

HADMÉRNÖK

Kiemelt közlemények

Cséplő Zoltán, Kátai-Urbán Maxim, Vass Gyula: *Az iparbiztonsági oktatás és képzés rendszerének vizsgálata*

Norbert Daruka, Kálmán Dénes, Zoltán Kovács, Róbert Vég, István Ember: *The Impact of Additive Manufacturing Used in the Russo–Ukrainian Conflict on Decentralised Manufacturing*

Farkas Athéné: *A mesterséges intelligencia alkalmazási lehetőségei a kiberbiztonsági auditok gyakorlatában*

21. évf. (2026)
3. szám

ISSN 1788-1919 (elektronikus)

LUDOVIKA
EGYETEMI KIADÓ

IMPRESSZUM

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

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

Tartalom

Védeleminformatika

Farkas Athéné: *A mesterséges intelligencia alkalmazási lehetőségei a kiberbiztonsági auditok gyakorlatában* 5

Olga Lavro-Gazdag: *Doxxing as an Information Operation* 21

Ferenc Nyizsnyik: *Crowdsourcing Intelligence*. 43

Pozderka Gábor: *Kibertől az MI-ig: A mesterséges intelligencia az új kiber?* 55

Környezetbiztonság

Almási Csaba, Cséplő Zoltán: *A nagy közbiztonsági kockázattal járó veszélyes áruk szállítását érintő szabályozás vizsgálata* 75

Cséplő Zoltán, Kátai-Urbán Maxim, Vass Gyula: *Az iparbiztonsági oktatás és képzés rendszerének vizsgálata*. 89

Földes Tibor: *A működésfolytonosság mint stratégiai képesség a kritikus infrastruktúrák védelmében* 105

Takács Dániel, Négyesi Imre: *A nukleáris energia hasznosításának új korszaka* . . 119

Katonai logisztika

Norbert Daruka, Kálmán Dénes, Zoltán Kovács, Róbert Vég, István Ember: *The Impact of Additive Manufacturing Used in the Russo–Ukrainian Conflict on Decentralised Manufacturing*. 137

Szajkó Gyula, Lévai Zsolt: *A közúti infrastruktúrák katonai megfelelőségi vizsgálata a logisztikai felderítés végrehajtásakor, 2. rész* 149

Szajkó Gyula, Pap Andrea, Vég Róbert László: *A 3D-nyomtatással készült üzemanyag-szaktechnikai eszköz felhasználása a katonai felsőoktatásban* . . . 165

HADMÉRNÖK
VÉDELEMINFORMATIKA
21. évfolyam (2026) 3. szám 5–19.
DOI: 10.32567/hm.2026.3.1

Farkas Athéné[1]

A mesterséges intelligencia alkalmazási lehetőségei a kiberbiztonsági auditok gyakorlatában

Application Possibilities of Artificial Intelligence in the Practice of Cybersecurity Audits

Absztrakt

A kiberbiztonság napjainkra stratégiai jelentőségűvé vált a kritikus infrastruktúrák védelmében, amit a 2024. évi LXIX. törvény és annak kapcsolódó rendeletei is megerősítenek a NIST SP 800-53 Rev. 5-re épülő védelmi intézkedéskatalógus bevezetésével. A növekvő számú és összetettségű auditok jelentős erőforrásigénnyel járnak, ezért szükségessé válik a NIS2-nek való megfeleléshez végzett hazai kiberbiztonsági auditfolyamatok automatizálási lehetőségeinek vizsgálata. E tanulmány kifejezetten az alap biztonsági osztályba sorolt elektronikus információs rendszerekhez rendelt 164 védelmi intézkedéshez kapcsolódó auditbizonyítékok mesterségesintelligencia- (MI-)alapú feldolgozhatóságát vizsgálja, a hazai NIS2 auditmódszertanra építve. Újszerű eleme az auditbizonyítékok T1–T7 szerinti tipizálása, amely három dimenzió – a vizsgálati típus, a bizonyíték formátuma, az alkalmazható MI-technológia – összekapcsolásával rendszerezi az evidenciákat. A tipológia lehetővé teszi az egyes bizonyítéktípusok MI-szempontú minősítését, és kijelöli azokat a területeket, ahol reális a részleges vagy jelentősebb automatizálás. Az eredmények rámutatnak arra, hogy a szövegalapú, strukturált nyelvezetű dokumentumok ismétlődő mintázataik és sablonszerű megfogalmazásaik miatt alkalmasak természetesnyelv-feldolgozási technológiák alkalmazására, míg a képi vagy nem strukturált formátumú auditbizonyítékok – például képernyőképek, szkennelt dokumentumok – feldolgozásához

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Katonai Műszaki Doktori Iskola, e-mail: athene.farkas@proton.me

az optikai karakterfelismerés és a számítógépes látás integrációja szükséges. A tanulmány megállapítja, hogy a kiberbiztonsági auditok részleges automatizálása nem valósítható meg kizárólag szövegalapú mesterségesintelligencia-eszközökkel: hatékony auditautomatizáláshoz multimodális megközelítés szükséges, amely a természetesnyelv-feldolgozás mellett képfeldolgozó technológiákat is alkalmaz.

Kulcsszavak: kiberbiztonság, NIS2, audit, mesterséges intelligencia

Abstract

Cybersecurity has become a factor of strategic importance in the protection of critical infrastructures, a development reinforced by Act LXIX of 2024 and its implementing decrees through the introduction of a catalogue of security controls based on NIST SP 800-53 Rev. 5. The increasing number and complexity of audits require significant resources, which makes it necessary to examine the possibilities for automating national cybersecurity audit processes aimed at NIS2 compliance. The study specifically investigates the artificial intelligence (AI)-based processability of audit evidence associated with the 164 security controls assigned to electronic information systems classified in the basic security category, building on the national NIS2 audit methodology. A novel element of the study is the classification of audit evidence into types T1–T7, which systematises the evidence by linking three dimensions: type of examination, format of evidence, and applicable AI technology. This typology enables the AI-oriented evaluation of different types of evidence and identifies the areas where partial or more substantial automation is realistic. The results show that text-based documents with structured language are suitable for the application of natural language processing technologies due to their recurring patterns and template-like formulations, while the processing of image-based or unstructured audit evidence – such as screenshots and scanned documents – requires the integration of optical character recognition and computer vision. The study concludes that the partial automation of cybersecurity audits cannot be achieved solely with text-based artificial intelligence tools; effective audit automation requires a multimodal approach that, in addition to natural language processing, also applies image processing technologies.

Keywords: cybersecurity, NIS2, audit, artificial intelligence

Bevezetés

A kiberbiztonság az elmúlt években a kritikus infrastruktúrák védelmének egyik kulcstényezőjévé vált. Az ezeket érő kibertámadások közvetlenül veszélyeztethetik a társadalom működőképességét és az alapvető szolgáltatások folyamatosságát. Az Európai Unió NIS2 irányelve,[2] valamint annak hazai átültetése – különösen a 2024. évi LXIX. törvény Magyarország kiberbiztonságáról és az ehhez kapcsolódó végrehajtási rendeletek – érdemben szigorították a kiberbiztonsági követelményeket. Szélesebb

[2] Az Európai Parlament és a Tanács 2022/2555 irányelve.

szervezeti kört vontak be a szabályozás hatálya alá, és kötelezővé tették a rendszeres kiberbiztonsági auditokat a kritikus és fontos ágazatok szereplőinél.

Ezzel párhuzamosan a hazai jogszabályi környezet a NIST SP 800-53 Rev. 5[3] nemzetközi ajánlásra épülő védelmi intézkedéskatalógust alkalmazza. Az erre épülő NIST SP 800-53A Rev. 5[4] ellenőrzési módszertan rendkívül részletes, elemikövetelmény-szintű vizsgálatokat igényel. A megfelelési kötelezettségek bővülése, az auditált szervezetek számának növekedése és a kontrollkészletek komplexitása együtt azt eredményezik, hogy a hagyományos, manuális auditálási eljárások egyre inkább idő- és erőforrás-igényessé válnak. Ez a gyakorlatban a vizsgálatok elhúzódásához és a humán erőforrások túlterheléséhez vezethet.

A téma aktualitását az is erősíti, hogy a nemzetközi és ágazati szakirodalomban egyre hangsúlyosabban jelenik meg a mesterséges intelligencia. Különösen a gépi tanulás és a természetes nyelvfeldolgozás integrálása látható a kiberbiztonsági megfelelésértékelési folyamatokba, a kontrollok folyamatos monitorozásába és az auditbizonyítékok automatizált gyűjtésébe.

A kutatás szempontjából kulcskérdés, hogy a kiberbiztonsági auditok során használt szöveges auditdokumentumok – szabályzatok, tervek, nyilvántartások, jelentések – mennyiben alkalmasak strukturált, algoritmikus feldolgozásra, és hogyan illeszthetők be az MI eszközei a hazai auditmódszertanba. Ennek tisztázása azért különösen fontos, mert egyszerre jelenik meg az az elvárás, hogy az auditfolyamatok megfeleljenek a szigorodó jogszabályi követelményeknek és nemzetközi ajánlásoknak, miközben a szervezetek és az auditorok részéről is erős nyomás van a hatékonyság növelésére és az erőforrásigény csökkentésére.

A témát tovább árnyalja az az ellentmondás, hogy az MI-alapú automatizálás egyfelől jelentősen javíthatja az auditok lefedettségét és gyorsaságát, másfelől új kockázatokat teremt az átláthatóság, az MI-rendszerek saját megfelelősége és felülvizsgálhatósága tekintetében. Ezért a kiberbiztonsági auditok és a mesterséges intelligencia kapcsolatának vizsgálata nemcsak a folyamatok hatékonyságának növelése, hanem a jövőbeni szabályozói elvárások, felelősségi kérdések és a kritikus infrastruktúrák biztonságának szempontjából is kiemelten fontos kutatási terület.

A kutatás hatóköre

A hazai implementáció jelenlegi állapotában az alap biztonsági osztályba sorolt elektronikus információs rendszerekhez rendelt 164 védelmi intézkedés képezi azt a minimális, de minden érintett szervezetnél kötelező kontrollkészletet, amelyre a megfelelésértékelés első hulláma épül. A tanulmány ezért az auditautomatizálási kérdéseket e kontrollkészlethez kapcsolódó auditbizonyítékokra fókuszálva vizsgálja.

A továbbiakban a vizsgálat kizárólag az alap biztonsági osztályhoz rendelt védelmi intézkedésekhez kapcsolódó dokumentumvizsgálat, interjú és tesztelés során keletkező evidenciákat elemzi mint a NIS2-alapú hazai kiberbiztonsági auditmódszertan

[3] NIST 2020.
[4] NIST 2022.

kiindulópontját. Ezzel biztosítható, hogy az MI-alapú automatizálhatósági eredmények közvetlenül értelmezhetők legyenek a gyakorlatban már alkalmazott hazai módszertan szempontjából.

Kutatási kérdés

A jelen kutatás központi kérdése, hogy mely auditbizonyíték-típusok alkalmasak leginkább MI-alapú vizsgálatra és algoritmikus feldolgozásra a NIS2-irányelvnek való megfeleléshez végzett kiberbiztonsági auditok során. A vizsgálat fókusza az SZTFH rendelet[5] szerinti módszertan alapján lefolytatott auditok azon részére esik, amely az alap biztonsági osztályba sorolt elektronikus információs rendszerekhez rendelt 164 védelmi intézkedés teljesülését értékeli. A kutatás azt elemzi, hogy a dokumentumvizsgálat, az interjú és a tesztelés során keletkező különböző formátumú evidenciák miként integrálhatók mesterségesintelligencia-modellekbe.

Célkitűzés

Célul tűztem ki a magyarországi NIS2-alapú kiberbiztonsági auditmódszertan fejlesztési lehetőségeinek feltárását az alap biztonsági osztályba sorolt elektronikus információs rendszerek körében. Célom megállapítani, hogy a kiberbiztonsági auditokban használt dokumentumok és digitális bizonyítékok milyen mértékben alkalmasak strukturált, algoritmikus feldolgozásra. A vizsgálat során rendszerezem az auditokhoz kapcsolódó dokumentumtípusokat és egyéb evidenciákat, illetve saját auditbizonyíték-tipológiát (T1–T7) dolgozok ki. Ennek során a vizsgálati eljárást, a bizonyíték formátumát és az alkalmazható MI-technológiát együttesen veszem figyelembe. A tipológia elkészítése után elemzem, hogy ezek az MI-technológiák miként illeszthetők be a jelenlegi manuális auditgyakorlatba anélkül, hogy sérülne az auditfolyamat bizalmasságára vonatkozó szigorú előírás. Célom javaslatot tenni olyan fejlesztési irányokra, amelyek támogatják a kiberbiztonsági auditok hatékonyságának növelését és a megfelelőség biztosítását.

Módszer

A tanulmány feltáró jellegű kutatás, amelynek célja a hazai NIS2-alapú kiberbiztonsági auditmódszertan és az MI alkalmazási lehetőségei közötti kapcsolódási pontok rendszerezett feltárása. Ennek megfelelően a kutatás módszertani alapját a releváns jogszabályi, nemzetközi ajánlási és tudományos-szakmai források célzott, kvalitatív feldolgozása képezi.

A forrásbázis három pillérre épül. Egyrészt a normatív keretet meghatározó jogforrásokra, különösen a NIS2 irányelvre, a 2024. évi LXIX. törvényre, a 7/2024. (VI. 24.) MK rendeletre és az 1/2025. (I. 31.) SZTFH rendeletre. Másrészt a módszertani háttérre,

[5] 1/2025. (I. 31.) SZTFH rendelet.

elsősorban a NIST SP 800-53 Rev. 5 és a NIST SP 800-53A Rev. 5 dokumentumokra. Harmadrészt pedig azokra a hazai és nemzetközi szakirodalmi forrásokra, amelyek a kiberbiztonsági auditok, a *compliance*-automatizálás, a természetesnyelv-feldolgozás, az OCR, a *computer vision,* az anomáliadetektálás és a magyarázható mesterséges intelligencia alkalmazhatóságát tárgyalják.

A szakirodalom-feldolgozás során a bevont források kiválasztása relevanciaalapon történt. A beválasztás elsődleges szempontja az volt, hogy az adott munka közvetlenül kapcsolódjon legalább egyhez a következő tématerületek közül: kiberbiztonsági audit, megfelelőségértékelés, NIS2- vagy kontrollalapú auditmódszertan, illetve mesterséges intelligencia alkalmazása dokumentum-, log- vagy vizuális bizonyítékok feldolgozásában. A kizárás szempontjai közé tartoztak azok a források, amelyek kizárólag általános MI-alkalmazásokat tárgyaltak audit- vagy megfelelőségi kontextus nélkül, illetve amelyek nem nyújtottak érdemi módszertani vagy technológiai kapcsolódást a vizsgált problémához.

Az elemzés kvalitatív tartalomelemzési logikát követett. A feldolgozott forrásokból először az auditfolyamat szempontjából releváns bizonyítékformátumokat, majd az ezekhez rendelhető technológiai feldolgozási módokat azonosítottam. Ezt követően a hazai auditmódszertanban megjelenő három fő vizsgálati eljárás – dokumentumvizsgálat, interjú, tesztelés – szolgált elsődleges rendezőelvként. A második rendezőelvet a bizonyíték formátuma jelentette, amely alapján a strukturált szöveg, félig strukturált adat, vizuális vagy zárt dokumentum, hangalapú szöveg, jegyzőkönyvi szöveg, valamint log- és eseményadat különült el. A harmadik rendezőelv az elsődlegesen alkalmazható MI-technológia volt, vagyis az, hogy az adott bizonyítéktípus esetében mely technológia jelent reális belépési pontot az automatizált feldolgozáshoz.

E három szempont metszetében jött létre a szerző által kialakított T1–T7 auditbizonyíték-tipológia. A T1–T7 kategóriákhoz az MI-technológiák hozzárendelése funkcionális megfeleltetés alapján történt, vagyis annak figyelembevételével, hogy az adott evidenciatípus elsődlegesen milyen adatformátumban áll rendelkezésre, és e formátum gépi feldolgozására a szakirodalom szerint mely technológia alkalmas.

A módszer eredménye egy fogalmi és módszertani keret, amely megalapozhat későbbi kvantitatív vagy esettanulmány-alapú vizsgálatokat.

