Ross (2020): *Security Engineering. A Guide to Building Dependable Distributed Systems*. Cambridge: Cambridge University Press. Online: <https://doi.org/10.1002/9781119644682>
- ANDERSON, Elliot (2025): CVE-2024-24996, CVE-2024-29204 Ivanti Avalanche Buffer Overflow Vulnerabilities. Online: www.lumifycyber.com/threat-library/cve-2024-24996-cve-2024-29204-ivanti-avalanche-buffer-overflow-vulnerabilities/
- AZODOLMOLKY, Siamak (2013): *Software Defined Networking with OpenFlow*. Online: https://speetis.fei.tuke.sk/KomunikacnaTechnika1/prednasky/7_11_2016/kniha_sietovanie.pdf
- BÁLINT, Ferenc – PETŐ, Richárd (2025): Sustainable and Safe Cities Through Computer Applications 2025. *Interdisciplinary Description of Complex Systems*, 23(3), 207–216. Online: <https://hrcak.srce.hr/file/481559>
- CAPPOS, Justin – SAMUEL, Justin – BAKER, Scott M. – HARTMAN, John H. (2008): *A Look in the Mirror: Attacks on Package Managers*. CCS '08: Proceedings of the 15th ACM Conference on Computer and Communications Security. New York: Association for Computing Machinery, 565–574. Online: <https://doi.org/10.1145/1455770.1455841>
- CELIK, Osman (2025): *Attack Surface Management Report*. Online: www.wisdominterface.com/wp-content/uploads/2025/07/Report2025KuppingerColeLeadershipCompassAttackSurfaceManagement-1.pdf
- Center for Cybersecurity Belgium (2025): *Warning: CVE-2025-22462, Authentication Bypass Vulnerability in Ivanti Neurons for ITSM Leading to Remote Unauthenticated Administrative Access, Patch Immediately!* Online: <https://ccb.belgium.be/advisories/warning-cve-2025-22462-authentication-bypass-vulnerability-ivanti-neurons-itsm-leading>
- CIPOLLA, Tom – AL DANA, Lina – KUMAR, Sunil (2025): *Market Guide for Endpoint Management Tools*. Gartner Research. Online: www.gartner.com/en/documents/4018596
- CISA (2024): *Known Exploited Vulnerabilities Catalog. Ivanti*. Online: www.cisa.gov/known-exploited-vulnerabilities-catalog
- Computer Incident Response Center Luxembourg (2023): CVE-2023-46806 (GCVE-0-2023-46806). Online: <https://cvepremium.circl.lu/vuln/CVE-2023-46806>
- CVE Details (2026): *Ivanti: Vulnerability Statistics*. Online: www.cvedetails.com/vendor/17398/ivanti.html
- ELYASSA, Mehdi (2024): *Red Teaming Like an APT, a MobileIron 0-day Exploit Chain*. Online: www.sstic.org/media/SSTIC2024/SSTIC-actes/simulation_dun_apt_en_red_team__recherche_et_dcouv/SSTIC2024-Article-simulation_dun_apt_en_red_team__recherche_et_dcouverte_de_0-day_sur_mobileiron-elyassa.pdf

- ENISA (2025): *ENISA Threat Landscape 2025*. European Union Agency for Cybersecurity. Online: www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf
- ENISA Cyber Threats (2026): *Single Points of Failure in Critical ICT Systems*. Online: www.enisa.europa.eu/topics/cyber-threats
- HAYES, Darren – CAPPA, Francesco – LE-KHAC, Nhien An (2020): An Effective Approach to Mobile Device Management. *Digital Business*, 1(1). Online: <https://doi.org/10.1016/j.digbus.2020.100001>
- HOGAN-BURNEY, Amy – TSYGANSKIY, Igor (2025): *Microsoft Digital Defense Report 2025*. Online: www.microsoft.com/security/blog
- HOWELL, Gema et al. (2023): *NIST SP 800-124 Rev.2. Guidelines for Managing the Security of Mobile Devices in the Enterprise*. Online: <https://doi.org/10.6028/NIST.SP.800-124r2>
- ISO/IEC (2022): *ISO/IEC 27001:2022. Risk-based Security Methodology*. Online: www.iso.org/standard/27001
- KOVACEVIC, Ivana – RANKOVIC, TAMARA – STOJKOV, MILAN – SIMIC, Milos (2024): Token-Based Identity Management in Distributed Cloud Systems. *arXiv*. Online: <https://arxiv.org/abs/2410.21865>
- Microsoft (2023): *Enterprise Access Model. Microsoft Security Documentation 2023*. Online: <https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-access-model>
- MOORE, Justin (2025): *Critical Vulnerabilities in Ivanti EPMM Exploited*. Online: <https://unit42.paloaltonetworks.com/ivanti-cve-2026-1281-cve-2026-1340/>
- NARANG, Satnam (2023): *CVE-2023-38035: Ivanti Sentry API Authentication Bypass Zero-Day Exploited in the Wild*. Online: <https://fr.tenable.com/blog/cve-2023-38035-ivanti-sentry-api-authentication-bypass-zero-day-exploited-in-the-wild>
- NIST (2024): *CVE-2024-22026 Detail*. National Vulnerability Database. Online: <https://nvd.nist.gov/vuln/detail/CVE-2024-22026>
- ROSE, Scott – BORCHERT, Oliver – MITCHELL, Stu – CONNELLY, Sean (2020): *Zero Trust Architecture. NIST SP 800-207*. Online: <https://doi.org/10.6028/NIST.SP.800-207>
- SALTZER, Jerome H. – SCHROEDER, Michael D. (1975): The Protection of Information in Computer Systems. *Proceedings of the IEEE*, 63(9), 1278–1308. Online: <https://doi.org/10.1109/PROC.1975.9939>
- SINGER, Peter W. – FRIEDMAN, Allan (2014): *Cybersecurity and Cyberwar. What Everyone Needs to Know*. Oxford: Oxford University Press. Online: <https://doi.org/10.1093/wentk/9780199918096.001.0001>
- SMITH, Ben (2025): *CVE-2025-4427, CVE-2025-4428: Ivanti Endpoint Manager Mobile (EPMM) Remote Code Execution*. Online: www.tenable.com/blog/cve-2025-4427-cve-2025-4428-ivanti-endpoint-manager-mobile-epmm-remote-code-execution
- SYNIMAA, Nestori (2022): *Exploring Azure Active Directory Attack Surface: Enumerating Authentication Methods with Open-Source Intelligence Tools*. Proceedings of the 24th International Conference on Enterprise Information Systems, Volume 2, ICEIS, 142–147. Online: <https://doi.org/10.5220/0011077100003179>

- TÓTH, András (2025): Enhancing Situational Awareness and Decision-Making: The Impact of Advanced ISR Solutions on Command and Control Systems. *Hadmérnök*, 20(2), 143–160. Online: <https://doi.org/10.32567/hm.2025.2.9>
- TÓTH, András – FARKAS, Tibor (2023): Opportunities and Directions for the Evolution of Command and Control Systems in the Context of Multi-domain Operations. *Vojenské Reflexie*, 18(3), 59–73. Online: <https://doi.org/10.52651/vr.a.2023.3.59-73>
- WINDLEY, Phillip (2005): *Digital Identity*. Sebastopol, CA: O'Reilly. Online: <https://dl.acm.org/doi/abs/10.5555/1098715>
- YAMIN, Muhammad – KATT, Basel (2019): *Mobile Device Management (MDM): Technologies, Issues, and Challenges*. ICCSP '19: Proceedings of the 3rd International Conference on Cryptography, Security and Privacy. New York: Association for Computing Machinery, 143–147. Online: <https://doi.org/10.1145/3309074.3309103>

Tamás Stadler¹

Military-related Heavy Metal Pollution in Soil

A Scientific Review

Abstract

It is well known that during armed conflicts, as well as military trainings, large amounts of pollutants can be released into nature. Of the eleven environmentally toxic elements, Pb, Zn and Cu are often present in high concentrations in the soils of military sites, along with Cd and As. According to newer data from the Russo–Ukrainian War, the inorganic contaminants (mostly toxic elements) show a concentric distribution in the affected areas, caused by artillery activity; however, the spatial distribution of Pb in the training sites is more dispersed.

Risk assessment, then physicochemical and bioremediation methods can be used for cleaning up the polluted areas from the contaminants after the closure of the armed conflicts or training; however, the complexity, caused by the contaminant mixtures and the great variability of soil components, of the pollution affects the success of the procedure heavily.

Keywords: military sites, inorganic contaminants, physicochemical and bioremediation methods, armed conflict

Introduction

Nowadays, the importance of environmental protection – despite several new economic and political factors – is still high. Since the outbreak of the Russo–Ukrainian War and the freshly renewed conflicts in the Middle East, the topic of military-related environmental pollution has caught the interest of the daily news consumers. However, from

¹ PhD student, Ludovika University of Public Service, Doctoral School of Military Engineering, e-mail: stadlert@nszkk.gov.hu

a scientific point of view, it is a challenging field: behind the destruction of different explosives, which clearly produce significant damage in the geo- and biospheres, the released chemical agents can also play a significant role in the contamination of the natural environment.

There are several chemical components – applied mostly in the ammunition – that are dangerous for the environment. Basically, these agents can be divided into two main groups: organic and inorganic pollutants. In this article, I would like to focus on a subgroup of inorganic components, the so-called *potentially toxic elements* (PTEs), which were also known as *heavy metals*. The usage of those elements is frequent in the ordnance that leads to their higher concentrations in active and former military-affected areas.²

The potentially toxic elements and their occurrence in military-related areas

For several decades and centuries, the toxic effects of some chemical elements have been well known. Nowadays, eleven elements are defined as environmentally toxic, namely: arsenic (As), cadmium (Cd), chromium (Cr), cobalt (Co), copper (Cu), mercury (Hg), lead (Pb), manganese (Mn), nickel (Ni), selenium (Se) and zinc (Zn). However, there are more elements, such as antimony (Sb), barium (Ba), gold (Au), molybdenum (Mo), silver (Ag), thallium (Tl), tin (Sn), tungsten (W), uranium (U) and vanadium (V) that also have a negative effect on the environment.³ Most of these elements are found in ordnance, particularly in ammunition.

The most well-known element from the list above is lead. However, lead can be found in natural geological media; anthropogenic processes are important sources of pollution.⁴ Lead is a key component of ammunition (usually the bullet itself, made from it, but also found in shell fragments), which explains its common occurrence at firing ranges and in conflict zones. The concentration of lead often exceeds the permitted limits in the examined areas.⁵

Nickel, copper and zinc are the second most common metals, as they are the main components of bullet shells and can also be found in missiles, projectile fragments and coatings. These elements can be found in both residual and mobile forms in the polluted areas.⁶

Cadmium and chromium are both highly toxic elements that can be present in explosives and other military debris.⁷

However, their occurrence is less common; mercury, arsenic, antimony, cobalt and vanadium can be found in specific ammunition. According to Anastasiia O. Splodytel, mercury and arsenic are highly hazardous contaminants. While mercury can be linked to the detonation of fuses and some specific explosives, arsenic is a common

² DENTON et al. 2016; FAYIGA–SAHA 2016; TEŠAN TOMIĆ et al. 2018; SKALNY et al. 2021.

³ ALLOWAY 2013.

⁴ KORRE et al. 2002; FÜGEDI 2004; HOOKER–NATHANAIL 2006.

⁵ ALTAHAAN–DOBSLAW 2024; YASHCHENKO et al. 2025.

⁶ MOLISZEWSKA et al. 2025.

⁷ TEŠAN TOMIĆ et al. 2018; SPODYTEL 2020; PETRUSHKA–PETRUSHKA 2025.

byproduct of pyrotechnic mixtures. Cobalt and vanadium are less dangerous elements than the aforementioned ones, and their presence can be a consequence of heavy vehicle traffic.⁸

Besides the most abundant pollutants, we have to mention some emerging elements, too. Silver, bismuth, indium, tin and thallium. These contaminants are usually concentrated in industrial areas, for example smelter sites. Although their occurrence is not closely related to military activity, these metals can be released into the environment during military manufacturing processes, such as ammunition and vehicle production.⁹

Spatial distribution of potentially toxic elements in the soils of military areas

According to Nóra Szűcs-Vásárhelyi, the sources of environmental pollution can be grouped as point sources or diffuse sources.¹⁰

The military-related environmental pollution can be linked to different activities, from productive processes to training and real conflicts. Upon this approach, military-related activities should be differentiated before the application of the aforementioned source-grouping:

1. Military production plants and storage facilities: usually present at a discrete geographical place. These kinds of sources can be defined as point sources.
2. Military training sites: most commonly shooting ranges, where there are several point-like sources for the firing positions and bullet catchers. These sites are in the middle of the point source – diffuse source axis.
3. Conflict zones (e.g. Ukraine) can be expanded to several hundred square kilometres. However, there are discrete sites (e.g. damaged ammunition storage facilities) where the local concentration of pollutants is higher than in its surroundings, the whole conflict zone can be interpreted as a diffuse source.

The heavy metal contamination can be linked mostly to the impact of the artillery ammunition as well as the usage of explosives. As a result of these events, smaller fragments of ammunition reach the topsoil, from which, due to the large specific surface area of the fragments, the metals can be released into the environment.

However, the distribution of the aforementioned ammunition fragments follows the shape of the affected area. Based on the recent examinations of Liudmyla Yashchenko and her colleagues, the areas affected by the Russo–Ukrainian conflict exhibit a spherical structure in terms of contaminants.

The inner part – the direct impact/bombardment zone – is the explosion crater itself, where the highest concentrations of heavy metals are measured. In the Ukrainian example, lead, nickel, copper and manganese show significant pollution (for example, lead reached 3.9 times the maximum permissible concentration). The soil structure

⁸ SPLYDYTEL 2020.

⁹ MEES et al. 2013; LI et al. 2016.

¹⁰ SZÜCS-VÁSÁRHELYI 2019.

(soil particle size distribution), pH and humus content are also affected by the impact. The diameter of the impact crater varies between 20–100 metres.

The outer part is known as the contamination zone. This area surrounds the impact crater but is not directly affected by the exploded ammunition. The outer frontier of the zone can reach 500 metres from the centre of the impact zone. The contamination zone usually refers to the secondary accumulation area of the PTE contaminants, which may originate from small ammunition fragments and fine-grained dust released during the explosion. According to the research, the soil of this area is enriched in nickel and cadmium.¹¹

In summary, the spatial distribution of potentially toxic elements follows the geometry of the impact zone, where the most relevant contamination is characteristic of the centre, but lower concentrations can be measured in its surroundings.

Geochemical accumulation, transport and bioavailability of heavy metals

Independently from their source, heavy metals can be enriched in soils. As the PTEs are usually cationic, they can be adsorbed onto mineral surfaces of specific mineral species as well as onto soil organic matter (SOM).

Clay minerals are key components of soils. Most clay minerals are sheet silicates (phyllosilicates) that have the ability for cation exchanges in their crystalline structure. This cation exchange leads to a charge imbalance, which can be equalised via the adsorption of different (so-called *charge balancer*) cations, particularly heavy metals.

As lead, copper and zinc are the most abundant among the potentially toxic elements, their adsorption properties are well examined. Clay-rich soils, especially those whose mineralogical assemblage contains swelling clays (e.g. smectites, vermiculite), can adsorb large amounts of metal cations.¹² Besides the phyllosilicate mineral phases, iron and manganese oxides/-hydroxides also act as heavy metal adsorbents.¹³

The efficiency of adsorption depends on the pH value of the examined soils: acidic conditions usually favour lower adsorption rates in soils, which makes heavy metals more mobile. For lead, the highest experimental retention rate was observed at pH 7.¹⁴ But usually, the alkaline conditions facilitate the adsorption of heavy metals.¹⁵

Based on the above, the soil mineralogy and chemical analysis play an important role during the examination of each polluted area. Adsorption to mineral surfaces and soil organic matter, or rock layers/bodies with poor hydraulic conductivity (e.g. clays, unfractured igneous and metamorphic rocks) generally obstructs the spreading of contaminants in geological media. However, there are several ways that facilitate the extension of the pollution. Water-soluble species, like arsenic, cadmium or lead,

¹¹ YASHCHENKO et al. 2025.

¹² NÉMETH et al. 2011.

¹³ SINGH et al. 1984.

¹⁴ CHAMORRO – SÁNCHEZ-ÁNDICA 2024.

¹⁵ SIPOS 2009.

can be released easily in wet conditions and then reach deeper geological areas. Heavy rainfall – seasonal, such as the monsoon, or associated with severe weather events – supports the leaching and downward migration of pollutants.¹⁶ Ongoing climate change causes more frequent and severe storms, leading to more efficient leaching and migration of contaminants in geological media.¹⁷

When pollutants reach groundwater, spreading speed increases and a larger volume of the geological media is contaminated, including both solid and liquid phases. The worst scenarios are connected to karstic systems, where a large amount of water is present in continuous water bodies.¹⁸ Karstic systems are frequently used for irrigation and as a source of drinking water, making them one of the most vulnerable geological media.

Besides the contamination of the geo- and hydrosphere, we must not forget the atmosphere too. Due to the explosive nature of military-related sources, heavy metal-containing dust particles remain in the air for extended periods. Atmospheric currents disperse contaminants over a larger area, where heavy metals can fall onto the soil surface.¹⁹

As for contamination, exposure pathways should be determined as well. Exposure pathways are practical routes from the sources to the consumers. Bioavailable contaminants enter the food chain through plant uptake and, via a series of herbivores and carnivores, reach the final consumer: an animal or a human. In some cases, the final consumer is exposed to the contaminant directly through inhalation or ingestion. The former is common with fine-grained materials or dust, while the latter is common in polluted drinking water.

With the knowledge of the exposure pathway, the risk can be calculated. The main problem with potentially toxic elements is their bioaccumulation: most heavy metals can accumulate in mammals' organs. Lead is infamous for degenerating the nervous system. Arsenic and chromium (mostly its highly mobile form, the Cr[VI]) can cause tumours.²⁰ Most heavy metals (such as Pb, Cd, Cr and As) are linked to increased risk of cancer and reproductive disorders.²¹ Children are generally more exposed to pollution and resulting diseases.²²

Not only can mammals be affected by metal pollution, but microbial activity in contaminated soils can also change. Chronic Cd and Cr pollution reduces the microbial mass and diversity.²³ The destruction of microbial activity affects the overall health of the soil, too.

¹⁶ XU et al. 2024.

¹⁷ WIJNGAARD et al. 2017.

¹⁸ FREEZE–CHERRY 1979; DAI et al. 2024.

¹⁹ FAN et al. 2022.

²⁰ SONG et al. 2006.

²¹ MANDUCA et al. 2020; BAAH et al. 2024.

²² RAHEEMAH et al. 2025.

²³ LI et al. 2024; POPOOLA et al. 2024.

Detoxification and remediation

Serious soil contamination requires immediate intervention to halt the migration of the pollutant. There are several technical methods to achieve a clear soil from a contaminated one.

Basically, the easiest *ex situ* method is the complete removal of the polluted soil. It can work when the polluted area is shallow, the excavated soil volume is small, and no other methods can be applied. The downside of this technology is that the contaminated soil is not cleared but disposed of at a safe site as hazardous waste, and the remediated area should be covered with healthy soil from an external source.

A more sophisticated, *in situ* method is the stabilisation of the pollutant by binders, such as lime, cement or phosphate. The binders stabilise pollutants underground, reducing their leachability. This cost-effective method works well when there are no direct expositional pathways to the consumers (plants, mammals).²⁴

Chemical extraction of pollutants is an effective *in situ* technology, where the contaminated media has high permeability and conductivity (e.g. sandy soils). Chelating agents, such as the biodegradable EDDS ([S,S] – ethylene – diamine – disuccinic acid), can be used for soil washing. The washing removes metal pollutants from the soil. The method is highly effective for lead extraction from the soil of shooting ranges.²⁵

Further physical-chemical solutions, such as electrokinetic remediation or thermal treatment, are also widely applied technologies.²⁶

Beside the aforementioned detoxification technologies, bioremediation methods are also playing an important role. Compost and biochar additives also reduce the mobility and bioavailability of several heavy metals (e.g. Cd, Cu, Pb, Zn).²⁷ Phosphate amendment, as well as bamboo and rice biochars are great additives for the immobilisation of Pb and Cd. These components are reducing the plant uptake too.²⁸

Some plants can bioaccumulate high levels of heavy metals. These plants are known as hyperaccumulators.²⁹ Hyperaccumulators take up contaminants through their root systems and store them without affecting the plants' fundamental mechanisms. To date, more than 700 species, mostly from the Phyllanthaceae and Brassicaceae families, have been identified as hyperaccumulators.³⁰ These plants can be planted in polluted areas and, after some time, can be harvested with the accumulated contaminants absorbed. This method is cost-effective, but less productive than the physicochemical ones.

²⁴ DU–JIANG 2022.

²⁵ SANDERSON et al. 2019.

²⁶ HANSEN et al. 1997; ORCINO–BRICKA 1998; OTTOSEN et al. 2003; BECH et al. 2014; LI et al. 2019.

²⁷ AHMAD et al. 2012a; YANG et al. 2016.

²⁸ AHMAD et al. 2012b; LU et al. 2017.

²⁹ REEVES et al. 2018.

³⁰ YAASHIKAA et al. 2022.

Synthesis and future directions

Military-related soil contamination is a complex, persistent and globally significant problem. The diversity of the contaminants causes a large variety in the type of pollution, which can be more complex due to the knowledge of the characteristics of different soils. Remediation processes are often site-specific, based on risk assessment calculations and soil properties.

As new technologies emerge, such as shotgun-like counter-drone systems, new mixtures of contaminants are entering the environment, which should be monitored in conflict zones.

From a scientific point of view, there is a lack of long-term, field-based studies, as well as chronic laboratory tests on different trophic levels. Newly introduced industrial materials, e.g. In or Bi, have only limited scientific data on their health effects. There is also very little knowledge on the mixture of contaminants: organic and inorganic ones, or just inorganic combinations.

Ongoing armed conflicts worldwide are producing ever more data. After the closure of each conflict, it is the common responsibility of the Army and the scientific actors to make those areas clean and livable again.

References

- AHMAD, Mahtab et al. (2012a): An Assessment of the Utilization of Waste Resources for the Immobilization of Pb and Cu in the Soil from a Korean Military Shooting Range. *Environmental Earth Sciences*, 67(4), 1023–1031. Online: <https://doi.org/10.1007/s12665-012-1550-1>
- AHMAD, Mahtab et al. (2012b): Effects of Soil Dilution and Amendments (Mussel Shell, Cow Bone, and Biochar) on Pb Availability and Phytotoxicity in Military Shooting Range Soil. *Ecotoxicology and Environmental Safety*, 79, 225–231. Online: <https://doi.org/10.1016/j.ecoenv.2012.01.003>
- ALLOWAY, Brian J. (2013): Sources of Heavy Metals and Metalloids in Soils. In ALLOWAY, Brian J. (ed.): *Heavy Metals in Soils. Trace Metals and Metalloids in Soils and their Bioavailability*. Dordrecht: Springer, 11–50. Online: https://doi.org/10.1007/978-94-007-4470-7_2
- ALTAHAAN, Zena – DOBSLAW, Daniel (2024): The Impact of War on Heavy Metal Concentrations and the Seasonal Variation of Pollutants in Soils of the Conflict Zone and Adjacent Areas in Mosul City. *Environments*, 11(11). Online: <https://doi.org/10.3390/environments11110247>
- BAAH, Douglas S. – FOSU-ASANTE, David – AGYEKUM, Crentsil Kofi – EDZESI, Wisdom Mawuli – ACHEAMPONG, Eric B. (2024): Geochemical Assessment of Metals in Soils and Food Crops around Alluvial Gold Mining in Abuakwa South Municipal, Ghana. *Soil and Sediment Contamination*, 33(5), 543–559. Online: <https://doi.org/10.1080/15320383.2023.2225624>
- BECH, Jaume – ABREU, Maria M. – CHON, Hyo-Taek – ROCA, Núria (2014): Remediation of Potentially Toxic Elements in Contaminated Soils. In BINI, Claudio – BECH,

- Jaume (eds.): *PHEs, Environment and Human Health. Potentially Harmful Elements in the Environment and the Impact on Human Health*. Dordrecht: Springer, 253–308. Online: https://doi.org/10.1007/978-94-017-8965-3_7
- CHAMORRO, Andrés F. – SÁNCHEZ-ANDICA, Rubén A. (2024): Understanding the Leaching Dynamics of Lead (Pb+2) in Artificial Soils under Different Conditions. *Agronomy*, 14(7). Online: <https://doi.org/10.3390/agronomy14071520>
- DAI, Sen – WANG, Zhe – ZENG, Qiuping – ZHANG, Gang (2024): Research on the Application of Comprehensive Physical Exploration in the Detection of Heavy Metal Contaminated Sites – Take the Case of Jijie Town in Yunnan Province as an Example. *2024 Photonics and Electromagnetics Research Symposium (PIERS)*, Chengdu, 21–25 April 2024. Online: <https://doi.org/10.1109/PIERS62282.2024.10618058>
- DENTON, Gary R. W. – EMBORSKI, Carmen A. – HACHERO, April A. B. – MASGA, Ray S. – STARMER, John A. (2016): Impact of WWII Dumpsites on Saipan (CNMI): Heavy Metal Status of Soils and Sediments. *Environmental Science and Pollution Research*, 23(11), 11339–11348. Online: <https://doi.org/10.1007/s11356-016-6603-7>
- DU, Yan-Jun – JIANG, Ning-Jun (2022): Stabilization/solidification of Contaminated Soils: A Case Study. In TSANG, Daniel C. W. – WANG, Lei (eds.): *Low Carbon Stabilization and Solidification of Hazardous Wastes*. Amsterdam: Elsevier, 75–92. Online: <https://doi.org/10.1016/B978-0-12-824004-5.00007-4>
- FAN, Tingting et al. (2022): Meta-analysis of Cd Input-output Fluxes in Agricultural Soil. *Chemosphere*, 303. Online: <https://doi.org/10.1016/j.chemosphere.2022.134974>
- FAYIGA, Abioye O. – SAHA, Uttam K. (2016): Soil Pollution at Outdoor Shooting Ranges: Health Effects, Bioavailability and Best Management Practices. *Environmental Pollution*, 216, 135–145. Online: <https://doi.org/10.1016/j.envpol.2016.05.062>
- FREEZE, R. Allan – Cherry, John A. (1979): *Groundwater*. Englewood Cliffs: Prentice-Hall.
- FÜGEDI, Ubul (2004): Geokémiai háttér és nehézfémzennyezés Gyöngyösorszi térségében [Geochemical Background and Heavy Metal Pollution Near Gyöngyösorszi (NE Hungary)]. *Földtani Közlöny*, 134(2), 291–301.
- HANSEN, Henrik K. – OTTOSEN, Lisbeth M. – KLIEM, Bodil K. – VILLUMSEN, Arne (1997): Electrodialytic Remediation of Soils Polluted with Cu, Cr, Hg, Pb and Zn. *Journal of Chemical Technology and Biotechnology*, 70(1), 67–73. Online: [https://doi.org/10.1002/\(SICI\)1097-4660\(199709\)70:1<67::AID-JCTB662>3.0.CO;2-V](https://doi.org/10.1002/(SICI)1097-4660(199709)70:1<67::AID-JCTB662>3.0.CO;2-V)
- HOOKE, Paul J. – NATHANAIL, C. Paul (2006): Risk-based Characterisation of Lead in Urban Soils. *Chemical Geology*, 226(3–4), 340–351. Online: <https://doi.org/10.1016/j.chemgeo.2005.09.028>
- KORRE, Anna – DURUCAN, Şevket – KOUTROUMANI, A. (2002): Quantitative-spatial Assessment of the Risks Associated with High Pb Loads in Soils around Lavrio, Greece. *Applied Geochemistry*, 17(8), 1029–1045. Online: [https://doi.org/10.1016/S0883-2927\(02\)00058-6](https://doi.org/10.1016/S0883-2927(02)00058-6)
- LI, Jining et al. (2019): Removal and Immobilization of Heavy Metals in Contaminated Soils by Chlorination and Thermal Treatment on an Industrial-scale. *Chemical Engineering Journal*, 359, 385–392. Online: <https://doi.org/10.1016/j.cej.2018.11.158>
- LI, Yuntao – GAO, Yan – CHEN, Wei – ZHANG, Weiguo – LU, Xin (2024): Shifts in Bacterial Diversity, Interactions and Microbial Elemental Cycling Genes under Cadmium Contamination in Paddy Soil: Implications for Altered Ecological

- Function. *Journal of Hazardous Materials*, 461. Online: <https://doi.org/10.1016/j.jhazmat.2023.132544>
- LI, Zhu et al. (2016): Metal Contamination Status of the Soil-Plant System and Effects on the Soil Microbial Community Near a Rare Metal Recycling Smelter. *Environmental Science and Pollution Research*, 23(17), 17625–17634. Online: <https://doi.org/10.1007/s11356-016-6958-9>
- LU, Kouping et al. (2017): Effect of Bamboo and Rice Straw Biochars on the Mobility and Redistribution of Heavy Metals (Cd, Cu, Pb and Zn) in Contaminated Soil. *Journal of Environmental Management*, 186, 285–292. Online: <https://doi.org/10.1016/j.jenvman.2016.05.068>
- MANDUCA, Paola – AL BARAQUNI, Nabil – PARODI, Stefano (2020): Long Term Risks to Neonatal Health from Exposure to War – 9 Years Long Survey of Reproductive Health and Contamination by Weapon-delivered Heavy Metals in Gaza, Palestine. *International Journal of Environmental Research and Public Health*, 17(7). Online: <https://doi.org/10.3390/ijerph17072538>
- MEES, Florias et al. (2013): Concentrations and Forms of Heavy Metals around Two Ore Processing Sites in Katanga, Democratic Republic of Congo. *Journal of African Earth Sciences*, 77, 22–30. Online: <https://doi.org/10.1016/j.jafrearsci.2012.09.008>
- MOLISZEWSKA, Ewa et al. (2025): Analysis of Variations in Heavy Metal Levels and Soil Microorganism Counts Resulting from Shelling Incidents in Ukraine. *Archives of Environmental Protection*, 51(1), 83–91. Online: <https://doi.org/10.24425/aep.2025.153752>
- NÉMETH, Tibor – JIMÉNEZ-MILLÁN, Juan – SIPOS, Péter – ABAD, Isabel – JIMÉNEZ-ESPINOSA, Rosario – SZALAI, Zoltán (2011): Effect of Pedogenic Clay Minerals on the Sorption of Copper in a Luvisol B Horizon. *Geoderma*, 160(3–4), 509–516. Online: <https://doi.org/10.1016/j.geoderma.2010.09.031>
- ORCINO, Michael A. – BRICKA, R. Mark (1998): Electrochemical Remediation of Heavy Metal Contaminated Soils. *Remediation*, 9(1), 23–47. Online: <https://doi.org/10.1002/rem.3440090104>
- OTTOSEN, Lisbeth M. – KRISTENSEN, Iben V. – PEDERSEN, Anne J. – HANSEN, Henrik K. – VILLUMSEN, Arne – RIBEIRO, Alexandra B. (2003): Electrodialytic Removal of Heavy Metals from Different Solid Waste Products. *Separation Science and Technology*, 38(6), 1269–1289. Online: <https://doi.org/10.1081/SS-120018809>
- PETRUSHKA, Kateryna – PETRUSHKA, Ihor (2025): Ecological Risks of Chromium Contamination in Ukrainian Soils Affected by Military Activity: SEM-EDS and EPMA Analysis. *Environmental Problems*, 10(3), 298–309. Online: <https://doi.org/10.23939/ep2025.03.298>
- POPOOLA, Olaniyi J. – OGUNDELE, Olusola D. – LADAPO, Emmanuel A. – SENBORE, Samson (2024): The Impact of Heavy Metal Contamination in Soils on Soil Microbial Communities and Its Potential Health Risks for Humans. In ARANSIOLA, Sesan A. – ATTA, Habiba I. – MADDELA, Naga R. (eds.): *Soil Microbiome in Green Technology Sustainability*. Cham: Springer, 351–375. Online: https://doi.org/10.1007/978-3-031-71844-1_15

- RAHEEMAH, Oday H. – KADHIM, Inaam H. – BOUDAYA, Chokri (2025): Measuring Uranium Levels in Nail Samples of Cancer Patients in Babylon Governorate, Iraq. *Environment Asia*, 18(3), 158–169. Online: <https://doi.org/10.14456/ea.2025.59>
- REEVES, Roger D. – BAKER, Alan J. M. – JAFFRÉ, Tanguy – ERSKINE, Peter D. – ECHEVARRIA, Guillaume – VAN DER ENT, Antony (2018): A Global Database for Plants that Hyperaccumulate Metal and Metalloid Trace Elements. *New Phytologist*, 218(2), 407–411. Online: <https://doi.org/10.1111/nph.14907>
- SANDERSON, Peter et al. (2019): Effectiveness of Gravity Based Particle Separation and Soil Washing for Reduction of Pb in a Clay Loam Shooting Range Soil. *Environmental Technology and Innovation*, 16. Online: <https://doi.org/10.1016/j.eti.2019.100480>
- SINGH, Shailendra K. – SUBRAMANIAN, V. – GIBBS, Ronald J. (1984): Hydrous FE and MN Oxides – Scavengers of Heavy Metals in the Aquatic Environment. *Critical Reviews in Environmental Control*, 14(1), 33–90. Online: <https://doi.org/10.1080/10643388409381713>
- SIPOS, Péter (2009): Distribution and Sorption of Potentially Toxic Metals in Four Forest Soils from Hungary. *Central European Journal of Geosciences*, 1(2), 183–192. Online: <https://doi.org/10.2478/v10085-009-0009-4>
- SKALNY, Anatoly V. et al. (2021): Environmental and Health Hazards of Military Metal Pollution. *Environmental Research*, 201. Online: <https://doi.org/10.1016/j.envres.2021.111568>
- SONG, Jinkun – TOWNSEND, Timothy – SOLO-GABRIELE, Helena – JANG, Yong-Chul (2006): Hexavalent Chromium Reduction in Soils Contaminated with Chromated Copper Arsenate Preservative. *Soil and Sediment Contamination*, 15(4), 387–399. Online: <https://doi.org/10.1080/15320380600751751>
- SPLODYTEL, Anastasiia (2020): Ландшафтно-геохімічні умови та закономірності розподілу токсичних елементів на території військового полігону “Олешківські піски” [Landscape and Geochemical Preconditions and Patterns of Toxic Element Distribution at the “Oleshky Sands” Military Training Range]. *Mineral Resources of Ukraine*, (1), 34–43. Online: <https://doi.org/10.31996/mru.2020.1.34-43>
- SZŰCS-VÁSÁRHELYI, Nóra (2019): A talajszennyezésről általában, különös tekintettel a szervesen szennyező anyagokra [Soil Pollution in General, with Particular Regard to Inorganic Pollutants]. *Hadmérnök*, 14(4), 127–146. Online: <https://doi.org/10.32567/hm.2019.4.8>
- TEŠAN TOMIĆ, Neda et al. (2018): Examining the Effects of the Destroying Ammunition, Mines and Explosive Devices on the Presence of Heavy Metals in Soil of Open Detonation Pit; Part 2: Determination of Heavy Metal Fractions. *Water, Air, & Soil Pollution*, 229(9), 1–20. Online: <https://doi.org/10.1007/s11270-018-3950-7>
- WIJNGAARD, René R. – VAN DER PERK, Marcel – VAN DER GRIFT, Bas – DE NIJS, Ton C. M. – BIERKENS, Marc F. P. (2017): The Impact of Climate Change on Metal Transport in a Lowland Catchment. *Water, Air, and Soil Pollution*, 228(3). Online: <https://doi.org/10.1007/s11270-017-3261-4>
- Xu, Zixin et al. (2024): Simulation of Vertical Migration Behaviors of Heavy Metals in Polluted Soils from Arid Regions in Northern China under Extreme Weather.