Kiberbiztonsági szabályozás Magyarországon

Az európai irányelvek nem alkalmazandók közvetlenül a tagállamokban, így a NIS2 direktíva előírásait a nemzeti jogrendszerekbe kellett integrálni. Magyarország az első tagállamok között volt, amelyek megkezdték a NIS2 irányelv átültetését a hazai jogrendbe. A 2024. évi LXIX. törvény 2025. január 1-jén lépett hatályba. A törvény a Szabályozott Tevékenységek Felügyeleti Hatóságát (SZTFH) jelölte ki általános nemzeti kiberbiztonsági hatóságként, amely felügyeli az érintett szervezetek megfelelőségét és a nyilvántartásba vételi folyamatokat. Mivel a törvény csak a kereteket adja meg, a Miniszterelnöki Kabinetirodát vezető miniszter 7/2024. (VI. 24.) rendelete[6] rögzíti az elektronikus információs rendszerek biztonsági osztályba sorolásának

[6] 7/2024. (VI. 24.) MK rendelet.

követelményeit, valamint az egyes biztonsági osztályokhoz (alap, jelentős, magas) rendelt konkrét védelmi intézkedéseket. Fontos tudományos és szakmai aspektus, hogy ez a rendelet az Egyesült Államok szabványügyi és méréstechnikai hivatalának NIST SP 800-53 Rev. 5 számú, nemzetközileg elismert kontrollkatalógusára épül. Ez az adaptáció biztosítja, hogy a magyar szervezetek a széles körben alkalmazott nemzetközi technológiai és szervezési intézkedéseket alkalmazzák az adatvagyonuk és a rendszereik védelmében.

Míg az MK rendelet az információs rendszerek felett rendelkező szervezetek számára fogalmaz meg védelmi követelményeket, addig az 1/2025. (I. 31.) SZTFH rendelet a megfelelés ellenőrzésének gyakorlati szabályait fekteti le. Ez a jogszabály határozza meg a kiberbiztonsági audit lefolytatásának rendjét, az auditori módszertant és az auditok legmagasabb díját. A rendelet módszertani alapját a NIST SP 800-53A rev5 képezi, amely strukturált eljárásokat biztosít a kontrollok hatékonyságának objektív felméréséhez, biztosítva ezáltal az auditok minőségét és a hatósági elvárások teljesülését. Ez a jogszabályi hierarchia auditálható kiberbiztonsági keretrendszer kialakítására kötelezi a gazdaság és a társadalom működése szempontjából kritikus szervezeteket.

Az elektronikus információs rendszerek biztonsági osztályba sorolása

A NIS2 hazai implementációja során a jogalkotó egyértelművé tette, hogy a kiberbiztonság nem kezelhető egyetlen, mindenre egyformán érvényes sablonként. Ahhoz, hogy a védelem ott legyen a legerősebb, ahol a legnagyobb veszteség érheti a szervezetet, az elektronikus információs rendszereket (EIR) saját jelentőségük és kockázati szintjük alapján három osztályba (alap, jelentős, magas) sorolják, amelyek meghatározzák a vizsgálandó kontrollok számát is. A biztonsági osztályba sorolás közvetlenül meghatározza, hogy a szervezetnek a 7/2024 MK rendelet 2. mellékletében, a védelmi intézkedések katalógusában szereplő kontrollok közül mennyit és milyen mélységben kell implementálnia. A kötelező védelmi intézkedéseket az 1/2025. SZTFH rendelet 6. melléklete szervezeti (SZ) és elektronikus információs rendszer (EIR) szintre bontja. Alap biztonsági osztály esetében 164 védelmi intézkedésnek kell megfelelni, ami a kötelező minimum. Ezt a 164 kontrollt minden, a jogszabály hatálya alá tartozó szervezetnek implementálnia kell, még a legkisebb kockázatú rendszerek esetében is. A jogszabályi mellékletek szerzői elemzése (saját kigyűjtés) alapján megállapítható, hogy alap biztonsági osztály esetében a 164 védelmi intézkedés közül 82 szervezeti és 82 EIR-szintű. Jelentős biztonsági osztály esetén az alap biztonsági osztály kontrolljai kiegészülnek további 139 EIR-szintű, szigorúbb követelménnyel, míg a legkritikusabb, magas biztonsági osztályú rendszereknek további 83, gyakran automatizációt, redundanciát és folyamatos valós idejű monitorozást megkövetelő intézkedésnek kell megfelelniük.

Tekintettel a jelen kutatás fókuszára és a szerző gyakorlati tapasztalataira, e tanulmány a továbbiakban kizárólag az alap biztonsági osztályba sorolt elektronikus információs rendszerekkel és az azokra vonatkozó 164 védelmi intézkedéssel – mint a NIS2-alapú hazai kiberbiztonsági auditmódszertan kiindulópontjával – foglalkozik.

Az alaposztályú intézkedések elsősorban az alapvető kiberhigiénia megteremtésére, az erős dokumentációs, szabályozási alapokra és a transzparens folyamatok kialakítására fókuszálnak.[7]

Vizsgálati eljárások

Az audit célja annak objektív, bizonyítékokkal történő alátámasztása, hogy az elvárt védelmi intézkedések megvalósítása hiánytalan-e, és a gyakorlatban a tervezett módon működnek-e. A vizsgálat során az auditor három fő módszert alkalmaz: dokumentumvizsgálatot, interjút és tesztelést.

Dokumentumvizsgálat

A dokumentumvizsgálat a módszertan alapján minden követelménycsoport esetében kötelezően alkalmazandó módszer. A vizsgálódás során az auditornak a 7/2024. MK rendelet alapján többféle dokumentumtípust kell részletesen áttekintenie. Magas szintű irányítási dokumentumok közé tartozik az 1. kontrollcsaládba tartozó információbiztonsági szabályzat, majd minden további kontrollcsalád esetében a szabályzat és az eljárásrend, összesen 18-18 dokumentum.

1. táblázat: Elkészítendő és vizsgálandó dokumentumok

Ssz.	Dokumentum neve	Dokumentum típusa
1.	Kockázatmenedzsment-stratégia	stratégia
2.	Ellátási lánc kockázatmenedzsmentjének stratégiája	stratégia
3.	Folyamatos felügyeleti stratégia	stratégia
4.	Elektronikus információs rendszerek nyilvántartása	nyilvántartás
5.	Karbantartási nyilvántartás	nyilvántartás
6.	Fizikai belépést ellenőrző eszközök nyilvántartása	nyilvántartás
7.	Látogatói belépések nyilvántartása	nyilvántartás
8.	Be- és kiszállításról szóló nyilvántartás	nyilvántartás
9.	Rendszerelemleltár	leltár
10.	Belépésre jogosult személyek listája	lista
11.	Intézkedési terv és mérföldkövei	terv
12.	Kritikus infrastruktúra és kulcsfontosságú erőforrások biztonsági terve	terv
13.	Rendszerbiztonsági terv	terv
14.	Biztonságértékelési terv	terv
15.	Üzletmenet-folytonossági terv	terv
16.	Biztonsági eseménykezelési terv	terv
17.	Beruházási terv	terv
18.	Munkaköri leírások	leírás

Forrás: a szerző szerkesztése

[7] Váczi–Orbók 2025.

További dokumentumfajtaként megjelennek még stratégiák, nyilvántartások, leltárak, listák, tervek, leírások (1. táblázat). Az auditor nem csupán a dokumentumok meglétét ellenőrzi, hanem azt is vizsgálja, hogy a szabályzatok naprakészek-e, amennyiben szükséges, akkor a megfelelő személy által jóváhagyottak-e, és hogy összhangban állnak-e a jogszabályi előírásokkal és a valós szervezeti környezettel, tehát tartalmilag minimálisan a jogszabály által elvártaknak megfelelnek-e.

Interjú

Az interjú célja, hogy az auditor személyes interakciókon keresztül gyűjtsön további bizonyítékokat, tisztázza a felmerült kérdéseket, és megismerje a leírt folyamatok, eljárások tényleges, gyakorlati megvalósulását. A szóban megbeszélteket ezután alátámasztó dokumentumokkal, evidenciákkal igazolja a szervezet, amiket megküld az auditornak, aki ezekre hivatkozva bővíti az adott kontrollról írt értékelő leírását.

Tesztelés

A tesztelés az audit leggyakorlatiasabb része, ahol az auditor a tényleges és az elvárt működés összehasonlítása érdekében megvizsgálja a rendszerek működését. Ezen a ponton kell a szervezetnek azokat a konkrét evidenciákat (bizonyítékokat) bemutatnia, amelyek technológiailag is igazolják a megfelelést, például határvédelmi megoldások konfigurációjáról vagy jelszókomplexitási beállításokról készült képernyőképekkel, szervezeti tevékenységek és rendszeresemények naplóival. A tesztelési bizonyítékok jelentős része nem tisztán szöveges, gépileg könnyen olvasható formátumú. A technológiai kontrollok beállításait és működését leggyakrabban a rendszerekből kimentett képernyőképekkel, jellemzően PNG, JPG és hasonló képformátumokkal támasztják alá.

Új technológiák a kiberbiztonsági auditokban

Az információbiztonsági auditorokkal szemben szigorú követelmények vannak.[8] A hagyományos, tisztán manuális vizsgálatok rendkívül idő- és erőforrás-igényesek. Ezen komplexitási és kapacitásproblémák kezelésére a szakirodalom egyre hangsúlyosabban az MI-technológiák integrációját javasolja. Fehér elméleti alapvetése szerint[9] az MI képes érdemben növelni a védelmi intézkedések ellenőrzésének hatékonyságát, az ismétlődő folyamatok automatizálását. Ezt az irányvonalat támasztják alá Folorunso és munkatársai,[10] akik a kutatásaik alapján megerősítik, hogy az MI az anomáliadetektálás, a csalásfelismerés és a szabályozói jelentések automatizálása révén növeli a hatékonyságot és csökkenti az adminisztratív terheket. A dokumentumalapú

[8] Krasznay 2020; Baglyos 2022; Barna–Kollár–Oroszi 2023.
[9] Fehér 2022.
[10] Folorunso et al. 2024: 167–184.

megfelelésértékelés automatizálásában különösen a természetesnyelv-feldolgozás (*natural language processing,* NLP) játszik jelentős szerepet.[11] Az NLP-modellek képesek a terjedelmes biztonsági szabályzatok, rendszerbiztonsági tervek és egyéb dokumentumok algoritmikus elemzésére, felismerve az ismétlődő mintázatokat, a szabályozási hiányosságokat, az egymásra hivatkozó szabályzatokat vagy a folyamatleírások közötti ellentmondásokat. Ez a folyamat a megfelelésértékelés leginkább időigényes része. Kutatások igazolják, hogy a megfelelően betanított NLP-rendszerek hatékonyságuk által jelentősen csökkenthetik a dokumentumok értelmezésére fordított időt. A pénzügyi szektorban végzett esettanulmányok is jelentős mértékű auditidő-csökkenést és működési költségmegtakarítást mutattak ki a manuális auditfolyamatokhoz képest.[12]

Az auditbizonyítékok nem kizárólag gépileg olvasható, strukturált szövegek formájában állnak rendelkezésre. A megfelelőséget igazoló alapvető irányítási dokumentumokat, mint amilyen az IBSZ, a rendszerbiztonsági terv vagy a kockázatokat felvállaló dokumentáció, a szervezet vezetőjének vagy a kijelölt felelős személynek formálisan jóvá kell hagynia. A technológiai tesztelések és a formálisan jóváhagyott dokumentációk által az auditbizonyítékok egy része vizuális, képi formátumban, például képernyőképek vagy szkennelt, zárt PDF-ek formájában áll rendelkezésre. Ezen gépileg nem olvasható, nem strukturált adatok algoritmikus feldolgozásához az NLP mellett az optikai karakterfelismerő (*optical character recognition,* OCR) és a számítógépes látás *(computer vision)* technológiák integrációja elengedhetetlen.

Az MI auditokba történő beemelése ugyanakkor új etikai, adatvédelmi és átláthatósági kockázatokat is generál, amelyeket a jogi keretrendszereknek szigorúan egyensúlyban kell tartaniuk az információbiztonsági célokkal.[13] A generatív MI-modellek auditcélú alkalmazásának egyik legnagyobb technológiai kockázata a hallucináció. Előfordulhat, hogy az algoritmus a valóságban nem létező kontrollokra (például egy fiktív elemre) hivatkozik, vagy tévesen határozza meg egy adott biztonsági osztály alapkövetelményeit, ami téves megfelelőségi megállapításokhoz vezethet.[14] Ezen kockázatok miatt a szakirodalom és a szabályozói gyakorlat is egybehangzóan az emberi felügyelet *(human-in-the-loop)* kötelező fenntartását és a gépi döntéshozatal teljes visszakövethetőségének *(traceability)* kialakítását szorgalmazza. A legkorszerűbb és legelterjedtebb neurális hálózatok, valamint a mélytanulási *(deep learning)* modellek – bár kiemelkedő alkalmazkodóképességet mutatnak a hálózati anomáliák felismerésében – úgynevezett „fekete doboz" *(black box)* jellegükből fakadóan alapvetően alkalmatlanok az átlátható és megismételhető logikai láncok biztosítására.[15] Ezekből a gépi tanulási algoritmusokból hiányzik az egzakt szabály-visszavezetés képessége. Döntéseiket átláthatatlan matematikai súlyozásokra és statisztikai korrelációkra alapozzák, nem pedig olyan transzparens, következtethető logikára, amely egy audit során elvárás lenne. Mivel a rendszerek nem képesek megindokolni egy-egy hiányosság okát, kimeneteik önmagukban, emberi felülvizsgálat nélkül nem szolgáltatnak

[11] Smith 2024.
[12] Smith 2024.
[13] Folorunso et al. 2024.
[14] Váczi–Orbók 2025.
[15] Loumachi et al. 2025.

jogilag és szakmailag elfogadható auditbizonyítékot. Ez az átláthatatlanság jelentősen hátráltatja a technológiába vetett felhasználói és szabályozói bizalom kialakulását.[16]

Ezzel a megközelítéssel szemben a szimbolikus MI-modellek architektúrájukból fakadóan más tulajdonságokkal bírnak. Mivel előre definiált, világos szabálykészletek mentén működnek, natív módon garantálják a magyarázhatóságot. A szakirodalom e technológiai dilemma feloldását elsődlegesen a magyarázható mesterséges intelligencia (*explainable AI,* XAI) eszközök integrációjában látja.[17] Az XAI-technológiák célja, hogy láthatóvá váljanak az MI döntéshozatali folyamatai, lehetővé téve, hogy az algoritmus megmutassa a munkáját, azaz világos, transzparens és auditálható nyomot biztosítson az összegyűjtött bizonyítékokról.[18] Az átláthatóság megteremtése nemcsak a bizalmat növeli, hanem kritikus feltétele annak, hogy az auditor megérthesse az automatizált megfelelőségi vizsgálatok eredményeit.

A nemzetközi szakirodalom az MI-alapú kiberbiztonsági auditokat a folyamatos ellenőrzés megteremtésének eszközeként is leírja. Ennek oka a technológiai környezet olyan mértékű előrehaladása, amely a sebezhetőségvizsgálat és a megfelelőségértékelés hatékonyságát növeli.[19] Anwar bemutatja, hogy a gépi tanulásra épülő algoritmusok – a korábban azonosított sérülékenységek mintázataira támaszkodó, felügyelt tanulási modellek, valamint a címkézetlen adatokból rendellenes viselkedést feltáró nem felügyelt tanulási eljárások – képesek gyorsítani a sebezhetőségazonosítást, csökkenteni az emberi hiba kockázatát és proaktívabbá tenni az auditfolyamatot. A természetesnyelv-feldolgozásra épülő eszközök emellett támogathatják a szabályozói követelmények, például adatvédelmi és pénzügyi megfelelőségi keretek szöveges előírásainak automatikus feldolgozását, a belső szabályzatokkal való összevetését és a hiányosságok gyors jelzését.[20]

Aliliele és munkatársai áttekintése az MI-vel támogatott folyamatos auditálási rendszerekre fókuszál, amelyek a hagyományos, időszakos vizsgálatokkal szemben folyamatos adatgyűjtésre és közel valós idejű elemzésre épülnek. A tanulmány szerint a gépi tanulás, a természetesnyelv-feldolgozás és az anomáliadetektálás együttes alkalmazása lehetővé teszi a hozzáférés-ellenőrzés, a konfigurációmenedzsment, az incidenskezelés és a szabályozói megfelelőség folyamatos monitorozását. Ezzel együtt a riasztáskezelés és az automatizált jelentéskészítés csökkenti az audit operatív terheit. A szerzők ugyanakkor rámutatnak arra, hogy az ilyen rendszerek sikeres bevezetése feltételezi az adatok minőségét biztosító vezetői kereteket, a magyarázható mesterséges intelligencia elveinek érvényesítését, valamint azt, hogy az auditorok szerepe a manuális ellenőrzésből a gépi eredmények értelmezésére és felügyeletére épülő szakértői kontroll irányába mozdul el.[21]

A mesterséges intelligencia kiberbiztonsági auditokban betöltött szerepe tehát kettős: egyszerre kínál jelentős hatékonyságnövelést, és hoz magával új, kezelendő kockázatokat. A nemzetközi áttekintés rámutat arra, hogy a gépi tanulás

[16] Loumachi et al. 2025.
[17] Folorunso et al. 2024; Smith 2024.
[18] Kewat 2025.
[19] Anwar 2023.
[20] Anwar 2023.
[21] Aliliele 2025.

és a természetesnyelv-feldolgozás különösen a nagy mennyiségű, szabályozási tartalmú dokumentumok elemzésében, a sebezhetőségek azonosításában és az anomáliák feltárásában kínál érdemi automatizálási potenciált. Ez mérhető auditidő-csökkenést és erőforrás-megtakarítást eredményezhet. Ugyanakkor hangsúlyos, hogy az auditbizonyítékok egy része vizuális vagy zárt formátumú, ezért – mint említettük – az optikai karakterfelismerés és a számítógépes látás bevonása nélkül nem alakítható át megbízhatóan gépileg értelmezhető adattá. Az MI-vel támogatott auditálás felé mutató nemzetközi trendek ugyanakkor egyértelművé teszik azt is, hogy az automatizált elemzés és az emberi szakértői kontroll elválaszthatatlanul egymásra épül.

Auditbizonyíték-tipológia

Az auditbizonyíték-tipológia T1–T7 kategóriák kialakítása a hazai auditmódszertan három fő vizsgálati eljárásának és az ezek során tipikusan előforduló bizonyítékformátumoknak az összevetéséből jött létre. A kategorizálás első szintjén az SZTFH-módszertan szerinti dokumentumvizsgálat, interjú és tesztelés szolgált rendezőelvként. A második szinten a bizonyíték formátuma alapján különülnek el a strukturált szövegek (például információbiztonsági szabályzatok, rendszerbiztonsági tervek), a félig strukturált adatok (leltárak, jogosultsági táblázatok, űrlapok), a strukturálatlan szöveges anyagok (interjújegyzőkönyvek, szabad szövegű jelentések), valamint a vizuális bizonyítékok (képernyőképek, beszkennelt, zárt PDF-ek). Az MI-technológiai dimenzió ezzel párhuzamosan azokat a fő eszközcsoportokat jelöli, amelyek a különböző formátumú bizonyítékok algoritmikus elemzését lehetővé teszik, vagyis a már említett természetesnyelv-feldolgozást (NLP), az optikai karakterfelismerést (OCR), illetve a gépi tanuláson alapuló log- és mintázatelemzést, ideértve a számítógépes látás *(computer vision)* megoldásait is. A végleges T1–T7 felosztás célja az volt, hogy a hazai auditgyakorlatban ténylegesen előforduló bizonyítéktípusok mindegyike egyértelműen besorolható legyen, és egyben összekapcsolhatóvá váljon az elsődlegesen releváns MI-technológiával.

Az auditbizonyítékok MI-szempontú értelmezése

A saját auditbizonyíték-tipológia nemcsak leíró kategóriákat ad, hanem lehetővé teszi az egyes bizonyítéktípusok MI-szempontú minősítését is. A 2. táblázat tartalmazza, hogy mely bizonyítékformátumok esetében reális a mesterséges intelligencia részleges vagy akár jelentős mértékű bevonása. A táblázat a T1–T7 típusok mellett röviden összefoglalja az adott bizonyítékra jellemző automatizálhatósági lehetőségeket, így kirajzolva, hogy a magyar NIS2-alapú auditgyakorlatban mely területek kínálják a legkézenfekvőbb MI-fejlesztési célpontokat. A hozzárendelés minden esetben abból indult ki, hogy az adott bizonyítéktípus milyen módon tehető gépileg értelmezhetővé és auditcélból feldolgozhatóvá.

2. táblázat: Auditbizonyíték-típusok MI-szempontú elemzése

Kód	Vizsgálat típusa	Bizonyíték formátuma	Példa	Javasolt MI-technológia
T1	Dokumentumvizsgálat	Strukturált szöveg	Információbiztonsági szabályzat, rendszerbiztonsági terv, eljárásrendek	NLP (szövegértelmezés, kulcsszavas és szemantikus keresés)
T2	Dokumentumvizsgálat	Félig strukturált szöveg (táblázat, jegyzék)	Eszközleltár, jogosultsági mátrix, incidens-nyilvántartás	NLP + klasszikus ML (mezőkivonás, konzisztencia-ellenőrzés)
T3	Dokumentumvizsgálat	Vizuális/zárt dokumentum (szkennelt, aláírt irat)	Beszkennelt IBSZ, formálisan jóváhagyott nyilatkozatok, zárt PDF-ek	OCR + NLP (karakterfelismerés, tartalmi ellenőrzés)
T4	Interjú	Hangfelvételből szöveg	Felelősökkel készített strukturált interjúk, *kick off* megbeszélés rögzítése	ASR + NLP (átiratkészítés, kulcstémák és hiányzó elemek azonosítása)
T5	Interjú	Szöveges jegyzőkönyv, emlékeztető	Interjújegyzőkönyvek, összefoglalók, emlékeztetők	NLP (kivonatolás, ellentmondás-keresés, szabályzatokkal való összevetés)
T6	Tesztelés	Logfájlok, eseményadatok (strukturált vagy félig strukturált)	Hozzáférési naplók, hálózati forgalmi logok, tűzfallogok	ML/anomáliadetektálás (felügyelt és nem felügyelt tanulás)
T7	Tesztelés	Vizuális bizonyíték (képernyőkép, UI-kimenet)	Konfigurációs képernyőképek (PNG, JPG), biztonsági beállítások grafikus felületről mentett képei	Computer vision + OCR (UI-elem felismerése, beállítások kinyerése)

Forrás: a szerző szerkesztése

A dokumentumvizsgálat során használt strukturált szöveges bizonyítékok (T1) esetében a természetesnyelv-feldolgozás alkalmazása különösen ígéretes, mivel a szabályzatok és tervek sablonszerű felépítése, ismétlődő szóhasználata és jól definiált jogszabályi háttérre való hivatkozása támogatja a kulcsfogalmak automatikus keresését, a követelményekhez rendelést és a hiányosságok jelzését. A félig strukturált dokumentumok (T2) már egyrészt táblázatos jellegük, másrészt a mezők közötti kapcsolatok miatt igénylik a szöveges modelleket kiegészítő, klasszikus gépi tanulási módszerek bevonását.

A vizuális vagy zárt formátumú dokumentumok (T3) és a tesztelési bizonyítékok körébe tartozó képernyőképek (T7) esetében a gépi feldolgozás első lépését az optikai karakterfelismerés jelenti, amely a képi formátumú tartalmat gépileg olvasható szöveggé alakítja. Ezt követően a szöveg már NLP-vel, a képi elemek pedig számítógépes látási algoritmusokkal elemezhetők. Ugyanakkor a tipológia már ebben a pontban rámutat arra, hogy ezeknél a bizonyítéktípusoknál a feldolgozás pontossága függ az elrendezéstől és a vizuális zajtól, emiatt – mint korábban erre felhívtuk a figyelmet – a teljes automatizálás csak erős humán ellenőrzés mellett képzelhető el.

Az interjúalapú bizonyítékoknál a tipológia külön kategóriába sorolja a hangfelvételről automatikusan készített átiratokat (T4) és a közvetlen szöveges jegyzőkönyveket (T5). Előbbi esetben az automatikus beszédfelismerés (ASR) és az NLP együttes

alkalmazása teszi lehetővé a kulcstémák, hiányzó elemek és esetleges ellentmondások azonosítását, míg a jegyzőkönyvek közvetlenül alkalmasak kivonatolásra és a formális szabályzatokkal, eljárásrendekkel való összevetésre. A tesztelési eljárások során keletkező fájlok és eseményadatok (T6) a gépi tanulás szempontjából önálló, kiemelt kategóriát alkotnak: folyamatos monitorozásra, trend- és anomáliadetektálásra használhatók, és lehetőséget teremtenek arra, hogy az auditor ne csupán pillanatfelvételek alapján ítélje meg a kontrollok működését. Ez előrevetíti az auditmódszertan fejlődése mellett az auditra való felkészülés módját is, valamint az egész audit folyamatának átalakíthatóságát.

Következtetés

A tanulmány újszerűsége abban áll, hogy a magyar NIS2-alapú kiberbiztonsági auditmódszertan alap biztonsági osztályú védelmi intézkedéseihez kapcsolódó auditbizonyítékokat MI-szempontú tipológiai keretbe rendezi. Emellett a különböző evidenciákhoz konkrét, technológiailag releváns MI-eszközcsoportokat rendel. A tanulmány rámutat, hogy a hazai NIS2-alapú kiberbiztonsági auditmódszertan ugyan strukturált, jogszabályokra és nemzetközi ajánlásokra épülő keretet biztosít, a gyakorlatban használt auditbizonyítékok jelentős része mégis nehezen vagy egyáltalán nem gépileg olvasható formátumban áll rendelkezésre. A saját auditbizonyíték-tipológia megmutatta, hogy a dokumentumvizsgálat, az interjú és a tesztelés során keletkező bizonyítékok formátum és tartalom szerint jól elkülöníthető csoportokba rendezhetők, és ezekhez egyértelműen hozzárendelhetők a releváns MI-technikák. A gyakorlati következmények szempontjából ez azt jelenti, hogy rövid távon érdemes az MI-fejlesztéseket elsősorban a szabályzatok, tervek, eljárásrendek algoritmikus elemzésére fókuszálni, mivel ez a terület úgy kínál érdemi hatékonyságnövekedést, hogy közben a módszertani és megfelelőségi kockázatok kezelhetők maradnak. A vizuális bizonyítékok esetében jelenleg elsősorban az OCR és a számítógépes látás előfeldolgozó szerepe indokolt, miközben a végső értékelői döntés felelőssége továbbra is az auditoroknál marad.

A tipológia egyúttal alapot teremt egy későbbi, kvantitatív jellegű vizsgálat számára is, amelyben az egyes bizonyítéktípusok MI-alapú automatizálhatósága és kockázati szintje – például külön automatizálhatósági és kockázati mutatók formájában – számszerűen értékelhető. Jelen tanulmány ezért elsősorban a fogalmi keretek megteremtésére és a legfontosabb technológiai paraméterek azonosítására koncentrál.

Felhasznált irodalom

Aliliele, Chime et al. (2025): A Review of AI Assisted Continuous Auditing Systems in Technology Risk and Cybersecurity Oversight. *Gyanshauryam, International Scientific Refereed Research Journal,* 8(4), 210–250. Online: https://doi.org/10.32628/GISRRJ258369

Anwar, Mohammed (2023): Elevating Cybersecurity Audits. How AI is Shaping Compliance and Threat Detection. *Aitoz Multidisciplinary Review,* 2(1), 35–43. Online: www.academia.edu/127357785/Elevating_Cybersecurity_Audits_How_AI_is_Shaping_Compliance_and_Threat_Detection

Baglyos Sándor (2022): Az információbiztonsági auditálás fontossága. *Ludovika.hu,* 2022. június 23. Online: www.ludovika.hu/blogok/cyberblog/2022/06/23/az-informaciobiztonsagi-auditalas-fontossaga

Barna Bianka Rita – Kollár Csaba – Oroszi Eszter Diána (2023): A social engineering helye az információbiztonsági auditban. *Biztonságtudományi Szemle,* 23(1), 25–41. Online: https://real-j.mtak.hu/26698/1/Biztons%C3%A1gtudom%C3%A1nyi_Szemle_2023_5_1.pdf

Fehér András Tibor (2022): Mesterséges intelligencia a kibervédelemben. In Szelei Ildikó (szerk.): *A hadtudomány aktuális kérdései napjainkban II.* Budapest: Ludovika Egyetemi Kiadó, 123–137. Online: https://openaccess.ludovika.hu/nke/catalog/download/185/1520/3619?inline=1

Folorunso, Adebola et al. (2024): Impact of AI on Cybersecurity and Security Compliance. *Global Journal of Engineering and Technology Advances,* 21(1), 167–184. Online: https://doi.org/10.30574/gjeta.2024.21.1.0193

Kewat, Rajnish (2025): Why Is the Use of AI in Cybersecurity Audits Rising Among Regulated Industries? *Cyber Security Training Institute,* 2025. augusztus 2. Online: www.cybersecurityinstitute.in/blog/why-is-the-use-of-ai-in-cybersecurity-audits-rising-among-regulated-industries

Krasznay Csaba [@The Prof and The Geek] (2020): Információbiztonsági audit. *YouTube,* 2020. április 2. Online: www.youtube.com/watch?v=nb0GQQyCG6I

Loumachi, Fatma Yasmine et al. (2025): AI in Control. Rethinking Cybersecurity Compliance and Auditing. *Information and Software Technology,* 195. Online: https://doi.org/10.1016/j.infsof.2026.108132

NIST (2022): *Security and Privacy Controls for Information Systems and Organizations.* NIST Special Publication 800-53, Revision 5. Gaithersburg: National Institute of Standards and Technology. Online: https://doi.org/10.6028/NIST.SP.800-53r5

NIST (2020): *Assessing Security and Privacy Controls in Information Systems and Organizations.* NIST Special Publication 800-53A, Revision 5. Gaithersburg: National Institute of Standards and Technology. Online: https://doi.org/10.6028/NIST.SP.800-53Ar5

Smith, Jane (2024): The Role of Natural Language Processing in Automating Cybersecurity Compliance Audits. *Distributed Learning and Broad Applications in Scientific Research,* 24(10), 360–366. Online: https://dlabi.org/index.php/journal/article/view/163

Váczi Dániel – Orbók Ákos szerk. (2025): *Whitepaper: NIS 2 Magyarországon.* Budapest: Dr. Váczi Dániel. Online: www.nis2whitepaper.eu/hu/_files/ugd/3dac62_3efe3e64753d4d0faa561b6cd69cd880.pdf

Jogi források

2024. évi LXIX. törvény Magyarország kiberbiztonságáról. Online: https://njt.hu/jogszabaly/2024-69-00-00

7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről. Online: https://njt.hu/jogszabaly/2024-7-20-7G

1/2025. (I. 31.) SZTFH rendelet a kiberbiztonsági audit lefolytatásának rendjéről és a kiberbiztonsági audit legmagasabb díjáról. Online: https://njt.hu/jogszabaly/2025-1-20-8K

Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv). Online: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=OJ:L_202590613

HADMÉRNÖK
VÉDELEMINFORMATIKA
21. évfolyam (2026) 3. szám 21–42.
DOI: 10.32567/hm.2026.3.2

Olga Lavro-Gazdag[1]

Doxxing as an Information Operation[2]

A Theoretical Synthesis and Classification Framework

Abstract

Doxxing is commonly defined as the intentional gathering and non-consensual public release of personal information online, with the aim of humiliating, intimidating, threatening, or punishing a target. Military doctrine defines information operations as activities intended to influence, disrupt, corrupt, or disable decision-making. Information operations may take place in the physical sphere (e.g. damaging communication cables) or in the cognitive dimension. The aim of this paper is to determine when doxxing is only a privacy issue and when it is functionally equivalent to an information operation. The literature shows that online harassment can lead to heightened distress, a state that may resemble post-traumatic stress disorder and cause interference across several domains of a person's life. The literature also documents behavioural change, such as self-censorship and withdrawal from social activities. Targeted doxxing has been documented against police and military personnel. Such acts can signal to members of the national bodies responsible for a society's security and safety that their work carries a high personal price. This broader interpretation of information operations renders the phenomenon intelligible beyond conventional military confrontation, in relation to the threat posed by non-state actors and hybrid threats, which are connected to society and to the diverse possibilities and freedoms of the information space in substantially wider ways. In peacetime, one of the greatest challenges is the use of various elements of information operations in many

[1] PhD student, Ludovika University of Public Service, Doctoral School of Military Sciences.

[2] Artificial intelligence (Claude Opus 4.8) was used in the preparation of this paper to improve language and to assemble the rubric table, the illustrative scoring table of the examples and the figure summarising how certain doxxing events evolve and become an instance of information operation.

parts of the world, among which numerous activities in cyberspace can be observed. The interpretation of doxxing as an information operation is one such case.

Keywords: doxxing, information operation, psychological operation, target degradation, cognitive effect, hybrid warfare, fear, technology-facilitated violence

Introduction

Doxxing of people working in national security has become a recurring threat across the globe. Recent high-profile incidents remind us that, where data protection, digital-footprint awareness, and mitigating measures are not applied, the scale and the consequences of doxxing can be devastating.[3]

Doxxing campaigns targeting soldiers, police officers, and special agents reveal a consistent pattern. The published – usually large – datasets are weaponised to threaten individuals and their families, and resorting to doxxing degrades operational security. For example, a website known as the "ICE List" reportedly published the identities of thousands of alleged ICE and Border Patrol personnel.[4] In Portland, anarchist-affiliated groups publicly posted the names, photographs, home addresses, and even images of the families of ICE agents. The U.S. Department of Homeland Security reported an approximately 700% increase in assaults on ICE personnel in that jurisdiction following such activity.[5] The data used in doxxing campaigns can come from manifold sources. So-called combolists, for instance, are sold on the deep and dark web. They contain names, usernames, telephone numbers and email addresses, and in some cases cleartext passwords, which can lead to further breaches. A determined threat actor can then conduct reconnaissance, which can be done easily in the online space by anyone with modest technical knowledge. Doxxed personnel may face physical danger (e.g. harassment and attacks) and operational degradation (e.g. reduced willingness to share intelligence or to serve in sensitive roles). Mitigating such a threat requires an integrated approach. First and foremost, the nature of doxxing itself must be studied.