Science of the Total Environment, 919. Online: <https://doi.org/10.1016/j.scitotenv.2024.170494>

YAASHIKAA, Ponnambalam R. – SENTHIL KUMAR, P. – SATHASIVAM, Jeevanantham – RAJENDRAN, Saravanan (2022): A Review on Bioremediation Approach for Heavy Metal Detoxification and Accumulation in Plants. *Environmental Pollution*, 301. Online: <https://doi.org/10.1016/j.envpol.2022.119035>

YANG, Xing et al. (2016): Effect of Biochar on the Extractability of Heavy Metals (Cd, Cu, Pb, and Zn) and Enzyme Activity in Soil. *Environmental Science and Pollution Research*, 23(2), 974–984. Online: <https://doi.org/10.1007/s11356-015-4233-0>

YASHCHENKO, Liudmyla – ANDROSHCHUK, Oleksandr – VASYLENKO, Liudmyla – CHORNOIVAN, Yuliya (2025): Environmental Risks of Heavy Metal Pollution in War-Affected Soils in Ukraine. *European Journal of Environmental Sciences*, 15(1), 18–27. Online: <https://doi.org/10.14712/23361964.2025.3>

Földes Tibor¹

Védett létesítmények fizikai védelme

Különös tekintettel a katonai kritikus
infrastruktúrákra

Physical Protection of Secured Facilities

With Special Emphasis on Military Critical Infrastructures

Absztrakt

A kritikus infrastruktúrák fizikai védelme olyan összetett, többváltozós rendszertervezési kérdés, ahol a fizikai, információs és humán alrendszerek nem izoláltan, hanem egymás működését folyamatosan befolyásolva határozzák meg a rendszer egészének teljesítményét. Ez a komplexitás különösen a katonai létesítményeknél érzékelhető, ahol a tapasztalatok tartósan magas fenyegetési terhelést és jelentős sokféleséget mutatnak, és ezek a tényezők a tervezési és üzemeltetési döntéseket közvetlenül befolyásolják.

A tanulmány a katonai kritikus infrastruktúrák fizikai védelmét rendszerszintű összefüggések mentén elemzi, külön figyelmet fordítva a többretegű védelmi architektúrákra, a korszerű műszaki megoldások alkalmazhatóságára és a szabályozási környezet tényleges hatásaira. A vizsgálat olyan nemzetközi doktrínákra, mérnöki irányelvekre és hazai-európai szabványokra épül, amelyek a gyakorlatban bizonyítottan stabil és összehasonlítható keretet adnak a fizikai védelmi rendszerek tervezéséhez és értékeléséhez. A vizsgálat rámutat, hogy a fizikai védelem hatékonyságát döntően az alrendszerek közötti információáramlás minősége, a késleltetési képesség és a reagálási lánc integráltsága határozza meg, amelyek együttesen befolyásolják a rendszer műveleti teljesítményét.

Kulcsszavak: fizikai védelem, kritikusinfrastruktúra-védelem, védelmi architektúra, humán tényező, ellenálló képesség

¹ Okleveles kiberbiztonsági szakértő, doktori hallgató, Nemzeti Köszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: foldestibor252@gmail.com

Abstract

The physical protection of critical infrastructures is a complex, multivariable system-design challenge in which the physical, informational, and human subsystems do not operate in isolation, but continuously influence one another's functioning and jointly determine the overall performance of the system. This complexity is particularly evident in military facilities, where operational experience consistently indicates high threat intensity and considerable diversity, factors that directly shape planning and operational decision-making. The study analyses the physical protection of military critical infrastructures through system-level interdependencies, with particular emphasis on multilayered defence architectures, the applicability of modern engineering solutions, and the practical effects of the regulatory environment. The analysis builds on international doctrines, engineering guidelines, and national–European standards that have proven in practice to provide a stable and comparable framework for the design and evaluation of physical protection systems. The findings highlight that the effectiveness of physical protection is fundamentally determined by the quality of information flow between subsystems, the system's ability to delay hostile actions, and the integration of the response chain – factors that collectively shape the operational performance of the entire system.

Keywords: physical security, critical infrastructure protection, protective architecture, human factors, resilience

Bevezetés

A tudományos felfedezések, az innovációban rejlő képességek és lehetőségek szinte folyamatosan változtatták és változtatják a biztonsági környezetet.² A védett létesítmények fizikai védelme a biztonságstudomány, a hadtudomány és a mérnöki tudományok olyan metszéspontján helyezkedik el, ahol a tervezési és műveleti döntések során az interdiszciplinaritás nem elméleti jelenség, hanem a mindennapi gyakorlatot meghatározó működési feltétel.

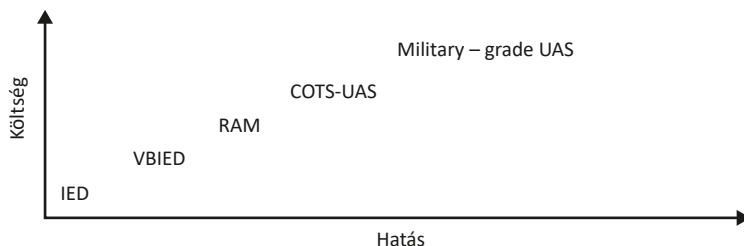
A katonai kritikus infrastruktúrák – a repülőterektől a logisztikai és parancsnoki központokon át a kommunikációs hálózatokig – közvetlen hatást gyakorolnak a haderő műveleti és reagálóképességére, így működésük sérülése azonnal stratégiai következményekkel jár. Ez a közvetlen összefüggés magyarázza, hogy a kritikus infrastruktúrák védelme miért kiemelt stratégiai jelentőségű a katonai tervezésben. Az elmúlt két évtized tapasztalatai szerint a fenyegetési skála jelentősen bővült és differenciálódott, ami a tervezési folyamatok számos elemét – különösen a zónarendszer kialakítását és a reagálási protollokat – újragondolásra kényszerítette. E fenyegetések közös jellemzője a nehezen előre jelezhető működés és az aránytalan műveleti hatás. Az IED³-k – különösen a járműbe telepített robbanóeszközök (VBIED⁴), a járművel

² FÖLDES 2025: 146.

³ IED: *improvised explosive device* – házilag összeállított, nem ipari gyártású robbanóeszköz.

⁴ VBIED: *vehicle-borne improvised explosive device* – járműbe rejtett rögtönzött robbanóeszköz.

végrehajtott támadások (RAM⁵), valamint a kereskedelmi drónok (COTS UAS⁶) nemcsak fizikai károkat okoznak, hanem a műveleti folytonosságot és a személyi állomány biztonságát is komolyan veszélyeztetik. A fenyegetések heterogén természete miatt a védelmi rendszernek képesnek kell lennie arra, hogy a közvetlen támadásokat, a rejtett behatolást és a robbanóanyag-bejuttatást párhuzamosan vagy gyors egymásutánban kezelje, amit az 1. ábra a fenyegetési skála alakulásán keresztül szemléltet.



1. ábra: A fenyegetési skála alakulása

Forrás: a szerző szerkesztése

Kovács Zoltán rámutat, hogy az IED-knek az egyszerű előállíthatóság, az alacsony költség és a médiában kiváltott pszichológiai hatás miatt nemcsak harcászati, hanem stratégiai jelentősége is van. A közelmúlt műveleti tapasztalatai jól szemléltetik a fentiek gyakorlati jelentőségét.⁷ Az ukrajnai hadszíntéren 2022 óta több esetben is megfigyelhető volt, hogy viszonylag alacsony költségű, kereskedelmi forgalomban elérhető pilóta nélküli eszközök képesek voltak jelentős hatást gyakorolni katonai infrastruktúrára. Ezek az esetek rávilágítanak arra, hogy a fenyegetések hatékonysága nem feltétlenül a technológiai komplexitásból, hanem a védelmi rendszer hiányosságainak kihasználásából ered.

A NATO doktrínái – különösen az AJP-3.14 (2024) – a fizikai védelmet a force protection olyan integrált elemének tekintik, amely a fenyegetések észlelésétől a késleltetésen át a végrehajtott elhárításig a teljes műveleti ciklus minden szakaszában meghatározó szerepet tölt be. Az AJP-3.14 (2024) a fizikai védelem négy funkcióját – megelőzés, észlelés, késleltetés, elhárítás – egymásra épülő folyamatként értelmezi, hangsúlyozva, hogy az idő és az információáramlás minősége döntően befolyásolja a rendszer valós műveleti hatékonyságát. A doktrína kiemelten kezeli a rendszerszemléletű megközelítést, és a többrétegű védelem következetes alkalmazását tekinti alapelvnek, mivel ez biztosítja a fenyegetések gyengítését több ponton. A 2024. évi LXXXIV. törvény a hazai ellenállóképesség-szabályozást a szolgáltatásalapú ellenálló képességi modell irányába mozdította el, amely a korábbi létesítmény-központú megközelítést kiegészítve a működésfolytonosság, az éves gyakorlatok és a bizonyítható kockázatértékelés követelményeit erősítette meg. A normatív átalakulás következtében a hangsúly mindinkább a működésfolytonosság bizonyítható biztosítására, az éves gyakorlatok

⁵ RAM: rocket-assisted munition – rakétahajtással indított lőszer.

⁶ COTS: commercial-off-the-shelf – kereskedelmi forgalomban beszerezhető (polgári célú).

⁷ Kovács 2013: 78.

szabályozott végrehajtására és az intézményközi együttműködés mérhető fejlesztésére került, amelyek együtt az ellenálló képesség tényleges erősödését szolgálják. A fizikai védelem ebben a megközelítésben már nem csupán műszaki vagy építészeti feladat, hanem olyan alkalmazkodó biztonsági rendszer, amelynek működése folyamatos alkalmazkodást igényel a változó fenyegetési mintázatokhoz és a műveleti környezet dinamikus sajátosságaihoz.

A fizikai védelem rendszerszintű értelmezése

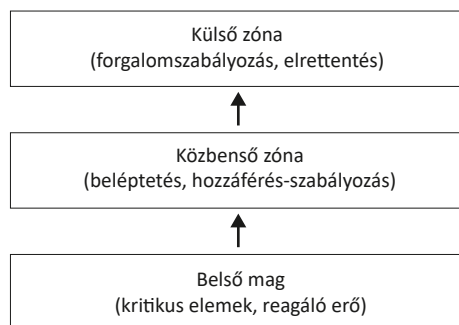
A fizikai védelem a katonai és kritikus infrastruktúrák biztonsági architektúrájának azon eleme, ahol a műszaki megoldások, a működési eljárások és az emberi tényezők nem elkülönülten, hanem valós időben, egymásra ható, folyamatos visszacsatolásban működő rendszerként jelennek meg.

A katonai infrastruktúrák sajátossága miatt a fizikai védelemnek nemcsak a közvetlen támadások elhárítására kell fókuszálnia, hanem a túlélőképesség és a műveleti folytonosság fenntartására is. Ez magában foglalja a kritikus képességek megfelelő redundanciáját, a parancsnoki struktúrák rezilienciáját és a támadás utáni helyreállítási folyamatok olyan szintű integrációját, amely lehetővé teszi a műveleti képességek gyors visszaállítását. A cél tehát nem csupán a támadás megállítás, hanem annak biztosítása is, hogy a létfontosságú katonai funkciók a támadás közben és azt követően is fenntarthatók legyenek.

A rendszerszemlélet egyik központi eleme a többrétegű védelem, amely térben és funkcionálisan elkülönülő, egymást kiegészítő védelmi zónákból áll. A külső zónák elsődleges feladata az elrettentés, a korai észlelés támogatása és a forgalom kontrollálása; a közbenső zónák a hozzáférés korlátozására és a támadó késleltetésére szolgálnak; míg a belső zónák a kritikus elemek közvetlen védelmét és a gyors reagálást biztosítják. A belső mag a kritikus rendszerek közvetlen védelmét és a gyors reagálás feltételeit teremti meg. A kockázatalapú megközelítés jelentőségét a NATO-szintű értékelések és a gyakorlati tapasztalatok is alátámasztják, különösen azokban az esetekben, amikor a fenyegetések gyors változása miatt a statikus védelmi modellek már nem alkalmazhatók. A kockázatelemzés gyakorlati alkalmazása ugyan nem minden esetben követi a formális módszertani előírásokat, mégis a fenyegetés–sebezhetőség–következmény hármasának elemzése nélkülözhetetlen a megalapozott védelmi döntésekhez. A CARVER⁸- és RAMCAP⁹-alapú rangsorolási módszerek alkalmazása tovább növeli a döntéshozatal átláthatóságát és objektivitását, különösen akkor, amikor a rendelkezésre álló erőforrások szűkösek, ami jól látható a többrétegű fizikai védelmi architektúra egymásra épülését bemutató 2. ábrán is.

⁸ CARVER: *criticality, accessibility, recuperability, vulnerability, effect, recognizability* – célpontértékelési módszer.

⁹ RAMCAP: *risk analysis and management for critical asset protection* – kockázatalapú értékelési módszer.



2. ábra: Többretegű fizikai védelmi architektúra

Forrás: a szerző szerkesztése

Kovács repülőtéri példái is megerősítik, hogy a külső és belső védelmi zónák csak integrált működésükben hatékonyak: a járművek előszűrése, az ellenőrző-átesztelő pontok működtetése és az optikai-elektronikai érzékelőrendszerek együttese teremti meg a többvonalas védelmi architektúra tényleges hatékonyságát.¹⁰ A szerző repülőtéri esettanulmánya alapján a VBIED-ek elleni védelem kulcsa a megközelítési útvonalak kontrollja: a forgalomlassító berendezések, tüskés útzárak, kiemelkedő oszlopok és sorompók alkalmazása hatékonyan csökkenti annak esélyét, hogy a jármű a kritikus létesítmények közvetlen közelébe jusson.¹¹

A fizikai védelmi rendszerek tervezése a helyzetértékeléstől a követelmények meghatározásán át a megvalósításig és a visszamérésig tartó, PDCA¹²-logikára épülő iteratív folyamat, amely minden ciklusban új finomhangolási lehetőségeket tár fel. E folyamat a dokumentált működés rendjét – biztonsági terveket, üzemeltetési eljárásokat, karbantartási protokollokat – is integrálja, amelyek a rendszer stabilitásának alapfeltételei. A műszaki követelményrendszer – beleértve a DoD UFC-szabványokat, a FEMA 42613 ajánlásait és az EN 1354114 vizsgálati kereteit – meghatározza a robbanás elleni védelem fő paramétereit, különös tekintettel a védőtávolságok megállapítására és a szerkezeti megerősítési követelményekre. Ugyanakkor e dokumentumok alkalmazása mindig telephely-specifikus értelmezést igényel. E szabványok közös pontja, hogy a védelmet rendszerszinten értelmezik: az üvegezés, a keret, a rögzítés és a csatlakozó szerkezet egységét tekintik a teljesítmény mércéjének.

A fizikai védelem ugyanakkor nem választható el a C2/C4ISR15-rendszerek által biztosított információs és vezetésirányítási környezettől. Az érzékelőrendszerekből, beléptetési pontokból és megfigyelő alrendszerekből származó adatok csak akkor képeznek valódi védelmi értéket, ha integrált módon, döntéstámogató logikába

¹⁰ Kovács 2013: 81–82.

¹¹ Kovács 2014: 108.

¹² PDCA: *plan-do-check-act* – tervezés, végrehajtás, ellenőrzés, beavatkozás.

¹³ FEMA 426: kézikönyv, amely az épületek terrorcselekményekkel szembeni védelmének alapelveit, a robbanás hatás csökkentésére szolgáló tervezési megoldásokat és a telephelyi védelmi beavatkozások módszereit foglalja össze.

¹⁴ EN 13541: európai szabvány biztonsági üvegek robbanásálló vizsgálatára és osztályozására.

¹⁵ C2: *command and control*; C4ISR: *command, control, communications, computers, intelligence, surveillance and reconnaissance*.

rendezve jelennek meg. A hatékonyság kulcsa ezért a detektálás, az értékelés és a reagálás folyamatainak összehangoltsága.

A rendszer működésének mérhetősége pedig a visszacsatolási ciklus alapját képezi. Az olyan teljesítménymutatók, mint az észlelési idő, a reagálási idő, a téves riasztások aránya vagy a kritikus alrendszerek rendelkezésre állása, lehetővé teszik a rendszer objektív értékelését és célzott fejlesztését. A folyamatos monitorozás és elemzés biztosítja, hogy a védelem képes legyen alkalmazkodni a változó fenyegetésekhez, és a rendszer rezilienciája a gyakorlatban is fenntartható legyen.

A fenyegetések és a többrétegű védelem gyakorlata

Az elmúlt évtizedben a katonai kritikus infrastruktúrák elleni fenyegetések olyan mértékben változtak meg szerkezetükben és dinamikájukban, hogy a korábban alkalmazott védelmi modellek több ponton már nem bizonyultak megfelelőnek, ezért részbeni újraértelmezésük vagy akár teljes felülvizsgálatuk vált szükségessé. A hagyományos fegyveres fenyegetések mellett az elmúlt években egyre nagyobb hangsúlyt kaptak az aszimmetrikus és hibrid módszerek, ideértve az IED- és VBIED-támadásokat, a RAM-típusú fenyegetéseket, valamint a pilóta nélküli rendszerek sokszínű alkalmazását. E fenyegetéstípusok közös sajátossága, hogy a támadó fél viszonylag alacsony erőforrás-ráfordítással is olyan hatást érhet el, amely jelentős műveleti következményekkel járhat a védett infrastruktúra működésére nézve. A támadási formák közös pontja a nehezen előre jelezhető támadási mintázat, a minimális előkészítési igény és az a jellegzetes *low-cost/high-impact dinamika, amely kis ráfordítással is aránytalan műveleti hatást tesz lehetővé*. A NATO AJP-3.14¹⁶ doktrína a fenyegetések változó mintázataira válaszul továbbra is a force protection rendszerébe illesztve határozza meg a fizikai védelem szerepét, és a védelmi intézkedéseket konkrét fenyegetéstípusokhoz rendelt funkciók szerint strukturálja. Ezzel összhangban a FEMA 426 és a DoD UFC 4-010-01¹⁷ szabványai is a fizikai védelmet konkrét, mérhető kockázati kategóriákhoz kapcsolják, nem pedig általános, nehezen operacionalizálható elvekhez. Ez a keretrendszer lehetővé teszi, hogy a tervezés és az üzemeltetés ne elvont biztonsági elvekre, hanem tényleges támadási profilokra és azok mérhető kockázati paramétereire épüljön.

A robbantásos támadások elemzésekor a támadás módja, a töltet nagysága és az elhelyezés környezeti sajátosságai különösen meghatározó tényezők, mivel ezek döntik el a robbanás terjedésének és károkozásának fő paramétereit. A VBIED-ok elsősorban a külső védelmi zónák nagy energiájú áttörését célozzák, míg az IED-k többnyire a belső mozgási útvonalak mentén okoznak kritikus károkat, megzavarva a személyi és logisztikai folyamatokat. A két támadástípus eltérő detektálási és késleltetési stratégiákat követel meg, mivel a fenyegetés időbelisége, észlelhetősége és a károkozás várható módja jelentősen különbözik. Ezt jól illusztrálják az afganisztáni

¹⁶ NATO AJP-3.14: doktrína, amely meghatározza a haderők védelmének alapelveit, a megelőzés–észlelés–késleltetés–elhárítás folyamatát, valamint a többrétegű fizikai védelem és a vezetésirányítás integrált követelményeit.

¹⁷ DoD UFC 4-010-01: amerikai katonai építészmérnöki szabvány.

műveletek során tapasztalt esetek, ahol a VBIED-támadások elsősorban a külső ellenőrzési pontok ellen irányultak, míg az IED-k a belső mozgási útvonalak mentén okoztak veszteségeket. A tapasztalatok szerint azok a létesítmények bizonyultak ellenállóbbnak, ahol a védelmi zónák közötti információáramlás gyors és strukturált volt, lehetővé téve a reagáló erők időbeni alkalmazását. Ennek megfelelően a védekezés két alapvető pillére a védőtávolság növelése – amely a csúcstúlnyomás és az impulzus csillapításán keresztül csökkenti a terhelést – valamint a szerkezeti ellenálló képesség növelése, amely a láncszerű összeomlással szembeni védelmet biztosítja. A robbanás hatás mérésének két kulcsparamétere, a csúcstúlnyomás (P_{peak} ¹⁸) és az impulzus (I)¹⁹, nemcsak a töltet méretétől, hanem a környezet geometriájától, a visszaverődési felületektől és a csatornázódási hatásoktól is jelentősen függ.

A nyílászárók és az üvegezett felületek különösen sérülékenyek robbanás esetén, mivel az üvegtörmelék által képzett repeszek a másodlagos sérülések leggyakoribb forrásai. A sérülési kockázatot nemcsak az üveg típusa, hanem a keret, a rögzítés és a csatlakozó felület együttes viselkedése határozza meg. Az EN 13541 szabvány a védelem értékelését nem az üveg önálló tulajdonságaira, hanem az üveg–keret–rögzítés–falcsatlakozás egészének viselkedésére alapozza. Ez a rendszerszintű szemlélet tükrözi, hogy a robbanásállóság tényleges mértékét mindig a teljes szerkezeti kombináció határozza meg. Ez a szemlélet egyre inkább megjelenik a nemzetközi gyakorlatban is, ahol a robbanásbiztosítás már nem tekinthető pusztán anyagminőségi kérdésnek.

A RAM-fenyegetések legnagyobb kihívása a kiszámíthatatlanság és a minimális előkészületi idő. A RAM-fenyegetések kezeléséhez a védelem passzív és aktív elemek kombinációjára van szükség. Ide tartozik a kritikus elemek térbeli szétválasztása, a védett útvonalak kijelölése és a menedékhelyek kialakítása, ugyanakkor mindez csak akkor működik hatékonyan, ha gyors riasztási és reagálási lánc kapcsolódik hozzá, amelyet megfelelően integrált C2/C4ISR-rendszer támogat.

Az utóbbi években a pilóta nélküli rendszerek elleni védelem önálló, gyorsan fejlődő szakterületté vált, ami egyértelműen tükrözi a fenyegetés stratégiai jelentőségét és a technológiai fejlődés ütemét. Az UAS²⁰-fenyegetések detektálása különösen összetett feladat, mivel a drónok kis radarkeresztmetszete, csökkentett akusztikus és infravörös emissziója, valamint a kommunikációs protokollok sokfélesége jelentősen korlátozza az egyes szenzortípusok önálló hatékonyságát. Ennek következtében az egyszenzoros detektálási rendszerek megbízhatósága korlátozott, és gyakran nem képesek a fenyegetések időbeni felismerésére. A gyakorlatban ezért multisenzoros adatfúziós megközelítéseket alkalmaznak – például RF-felderítést radarral, elektro-optikai és infravörös érzékeléssel kombinálva –, amelyek képesek a detektálási valószínűséget (P_d) növelni a téves riasztási arány szinten tartása mellett.

A többrétegű védelem gyakorlati hatékonysága elsősorban azon múlik, hogy a különböző védelmi zónák között milyen minőségű funkcionális és információáramlási kapcsolatok jönnek létre. A külső zónák elsősorban az elrettentést és a korai észlelést szolgálják, a közbenső zónák feladata a hozzáférés-korlátozás és a támadó

¹⁸ P_{peak} : a robbanáshullám által keltett maximális túlnyomás.

¹⁹ I : a robbanáshullám időben integrált nyomásterhelése.

²⁰ UAS: *unmanned aircraft system* – pilóta nélküli légi rendszer.

késleltetése, míg a belső zóna a kritikus elemek közvetlen védelmét és a gyors reagálás feltételeinek biztosítását látja el. A zónák hatékonysága valójában nem az egyes zónák önálló teljesítményétől, hanem az egymás közötti információ- és cselekvésáramlás minőségétől függ; ha ez sérül, a védelmi rendszer gyorsan fragmentálódik. A védelem működési teljesítményének objektív mérése elengedhetetlen a fejlesztési ciklus során, mivel csak így azonosíthatók a rendszer gyenge pontjai és a késleltetésből vagy információhiányból eredő hibák. A rendszer működési teljesítménye kvantitatív mutatókkal értékelhető, például az észlelési idővel, a reaklási idővel, a téves riasztási aránnyal és a rendelkezésre állással. Ezek együtt adják a védelmi architektúra működési profilját. Az adatok objektív visszajelzést adnak arról, hogy a rendszer mennyire képes megfelelni a műveleti követelményeknek. A folyamatos monitorozás és az értékelési mechanizmusok lehetővé teszik a rendszer gyenge pontjainak gyors azonosítását, és olyan beavatkozások meghatározását, amelyek javítják a teljes védelmi architektúra adaptivitását.

Műszaki és szabványosított védelmi megoldások

A fizikai védelem műszaki alapját azok a szabványok és követelményrendszerek adják, amelyek egyfelől meghatározzák a létesítmények robbanásállóságának és szerkezeti ellenálló képességének minimumát, másfelől pedig biztosítják a védelmi intézkedések mérhetőségét, ellenőrizhetőségét és dokumentálható igazolhatóságát. Katonai infrastruktúrák esetében ezek a követelmények nem egyszerű ajánlások, hanem kötelező érvényű tervezési alapelvek, amelyek be nem tartása közvetlenül csökkentené a létesítmények túlélőképességét.

A DoD egységes létesítményi szabályozása, az UFC 4-010-01, a minimális antiterro rizmus-követelményeket úgy rögzíti, hogy a tervezők számára egy jól értelmezhető és mérnöki le következetes referenciakeretet adjon a fizikai terhelések, robbanás-védelmi paraméterek és biztonsági funkciók meghatározásához. A követelmények nemcsak új létesítményekre, hanem meghatározott esetekben a meglévő épületekre is vonatkoznak, különösen akkor, ha felújítás, bővítés vagy funkcióváltás történik. A szabvány részletesen rögzíti a robbanás elleni védelem paramétereit, a szükséges védőtávolságokat, valamint azokat a szerkezeti és építészeti kialakítási szempontokat, amelyek a láncszerű összeomlás megelőzését szolgálják.

A robbanás elleni védelem egyik legfontosabb alapelve a védőtávolság, amely lehetővé teszi, hogy a robbanáshullám csúcstúlnyomása és impulzusa már a célobjektum előtt számottevően lecsökkenjen. A robbanáshullám túlnyomása a távolság köbével fordított arányban csökken ($\sim 1/R^3$), ezért a védőtávolság növelése a leghatékonyabb passzív védelmi eszközök közé tartozik: már néhány méteres növelés is jelentős tehersökkenést eredményez. Az UFC 4-010-02²¹ ezt az alapelvet konkrét, számítható tervezési követelményekre bontja le, amelyek egyértelmű iránymutatást adnak a minimális védőtávolság meghatározásához.

²¹ DoD UFC 4-010-02: amerikai katonai építésztechnikai szabvány.

A szerkezeti védelem célja nem pusztán a robbanás elsődleges terhelésének elviselése, hanem annak biztosítása is, hogy egyes teherhordó elemek károsodása ne indítson el láncszerű összeomlást. Ennek érdekében alternatív teherutakat, duktilitást biztosító csomópont-kialakítást és energiaelnyelő szerkezeti megoldásokat szükséges alkalmazni. Ez azt jelenti, hogy egyetlen teherhordó elem kiesése nem indít el olyan láncreakciót, amely az egész épület részleges vagy teljes összeomlásához vezetne. A szabványok ezért redundáns teherhordási megoldásokat és olyan szerkezeti kialakítási elveket követelnek meg, amelyek biztosítják a terhek átvitelét alternatív útvonalakon.

A nyílászárók és az üvegezett felületek különösen érzékenyek, mivel robbanás esetén az üvegtörmelékből származó repeszek adják a másodlagos sérülések legnagyobb részét. A nyílászárók teljesítményét azonban nem önmagában az üveg minősége határozza meg, hanem a keret, a rögzítési rendszer és a csatlakozó felületek együttes, rendszerszintű viselkedése. Az EN 13541 szabvány részletesen meghatározza az üvegezések vizsgálati módszereit és teljesítményosztályait, rendszerszintű megközelítést alkalmazva az üveg–keret–rögzítés–falcsatlakozás egészére. A teljesítményt az üveg–keret–rögzítés rendszere határozza meg (3. ábra).



3. ábra: Üvegezési rendszerek teljesítménye rendszerszinten (EN 13541 logika szerint)

Forrás: a szerző szerkesztése

Kovács Zoltán vizsgálatai szerint a robbanásállóság növelésének leghatékonyabb módszerei közé tartoznak a falszerkezetek hossz- és keresztirányú merevítései, a szénszálas megerősítések alkalmazása, valamint a gyantás, többretegű biztonsági üvegezés, amelyek a repeszhatás és a túlnyomás jelentős részét képesek elnyelni.²² Balogh Zsuzsanna rámutat, hogy a robbanáskor keletkező üvegszilánkok akár 40 m/s sebességgel is kirepülhetnek, ezért a biztonsági fólia önmagában nem elég; a hatásosság jelentősen növelhető, ha az üvegréteget a kerethez rugalmas szilikonragasztással rögzítik, amely a repeszek szétszóródását érdemben csökkenti.²³

A meglévő épületek védelmi fejlesztése gyakran komoly műszaki korlátokba ütközik, ezért a FEMA 426 külön hangsúlyt helyez azokra a fokozatos, kisebb beavatkozást igénylő megoldásokra, amelyekkel a védettség jelentősen növelhető. Ide tartozik például az üvegezések megerősítése, a belső terek átszervezése vagy a forgalom szabályozása.

A fizikai védelem ma már messze túlmutat a statikus szerkezeti elemek alkalmazásán: a modern rendszerek egyre inkább valós idejű érzékelési láncokra, multiszenzoros adatfúzióra és gyors reagálási képességet támogató informatikai infrastruktúrára épülnek. Különösen igaz ez a pilóta nélküli eszközök elleni védelemben, ahol többféle szenzor együttes alkalmazása szükséges.

²² KOVÁCS 2013: 77–78.

²³ BALOGH 2010: 267.

A korszerű C-UAS-rendszerek többféle érzékelési módot kombinálnak, köztük a rádiófrekvenciás skála figyelést, a radarérzékelést és az optikai rendszereket, hogy növeljék a detektálási valószínűséget és csökkentsék a téves riasztások arányát. Ezek célja elsősorban a korai észlelés és a helyzetkép pontosítása.

A műszaki rendszerek hatékonysága nagyrészt azon múlik, hogy mennyire képesek együttműködni és milyen minőségben integrálódnak a döntéstámogató rendszerekbe. A gyakorlati tapasztalatok szerint sok esetben az integráció hiánya nagyobb működési problémát okoz, mint az egyes eszközökön belüli műszaki korlátok. A szenzorok és védelmi eszközök működése csak akkor tekinthető hatékonynak, ha szorosan kapcsolódik a döntéstámogató és irányítási rendszerekhez, biztosítva az információ gyors és torzításmentes továbbítását. A detektálás, az értékelés és a reagálás így egy koherens folyamatláncot alkot, ahol minden késedelem vagy információs veszteség közvetlenül rontja a védelmi képességet.

A szabványok is ezt a rendszerszemléletet követik: a fizikai védelmi elemeket nem önálló megoldásként, hanem egy összekapcsolt, integrált rendszer komponenseiként kezelik. A műszaki védelem ezért nem csupán szerkezeti, hanem információs és működtetési kérdés is, amelyben az adatáramlás minősége és a reagálási lánc hatékonysága legalább olyan fontos, mint az alkalmazott szerkezeti megoldások.

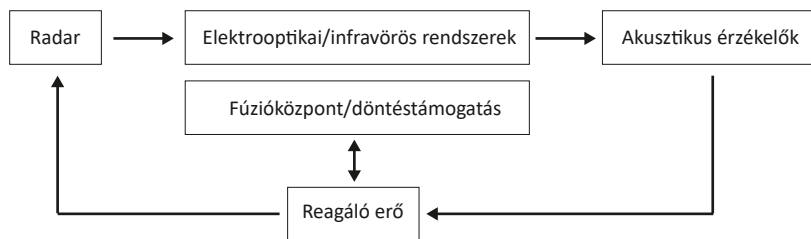
Integrált védelem és jövőbeli irányok

A robbantásos támadások elemzésekor kiemelt jelentősége van a támadás módjának, a töltet nagyságának és az elhelyezés környezeti geometriájának, mivel ezek döntik el a csúcstűlnyomás alakulását és a szerkezet várható válaszát. Emiatt e tényezők tervezési szinten való kezelése alapvető követelmény.

A nyílászárók és üvegezett felületek különösen érzékenyek a robbanás hatására, mivel a másodlagos repeszkarok döntő része ezekből a szerkezetekből ered. Az EN 13541 szabvány rendszerszintű megközelítést alkalmaz: az üvegezés ellenálló képességét nem az üveg tulajdonságai, hanem az üveg–keret–rögzítés–falcsatlakozás teljes szerkezeti együttese határozza meg. Ez a szemlélet mára széles körben elfogadott követelménnyé vált a nemzetközi mérnöki gyakorlatban. A RAM-fenyegetések sajátossága a kiszámíthatatlanság és a rendkívül rövid előkészületi idő, amely a védelem számára kifejezetten szűk reakcióablakot eredményez. E kihívás kezelése érdekében a védelem passzív és aktív elemek kombinációjára épít, amelyek együtt biztosítják a reakcióidő csökkentését és a támadási hatás mérséklését.