The information environment is now a contested space. States, non-state actors, and ordinary online bystanders compete within it for attention and for influence over decisions. One keyword of this paper is fear – fear of what happens in the online sphere, whether through network intrusions via internet-connected devices or through the information uploaded online. Anxiety can arise because a person's personal data was released online, without consent, in order to cause harm. As one military historian observes, military action is driven either by commands grounded in fear or by moral and ethical values and goals.[6] Doxxing builds on fear: a published name, address, family relationship, or interest can be weaponised against a target. Doxxing began as hacker slang, from "dropping docs", when rival hacker groups sought to expose one another's identities. Today it is largely a privacy issue that may breach data protection law – in

[3] Kovács 2020.
[4] Putman 2026.
[5] U.S. Department of Homeland Security 2025.
[6] Boda 2018.

particular the European Union's General Data Protection Regulation (GDPR). Doxxing is the intentional release of an individual's personal information onto the internet by a third party, typically without consent and with the aim of humiliating, threatening, intimidating, or punishing the target.[7] The author distinguishes three forms: deanonymising (exposing the identity of a previously anonymous person), targeting (revealing otherwise obscured details such as a home address), and delegitimising (disclosing information meant to damage a person's credibility).[8]

Information operations are studied by military scholars, strategists and political scientists alike. In U.S. joint doctrine, an information operation is the disabling and altering of information in order to influence or disable the decision-making capabilities of the adversary while protecting one's own.[9] It is not a single weapon and may be insufficient on its own. Psychological operations, electronic warfare, and computer network operations are distinct fields that fall within information operations.

Doxxing has been reported in relation to military personnel: by publishing addresses, perpetrators sought to incite public fury and to provoke aggression against uniformed individuals.[10] Doxxing has also been described as a political harassment tactic used against police officers. Research indicates that the aim of such acts was to raise the transactional costs of protest policing so that officers refrain from volunteering.[11] These examples align with what an information operation is: doxxing here seeks to influence behaviours and perceptions. Moreover, if service members are intimidated through the publication of their information online, one possible outcome is that they leave the service. Deprived of their knowledge and skills, the decision-makers of the body may then make ill-informed decisions.[12]

This paper develops a theoretical framework for determining when doxxing can be classified as information or influence operations. It draws on published definitions and typologies of doxxing, reviews the psychological and behavioural effects of online harassment, and proposes criteria for classifying doxxing events as information operations. As a preliminary statement, the deciding factors are target selection, scale and coordination.

As a conceptual study, the paper employs structured synthesis of the previously produced literature with a doctrinal analysis of information operations frameworks as its tool. The paper does not test the propositions empirically. The contribution is the theoretical framework and a classification rubric. All of this is derived from synthesis. The research questions and hypothesis are laying the ground for further empirical work. Even though they are not tested in this paper, they are important stepping stones to secure the digital presence of a nation's military, police and special security services personnel.

7 Douglas 2016.
8 Douglas 2016.
9 Joint Chiefs of Staff 2012.
10 Tucker 2015.
11 Huey et al. 2025.
12 NATO 2023.

Conceptual framework

Doxxing and information operations both operate through the information environment.[13] The information environment is the aggregate of social, cultural, linguistic, psychological, technical, and physical factors that affect how people derive meaning from information and act on it.[14] Doxxing also bridges online and offline spaces, because it moves personal information into undesired spaces and makes it available to hostile individuals or entities.[15]

Defining information operations and influence operations

Joint doctrine defines information operations as the integrated employment of communication- and information-related capabilities in order to influence, disrupt, corrupt, or usurp the decision-making of adversaries while protecting one's own.[16] The keywords are integrated employment and influence over decision-making.[17] At the same time, it is essential to protect one's own information systems. The target is cognitive, because the cognitive dimension encompasses the minds of those who collect, transmit, receive, respond to, or analyse information.[18] NATO doctrine similarly defines information operations as a function that works with and on information to achieve mission objectives, and as supporting activities focused on convincing, reinforcing, or altering the opinions of adversarial populations in support of objectives.[19]

Psychological operations are always planned and approved. Their goal is to convey previously prepared information in order to influence the emotions, motives, objective reasoning, and behaviour of foreign governments, organisations and individuals.[20] A NATO definition of psychological operations similarly emphasises planned activities directed at approved audiences in order to influence perceptions, attitudes, and behaviour in support of political and military objectives.[21]

Influence operations are not employed by militaries alone. Various cyber actors, nation-state-affiliated advanced persistent threat (APT) groups and hacktivist groups also seek to influence how information is perceived by the public. Social media researchers have observed deliberate activities by cyber threat actors intended to sway public opinion and to manipulate decision-making globally.[22] Examples include the election influence campaigns of recent years in Moldova, Romania and Hungary.[23] Like other military operations, influence operations cannot be executed without

[13] Eckert – Metzger-Riftkin 2020a.
[14] U.S. Department of Defense 2023.
[15] Eckert – Metzger-Riftkin 2020a.
[16] Joint Chiefs of Staff 2014.
[17] National Institute of Standards and Technology s. a.
[18] Joint Chiefs of Staff 2012.
[19] NATO 2023.
[20] Joint Chiefs of Staff 2010.
[21] Avădănei 2022.
[22] Pastor-Galindo et al. 2025.
[23] Harward 2025; Swanson 2018.

being broken down into phases – namely planning, information gathering, execution and assessment.[24]

Definition of doxxing

As a first step, doxxing must be distinguished from accidental information disclosure.[25] Accidental disclosure can occur – among other ways – during a ransomware attack (as in the case of the Hungarian Védelmi Beszerzési Ügynökség [Defence Procurement Agency])[26] or through misconfigured cloud storage (as in the 2023 Pentagon email leak).[27]

Doxxing is frequently defined as the intentional publication of personal information that makes an individual recognisable, with the aim of disclosing, humiliating and threatening.[28] This account explains how doxxing moves personal information from expected, private spaces to undesired surfaces, through which the data becomes available to hostile individuals or entities.[29]

For this paper, doxxing is defined as the non-consensual public dissemination of personally identifying or private information, intended to expose, intimidate, harass, delegitimise, or physically endanger a person.[30] By publishing personal information, the threat actor seeks an audience that may act on it.

Literature review

The literature on doxxing comes mainly from research on online harassment and minority group rights. Case studies, legal analysis, and some conceptual work form the core of most published papers and books, and the literature treats doxxing as technology-facilitated violence and as part of broader harassment processes.[31] This section synthesises definitions, harms, target selection, coordinated campaigning, and effects on behaviour and decision-making, opening the way to treating doxxing as a form of information operation under certain conditions.

[24] Pastor-Galindo et al. 2025.
[25] Anderson–Wood 2021.
[26] The Hungarian Védelmi Beszerzési Ügynökség [Defence Procurement Agency] (VBÜ) is responsible for the procurement of military equipment. In 2024 the organisation was attacked by the INC Ransomware group. Besides stolen procurement-related documents, personal information was also published on the threat actor's dark web page. See Antoniuk 2024.
[27] According to an independent security researcher, the U.S. military's internal emails were accessible for two weeks without authentication. The exposed server leaked approximately three terabytes of U.S. Special Operations Command (USSOCOM) internal emails. See Hope 2023.
[28] Douglas 2016.
[29] Eckert – Metzger-Riftkin 2020a.
[30] Ong 2025.
[31] Eckert – Metzger-Riftkin 2020a.

Typologies of doxxing

Doxxing is described as a serious violation of privacy and security because it involves the unauthorised and often malicious publication of personal or confidential information.[32] It is also described as an attack that can cause substantial harm, ranging from harassing comments to direct physical danger.[33] In the first months of the Russia–Ukraine war, the personal data of around 120,000 Russian soldiers was reportedly published on Telegram channels. Although the recency and accuracy of the data may be questioned, such disclosure could cause irreparable damage to operations.[34] In a 2015 Facebook post, U.S. Central Command stated that the compilation of "death lists" containing service members' data had become the "new norm", and asked personnel and their families to limit their online data sharing.[35] Beyond personal data (names, addresses, telephone numbers, email details, financial information and images), the doxxing of uniformed personnel not infrequently extends to the same data about their loved ones.[36]

Typologies classify doxxing by the mechanism of exposure.[37] One widely used typology distinguishes deanonymisation, targeting and delegitimisation:[38]

- Deanonymising doxxing releases information that reveals the identity of a previously anonymous or pseudonymous person.
- Targeting doxxing reveals information that allows a person to be physically located.
- Delegitimising doxxing releases private information intended to undermine credibility, reputation, or character.[39]

A second typological strand focuses on motivations and uses, identifying extortion, silencing, retribution, control and reputation-building.[40] Process models highlight that doxxing involves a reconnaissance stage, a release stage, and a response stage – the last of which requires an audience that may wish to inflict harm on the identified individual.[41]

Psychological effects

Several articles describe doxxing as capable of causing psychological distress. In harassment and cyberstalking research, victims may suffer high levels of distress. As

[32] Tan 2023.
[33] Snyder et al. 2017.
[34] Jensen–Watts 2022.
[35] U.S. Central Command 2015.
[36] Factually 2026.
[37] Anderson–Wood 2022.
[38] Douglas 2016.
[39] Douglas 2016.
[40] Anderson–Wood 2021.
[41] Bulgakova 2025.

scholars note, this stress is broadly comparable to the symptoms seen in post-traumatic stress disorder.[42]

Harassment research – in studying street harassment – has documented trauma narratives.[43] Victims reported longer-term fear, anxiety and anger. In the worst cases, these feelings outlasted the initial incident, leaving the harassed individuals with the tormenting sense of being constantly about to be attacked.[44] Harassment also damaged self-esteem, with participants describing being made to feel low, dirty, disgusting and degraded.[45]

Doxxing-specific qualitative research likewise supports the experience of acute shock. Participants reported being in an *emergency mode*. This might indicate the state of acute stress in which victims struggle to regain control over their exposed information. Contacting the exposing platforms, warning family members, locking down accounts are all steps taken by victims to mitigate the risk arising from the doxxing event. Despite their effort, they most probably cannot stop its spreading. Even as they tried to regain control over their information once they became aware of the doxxing, they could not.[46]

Behavioural effects

Inciting fear and threatening violence can lead directly to behavioural change. At the beginning of 2026, three Hungarian and one Romanian teenager were arrested after using leaked personal data to threaten attacks on police units. Authorities stated that the incidents formed part of coordinated swatting and doxxing campaigns.[47] Such campaigns are able to cause damage because their aim is not disclosure for its own sake but the intimidation of the targets. Intimidation could incite behavioural change, and behavioural change has been documented in response to online harassment and doxxing exposure.[48] Because journalism research has examined how doxxing produces behavioural change most thoroughly, the effect is illustrated here through that field. In journalism research, self-censorship was used when reporting on certain topics in order to avoid threats and hatred.[49] Other journalism research indicates that online comments influence job satisfaction, focus, self-esteem, frustration and anger. It can lead journalists to avoid certain topics or stories.[50]

It has also been shown that personal accounts (e.g. social media accounts) referenced in doxxing files are more likely to be closed or made private than comparable accounts after the doxxing occurs.[51] This is a clear illustration of behavioural change,

[42] Short et al. 2015.
[43] Thornton et al. 2024.
[44] Thornton et al. 2024.
[45] Thornton et al. 2024.
[46] Eckert – Metzger-Riftkin 2020b.
[47] Antoniuk 2026.
[48] Snyder et al. 2017.
[49] Björkenfeldt 2026.
[50] Carlson–Witt 2020.
[51] Snyder et al. 2017.

as personal data exposure led targets to reduce their visibility and participation in order to avoid further harm.[52]

Target populations

Target selection is extremely important for classifying an event as an information operations manoeuvre. Doxxing perpetrators may target not only the victim but also members of their household, family and circle of friends. This matters for behaviour change because threatening or exposing family members can increase perceived vulnerability.[53]

Studies of the doxxing of police officers illustrate how targeting helps threat actors physically locate a victim. In certain cases, the unauthorised disclosure of a location was accompanied by messages urging followers to harass an individual or his family.[54] In one documented case, online doxxing immediately resulted in a police chat group receiving numerous death threats.[55]

Journalistic pieces and security reportings also describe military and security targets.[56] In 2015, an ISIS-linked group posted the names, photographs, and addresses of U.S. combat pilots and other military personnel.[57] After releasing the information, the group asked its followers to "take the final step".[58]

Coordinated campaigns

Doxxing cannot be described as an act that stands alone. Embedded in a complex influence campaign, it can cause greater damage.[59] Some authors describe doxxing as an offshoot of espionage, reasoning that information obtained through a cyberattack can be disclosed in order to undermine an adversary.[60] In my opinion this perspective offers further reason why doxxing could, and should, be considered an information operation.

Bots have featured in many information operations, mainly influence operations, but they can also be used in doxxing. Coordinated bot groups can attack specific users effectively, frightening the targeted user into silence or driving them off the platform on which they were attacked.[61]

[52] Ong 2025.
[53] Budianto–Hendrayadi 2023.
[54] Huey et al. 2025.
[55] Huey et al. 2025.
[56] Arizanti 2026.
[57] Tucker 2015.
[58] Tucker 2015.
[59] Brangetto–Veenendaal 2016.
[60] Brangetto–Veenendaal 2016.
[61] Woolley 2024.

Research gaps

The reviewed literature describes how doxxing has evolved from a privacy violation into something that can be read as an information operation. No direct link, however, has yet been established. This paper identifies the following research gaps:

- *Conceptual gap.* Doxxing is rarely listed in information operations doctrine. Both U.S. and NATO doctrines stress influencing decision-making and audience behaviour rather than personal data exposure as a distinct method.[62] Yet doxxing is itself capable of intimidating service members, and when used against personnel working in national security it can function as a weapon.[63] Future work should consider doxxing as an act that may affect an adversary's decision-making process.
- *Fragmented definitions.* Definitions of doxxing varies greatly. Some authors highlight the non-consensual publication of private or identifying information.[64] Others stress contextual integrity and the movement of information into *undesired online spaces.*[65] Still others argue that some definitions are too vague, covering almost any disclosure.[66] Closing this gap requires a cross-disciplinary definition narrow enough to serve as a basis for measurement.
- *Limited research on military, police and national security personnel.* As illustrated above, doxxing targets police officers, special agents and military personnel. Future studies should compare doxxing impacts across roles and institutional affiliations, including these groups.[67]
- *Attribution and intent.* Most definitions hold that doxxing is intentional and that its goal is to humiliate, intimidate and punish.[68] Although motivations are usually identified, little research asks whether a given instance is an isolated incident or campaign-integrated.[69] Research should develop attribution grounded in observable features, such as integration with espionage-derived disclosure and connection to other influence operations.[70]

This paper addresses the conceptual gap by aligning the information disclosure mechanism of doxxing with doctrinal definitions that focus on affecting cognition, decision-making, and behaviour through integrated information activities.[71] It narrows definitional ambiguity by adopting an intentional, non-consensual disclosure definition, and it uses typologies that distinguish deanonymising, targeting and delegitimising harms.[72] The article does not resolve attribution and scale questions

[62] Joint Chiefs of Staff 2012; NATO 2023.
[63] Anderson–Wood 2021; Ong 2025.
[64] Douglas 2016; Ong 2025; Tan 2023.
[65] Eckert – Metzger-Riftkin 2020a.
[66] Fang et al. 2023.
[67] Tucker 2015.
[68] Anderson–Wood 2021.
[69] Bulgakova 2025.
[70] Brangetto–Veenendaal 2016; Pastor-Galindo et al. 2025.
[71] Joint Chiefs of Staff 2012; NATO 2023; U.S. Department of Defense 2023.
[72] Anderson–Wood 2021; Douglas 2016.

empirically, but it argues that audience size and attacker coordination are central to downstream effects.[73] My goal is to make the link explicit. Today the existing literature treats doxxing as a privacy harm, while information operation as a strategic capability, I argue that these two meet at a certain point. In my paper I define that point and develop criteria for that.

Research questions and hypotheses

This paper treats doxxing as a potential form of information operation, on the grounds that it can change cognition and behaviour in target audiences. The research questions concern classification and the points at which disclosure can lead to behavioural change.

Research questions

RQ1. When should doxxing be understood as targeting a single individual, and when does it involve a larger community? Answering this question clarifies how such an act can be called an information operation aimed at influencing decision-making in a target population.
RQ2. How can personal data exposure lead to long-term fear, distress and PTSD-like, complex mental states, including withdrawal from public roles?
RQ3. Which behavioural changes signal success from the perspective of an influence campaign?
RQ4. What kinds of coordination, amplification, and persistence make doxxing more likely to function as a campaign rather than a one-off event?

Hypotheses

H1. Doxxing is more likely to qualify as an information operation when it is integrated with other influence techniques.
H2. Doxxing produces behaviour change through psychological distress and perceived vulnerability, because harassment is associated with distress and trauma-like symptoms.
The hypotheses are conceptual propositions, not foreseen to produce empirical results. Future research must follow to operationalise the hypotheses.

Theoretical argument

To argue that doxxing belongs to the sphere of information operations, one must accept that the claim is conditional – doxxing is not always an information operation.

[73] Wang et al. 2025.

Some doxxing events can be functionally equivalent to information operations when they are planned information activities designed to create cognitive effects. To examine H1, this paper draws on doctrinal definitions of information and psychological operations, as well as on doxxing typologies and the motives behind doxxing (notably coercion and targeting).

Functional equivalence

I argue that doxxing can be equated with information operation in case doxxing fulfils the following three criteria:

- role-bearing target
- an intent to shape behaviour
- dissemination of information to mobilise the receivers of the information

Information operations target an audience's situational assessment, intentions and capabilities – not only for military purposes but also in political, civilian and hybrid environments.[74] Achieving the intended effect therefore requires accurately identifying the audience and selecting the message and the means by which the operation is conducted. The audience must comply with, identify with, or internalise the message for the objective – or to say it more simply, influence the decision-making process.[75] This feature aligns with the information operations focus on affecting cognition and decision-making by shaping perceived risks through information disclosure and audience mobilisation.[76] The terms information operation and doxxing should be treated as equated on certain terms. In the doctrinal definition of information operation influence, disruption and altering of the decision-making process appear. These effects can be found in doxxing as well. Because of their shared mechanism and effect, I treat equivalence not as a metaphor but as a claim.

NATO information operations doctrine likewise defines such planned activities as supporting manoeuvres to influence behaviour, attitudes and perception. When doxxing is planned and integrated into a campaign, it can be seen as an information-related technique used to create desired cognitive and behavioural effects.[77]

Mechanisms of behaviour change

The three dimensions of information operations are the cognitive, the physical and the informational, representing the human, material, and technological domains in which influence effects are applied.[78]

[74] Haig 2022.
[75] Joint Chiefs of Staff 2014.
[76] Bulgakova 2025; Joint Chiefs of Staff 2012.
[77] Brangetto–Veenendaal 2016.
[78] Haig 2022.

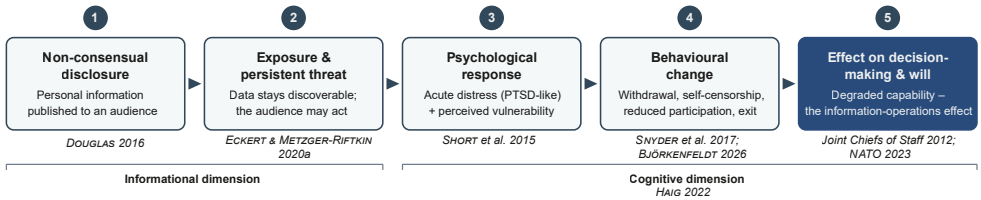


Figure 1: The doxxing-to-behaviour mechanism
Source: compiled by the author

The mechanisms of doxxing are partly informational and partly cognitive. They are informational because publishing unwanted information online disrupts privacy. Once personal information is shared on an open platform, the victim may fear physical harm in the real world.[79] Because at present there is no reliable means of removing information from the internet, doxxing information may remain discoverable indefinitely.

Distress follows directly from unwanted information exposure. According to the literature, it can resemble PTSD symptoms, which are described as interfering with occupational activity and social relations, and the affected person may withdraw from public engagement (see Figure 1).[80]

Journalists have described fear for their personal safety and hesitation before covering controversial topics or posting certain information online, indicating a direct link to behavioural restraint.[81]

Boundary cases and counterarguments

A classification framework must separate doxxing from legitimate information publishing, such as whistleblowing, where disclosure occurs in the public interest rather than out of ill will.[82] Because doxxing definitions are sometimes overly broad and cover almost any disclosure, the framework must clearly specify who may legitimately be subject to public scrutiny through disclosed information. Such guidance belongs to research and policy classification.[83]

A second boundary concerns intent and effect. Unintentional or accidental publication occurs (e.g. an email containing personal data sent to the wrong address, or a lost storage device holding personal data). Doctrine emphasises that information operations must be integrated and orchestrated within a previously approved plan, which implies that isolated doxxing cannot be called an information operation.[84]

[79] Ong 2025.
[80] Short et al. 2015.
[81] Carlson–Witt 2020.
[82] Fang et al. 2023.
[83] Fang et al. 2023.
[84] Joint Chiefs of Staff 2012.

Finally, not all doxxing aims to achieve behaviour change in the target. Yet even without that intention, a threatening audience may form and seek to harass the doxxed person.[85]

Criteria

Merging information operations doctrine with the doxxing literature calls for a multi-criteria approach. The doctrine focuses on integration, targeting, cognitive effects and behavioural change as the final step.[86] The doxxing literature focuses on intentional information release, the inducement of fear and audience response.[87]

Intent

Intent is central to the definitions of both doxxing and information operations. Doxxing is defined as the intentional public release of personal information, often intended to intimidate or punish. Information operations are defined as deliberate activities aimed at influencing decision-making to achieve objectives. Where an intent to influence the public or decision-making bodies can be identified in the motives behind doxxing, the event can be said to constitute an information operation.

Target

Choosing the target is an essential part of both doxxing and information operations. Doxxing is more likely to constitute a form of information operation when it is directed at organisational roles (e.g. police officers, military personnel). Such targets are chosen in order to pressure behaviour change.[88]

Scale

Scale – the size of the audience – is relevant because doxxing is intended to reach many people.[89] Because information posted online may remain available indefinitely, scale increases exposure and the probability of further audience action over time.[90] Scale can also confer an operational advantage – a large target population, such as a doxxing list of many military personnel, can heighten collective fear.[91]

[85] Flewelling 2023.
[86] Joint Chiefs of Staff 2012; NATO 2023.
[87] Anderson–Wood 2021; Eckert – Metzger-Riftkin 2020a.
[88] Huey et al. 2025; Tucker 2015.
[89] Ong 2025.
[90] Eckert – Metzger-Riftkin 2020a.
[91] Huey et al. 2025; Tucker 2015.

Coordination

Coordination is a key element of information operations doctrine, requiring planning, integration, and thorough orchestration to achieve the set goals.[92] Influence operations frameworks use techniques such as amplification and the flooding of the information space.[93] As shown in earlier examples, doxxing can be integrated into influence operations. Moreover, gathering information for doxxing requires reconnaissance and can be seen as an offshoot of espionage, in which stolen information is disclosed to undermine an adversary.[94] Doxxing can therefore be listed among information operations techniques when it is coordinated with other campaign elements.

Behavioural effect

Information operations doctrine holds that information activities aim to alter behaviour.[95] Doxxing is defined as an intimidating act achieved through the non-consensual publication of personal information.[96] Empirical work shows that withdrawal behaviour follows such acts – including account closure, increased privacy settings, self-censorship, or the avoidance of certain topics.[97] A doxxing event can be listed among information operations where there is observable change in the target's organisational engagement, participation, or speech.[98]

Scoring rubric

The rubric in Table 1 summarises the criteria for classifying a doxxing episode as an information operations candidate.[99] It is designed for research coding and structured case comparison rather than for legal adjudication. A simple additive scoring function is used, $S = \Sigma\, s_i$ for $i = 1$ to 5, where each criterion is scored from 0 to 3, giving a maximum of 15. Higher scores indicate stronger functional similarity to information operations doctrine and influence campaign logic.

A classification threshold of $S \geq 11$ is proposed for an *information operations candidate,* because this level requires several criteria to be at least moderate rather than allowing qualification on intent or individual harm alone. Consistent with Section *Boundary cases and counterarguments,* coordination has a special status. Because doctrine treats integration as constitutive of an information operation, a score of 0 on Coordination is a strong contraindication even where other criteria score highly. Both the threshold and this qualification are proposed heuristics for research use and require empirical calibration.

[92] Joint Chiefs of Staff 2012.
[93] Pastor-Galindo et al. 2025.
[94] Brangetto–Veenendaal 2016.
[95] NATO 2023.
[96] Ong 2025.
[97] Björkenfeldt 2026; Snyder et al. 2017; Wang et al. 2025.
[98] Huey et al. 2025; Wang et al. 2025.
[99] NATO 2023.

Table 1: Scoring rubric for classifying a doxxing episode as an information operations candidate

Criterion	0 score	1 score	2 score	3 score
Intent	No evidence of intent to influence beyond interpersonal harm[100]	Intent to punish or shame a target[101]	Intent to intimidate or silence a target, or to enact revenge, as reported by targets or described by perpetrators[102]	Intent linked to objectives to influence decision-making or participation, consistent with influence and information operations logic[103]
Target	Target is not linked to institutional roles or collective decision nodes[104]	Target is an individual without clear organisational relevance, though exposure creates a risk of harassment[105]	Target is a role-bearing individual (journalist, activist, officer) with a public-facing function, with explicit intimidation or targeting to enable physical location[106]	Target set is an organisational choke-point population (e.g. officers policing protests, military personnel lists), with an explicit logic of raising costs so that members refrain from serving[107]
Scale	Limited dissemination and minimal evidence of audience response[108]	Public release occurs, but audience mobilisation is unclear[109]	Release is publicised to create an audience that may act, consistent with a response stage requiring an audience[110]	High-volume audience attack or list-style targeting that plausibly increases behavioural change[111]
Coordination	No evidence of planning or integration with other actions[112]	Some sequencing or staging (reconnaissance–release–response) without broader campaign context[113]	Evidence of phased planning or integration with other influence techniques[114]	Evidence of integration into a wider influence operation or espionage-derived disclosure[115]
Behavioural effect	No detectable change in behaviour, participation, or expression[116]	Individual-level withdrawal, such as making accounts private or closed[117]	Withdrawal from public appearances or self-censorship to avoid threats and hatred[118]	Organisational or role-level behaviour change, such as reduced volunteering, ingrained self-censorship, or delayed posting under sustained attack[119]

Source: compiled by the author

[100] Tan 2023.
[101] Flewelling 2023.
[102] Eckert – Metzger-Riftkin 2020b; Ong 2025.
[103] Joint Chiefs of Staff 2012; Pastor-Galindo et al. 2025.
[104] Anderson–Wood 2021.
[105] Snyder et al. 2017.
[106] Douglas 2016; Huey et al. 2025.
[107] Huey et al. 2025; Tucker 2015.
[108] Anderson–Wood 2021.
[109] Snyder et al. 2017.
[110] Bulgakova 2025; Ong 2025.
[111] Tucker 2015; Wang et al. 2025.
[112] Fang et al. 2023.
[113] Bulgakova 2025; Ong 2025.
[114] Pastor-Galindo et al. 2025.
[115] Arizanti 2026; Brangetto–Veenendaal 2016.
[116] Fang et al. 2023.
[117] Snyder et al. 2017.
[118] Björkenfeldt 2026; Carlson–Witt 2020.
[119] Björkenfeldt 2026; Wang et al. 2025.

Application to cases

I applied the above detailed scoring rubric to three cases. Two cases were described earlier, while one boundary case is brought in to test. The scores are based on my analytical judgement and the reported claims should be read with the caveats in Section *Limitations*.

Case 1. The Islamic State's "hit list" of U.S. military personnel[120]

I score Intent at 3 because the group not only disclosed the information but urged its followers to harm the soldiers. The threat was not against a single person but against the military community. Target is also 3. The released names were those of combat pilots. Specially trained, hard to substitute population. The Scale is also 3. ISIS disclosed a list to a population which was known to be aggressive towards U.S. military personnel. Coordination is on 2. This is so, because even though the release of the information was carried out in an organised way, it has not been proved to be part of a wider propaganda effort. The Behavioural effect is also 2. The U.S. Central Command issued a public advisory. However, direct measurements of withdrawal from online engagement are not tracked. The total point is 13, therefore this event classifies as an information operation candidate.

Doxxing police officers during protest duties[121]

I score Intent as 3 because the disclosures were aimed at deterring police officers from taking on protest policing duties. Target is 3, since the officers who assigned to control protesters were a special group at that time in the police force. Scale is 2. The published information was not evenly distributed, even though it sometimes called for violence. Coordination is 2 since this event is not directly related to broader information operation. However, it had a strong aim to disturb protest policing forces. Behavioural effect is 3. The role-based pressure achieved its goal – numerous police officers retained from serving on such duty. The total is 13, so this event qualifies as information operation as well.

Disclosure of a former partner's address as a revenge (boundary case)

Intent is 1, because the aim is not to influence the general population, but to punish a single person. Target is 0, since the doxxed person is not important in the collective decision-making, nor does he/she hold an important function. Scale is 1. Despite the fact that the information is published, there is no or low audience mobilisation.

[120] Tucker 2015.
[121] Huey et al. 2025.

Coordination is 0. Since the action was not prepared for staging, integration in other actions, this category can be dismissed. The Behavioural effect can be set at 3, since the victim will most probably withdraw. Population-level effect is non-existent in this case. The total is 5.

Table 2: Illustrative application of the rubric to three cases

Case	Intent	Target	Scale	Coordination	Behaviour	Total	Result
1. IS military "hit list"	3	3	3	2	2	13	IO candidate
2. Protest-policing doxxing	3	3	2	2	3	13	IO candidate
3. Private revenge doxxing	1	0	1	0	3	5	Private abuse

Note: Criteria are scored 0–3. The maximum is 15 and the classification threshold is S ≥ 11. Scores are the author's analytical judgements applied to the published record. Figures in the security cases are reported claims.
Source: compiled by the author

Discussion

The literature supports listing doxxing among information operations, because doxxing can serve as a planned information activity that targets cognition and behaviour through intimidation, delegitimisation and audience mobilisation.[122] This is consistent with the information operations doctrines, which hold that the ultimate target of an information operation is the human decision-making process, and with influence operations frameworks that include harassment and target degradation to discredit, intimidate, or silence challengers to a narrative.[123] Placing it together, it can be stated that the observations are not of a mere surface resemblance. The doctrinal definitions and the doxxing evidence describe the same sequence. It looks as the following: information is disclosed and the target's behaviour changes in a way that the discloser planned. While this happens, an audience is mobilised. Based on these observations, I treat the two bodies of work as describing one phenomenon from two vantage points. Doxxing does not just resemble information operation but it is an example of that whenever the set conditions are met.

Doxxing used against police officers during protests, intended to raise the costs of participation, exemplifies an explicit behaviour change objective.[124] The mobilising and intimidating effect of doxxing is also illustrated by the threatening telephone calls received by doxxed military personnel.[125] If I examine the patterns across these cases, it will be revealed that actors as different as protest groups, state-linked threat actors or jihadi groups arrived at the same technique. All of them recognised that

[122] Bulgakova 2025; Douglas 2016; NATO 2023.
[123] Pastor-Galindo et al. 2025.
[124] Huey et al. 2025.
[125] Tucker 2015.

publishing the personal data of role-bearing personnel will produce the same result. This convergence matters, because it proves that the deterring effect of doxxing is reproducible and is understood by those who engage in it. A single act of information disclosure most probably will not change the population's behaviour. However, targeted disclosure aimed at the professional community can. From the previously described examples it is clear that threat actors are aware of it.

The literature on coordinated campaigns further supports listing doxxing among influence operations. By shaming and embarrassing the victim, doxxing – like other influence operations – undermines an adversary through the disclosure of information.[126] This reframes where the harm of operational doxxing actually is. The named individual is only a tool in this operation. The intended target is the audience that watches – which can be the fellow servicemen or the general public. The goal of the threat actor is to deter others of taking on the responsibilities and to discredit the unit or the whole service. In one sentence: the individual is harmed while the audience is influenced.

Limitations

Several limitations qualify this argument. Direct empirical evidence that doxxing causes behaviour change is limited, as demonstrated in this paper, and much of the psychological evidence is drawn from harassment and cyberstalking samples rather than from doxxing-only studies.[127] In addition, the proposed rubric is not empirically validated, and the $S \geq 11$ threshold is a reasoned heuristic that requires calibration against coded cases. The doctrinal focus is also primarily Western (U.S. and NATO), and other doctrinal traditions might conceptualise information confrontation differently.

Conclusion

Doxxing is the intentional, non-consensual publication of personal information online, often with the aim of humiliating, intimidating, threatening, or punishing. It can enable real-world harassment and physical danger. Information operations are the integrated employment of information-related capabilities to influence or disrupt decision-making.[128] The literature shows that harassment can generate distress resembling PTSD, which can interfere with occupational and social functioning,[129] and that doxxing produces behavioural and withdrawal effects, such as withdrawal behaviour and the avoidance of contacts and topics.[130]

Together, these bodies of evidence support a structured argument that doxxing can be listed among information operations under specified conditions. Doxxing can be classified as an information operation when:

[126] Brangetto–Veenendaal 2016.
[127] Ong 2025; Short et al. 2015.
[128] Joint Chiefs of Staff 2012; NATO 2023.
[129] Short et al. 2015.
[130] Björkenfeldt 2026; Snyder et al. 2017; Wang et al. 2025.

- it is planned and coordinated
- it targets role-bearing persons or key figures
- it mobilises an audience to act
- it produces observable behavioural change aligned with an objective

If doxxing is treated as a privacy violation, it will be on the table of data protection officers. However, if it is treated as an information operation, it will be an urgent topic for force protection and institutional resilience. I argue that scholars studying security should accept the second register.