Az UAS-fenyegetések az elmúlt években olyan gyors technológiai és taktikai fejlődésen mentek keresztül, hogy mára önálló, specializált védelmi szakterületet alkotnak. Ez nemcsak a fenyegetés súlyát mutatja, hanem azt is, hogy a hagyományos védelmi architektúrák számos elemét újra kellett értékelni. A gyakorlatban több katonai repülőtér esetében is azonosították, hogy az egyszenzoros rendszerek nem biztosítanak megfelelő megbízhatóságot, különösen összetett környezeti háttér esetén. Az ilyen tapasztalatok vezettek a multisenzoros rendszerek szélesebb körű alkalmazásához. A drónok alacsony radarkeresztmetszete, változatos kommunikációs

csatornái és gyors konfigurálhatósága miatt a hatékony detektálás multiszenzoros megközelítést igényel, amelynek felépítését a 4. ábra szemlélteti.



4. ábra: A multiszenzoros C-UAS²⁴ detektálási architektúra

Forrás: a szerző szerkesztése

Napjainkban a radar-, az elektro-optikai és infravörös rendszerek, valamint az akusztikus érzékelők együttes alkalmazása biztosítja a megfelelő észlelési megbízhatóságot. A C-UAS-védelem ugyanakkor nem kizárólag technikai feladat. Legalább ilyen fontos az eljárási és döntési folyamatok megfelelő szabályozása: a felderítés, az azonosítás és a reagálás eljárási integritása, valamint a felelősségi körök pontos kijelölése legalább olyan meghatározó, mint a használt technológia minősége.

A többretegű védelem gyakorlati hatékonyságát elsősorban a védelmi zónák közötti funkcionális kapcsolatok és az információáramlás minősége határozza meg. A késleltetésből nyerhető időablak csak akkor érvényesíthető, ha az érzékelési információk gyorsan, torzításmentesen és a döntéshozatal szempontjából értelmezhető formában jutnak el a megfelelő szereplőkhöz. A védelmi rendszer teljesítményének mérése a fejlesztési ciklus elengedhetetlen eleme. Az olyan mérőszámok, mint az észlelési idő, a reagálási idő, a téves riasztások aránya vagy az alrendszerek rendelkezésre állása objektív visszajelzést adnak a rendszer működési hatékonyságáról és gyenge pontjairól. A folyamatos monitorozás és visszacsatolás nemcsak az aktuális működés optimalizálását segíti elő, hanem a hosszú távú adaptivitás feltételeit is megteremti.

A jövőbeli fejlesztések kulcsterülete az automatizált döntéstámogatás, a mesterségesintelligencia-alapú fenyegetésazonosítás, valamint a fizikai és kiberbiztonsági rendszerek konvergenciája, amelyek új típusú integrációs kihívásokat és egyben lehetőségeket is teremtenek. Összességében a fizikai védelem jövője nem egyetlen technológiai újítástól függ, hanem a különböző műszaki, informatikai és szervezeti megoldások olyan integrációjától, amely képes egységes, alkalmazkodó és közösen fejlődő rendszert alkotni. A tapasztalatok a multiszenzoros rendszerek elsődlegességét igazolják az UAS-fenyegetések kezelésében.

²⁴ C-UAS: *counter-unmanned aircraft system* – pilóta nélküli légi rendszerek elleni védelem (drónellenes rendszerek).

Szervezeti és humán tényezők

A fizikai védelem hatékonysága nem kizárólag a telepített műszaki rendszerek teljesítményétől függ, hanem attól is, hogy a működtető szervezet és a személyi állomány mennyire képes ezeket működtetni. A technikai rendszerek valós teljesítménye végső soron az állomány kompetenciáját tükrözi: még a legkorszerűbb szenzor- és döntéstámogató rendszerek sem működnek hatékonyan, ha a kezelők nem értik azok működési logikáját és a potenciális hibamódokat. A NATO AJP-3.14 (2024) szerint a *force protection* hatékonyságának egyik kulctényezője a jól képzett állomány és a világosan meghatározott parancsnoki felelősségi struktúra, amely garantálja, hogy a döntések időben, torzításmentesen és megfelelő prioritási sorrendben szülessenek meg. A védelem akkor tekinthető működőképesnek, ha a szervezet képes a fenyegetések gyors felismerésére, a helyzetek értelmezésére és a szükséges reakciók következetes végrehajtására. Tapasztalatok szerint az incidensek jelentős részében nem a technikai rendszer hibája, hanem az eljárások nem megfelelő alkalmazása vezetett a védelmi hiányosságokhoz. Ez különösen igaz olyan helyzetekben, ahol a kezelőszemélyzet nem rendelkezett kellő gyakorlattal a komplex riasztási helyzetek kezelésében.

Az amerikai ADP 3-37²⁵ doktrína szintén hangsúlyozza, hogy a védelem operatív hatékonysága alapvetően az eljárások ismeretén és következetes alkalmazásán múlik. A tapasztalatok szerint az eljárási fegyelem hiánya sok esetben nagyobb kockázatot jelent, mint a műszaki rendszer hiányosságai, mivel közvetlenül érinti a reakálás időbeliségét és pontosságát. A szabályok pusztá végrehajtása azonban nem elegendő: az állománynak értenie kell az eljárások mögötti célokat, összefüggéseket és várható következményeket, különösen gyorsan változó fenyegetési helyzetben.

A felkészítés három, egymást kiegészítő területet foglal magában: a fenyegetések felismerését és értelmezését; a technikai rendszerek biztonságos, hibatudatos használatát; valamint a jelentési és parancsnoki lánc torzításmentes működtetését. E készségek bármelyikének hiánya – még fejlett technikai infrastruktúra mellett is – gyorsan a védelem gyengüléséhez, súlyosabb esetben pedig működésképtelenséghez vezethet.

A hatékony működés alapját az egyértelműen dokumentált és rendszeresen validált eljárások adják, amelyek biztosítják, hogy a döntések ne improvizáción, hanem előre meghatározott és gyakorlatban is tesztelt folyamatokon alapuljanak. A Standard Operating Procedure dokumentumok intézményesítik azokat a működési folyamatokat, amelyek különböző helyzetekben meghatározzák a szükséges lépéseket és felelősségi köröket, ezzel minimalizálva az improvizációból eredő hibák lehetőségét. A szakirodalom hangsúlyozza, hogy a stabil és konzisztensen alkalmazott eljárásrend közvetlenül hozzájárul a működési ellenálló képesség növeléséhez, mivel csökkenti a bizonytalanságból eredő hibák előfordulását.

A szervezeti felépítés határozza meg, hogy a védelmi funkciók miként oszlanak meg az őrszolgálat, a beléptetés, a műszaki üzemeltetés, a reagáló erők és az irányítás között, és hogy a funkciók összhangja mennyire támogatja a működési rezilienciát.

²⁵ ADP 3-37: doktrína, amely meghatározza a védelem (*protection*) alapelveit, a fizikai védelem, erővédelem és veszteségminimalizálás eljárásrendjeit, valamint a műveletek folytonosságát biztosító szervezeti és technikai követelményeket.

A fizikai védelemben részt vevő alrendszerek – az őrszolgálatról és beléptetéstől kezdve a műszaki üzemeltetésen át a reagáló erőig és az irányítási struktúráig – csak akkor képesek hatékonyan működni, ha a feladat- és felelősségi körök egyértelműek, a kommunikációs utak pedig redundánsak és torzításmentesek. A riasztások, jelentések és parancsok áramlása gyakran a védelem legérzékenyebb pontját jelenti: a késedelem vagy információtorzulás gyorsan rontja a teljes rendszer teljesítményét.

A humán tényező nemcsak a végrehajtásban, hanem a helyzetértékelésben és a döntéshozatalban is fontos, különösen akkor, amikor a beérkező adatok hiányosak vagy ellentmondásosak. Bár a modern rendszerek egyre nagyobb szerepet szánnak az automatizált döntéstámogató megoldásoknak, az emberi ítélőképesség továbbra is nélkülözhetetlen, különösen összetett vagy bizonytalan helyzetekben. A kutatások egybehangzóan jelzik, hogy az automatizált rendszerek hatékonyan képesek támogatni, de nem tudják helyettesíteni az emberi megfontolást, különösen nem magas kockázatú döntési helyzetekben.

A folyamatos képzés és a rendszeres gyakorlatoztatás ezért nem adminisztratív teher, hanem a működési ellenálló képesség alapfeltétele. A gyakorlatok lehetőséget adnak a technikai rendszerek tesztelésére, a szervezet együttműködésének vizsgálatára és a reagálóképesség valós körülmények közötti értékelésére. A jól megtervezett és végrehajtott gyakorlatok rendszerint rávilágítanak a szervezet rejtett gyenge pontjaira, és értékes visszajelzést adnak a folyamatok finomhangolásához.

Mindezek alapján a fizikai védelem akkor tekinthető valóban működőképesnek, ha a műszaki rendszerek és a humán tényezők nem egymástól elkülönülten, hanem szerves módon, egymást erősítve vesznek részt a kritikus infrastruktúrák védelmében. A technológiai fejlődés csak akkor válik valós értékkel, ha a mögötte álló szervezet és állomány képes azt integrálni, értelmezni és a gyakorlatban is hatékonyan működtetni.

Összegzés

A katonai kritikus infrastruktúrák fizikai védelme olyan összetett, többszintű rendszerként értelmezhető, amelynek hatékonysága nem egyetlen komponens teljesítményétől, hanem a rendszer egészének összehangolt működésétől függ. A vizsgálatok és a gyakorlati tapasztalatok is azt mutatják, hogy a védelmi rendszer csak akkor működik megbízhatóan, ha a műszaki megoldások, az eljárási folyamatok és a humán tényezők egymást kiegészítve, összehangoltan járulnak hozzá a működéshez. A védelem hatékonysága emergens tulajdonság,²⁶ amelyet elsődlegesen az elemek közötti kapcsolatok minősége – például az illesztések, a reakcióidők vagy a döntéstámogatási folyamatok – határozza meg.

A fenyegetési környezet nemlineáris, nehezen előre jelezhető dinamikája – különösen a robbanóeszköz-alapú támadások, a hibrid módszerek és a pilóta nélküli rendszerek terjedése – elkerülhetetlenné teszi a többrétegű védelem következetes

²⁶ Emergens tulajdonság: olyan rendszerjellemző, amely az elemek kölcsönhatásából, nem pedig az elemek önálló tulajdonságaiból ered.

alkalmazását. A többrétegű védelmi logika mára a nemzetközi szabványok és doktrínák egyik alapvető, univerzálisan alkalmazott elvévé vált.

A szabályozási és doktrinális környezet világos keretet ad a fizikai védelem kialakításához, ugyanakkor a gyakorlati hatékonyság végső soron azon múlik, hogy ezek az elvek hogyan jelennek meg a konkrét rendszerekben, a szervezeti folyamatokban és a működési döntésekben. A védelmi architektúra valódi értékét az mutatja meg, hogy a szabványokban rögzített követelmények mennyire épülnek be a napi működésbe, és mennyire képesek iránymutatást adni egy gyorsan változó fenyegetési környezetben.

A technológiai fejlődés számos új lehetőséget nyit a védelem számára – legyen szó korszerű érzékelőkről, adatfúziós algoritmusokról vagy automatizált elemzőrendszerekről –, a gyakorlat azonban egyértelműen megmutatja, hogy ezek az eszközök önmagukban nem helyettesítik a fizikai védelem alapvető struktúráit. A stabil műszaki kialakítás, a szabályozott és jól dokumentált működési környezet, valamint a felkészült személyi állomány továbbra is a védelmi rendszer hatékonyságának legfontosabb meghatározói.

A fizikai védelem jövője ezért nem egyetlen technológiai megoldáson múlik, hanem azon, hogy a műszaki rendszerek, az informatikai háttér, a vezetésirányítás és a humán tényezők mennyire képesek egységes, alkalmazkodó és folyamatosan fejlődő rendszert alkotni. A hatékony védelem lényegében egy folyamatosan karbantartott és időről időre újragondolt struktúra, amelyben a mérés, az értékelés és az alkalmazkodóképesség együttesen biztosítja az ellenálló képesség fenntartását.

A fizikai védelem napjainkban nem tekinthető statikus vagy lezárt megoldásnak. Sokkal inkább dinamikus, életciklus-alapú biztonsági rendszerként értelmezhető, amely folyamatosan alkalmazkodik a környezeti változásokhoz. Fejlesztése nem csupán a szabványok követésén múlik, hanem azon is, hogy a szervezetek mennyire képesek a tapasztalatokat beépíteni és intézményesített tanulási folyamatokká alakítani.

A tanulmány egyik fő megállapítása, hogy a fizikai védelem hatékonyságát nem elsősorban az egyes technológiák fejlettsége, hanem az integráció minősége és a reagálási lánc időkritikus működése határozza meg.

Felhasznált irodalom

BALOGH Zsuzsanna (2010): Üveg az építészetben, a terrorista robbantások tükrében. *Műszaki Katonai Közlöny*, 20(1–4), 257–271.

EN 13541. *Security Glazing – Testing and Classification of Resistance Against Explosion Pressure* (2012).

FÖLDES Tibor (2025): A biztonság szerepe és fontossága a szövetségi kritikus infrastruktúra szabályozásának kialakításában. *Katonai Nemzetbiztonsági Szolgálat Szakmai Szemle*, 1, 146–163. Online: <https://ojs.knbsz.gov.hu/index.php/szakmai/article/view/234/130>

Joint Forward Operating Base Force Protection Handbook (2005).

- Kovács Zoltán (2012): Repülőterek védelme improvizált robbanóeszközök (IED) ellen. *Repüléstudományi Közlemények*, 24(2), 70–79. Online: www.repulestudomany.hu/kulonszamok/2012_cikkek/05_Kovacs_Zoltan.pdf
- Kovács Zoltán (2013): Repülőterek robbantások elleni védelmének technikai lehetőségei. *Repüléstudományi Közlemények*, 25(2), 78–88. Online: www.repulestudomany.hu/kulonszamok/2013_cikkek/2013-2-06-Kovacs_Zoltan.pdf
- Kovács Zoltán (2014): Repülőtéri létesítmények fizikai védelme IED ellen. *Repüléstudományi Közlemények*, 26(2), 106–113. Online: <https://folyoirat.ludovika.hu/index.php/reptudkoz/article/view/4602/3759>
- NATO Standardization Office (2024): *AJP-3.14. Allied Joint Doctrine for Force Protection. Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA 426)* (2011).
- U.S. Army (2009): *FM 3-37 Protection*.
- U.S. Army (2018): *ADP 3-37 Protection*.
- UFC 4-010-01. *DoD Minimum Antiterrorism Standards for Buildings* (2024). Whole Building Design Guide. Online: www.wbdg.org/dod/ufc/ufc-4-010-01
- UFC 4-010-02. *DoD Minimum Antiterrorism Standoff Distances for Buildings* (2020). Online: www.wbdg.org/dod/ufc/ufc-4-010-02

Jogi forrás

2024. évi LXXXIV. törvény a kritikus infrastruktúrák ellenálló képességéről

Szajkó Gyula,¹ Lévai Zsolt²

A közúti infrastruktúrák katonai megfelelőségi vizsgálata a logisztikai felderítés végrehajtásakor, 1. rész

The Military Suitability Assessment of Road Infrastructure During Logistical Reconnaissance, Part 1

Absztrakt

A közúti alágazat meghatározó szerepet tölt be az integrált közlekedési rendszerben, működtetése és fenntartása szintén lényeges a Magyar Honvédség (MH) számára, hiszen összekötő kapcsolatot biztosít a katonai szervezetek bázisai, a repülőterek, a tengeri és folyami kikötők, valamint a vasútállomások között. A csapatok haditechnikai eszközeinek és személyi állományának mozgatása – a kirakó pontok (tengeri, légi, vasúti kirakó pontok), valamint a fogadó, alkalmazási körlet között – közúton valósul meg, ráadásul a hadszíntéri közlekedés legnagyobb volumenét is a közúti szállítási feladatok teszik ki. Jelentőségét tovább növeli, hogy minősített időszakban a vasúti alágazatnál jelentkező kapacitáshiányt a közúthálózatnak kell pótolnia, úgy, hogy lehetővé tegye az ország mélységéből kiindulva a határszakaszok gyors elérését. Ennek megfelelően a közúti infrastruktúrák kapacitásadatainak gyűjtésére, valamint naprakész nyilvántartására a logisztikai szervezeteknek kiemelt figyelmet kell fordítaniuk a műveletek előkészítésekor és annak teljes időszakában is. Az információk célirányos felderítéséhez érdemes szemrevételezési szempontlistákat alkalmazni és a szempontokhoz követelményeket meghatározni. Ezzel az eljárással gyorsabban és hatékonyabban lehet kiértékelni a közúti infrastruktúrák kapacitásadatait, ami jelentős segítséget nyújthat az erők mozgatás-szállítási feladatainak tervezésekor és szervezésekor. A cikkben a szerzők célja,

¹ Tanársegéd, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Katonai Logisztikai Intézet, Hadtáp, Pénzügyi és Katonai Közlekedési Tanszék, e-mail: szajko.gyula@uni-nke.hu

² Adjunktus, Széchenyi István Egyetem, e-mail: levai.zsolt@sze.hu

hogyan a szemrevételezési szempontlistákhoz olyan követelményeket határozzanak meg, amelyeket alkalmazva gyorsítható és hatékonyabbá tehető a közúti alágazat katonai szempontú értékelése.

Kulcsszavak: logisztikai felderítés, közúti infrastruktúrák, megfelelőség, követelmények, szemrevételezés, szempontlisták

Abstract

The road transport sector plays an important role in the integrated transportation system, and its operation and maintenance are also significant for the Hungarian Defence Forces (HDF), as it provides a link between the bases of military units, airports, seaports and river ports, and railway stations. The movement of forces including military equipment, and personnel – between the unloading ports (sea, air, and rail) and the receiving operational areas – is carried out by road transport. Moreover, the largest volume of battlefield transport is carried out by road. Its importance is further increased by the fact that, during wartime, any capacity shortage in the railway sector must be compensated by the road network, enabling rapid access to border areas from the centre of the country. Accordingly, logistical organisations must pay special attention to the gathering and up-to-date maintenance of road infrastructure capacity during the preparation and the entire duration of operations as well. For the targeted collection of information, it is advisable to use checklists and to define requirements for each criterion. This procedure allows for a faster and more efficient assessment of road infrastructure capacities, which can provide significant support in planning and organising the movement and transportation of forces. Therefore, the aim of this article is to define requirements for checklists that can enhance the efficiency and speed of military assessment of road infrastructure.

Keywords: logistical reconnaissance, road infrastructures, adequacy, requirements, site survey, checklists

Bevezetés

Napjainkban több katonai konfliktus is zajlik a világban, amelyekben a közlekedési rendszer meghatározó szerepet tölt be a haderők felvonulásában és a katonai szállítási feladatok végrehajtásában. Példaként lehet említeni a műveletek előkészítéseként a NATO RSOM³-feladatokat, mivel általuk valósulnak meg az erők fogadása, állomásoztatása és előre mozgatása,⁴ vagyis a személyek és eszközök átcsoportosítása.

A közúti infrastruktúrák lényeges részét képezik az integrált közlekedési rendszernek, működtetése és fenntartása az MH számára is kulcsfontosságú, hiszen összekötő

³ Reception, staging, onward movement – erők fogadása, állomásoztatása és előre mozgatása.

⁴ Az RSOM-műveletek legfontosabb célja, hogy a feladatok végrehajtására kijelölt erők az összhaderőnemi parancsnok követelményeinek figyelembevételével a megfelelő időben, a megfelelő helyre, a megfelelő állapotban érkezzenek meg, majd hatékony támogatásukkal a személyek és eszközök elérjék a teljes műveleti képességet. HORVÁTH 2018.

kapcsolatot biztosít a katonai szervezetek bázisai, a repülőterek, a tengeri és folyami kikötők, valamint a vasútállomások között. A csapatok haditechnikai eszközeinek és személyi állományának mozgatása – a be- és kirakó pontok (tengeri, légi, vasúti be- és kirakó pontok), valamint a fogadó, alkalmazási körlet között – alapvetően közúton valósul meg, ehhez párosul továbbá, hogy a hadszíntéri közlekedés legnagyobb volumenét is jellemzően a közúti szállítási feladatok teszik ki. Ráadásul minősített időszakban a vasúti alágazatnál jelentkező kapacitáshiányt a közúthálózatnak kell pótolnia úgy, hogy lehetővé tegye az ország mélységéből kiindulva (a fő irányokban 5-6 ezer jármű/nap, míg haránt irányokban 3-4 ezer jármű/nap átbocsátó képességgel) a határszakaszok gyors elérését.⁵ Elmondható, hogy a közúti szállítási igény szignifikánsan jelenik meg mind a békeidőszaki katonai, mind a különleges jogrendi feladatok végrehajtásakor. Ennek megfelelően a közúti alágazat kapacitásadatainak összegyűjtésére és annak naprakész nyilvántartására figyelmet kell fordítania a műveletek logisztikai támogatását tervező, szervező és végrehajtó katonai szervezeteknek. Az adatok feltérképezéséhez célszerű szemrevételezési szempontlistákat alkalmazni, hogy minden lényeges információra kitérjenek a logisztikai felderítést végző személyek.

A közúti infrastruktúrák katonai értékelésének gyors és eredményes végrehajtását segítheti továbbá, ha a szemrevételezési szempontokhoz követelményeket is meghatározunk. Ennek megfelelően a feladatlistákkal és a hozzájuk kapcsolódó követelményekkel el lehet végezni a közúthálózatok megfelelőségi vizsgálatát, így eredményesebbé lehet tenni az erők mozgatás-szállítási feladatainak tervezését. A hazai katonai szabályzók azonban nem részleteznek szemrevételezési listákat és a szempontokhoz tartozó követelményeket sem. Ennek megfelelően a fő célkitűzésünk, hogy kidolgozzuk a közúti infrastruktúrára vonatkozó azon követelményeket, amelyeket hozzá lehet rendelni a szemrevételezési szempontlistákhoz. A cikkben szereplő feladatlistával, valamint a meghatározott követelményekkel növelni lehet a műveletek logisztikai támogatás (azon belül a közlekedési támogatási feladatok) tervezésének és végrehajtásának hatékonyságát is.

A követelmények meghatározására alkalmazott módszer

A tanulmányban összesen 4 fő infrastruktúra-elem szempontrendszerét mutatjuk be. A táblázatokba foglalt közutak elemeit (útpálya, csomópont, műtárgy, útpálya környezete) külön szükséges pontozni, súlyozni és értékelni. Ez abból adódik, hogy például egy útpálya adott szakasza megfelelő lehet a haditechnikai eszközök közlekedtetésére, és magasabb pontszámokkal értékelhetjük, ugyanakkor elképzelhető, hogy a vonalra épített műtárgy csak korlátozottan használható a katonai járművek számára, amelyhez kevesebb pontszámot rendelünk. Az egyes elemek súlyozott pontjainak összege (amennyiben együtt értékeljük azokat) olyan eredményre vezethet, amelynél a vizsgált útszakaszt alkalmasnak ítéljük a haditechnikai eszközök közlekedtetésére. Ez akkor jelent problémát, ha a műtárgyak pontszámai alapján azt az eredményt kapjuk, hogy csak korlátozottan lehet használni a katonai járművek számára

⁵ PÓCSMEGYERI 2003.

az infrastruktúra-elemet, ugyanakkor az egész útszakasz együttes pontszáma szerint a korlátozás nélkül használható minősítést kapja. Ezért mindenképp szükséges külön vizsgálni a súlyozás szerint az egyes elemeket és azok alapján összefoglaló értékelést állítani össze. A táblázat követelményeihez rendszerint 0,5, 1, illetve 1,5 pontértékeket rendeltünk, amelyek közül a magasabb pontszám a haditechnikai eszközökkel történő közlekedés nagyobb mértékű megvalósíthatóságát jelzi. A cikk első részében elsőként az útpálya és a csomópont követelményeit ismertetjük, majd ezt követi az értékelésükre meghatározott módszertan bemutatása.

A közúti infrastruktúrák logisztikai felderítéséhez használható szempontlista

A cikkben szereplő szempontlista már elemezve lett egy korábban írt értekezésben⁶ és egy publikációban,⁷ ezért a szempontoknál csak a kialakított követelmények részletezésére térünk ki. A kritériumok meghatározásához elsősorban figyelembe vettük a NATO által kiadott *Criteria and Standards for the Zones of the Reinforcement and Sustainment Network*⁸ című dokumentumot, valamint a Bizottság (EU) 2021/1328 a kettős felhasználású infrastruktúrával kapcsolatos intézkedések egyes kategóriáira alkalmazandó infrastrukturális követelmények meghatározásáról című végrehajtási rendeletét. Az általunk kidolgozott listában 4 fő szemponthoz (útpálya, csomópontok, műtárgyak, útpálya környezete) határoztunk meg követelményeket (1. táblázat).

A megengedett legnagyobb sebességnél (5. pont) a 30 km/h-tól az 50 km/h-ig határérték az adott útszakaszra előírt (amennyiben érvényben van ilyen) korlátozásra vonatkozik, amelyet minden közlekedő járműnek be kell tartania. A magasabb pontszám ennél a szempontnál azt jelenti, hogy a menetet tervező és szervező személyeknek lehetőségük van az 50 km/h-nál nagyobb sebességet meghatározni, mivel egyéb, a forgalmat lassító, befolyásoló vagy akadályozó tényező nem fog jelentkezni az útpályán. Ugyanakkor a konvojok menetére hatással lehet a túlméretes és túlsúlyos eszközök szállítása, mozgatása. A 36/2017. (IX. 18.) NFM rendelet alapján a főbb közlekedési feltételek között szerepel, hogy például 2,6 m szélesség és 12 m hosszúság felett rendelkező járművek az autópályán maximum 80 km/h-val, lakott területen kívül 70 km/h-val, míg lakott területen belül 50 km/h-val közlekedhetnek.⁹ Ebből adódik, hogy az adott útszakaszra előírt korlátozásokon kívül más tényezőket is szükséges figyelembe venni a közúti menetek tervezésekor.

⁶ SZAJKÓ 2025.

⁷ SZAJKÓ 2019.

⁸ ACO Directive 084-004.

⁹ A 36/2017. (IX. 18.) NFM rendelet és a Magyar Közút Nonprofit Zrt. Általános tájékoztató (2025) szerint meghatározott adatok alapján.

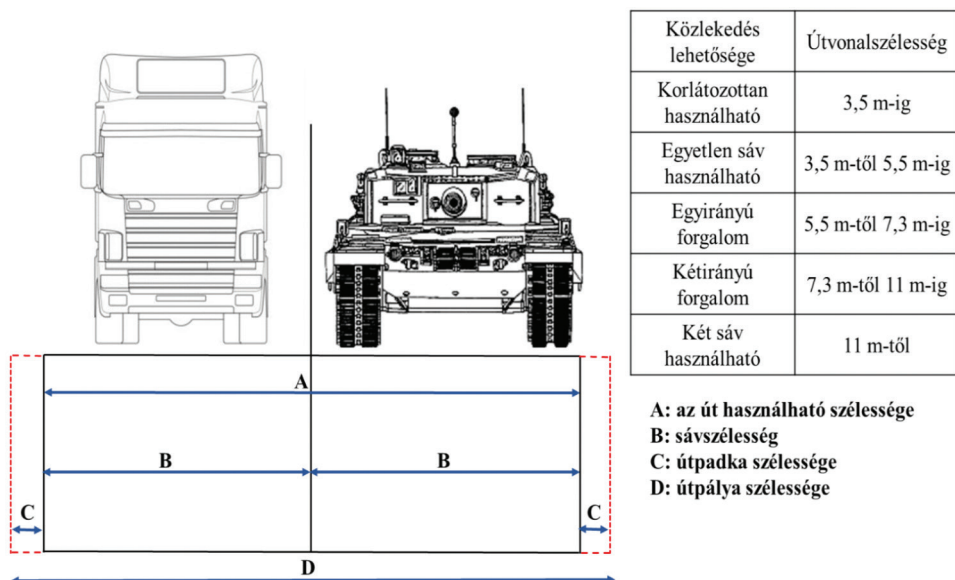
1. táblázat: Az útpálya szempontjai és a hozzájuk rendelt követelmények

Fsz.	Szempontok	Megjegyzés	
Alapadatok			
1.	Szemrevételezés időpontja	x	
2.	Időjárási körülmények	x	
3.	Az útszakasz útosztálya (például elsőrendű főútvonal)	x	
4.	Az útszakasz hálózati jelölése, száma (például M3)	x	
Részletezett adatok			
5.	Megengedett legnagyobb sebesség súlyozás: 1x	30–50 km/h	1 pont
		50 km/h ≤ 50	1,5 pont
6.	Az útpálya burkolatszélessége súlyozás: 2x	3,5–5,5 m	0,5 pont
		5,6–7,2 m	1 pont
		7,3 m ≤	1,5 pont
7.	A pálya tengelyterhelése súlyozás: 2x	< 12,23 t/tengely	1 pont
		= 12,23 t/tengely	1,5 pont
8.	Az útpálya minősége, az időjárás hatása a közlekedésre súlyozás: 2x	Z típus	0,5 pont
		Y típus	1 pont
		X típus	1,5 pont
9.	A pálya forgalmi sávjainak száma (egy forgalmi irányba) súlyozás: 2x	egypályás út	0,5 pont
		egy forgalmi sáv	1 pont
		két forgalmi sáv vagy több	1,5 pont
10.	A forgalomtechnikai elemek minimális távolsága a burkolat szélétől (például zajvédő falak, vezetőoszlopok, szalagkorlátok) súlyozás: 1x	≤ 1,5m	1 pont
		1,5m ≤	1,5 pont
11.	A pályán meglévő akadályok fajtája és megszűnésének várható időpontja (például burkolatjavítás, burkolathiba, átfolyás) súlyozás: 1x	30 nap ≤	0,5 pont
		14–30 nap	1 pont
		14 nap ≤	1,5 pont
12.	A pályán meglévő akadályok koordinátái	x	
13.	Az akadály forgalomra gyakorolt hatásának mértéke (például teljes pálya, egy sáv) súlyozás: 1x	nagy hatás	0,5 pont
		közepes hatás	1 pont
		kis hatás	1,5 pont
14.	A pályán érvényben lévő korlátozások (például behajtási tilalmak) és a forgalomra gyakorolt hatásának mértéke súlyozás: 1x	nagy hatás	0,5 pont
		közepes hatás	1 pont
		kis hatás	1,5 pont
15.	Az adott útszakaszon leközlekedhető maximális jármű szerelvényhosszúsága súlyozás: 2x	≤ 18,75m	1 pont
		18,8–27,5m	1,5 pont

Forrás: a szerzők szerkesztése

A második szempontnál az útpálya burkolatszélességére 3 db – a méterekre vonatkozó – intervallumot határoztunk meg. A szemponthoz tartozó információk begyűjtésére

azért is van szükség, mert a burkolatszélesség befolyásolhatja a forgalmi irányokat és az egy irányban használható sávok számát. A speciális – túlsúlyos és túlméretes – katonai járművek (például harcjárművek, szállító járművek) részére különösen fontos, hogy megfelelő szélességű és teherbírású útpálya álljon rendelkezésre a technikai eszközök biztonságos közlekedéséhez. A NATO már 2004-ben kiadott egy egységesítési egyezményt a katonai közúti közlekedés és forgalomirányításra vonatkozóan, amely segítséget nyújtott az utak szélesség szerinti osztályozásához és az e szemponthoz tartozó intervallum meghatározásához.¹⁰ A 1. ábra – a NATO-dokumentummal összhangban – az útpálya szélesség szerinti osztályozását mutatja be.



1. ábra: Az utak szélességére és forgalomáramlására alkalmazható méretek

Forrás: a szerzők szerkesztése AMovP-1(A) alapján

Az 1. ábrában szereplő adatokból kiindulva a kerekes gépkocsik részére (például a Kraz-255 terepjáró gépjármű szélessége 2,75 m) minimum 3,5 m, míg a láncalpas, túlméretes haditechnikai eszközök részére (például a Leopard 2A7 harcjármű szélessége 4 m) legalább 5,5 m sáv szélesség szükséges az akadálymentes haladáshoz a közutakon. Az 1. ábrában szereplő adatok alapján, ha a burkolatszélességnek 3,5 és 5,5 m-t állapít meg a szemrevételező csoport, akkor 0,5 pontot célszerű rendelnie a szemponthoz, mivel a hasonló útszakaszt csak korlátozott mértékben lehet használni a haditechnikai eszközök közlekedtetésére. Az 5,5 m-től szélesebb útpályát (5,6–7,2 m-ig) már 1 ponttal, míg 7,3 m fölött 1,5 ponttal érdemes értékelni.

A pálya tengelyterhelésével kapcsolatban az információk begyűjtésekor figyelembe kell venni a nemzeti szintű szabályozásokat is. A magyarországi eljárásrendeket figyelembe véve a 36/2017. (IX. 18.) NFM rendelet határozza meg, mely járművek

¹⁰ AMovP-1(A) 2004.

minősülnek túlsúlyos vagy túlméretes eszközöknek. A táblázatban olyan határértékeket választottunk, amelyek igazodnak a nemzeti rendelethez és a korábban már említett kettős felhasználású infrastruktúrákkal szembeni követelményekhez. Ennek megfelelően 1 pontot lehet rendelni a 12,23 t/tengely maximális tengelyterhelésű járművek engedélyezett közlekedésére, míg 1,5 pontot, ha ennél nagyobb kategóriájú járművek közlekedése is biztosított az útpályán. Természetesen ezeknek az eszközöknek az alkalmi mozgásaihoz különleges engedélyekre vagy mentességekre, valamint megfelelő kockázatcsökkentő intézkedésekre is szükség lehet, amelyeket az adott ország kivételes jelleggel jogszabályokban határozhat meg.

Az útpálya minőségének, járhatóságának vizsgálata során az útvonalakat három csoportba lehet sorolni, amelyek a következők:

- X típus: az utakat időjárási viszonyoktól függetlenül lehet használni, megfelelő karbantartás mellett egész évben járható akkora forgalom számára, amely megfelel az út maximális átbocsátóképességének, továbbá felszíne vízálló, így az eső, a fagy, az olvadás és a meleg csak kis mértékben hat rájuk. Ennek megfelelően 1,5 pontot célszerű rendelni a szemponthoz, mivel az időjárási körülmények csak kis mértékben befolyásolják a technikai eszközök adott útszakaszon történő közlekedtetését.
- Y típus: jellemzői, hogy korlátozott időjárási viszonyok között használható, időnként a forgalom mennyisége lényegesen kevesebb a maximális átbocsátóképességnél, az utak felszíne nem vízálló, ezért az eső, a fagy, az olvadás és a meleg erősen hatnak rájuk, ebből következik, hogy kedvezőtlen időjárási körülmények miatt rövid ideig lezárhatják. Ehhez a szemponthoz érdemes 1 pontot adni, amennyiben csak korlátozott mértékben lehet használni az útszakaszt a környezeti hatások miatt.
- Z típus: csak jó időjárási viszonyok között használható, a kedvezőtlen körülmények miatt hosszabb ideig lezárhatják, és javításuk kizárólag át-, illetve újjáépítéssel valósítható meg. Ennek megfelelően célszerű a táblázatban csak 0,5 pontot adni a szemponthoz.¹¹

A pálya forgalmi sávjainak vizsgálatához (9. pont) három jellemzőt határoztunk meg. Az egy irányba kialakított egypályás úthoz 0,5 pontot rendeltem, mivel itt nagy valószínűséggel csak korlátozással lehet közlekedni (a haditechnikai eszközökkel) a menetek végrehajtásakor. Az egy forgalmi sávós útszakasznál már 1 pont szerepel a táblázatban, ugyanis – a forgalmi tényezőket figyelembe véve – ezen az útszakaszon (az előző szemponthoz képest) kedvezőbb feltételekkel lehet haladni a járműveknek. A két vagy több forgalmi sávós útpályát továbbá 1,5 ponttal célszerű értékelni, amennyiben biztosított a konvojok számára – egy forgalmi irányban – akár több sáv használata is, ennek megfelelően például a túlméretes eszközöknek elegendő tér áll rendelkezésükre a közlekedéshez, a menetrendben szereplő járművekkel könnyebben végrehajtható a polgári gépkocsik előzése, vagy tartható a parancsnok által meghatározott menetsebesség.

¹¹ AMovP-1(A) 2004: 39.

A forgalomtechnikai elemek burkolat szélétől való távolságának megállapítása fontos abból a szempontból, hogy a felderítő csoport információkat gyűjtsön azokról „az út menti” elemekről is, amelyek befolyásolhatják – a vizsgált útszakaszon – a konvojok biztonságos továbbhaladását. Amennyiben ez a távolság 1,5 méternél¹² kevesebb, úgy 1 pontot, míg az ezt meghaladó értékhez 1,5 pontot érdemes rendelni.

A pályán meglévő akadályok szintén hatással lehetnek a menetek tervezésére, szervezésére és időbeni végrehajtására. Az adatok elemzésekor szükséges arra kitérni, hogy például hol alakultak ki az útpályán burkolathibák, és mikorra várható a megszüntetésük. Az értékeléshez támpontként adtuk meg, hogy a 30 napnál tovább fennmaradó akadályokhoz 0,5 pontot, a 14 és 30 nap között meglévőhöz 1, míg az ennél rövidebb ideig maradó „gátló tényezőkhöz” 1,5 pontot célszerű adni. Azonban fontosnak tartjuk megjegyezni, hogy a 10. és a 11. szemponthoz csak 1x-es súlyozást határoztunk meg, mivel ezek a tényezők kisebb mértékben befolyásolhatják a közlekedést, mint például a táblázat 6. és 9. pontja közötti jellemzők.

Az akadályokkal kapcsolatban fontos lehet információt gyűjteni arról is, hogy milyen mértékű hatást gyakorol a forgalomra. Amennyiben az útpálya teljes sávját érinti, és ezáltal nagymértékben befolyásolja a közlekedés, úgy 0,5 ponttal, közepes és kis hatásnál 1, valamint 1,5 ponttal érdemes értékelni a vizsgált útszakaszt. Azonban felmerülhet, hogy a felderítő csoport szubjektíven értékelheti az útpályát, mivel ehhez a szemponthoz nem alakítottunk ki előre meghatározott határértékeket. Itt a szemrevételező állománynak azt szükséges vizsgálnia, hogy a menetrendbe sorolt járművek el- vagy át tudnak-e haladni sérülés nélkül az akadályon, vagy ez csak műszaki előmunkálatok elvégzése után valósítható meg. Az erre vonatkozó információt (a döntés megalapozottsága érdekében) mindenképp szükséges feltüntetni a táblázat megjegyzés rovatában.

A következő szempont azokra a korlátozásokra tér ki, amelyeket a közlekedési hatóságok alakítottak ki, és az időtartamuk állandónak tekinthető (például a behajtási tilalmak). A meghatározott követelmények súlyozásához szintén 1x-es szorzót alkalmaztunk, mivel ezek a „forgalmi intézkedések” is kisebb mértékben befolyásolhatják a haditechnikai eszközök közlekedését. Például egy adott útszakaszra kihelyezett behajtani tilos jelzés feloldható a forgalom irányítására jogosultak (a rendőrség, valamint a katonai rendész általi együttműködés alapján) intézkedésén keresztül.¹³ Ezzel szemben, ha az útpálya burkolatszélessége nem éri el a 3,5 m-t, úgy a menetek végrehajtása sokkal nagyobb nehézséget jelent (nagy hatást gyakorol) az alegységek részére, mint akkor, ha csak az előzőekben említett korlátozásokat alkalmaznak az adott útszakaszon. A szempontnál azt érdemes vizsgálni, hogy a közlekedésre milyen hatást gyakorolnak a létesített forgalomszabályozási intézkedések, ennek megfelelően sorrendben 0,5, 1, illetve 1,5 pontot célszerű adni a kis, a közepes és a nagy hatást kiváltó korlátozásokra.

Az adott útszakaszon leközelekedtethető maximális járműszerelvénnyel hosszúságára vonatkozó méretek fontosak abból a szempontból, hogy pontos adatokkal tervezzenek

¹² Az 1,5 m határértéket az útügyi műszaki előírás alapján határoztuk meg, amely általánosságban értendő; ez a távolság az útosztály besorolása szerint változhat (például a gyorsforgalmi utaknál az útpadkától minimum 2,5 m-re létesíthető zajárnyékoló fal). Magyar Közút Nonprofit Zrt. 2024.

¹³ 1/1975. (II. 5.) KPM–BM együttes rendelet a közúti közlekedés szabályairól.

a katonai szervezetek, információkat kapjanak arról, hogy milyen engedélyezési és szabályozási eljárásrend vonatkozik a túlméretes járművekre. A haditechnikai eszközök (például a Leopard 2A7+) közúti vontatásakor a járművek együttes szerelvényhosszúsága (vontató + a harckocsit szállító pótkocsi) elérheti a 24 m-t. Ebből is adódik, hogy az EU 2021/1328 számú rendeletében meghatározzák a tagállamok számára, hogy a közúti infrastruktúrák igénybevételekor biztosítaniuk kell a 18,75 m és a 27,5 m közötti szerelvényhosszúsággal rendelkező járművek közlekedtetését.¹⁴ Ennek megfelelően a követelményeknél 1 pontot rendeltünk a (külön intézkedés nélkül) 18,75 m-ig közlekedhető eszközökhöz, míg az ennél nagyobb méretekkal rendelkező (amelyek korlátozás nélkül mozoghatnak az útpályán) járművekhez 1,5 pontot határoztunk meg. Az értékeléskor szintén szükséges elemezni azt, hogy a hatóságok milyen engedélyezési eljárásrendet határoznak meg a túlméretes eszközökre.¹⁵ Amennyiben például a kérelmek benyújtását követően a járművek közlekedése a kijelölt útszakaszon lehetségessé válik, a szemponthoz tartozó kritériumot 1,5 ponttal célszerű értékelni.

A csomópont forgalmi irány szerinti sávszáma jelentősen befolyásolja a kereszteződés átbocsátó képességét és a forgalom szervezhetőségét. Minél több sáv áll rendelkezésre egy irányban, annál könnyebben lehet kezelni a konvojok közlekedését, a sávváltásokat és az irányváltoztatásokat. Az egysávos irányt 0,5 ponttal célszerű értékelni, mivel jellemzői közé tartozhat, hogy a forgalom torlódásra hajlamos, alacsony kapacitással rendelkezhet és a sávváltások nehezen kivitelezhetők. A kétsávos csomópont 1 pontot rendeltünk, amelyről általánosságban elmondható, hogy nagyobb kapacitással rendelkezik, és biztosított a lehetőség a konvojok párhuzamos haladására, sávváltására.

A három vagy több sávval rendelkező csomópontot várhatóan magas kapacitás, viszonylag rugalmas forgalomszervezés jellemzi, ahol egyszerre több jármű könnyen közlekedhet, és a sávváltások, valamint az irányváltoztatások is gyorsabban végrehajthatók. Ennek megfelelően 1,5 pontot rendeltünk a kritériumhoz. A szempontot figyelembe véve a súlyozásához 2x-es szorzót alkalmaztunk, mivel a csomópont átbocsátóképességét jelentősen befolyásolhatja a sávok kialakítása.

A csomóponti ágak útosztálya meghatározó szerepet tölt be a csomópont funkcionális besorolásában, forgalmi terhelésében és hálózati jelentőségében. A magasabb rendű úthálózati elemekhez kapcsolódó csomópontok jellemzően nagyobb forgalmi volumen kezelésére alkalmasak, valamint lényegesek a térségi és országos forgalmi kapcsolatok biztosításában. A 2. táblázatban az egyéb utakat 0,5 ponttal értékeltük, mivel ezek a csomópontok alapvetően alacsonyabb forgalmi igénybevételre alkalmasak és korlátozott hálózati szereppel, valamint kisebb geometriai méretekkal rendelkeznek.

A 2. táblázatban a csomópont 6 követelményt határoztunk meg.

¹⁴ A Bizottság (EU) 2021/1328 végrehajtási rendelete.

¹⁵ A 36/2017 (IX. 18.) NFM rendelet írja le például hazai viszonylatban a túlsúlyosnak és túlméretesnek minősülő járművek közlekedésének szabályait.

2. táblázat: A csomópont szempontjai és a hozzájuk rendelt követelmények

Fsz.	Szempontok	Megjegyzés	
Alapadatok			
Csomópontok			
16.	Csomópont típusa (például közúti vagy vasúti)	x	
17.	A közúti csomópont fajtája (szintbeni, körforgalom vagy külön szintű)	x	
18.	Csomópont helye, földrajzi koordinátái	x	
19.	Forgalom irányításának fajtája (például jelzőlámpás)	x	
20.	Csomópont ágainak száma	x	
21.	Csomópont forgalmi irány szerinti sávszáma súlyozás: 2x	egysávos	0,5 pont
		kétsávos	1 pont
		háromsávos v. több	1,5 pont
22.	Csomóponti ágak útosztályai súlyozás: 2x	egyéb utak	0,5 pont
		másodrendű főút-vonal	1 pont
		elsőrendű főút-vonal	1,5 pont
23.	A csomópont minimális kanyarodási ívsugara (például a körforgalom ívsugara) súlyozás: 2x	< 12,5m	1 pont
		12,6 ≤	1,5 pont
24.	Csomópontban elhelyezett elemek típusa, méretei (például növényzet, körforgalom közepén elhelyezett díszítő elemek stb.) hatása a forgalomra súlyozás: 1x	nagy hatás	0,5 pont
		közepes hatás	1 pont
		kis hatás	1,5 pont
25.	A csomópont környezetében elhelyezett, a metrvonalat érintő egyéb elemek elhelyezkedése (például épület minimális távolsága az útpályától) hatása a forgalomra súlyozás: 1x	nagy hatás	0,5 pont
		közepes hatás	1 pont
		kis hatás	1,5 pont
26.	A csomópont igényel-e katonai forgalomirányítást? Igen/Nem	igen	1 pont
		nem	1,5 pont

Forrás: a szerzők szerkesztése

A következő kritériumhoz 1 pontot rendeltünk, amelynek fő jellemzői közé tartozik, hogy az egyéb utakhoz képest nagyobb forgalmi terhelést bonyolítanak le, és fontos szerepet töltenek be a térségi összeköttetések biztosításában. Az elsőrendű főútvonalak

már 1,5 pontot kapnak a táblázatban, figyelembe véve azt tényezőt, hogy ezek a csomópontok forgalmilag jelentősek, nagy átbocsátóképességgel és akár országos hálózati szerepkörrel is rendelkezhetnek. A szemponthoz szintén kétszeres súlyozást alkalmaztunk, mivel az útosztály determinálhatja a csomópont forgalmi működését és jelentőségét.

A következő szempontnál (23. pont) az infrastruktúra-elem minimális kanyarodási ívsugara – például körforgalom esetén a középmezőhöz tartozó ívsugár – alapvetően meghatározza a csomópont forgalomtechnikai működését, a járművek áthaladási sebességét, valamint a túlméretezett és túlsúlyos járművek biztonságos és akadálymentes közlekedését. A kisebb ívsugarú csomópontok elsősorban forgalomcsillapító hatásúak, ugyanakkor korlátozottabb kapacitással rendelkeznek, és kevésbé alkalmasak nagyobb forgalmi volumen vagy nehézgépjármű-forgalom kezelésére. Ennek megfelelően – figyelembe véve a Bizottság (EU) 2021/1328 végrehajtási rendeletét – a 12,5 m-nél kisebb minimális ívsugárral rendelkező infrastruktúra-elemek 1 pontot kaptak, mivel ezek elsősorban helyi jelentőségű, alacsonyabb sebességű és kisebb forgalmi terhelésű csomópontként funkcionálnak. A 12,6 m fölötti ívsugár-méret már kedvezőbb geometriai kialakítást biztosít, ami lehetővé teszi a nagyobb járművek biztonságosabb irányváltoztatását, áthaladását, valamint javítja a csomópont átbocsátóképességét, és mérsékli a torlódás kialakulásának kockázatát. Ezért ezt a szempontot 1,5 ponttal értékeltük. A kritériumhoz 2-es szorzót rendeltünk, mivel a geometriai kialakítás – különösen az ívsugár – hatással van a csomópont forgalmi teljesítményére és funkcionális besorolására.

A csomópontban elhelyezett elemek típusa és mérete – például növényzet, burkolt vagy épített díszítőelemek, műtárgyak, illetve a körforgalom közepén kialakított központi elemek – jelentős hatással lehet az infrastruktúra-elem forgalmi működésére, a járművezetők észlelésére, valamint a közlekedésbiztonságra. Ezek az elemek befolyásolhatják a beláthatóságot, a tájékozódást, továbbá pszichológiailag hatással lehetnek a járművek sebességválasztására és a forgalmi döntésekre. A pontozási rendszer kialakításánál fontos szempont volt, hogy az egyes kategóriák megnevezései (nagy, közepes, kis) nem a kedvező hatást, hanem az adott elemek forgalomra gyakorolt negatív befolyásának mértékét tükrözik. Azok a csomópontok, ahol az elhelyezett elemek nagymértékben korlátozzák a beláthatóságot, elvonják a járművezetők figyelmét vagy akadályozzák a forgalmi mozgásokat, 0,5 ponttal célszerű értékelni. Amennyiben az elhelyezett elemek közepes mértékű hatást gyakorolnak a forgalomra, úgy azok már kedvezőbb megítélés alá esnek, és 1 pontot kapnak. Továbbá, ha az infrastruktúra-elemben létesített természetes tereptárgyak vagy mesterséges létesítmények mérete és kialakítása minimális mértékben befolyásolja a forgalmi viszonyokat, nem rontja a beláthatóságot, és harmonikusan illeszkedik a csomópont geometriai kialakításához, akkor érdemes 1,5 pontot adni a kiértékeléskor. A követelmény 1-es súlyszorzója azt tükrözi, hogy az említett elemek hatása fontos, ugyanakkor a geometriai és forgalmi alapparaméterekhez képest kisebb jelentőségű a csomópont összesített értékelése során.

A csomópont közvetlen környezetében elhelyezkedő, a menetvonalhoz kapcsolódó egyéb elemek – például az útpályához közel álló épületek, térfalak, kerítések vagy egyéb fix létesítmények – elsősorban a csomópont térbeli kialakítását és használhatóságát befolyásolják. Ezeknek az elemeknek az elhelyezkedése hatással lehet a járművek mozgásterére, a rendelkezésre álló oldaltávolságra, valamint a csomópont áttekinthetőségére, ezáltal közvetetten a forgalom biztonságára és folyamatosságára is. A túlzottan közeli környezeti beépítés szűkítő hatást eredményezhet, amely növeli a vezetői terhelést és a konfliktushelyzetek kialakulásának valószínűségét. A pontozás során a „nagy hatás” kategóriába azok az esetek kerültek, ahol a környező elemek elhelyezkedése jelentősen befolyásolja a forgalmi viszonyokat – például az épületek minimális oldaltávolsága korlátozza a beláthatóságot vagy szűkíti a menetvonalat –, ezért ezek 0,5 pontos értékelést kaptak. A „közepes hatás” kategória azon csomópontokat foglalja magában, ahol a környezeti elemek ugyan érzékelhető módon hatnak a forgalomra, de nem okoznak számottevő működési vagy biztonsági problémát; ezért ezekhez 1 pontot rendeltünk a táblázatban. A forgalomra gyakorolt „kis hatás” azoknál a csomópontoknál jelentkezik, ahol a környező elemek megfelelő távolságban helyezkednek el az útpályától, nem korlátozzák a beláthatóságot és nem befolyásolják érdemben a forgalmi mozgásokat, így ezek a legkedvezőbb, 1,5 pontos értékelést kapták. A kritérium 1-es súlyszorzója azt jelzi, hogy a környezeti elemek elhelyezkedése fontos szempont a csomópont értékelése során, ugyanakkor hatása mérsékelt, például a sávszámokhoz vagy az ágak útosztályához képest.

Amennyiben a csomópont katonai forgalomirányítási igénye fennáll, az olyan speciális üzemeltetési és funkcionális sajátosságra utal, amely túlmutat a hagyományos közúti forgalomszervezési megoldásokon. Azok a csomópontok, ahol katonai forgalomirányítás válik szükségessé, jellemzően időszakos vagy rendkívüli forgalmi helyzetek alakulhatnak ki, például a katonai konvojok áthaladása, haditechnikai eszközök mozgatása miatt. Ezek a helyzetek a közúti forgalom ideiglenes korlátozásával, sebességcsökkentéssel vagy a forgalmi rend megváltoztatásával járhatnak, ami csökkenti a csomópont általános forgalmi hatékonyságát.

Amennyiben a csomópont igényel katonai forgalomirányítást, úgy célszerű 1 ponttal értékelni az infrastruktúra-elemet, mivel az ilyen beavatkozások rendszerint a normál forgalmi működés korlátozását és többletüzemeltetési igényt jelentenek. Azok a csomópontok, amelyek nem igényelnek katonai forgalomirányítást, stabilabb, kiszámíthatóbb forgalmi viszonyokat biztosítanak, ezért 1,5 pontot kapnak a táblázatban. A kritérium 1-es súlyszorzója azt fejezi ki, hogy bár ez a szempont nem minden csomópont vizsgálata során releváns, ahol megjelenik, ott érdemi hatással lehet a csomópont működésére és összesített megítélésére.

A szempontlista és a meghatározott követelmények alapján gyűjtött adatok kiértékelése

A szemrevételezési szempontlista követelményeihez előre definiált, diszkrét pontértékeket rendeltünk (0,5, 1 és 1,5 pont), amelyek az adott jellemző katonai, forgalmi és/vagy geometriai megfelelőségét fejezik ki. A pontértékekhez kapcsolódó súlyozást (1x vagy 2x) úgy alakítottuk ki, hogy a szempontok egymáshoz viszonyított jelentőségét tükrözze. Ezek alapján elsőként az összpontszámot határoztuk meg, amely a következőképpen számolható ki:

$$P = \sum_{i=1}^n p_i \times w_i$$

- p_i az i -edik értékelési szempont pontértéke (0,5, 1, 1,5 pont),
- w_i az i -edik szempont súlyszorzója (1x vagy 2x),
- n az értékelési szempont száma.

A képletet használva a legfontosabb paraméterek (például az útpályánál a burkolat-szélesség jellemzői) kiemelt szerepet kapnak az összesített értékelés során. A kapott összpontszámok értelmezése nem abszolút küszöbértékek alapján történik, hanem a teljes mintára jellemző ponteloszlás statisztikai jellemzőinek figyelembevételével. Ennek során az összpontszámok átlagát és szórását határoztuk meg, amely lehetővé teszi az infrastruktúra-elemek besorolását és összehasonlítását. Az infrastruktúra-elemek (az útpálya és a csomópont) alkalmassági kategóriáit az átlag környezetében, a szórás figyelembevételével jelöltük ki, amelyhez az alábbi képleteket használtuk:¹⁶

$$\sigma = \sqrt{\frac{\sum_{i=1}^k f_i \times (x_i - \bar{x})^2}{\sum_{i=1}^k f_i}}$$

ahol:

- x_i az i -edik adatérték a vizsgált adathalmazban;
- $\bar{x}$ az adatok számtani átlaga;
- f_i az i -edik adatérték előfordulásának száma;
- $\sum_{i=1}^k f_i \times (x_i - \bar{x})^2$ az eltérések négyzetének súlyozott összege;
- $\sum_{i=1}^k f_i$ az összes adatdarabok száma.

A számítások eredményeként az alábbi alkalmassági tartományokat határoztuk meg az útpályák esetében:

- átlag + szórás feletti értékek → korlátozás nélkül alkalmas;
- átlag körüli értékek → korlátozással alkalmas;
- átlag alatti, szórással csökkentett értékek → csak meghatározott eszközök számára alkalmas.

¹⁶ SPIEGEL–STEPHENSEN 2018.

A kapott értékeket és a kategóriákat az útpálya és a csomópont vonatkozásában a 3. táblázat tartalmazza részletesen.

3. táblázat: Az útpálya és a csomópont szempontjai és a hozzájuk rendelt követelmények

Fsz.	Infrastruktúra-elem	Súlypont	Osztályozás	Megjegyzés
1.	Útpálya	22,5–20,5	Korlátozás nélkül alkalmas haditechnikai eszközök közlekedtetésére	Az útszakasz akkor is alkalmas lehet minden eszköz közlekedésére, ha két ponttal kevesebbre osztályozzuk. Ez vonatkozik a megengedett sebességre és az akadályok megszüntetésének várható időpontjára ¹⁷
		20–14	Korlátozással alkalmas haditechnikai eszközök közlekedtetésére	Az útszakasz a megadott intervallum alapján csak korlátozással, de a legtöbb haditechnikai eszköz számára alkalmas közlekedésre
		14,5–10,5 pont	Csak meghatározott eszközök számára alkalmas közlekedtetésre	Nagy valószínűséggel csak terepjáró képességgel rendelkező járművek vagy kis méretű eszközök számára és korlátozottan ¹⁸ alkalmas közlekedésre
2.	Csomópontok	13,5–12,5 pont	Korlátozás nélkül alkalmas a haditechnikai eszközök közlekedtetésére	A csomópont akkor is alkalmas lehet minden eszköz közlekedésére, ha 1 ponttal kevesebbre osztályozzuk. Ez vonatkozik a katonai forgalomszabályozásra ¹⁹
		12–8	Korlátozással alkalmas a haditechnikai eszközök számára	A csomópont a megadott intervallum alapján csak korlátozással, de a legtöbb haditechnikai eszköz számára alkalmas közlekedtetésre
		7,5–6	Csak meghatározott eszközök számára alkalmas közlekedtetésre	Túlméretes, vagy rosszabb esetben az összes haditechnikai eszköz számára nem használható az infrastruktúra-elem

Forrás: a szerzők szerkesztése

A 22,5–20,5 pont korlátozás nélkül alkalmas haditechnikai eszközök közlekedtetésére ponttartomány az átlag feletti, illetve az átlag + szórás környezetében elhelyezkedő értékeket foglalja magában. Az ide sorolt útszakaszok geometriai kialakítása, teherbírása, burkolatszélessége és forgalmi jellemzői összességében megfelelnek a legtöbb haditechnikai eszköz közlekedési követelményeinek. A vizsgálat során megállapítottuk, hogy ezen kategóriába sorolt útszakaszok akkor is alkalmasak maradhatnak minden haditechnikai eszköz közlekedtetésére, ha egyes, kisebb jelentőségű szempontok (például különösen a megengedett legnagyobb sebesség és az akadályok megszüntetésének

¹⁷ Magyarázat: Ha csak 30 km/h sebességgel lehet egy útszakasz bizonyos pontján közlekedni, vagy az úton meglévő akadály megszüntetése csak 14 és 30 nap között várható, ebből még nem következik, hogy az útszakasz nem lesz alkalmas a haditechnikai eszközök közlekedtetésére.

¹⁸ A korlátozás a terepjáró képességgel rendelkező eszközöknél a konvojok együtt mozgatására vagy a szállítmányozó járművek alkalmazására vonatkozhat.

¹⁹ A csomópont alkalmas lehet minden eszköz közlekedtetésére függetlenül attól, hogy forgalomirányításra van-e szükség, vagy nem. Bár ez többletfeladatként jelentkezik a szállítások tervezésekor, nem jelent külön nagy mértékű korlátozást az infrastruktúra-elem fizikai értelemben vett használhatóságára.

várható időpontja) miatt legfeljebb két pontnyi csökkenés következik be. Ez alátámasztja, hogy az útpálya alkalmasságát elsősorban a nagyobb súlysorzóval rendelkező paraméterek határozzák meg.

A 20–14-ig a korlátozással alkalmas haditechnikai eszközök közlekedtetésére elnevezésű intervallum az átlag környezetében elhelyezkedő pontszámokat tartalmazza. Az ide sorolt útszakaszok alapvetően alkalmasak haditechnikai eszközök közlekedtetésére, azonban egyes paraméterek (például burkolatszélesség, tengelyterhelés, forgalmi sávszám vagy ideiglenes akadályok) korlátozást tehetnek szükségessé. Ezek az útszakaszokon a közlekedés jellemzően sebesség-, tengelyterhelés- vagy járműméret-korlátozással biztosítható.

A 14,5–10,5-ig terjedő csak meghatározott haditechnikai eszközök számára alkalmas közlekedtetésre ponttartomány az átlag alatti, illetve az átlag – szórás környezetében elhelyezkedő értékeket fedi le. Az ide tartozó útszakaszoknál a geometriai kialakítás, a burkolat minősége, a teherbírás vagy a forgalmi környezet jelentős mértékben korlátozza a közlekedést. Nagy valószínűséggel ezek az útszakaszok elsősorban terepjáró képességgel rendelkező, kisebb tengelyterhelésű haditechnikai járművek számára használhatók, és csak fokozott körültekintéssel vehetők igénybe.

A csomópont vonatkozásában a 13,5–12,5-ig terjedő korlátozás nélkül alkalmas a haditechnikai eszközök közlekedtetésére elnevezésű intervallum az átlag feletti, illetve az átlag + szórás környezetében elhelyezkedő csomópontokat foglalja magában. Az ide sorolt infrastruktúra-elemek geometriai kialakítása, csomóponti sugarai, forgalmi rendje és teherbírása lehetővé teszik a haditechnikai eszközök zavartalan áthaladását és kanyarodását. A vizsgálat során megállapítottuk, hogy ezek a csomópontok akkor is alkalmasak maradhatnak minden haditechnikai eszköz közlekedésére, ha a katonai forgalomszabályozás szempontjából legfeljebb 1 ponttal alacsonyabb értékelést kapnak.

A 12–8-ig a korlátozással alkalmas a haditechnikai eszközök számára ponttartomány az átlag környezetében elhelyezkedő csomópontokat jelöli. Az ide tartozó csomópontok alapvetően alkalmasak a haditechnikai eszközök közlekedtetésére, azonban bizonyos korlátozások (például forgalomtechnikai elemek telepítése, ideiglenes forgalomirányítás vagy sebességcsökkentés) alkalmazása szükségessé válhat. A legtöbb haditechnikai eszköz ezeken a csomópontokon áthaladhat, de a közlekedés jellemzően szervezési intézkedésekhez kötött.

A 7,5–6-ig terjedő csak meghatározott haditechnikai eszközök számára alkalmas közlekedtetésre intervallum az átlag alatti, illetve az átlag – szórás környezetében elhelyezkedő csomópontokat tartalmazza. Az ide sorolt infrastruktúra-elemek geometriai kialakítása, méretei vagy forgalmi környezete jelentős mértékben korlátozza a haditechnikai eszközök mozgását. A túlméretes járművek, illetve kedvezőtlen esetben a legtöbb haditechnikai eszköz számára ezek a csomópontok nem, vagy csak nagyon korlátozottan használhatók.

Összességében elmondható, hogy a tanulmányban rögzített követelmények és a hozzájuk rendelt pontszámok lehetővé teszik a szemrevételező csoportok számára a közúti infrastruktúra-elem katonai (logisztikai) szempontú felmérését, valamint az elemek egzakt besorolását a megfelelő alkalmassági csoportokba.

Ezzel gyorsítható és hatékonyabbá tehető a közutak szemrevételezése és az adatok alapján az elemek kiértékelése. A cikk második része a műtárgyak és az útpálya környezetének szempontrendszerét, valamint a követelmények meghatározását részletezi.

Felhasznált irodalom

- ACO Directive 084-004. *Criteria and Standards for the Zones of the Reinforcement and Sustainment Network*, Supreme Headquarters Allied Powers Europe (2024). Mons.
- Általános tájékoztató a meghatározott össztömeget, tengelyterhelést, tengelycsoport-terhelést és méretet meghaladó járművek közúti közlekedésének engedélyezéséről [é. n.]. Magyar Közút Nonprofit Zrt. Online: <https://internet.kozut.hu/ugyfelszolgalat/utvonallengedely-uvr-e-office/altalanos-tajekoztato/>
- HORVÁTH Attila (2018): A katonai logisztika alapképzési szak RSOM felkészítés tapasztalatai. *Hadmérnök*, 13(4), 81–96. Online: <https://folyoirat.ludovika.hu/index.php/hadmernok/article/view/3582>
- Közutak tervezése. e-ÚT 03.01.11:2008 [é. n.]. Magyar Közút Nonprofit Zrt. Online: <https://ume.kozut.hu/dokumentum/1490>
- NATO Standardization Agency (2004): *AMovP-1(A) Road Movements and Movement Control*. Brussels.
- PÓCSMEGYERI Gábor (2003): *A katonaföldrajzi tényezők hatása a Magyar Köztársaság közlekedési rendszerének védelmi célú előkészítésére*. PhD-disszertáció. Budapest: Zrínyi Miklós Nemzetvédelmi Egyetem Hadtudományi Doktori Iskola.
- SPIEGEL, Murray R. – STEPHENSEN, Larry J. (2018): *Statistics* [ePub]. New York: McGraw-Hill Education.
- SZAJKÓ Gyula (2019): Az út és úthálózatok értékelése a hadszíntéri logisztikai felderítés végrehajtásakor. *Hadmérnök*, 14(4), 61–77. Online: <https://doi.org/10.32567/hm.2019.4.4>
- SZAJKÓ Gyula (2025): *A logisztikai felderítés rendszerének továbbfejlesztési lehetőségei a Magyar Honvédség műveleteinek előkészítésében*. PhD-disszertáció. Budapest: Nemzeti Közzolgálati Egyetem Katonai Műszaki Doktori Iskola. Online: <https://doi.org/10.32567/hm.2019.4.4>

Jogi források

- 1/1975. (II. 5.) KPM–BM együttes rendelet a közúti közlekedés szabályairól. Online: <https://njt.hu/jogszabaly/1975-1-20-24>
- 36/2017. (IX. 18.) NFM rendelet a meghatározott össztömeget, tengelyterhelést, tengelycsoport-terhelést és méretet meghaladó járművek közlekedéséről. Online: <https://net.jogtar.hu/jogszabaly?docid=a1700036.nfm>
- A Bizottság (EU) 2021/1328 végrehajtási rendelete az (EU) 2021/1153 európai parlamenti és tanácsi rendelet értelmében a kettős felhasználású infrastruktúrával kapcsolatos intézkedések egyes kategóriáira alkalmazandó infrastruktúrális követelmények meghatározásáról. Online: https://eur-lex.europa.eu/eli/reg_impl/2021/1328/oj

Gábor Farkas¹ 

Augmentation of Training Data for AI-based Drone Detection System

Abstract

The increasing use of FPV drones in modern conflicts necessitates compact and energy-efficient detection systems capable of operating in dynamic electromagnetic environments. AI-based RF signal detection is a promising solution. However, its application can be limited by the lack of labelled datasets and the constraints of embedded platforms. This article presents a method for generating and augmenting training data directly from signals captured from analogue FPV video transmitters. Finally, a convolutional neural network was trained using the generated dataset and evaluated in a real-time environment. Experimental results demonstrate reliable detection performance, indicating that the proposed method is an effective and efficient solution for embedded FPV drone detection systems.

Keywords: electronic warfare, machine learning, ESM, software-defined radio, CUAV, FPV drone

Introduction

The rapid proliferation of unmanned aerial systems (hereinafter UAS), and in particular first-person-view (hereinafter FPV) drones, has fundamentally altered the character of contemporary battlefield operations. Originally developed for civilian and recreational purposes, FPV drones have been rapidly adapted for military use due to their low cost, ease of modification, and high operational effectiveness.² Recent conflicts, especially the Russo–Ukrainian war, have demonstrated the large-scale use of FPV drones for reconnaissance, target acquisition, and direct kinetic attacks against personnel and equipment.³ Their widespread availability and expendability enable adversaries to deploy them in large numbers, creating a persistent and asymmetric

¹ PhD student, Ludovika University of Public Service, Doctoral School of Military Engineering, e-mail: farkas.gabor.csp@gmail.com

² SEO et al. 2023.