References

Anderson, Briony – Wood, Mark A. (2021): Doxxing: A Scoping Review and Typology. In Bailey, Jane – Flynn, Asher – Henry, Nicola (eds.): *The Emerald International Handbook of Technology-Facilitated Violence and Abuse.* Leeds: Emerald Publishing, 205–226. Online: https://doi.org/10.1108/978-1-83982-848-520211015

Anderson, Briony – Wood, Mark A. (2022): Harm Imbrication and Virtualised Violence: Reconceptualising the Harms of Doxxing. *International Journal for Crime, Justice and Social Democracy,* 11(1), 196–209. Online: https://doi.org/10.5204/ijcjsd.2140

Antoniuk, Daryna (2024): Hungary Confirms Hack of Defense Procurement Agency. *The Record,* 14 November 2024. Online: https://therecord.media/hungary-defense-procurement-agency-hacked

Antoniuk, Daryna (2026): Teen Swatting Suspects Arrested in Hungary and Romania. *The Record,* 28 January 2026. Online: https://therecord.media/teen-swatting-doxxing-suspects-arrested-hungary-romania

Arizanti, Michael (2026): Doxxing of India's Top Military Officer Reflects a New China–Pakistan Tactic. *The Times of Israel,* 14 May 2026. Online: https://blogs.timesofisrael.com/doxxing-of-indias-top-military-officer-reflects-a-new-china-pakistan-tactic/

Avădănei, Angela-Karina (2022): Influence Operations, between the Ethical and Critical Facet. *Romanian Military Thinking,* (3), 74–87. Online: https://doi.org/10.55535/RMT.2022.3.05

Björkenfeldt, Oscar (2026): Self-Censorship in Journalism: The Role of Emotional, Professional, and Institutional Factors. *Digital Journalism,* 14(3), 493–510. Online: https://doi.org/10.1080/21670811.2025.2601961

Boda, Mihály (2018): Az alapvető katonai erények mibenléte és helyük a hosszú 19. századi magyar hadtudományos gondolkodásban: 3. rész – A becsület. *Hadtudomány,* 28(3–4), 17–30. Online: https://doi.org/10.17047/HADTUD.2018.28.3-4.17

Brangetto, Pascal – Veenendaal, Matthijs A. (2016): Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations. In *2016 8th International Conference on Cyber Conflict (CyCon),* 113–126. Online: https://doi.org/10.1109/CYCON.2016.7529430

Budianto, Azis – Hendrayadi, Agus (2023): Juridical Review of the Criminal Act of Doxing: Dissemination of Personal Data without Permission in the Perspective of Law No. 19 of 2016 Concerning EIT. In *Proceedings of the 3rd Multidisciplinary International Conference (MIC 2023).* Online: https://doi.org/10.4108/eai.28-10-2023.2341796

Bulgakova, Daria (2025): Doxing: The Sandy Hook Case Study. *NaUKMA Research Papers. Law,* 14, 3–18. Online: https://doi.org/10.18523/2617-2607.2024.14.3-18

Carlson, Caitlin R. – Witt, Haley (2020): Online Harassment of U.S. Women Journalists and Its Impact on Press Freedom. *First Monday,* 25(11). Online: https://doi.org/10.5210/fm.v25i11.11071

Douglas, David M. (2016): Doxing: A Conceptual Analysis. *Ethics and Information Technology,* 18(3), 199–210. Online: https://doi.org/10.1007/s10676-016-9406-0

Eckert, Stine – Metzger-Riftkin, Jade (2020a): Doxxing. In Ross, Karen – Bachmann, Ingrid – Cardo, Valentina – Moorti, Sujata – Scarcelli, Cosimo M. (eds.): *The International Encyclopedia of Gender, Media, and Communication.* Hoboken: Wiley Blackwell – ICA, 1–5. Online: https://doi.org/10.1002/9781119429128.iegmc009

Eckert, Stine – Metzger-Riftkin, Jade (2020b): Doxxing, Privacy and Gendered Harassment: The Shock and Normalization of Veillance Cultures. *Medien & Kommunikationswissenschaft,* 68(3), 273–287. Online: https://doi.org/10.5771/1615-634X-2020-3-273

Factually (2026): Have ICE Agents or Their Families Been Doxxed? *Factually,* 27 January 2026. Online: https://factually.co/fact-checks/politics/have-ice-agents-or-families-been-doxxed-23887e

Fang, Yuan – Risius, Marten – Cheung, Christy (2023): Understanding the Current State of Knowledge and Future Directions of Doxing Research: A Social Cognitive Theory Perspective. In *Proceedings of the 56th Hawaii International Conference on System Sciences.* Online: https://doi.org/10.24251/HICSS.2023.672

Flewelling, Riley (2023): Not Just Words: Grappling with the Doxing of Civilians in War. *Center on Law, Ethics and National Security, Essay Series,* (19). Online: https://sites.duke.edu/lawfire/files/2023/07/R.-Flewelling-Essay-7.25.23.pdf

Haig, Zsolt (2022): Kibertéri kognitív befolyásolás az információs műveletekben. *Hadtudományi Szemle,* 15(2), 115–130. Online: https://doi.org/10.32563/hsz.2022.2.7

Harward, Christina (2025): Russia Continues Efforts to Regain Influence over Moldova. *Institute for the Study of War,* 5 September 2025. Online: https://understandingwar.org/research/russia-ukraine/russia-continues-efforts-to-regain-influence-over-moldova/

Hope, Alicia (2023): The Pentagon Leaked Sensitive Military Emails via a Misconfigured Microsoft Azure Government Cloud. *CPO Magazine,* 2 March 2023. Online: www.cpomagazine.com/cyber-security/the-pentagon-leaked-sensitive-military-emails-via-a-misconfigured-microsoft-azure-government-cloud/

Huey, Laura – Ferguson, Lorna – Towns, Zachary (2025): „Cops Need Doxxed": Releasing Personal Information of Police Officers as a Tool of Political Harassment. *Crime & Delinquency,* 71(3), 714–739. Online: https://doi.org/10.1177/00111287241271069

Jensen, Eric – Watts, Sean (2022): Ukraine Symposium – Doxing Enemy Soldiers and the Law of War. *Lieber Institute West Point,* 31 October 2022. Online: https://lieber.westpoint.edu/doxing-enemy-soldiers-law-of-war/

Joint Chiefs of Staff (2010): *Joint Publication 3-13.2. Military Information Support Operations.* Online: https://info.publicintelligence.net/JCS-MISO.pdf

Joint Chiefs of Staff (2012): *Joint Publication 3-13. Information Operations.* Online: https://defenseinnovationmarketplace.dtic.mil/wp-content/uploads/2018/02/12102012_io1.pdf

Joint Chiefs of Staff (2014): *Chairman of the Joint Chiefs of Staff Instruction 3210.01. Joint Information Operations Proponent.* Online: www.jcs.mil/Portals/36/Documents/Library/Instructions/3210_01.pdf

Kovács, László (2020): A kiberbiztonság és a kiberműveletek megjelenése Magyarország új Nemzeti Biztonsági Stratégiájában. *Honvédségi Szemle,* 148(5), 3–18. Online: https://doi.org/10.35926/HSZ.2020.5.1

National Institute of Standards and Technology (s. a.): Information Operations (IO). *Computer Security Resource Center.* Online: https://csrc.nist.gov/glossary/term/information_operations

NATO (2023): *Allied Joint Publication 10.1. Allied Joint Doctrine for Information Operations.* North Atlantic Treaty Organization.

Novak, Matt (2026): How the Definition of "Doxxing" Is Being Twisted into a Weapon of Anonymity. *Gizmodo,* 14 January 2026. Online: https://gizmodo.com/how-the-definition-of-doxxing-is-being-twisted-into-a-weapon-of-anonymity-2000709404

Ong, Rebecca (2025): Hong Kong's Response to the Fight against Doxxing. *Common Law World Review,* 54(1), 17–42. Online: https://doi.org/10.1177/14737795241267290

Pastor-Galindo, Javier – Nespoli, Pantaleone – Ruipérez-Valiente, José A. – Camacho, David (2025): Influence Operations in Social Networks. *arXiv*. Online: https://doi.org/10.48550/ARXIV.2502.11827

Putman, Joanna (2026): "ICE List" Doxxing Site Alleges DHS Whistleblower Leaked Identities of 4,500 Agents. *Police 1,* 14 January 2026. Online: https://globalordnancenews.com/2026/01/14/ice-list-doxxing-site-alleges-dhs-whistleblower-leaked-identities-of-4500-agents/

Short, Emma – Guppy, Andrew – Hart, Jacqui A. – Barnes, James (2015): The Impact of Cyberstalking. *Studies in Media and Communication,* 3(2), 23–37. Online: https://doi.org/10.11114/smc.v3i2.970

Snyder, Peter – Doerfler, Periwinkle – Kanich, Chris – McCoy, Damon (2017): Fifteen Minutes of Unwanted Fame: Detecting and Characterizing Doxing. In *Proceedings of the 2017 Internet Measurement Conference,* 432–444. Online: https://doi.org/10.1145/3131365.3131385

Swanson, Robert C. R. (2018): Two Case Studies of Russian Propaganda in Romania and Hungary. *The International Affairs Review,* 15 February 2018. Online: www.iar-gwu.org/print-archive/64g7lshepy1awksgtiyvj3bsqfipw0

Tan, Albert (2023): *To Dox or Not to Dox, That Is the Question.* Online: www.researchgate.net/publication/368851607_To_Dox_or_Not_to_Dox_that_is_The_Question

Thornton, Georgina – Willmott, Dominic – Richardson, Emma – Hudspith, Lara (2024): Examining the Immediate and Enduring Psychological Impact of Street Harassment on Women's Mental Health. *Mental Health and Social Inclusion,* 28(5), 734–744. Online: https://doi.org/10.1108/MHSI-07-2023-0080

Tucker, Patrick (2015): War by Doxxing. *Defense One,* 23 March 2015. Online: www.defenseone.com/technology/2015/03/war-doxxing/108238/

U.S. Central Command (2015): Message to Service Members Regarding Online Security. *Facebook,* 2015. Online: www.facebook.com/CENTCOM/posts/10153676790449606/

U.S. Department of Defense (2023): *Strategy for Operations in the Information Environment.* Online: https://govwhitepapers.com/whitepapers/strategy-for-operations-in-the-information-environment

U.S. Department of Homeland Security (2025): Anarchists and Rioters in Portland Illegally Dox ICE Officers and Federal Law Enforcement. *U.S. Department of Homeland Security,* 11 July 2025. Online: www.dhs.gov/news/2025/07/11/anarchists-and-rioters-portland-illegally-dox-ice-officers-and-federal-law

Wang, Yian – Umashankar, Mukhilshankar – Chandrasekharan, Eshwar – Sundaram, Hari (2025): The Chilling: Identifying Strategic Antisocial Behavior Online and Examining the Impact on Journalists. *Proceedings of the ACM on Human-Computer Interaction,* 9(7), 1–67. Online: https://doi.org/10.1145/3757668

Woolley, Samuel C. (2024): Propaganda Digital: El poder de las/los influencers [Digital Propaganda: The Power of Influencers]. *Revista Elecciones,* 23(28), 15–40. Online: https://doi.org/10.53557/Elecciones.2024.v23n28.01

HADMÉRNÖK
VÉDELEMINFORMATIKA
21. évfolyam (2026) 3. szám 43–53.
DOI: 10.32567/hm.2026.3.3

Ferenc Nyizsnyik[1]

Crowdsourcing Intelligence

Abstract

The widespread nature of privately owned smart equipment, such as cellphones, tablets and computers enables the general public to record virtually any event all over the world. These tools are able to provide text, image or video along with accurate time and location data. They can be considered sensors, and the owners can contribute valuable data on events happening in their vicinity. Several countries, most notably Ukraine is already exploiting this potential. According to the popular term of outsourcing a task for the public, it is called crowdsourcing. Crowdsourcing information gathering is an effective supplement to traditional intelligence methods. It is low cost and widely available, providing a large amount of information. This information must be processed and analysed, which is a time-consuming task. Artificial intelligence can help, but it must be used with caution.

Keywords: crowdsourcing, intelligence, CITINT, information, analysis

Introduction

In traditional warfare, intelligence is a key element of the decision-making process. Knowing the situation and activity of the opposing forces is vital information for the commander and mission planners to develop feasible missions. Traditionally, collecting this type of information is a job for the reconnaissance troops. More recently, as advanced sensors appeared on the battlefield, it is done by the Intelligence, Surveillance and Reconnaissance units, widely known as ISR.

The widespread nature of Internet-enabled devices paved the way for yet another possibility of information gathering: people connected to the Internet can contribute based on their skills and opportunities. This distributed work is called crowdsourcing.[2]

The aim of this paper is to get an insight on the potential incorporation of crowdsourced information into the intelligence gathering process and use the obtained information to support military decision-making. Based on the capabilities of the

[1] PhD student, Ludovika University of Public Service, e-mail: nyizsnyik.ferenc@stud.uni-nke.hu
[2] Dobák 2025.

sensors, the information provided meets the criteria for timeliness, accuracy and completeness; however, the employment of these sensors is completely based on the owners' discretion and cannot be tasked as a traditional sensor can.

Based on the sheer number of available sensors, crowdsourcing intelligence seems to be a viable tool for gathering information and assisting the decision-making process. Among others, this paper investigates the advantages and disadvantages of this method, based on researching the available literature and already existing solutions.

Collaborating citizens usually provide information on events they deem important. These events are usually, but not necessarily valuable for the intelligence community and the decision-makers. Information can be abundant in some cases, and at some point, the selection and categorisation of all the reports can be time-consuming. Artificial intelligence (AI) is a possible tool to accelerate this process. However, artificial intelligence has its own limitations at the time of writing this paper. These limitations need to be taken into consideration when employing AI in decision-making.

Theoretical overview

A definition of journalism crowdsourcing can be found in the book authored by Onuoha et al. in 2015 entitled: *Guide to Crowdsourcing*. Although this is about journalism, the definition fits quite well for intelligence collection activities.

"Journalism crowdsourcing is the act of specifically inviting a group of people to participate in a reporting task – such as newsgathering, data collection, or analysis – through a targeted, open call for input; personal experiences; documents; or other contributions."[3]

The Ministry of Digital Transformation of Ukraine issued an application (DIIA[4]) to manage their documentation, pay taxes and interact with public services.[5] "This app was later repurposed to allow Ukrainian citizens to provide real-rime reporting of Russian military troop dispositions, movements, strengths and equipment."[6]

Although reports by citizens include high-resolution photo or video footage complete with timestamps and geo-reference data, these reports still need to be verified by a trained intelligence specialist. This work is still overwhelming for humans, given the huge amount of raw data coming in. However, verification can be crowdsourced again: multiple reports from different citizens may confirm the event. The same process can be used to do Battle Damage Assessment (BDA), confirming the effectiveness of the strike.[7]

Stottlemyre (2015) further defines the nature of crowdsourced intelligence, and a simple way to tell it apart from OSINT[8] and HUMINT.[9] OSINT collectors acquire

[3] Onuoha et al. 2015: 4.
[4] Держава і Я [The State and I].
[5] Digital Citizen [DÁP, Digitális Állampolgár] is a Hungarian website that implements the same functionality (https://dap.gov.hu/).
[6] Burke 2022: 96.
[7] Burke 2022.
[8] Open Source Intelligence.
[9] Human Intelligence.

information "second hand", as the information was not originally provided to support national security objectives. HUMINT collection involves eliciting information by issuing intelligence questions to the collector. Crowdsourced intelligence requires open calls to enlist the community's assistance.

Stottlemyre (2015) also states three requirements that make crowdsourcing intelligence possible: first, an organisation that wishes to solve a problem. Second, that the organisation solicit the participation of a large, likely online, community to solve the problem. And finally, it is required that individual members of the at-large community choose to participate.[10]

The first requirement can be considered fulfilled; the armed forces is an organisation with constant need for information. The second requirement – when applied to dedicated sensors – is equivalent to tasking. In case of the third one, further investigation is necessary, and it always depends on multiple factors of the theatre and the operation.

Intelligence sensors

From the aspect of this paper, sensors can be classified into three main categories: dedicated sensors, operated by specialised units, sensors carried by the soldiers and crowdsourced sensors. All of the above types have their own advantages and disadvantages, complementing each others' functionality.

In case of dedicated sensors and soldier-mounted equipment, tasking is part of the process and willingness to participate is taken for granted. In case of the civilian population, however, cooperation depends on a variety of circumstances, mainly on how the population perceives the military. Even if the perception is positive, a level of trust is also needed, given the high risk of cooperation.

Dedicated sensors

Traditionally, sensors are dedicated platforms of information gathering with specific abilities, such as detection of electro-optical or electromagnetic signals. These platforms are often very expensive and therefore limited in number. They are critical assets, and as such, high value targets of the opposing forces. Their employment must be coordinated and deconflicted in order to avoid targeting the same area, wasting precious sensor time.

According to the Military Decision-Making Process (MDMP), decision points are points in space and time when the commander or staff anticipates making a key decision concerning a specific course of action. These decision points are often associated with a named area of interest (NAI).[11]

[10] Stottlemyre 2015.
[11] Center for Army Lessons Learned 2015.