³ MOLLOY 2024: 17.

threat to ground forces. This transformation is consistent with the broader evolution of modern warfare and hybrid operational environments.⁴

Unlike larger UAS, FPV drones operate at low altitude, exhibit small radar cross-sections, and often rely on commercially available radio-frequency (hereinafter RF) components. As a result, traditional air defence and surveillance systems are frequently ineffective or economically impractical against such targets.⁵ From the perspective of troop protection, early detection of approaching FPV drones is therefore critical, as it directly increases reaction time and enables the application of countermeasures.⁶ Electronic support measures (ESM) as part of electronic warfare (EW), operating in the electromagnetic spectrum, provide a promising means of detecting these systems by exploiting their RF emissions rather than relying solely on optical sensors.⁷

FPV drones typically transmit a continuous video stream from an onboard video transmitter (hereinafter VTX) to the remote operator. These transmissions, most commonly located in the 1.2 GHz and 5.8 GHz bands, are characterised by relatively high output power and distinct spectral features. As the drone approaches its target, the strength of the received signal of the video link increases, making RF-based detection particularly suitable for short-range warning systems. Consequently, recognising FPV-related RF signals has become a key research topic within modern counter-UAS and EW applications.⁸

The long-term objective of this research is the development of a compact EW device, that can be carried by soldiers and capable of autonomously detecting approaching FPV drones and issuing an immediate warning. Such a system must operate in real time, be lightweight and energy-efficient, and function reliably in a highly dynamic and contested electromagnetic environment. The proposed concept is based on a software-defined radio (hereinafter SDR) front-end coupled with an embedded computing module, forming a mobile RF sensing platform.⁹ Within this architecture, artificial intelligence-based (hereinafter AI) signal recognition is employed to distinguish FPV drone transmissions from other RF activity present on the battlefield.¹⁰

The application of AI techniques to the classification of RF signals in embedded EW systems introduces several significant challenges. First, to ensure suitability for mobile, battery-powered operation, the neural network used must be as compact and computationally efficient as possible, while still maintaining adequate detection performance. Second, publicly available and labelled training datasets for FPV drone RF signals are essentially nonexistent. Even if such datasets were available, they would rapidly become outdated due to the evolution of drone hardware. Third, any practical detection system must be capable of incorporating newly captured RF signals and

⁴ HAIG et al. 2014.

⁵ HORVÁTH et al. 2024.

⁶ HELL 2017.

⁷ LEE et al. 2018.

⁸ POPPINGA et al. 2025.

⁹ FARKAS et al. 2025.

¹⁰ NÉMETH-VIRÁGH 2023.

generating updated training data to maintain effectiveness against emerging threats. Addressing these challenges requires methods that enable systematic creation and augmentation of training datasets directly from captured RF streams. This capability is essential for rapid adaptation and to keep pace with the fast-changing electromagnetic environment observed in modern conflicts. The focus of this article is therefore on determining and evaluating a possible method for generating and augmenting datasets suitable for AI-based FPV drone detection. The proposed approach leverages real-world RF captures obtained using an SDR-based EW framework and applies data augmentation techniques to compensate for limited training samples.

The contributions of this work are twofold. First, it presents practical methods for constructing and augmenting RF training datasets from raw SDR data, specifically tailored to FPV drone signal characteristics. Second, the resulting datasets are evaluated using an existing convolutional neural network (hereinafter CNN) architecture, which is subsequently integrated into a real-time RF capture environment. By validating the approach on embedded hardware under realistic conditions, this study aims to bridge the gap between laboratory-scale AI experiments and deployable EW systems capable of supporting troop protection on the battlefield.

Analogue FPV video stream

Detecting the VTX signal from FPV drones is particularly advantageous for RF-based warning systems. Compared to control links, the video downlink typically operates with higher transmit power, exhibits continuous transmission, and becomes progressively stronger as the drone approaches the receiver. Furthermore, analogue FPV video signals are highly repetitive and structured in time, making them well suited for pattern-based detection approaches.

Instead of fully demodulating or decoding the video content, which would impose significant computational overhead, the proposed method relies on a visualisation technique known as rasterisation. In this approach, consecutive samples of the captured RF stream are placed sequentially in image rows. Once a row is filled, subsequent samples continue in the next row. This process effectively converts a one-dimensional time-domain signal into a two-dimensional image representation. Although the semantic video content is not reconstructed, characteristic temporal structures remain clearly visible as seen in Figure 1.

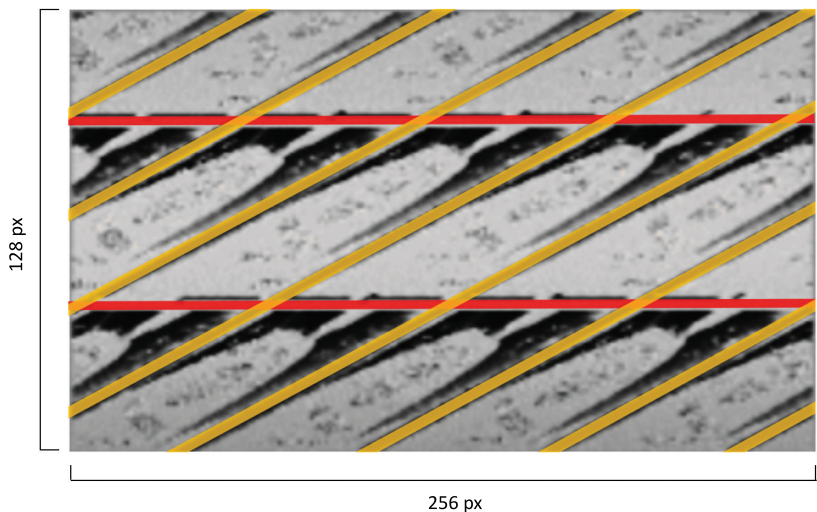


Figure 1: Synchronisation signals form a noticeable pattern on the rasterised image
Note: red line corresponds to vertical and yellow line to horizontal synchronisation
Source: compiled by the author

This representation closely resembles what a human observer would intuitively recognise as a video signal. Consequently, CNNs can be trained to identify these patterns automatically. Earlier work used an autocorrelation-based detection method, but its reliability proved insufficient under varying signal conditions and interference. The rasterised image-based approach could enable more robust detection by leveraging the spatial pattern recognition capabilities of CNNs.

Analogue FPV video standards

The majority of analogue FPV systems in current use rely on legacy composite video standards. While implementations may vary slightly across manufacturers, the fundamental timing characteristics remain consistent. The most encountered formats are summarised in Table 1.

Table 1: Typical analogue FPV video parameters

Standard	Frame rate	Horizontal line rate	Active lines	Approx. pixel clock
NTSC	29.97 Hz	15.734 kHz	480	12–14 MHz
PAL	25 Hz	15.625 kHz	576	14–15 MHz

Source: compiled by the author

These standards employ line-synchronous scanning, where each frame consists of a fixed number of horizontal lines, separated by synchronisation pulses.¹¹ For FPV detection purposes, precise pixel reconstruction is unnecessary. Only the repetitive timing structure of the signal is required.

Rasterised image construction

To generate a CNN-compatible input, the complex baseband IQ stream¹² captured by the SDR is first converted into a magnitude signal:

$$x[n] = \sqrt{I[n]^2 + Q[n]^2}$$

This operation removes phase information and produces a signal suitable for grayscale image generation. The magnitude samples are then rasterised into a two-dimensional array. In this work, an image resolution of 256×256 pixels is selected. This size provides a good compromise between computational efficiency and sufficient spatial resolution, and it closely matches the input tensor dimensions used by common CNN architectures such as ResNet-18.¹³

Sampling rate determination

To ensure that characteristic video patterns including horizontal and vertical synchronisation lines are preserved in the rasterised image, the SDR sampling rate must be carefully selected. To make the horizontal structure visually apparent, the image should contain multiple complete line crossings. In this work, the target is to display sixteen crossings in two rows to target a reliable detection. To visualise two vertical sync lines in the rasterised image we need to capture at least two frames. Therefore, the required time window is

$$T_V = \frac{2}{f_{frame}} = \frac{2}{30Hz} = 66.7ms$$

Taking into account the size of the image 256×256 pixels, the sampling rate can be determined in the following way:

$$f_{SR} = \frac{1}{\frac{T_V}{256 \times 256}} = \frac{1}{\frac{66.7ms}{65,536}} = 982.5kHz$$

¹¹ JACK 2011.

¹² IQ stream refers to a continuous sequence of sampled in-phase (I) and quadrature (Q) signal values acquired over time.

¹³ LIU et al. 2024.

This results in roughly two horizontal line intervals appearing within each image row block, which is sufficient to generate clearly distinguishable vertical and horizontal patterns in the rasterised image. Since many SDR platforms, like HackRF,¹⁴ allow only discrete sampling rates, a nominal value of 1 MSPS (millions of samples per second) is selected as a practical and widely supported configuration.¹⁵

Implications for dataset generation

With the sampling rate fixed and the rasterisation parameters defined, the SDR output can be consistently transformed into images that exhibit authentic FPV video patterns. These images form the basis for the training dataset used in subsequent CNN-based detection experiments. This makes it particularly suitable for real-time operation in dynamic battlefield RF environments.

Determining augmentation variables

When constructing a training dataset from captured FPV drone VTX signals, data augmentation is a necessity rather than an optional enhancement. Two primary motivations drive this requirement. First, RF signals encountered during operational deployment will inevitably differ from those recorded under laboratory conditions due to hardware variability, environmental effects and dynamic channel conditions. Second, in realistic field scenarios, only a limited amount of signal data may be available for capture. Consequently, the training dataset must be expanded synthetically to ensure sufficient variability and generalisation capability of the neural network.

Pixel frequency variability

Analogue FPV video transmitters are not frequency-stable precision instruments. Variations in component tolerances, oscillator drift, supply voltage and temperature can cause deviations in the effective pixel clock and line timing of the transmitted video signal. Practical measurements and manufacturer specifications indicate that these deviations typically fall within a range of approximately $\pm 1\%$ under normal operating conditions. In the rasterised image representation, such timing deviations manifest as a change in the slope or angle of the vertical synchronisation structures. A slightly higher effective pixel frequency causes vertical lines to tilt in one direction, while a lower frequency results in an opposite tilt. If the training dataset only contains perfectly aligned patterns, the CNN may overfit to a narrow representation and fail to generalise. To simulate this variability, the recorded RF stream is artificially under-sampled and over-sampled within a bounded range corresponding to the

¹⁴ HackRF One is an open source SDR hardware platform (<https://greatscottgadgets.com/hackrf/one/>).

¹⁵ HackRF documentation (s. a.).

expected pixel frequency deviation. This operation effectively introduces controlled geometric distortions in the rasterised images while preserving the underlying signal structure.

Signal-to-noise ratio variation

The clarity of the rasterised image is strongly influenced by the signal-to-noise ratio (hereinafter SNR) of the captured RF stream. In practice the SNR can vary significantly due to several factors, including distance between the drone and the detector, antenna orientation, multipath propagation, and the presence of other RF emitters operating in the same frequency band. To account for these effects, noise is added synthetically to the magnitude signal prior to rasterisation. This allows the generation of image samples corresponding to different SNR conditions. The range of applied Gaussian noise values is chosen such that the characteristic horizontal and vertical synchronisation patterns remain visually discernible. If the noise level is too high, the repetitive structure of the video signal is completely obscured, rendering the sample unusable for both human and machine recognition. Therefore, augmentation is constrained to a range where degradation is realistic but still informative for training.

Temporal offset of the rasterisation window

Each rasterised image is constructed from a fixed-length segment of the RF stream, consisting of 65,536 consecutive samples. In a continuous video transmission, the starting point of this segment is arbitrary. As a result, the captured window may begin in any phase relative to the video line or frame synchronisation. This offset causes horizontal and vertical features to appear at different spatial positions in the rasterised image. If the dataset only contains images with aligned structures, CNN may implicitly learn absolute positional dependencies rather than the presence of the pattern itself. To mitigate this effect, the starting index of the sampled segment varies during dataset generation. By randomly shifting the capture window within the continuous stream, the resulting images exhibit the same structural elements at different locations, promoting translation invariance in the trained model.

Scene-dependent video content

Although the proposed method does not decode the video signal, the analogue video content still influences the rasterised representation. Changes in brightness, contrast, and scene dynamics introduce variations in the amplitude envelope of the signal, which in turn affect the grayscale texture of the generated images. During laboratory

recordings, it is therefore advantageous to expose the FPV camera to scenes that are approximately expected operational environments, such as open terrain, vegetation, or mixed backgrounds. This ensures that the captured signal exhibits realistic amplitude fluctuations. In contrast, battlefield captures are inherently uncontrolled, and the observed video content may vary widely. Because it is not feasible to control video content in operational scenarios, the augmentation strategy must account for this uncertainty. By combining multiple laboratory recordings with different visual scenes and applying the previously described augmentation methods, the resulting dataset captures a broader range of signal appearances, improving robustness under real-world conditions.

Capturing RF signal for dataset generation

To generate training data suitable for AI-based FPV drone detection, a live analogue VTX signal must first be captured. Based on the previous analysis, the SDR sampling rate and rasterised image dimensions are fixed at 1 MSPS and 256×256 pixels, respectively. In this experiment, 1 second of data was captured that contains FPV VTX signal.

Frequency variation via resampling

As discussed previously, the effective pixel frequency of analogue FPV video signals may vary due to hardware tolerances and environmental effects. To simulate this variability, the recorded RF stream is resampled to emulate small deviations in timing. In this study, 100 resampled versions of the captured stream are generated, spanning a frequency variation range from -1% to $+1\%$ around the nominal sampling rate. For this experiment the resampling is performed in 100 steps. Each resampled stream represents a slightly different effective pixel clock and produces a distinct geometric appearance in the rasterised images.

Capture length

Each rasterised image is constructed from a fixed-length segment of the magnitude signal containing 65,536 samples. To enable sufficient variability in temporal alignment, multiple image windows are extracted from each captured and resampled stream using different starting offsets. In the proposed approach, the stream is divided into 40 partially overlapping segments, each producing one rasterised image.

Noise augmentation and image count

To model varying channel conditions and detection ranges, additive noise is applied to each image segment. Ten noise levels are used, ranging from 0% to 50% relative distortion, corresponding to progressively decreasing SNR while preserving recognisable structural patterns. Taking into account the 40 segments taken from the original stream, resampling applied in 100 steps and adding relative distortion gives the total number of generated training images all together 40,000. This dataset size is considered sufficient as an initial training set for a CNN architecture such as ResNet-18.¹⁶

Laboratory capture setup

The RF data used for dataset generation were collected under laboratory conditions using GNU Radio¹⁷ as the signal acquisition and visualisation environment. A HackRF One SDR was employed as the RF front-end. A simple GNU Radio flowgraph was constructed with the following functional blocks:

- Frequency scanning and tuning, enabling manual identification of active VTX carriers.
- Time Raster Sink, providing real-time visualisation of the incoming signal in a rasterised format. This visualisation closely resembles the images later generated for CNN input, enabling intuitive confirmation of signal presence and structure.
- File Sink, used to store raw complex baseband samples for offline processing and dataset generation.

The user interface for the flowgraph can be seen in Figure 2. This setup allows efficient discovery of VTX signals even when the exact carrier frequency is initially unknown. Once a suitable signal is identified, a short recording of a few seconds is sufficient to generate the full augmented dataset described above. As a signal source, a small "Tiny Whoop" class FPV drone¹⁸ equipped with an analogue video transmitter was used. Several seconds of continuous video transmission were captured at close range, resulting in a high-quality reference recording. Although the capture environment was controlled, the subsequent augmentation steps ensure that the generated dataset reflects a wide range of realistic operational conditions.

¹⁶ SHIN et al. 2016.

¹⁷ GNU Radio is an open-source software development toolkit for software-defined radio, enabling the construction of signal processing pipelines ("flowgraphs") using modular functional blocks (www.gnuradio.org/).

¹⁸ "Tiny Whoop" refers to a class of small FPV quadcopters with ducted propellers and low-power analogue video transmitters, typically used for short-range flight (www.tinywhoop.com/collections/bnf).

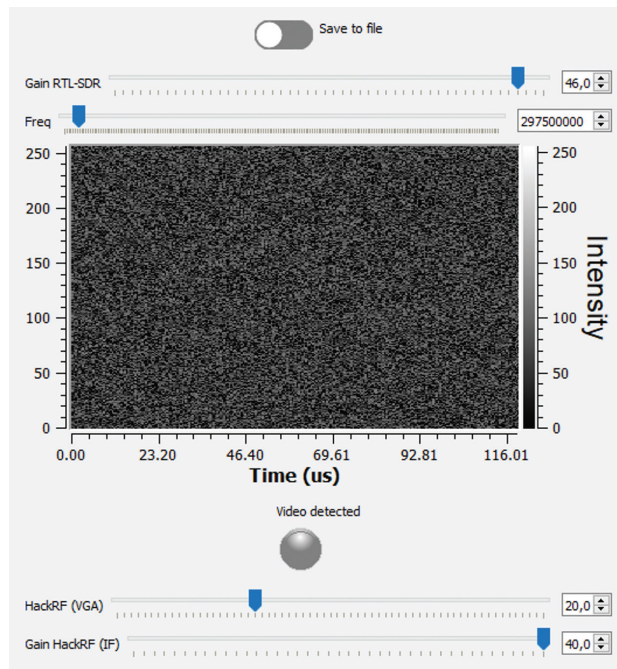


Figure 2: User interface of a GNU Radio project where the rasterised signal is displayed in real time

Note: additional controls can be seen for fast signal discovery

Source: compiled by the author

Implications for rapid dataset creation

The described capture and augmentation strategy enables the generation of a large and diverse training dataset from minimal raw RF data. This is particularly important in field scenarios, where capture opportunities may be limited to short time windows. By relying on systematic resampling, temporal offset variation and controlled noise injection, the approach supports rapid dataset preparation and iterative retraining, which are essential for maintaining detection performance in evolving electromagnetic environments.

Creating dataset

Once the RF capture is stored as a file containing complex IQ samples, the preparation of the training dataset can begin. All dataset generation and processing steps are implemented using Python scripts, chosen for their portability, readability and compatibility with common scientific computing environments. This design choice ensures that the dataset creation pipeline can be reproduced on a wide range of platforms, including embedded systems and standard development workstations.

Stream resampling and normalisation

As described previously, the first step in dataset preparation is the resampling of the initial portion of the captured RF stream. From the original recording, 100 resampled streams are generated to simulate small variations in effective pixel frequency. Each resampled stream is converted to a nominal sampling rate of 1 MSPS. The magnitude of each complex sample is computed and normalised to an 8-bit grayscale range. This normalisation ensures consistent intensity scaling across all samples and allows the resulting data to be directly represented as grayscale images without further conversion.

Manual validation of signal presence

Before proceeding with large-scale augmentation, a manual validation step is introduced to ensure data quality. Each resampled stream is split into 16 non-overlapping segments of 65,536 samples, corresponding to 16 rasterised images per stream. These images are saved to disk and visually inspected. This process yields a total of 1,600 images. The purpose of this step is to confirm that each resampled stream contains the expected FPV video patterns, such as stable horizontal and vertical synchronisation structures. Streams that do not meet these criteria due to interference, signal loss, or incorrect tuning are excluded from further processing. Introducing this validation stage prevents mislabelled or corrupted data from degrading training performance. Two rasterised images from the validation stage can be seen in Figure 3.

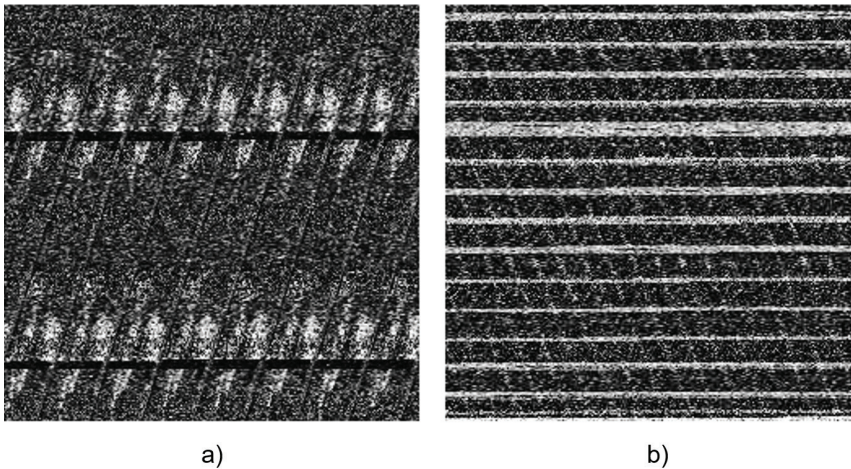


Figure 3: Captured RF stream converted to rasterised image

Note: a) signal from an FPV drone; b) signal from an unknown source

Source: compiled by the author

Randomised slice selection and SNR augmentation

For the remaining validated streams, the dataset is randomly distributed into three subsets before augmentation. This split follows common best practices in supervised learning and provides a balanced framework for model optimisation and unbiased performance evaluation:

- training set: 80%
- validation set: 10%
- test set: 10%

The dataset generation script selects random 65,536 sample slices from each stream to introduce temporal diversity. Noise is then applied to each slice at predefined levels to simulate varying SNR conditions. Each processed slice is rasterised into a 256×256 grayscale image and saved to disk. All images generated from FPV VTX recordings are labelled as *Signal*, representing the positive detection class that the neural network is intended to recognise.

Negative class (noise) dataset generation

To enable binary classification, an equally sized dataset representing the negative class is required. This class is labelled *Noise* and contains RF captures that do not include FPV video transmissions. The noise dataset is generated using the same processing pipeline as the signal dataset, ensuring consistent preprocessing and image characteristics. RF captures for this class include:

- background noise
- other communication signals (Wi-Fi, Bluetooth)
- unrelated RF activity within the monitored frequency bands

By maintaining symmetry in dataset size and processing steps, the risk of class imbalance and preprocessing bias is minimised. Once both classes are generated, the complete dataset consists of balanced *Signal* and *Noise* samples suitable for supervised CNN training. If additional FPV VTX recordings are later acquired, they can be incorporated by generating new *Signal* samples using the same procedure and merging them with the existing dataset. This modular approach supports incremental dataset expansion without requiring a complete regeneration of previously collected data. Representations of different amounts of noise applied to the stream can be seen in Figure 4.

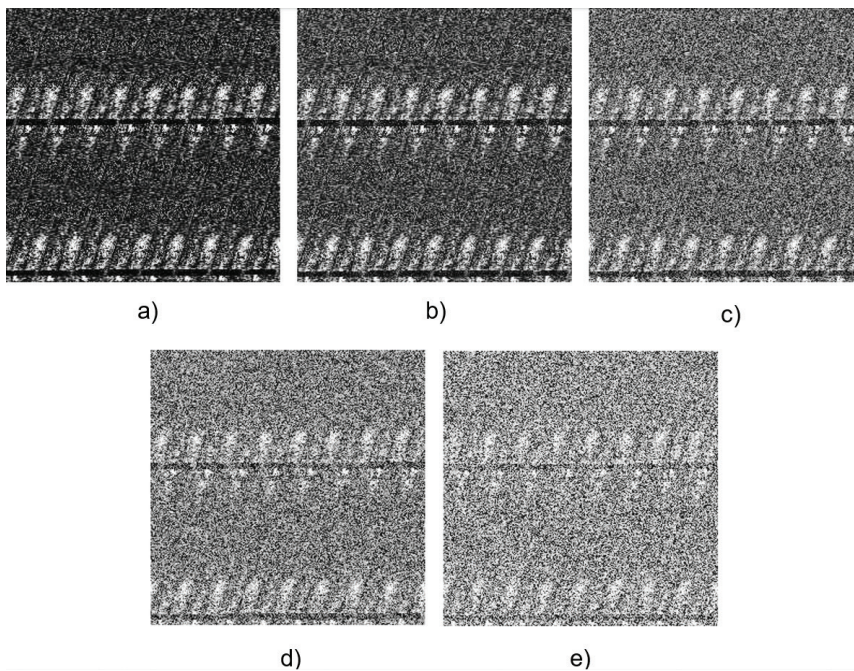


Figure 4: Different levels of noise applied to the same image

Note: a) 10%; b) 20%; c) 30%; d) 40%; e) 50%

Source: compiled by the author

Model training preparation

With the dataset prepared, the system is ready for neural network training. In this work, a ResNet-18 architecture is selected as the initial model due to its favourable trade-off between accuracy, computational complexity and suitability for embedded deployment. Training is performed using the PyTorch¹⁹ framework with transfer learning. The rasterised grayscale images are transformed into the appropriate input tensor format required by ResNet-18.²⁰ No additional image-domain augmentation techniques such as rotation, cropping, or flipping are applied, as the dataset already incorporates signal-domain variability through resampling, temporal shifting and SNR manipulation. Given the dataset size generated, training converges within a few minutes on standard computing hardware. This rapid training cycle is an important practical advantage, enabling frequent retraining and adaptation as new RF data becomes available.

¹⁹ PyTorch is an open-source machine learning framework used for building and training neural networks, particularly well-suited for deep learning applications (<https://pytorch.org/>).

²⁰ CHAPPELL-WHITEHEAD 2022.

Testing the model in real environment

After completing training, the performance of the neural network was first evaluated using the reserved test dataset. On this offline test batch, the model achieved a classification accuracy of 100%. While this result confirms correct dataset labelling and successful convergence, offline accuracy alone is insufficient to assess operational suitability. Therefore, further validation was conducted in a real-time RF acquisition and inference environment.

Model deployment and integration

To enable real-time inference, the trained ResNet-18 model was exported to the Open Neural Network Exchange (hereinafter ONNX) format. ONNX was selected due to its framework-independent representation and widespread support across inference engines and embedded platforms.

A custom Python processing block was implemented within the GNU Radio environment. This block operates directly on the live SDR data stream and performs the following steps:

- collection of 65,536 consecutive complex samples from the SDR output
- conversion of the IQ samples to magnitude values
- normalisation and reshaping of the data into a 256×256 grayscale image
- transformation of the image into the tensor format required by the neural network
- execution of model inference using the ONNX runtime

The model outputs class probabilities for the labels signal and noise. A detection event is declared if the confidence score for the signal class exceeds 90%. This threshold was chosen to reduce false alarms while maintaining high sensitivity to genuine FPV video transmissions.

Field testing

Real-time tests were conducted using three different analogue FPV video transmitters operating in a dense urban environment characterised by heavy RF background activity. The transmitters were mounted on small FPV platforms and moved within a radius of approximately 50 metres from the detector. To ensure a conservative evaluation, the VTX output power was limited to 100 mW. This power level is significantly lower than typical battlefield configurations, where FPV transmitters commonly operate at output powers exceeding 1 W. As a result, the test conditions represent a challenging detection scenario with reduced signal strength and increased interference. Under these conditions, the system achieved a detection success rate exceeding 96%.

False alarm assessment

To evaluate robustness against false detections, the system was operated continuously for an 8-hour period in the same urban RF environment, without any active FPV transmissions present. During this interval, the detector processed live RF data and performed inference continuously using the same confidence threshold. No false positive detections were recorded during the entire observation period. This result indicates strong discrimination between FPV video signals and background RF activity, including other communication systems operating in the monitored bands.

Discussion of results

The real-time experiments demonstrate that the proposed detection approach is not only effective under controlled offline conditions but also robust when deployed in a realistic and noisy RF environment. The combination of rasterised signal representation and CNN-based classification provides reliable detection even at reduced transmit power levels and in the presence of significant background interference.

While the observed performance metrics are highly promising, it should be noted that the tested scenarios represent short-range engagements and analogue FPV systems. Detection range and generalisation to other modulation schemes will depend on SDR sensitivity, antenna characteristics and further dataset expansion. Nevertheless, the absence of false alarms during extended operation is a particularly important result for practical deployment, where excessive false positives can significantly degrade operational usability.

Conclusion

This article addressed the problem of creating effective training data for AI-based detection of FPV drone video transmitters in scenarios where labelled RF datasets are unavailable, and signal characteristics change rapidly. The motivation arises from the operational need for compact, mobile electronic warfare systems capable of detecting approaching FPV drones in real time and under realistic battlefield conditions. The primary challenge is to enable reliable detection using limited captured data, while maintaining computational efficiency suitable for embedded, low-power platforms. To overcome this challenge, a complete workflow was presented, starting from live RF signal capture and extending through dataset generation, augmentation, neural network training and real-time deployment. The study demonstrated how a few seconds of captured analogue FPV video signal can be transformed into a sufficiently large and diverse training dataset through controlled resampling, temporal shifting and noise augmentation. The resulting dataset was used to train a convolutional neural network and validated both offline and in a real-time SDR-based detection environment.

A key contribution of this work is the use of image-based recognition applied to rasterised RF signals. Unlike common AI-based RF detection approaches that rely on frequency-domain representations such as FFTs or waterfall spectrograms, the proposed method operates entirely in the time domain. The preprocessing pipeline is computationally lightweight, requiring only magnitude calculation and rasterisation, which is significantly less demanding than spectral analysis. Compared to traditional autocorrelation-based detection, the CNN-based approach offers improved robustness and scalability, particularly when multiple repetitive signal types must be distinguished. The method is especially well suited for continuous and highly repetitive transmissions, such as analogue FPV video streams. It is emphasised that the presented approach represents only one possible solution among many for RF-based drone detection. Alternative signal representations, neural network architectures and detection strategies may be more appropriate for other signal types or operational constraints. Nevertheless, the results indicate that rasterised image-based recognition is a viable and effective technique for FPV drone detection in embedded EW applications. Future work will focus on designing and evaluating custom, lightweight CNN architectures tailored specifically to rasterised RF data. The objective is to reduce model size and energy consumption while preserving detection accuracy, enabling deployment on resource-constrained embedded platforms. Additional studies will also explore extending the approach to other signal classes and modulation schemes, further enhancing adaptability in dynamic electromagnetic environments.

References

- CHAPPELL, Andrew – WHITEHEAD, Leigh H (2022): Application of Transfer Learning to Neutrino Interaction Classification. *The European Physical Journal C*, 82(12). Online: <https://doi.org/10.1140/epjc/s10052-022-11066-6>
- FARKAS, Gábor – FAZEKAS, Gábor – NÉMETH, András (2025): FPV-drónok detektálásának alternatív megoldása konvolúciós neurális hálózattal. *Haditechnika*, 59(2), 2–7. Online: <https://doi.org/10.23713/HT.59.2.01>
- HackRF documentation (s. a.). Online: <https://hackrf.readthedocs.io/en/latest/index.html>
- HAIG, Zsolt – KOVÁCS, László – VÁNYA, László – VASS, Sándor (2014): *Elektronikai hadviselés*. Budapest: Nemzeti Közzolgálati Egyetem. Online: <https://opac.uni-nke.hu/webview?infile=&sobj=9276&source=webvd&cgimime=application%2Fpdf%0D%0A>
- HELL, Péter (2017): Drónelhárító rendszerek az objektumvédelemben. *Hadmérnök*, 12(3), 37–47. Online: www.hadmernok.hu/173_04_hell.pdf
- HORVÁTH, Tamás – ÖRDÖGH, Attila – BORKÓ, Máté (2024): Dróndetektáló fejlesztés. *Haditechnika*, 58(1), 55–59. Online: <http://doi.org/10.23713/HT.58.1.10>
- JACK, Keith (2011): *Video Demystified. A Handbook for the Digital Engineer*. Amsterdam: Elsevier.
- LEE, Dongkyu – LA, Woong Gyu – KIM, Hwangnam (2018): Drone Detection and Identification System Using Artificial Intelligence. *2018 International Conference on*

- Information and Communication Technology Convergence (ICTC)*, 1131–1133. Online: <https://doi.org/10.1109/ICTC.2018.8539442>
- LIU, Haixia – BRAILSFORD, Tim – BULL, Larry (2024): Resnet18 Performance: Impact of Network Depth and Image Resolution on Image Classification. *Proceedings of the 2024 8th International Conference on Advances in Artificial Intelligence*, 351–356. Online: <https://doi.org/10.1145/3704137.3704173>
- MOLLOY, Oleksandra (2024): *Drones in Modern Warfare: Lessons Learnt from the War in Ukraine*. Australian Army Research Centre. Online: <https://doi.org/10.61451/267513>
- NÉMETH, András – VIRÁGH, Krisztián (2023): Mesterséges intelligencia és haderő – Katonai alkalmazási lehetőségek VII. rész. *Haditechnika*, 57(1), 2–6. Online: <https://doi.org/10.23713/HT.57.1.01>
- POPPINGA, Gerald – ANDERSON, David – AMENDOLA, Danilo (2025): *Technical Developments in Counter-drone Technology: C-UAS Detection, Tracking and Identification Technology*. Luxembourg: Publications Office of the European Union. Online: <https://doi.org/10.2760/1517220>
- SEO, Kang-Il – CHO, Sang-Keun – PARK, Sang-Hyuk (2023): A Case Study on FPV Drone Combats of the Ukrainian Forces. *The Journal of the Convergence on Culture Technology*, 9(3), 263–270. Online: <https://doi.org/10.17703/JCCT.2023.9.3.263>
- SHIN, Hoo-Chang – ROTH, Holger R. – GAO, Mingchen – LU, Le – XU, Ziyue – NOGUES, Isabella (2016): Deep Convolutional Neural Networks for Computer-Aided Detection: CNN Architectures, Dataset Characteristics and Transfer Learning. *IEEE Transactions on Medical Imaging*, 35(5), 1285–1298. Online: <https://doi.org/10.1109/TMI.2016.2528162>

Halmi Lajos¹

Szívfrekvencia-variabilitás monitorozása légi járművek fedélzetén

In-flight Heart Rate Variability Monitoring

Absztrakt

A légi járművek irányítása komplex, az emberi figyelem egészét kívánó tevékenység, amely mélyreható információfeldolgozást igényel, ezáltal aktív pszichológiai, kognitív és fizikai terhelést jelent az operátorok számára. A fellépő stresszorok teljesítménycsökkenéshez vezethetnek és redukálhatják a repülésbiztonságot, ennek érdekében a repülőgép-vezetők mentális terhelésének monitorozása kulcsfontosságú adatokkal szolgálhat a biztonság növelésének szempontjából. A mentális terhelés ugyanakkor többtényezős dimenzió, amelyet számos külső és belső (emberi) tényező befolyásolhat, ugyanakkor a mai magasan automatizált fülkékben a konvencionális mérési protokollok kihívásokba ütközhetnek. A szívfrekvencia-variabilitás (heart rate variability, HRV) ígéretes eszközként jelent meg a szakemberek mentális terhelésének valós repülési körülmények közötti detektálására. A szívfrekvencia-variabilitás mérésének lehetősége az operátorok terhelésének vizsgálatára összetett környezetben a jövőben számos új lehetőséget nyit meg. A módszer segítségével generált adatok révén alkalmas az autonóm idegrendszer stresszválaszának és regenerációs képességének feltérképezésére. Szemléltetésül: a fáradtság szubjektív, egyénenként változó ütemben és mélységben megjelenő érzet, amelynek objektív értékelése esetenként nehézségekbe ütközik. A szívfrekvencia-variabilitás olyan minőségű biomarker a fáradtsági állapot felmérésére, amely hozzásegíthet a fáradtság részletesebb megértéséhez.²

Kulcsszavak: emberi tényező, repülésbiztonság, mentális terhelés, szívfrekvencia, stressz, fáradtság

¹ Doktori hallgató, Nemzeti Közszerológiai Egyetem Katonai Műszaki Doktori Iskola, e-mail: halmi.lajos@gmail.com

² WANG-HOUGHTON-MAJUMDAR 2024.