As NAIs indicate the occurrence of one course of action or the other, they are often observed thoroughly, using dedicated intelligence platforms. This means that these areas are under observation even when no significant event is happening, and also that due to the scarcity of dedicated platforms, key events may happen unnoticed elsewhere and remain unknown to own forces.

Another disadvantage of these platforms is the limited range. More often than not, these are operated from far behind the front line of own troops in order to protect the high value assets. Therefore, they are unable to take advantage of their full range and can only provide information on a certain depth of the area of interest.

Networked soldiers

Modern technology enables manufacturing communication equipment and sensors in portable sizes. Networked soldiers are equipped with these kind of tools, and are integrated into a digital battlefield. They are not only able to discover the opposing forces from a greater distance than before, but are also able to transfer this information to the command post in real time.[12] The advantages are twofold: situational awareness is maintained at the headquarters at all times, providing vital information to the decision-making process, and virtually all the operational area is covered, since soldiers are present throughout.

Although this seems to be a straightforward method of information gathering, there are several disadvantages. The sensors must be small and light in order to allow soldiers to move and fight undisturbed, but it also decreases the capability and range of the sensors. They also must be autonomous, because operating them may distract the soldier, and in a battle situation the consequences of a distraction may be grave.

Crowdsourced intelligence

There are also very capable sensors and communication devices in the hands of most citizens: cell phones, tablets and other smart devices. These, in the hands of collaborating individuals, can be turned into very powerful intelligence platforms able to provide immediate, accurate and original information. This is crowdsourced intelligence gathering.

A recent example is the e-enemy (eVorog) Telegram chatbot, operated by the Ministry of Digital Transformation of Ukraine.[13] This platform enables any Ukrainian citizen to report on Russian military activities. This way information is obtained from all over the theatre, even if it is controlled by the opposing forces, or even from the rear area of the belligerent country.

Dobák (2025) and Burke (2022) investigated the e-enemy chatbot, so their findings are applicable to the Russo–Ukrainian conflict. Application of a similar

[12] Kollár 2017.
[13] Dobák 2025; Burke 2022.

method in different conflicts may show different outcomes. The key is the population's willingness to cooperate with the military. This depends on a variety of factors, and must be taken into consideration not only for the possibility of crowdsourcing, but for the success of the whole operation. A force entering a hostile environment must be entirely self-sustaining. Members of neutral population may be recruited as contractors, mostly in the field of logistics. In order to fully exploit crowdsourcing, a friendly and supportive community is necessary.

There are, however, several disadvantages of this method. First, the background knowledge of the reporters are very diverse. They may misinterpret events or misjudge actions. They may also misrecognise military equipment. It is also possible that they deliberately provide misleading information. This information is therefore not suitable for immediate processing, thorough validation is necessary. As this method is public, the infrastructure and the participants will be targeted by the enemy in many different ways. This activity is called CITINT, i.e. the intelligence activities conducted by citizens and NGOs.[14]

As it was mentioned before, in order to effectively exploit this method, the community must willingly participate. In case of the Russo–Ukrainian conflict, citizens take a chance to actively counter the occupying forces, so their willingness is evident. Expeditionary forces, however, are already in a disadvantageous situation. The local population is indifferent at best; they may as well consider the troops an occupying force. In this case, crowdsourcing works against the organisation.

To turn the tables, the population has to be convinced to cooperate. There are several methods for doing that, for example, psychological operations, but the success is never guaranteed. These activities are out of the scope of this paper.

The properties of the different sensor types are summarised in Table 1. The table shows that every sensor type has its own field of advantage. Dedicated sensors can be used in multiple intelligence disciplines; however, they are limited in numbers, therefore not able to monitor every possibly important event. Networked soldiers and community contributors can only provide information in the IMINT[15] discipline, but they are present in the battlefield and the rear area of the hostile country, respectively. This supports the theory that they augment each other in the information gathering process and employing all three grants leaders the ability to be aware of as many important events as possible.

Table 1: Properties of different sensor types

	Dedicated sensors	**Networked soldiers**	**Community contributions**
Multiple intelligence disciplines	Yes	No	No
Availability in the decisive locations for planning	Limited	No	Yes
Availability in the decisive locations for engagement control	Limited	Yes	No

Source: compiled by the author

[14] Pietilä et al. 2024.
[15] Imagery Intelligence.

Verification of crowdsourced information

The information gathered must be verified for credibility and genuineness. Comparing the report to the actual ground truth is a complex task. It can be done by cross-cueing using different types of sensors. Based on the presence of sensors throughout the battlefield and the rear area, significant events are likely to be reported either by own forces or citizens. These reports can be considered heads-ups and dedicated sensors may be tasked to monitor the situation.

Identifying the source is a good general method for filtering unusable noise or intentional misinformation out. When using crowdsourced information, extra attention is needed in order to determine the average attitude of the population in the theatre, and also the possible presence of malevolent actors. The general public, given enough congruent reports, can self-confirm any information.

Identification

Sensors must be identified in order to prevent injection of false information. In case of dedicated intelligence platforms and soldier-mounted equipment this is already handled by design. In case of citizens, identification may vary on a wide range of possibilities. The simplest way is registering with an e-mail address, which can be created in a matter of minutes, like in the case of OpenStreetMap.[16] Other applications, like the Viber instant messaging service, require a working phone with an active phone number.[17]

Reporting on enemy troops is subject to cyberattacks. The DIIA system was almost immediately targeted by Russian spambots after the ability to report on enemy movements had been added to it. In response, reporting required logging in using valid Ukrainian identity credentials.[18] This measure successfully addressed the spam issue, but identification allowed reports to be connected with the reporters. Should the enemy acquire this information, it can lead to severe retaliation, therefore protection of this database is essential.

Verification of genuineness

The amount of reports coming in from citizens makes it overwhelming for intelligence analysts to process and exploit the information in a timely manner, especially in case of a highly dynamic battlefield. Spam messages can be avoided if strict login is required, but the remaining reports still need to be verified.[19] Mass confirmation is one of the

[16] The sign-up process for contribution to OpenStreetMap requires only a valid e-mail address, a display name and a password (www.openstreetmap.org/user/new).
[17] Viber Terms of Service (www.viber.com/en/terms/viber-terms-use/#account-and-registration).
[18] Burke 2022.
[19] Burke 2022.

possibilities to verify the existence of the reported activity, but it depends on citizens present in the area. In the vicinity of military movements this may not be enough.

As mentioned earlier, dedicated intelligence platforms are traditionally observing named areas of interest. Due to the limited availability of these sensors, key events may go unnoticed while nothing happens in the designated NAI. A feasible option to increase the efficiency of these platforms is using them to verify citizen-reported information. This would allow mission planners to further accelerate the planning process, giving serious advantage over the opposing forces.

On tactical level, this information can be confirmed by drones, if available at the unit. It can provide targeting information to artillery or other fire units, or it can carry out the strike itself.[20] The aim of the information gathering on the operations level may not be direct targeting, but likely confirmation of one of the enemy courses of action.

Threats to crowdsourced intelligence

Credible and genuine information is necessary for the right decision to be made. Information warfare tactics will be employed by the opposing forces to disrupt the decision-making capability of friendly leadership. Even in case of a cooperative population in the area, threats to the information gathering process may arise.

As all intelligence platforms are high value targets to opposing forces, citizens providing reports are no exception. The reporters themselves and the platform providing the functionality are both vulnerable. Citizens contributing information on enemy activity are risking their freedom or even their life.

The information flow can be disrupted using electromagnetic warfare or cyber-attacks. A malicious reporter may provide false information, confusing the targeting and the mission planning process. A legit reporter may also provide false information due to insufficient knowledge and expertise.

Electromagnetic warfare

Citizens are using their own devices, such as cell phones, tablets or personal computers. They usually access the Internet through their Internet Service Provider (ISP) using mobile Internet or Wi-Fi. These services operate on well specified frequencies, so they are easy targets for electromagnetic jamming.

Global positioning systems can also be targeted by jamming or spoofing, providing false location data to the report. One example of GPS-jamming equipment is the Zhitel (RH–330 Zh).[21] The geotags of the information provided by a source suffering GPS-jamming are still valid, therefore it is very hard to filter out or correct these contributions. One clue may be the image not corresponding to the related coordinates.

[20] Burke 2022.
[21] Clark 2022.

This is a fatiguing and time-consuming work for humans; artificial intelligence may be able to spot and handle these anomalies.

The Starlink service provides Internet access for both Ukrainian troops and civilians. It has proven highly resistant to electromagnetic jamming,[22] even if the Krasukha–4 (1RL257) is able to jam low-Earth orbit satellites.[23] "Starlink has a constellation of thousands of satellites that orbit the planet […] at about 550 km, and cover the entire globe."[24] This redundancy makes the service accessible, even if some of its satellites are being jammed.

Cyberattacks

As it was mentioned, the DIIA service was subject to a high level of spam messages by Russian cyber warfare units. The requirement of logging in with valid Ukrainian credentials significantly reduced the amount of spam.

A malicious contributor may provide false information, of which the confirmation uses up valuable resources. In the worst case, the false information ends up being used in the military decision-making process, resulting in a wrong or suboptimal mission plan. This may have severe consequences regarding to the manpower and equipment of the friendly forces.

A contributor lacking the necessary knowledge, even with a good intent, may also provide false information. From the viewpoint of verification and mission planning, this information must be handled the same way. In both cases, identifying false information is very time-consuming for humans. These are usually single-source, unconfirmed reports, usually, but not necessarily contradicting confirmed information. AI may be able to filter these out, but it is up to the leadership to decide whether just drop it, possibly missing a significant event, or use another sensor to confirm, possibly wasting resources.

Processing and analysis

Until recently, intelligence communities were struggling to acquire enough information to support the requirements of the operations. After the exploitation of social media and crowdsourcing intelligence, information became abundant. The communities are now suffering from the overwhelming amount of data, and struggling to select, confirm and prioritise the information in a timely manner.

Tactical level command structures often lack the necessary personnel and equipment to process the large quantity of acquired information. In addition they are often operating from a makeshift command post, which is often relocated in order to avoid being localised and targeted by enemy fires. Also, units on this level focus on short

[22] Burke 2022.
[23] Clark 2022.
[24] Starlink 2026.

term goals, and may skip over details that otherwise could be used to predict larger scale courses of enemy actions.

Operational level structures are more adequate for this kind of work, as their staff includes a dedicated mission planner element and an intelligence section responsible for supporting the planners. However, the amount of information gathered by crowdsourced intelligence may overwhelm even this group of specialists, as they need to systematically review each piece of information and determine their relevance to the mission. This work is time consuming, and a delay in the decision-making is favourable for the opposing forces.

It is tempting to use the crowdsourcing model again – after all, it was invented for the distributed processing of large amount of data. However, the general public lacks the proper training that intelligence personnel go under in order to be able to fulfil their mission. They also lack the databases and historical data available for mission planners. Also, contributors usually work according to their own time schedule, and are not obligated to follow the battle rhythm of the armed forces. As a consequence, crowdsourced analysis can be considered unfeasible.

Using AI for analysis

Artificial intelligence (AI) has gone through a huge development in recent years. Properly trained models are capable of carrying out increasingly difficult tasks. The question naturally arises: Can AI be used for intelligence analysis?

As of the time of writing this paper, using AI is adequate for many different tasks. However, there are issues with AI: they may seem to be omniscient at first, but they cannot substitute human reasoning. They can be used to process large amount of data, but possible risks must be taken into account in order to operate them safely.

According to Probasco et al. (2025), the scope of the model must be thoroughly understood. A model providing excellent results in its own scope may fail when used outside of this scope. Nevertheless, AI will state the results very confidently, even if they are wrong. Humans tend to be biased toward these results, as computers are considered authentic sources. Confirmation bias is also important to be aware of, as humans tend to believe information supporting their own opinions.

AI can be of great help in categorising and organising large amount of data. However, at the time of writing this paper, they should not be used for the automation of decision-making. Critical thinking is required in the process, and AI lacks critical thinking. Human supervision is therefore essential when AI is involved in the decision-making process.[25]

[25] Probasco et al. 2025.

Dissemination

Every soldier at every level needs to be aware of the surrounding situation. One of the aims of intelligence gathering is providing this situation awareness (SA) for all friendly forces. Carrying out missions is only possible if the units involved are in the possession of this SA.

Situation in military operations are dynamic in nature, both in time and space. The most straightforward way to depict and disseminate dynamic information is using a geographic information system (GIS). A GIS can display the situation in real time for everyone with appropriate equipment. This information, should fall in enemy hands, will cause significant disadvantage for own forces. This system therefore must be considered a high value asset, and must be protected accordingly.

In this paper, the focus is not on the dissemination of SA. This topic has been discussed extensively and the problem is addressed in different ways. The methods of dissemination are outside of the scope of this paper, the focus is on information gathering.

Conclusion

Crowdsourcing intelligence is a proven method for information gathering. It is considered to be a new discipline of intelligence by some: CITINT.[26] It requires little financial investment as the necessary equipment is owned by the contributors. Contributors – given their willingness to cooperate – are present and provide information virtually everywhere, resulting in a multitude of sensors available for the intelligence community.

As a result, traditional sensors can be used for confirmation of events instead of wasting these platforms for continuous observation of NAIs. The sensors becoming available can be retasked for time sensitive operations.

Every intelligence system is a high value target of the opposing forces, crowdsourced intelligence being no exception. The bottleneck of the system is the underlying communication and information infrastructure, so most likely this will be targeted by different ways in order to suppress or destroy this gathering method.

Processing the overwhelming amount of data requires time. Intelligence specialists are under constant time pressure to provide timely support for mission planning. This contradiction can be resolved by utilising artificial intelligence. However, AI has its own drawbacks, so human supervision cannot be avoided.

This paper investigated the feasibility of crowdsourced intelligence among traditional methods and the inclusion of the information obtained this way into the military decision-making process. The final finding is that crowdsourced intelligence is a valuable asset in the hands of modern armed forces. It can be considered a relatively low-cost force multiplier, and employed together with traditional sensors and networked soldiers greatly enhances the decision-makers' situation awareness.

[26] Pietilä et al. 2024.

References

Burke, Paul (2022): The Issues in the Collection, Verification and Actionability of Citizen-Derived and Crowdsourced Intelligence during the Russian Invasion of Ukraine, 2022. *Strategic Panorama,* (Special Issue), 94–103. Online: https://doi.org/10.53679/2616-9460.specialissue.2022.09

Center for Army Lessons Learned (2015): *MDMP Handbook.* Center for Army Lessons Learned. Online: https://apps.dtic.mil/sti/pdfs/AD1018227.pdf

Clark, Bryan (2022): The Fall and Rise of Russian Electronic Warfare: The Ukraine Invasion Has Become an Old-fashioned Slog, Enabling Russia to Unleash Its Electronic Weapons. *IEEE Spectrum,* 30 July 2022. Online: https://spectrum.ieee.org/the-fall-and-rise-of-russian-electronic-warfare

Dobák, Imre (2025): Crowdsourcing for Security in the Age of Hybrid Threats. *Security and Defence Quarterly,* 49(1), 98–111. Online: https://doi.org/10.35467/sdq/197309

Kollár, Csaba (2017): Az IoT katonai felhasználási lehetőségei és a fejlesztés irányai. *Hadmérnök,* 12(4), 146–158. Online: http://hadmernok.hu/174_15_kollar.pdf

Onuoha, Mimi – Pinder, Jeanne – Schaffer, Jan (2015): *Guide to Crowdsourcing.* Columbia Journalism School. Online: https://data.journalism.columbia.edu/sites/data.journalism.columbia.edu/files/content/guide-to-crowdsourcing.pdf

Pietilä, Iikka – Kortesuo, Katleena – Pohjanen, Ulla – Tuominen, Mikko (2024): Shift in Intelligence Issue Ownership: Conceptualizing CITINT – Intelligence Conducted by Citizens. *Frontiers in Political Science,* 6. Online: https://doi.org/10.3389/fpos.2024.1379789

Probasco, Emelia – Toner, Helen – Burtell, Matthew – Rudner, Tim G. J. (2025): AI for Military Decision-Making. Harnessing the Advantages and Avoiding the Risks. *Center for Security and Emerging Technology,* April 2025. Online: https://doi.org/10.51593/20240028

Starlink (2026): *Satellite Technology.* Online: https://starlink.com/hu/technology

Stottlemyre, Steven A. (2015): HUMINT, OSINT, or Something New? Defining Crowdsourced Intelligence. *International Journal of Intelligence and Counterintelligence,* 28(3), 578–589. Online: https://doi.org/10.1080/08850607.2015.992760

HADMÉRNÖK
VÉDELEMINFORMATIKA

21. évfolyam (2026) 3. szám 55–74.
DOI: 10.32567/hm.2026.3.4

Pozderka Gábor[1]

Kibertől az MI-ig: A mesterséges intelligencia az új kiber?

From Cyber to AI: Is Artificial Intelligence the New Cyber?