Abstract

Aircraft operation is a complex task that requires the full capacity of human attention and involves extensive information processing, consequently, it imposes significant psychological, cognitive, and physical workload on operators. Stressors encountered during flight can lead to performance degradation and may reduce flight safety. Therefore, monitoring pilots' mental workload can provide valuable data for improving operational safety. Mental workload is a multidimensional construct influenced by numerous external and internal (human-related) factors. However, in today's highly automated cockpit environments, conventional workload measurement protocols may face considerable limitations. Heart rate variability (HRV) has emerged as a promising tool for detecting professionals' mental workload under real flight conditions. The application of HRV measurement to assess operator workload in complex environments opens up numerous future opportunities. Data generated through this method can be used to characterise the stress response and recovery capacity of the autonomic nervous system. Fatigue, for instance, is a subjective sensation that manifests at different rates and intensities across individuals, which makes its objective assessment challenging. Heart rate variability represents a high-quality biomarker for evaluating fatigue status and may contribute to a more comprehensive understanding of fatigue-related processes.

Keywords: human factors, aviation safety, mental workload, heart rate, stress, fatigue

Bevezetés

A katonai és más kiképzési tevékenységekről ismert, hogy magas szintű stresszt idéznek elő, akár felkészítés, akár tényleges műveletek során. Ezen feladatok közül a repülés különösen kiemelkedik a stresszterhelés szempontjából. A repülésben rejlő egyértelmű kockázatok mellett a komplex környezeti hatások magas szintű kognitív aktivitást követelnek meg az operátoroktól, továbbá olyan nem ideális helyzetek kialakulásáért felelősek, amelyek negatívan befolyásolják a teljesítményt, például: dehidratáció, fáradtság, optikai illúzió és térbeli dezorientáció. Ezeknek a pszichológiai, fizikai és kognitív tényezőknek az összessége alkotja a repülőgép-vezetők általános terhelését, amelyekkel számolni kell egy feladat végrehajtása során. Ha ezek a hatások elérnek egy bizonyos mértéket (amely értékek mindenkinél különböznek), akkor, az emberi információfeldolgozás korlátossága miatt, a teljesítményben visszaesés figyelhető meg. Ennek az egyéni korlátnak az elérése fáradtságot okoz, ami korlátozza a munkavégzés folyamatosságát és csökkenti a repülésbiztonság mértékét. A terhelés és a teljesítmény monitorozása tehát kulcsfontosságú, mivel a mért paraméterek előre jelzik, hogy a repülőgép-vezetők hatékonysága rövid időn belül romolhat. A tanulmány célja annak vizsgálata, hogy a szívfrekvencia-variabilitás (HRV) milyen mértékben alkalmazható objektív biomarkerként a repülőgép-vezetők mentális és fiziológiai terhelésének monitorozására a repülési környezetben. A kutatás továbbá arra törekszik, hogy feltárja a HRV-mutatók és a pilóták teljesítményét

befolyásoló stressz- és fáradtsági tényezők közötti kapcsolatot, hozzájárulva ezzel a repülésbiztonságot támogató monitorozási és prevenciós rendszerek fejlesztéséhez.

Az utóbbi évtizedekben a kutatások növekvő számban használták fel a szívfrekvencia-variabilitást (HRV) a repülésben részt vevők terhelésének vizsgálatára.³

Az 1. táblázat a fő HRV-indexeket és azok értelmezését mutatja be.

1. táblázat: A fő HRV-indexek

Módszer	Index	Leírás	Autonóm hatás
Időtartomány	SDNN standard deviation of NN intervals	A normál szinuszritmusú szívütések közötti időintervallumok szórása ezredmásodpercben (ms)	Szimpatikus és paraszimpatikus
	RMSSD root mean square of successive differences	A normál szívütések közötti egymást követő különbségek négyzetes középértéke (ms)	Paraszimpatikus
	pNN50 percentage of successive NN	Az egymást követő R-R intervallumok azon százaléka, amelyek több mint 50 ms-mal térnek el egymástól (%)	Paraszimpatikus
	HRVti triangular index	HRV háromszög index: az RR-intervallum-hisztogram sűrűségének integrálja osztva annak magasságával	–
Frekvencia-tartomány	ULF ultra low frequency	Ultraalacsony frekvenciájú teljesítmény: $\leq 0,003$ Hz (ms^2)	Szimpatikus és paraszimpatikus
	VLF very low frequency	Nagyon alacsony frekvenciájú teljesítmény: $0,0033\text{--}0,04$ Hz (ms^2)	–
	LF low frequency	Alacsony frekvenciájú teljesítmény: $0,04\text{--}0,15$ Hz (ms^2)	Főként szimpatikus, részben paraszimpatikus
	HF high frequency	Magas frekvenciájú teljesítmény: $0,15\text{--}0,4$ Hz (ms^2)	Paraszimpatikus
	LF/HF	Az LF és HF aránya (%)	Vegetatív egyensúly
	TOTpow total power	Teljes spektrális teljesítmény (ms^2)	–
Nemlineáris módszerek	SD1 standard deviation	Poincaré-diagram szórása az identitásvonalra merőlegesen (ms)	Paraszimpatikus
	SD2	Poincaré-diagram szórása az identitásvonal mentén (ms)	Szimpatikus és paraszimpatikus
	SampEn	Mintázatterófia, amely az idősor szabályosságát és komplexitását méri	–
	$\alpha 1$	Detrended fluctuation analysis (DFA) paraméter, amely a rövid távú fluktuációkat írja le	–

Forrás: SHAFFER–GINSBERG 2017

³ MANSIKKA et al. 2015.

A HRV-érték a szívütések közötti időintervallumokon (RR-intervallum, kamrai összehúzódások) alapuló matematikai számítások összessége, segítségével következtetni lehet az autonóm idegrendszer (*autonomic nervous system*, ANS) aktivitására, avagy a szimpatikus és paraszimpatikus idegrendszeri működés arányára. Leggyakrabban a HRV-érték csökken a kognitív igénybevétel hatására, ami szimpatikus működést indikál. Abban az esetben, ha a stresszhatás félbeszakad, vagy a terhelés mérséklődik, a homeosztázis (önszabályozás) helyreáll a paraszimpatikus összetevők bekapcsolódása révén. A gyakorlati orvosi alkalmazásokban a magas HRV-érték egészséges, ideális alkalmazkodóképességgel rendelkező egyéneket jelez. A HRV-érték kulcsfontosságú mérőeszköz az akut ingerekre adott fiziológiai válaszok értékelésére, jöllehet az érték egyéni, és függ az alany kognitív kompetenciáitól, pszichomotoros készségeitől és teljesítménykapacitásától. A magas HRV-vel rendelkező repülő személyek magasabb pontossággal és gyorsabban hajtják végre a kognitív kihívásokat, valamint hatékonyabban reagálnak a stressz okozta hatásokra.⁴

A szívfrekvencia mérését széles körben alkalmazzák a klinikai területeken, sportteljesítmény meghatározásában és egyes wellness programokban, napjainkban kezd a repülésben adaptálódni és terjedni. A repülésben gyűjtött és értékelt HRV-adatok hozzásegítenek a repülőgép-vezetők aktuális fiziológiai állapotának mélyebb megértéséhez valós időben, ami hozzájárulhat a képzési és regenerációs időszakok optimalizálásához, valamint a túlteljesítés és az azt követő teljesítménycsökkenés prevenciójához. A módszert kihasználva lehetőségünk nyílik szisztematikusan feltérképezni a pilóták repülés közbeni autonóm szabályozásában bekövetkező változásokkal kapcsolatos hatásokat, annak érdekében, hogy objektív mérőszámok segítségével jellemezzük terhelésüket a repülés különböző szakaszaiban és repülési profiljaiban.

HRV-mérés alapjai

A szívfrekvencia-variabilitás (HRV) a pszicho-fiziológiai jellemzők szemléltetésére és elemzésére szolgáló mérhető mutató, amely az egymást követő szívverések közötti időintervallumok (*inter-beat interval*, IBI) matematikai vizsgálatára támaszkodik. Az IBI-időt az EKG-mérés során állapítják meg, mégpedig a szív elektromos jelének legjellegzetesebb pontjai, az R-csúcsok (kamrai összehúzódás fő elektromos jele) alapján, nagy pontosságú mintavételezéssel, jellemzően 250–1000 Hz közötti frekvenciával. Minél nagyobb a mintavételi frekvencia, annál pontosabb HRV-mutatókat kaphatunk, különösképpen a dinamikus cselekvések és komplex kognitív folyamatok során. A HRV-érték az autonóm idegrendszer aktivitásának közvetett mutatója. A szimpatikus aktivitás és a paraszimpatikus (vagális) aktivitás mérséklődése rövidebb és nem oly változékony R–R-intervallumokat produkál, ami az esetek nagy hányadában a HRV-mutató csökkenésében nyilvánul meg. Ugyanakkor a paraszimpatikus fölény nagyobb HRV-vel jár, amely a szervezet jobb adaptációs és regenerációs képességére enged következtetni. A szívfrekvencia-variabilitás időbeli változásainak vizsgálata lehetővé teszi a stresszreakció, a terhelés és a regeneráció tárgyilagos értékelését, továbbá a teljesítményt meghatározó pszicho-fiziológiai események

⁴ BRANDELLO FARIAS SOARESET et al. 2025.

nyomon követését.⁵ A gyakorlati mérések során a leghatékonyabban alkalmazható HRV-paramétereket az időtartományi és frekvenciatartományi módszerekkel elemzik. Ezek az eljárások statisztikai megközelítéseket alkalmaznak a szívfrekvencia időbeli alakulásának középértékére vonatkozóan. A HRV segítségével a szívfrekvencia szabályozását az átlagértékek és a kilengések komplett skálájának figyelembevételével számszerűsítik az idő függvényében. Mindazonáltal előfordulhat, hogy két alany meg egyező átlagos R–R-intervallummal és szívfrekvenciával reagál egy adott eseményre, miközben az intervallumok variabilitása szignifikánsan eltér. Időtartományi mutatók tekintetében a két leggyakrabban alkalmazott az R-intervallumok szórása (SDNN) és az egymást követő R-intervallumok különbségeinek négyzetes középértéke (RMSSD). Az SDNN az autonóm szabályozás nagyságrendi számszerű leírását adja, mivel a szimpatikus és a paraszimpatikus jellemzőket is leírja. Ezzel szemben az RMSSD elsősorban a paraszimpatikus aktivitást reprezentálja. Az SDNN-nel ellentétben az RMSSD nem tartalmazza a szívfrekvencia lassú hullámú összetevőit, ennek köszönhetően elenyésző befolyás éri a légzés által keltett mikromozgásokból, ezáltal pontosabb képet ad a paraszimpatikus működésről.⁶ A frekvenciatartományi HRV-mutatók az R–R-intervallumok matematikai transzformációján alapulnak, amelyek lehetőséget adnak a jel egyes frekvenciasávokban történő modulációjának számszerű kifejezésére: ultraalacsony frekvencia (ULF), nagyon alacsony frekvencia (VLF), alacsony frekvencia (LF) és magas frekvencia (HF). Az időtartományi mutatókhoz képest a frekvenciatartományi HRV-mérőszámok részletesebb adatot generálnak a jelek tulajdonságairól, az egyes elemek szerepéről, valamint azok viselkedéssel kapcsolatos kimenetéről. Az LF-teljesítményt mind a szimpatikus, mind a paraszimpatikus idegrendszer befolyásolja, nyugalmi állapotban (például alvás) az LF inkább a vérnyomás-szabályozó mechanizmus (baroreflex) működését mutatja meg, nem pedig a szív szimpatikus viselkedését, ennek okán nem minden esetben alkalmas a teljesítmény és regeneráció értékelésére. A HF-sáv közvetlenül a paraszimpatikus tevékenységet tükrözi, azonban nagyban befolyásolja a légzési ciklus, továbbá a kognitív terhelés (például érzelmi állapot). A mérsékelt vagy csökkenő HF-értékek sok esetben a paraszimpatikus erőforrások apadására, negatív stresszhatásra (például szorongás) vagy nem hatékony erőforrás-felhasználásra utalnak, ami teljesítményromláshoz vezethet.⁷

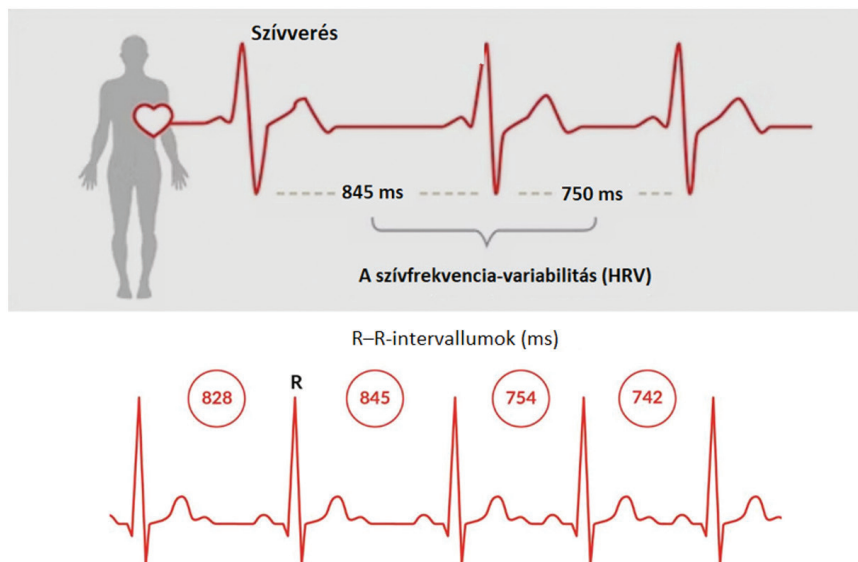
Együttvéve sokféle HRV-mutató létezik, amelyek az idegrendszer eltérő aspektusait reprezentálják, azonban alkalmazhatóságukat minden esetben az adott környezet kontextusában kell értelmezni és értékelni. Az adatok információtartalma számos tényezőtől függ (életkor, nem, fizikai állapot, demográfiai jellemzők), ennek tükrében az eredmények kiértékelései mindig egyéni szubjektív szempontok alapján kell hogy történjenek. Akut stressz, alváshiány, nem megfelelő táplálkozás, mérsékelt fizikai aktivitás vagy tartós pszichikai terhelés esetén (például egy hosszú távú repülésekben érintett repülőgép-vezető esetében) a HRV-értékek csökkenhetnek, ami gyors kimerüléshez és az immunrendszer legyengüléséhez vezet. Ugyanakkor magasabb

⁵ MAKIVIĆ – DJORDJEVIĆ NIKIĆ – WILLIS 2013.

⁶ DONG 2016.

⁷ SCHERER–MARTINEK–MAYR 2019.

HRV-értékek általában kedvezőbb egészségi állapottal, jobb kardiovaszkuláris fittséggel és nagyobb stressztűrő képességgel társulnak.



1. ábra: A szívfrekvencia-variabilitás szemléltetése

Forrás: DUDER 2025

Mentális egészség és a szívfrekvencia

A légi közlekedésben részt vevő szakemberek körében tendenciaként figyelhető meg, hogy mentális egészségi problémáikat – beleértve a súlyosabb tüneteket, például az öngyilkossági gondolatokat – sok esetben nem jelentik vagy nem kommunikálják megfelelő hatékonysággal.⁸ A szívfrekvencia-variabilitás (HRV) fontos objektív biomarkerként jelenhet meg, amelyet mérhető hatékonysággal lehet alkalmazni a depresszió, a poszttraumás stressz-zavar (PTSD), valamint a differens stresszreakciók vizsgálatában. Ezek mellett a HRV-alapú visszajelzési módszerek egyre nagyobb szerepet tölthetnek be a mentális kihívások felszínre kerülésében és prevenciójában. Megfigyelésen alapuló vizsgálatok során megfigyelték, hogy a PTSD releváns összefüggést jelez mind a magas frekvenciájú (HF-HRV), mind az alacsony frekvenciájú (LF-HRV) komponensek csökkenésével.⁹

A HRV adatai az agyi működés tevékeny indikátoraként is felfoghatók: stressz vagy egyéb kognitív terhelés hatására csökkenés figyelhető meg, ami sok esetben párosul az agyi véráramlás mérséklődésével. Ugyanakkor a magasabb HRV-értékek

⁸ Wu et al. 2016.

⁹ Kim et al. 2018.

effektívebb érzelmszabályozással és jobban alkalmazkodó pszichofiziológiai működéssel azonosíthatók. Kutatások alapján az ismétlődő stresszhatások a vegetatív idegrendszer tartós tompulását és a szimpatikus idegrendszer fokozott tevékenységét eredményezhetik, ami fokozott izgalmi állapot kialakulásához vezet. Ez a megállapítás fontos kiindulási pontot biztosít a trauma és a szorongás neurofiziológiai értelmezéséhez, továbbá a terápiás beavatkozások hatékonyságának tárgyilagos vizsgálatához.¹⁰

HRV-vizsgálatok pilóták körében

A repülési környezetben alapvető a lelki-élettani státuszt befolyásoló tényezők vizsgálata az emberi hibák előfordulásának mérséklése szempontjából. Alacsonyabb HRV-értékek adódnak olyan tényezők fennállása esetén, mint a magas testtömegindex, az előrehaladott életkor vagy a megnövekedett feladat-végrehajtás és az azzal járó komplexitás, míg más környezeti mutatók – például a CO₂-koncentráció – nem mutattak jelentős hatást. A megfigyelések egyúttal azt is megvilágítják, hogy a stressz és a teljesítmény közötti kapcsolat nem szükségszerűen lineáris: bizonyos esetekben az emelkedett stressz-szint a teljesítmény javulásával társulhat.¹¹ Valós repülési körülmények között végzett HRV-mérések során – rövid, egyperces R–R-intervallum-szakaszok elemzésével – kimutatták, hogy bár a szimulált és a valós repülések között számszerű különbségek figyelhetők meg, a HRV-változások dinamikája a repülés különböző fázisaiban hasonló mintázatot mutat. Ez a tendencia független attól, hogy a repülés szimulált környezetben vagy valós körülmények között történik. A hasonló HRV-mintázatok elsősorban a repülés kritikus szakaszaiban, például a felszállás, a megközelítés és a leszállás során voltak megfigyelhetők.¹²

A HRV-mérési architektúrák integrálása a pilótafülkébe és repülőgép fedélzetére lehetőséget nyit a valós idejű monitorozás módszerére. Tapasztalatok és megfigyelések alapján az önbevalláson alapuló metódusok önmagukban korlátozott érvényességgel és megbízhatósággal bírnak, míg a HRV-alapú mérés objektívebb képet biztosít a mentális terhelés intenzitásáról, továbbá prediktív képessége is lehet a hibázások előfordulása tekintetében. Ezenfelül megfigyelték repülőgép-vezetők kiképzése során, hogy amikor analóg kijelzőkről digitális rendszerekre térnek át, csökkenés következik be a HRV-értékben, tehát növekszik a stressz-szintjük. Ezek ismeretében a HRV szignifikáns hozzáadott értéket képviselhet a repülési szimulációs képzések során a teljesítményértékelésben.

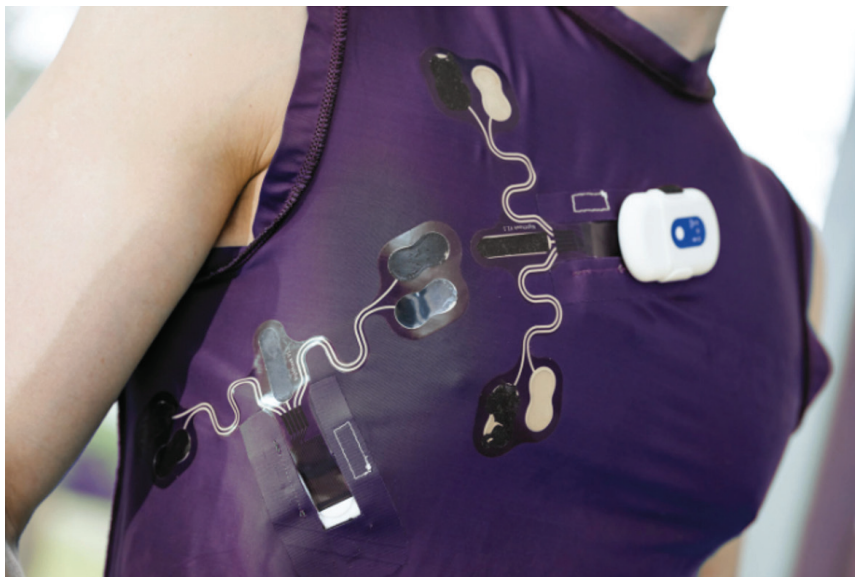
A HRV-adatok elemzése repülések közben lehetőséget biztosít a váratlan eseményekhez kapcsolódó fiziológiai reakciók – például ijedség – detektálására, amelyek szélsőséges esetben jelentős kognitív korlátoltsághoz vagy döntéshozatali blokkoláshoz vezethetnek. A szimulációs környezetben alkalmazott *biofeedback* technológiák elősegíthetik a repülőszemélyzet felkészítését ezen helyzetek megfelelő kezelésére, továbbá hozzájárulhatnak a stresszhez köthető belső élettani válaszok kontrolljához.

¹⁰ THAYER et al. 2012.

¹¹ PORGES 2022.

¹² CAO et al. 2019.

Természetesen az optimális állapot is kifejezésre kerülhet a szívfrekvencia-variabilitás segítségével, elősegítve a szimpatikus és paraszimpatikus idegrendszer kiegyensúlyozott működésének megértését, így a teljesítmény és a megfelelő regeneráció állapota is egyszerűbben indikálható. A HRV-alapú visszajelzők alkalmazása ígéretes eszköznek bizonyul a mentális ellenálló képesség és a pszichés jóllét elősegítésében. Emellett a HRV lehetségesen integrálható a repülőorvosi vizsgálatokba is mint kiegészítő diagnosztikai és beavatkozást segítő eszköz, amely támogatja az egyénre szabott, életmódalapú megközelítéseket különböző egészségügyi és munkakörnyezeti feltételek mellett.¹³



2. ábra: Ruhába épített szenzor

Forrás: www.2mel.nl/wearable-textile-electronics/

HRV a katonai repülésben

A jövőben az egyénre szabott *biofeedback* rendszerek alkalmazása a katonai repülőképzésben a humán-gép együttműködés modernizálódás fontos elemévé válhat. Ezek a rendszerek hozzájárulhatnak az olyan élettani folyamatok vizsgálatához is, amelyek szerepet játszanak a repülési események kialakulásában. A katonai repülésben alkalmazott élettani monitorozás a jövőben többféle mérési módszert is magában foglalhat. Ide tartozhat például a vér oxigénszintjének mérése, a funkcionális közeli infravörös spektroszkópia (*functional near-infrared spectroscopy*, fNIRS), amely infravörös fény segítségével méri a vér oxigénszintjének változását, és ezáltal a véráramlás növekedésén keresztül valós időben képes követni az agyi aktivitást. Emellett az EEG- és EKG-alapú

¹³ MASJET et al. 2023.

mérések is fontos szerepet kaphatnak a pilóták élettani állapotának monitorozásában. Ugyanakkor ezen technológiák egy részének alkalmazása további kutatásokat igényel, különösen a katonai felszerelésbe és a repülőgép fedélzeti rendszereibe történő integráció szempontjából. A HRV-alapú mutatók alkalmasak lehetnek a kognitív terhelés mérésére szimulált katonai környezetben, valamint képesek különbséget tenni sikeres és sikertelen manőverek között is. Ennek megfelelően a HRV-t egyre szélesebb körben alkalmazzák a mentális terhelés kvantitatív értékelésére repülési szimulációk során, hozzájárulva a pilótanövendékek képzésének biztonságosabbá és hatékonyabbá tételéhez. A HRV-t egyéb más mérési módszerekkel együtt több ország légierőinél már jelenleg is alkalmazzák szimulátorokban a stressz és a kognitív terhelés kimutatására, valamint a regeneráció hatékonyságának értékelésére.¹⁴

Összegzés

A megvizsgált és elemzett terület hangsúlyozza, hogy a szívfrekvencia-variabilitás (HRV) meghatározó a repülési környezetben előforduló kognitív terhelés, stressz és fáradtság objektív mérésében. A korszerű, nagymértékben automatizált pilótafülkékben a hagyományos, szubjektív értékelési metódusok egyre inkább elérik alkalmazhatóságuk határait, ezért szükségessé válik olyan megbízható, valós idejű monitorozási procedúrák alkalmazása, amelyek képesek reális képet adni az operátorok aktuális kognitív és fiziológiai állapotáról. A HRV mint fiziológiai marker lehetőséget biztosít az autonóm idegrendszer működésének leképzésére, ezáltal közvetett módon a kognitív terhelés, a stresszreakciók és a regenerációs folyamatok vizsgálatára és értékelésére. A tárgyalt módszerek és eredmények tényekkel igazolják, hogy a HRV nemcsak a pilótai teljesítmény kondíciójának indikátora, hanem prediktív értékkel is szolgálhat a hibavalószínűség és a kifáradás kialakulásának előrejelzésében. A HRV-alapú egységek integrálása a repülőgépek fedélzeti rendszereibe új lehetőségeket kínál a repülésbiztonság növelésében, továbbá a valós idejű megfigyelés, a *biofeedback* alkalmazása, valamint az egyénre szabott képzési és regenerációs eljárások kidolgozása elősegítik a humán teljesítmény optimalizálását és a kockázati tényezők redukálását. Különösen a katonai repülés területén jelenthet áttörést a szívfrekvencia-variabilitás alkalmazása, ahol a szélsőséges körülmények, a magas fokú terhelés és a fokozott stressz adnak értelmet a pontos élettani monitorozásnak. Ezenfelül a HRV integrálása során figyelembe kell venni az egyénenként változó élettani sajátosságokat, valamint a mérési és értelmezési módszerek standardizálását ezen szempontok alapján kell elvégezni. A jövőbeni kutatások kiemelt feladata a különböző HRV-paraméterek validálása repülési környezetben, valamint ezen mutatók integrálása komplex, multimodális élettani monitorozó rendszerekbe.

Összességében megállapítható, hogy a HRV ígéretes, multidiszciplináris megközelítést képviselő eszköz és rendszer, amely jelentősen hozzájárulhat a repülésbiztonság

¹⁴ SHAW–HARRELL 2023.

szintjének növeléséhez, az emberi tényezők mélyebb megértéséhez, valamint a jövő adaptív, intelligens repülési rendszereinek kialakításához.¹⁵

Felhasznált irodalom

- BRANDELLO FARIAS SOARES, Amanda et al. (2025): Heart Rate Variability in Military Pilots During Flight: A Scoping Review. *Military Medicine*, 190(3–4), e515–e522. Online: <https://doi.org/10.1093/milmed/usae390>
- CAO, Xiaodong et al. (2019): Heart Rate Variability and Performance of Commercial Airline Pilots during Flight Simulations. *International Journal Environmental Research Public Health*, 16(2). Online: <https://doi.org/10.3390/ijerph16020237>
- DONG, Jin-Guo (2016): The Role of Heart Rate Variability in Sports Physiology. *Experimental and Therapeutic Medicine*, 11(5), 1531–1536. Online: <https://doi.org/10.3892/etm.2016.3104>
- DUDER, Kate (2025): Your Guide to Heart Rate Variability Tracking–Prevent Burnout and Support Recovery from Illness. *Inside Matters*, 2025. április 23. Online: www.insidematters.co.nz/post/a-guide-to-heart-rate-variability-tracking-prevent-burnout-and-support-recovery-from-illness
- KIM, Hye-Geum et al. (2018): Stress and Heart Rate Variability: A Meta-Analysis and Review of the Literature. *Psychiatry Investigation*, 15(3), 235–245. Online: <https://doi.org/10.30773/pi.2017.08.17>
- LINDSAY, Karen – VAN DEN TOP, Erik (2025): The Utility of Heart Rate Variability in Aviation and Space Medicine. *Journal of the Australasian Society of Aerospace Medicine*, 14(1), 19–26. Online: <https://doi.org/10.2478/asam-2025-0002>
- MAKIVIĆ, Bojan – DJORDJEVIĆ NIKIĆ, Marina – WILLIS, Monte S. (2013): Heart Rate Variability (HRV) as a Tool for Diagnostic and Monitoring Performance in Sport and Physical Activities. *Journal of Exercise Physiology Online*, 16(3), 103–131. Online: <https://bit.ly/4vA3OK9>
- MANSIKKA, Heikki et al. (2015): Fighter Pilots' Heart Rate, Heart Rate Variation and Performance During Instrument Approaches. *Ergonomics*, 59(10), 1344–1352. Online: <https://doi.org/10.1080/00140139.2015.1136699>
- MASI, Giulia et al. (2023): Stress and Workload Assessment in Aviation. A Narrative Review. *Sensors*, 23(7). Online: <https://doi.org/10.3390/s23073556>
- PORGES, Stephen W. (2022): Heart Rate Variability: A Personal Journey. *Applied Psychophysiology and Biofeedback*, 47(4), 259–271. Online: <https://doi.org/10.1007/s10484-022-09559-x>
- SCHERER, Matthias – MARTINEK, Johannes – MAYR, Winfried (2019): HRV (Heart Rate Variability) as a Non-Invasive Measurement Method for Performance Diagnostics and Training Control. *Current Directions in Biomedical Engineering*, 5(1), 97–100. Online: <https://doi.org/10.1515/CDBME-2019-0025>

¹⁵ LINDSAY – VAN DEN TOP 2025.

- SHAFFER, Fred – GINSBERG, J. P. (2017): An Overview of Heart Rate Variability Metrics and Norms. *Frontiers in Public Health*, 5. Online: <https://doi.org/10.3389/fpubh.2017.00258>
- SHAW, David M. – HARRELL, John W. (2023): Integrating Physiological Monitoring Systems in Military Aviation: A Brief Narrative Review of Its Importance, Opportunities, and Risks. *Ergonomics*, 66(12), 2242–2254. Online: <https://doi.org/10.1080/00140139.2023.2194592>
- THAYER, Julian F. et al. (2012): A Meta-Analysis of Heart Rate Variability and Neuroimaging Studies: Implications for Heart Rate Variability as a Marker of Stress and Health. *Neuroscience & Biobehavioral Reviews*, 36(2), 747–756. Online: <https://doi.org/10.1016/j.neubiorev.2011.11.009>
- WANG, Peizheng – HOUGHTON, Robert – MAJUMDAR, Arnab (2024): Detecting and Predicting Pilot Mental Workload Using Heart Rate Variability: A Systematic Review. *Sensors*, 24(12). Online: <https://doi.org/10.3390/s24123723>
- WU, Alexander C. et al. (2016): Airplane Pilot Mental Health and Suicidal Thoughts: A Cross-Sectional Descriptive Study via Anonymous Web-Based Survey. *Environmental Health*, 15. Online: <https://doi.org/10.1186/s12940-016-0200-6>

Papp István,¹ Békési Bertold,² Károly Krisztián³

Pilóta nélküli légi járművek rajirányítási és rakétavezérlési vizsgálata komplex légi műveletek során⁴

Study of Unmanned Aerial Vehicle Flight Control and Missile Guidance During Complex Air Operations

Absztrakt

A pilóta nélküli légi járműveket (UAV) egyre szélesebb körben alkalmazzák mind a katonai, mind pedig a polgári szférában. Az orosz–ukrán háború bebizonyította ezen eszközök létjogosultságát, különösen a rakétahordozó jellegű támadásokban, és kulcsszerepet fognak betölteni a jövőbeni háborúkban mint különleges harci mód. A szerzők összegzik a rakétahordozó támadási művelet irányítási és vezérlési eljárásait, bemutatják az irányító- és vezérlőrendszer hagyományos tervezési megoldásait, ezt követően pedig elemzik a jellegzetes rajtámadás irányítási és vezérlési módszereit a megfelelő jellemzők figyelembevételével, és kitérnek a hagyományos tervezési módszerek korlátjaira. A cikk az intelligens integrált irányítási és vezérlési tervezés előnyeire koncentrál a hagyományos

¹ Gyakorlati oktató, Nemzeti Közszerológati Egyetem Hadtudományi és Honvédtisztképző Kar Repülőfedélzeti Rendszerek Tanszék (Szolnok), e-mail: papp.istvan@uni-nke.hu

² Egyetemi docens, Nemzeti Közszerológati Egyetem Hadtudományi és Honvédtisztképző Kar Repülőfedélzeti Rendszerek Tanszék (Szolnok), e-mail: bekesi.bertold@uni-nke.hu

³ Tanársegéd, Nemzeti Közszerológati Egyetem Hadtudományi és Honvédtisztképző Kar Katonai Repülő Intézet Repülésirányító és Repülő-Hajózó Tanszék (Szolnok), e-mail: karoly.krisztian@uni-nke.hu

⁴ A kutatás a 2022-2.1.1-NL-2022-00012 azonosító számú Kooperatív Technológiák Nemzeti Laboratóriuma projekt a Kulturális és Innovációs Minisztérium Nemzeti Kutatási, Fejlesztési és Innovációs Alapból nyújtott támogatásával, a 2022-2.1.1-NL Nemzeti Laboratóriumok Létrehozása, Komplex Fejlesztése pályázati program finanszírozásában valósul meg.

tervezési ötletekkel szemben. Összegzi az általánosan alkalmazott integrált irányítási és vezérléstervezési módszereket és azok felhasználásait, valamint feltárja az integrált irányító- és vezérlőrendszerhez megfelelő rakétahordozó kooperatív támadási stratégiáját. Megvizsgálja a rakétahordozók irányításának és vezérlésének kihívásait, és feltárja azokat a problémákat, amelyek a jövőben további kutatásra érdemesek. A rakéták irányítási és vezérlési módszereinek összefoglalása hozzájárul az innovatív kutatáshoz ezen a területen, ami elősegíti a pilóta nélküli rajtámadási technológia fejlődését.

Kulcsszavak: UAV, raj, rakéta, irányítás

Abstract

The unmanned aerial vehicles (UAVs) are being used more and more widely in both the military and civilian sectors. The Russian-Ukrainian war has demonstrated the value of these systems, particularly in missile-carrying attacks, and they will play an indispensable key role in future wars as a specialised combat method. The authors summarise the C2 (command and control) procedures for missile-based attack operations, present traditional design solutions for command and control systems, and then analyse the command and control methods for typical swarm attacks while considering relevant characteristics, and discuss the limitations of traditional design methods. The article focuses on the advantages of intelligent integrated guidance and control design over traditional design concepts. It summarizes commonly used integrated guidance and control design methods and their applications, and explores a cooperative attack strategy for missile carriers suitable for an integrated guidance and control system. It examines the challenges of missile guidance and control and identifies issues worthy of further research in the future. The summary of missile guidance and control methods contributes to innovative research in this field, which promotes the development of drone swarm attack technology.

Keywords: UAV, swarm, missile, guidance

Bevezetés

Az UAV elterjedt megnevezés a repülőgépeknek arra a típusára, amelyet precíziós irányítású fegyverként is használhatnak ellenséges célpontok megtámadására (például az öngyilkos UAV [*loitering munition*]).⁵ Az ember irányította vadászgéppel szemben az UAV előnyei a gyors reagálóképesség, az erős mobilitás, a személyi kockázat minimalizálása és a kényelmes, több repülőgép kooperatív működése.⁶ Különösen az UAV-kat értékeli nagyra a katonai erők szerte a világon, például az amerikai hadsereg MQ-1 Predatorját számos gyakorlati csataterén használták: a pakisztáni terrorizmus elleni küzdelemben, az afganisztáni háborúban és az iraki háborúban.⁷ A hiperszonikus,

⁵ MALIK-HAYDAR-ZIAR 2021.

⁶ SHIN 2018: 305.

⁷ HUANG et al. 2022.

mesterséges intelligencia és rajharc technológia csábítása alatt az UAV fokozatosan fontos eszközzé vált a légi harci előnyök megragadásában, fenntartásában, a jövőben pedig a légierő stratégiai és felforgató erejévé fejlődhet.⁸

Jelenleg az amerikai haderő MQ-1 Predator drónjának a földi irányítók közreműködésére van szüksége a támadási folyamat összes láncszemében, a „Földi irányító távvezérlése harci móddal” üzemmódban. A támadási időablak viszont nagyon rövid, és a harctéri szereplők dinamikusán változnak a konfrontációs környezetben. A földi irányításon alapuló hagyományos UAV harci mód nehezen felel meg a precíziós támadás és az időérzékeny célponttalálat követelményeinek. Az UAV autonóm támadási technológiája kritikus fejlesztési irányvá vált.⁹ Az autonóm támadás működési módban az UAV önállóan végzi el a céladatok feldolgozását és fúzióját, a helyzetértékelést, a fegyvercél kiosztását, a repülésirányítást, a fegyverindítást, a támadási célpontot és a műveleti hatékonyság értékelését a műveleti légtérben.¹⁰ Áttöri az „ember a hurokban” korlátait, teljesen kiaknázza a mesterségesintelligencia-technológiát, hogy teljesen kihasználja az UAV működési hatékonyságát, és képes megvalósítani a gyors támadási döntést és irányítást magas dinamikában és erős bizonytalanság mellett.

A drón a harci feladatok összetettsége miatt kooperatív támadással néz szembe, amikor a tényleges harci alkalmazásban vizsgáljuk. Egyetlen drónhoz képest több UAV kooperatív harcrendszert alkothat kölcsönös együttműködéssel, kiegészítő előnyökkel és jelentősen növelt hatékonysággal a repülési térben. Az Amerikai Egyesült Államok Légierője 2009–2047-es drónrendszerének repülési terve rámutat arra, hogy „az automatikus képességről az autonóm képességre való áttéréssel az UAV-k több repülőgép kooperatív műveletét valósítják meg, így egyetlen operátor egyszerre több többcélú UAV-t is megfigyelhet, és a támadás koncentráltabbá, tartósabbá és nagyszabásúbbá válik”.¹¹ Ezért a raj kooperatív működése lesz a több drón autonóm támadási üzemmód elkerülhetetlen fejlesztési trendje.

A *high-tech* pilóta nélküli harci repülőgépek a mostani élvonalbeli technológia, valamint a legfejlettebb harci eszközök ötvözete. Ilyen nagy teljesítményű technikákat a világon csak néhány ország birtokol.¹² Az Egyesült Államok mindig is a pilóta nélküli harci technológia fejlesztésére koncentrált. Az elmúlt években az Egyesült Államok Védelmi Minisztériuma erőteljesen fejlesztette az UAV-technológiát, ami megváltoztathatja a hadviselés jellegét, és beépítette az Egyesült Államok katonai ellentételezési stratégiájának harmadik fejlesztési tervébe. Az amerikai hadsereg már 1994-ben felszerelte az eredeti RQ-1 Predator felderítő pilóta nélküli rendszert lézer megjelölővel és levegő-föld (AGM-114 Hellfire) nagy sebességű rakétával, hogy az MQ-1 Predator támadó UAV-vá fejlődjön, földi precíziós csapásmérő képességgel. 2013-ra az Egyesült Államok sikeresen kifejlesztette az X-47B hiperszonikus lopakodó UAV új generációját. Bár a projekt végül zátonyra futott, ez nem befolyásolja az amerikai hadsereg fejlődését az UAV-technológia területén. 2015-ben az Egyesült Államok Védelmi Minisztériuma Fejlett Védelmi Kutatási Projektek Ügynökségének

⁸ ZHANG–WEI 2021.

⁹ DANIAL et al. 2019: 5.

¹⁰ NOBAHARI–NASROLLAH 2020: 15.

¹¹ ZHOU et al. 2020: 4.

¹² KUCHAR–YANG 2000: 133.

(DARPA) ELF projektje az UAV rajműveleti technológiájának fejlesztését tervezte, amely C-130-as szállító repülőgépekből állt, kölcsönös hálózatépítési és koordinációs képességekkel bocsátottak ki UAV-kat, hogy rajt alkossanak a támadási művelet végrehajtásához. Ugyanakkor az Egyesült Államok Légierőjének jövőbeli műveleti koncepciója először javasolta nagy légi platformok használatát több UAV-kivetési kooperatív támadási harci feladathoz. Ezenkívül az Egyesült Államok haditengerészete a Boeing csapatával karöltve olyan kis pilóta nélküli harci repülőgépeket fejleszt ki, amelyek kooperatív tengeralattjáró-ellenes hadviselésre alkalmazhatók. Ez a fejlesztési projekt mérföldkőnek számított az amerikai hadsereg tengeri harci képességének javításában. Az UAV-technológia fejlesztését illetően a világ más katonai hatalmai nem szeretnék lemaradni, és egymás után versenyezni a katonai parancsnoki szinteken, ahogy az az izraeli Harpy öngyilkos drón és az európai nEUOn UAV esetében történt. A vonatkozó híradások szerint 2016-ban az orosz katonai repülőgépgyártó MIG megállapodást írt alá a Kereskedelmi és Ipari Minisztériummal, és a Ray prototípuson alapuló UAV-projekt megvalósítására készült. Az említett UAV belső fegyverkabinja 2 t tömegű irányítható fegyvert képes szállítani, beleértve a levegő-föld nagy sebességű UAV-kat, síklóbombákat, utazó nagy sebességű UAV-kat és sugárzás elleni nagy sebességű drónokat.

Bár a Kínában fejlesztett UAV-berendezések alkalmasak földi célpontok megtámadására, még mindig jelentős technológiai lemaradás van az UAV autonóm precíziós támadási képessége és kooperatív harci képessége, valamint az Egyesült Államok és más, vezető UAV autonóm harctechnológiával bíró országok között, bonyolult viszonyok közepette, különösen dinamikus harctéri környezetben. Az UAV-raj autonóm támadásának sajátossága, hogy az olyan feladatokat, mint több UAV közös légtérben való irányítása, a környezet és a célok érzékelése, a döntéshozatal és a támadási pálya tervezése, a fegyverindítás és a nagy sebességű pilóta nélküli légi járművek zuhanó támadása, az UAV-k egymástól függetlenül végzik, az üzemeltetők és a külvilág közötti beavatkozás nélkül, és rengeteg együttműködési tényezőt kell figyelembe venni az UAV-k között annak érdekében, hogy teljes mértékben kihasználhassák a rajharc előnyeit, ami nagy kihívásokat jelent az ezen eszközök navigációs/irányító- és vezérlőrendszerének tervezésében.

Az irányítási probléma mindig is a repülőgép alapvető gondja volt. A célészlelés és a pozicionálás tévedése, valamint az UAV-k kooperatív vezérlőrendszer teljesítményének romlása nagymértékben csökkenti az UAV vezérlési pontosságát és támadási precizitását, valamint súlyosan befolyásolja az UAV pontos kooperatív támadási hatékonyságát. Ezért számos nemzetközi kutatóintézet és tudós tanulmányozza az UAV autonóm támadás irányítási és vezérlési technológiáját.

Összefoglalva: a szerzők kutatják és összegzik a nagy sebességű pilóta nélküli légi járművek rajirányítását és vezérlését összetett légi harci környezetben. Először bemutatják a hagyományos irányító- és vezérlőrendszer szétválasztási tervezési gondolatát, elemzik a tipikus rajtámadás irányítási és vezérlési módszereit, és felvázolják a hagyományos tervezési módszerek korlátait. Ennek alapján a cikk az integrált vezérlési és irányítási tervezés előnyeire koncentrál a hagyományos tervezési ötletekkel

szemben, összefoglalja az általánosan használt integrált irányítástervezési módszereket és azok felhasználásait, majd feltárja a rendszerhez megfelelő rajkooperatív támadási stratégiát. Ismerteti a drónrajok irányításának és vezérlésének kihívásait, és bemutatja azokat a problémákat, amelyek a jövőben további kutatásra szorulnak. Végezetül szimulációkkal szemlélteti egy UAV-raj mozgó ellenséges célpont elleni dinamikus támadásait harctéri környezetben.

A tudományos probléma megfogalmazása

A cikk által tárgyalt tudományos probléma az összetett, bizonytalan és magas dinamikájú harctéri környezetben operáló UAV-rajok autonóm, nagy pontosságú kooperatív támadásának megvalósítása, amely a hagyományos, földi távvezérlésen alapuló „ember a hurokban” üzemmód korlátai miatt vált sürgetővé. A fő kihívást az jelenti, hogy az időérzékeny célpontok sikeres megsemmisítéséhez a drónoknak emberi beavatkozás nélkül, teljesen önállóan kell elvégezniük a valós idejű céladatfűzést, a helyzetértékelést, a fegyverkiosztást, valamint a közös légtérben zajló repülésirányítást és pályatervezést. A folyamatot nehezítik a célészlelési és pozicionálási hibák, amelyek a kooperatív vezérlőrendszer teljesítményromlásához vezetnek, drasztikusan csökkentve a támadás precizitását. Mivel a hagyományos irányító- és vezérlőrendszerek szétválasztott tervezési módszerei a korlátaik miatt már képtelenek lekezelni ezeket a komplex tényezőket, a kutatás központi magva egy olyan integrált navigációs, irányítási és vezérlési stratégia kidolgozása, amely képes koordinálni a nagy sebességű pilóta nélküli légi járművek zuhanó támadását és precíz pályaszabályozását.

A rakéta pályájának szabályozása és irányítása

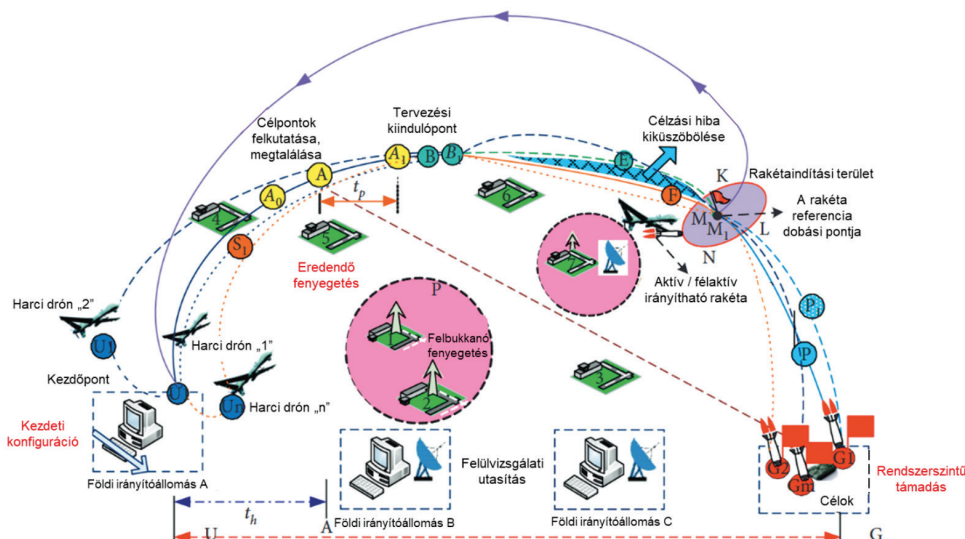
A több rakétát szállító pilóta nélküli harci légi jármű (UCAV) rajának autonóm támadási vázlata az 1. ábrán látható. Tegyük fel, hogy az UCAV-raj „n” számú UCAV-ból áll és az ellenséges célpontok megtámadásának feladatát végzi. Az egyéni UCAV-támadáshoz viszonyítva a rajalapú független támadás egyes szakaszaiban a következő eltérések tapasztalhatók.

UCAV-raj kooperatív repülési szakasz

Az utazó repülési szakaszban a sok UCAV-ból álló rajnak egy bizonyos kooperatív vezérlő mechanizmusra kell támaszkodnia, hogy garantálja több UCAV biztonságos repülését, és raj formájában repüljön a műveleti zónában. Ugyanakkor több ilyen eszköz együttműködési tényezőit is figyelembe kell venni a célkiosztás, a támadási övezet és az optimális indítási pozíció számítása közben.

Nagy sebességű UAV zuhanó támadási szakasz

Néhány kulcsfontosságú vagy speciális célpont vonatkozásában egyetlen rakéta sokszor nem elegendő a teljes megsemmisítés megvalósításához, így több rakétára van szükség a célpont egyidejű vagy meghatározott becsapódási szögben történő megtámadásához. Emiatt a támadási fázisban a több rakéta koordinációja visszatükröződik az összehangolt integrált irányítási és vezérlési stratégiában. A rakéták közötti együttműködési faktorokat átfogóan kell figyelembe venni, hogy konkrét célpontok ellen kooperatív telítettségi vagy szög behatolási támadást lehessen végrehajtani.



1. ábra: A hagyományos irányító- és vezérlőrendszer tervezési módszere

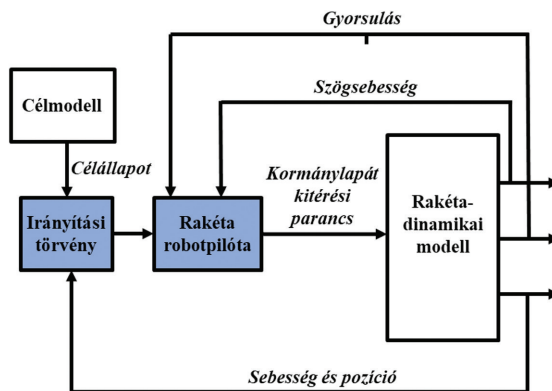
Forrás: a szerzők szerkesztése HUANG 2022: 3 alapján

Az önálló támadás végén a rakétairányító- és rakétavezérlő-rendszer a kulcs az autonóm és pontos támadás kivitelezéséhez, miután a pilóta nélküli légi járművek rakétákat indítanak. A rendszer teljesítőképessége végső soron meghatározza a támadási feladat hatását. Komplex hadműveleti környezetben a drónok és rakéták pontos és időérzékeny csapásmérő képessége a hagyományos irányítási rendszerek hiányosságainak felszámolásán múlik, és az integrált irányítás, valamint az intelligens vezérlési módja teljes mértékben kihasználhatja a különböző funkcionális modellek egymást kiegészítő előnyeit. Mindezek kiemelten fontosak a különböző külső zavarok közötti különbségek kiegyenlítése, a valós idejű kumulatív hiba csökkentése és az általános felügyelet megalapozottságának hatékony javítása érdekében.¹³

¹³ YU et al. 2013: 7.

A hagyományos irányítási rendszer tervezési megközelítése

A 2. ábrán a rakéta hagyományos irányító- és vezérlőrendszer-tervezési gondolata látható. Az elmélet az, hogy szétválasztják az irányítórendszert a vezérlőrendszertől, majd külön hajtják végre a rendszer megtervezését.¹⁴ A hagyományos irányítási és ellenőrzési tervezési mód lényege az irányítási parancs kidolgozásában rejlik. Az irányítási parancsot az irányítási törvény adja meg, majd a repülésirányító rendszer végrehajtja azt, annak érdekében, hogy fenntartsa a stabil repülési helyzetet és elvégezze a harctéri célpontok támadásának és megsemmisítésének feladatát.¹⁵



2. ábra: A hagyományos irányító- és vezérlőrendszer tervezési módszere

Forrás: a szerzők szerkesztése HUANG et al. 2022: 3 alapján

A rakéta precíziós irányítása szempontjából először az arányos irányítási szabályt használták a rakétavezérlő rendszer tervezésénél, amely egyszerű és hatásos módszernek bizonyult.¹⁶ Megtervezték az RBF neurális hálózaton alapuló rakéta háromdimenziós arányos vezérlési törvényét, amely nemcsak a vezérlési pontosságot, de az arányos vezérlési módszer robusztusságát is javította. Az 1970-es években széles körben kezdték alkalmazni az optimális vezérlési szabályt, minimális energiafogyasztással a rakéta sebességvektorának specifikus iránykorlátai szerint.

A rakéták nagyobb hatékonysága és pusztító ereje érdekében le kell küzdeni a repülés közben fellépő becsapódásiszög-korlátozásokat. Ugyanakkor az ellenséges célpontok telítettségi támadásának végrehajtásához meg kell felelni az időkoordinációnak, és a szinkrontámadás megvalósításának is eleget kell tenni. Ezért a multirakéták kooperatív irányítási és vezérlési technológiájának kutatása kiemelt kutatási területté vált.¹⁷ Egy olyan vezérlési szabályt szükséges megvizsgálni, amely a több rakéta cselekvési idejének konzisztenciáján alapuló arányos irányításon nyugszik, és a cselekvési idő hibáját visszajelzésként veszi figyelembe. Ez a módszer nemcsak a nyomkövető látómezőkorlátait kezeli, hanem a fix vagy változó kommunikációs

¹⁴ ZHU–DUAN 2013: 153.

¹⁵ LEVY–SHIMA–GUTMAN 2013.

¹⁶ YUEH–LIN 1984: 740.

¹⁷ YANG et al. 2013.

hálózat alapján a cselekvési idő konzisztenciáját is megvalósítja.¹⁸ Kifejlesztették az optimális irányítási és vezérlési módszert a rakétablokk korlátainak kielégítésére azáltal, hogy optimalizálták a gyorsulási parancs-impulzusokat az irányítórendszerben a becsapódási szög és a gyorsulási korlátozások alapján. A fejlesztő először egyetlen rakétára vonatkozó eltolt arányos irányítási eljárást dolgozott ki, végül hálózatba kapcsolt kooperatív irányítási és vezérlési módszert alakított ki becsapódási szöggel és időkorlátokkal más rakéták hátralévő támadási idejének valós idejű beállításával. A szimulációs eredmények azt mutatják, hogy ez a módszer jobban illeszkedik a támadási idő és a becsapódási szög koordinációjához.¹⁹

A klasszikus felépítés eredményes megoldásnak bizonyult, a rakétatámadás végén az irányítási kör időállandója kisebb lesz, a sávszélesség pedig nagyobb, a rakéta és a célpont közti relatív távolság csökkenésével. Ha a hagyományos metódust alkalmazzuk az irányítórendszer és a vezérlőrendszer tervezéséhez, az gyakorta olyan gondokhoz vezet, mint a nagymértékű tévedési távolság és a repülés instabilitása. Ugyanakkor az irányítórendszer és az ellenőrző rendszer szétválasztása bizonyos nehézségeket is felvet, például a rendszertervezési redundanciát és a magas mérnöki tervezési költségeket, és nem segíti elő a fegyverek általános potenciáljának és hatékonyságának teljes körű kiaknázását, ami súlyosan korlátozza a rakéták precíziós csapásmérő képességét és harci hatékonyságát.

Integrált irányítási és vezérlési megközelítés (IGC²⁰)

Az integrált irányítás és vezérlés, más néven irányítás és vezérlés fúziója és tervezési gondolata immár nem tesz különbséget a vezetőhurok és a vezérlőhurok között, a két hurkot egy egészként vizsgálja. A módszer keretrendszerét a 3. ábra mutatja. A kormánylapát elfordulási szögének felügyeleti parancsa közvetlenül a rakéta célpontjának relatív mozgása és a rakéta saját repülési állapota szerint generálódik, ami nemcsak az instabilitást tudja elkerülni, hanem nagymértékben javítja az irányítási pontosságot is. Ugyanakkor az integrált irányítás és vezérlés csökkentheti a vezérlőrendszer tervezési költségeit, javíthatja a fegyverrendszer általános megbízhatóságát, elősegítheti az alrendszerek közötti koordinációt, és nagymértékben javíthatja a rakéta működési hatékonyságát.²¹ Lényegében az integrált irányítás és vezérlés tervezése a rendszer kimeneti szabályozásának nemlineáris vezérlési problémájára redukálható. Mivel figyelembe kell vennie az irányító- és a vezérlőrendszer közötti erős kapcsolatot, eltér az általános nemlineáris vezérlési módszertől.

A rendszer fejlesztői 1983-ban indítványozták az IGC koncepcióját, a kutatók különféle tervezési eljárásokat javasoltak az integrált irányításra és szabályozásra, főleg az optimális szabályozási módszert, a visszalépéses szabályozási eljárást, a csúszó módú vezérlési módszert, a pályalinearizáló szabályozási módot és a dinamikus felületszabályozási eljárást.²²

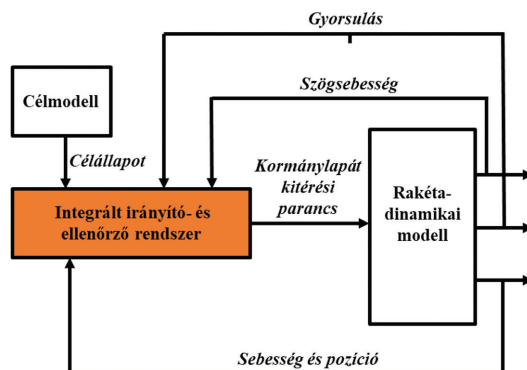
¹⁸ ZHANG-CHEN-SHEN 2013.

¹⁹ GU-ZHAO-ZHANG 2008.

²⁰ IGC: *integrated guidance and control* – integrált irányítási és vezérlési módszer.

²¹ MORGAN-THARP-VINCENT 2011.

²² ZHANYUAN et al. 2021: 244.



3. ábra: Az integrált irányító- és vezérlőrendszer tervezési módszere

Forrás: a szerzők szerkesztése HUANG et al. 2022: 4 alapján

Optimális vezérlési módszer (OC²³)

Az optimális vezérlés a rakéták integrált irányítási és vezérlési (IGC) módszerei közül a legkorábbi. Ezt a taktikai rakétákhoz tervezett rendszert az optimális irányítás és a Bank-to-Turn becslési elmélet alapján alakították ki. A koncepció helyességét és az optimális irányítás hatékonyságát mozgó célpont elleni numerikus szimulációkkal igazolták. Az IGC vezérlési problémát optimális szabályozási problémává transzformálták, és az IGC-vezérlőt a lineáris másodfokú szabályozó módszerrel alkották meg. Az irányítás célja az volt, hogy a kihagyási távolságot nullára redukálják, és biztosítsák a rakéta repülési állapotának stabilitását. A továbbfejlesztett, exponenciális átlag módszert a célpálya előrejelzésére alkalmazták, és a rakéta integrált irányítását és vezérlését nemlineáris optimalizálási problémává alakították át véges időtartományban, és megtervezték a gördülő időtartományú IGC-vezérlési stratégiát a Gauss-pszédo spektrum²⁴ (GPM) módszer alapján. Jóllehet az optimális ellenőrzési módszer egyszerű és hatékony, hátránya a hatékony analitikai megoldás hiányában rejlik.²⁵

Visszalépéses vezérlési eljárás (BC²⁶)

Tipikus nemlineáris szabályozási eljárásként a visszalépés-vezérlésnek megvan az az előnye, hogy jól tudja kezelni a rendszer páratlan bizonytalanságát. Ezért az integrált

²³ OC: *optimal control* – optimális vezérlés.

²⁴ A Gauss-pszédo spektrális módszer hatékony numerikus eljárás nemlineáris optimális vezérlési feladatok megoldására. A módszer a folytonos időtartományú problémát diszkrét nemlineáris programozási (NLP) feladattá transzformálja. Ehhez a rendszerállapotot és a vezérlést globális ortogonális polinomokkal közelíti, a dinamikai egyenleteket pedig specifikus Gauss-kvadratúrapontokban (kollokációs pontok) illeszti.

²⁵ LI-MA 2020: 998.

²⁶ BC: *backstepping control* – visszalépéses vezérlés.

irányítás és vezérlés tervezésénél is alkalmazták.²⁷ A szimulációs eredmények azt mutatták, hogy ez a módszer nemcsak a bemeneti korlátokat képes hatékonyan kezelni, hanem a rendszer bizonytalanságaival szemben is robusztus lehet. A visszalépéses vezérlési eljárás az előlről hátrafelé irányuló rekurzív ötleten alapul. Adaptív és robusztus vezérlésre alkalmas, és egyedülálló előnyökkel rendelkezik a bizonytalanság kezelésében. A virtuális vezérlő ismételt differenciálszámítása azonban túl bonyolult. Ezenkívül ennek a módszernek vannak problémái, mint például a dimenziórobbanás és a paraméterek beállítása.²⁸

Csúszó módú vezérlési módszer (SMC²⁹)

A nemlineáris problémák kezelésekor a csúszó módú vezérlési eljárás előnyei a gyors konvergencia, az egyszerű algoritmus és az erős robusztusság. Ugyanakkor ez a legszélesebb körben használt módszer az integrált irányítási és vezérlési tervezésben is.³⁰ A szimulációs eredmények azt mutatták, hogy ez az eljárás nemcsak a rakétarendszer stabilitását tudja biztosítani, hanem nagymértékben javítja a rendszer válaszidejét és a célpont becsapódási pontosságát is. Aktív zavarelhárítási eljárást terveztek a rakéta IGC-hez, amely csúszó módú vezérlésen és kiterjesztett állapotmegfigyelő technológián alapul. Ez a módszer nemcsak azt biztosítja, hogy a rakéta kis tévedési távolsággal és sima repülési pályával rendelkezzen, hanem a rakétát is robusztussá teszi a rendszer bizonytalanságával és a külső zavarokkal szemben. Ezen eljárásnál létrehozták a rakéta egyfajta referenciamodelljét, és új irányítási törvényt terveztek a visszalépés ötletének és a csúszó módú vezérlő algoritmusnak a felhasználásával, hogy a rakéta erős mobilitással pontosan megtámadhassa a célpontot. A csúszó módú vezérlési módszer legnagyobb hátránya, hogy a rakéta repülése közben pulzáló, magas frekvenciájú hangok sorozata alakul ki. A jelenség zajcsökkentése nehézkes eljárás. A harctéri célpont megtámadásának repülési folyamata során a rakétának nemcsak a gördülést kell minimalizálnia, hanem biztosítani kell a repülési stabilitást és a pálya simaságát is. Ezért a csúszó módú vezérlési eljárásnak nagy korlátai vannak a gyakorlati alkalmazásban.³¹

Pályalinearizációs vezérlési módszer (TLC³²)

Új és hatékony nemlineáris nyomkövetési és szétválasztási szabályozási eljárásként a pályamozgató linearizációs irányítást egyre inkább használják az új rakéták és UAV-k repülésirányító rendszerének tervezésében egyszerű és hatékony vezérlési struktúrája

²⁷ HOU-LIANG-DUAN 2013: 742.

²⁸ Fu et al. 2020.

²⁹ SMC: *sliding mode control* – csúszó módú vezérlés.

³⁰ WILLIAMS-RICHMAN-FRIEDLAND 1983: 60.

³¹ LIN et al. 1998.

³² *Trajectory linearization control method* – pályalinearizációs vezérlési módszer.

miatt.³³ A TLC szempontjából a hiperszonikus jármű a leginkább alkalmazott. A pályalinearizálás és az aktív zavarelutasító vezérlés ötvözésével egy olyan attitűdkövetési módszert alakítottak ki a hiperszonikus járművek visszatérési szakaszára, amely korlátos bizonytalanságok mellett is hatékony, emellett javaslat született egy olyan IGC-pályalinearizációs szabályozási eljárásra is, amely kezeli a jármű egyes csatornáit és a dinamikus korlátok közötti erős csatolást. A szimulációs eredmények azt mutatják, hogy ezen eljárás nagy előnyökkel jár az optimális szabályozási módszerrel szemben a szabályozási teljesítmény tekintetében.³⁴ Robosztus fúziós irányítási és vezérlési módszert terveztek a rakétához, amelyek a pályalinearizációs vezérlésen alapulnak, de ez csupán a hangmagassági csatornára fókuszál. A TLC-módszer tervezésének két fő nehézsége az IGC-rendszer magas rendjében és a rendszer számos bizonytalanságában rejlik, amelyek nagymértékben befolyásolják a TLC-módszer szabályozási pontosságát és robusztusságát.³⁵

Dinamikus felületszabályozási eljárás (DSC³⁶)

A visszalépéses vezérlési metódus és a csúszó módú vezérlési eljárás tárgyrobbanás problémájának megoldása érdekében a kutatók először a dinamikus felületszabályozási módszert javasolták. Az alapgondolat az, hogy az eredeti visszaléptetési vezérlés első és hátsó kétlépcsős vezérlési törvények kidolgozása között elsőrendű aluláteresztő szűrőt adjon, hogy kikerülje egyes nemlineáris jelek közvetlen differenciálását a következő fázisban. A szűrő bevezetése okán az egyes lépésvezérlők kialakítása lényegében különválik az előző szekció kidolgozásától. Egy sokkal egyszerűbb „felületi” vezérlési gonddal kell foglalkoznia, ami mérsékli a vezérlő megtervezésének komplexitását. Eddig a dinamikus felületszabályozási módszert számos mérnöki gyakorlatban sikeresen alkalmazták, továbbá az integrált vezetés és szabályozás megtervezésében használták. Számításba vették az előző látásmód korlátait, megtervezték a Ljapunov-függvényen és a dinamikus felületszabályozáson alapuló fúziós irányítási és vezérlési módszert, és bizonyították az IGC-rendszer stabilitását, Barbalat-lemma és Ljapunov stabilitási tétel³⁷ alkalmazásával dinamikus felületi fúziós irányítási és vezérlési módszert terveztek meg a rakéta rendszerében rögzített célokhoz, terminális leszállási szögkorlátozásokkal. A kooperatív fúziós irányításban és szabályozásban kevés szakirodalom alkalmazza a dinamikus felületszabályozási metódust. A fejlesztők megtervezték a kooperatív fúziós irányítási

³³ MENON–OHLMEYER 2001: 7.

³⁴ ZHAO–ZHOU 2016.

³⁵ SHARMA–RICHARDS 2004.

³⁶ DSC: *dynamic surface control* – dinamikus felületszabályozó vezérlés.

³⁷ A Barbalat-lemma és Ljapunov stabilitási tétel középpontjában a differenciálegyenlet stabilitásának vizsgálata áll. A Barbalat-lemma a differenciálegyenlet stabilitásának vizsgálata során a sajátértékek és a Routh–Hurwitz-kritérium segítségével stabil, instabil, centrális altér kategorizálását teszi. A Ljapunov stabilitási tétel pedig a differenciálegyenlet stabilitásának vizsgálata – sajátértékek segítségével, a Ljapunov stabilitási és instabilitási tételekkel, az aszimptotikus viselkedés vizsgálata során, az ω -határhalmaz fogalma és tulajdonságai, valamint az egyensúlyi pont stabilitás vizsgálata – linearizálással.

és szabályozási eljárást a dinamikus felületszabályozás alapján. Ez az eljárás azonban a hangmagasság-csatorna rögzített célpontját célozza meg, miközben a dinamikus rendszer változó sebessége csökkenti az IGC-rendszer tervezésének nehézségeit. Emiatt a kutatók egy dinamikus felületi irányításon alapuló multirakétás kooperatív fúziós irányítási és szabályozási módszert dolgoztak ki, ám ez kizárólag a földi rögzített célpontokat célozza meg, ami nagymértékben korlátozza a módszer felhasználhatóságát. A dinamikus felületszabályozási módszer a fúziós irányítási és szabályozási problémát a rendszer egyes állapotainak nemlineáris szabályozási problémájává formálja. Az irányítási cél világos, és a kihívás az, hogy miként lehet fejleszteni az IGC dinamikus felületi irányításának alkalmazkodóképességét és robusztusságát, amikor maga a rakétarendszer rendelkezik vezérlő bemenet telítettséggel, és a rendszerben nemlineárisan paraméterezett, nem egyező bizonytalanság van.³⁸ A különbségeket és az összehasonlítást az 1. táblázat mutatja be.

1. táblázat: Az integrált irányítási és vezérlési módszerek különbsége és összehasonlítása

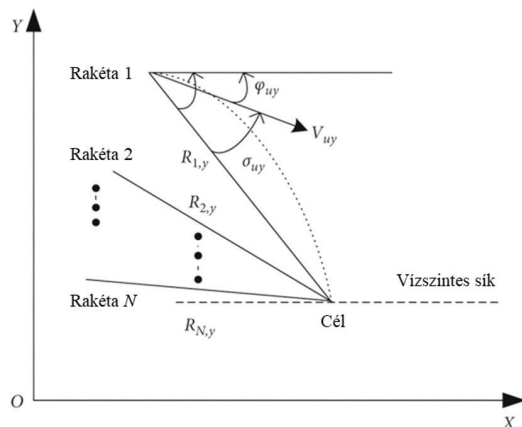
Módszerek	Előnyei	Hátrányai
Optimális szabályozás (OC)	A tervezés egyszerű és könnyen megvalósítható	A rendszerből hiányzik a hatékony analitikai megoldás
Visszalépés-szabályozás (BC)	Jól megbirkózik a bizonytalansággal	Ez az elem robbanási problémájához vezethet
Csúszó mód vezérlési módszer (SMC)	Gyors konvergenciával, egyszerű algoritmussal és erős robusztussággal rendelkezik	Problémája van a <i>chattering</i> jelenséggel
Pályalinearizációs vezérlési módszer (TLC)	A leválasztási ellenőrzési struktúra egyszerű	A bizonytalanságok magas rendje és nagy száma
Dinamikus felületszabályozási eljárás (DSC)	Leküzdheti az elemrobbanás problémáját	Javítani kell a bemeneti telítettség robusztusságát

Forrás: a szerzők szerkesztése

Együttműködési taktika a rajtámadáshoz

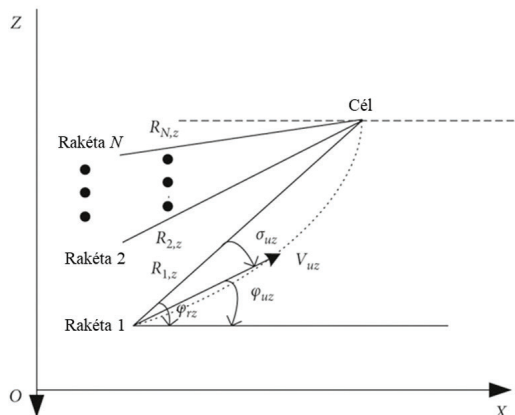
A megszokott klaszter kooperatív támadási műveleti elgondolást a 4. és az 5. ábra szemlélteti, amelyek az egy célpontot támadó N számú rakéta viszonylagos mozgási kapcsolatait a hosszanti és az oldalirányú síkban mutatják be.

³⁸ SHIMA–IDAN–GOLAN 2006: 255.



4. ábra: Relatív mozgás hosszanti síkban

Forrás: a szerzők szerkesztése HUANG et al. 2022: 6 alapján



5. ábra: Relatív mozgás az oldalsíkban

Forrás: a szerzők szerkesztése HUANG et al. 2022: 6 alapján

Amikor több nagy sebességű pilóta nélküli légi jármű együttműködik a harctéri célpontok megtámadásában, átfogóan figyelembe kell venniük az együttműködést a repülési folyamatban, és meg kell felelniük a végső támadási idő vagy támadási szög koordinációs követelményeinek. Az optimális irányítás ötlete alapján a kutatók a hajóelhárító nagy sebességű pilóta nélküli légi jármű támadási időszabályozási irányítási törvényét javasolták.³⁹ Beállították a hibakifejezést az előre beállított támadási idő és a hátra lévő támadási idő között, hozzáadták az arányos irányítási törvényhez, és új irányítási törvényt terveztek a csúszó módú vezérlési módszerrel, hogy az biztosítsa az előre beállított támadási időkorlátok betartását. Sem a támadási időszabályozási

³⁹ Huo et al. 2017.

törvény, sem a csúszó módú irányítási törvény nem veszi teljes mértékben figyelembe a drónok repülési folyamatában való kölcsönhatást és együttműködést.⁴⁰ Ezenkívül a hivatkozások a kooperatív irányelvek és a kooperatív arányos iránymutatási szabály kétrétegű szerkezetét hozták létre. A harci repülés alatt a hátralévő támadási időt online adatkapcsolaton keresztül elosztják a nagy sebességű pilóta nélküli légi járművek között, és valós időben módosítják saját repülési helyzetüket a végső támadási idő egyeztetése végett.⁴¹ A támadási szög koordinációját illetően kooperatív irányítást fejlesztettek ki a támadási idő és támadási szög korlátozásaival a csúszó mód szabályozása és az általánosan alkalmazott látószög-beállítási technika, valamint a másodrendű csúszó mód eljárás révén, amiatt, hogy megfeleljen a támadási idő és a támadási szög korlátainak. Kidolgozták az eltolásos arányos irányítási törvényét a visszalépés-szabályozási módszer használatával, amelyben az eltolási komponens átfogóan figyelembe vette a támadási idő és a támadási szög hibáját.⁴²

A támadási idő koordinációjával összefüggő fenti kutatásban elkerülhetetlen a hátralévő támadási idő megállapítása. A becslési pontossága nagy hatással van a pilóta nélküli légi járművek végső irányítási pontosságára. A gyakorlati alkalmazásokban rendkívül nehéz pontosan megbecsülni a hátralévő támadási időt, különösen a támadási idő korlátaival rendelkező irányítási törvény kidolgozásában; a nagy sebességű pilóta nélküli légi járműveknek gyakran különböző manőverekre van szükségük a végső támadási idő koordinációjának eléréséhez. A kooperatív irányítási törvénynek nem kell megbecsülnie a hátralévő támadási időt, a tervezett vezérlő túl specifikus, és meghibásodik, ha a támadási vezetési szög nulla, ezért nehéz a gyakorlati mérnöki munkában alkalmazni. A leszállási szög megkötésű nagy sebességű UAV irányítási problémájában a jelenlegi kutatás elsősorban a hagyományos irányítási törvény kidolgozására koncentrál, és nem veszi figyelembe a támadási szög korlátozását. Ezért tovább kell vizsgálni a kooperatív fúziós irányítást és a támadási szög szabályozását.⁴³

Kihívások és lehetőségek

Keletkező nehézségek

Javítani kell a fúziós irányítás és a rakétahordozó irányításának precizitását és stabilitását

Az UAV-támadás végső szakaszában a megszokott irányítórendszer és vezérlőrendszer tervezési technikái hajlamosak olyan gondokra, mint a nagy kihagyási távolság és a repülés instabilitása. Az integrált irányítás és ellenőrzés kialakításánál a meglévő módszerek eltérő szintű hiányosságokkal rendelkeznek. Ezzel szemben, habár a pálya linearizációs szabályozási módszere egyszerű és könnyen megvalósítható és jó szabályozási hatású, az IGC-rendszer magasrendű és nagy mennyiségű bizonytalanságának

⁴⁰ HONG et al. 2017.

⁴¹ JIAN et al. 2016.

⁴² ZHU-SHEN 2015.

⁴³ ZHOU et al. 2015.

kezelése ebben a módszerben két nehézséggé vált a komplex dinamikus környezetben. A nagy sebességű pilóta nélküli légi járművek IGC vezérlési pontosságát és robusztusságát még fejleszteni kell.

Nehéz kivitelezni a rakétahordozó irányítási és vezérlési stratégiáját

Jelenleg kevés szakirodalom vizsgálja a kooperatív integrált irányítási és vezérlési problémát, amely még az előzetes kutatási stádiumban van, és a hátralévő támadási idő becslésén alapuló kooperatív integrált irányítási és vezérlési stratégia nehezen alkalmazható. Ugyanakkor a tervből hiányzik a rendszer stabilitásának és robusztusságának problémáira vonatkozó teljes körű figyelembevétele és alapos kutatása, amelyeket a nagy sebességű UAV nemlinearitása és időbeli változékonysága, a nagy sebességű UAV aerodinamikai paramétereinek zavarása és a bemeneti telítettség korlátozása okoz.

A nyomon követési kutatás kilátásai

Nagy sebességű pilóta nélküli légi járművek és rakétahordozók IGC-vezérlőjének paraméterhangolására irányuló kutatás

A nagy sebességű UAV IGC-vezérlő paramétereinek nagyrészt bizonyos logikai levezetésekkel és ismételt próbálkozásokkal és hibákkal nyerjük. A számos szabályozási törvényi, szűrőállandó és zavarmegfigyelő paraméterek miatt a hibakeresési idő hosszú és nehézkes. Ezért a kooperatív IGC-vezérlő paraméterhangolási módszerének kutatása egy másik mélyreható vizsgálatra érdemes téma.

A rakéta (nagy sebességű UAV és raj kooperatív) vezérlőrendszerének műszaki megvalósítására irányuló kutatás

A vezérlési metódus tervezésekor, habár bizonyos tanulmányok figyelembe veszik az olyan szempontokat, mint a parancskészség, a bemeneti telítettség és a dinamikai határérték, nem veszik figyelembe a valós vezérlőrendszer nemlineáris bizonytalan jellemzőit, mint például a hiszterézist és a holtzónát, amelyek még mindig bizonyos távolságra vannak a műszaki megvalósítástól.⁴⁴

Szimulációk

A szimuláció egy (3) UAV-ból álló raj és egy indított rakéta mozgását modellezi egy védett, mozgó ellenséges célpont ellen dinamikus harctéri környezetben. A raj tagjai

⁴⁴ ZHANG et al. 2020.

koordinálják a pozíciójukat (konvergálnak a célra), miközben a rakéta az autonóm fázisoknak megfelelően, záró fázisú arányos navigációs (*proportional navigation*) vezérléssel semmisíti meg a célt.

Dinamikai modellek felírása

A raj tagjainak ($i = 1, 2, 3$) és a rakétának (m) kétdimenziós kinematikai egyenleteit az alábbi (1) és (2) differenciálműveletek írják le

$$\dot{x}_i = v_i \cos(\theta_i), \quad \dot{y}_i = v_i \sin(\theta_i) \quad (1)$$

$$\dot{x}_m = v_m \cos(\theta_m), \quad \dot{y}_m = v_m \sin(\theta_m) \quad (2)$$

Ahol (x, y) a pozíciókoordináták, (v) a sebességek, (θ) pedig a haladási irányok (pályaszögek).

Kooperatív rajirányítási törvény

A drónok közötti konszenzusos együttműködést egy kétszintű irányítási törvény biztosítja, amely minimalizálja a célponttól mért távolságot, miközben fenntartja a raj kohézióját

$$u_i = -k_d(p_i - p_{target}) - k_c \sum_{j \in N_i} (p_i - p_j) \quad (3)$$

Ahol $p = [x, y]^T$ a pozícióvektor, $k_d = 0,15$ a célratartás erősítése, $k_c = 0,08$ a drónok közötti kooperációs együtttható.

Rakétavezérléses arányos navigáció (PN)

A rakéta indítása után a vezérlőrendszer a látóvonal szögsebességét $\dot{\lambda}$ használja fel a szükséges oldalgyorsulási parancs (a_n) kiszámítására:

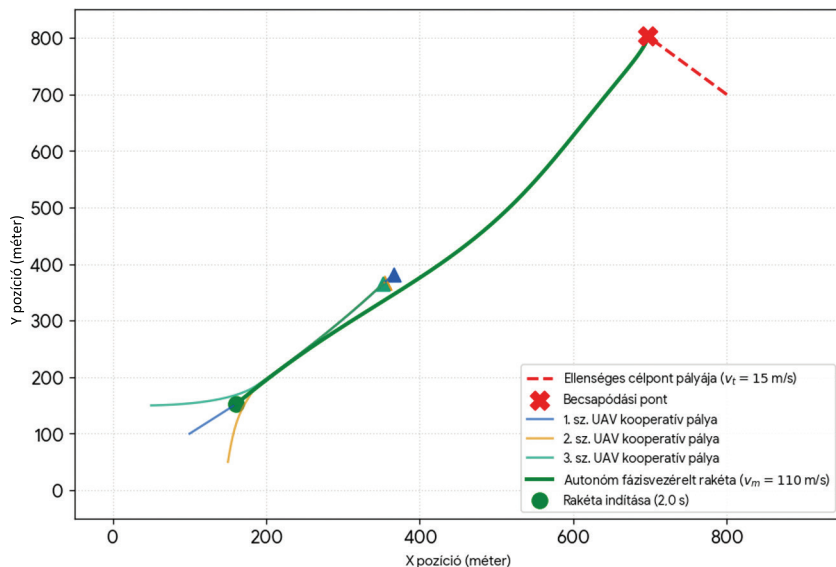
$$a_n = N v_r \dot{\lambda} \quad (4)$$

Ahol $N = 4,0$ a navigációs állandó, v_r a relatív sebesség, a látóvonal szög pedig:

$$\lambda = \arctan 2(y_{target} - y_m, x_{target} - x_m) \quad (5)$$

Időléptetéses szimuláció

A lefuttatott numerikus szimuláció, amely a 6. ábrán látható, igazolja cikkünk azon állítását, miszerint a mesterségesintelligencia-alapú autonóm vezérlés képes áttörni az „ember a hurokban” korlátokat dinamikus környezetben is.



6. ábra: UAV-rajkooperáció és autonóm fegyvervezérlés komplex légi műveletben

Forrás: a szerzők szerkesztése Python NumPy matematikai szoftverrel lefuttatott szimuláció alapján

A grafikon egy komplex légi harcászati szimuláció kétdimenziós (X , Y) koordináták méterben megadott helyzetképét mutatja be az idő függvényében.

Ellenséges célpont (piros szaggatott vonal és X): egy lassabb (15 m/s), egyenes vonalban haladó ellenséges objektum pályája. A piros X jelzi a becsapódási pontot, ahol a megsemmisítés megtörtént.

UAV-rajkooperáció (kék, sárga és világoszöld görbék): három különböző pontból induló drón pályáját mutatja. Jól látható, hogy a kezdeti szétszórt formációból a kooperatív algoritmus hatására a görbék gyorsan egy közös, rendezett alakzatba (rajba) konvergálnak, majd együtt repülnek a cél felé. A kis háromszögek a drónok pozícióját mutatják a szimuláció végpontjában.

Rakéta indítása (zöld kör): a 2,0 másodperces repülési időnél az egyik hordozó UAV elvégzi a helyzetértékelést, és elindítja a saját rakétáját az $X \approx 160$, $Y \approx 150$ koordinátáknál.

Autonóm fázisvezérelt rakéta (vastag zöld egyenes): a rakéta a leválás után rendkívül nagy sebességgel (110 m/s) halad. Az arányos navigációs (PN) vezérlésének köszönhetően nem közvetlenül a cél pillanatnyi helyzetét követi, hanem a jövőbeli pályáját kalkulálva egyenesen a találkozási (becsapódási) pontba navigálja önmagát.

Kiszámíthatatlan, cikcakk vonalú kitérő manőverek (evasive manoeuvres)

A 6. ábrán bemutatott elméleti modell gyakorlati kiterjesztéseként az alábbiakban részletesen bemutatunk két környezeti és harcászati tényezőt (a kiszámíthatatlan kitérő manőverek és a szélterhelés) matematikai modellezését, valamint vizsgáljuk azok hatását a rakéta arányos navigációs (PN) vezérlésére.

A manőverező célpont matematikai modellje

A célpont (t) irány szöge (θ_t) egy alapirányból, egy harmonikus (szinuszos) kitérésből és egy véletlenszerű (úgynevezett fehér zaj) zavarból tevődik össze. Az összefüggést a (6) egyenlet írja le.

$$\theta_t(t) = \theta_0 + A \sin(\omega t) + \eta(t) \quad (6)$$

Ahol:

$\theta_0 = 135^\circ$: az alapvető haladás iránya, $A = 0,5 \text{ rad/s} \approx 28.6^\circ$ a kitérés maximális amplitúdója (a cikcakk élessége), $\omega = 1,5 \text{ rad/s}$ a manőverezés frekvenciája (milyen gyorsan vált irányt), $\eta(t)$ pedig a Gauss-féle fehér zaj ($\sigma = 0,05$), amely a kiszámíthatatlan, hirtelen instabil működést (lengéseket) szimulálja.

A vezérlésre és a pályára gyakorolt hatásokat megvizsgálva a következőket állapíthatjuk meg:

- A folyamatos irányváltások miatt a látóvonal (*line of sight*) szögsebessége ($\dot{\lambda}$) konstans érték helyett hevesen oscillál, tehát a LOS szögsebessége ingadozik.
- Megnövekedett túlterhelésigény mutatkozik, mivel az arányos navigációs parancs $a_n = N v_r \dot{\lambda}$, a rakétának folyamatosan korrigálnia kell. Ez a rakéta részéről sokkal nagyobb oldalgyorsulást (G-erőt) és jelentős mozgásenergia-vesztést igényel.
- A rakéta a kanyargós pálya miatt már nem egyenes vonalon repül a becsapódási pontig, hanem S-alakú, finoman korrigáló görbét ír le, megpróbálva lekövetni a célpont jövőbeli pozícióját.

Szélterhelés és légköri zavarok (*wind disturbance & gusts*)

A szél külső aerodinamikai zavaró tényező, amely oldalirányban eltéríti mind a drónokat, mind a rakétát a tervezett pályájukról. A szélhatást egy konstans háttérszél és egy hirtelen fellépő szélleökés (szélnyírás) összegeként modellezzük.

A *szélterhelés matematikai modelljének* felírásakor a szélesebességvektort ($\vec{W} = [W_x, W_y]$) hozzáadjuk az eszköz saját hajtóereje által biztosított sebességkomponensekhez. A szél modelljét a (7) és (8) egyenletek írják le.

$$W_x(t) = W_{cst,x} + W_{gust} \cos \phi_{gust} \quad (7)$$

$$W_y(t) = W_{cst,y} + W_{gust} \sin \phi_{gust} \quad (8)$$

Ahol $W_{cst} = [12,0 - 5,0] m/s$ folyamatos, konstans északnyugati háttérszél, W_{gust} egy diszkrét széllokés (például a 4. és 6. másodperc között), amelyet az úrha-józásban és katonai szabványokban használt „1-minus-cosine” profillal modellezzünk [(9) egyenlet].

$$W_{gust}(t) = \frac{A_g}{2} \left(1 - \cos \left(\frac{2\pi(t-t_s)}{T_g} \right) \right) \quad (9)$$

Ahol $A_g = 25 m/s$ a széllokés ereje, $t_s = 4,0 s$ a kezdete, és $T_g = 2,0 s$ a lefutási időtartama.

A vezérlésre és a pályára gyakorolt hatása három tényezőt von maga után:

- Amennyiben a vezérlőrendszer nem kompenzálja, a szél egyszerűen elfújja a rakétát a cél mellett. A valóságban a rakéta sebességvektora elfordul az aktuális haladási iránytól (csúszásszög alakul ki). Ez az úgynevezett sodródás (*drift*).
- Módosult kinematikai egyenletek, ami annyit jelent, hogy a szimulációs hurokban a pozíciófrissítés az alábbiak szerint módosul:

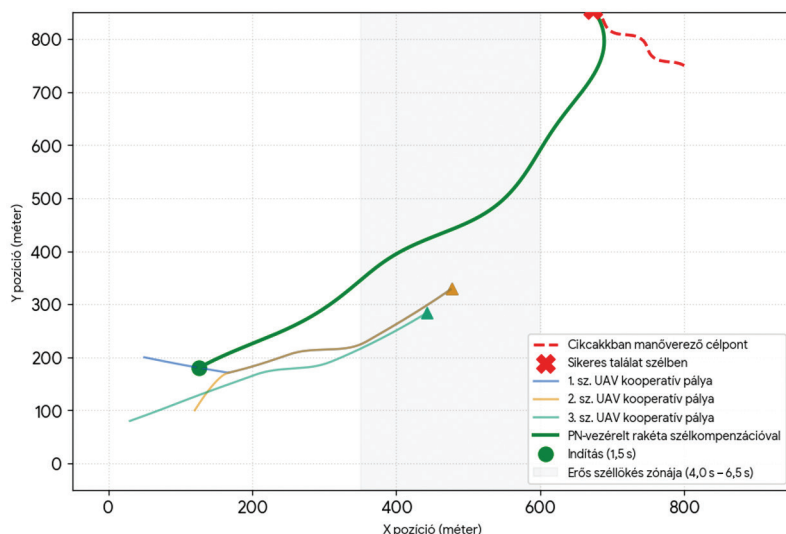
$$\dot{x}_m = v_m \cos(\theta_m) + W_x(t) \quad (10)$$

$$\dot{y}_m = v_m \sin(\theta_m) + W_y(t) \quad (11)$$

- A kormányfelületek leterheltsége tekintetében, amikor a rakéta belép a széllokés zónájába (4. másodperc), a látóvonal hirtelen elugrik. A PN-algoritmus ezt a célpont manővereként érzékeli, és azonnali, agresszív kormánymozdulattal válaszol.

A 7. ábrán a fentiek alapján részletezett kibővített numerikus szimulációt futtattuk le. A modellben a célpont kiszámíthatatlan cikcakkmanővereket végez, miközben a teljes légtérben erős északnyugati szél és egy hirtelen fellépő széllokés terheli az eszközt. A grafikonon ez a szakasz hirtelen törésként vagy irányváltási dudorként jelenik meg a zöld vonalon, amelyet a rakéta a szélzónát elhagyva csillapít le, hogy végül biztosítsa a találatot.

A grafikonon jól láthatók a bevezetett fizikai és harcászati módosítások közvetlen hatásai. Először is a célpont kiszámíthatatlansága (piros szaggatott vonal) egyértelműen mutatja a cikcakkos, hullámozó és kitérő manővereket. A célpont folyamatosan változtatta az irányát, hogy megnehezítse a befogást. Továbbá a (szélterhelés és sodródás) szürke sávval jelzett széllokészónájában (350 és 600 m között) a drónok és a rakéta pályáján egyaránt megfigyelhető az oldalirányú eltolódás. A szél megpróbálta délkeleti irányba elfújni a fegyvert. Végül a zöld vonal íve (intelligens PN-korrekció) mutatja, hogy az arányos navigációs algoritmus sikeresen reagált. Amikor a széllokés és a célpont hirtelen irányváltása együttesen lépett fel, a rakéta vezérlőrendszere agresszív pályamódosítással válaszolt, áttörte a zavaró tényezőket, és a végfázisban pontos közvetlen találatot (X) ért el.



7. ábra: Zavart környezeti szimuláció (manőverező célpont és szélterhelés)

Forrás: a szerzők szerkesztése Python NumPy matematikai szoftverrel lefutott szimuláció alapján

Kvantitatív eredmények

A cikk kvantitatív elemzése rávilágít, hogy az UAV-k fejlesztése 38 éves stratégiai időtávot (2009–2047) ölel fel, amely során a technológia a 7 egymásra épülő fázisból álló autonóm támadási folyamat irányába mozdul el. A hadtörténeti evolúció 4 fő mérföldkövön keresztül (1994, 2013, 2015, 2016) mutatja be a rendszerek fejlődését, amelyben 5 globális szereplő (USA, Izrael, Európa, Oroszország, Kína) verseng egymással. A cikkben vizsgált 6 konkrét dróntípus és projekt közül kiemelkedik az orosz Ray prototípus, amely 2 t-s belső fegyverkabin-kapacitással rendelkezik és 4 különböző típusú irányítható fegyver hordozására alkalmas. Ez a strukturális elmozdulás a korábbi, korlátozott hatékonyságú „egy operátor – egy gép” modelltől a mesterséges intelligencia által vezérelt, külvilági beavatkozás nélküli, tömeges rajtámadások felé mutat.

Összefoglalás

Jelen kutatás a nagy sebességű pilóta nélküli légi járművek rajirányítását és vezérlését vizsgálja összetett légiharc környezetben, például a rakétahordozóban. Bemutattuk a hagyományos irányító- és vezérlőrendszer elválasztási tervezési elgondolását, elemeztük a tipikus rajtámadás-irányítási és vezérlési módszereket, és megadtuk a hagyományos tervezési módszerek korlátait, amelyek súlyosan akadályozzák a rakéták precíziós csapásmérő képességét és harci hatékonyságát. A cikkben vizsgáltuk az integrált vezérlési és irányítástervezés előnyeit a hagyományos tervezési elképzelésekkel

szemben, és összefoglaltuk az általánosan használt integrált vezérlési és irányítástervezési módszereket és azok alkalmazásait. Feltártuk az integrált vezérlő- és irányítórendszerhez megfelelő rajkooperatív támadási stratégiákat, ismertettük a rakétahordozók irányításának és vezérlésének kihívásait, és részleteztük azokat a problémákat, amelyek a jövőben további kutatásra érdemesek. Végül rajirányítási és rakétavezérlési numerikus szimulációkat futtattunk le és elemeztük azokat. A jelenlegi háborús helyzet, valamint a drónok széles körű alkalmazása miatt, a fentebb taglalt rendszerek tervezése, a kooperatív intelligens integrált irányítás és vezérlés lehet e széles körű téma következő kutatási gócpontja.

Felhasznált irodalom

- DANIAL, Syed Nasir et al. (2019): Situation Awareness Modeling for Emergency Management on Offshore Platforms. *Human-centric Computing and Information Sciences*, 9(37), 1–26. Online: <https://doi.org/10.1186/s13673-019-0199-0>
- FU, Zhenhua et al. (2020): Integrated Guidance and Control with Input Saturation and Impact Angle Constraint. *Discrete Dynamics in Nature and Society*. Online: <https://doi.org/10.1155/2020/5917983>
- GU, Wenjin – ZHAO, Hongchao – ZHANG, Ruchuan (2008): A Three-Dimensional Proportional Guidance Law Based on RBF Neural Network. *Proceedings of the 7th World Congress on Intelligent Control And Automation, Chongqing, China*, 6978–6982. Online: <https://doi.org/10.1109/wcica.2008.4593997>
- HONG, Toan Dinh et al. (2017): Active Disturbance Rejection Control Design for Integrated Guidance and Control Missile Based SMC and Extended State Observer. *Proceedings of the 2017 International Conference on System Science and Engineering, Ho Chi Minh City, Vietnam*, 476–481. Online: <https://doi.org/10.1109/ICSSE.2017.8030920>
- HOU, Mingzhe – LIANG, Xiaoling – DUAN, Guangren (2013): Adaptive Block Dynamic Surface Control for Integrated Missile Guidance and Autopilot. *Chinese Journal of Aeronautics*, 26(3), 741–750. Online: <https://doi.org/10.1016/j.cja.2013.04.035>
- HUANG, Hanqiao et al. (2022): Intelligent Guidance and Control Methods for Missile Swarm. *Computational Intelligence and Neuroscience*. Online: <https://doi.org/10.1155/2022/8235148>
- HUO, Ran et al. (2017): Integrated Guidance and Control Based On High-Order Sliding Mode Method. *Proceedings Of the 36th Chinese Control Conference, Dalian, China*, 6073–6078. Online: <https://doi.org/10.23919/chicc.2017.8028323>
- JIAN, Chen et al. (2016): Integrated Guidance and Control Design Based on a Reference Model. *International Journal of Control, Automation and Systems*, 14(5), 1299–1308. Online: <https://doi.org/10.1007/s12555-015-0048-5>
- KUCHAR, James K. – YANG, Lee C. (2000): A Review of Conflict Detection and Resolution Modeling Methods. *IEEE Transactions on Intelligent Transportation Systems*, 1(4), 179–189. Online: <https://doi.org/10.1109/6979.898217>

- LEVY, Mital – SHIMA, Tal – GUTMAN, Shaul (2013): Linear Quadratic Integrated versus Separated Autopilot-Guidance Design. *Journal of Guidance, Control, and Dynamics*, 36(6), 1722–1730. Online: <https://doi.org/10.2514/1.61363>
- LI, Rui – MA, Hongzhong (2020): Research on UAV Swarm Cooperative Reconnaissance and Combat Technology. *Proceedings of the 2020 3rd International Conference on Unmanned Systems (ICUS), Harbin, China*, 996–999. Online: <https://doi.org/10.1109/icus50048.2020.9274902>
- LIN, Ching Fang et al. (1998): Optimal Design of Integrated Missile Guidance and Control. *Proceedings of the World Aviation Conference*, 1–13. Online: <https://doi.org/10.2514/6.1998-5519>
- MALIK, Zishan et al. (2021): Cooperative Guidance Scheme for Flight of Multiple Combat Uavs Against a Non-Accelerating Moving Target. *Proceedings of the 2021 International Bhurban Conference on Applied Sciences and Technologies (IBCAST)*. Islamabad. Online: <https://doi.org/10.1109/ibcast51254.2021.9393309>
- MENON, P. – OHLMEYER, Ernest J. (2001): Nonlinear Integrated Guidance-Control Laws for Homing Missiles. *Proceedings of the AIAA Guidance, Navigation, and Control Conference and Exhibit, Montreal, Canada*, 1–9. Online: <https://doi.org/10.2514/6.2001-4160>
- MORGAN, Robert Wes – THARP, Hal – VINCENT, Thomas L. (2011): Minimum Energy Guidance for Aerodynamically Controlled Missiles. *IEEE Transactions on Automatic Control*, 56(9), 2026–2037. Online: <https://doi.org/10.1109/tac.2011.2108619>
- NOBAHARI, Hadi – NASROLLAHI, Saeed (2020): A Nonlinear Robust Model Predictive Differential Game Guidance Algorithm Based on the Particle Swarm Optimization. *Journal of the Franklin Institute*, 357(15), 11042–11071. Online: <https://doi.org/10.1016/j.jfranklin.2020.08.032>
- SHARMA, Manu – RICHARDS, Nathan (2004): Adaptive Integrated Guidance and Control for Missile Interceptors. *Proceedings of AIAA Guidance, Navigation, and Control Conference, Rhode Island*, 1–15. Online: <https://doi.org/10.2514/6.2004-4880>
- SHIMA, Tal – IDAN, Moshe – GOLAN, Oded M. (2006): Sliding-Mode Control for Integrated Missile Autopilot-Guidance. *Journal of Guidance, Control, and Dynamics*, 29(2), 250–260. Online: <https://doi.org/10.2514/1.14951>
- SHIN, Heemin (2018): An Autonomous Aerial Combat Framework for Two-On-Two Engagements Based on Basic Fighter Maneuvers. *Aerospace Science and Technology*, 72, 305–315. Online: <https://doi.org/10.1016/j.ast.2017.11.014>
- WILLIAMS, Douglas – RICHMAN, Jack – FRIEDLAND, Bernard (1983): Design of an Integrated Strapdown Guidance and Control System for a Tactical Missile. *Proceedings of Guidance and Control Conference, Gatlinburg, TN, USA*, 57–66. Online: <https://doi.org/10.2514/6.1983-2169>
- YANG, Biao et al. (2013): Self-Adaptive PID Controller of Microwave Drying Rotary Device Tuning On-Line by Genetic Algorithms. *Journal of Central South University*, 20, 2685–2692. Online: <https://doi.org/10.1007/s11771-013-1784-4>
- YU, Wenwu et al. (2013): Distributed Control Gains Design for Consensus in Multi-Agent Systems with Second-Order Nonlinear Dynamics. *Automatica*, 49(7), 2107–2115. Online: <https://doi.org/10.1016/j.automatica.2013.03.005>

- YUEH, William R. – LIN, Ching F. (1984): Optimal Controller for Homing Missile. *Proceedings of the American Control Conference, San Diego, CA, USA*, 737–742. Online: <https://doi.org/10.23919/ACC.1984.4788473>
- ZHANG, Qirui – WEI, Ruixuan (2019): Ground Attack Strategy of Cooperative UAVs for Multitargets. *Complexity*. Online: <https://doi.org/10.1155/2019/9428087>
- ZHANG, Xue et al. (2020): Nonlinear Distributed Model Predictive Control for Multiple Missiles Against Maneuvering Target with a Trajectory Predictor. *Journal of Shanghai Jiaotong University*, 25, 779–789. Online: <https://doi.org/10.1007/s12204-020-2233-9>
- ZHANG, Yu – CHEN, Jing – SHEN, Lincheng (2013): Real-Time Trajectory Planning for UAV Air-To-Surface Attack Using Inverse Dynamics Optimization Method and Receding Horizon Control. *Chinese Journal of Aeronautics*, 26(4), 1038–1056. Online: <https://doi.org/10.1016/j.cja.2013.04.040>
- ZHANYUAN, Jiang et al. (2021): A Modified Proportional Navigation Guidance Law for Impact Time Control. *Proceedings of the 2021 6th International Conference on Automation, Control and Robotics Engineering (CACRE), Dalian, China*, 239–248. Online: <https://doi.org/10.1109/cacre52464.2021.9501293>
- ZHAO, Jinlong – ZHOU, Jun (2016): Receding Horizon Integrated Guidance and Control for Interceptors Based on Gauss Pseudospectral Method. *Proceedings of the 2016 IEEE Chinese Guidance, Navigation and Control Conference, Nanjing, China*, 1270–1275. Online: <https://doi.org/10.1109/CGNCC.2016.7828971>
- ZHOU, Huan et al. (2015): Robust Integrated Guidance and Control Design Method for UAV Based on Trajectory Linearization Control. *Proceedings of the 15th International Conference on Control, Automation and Systems, Busan, Korea (South)*, 1030–1035. Online: <https://doi.org/10.1109/ICCAS.2015.7364797>
- ZHOU, Kai et al. (2020): An Air Combat Decision Learning System Based on a Brain-Like Cognitive Mechanism. *Cognitive Computation*, 12(4), 128–139. Online: <https://doi.org/10.1007/s12559-019-09683-7>
- ZHU, Guodong – SHEN, Zuojun (2015): Three Dimensional Trajectory Linearization Control for Flight of Air-Breathing Hypersonic Vehicle. *Procedia Engineering*, 99, 1108–1119. Online: <https://doi.org/10.1016/j.proeng.2014.12.646>
- ZHU, Weiren – DUAN, Haibin (2013): Chaotic Predator-Prey Biogeography-Based Optimization Approach for UAV Path Planning. *Aerospace Science and Technology*, 32(1), 153–161. Online: <https://doi.org/10.1016/J.AST.2013.11.003>

Tartalom

VÉDELEMINFORMATIKA

BÁNYÁSZ-VÁCZI KINCSEŐ BORÓKA, RAJKI ZOLTÁN: <i>A bölcsészet-, társadalomtudományi és pedagógiai szakokon tanuló hallgatók perspektívái a mesterséges intelligencia lehetőségeiről és kockázatairól, 2. rész</i>	5
--	---

BIRÓ GABRIELLA: <i>A katonai és civil infrastruktúrák összefonódása az orosz–ukrán háború kiberműveleteiben</i>	27
--	----

GÁBOR FAZEKAS: <i>Multispectral Reconnaissance of Operational Areas</i>	45
--	----

ISTVÁN PARÁDA: <i>Cybersecurity Failures in Enterprise MDM Platforms</i>	61
---	----

KÖRNYEZETBIZTONSÁG

TAMÁS STADLER: <i>Military-related Heavy Metal Pollution in Soil</i>	75
---	----

KATONAI MŰSZAKI INFRASTRUKTÚRA

FÖLDES TIBOR: <i>Védett létesítmények fizikai védelme</i>	87
--	----

KATONAI LOGISZTIKA

SZAJKÓ GYULA, LÉVAI ZSOLT: <i>A közúti infrastruktúrák katonai megfelelőségi vizsgálata a logisztikai felderítés végrehajtásakor, 1. rész</i>	103
--	-----

HADITECHNIKA

GÁBOR FARKAS: <i>Augmentation of Training Data for AI-based Drone Detection System</i>	119
---	-----

HALMI LAJOS: <i>Szívfrekvencia-variabilitás monitorozása légi járművek fedélzetén</i>	137
--	-----

PAPP ISTVÁN, BÉKÉSI BERTOLD, KÁROLY KRISZTIÁN: <i>Pilóta nélküli légi járművek rajirányítási és rakétavezérlési vizsgálata komplex légi műveletek során</i>	149
--	-----