Absztrakt

A tanulmány a mesterséges intelligencia (MI) társadalmi és szervezeti hatásait vizsgálja, különös tekintettel arra a kérdésre, hogy az MI válhat-e az „új kiberszereplővé" a döntéshozatalban és a tudás elosztásában. A tanulmány rámutat arra, hogy az MI jelentősen átalakítja a hatalmi viszonyokat, gyorsítja a döntéshozatali folyamatokat, ugyanakkor kiemelt figyelmet igényel az etikai normák betartása és az ember-gép együttműködés fenntartható kialakítása, valamint gyakorlati javaslatokat is tartalmaz a szervezetek számára, többek között az átláthatóság biztosítását, a kritikai kompetenciák fejlesztését, a felelősségkeretek tisztázását, a kockázatkezelést és a hosszú távú stratégiai tervezést. Az eredmények hozzájárulnak a felelős és fenntartható MI-integráció megértéséhez és iránymutatást nyújtanak a társadalmi és szervezeti döntéshozók számára, amelynek szerves része a katonai szektor is.

Kulcsszavak: mesterséges intelligencia, kibertér, kognitív, technológia

Abstract

The study examines the social and organisational impacts of artificial intelligence (AI), with a particular focus on whether AI could become a new "cyber actor" in decision making and knowledge distribution. It highlights that AI significantly reshapes power dynamics and accelerates decision-making processes, while also requiring increased

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

attention to ethical standards and the sustainable development of human–machine collaboration. The study also provides practical recommendations for organisations, including ensuring transparency, developing critical competencies, clarifying responsibility frameworks, managing risks, and engaging in long-term strategic planning. The findings contribute to advancing the understanding of responsible and sustainable AI integration and provide guidance for societal and organisational decision makers, including those in the military sector.

Keywords: artificial intelligence, cyber domain, cognitive, technology

Bevezetés

Jelen tanulmány azt a hipotézist vizsgálja részletesen, amelyet alaptézisként több szakmai konferencia előadója is megfogalmazott, leginkább kérdés formájában, azonban valódi választ nem sikerült találni rá. Feltevésem az, hogy amikor egy új technológiai jelenség megjelenik, akkor az első reakciónk ritkán az, hogy önmagában próbáljuk megérteni, ehelyett ösztönösen hasonlítunk. Jellemzően analógiákat keresünk, korábbi tapasztalatokhoz nyúlunk vissza, és olyan fogalmakat hívunk segítségül, amelyek már „átmentek a tűzön", társadalmi és szakterületi elfogadottsággal rendelkeznek. Ebben az értelemben az a kijelentés, hogy egy új technológia – esetünkben a mesterséges intelligencia – „az új kiber", nem annyira technikai állítás, mint inkább pszichológiai és kulturális reflex. A hasonlat mögött mindig ott húzódik egy hallgatólagos ígéret, amely szerint az ismeretlen nem teljesen ismeretlen, már voltunk hasonló helyzetben, és végül akkor is kialakult valamilyen egyensúly. A kiber ebben a mondatban nem konkrét rendszereket, hálózatokat vagy protokollokat jelöl, hanem egy kollektív emléket. Egy korszakot, amikor a digitális technológia hirtelen mindent uralni kezdett, bizonytalanságot keltett, majd lassan beépült a hétköznapokba. Ahhoz azonban, hogy megértsük, mit ér ez az analógia, előbb azt kell tisztáznunk, mit is jelentett valójában a kiber, mielőtt közhellyé vált.

A kiber szó eredete messzebbre nyúlik vissza annál, mint ahogyan jelenleg használjuk. A kibernetika eredetileg nem digitális technológiát jelentett, hanem a szabályozás és irányítás általános elméletét, olyan rendszerek működését vizsgálta, amelyek képesek visszacsatolás alapján módosítani saját viselkedésüket, megalkotása Norbert Wiener nevéhez kötődik. Ebben az értelemben egy termosztát, egy élő szervezet és egy automatizált gép ugyanabba az elméleti keretbe tartozott. Ez az eredeti jelentés mára szinte teljesen eltűnt; amikor ma kiberről beszélünk, ritkán gondolunk szabályozáselméletre vagy visszacsatolásra. A szó jelentése fokozatosan átalakult, ahogy a számítógépek és hálózatok egyre nagyobb szerepet kaptak a társadalomban. A hangsúly eltolódott a rendszerelméleti gondolkodásról a digitális infrastruktúrára. A fogalom alkalmazkodott egy új technológiai valósághoz, és egy ideig viszonylag pontosan jelölte azt a közeget, amelyben a számítógépes kommunikáció zajlott. A kiber ekkor még nem volt metafora, inkább leírásként azonosítható. A technológiai fejlődés jelenlegi szakaszában hasonló értelmezési kísérlet figyelhető meg a mesterséges intelligencia esetében is. Az „MI az új kiber" megfogalmazás egyszerre utal a technológia várható társadalmi jelentőségére, valamint arra a feltételezésre, hogy

a korábbi digitális átalakulások tapasztalatai segítséget nyújthatnak az új jelenség megértésében. A tanulmány központi kutatási kérdése ezért az, hogy a mesterséges intelligencia értelmezhető-e a korábban kialakult kiberfogalom analógiájaként, illetve indokolt-e annak „új kiberként" történő meghatározása.

A tanulmány alapvető állítása, hogy bár a két jelenség között több strukturális hasonlóság azonosítható, az analógia csak korlátozottan alkalmazható. Míg a kiber elsősorban infrastruktúrát és technológiai környezetet jelölt, addig a mesterséges intelligencia egyre inkább kognitív közreműködőként jelenik meg a döntéshozatali, tudáselosztási és értelmezési folyamatokban. Ez a különbség a társadalmi hatások, a bizalom, a felelősség és a hatalom szerkezetének szempontjából minőségi eltérést eredményez, ezért az MI nem tekinthető egyszerűen a kiber következő fejlődési szakaszának. A tanulmány újszerű elemként a mesterséges intelligencia katonai alkalmazhatóságát nem kizárólag technológiai, hanem hadműveleti, döntéstámogatási szempontból is vizsgálja, kitérve annak kockázatára.

Kutatási módszertan

A tanulmány kvalitatív kutatási megközelítést alkalmaz annak vizsgálatára, hogy a mesterséges intelligencia milyen mértékben értelmezhető a korábban kialakult kiberfogalom analógiájaként, illetve milyen pontokon mutat olyan sajátosságokat, amelyek indokolttá teszik önálló társadalmi és szervezeti jelenségként történő kezelését. A kutatás központi kérdése az, hogy a mesterséges intelligencia által betöltött kognitív és döntéstámogató funkciók mennyiben jelentenek folytonosságot a kibertérhez kapcsolódó technológiai fejlődésben, illetve mennyiben képviselnek minőségi változást.

A kutatás két egymást kiegészítő módszertani elemre épül: szakirodalmi elemzésre és esettanulmány-alapú vizsgálatra. A szakirodalmi feldolgozás célja a kibernetika, a kibertér és a mesterséges intelligencia társadalmi szerepével kapcsolatos meghatározó megközelítések áttekintése és összevetése. Az elemzés során kiemelt figyelmet kaptak azok a munkák, amelyek a technológia és a döntéshozatal kapcsolatát, a bizalom kérdését, a tudáselosztás átalakulását, valamint az ember-technológia együttműködés különböző formáit vizsgálják. A szakirodalmi feldolgozás célja nem kizárólag az egyes szerzői álláspontok bemutatása, hanem azok összekapcsolása és értelmezése a kutatási kérdés szempontjából.

A szakirodalmi elemzést egy konkrét esettanulmány egészíti ki. A tanulmány a Project Maven programot olyan példaként vizsgálja, amely jól szemlélteti a mesterséges intelligencia szerepének változását a hagyományos informatikai támogatástól a döntéstámogató funkciók irányába. Az eset kiválasztását az indokolja, hogy a rendszer működése során a mesterséges intelligencia nem pusztán adatfeldolgozási és információkezelési feladatokat lát el, hanem közvetlenül támogatja az emberi döntéshozatalt és értelmezési folyamatokat. Az esettanulmány lehetőséget biztosít annak bemutatására, hogy a technológia miként jelenik meg egyre inkább kognitív közreműködőként, és ez milyen szervezeti, etikai és felelősségi kérdéseket vet fel.

Az elemzés három fő vizsgálati dimenzió mentén történik. Az első dimenzió az infrastruktúra és a kognitív képességek közötti különbségeket vizsgálja annak

érdekében, hogy meghatározható legyen, mennyiben tekinthető a mesterséges intelligencia a korábbi digitális technológiák folytatásának. A második a bizalom, az autoritás, valamint a tudás és a hatalom szerkezetének átalakulására fókuszál. A harmadik dimenzió az etikai, szabályozási és fenntarthatósági következményeket elemzi, különös figyelmet fordítva az átláthatóság, a felelősség és a hosszú távú ember-technológia együttműködés kérdéseire.

A kutatás célja nem a mesterséges intelligencia technikai teljesítményének értékelése, hanem annak feltárása, hogy a technológia milyen módon alakítja át a döntéshozatal, a tudáselosztás és a társadalmi felelősség hagyományos kereteit. Az elemzés eredményei alapján lehetőség nyílik annak értékelésére, hogy az „MI az új kiber" állítás milyen mértékben tekinthető megalapozottnak, illetve mely területeken válik elégtelenné a jelenség leírására, hogyan mutat azon túl.

Kezdeti lépések, alapvetés

A *cyberspace* szót a *cybernetics* (kibernetika) és a *space* (tér) szavak összevonásával William Gibson sci-fi-szerző alkotta meg 1982-ben megjelent *Burning Chrome* című novellájában, majd ezt követően felhasználta az 1984-es *Neurománc* című cyberpunk[2] regényében is. Gibsontól származik a *meatspace* (hús-tér) kifejezés is, amelyet a kibertér ellentéteként használ a fizikai világ jelölésére. Gibson novellájában a kiberteret egy „akarattól független hallucináció"-ként határozta meg, amelyet a felhasználók érzékelnek. A kilencvenes években a kiber egyre inkább térként jelent meg a gondolkodásban. A kibertér ekkor nem csupán technikai hálózatként, hanem egy újfajta társadalmi közegként jelent meg, ahol identitások, közösségek és gazdasági viszonyok alakultak ki. A digitális jelenlét elválaszthatóvá vált a fizikai testtől, és ez erős kulturális képzeletet mozgósított. Ebben az időszakban a kiber jelentése kifejezetten optimista felhangot kapott. A hálózat decentralizáltsága, az információ szabad áramlása és az alacsony belépési szint sokak számára a hagyományos hatalmi struktúrák fellazulásának ígéretét hordozta magában. A digitális tér egy ideig valóban jelentős alternatívának tűnt, amelyben új lehetőségek kapui nyílhatnak meg mindenki számára, újra értelmezhetők a korábban megalkotott szabályok. Ez az optimizmus és szabadságvágy törékenynek bizonyult; ahogy a digitális infrastruktúra egyre inkább a gazdaság, az állam és a mindennapi élet alaprétegévé vált, úgy változott meg a róla alkotott narratíva is.

A kiberfogalom jelentésének egyik legfontosabb fordulópontjaként azonosítható az az időszak, amikor a digitális tér biztonságpolitikai kérdéssé vált.[3] A hálózatok sebezhetősége, az adatlopások, a szolgáltatáskimaradások és az államközi konfliktusok új dimenziói mind hozzájárultak ahhoz, hogy a kiber egyre inkább a fenyegetés nyelvévé váljon. Ettől a ponttól kezdve a kiber már nem elsősorban lehetőséget, hanem kockázatot jelentett, a digitális tér láthatatlan, nehezen lokalizálható és nehezen

[2] A *cyberpunk* a kortárs tömegkultúra egyik népszerű stílusa, sok alkotásban előforduló világnézet, jellemzően a fejlett technológia és a lecsúszott társadalom találkozását mutatja be, az emberek általában óriási, túlzsúfolt metropoliszokban élnek, érzelmi életük ennek megfelelően sivár. Gibson 2004.

[3] Kovács 2020.

ellenőrizhetővé vált. Pontosan ezek a tulajdonságok tették alkalmassá arra, hogy stratégiai narratívák központi elemévé váljon. Fontosnak tartom hangsúlyozni, hogy ez nem csupán technológiai változás volt, ugyanazok a rendszerek, amelyek korábban az innováció és a szabadság szimbólumai voltak, hirtelen a sebezhetőség és a kiszolgáltatottság jelképeivé váltak. Ezen a ponton a kiber már nem pusztán leíró fogalomként működött, metaforává vagy más megfogalmazásban gyűjtőfogalommá vált, amely egyszerre sűrített össze technikai komplexitást és érzelmi tartalmat. Nem volt szükség arra, hogy pontosan értsük, mi történik egy digitális rendszerben ahhoz, hogy a kiberfenyegetés kifejezés hatásosan írja le az érzelmi állapotot. A fogalom egyre tágult, miközben fókusza egyre csökkent, minél több mindent jelentett, annál kevésbé volt alkalmas arra, hogy pontosan elhatárolható legyen. Logikai ellentmondásnak tűnik, azonban éppen ez a homályosság tette igazán hasznossá, aminek hatására a kiber olyan szóvá vált, amely mögé nagyon különböző érdekek, félelmek és célok sorakozhattak fel anélkül, hogy egymással közvetlenül ütköztek volna.

A kiber története jól példázza, hogyan működnek a technológiai kulcsszavak, megfogalmazások a közbeszédben. Egy fogalom kezdetben szűk, szakmai jelentéssel bír, majd fokozatosan kilép ebből a keretből. Ahogy egyre több terület kezdi használni, úgy válik egyre rugalmasabbá, végül pedig elkerülhetetlenül elmosódnak a határai. Egy fogalom akkor válik igazán elterjedtté, amikor már nem igényel részletes magyarázatot, amikor elegendő annyit mondani, hogy kiber, és mindenki tudja, miről van szó – még akkor is, ha senki sem ugyanarra gondol pontosan. Ebben az értelemben a kiber nem kudarcot vallott, hanem maximálisan betöltötte a funkcióját, közös nyelvet adott egy rendkívül összetett technológiai átalakuláshoz. Amikor ma egy új technológiát a kiberhez hasonlítunk, nem véletlenül tesszük azt. A kiber kollektív emlékezete magában foglalja az áttörés, a zavar, a félelem és a normalizálódás tapasztalatát. Ez ideális referenciapont egy olyan jelenség esetében, amely egyszerre ígér radikális változást és hordoz bizonytalanságot magában. Ez a hasonlat azt sugallja, hogy bár most még nehéz eligazodni, de idővel kialakulnak a szabályok, intézményi keretek és normák. Ez egy igazán megnyugtató narratíva, különösen akkor, amikor a technológiai változás gyorsabbnak tűnik, mint a társadalmi alkalmazkodás képessége. Határozottan kijelenthető, hogy a kiber soha nem kérdőjelezte meg közvetlenül azt, hogy ki gondolkodik, ki dönt és ki értelmez, a digitális infrastruktúra kizárólagosan eszköz volt, még ha rendkívül összetett is. Az analógia akkor kezd problematikussá válni, amikor egy új technológia nem pusztán eszközként, hanem aktív közreműködőként jelenik meg a gondolkodás és a döntéshozatal folyamataiban. A kiber technikai fogalomból mindent átfogó metaforává vált,[4] és belátható, hogy csábító ezt a mintát újra felhasználni. Érdemes a továbbiakban megvizsgálni, hogy hol válnak ezek az analógiák elégtelenné, és mi történik akkor, amikor a technológia nem pusztán infrastruktúrát, hanem értelmező és döntéstámogató képességet hoz magával.

A tanulmány kutatási módszere elsősorban kvalitatív megközelítésen alapul, az elemzés során esettanulmányokat és szakirodalmi áttekintést alkalmazok, hogy feltárjam, miként változik a döntéshozatal, a tudás és a hatalom szerkezete a technológia szereplővé válásának folyamatában. A kutatási irányok elsősorban három

[4] 2024. évi LXIX. törvény.

területre koncentrálnak: az ember-technológia együttműködés dinamikájára, az etikai és társadalmi normák átalakulására, valamint a hosszú távú fenntarthatóság és adaptáció feltételeire. E módszertan lehetővé teszi, hogy ne csupán a technológia technikai képességeit vizsgáljuk, hanem annak társadalmi, kulturális és etikai összefüggéseit is,[5] így a tanulmány komplex képet nyújt a jövőbeli kihívásokról és lehetőségekről.

Infrastruktúra és képesség: mi változik meg, amikor a technológia „gondolkodni" kezd?

Annak igazolásához, hogy az MI nem tekinthető egyszerűen a kiber következő generációjának, először meg kell vizsgálni, milyen funkcionális különbség van a digitális infrastruktúrák és a kognitív képességeket utánzó rendszerek között. A fentiekben azt láttuk, hogy a kiber miként vált technológiai fogalomból mindent lefedő metaforává. Ez a történet megmagyarázza, miért csábító egy új technológiai jelenséget ugyanebbe a keretbe helyezni ismét. A hasonlat azonban csak addig működik, amíg az összehasonlított dolgok valóban azonos természetűek. A problémák ott kezdődnek, ahol ez a feltételezés már nem áll meg. A kiber mindig olyan infrastruktúrát jelölt, amely lehetővé tette a kommunikációt, az adatkezelést és az automatizációt, de nem lépett be közvetlenül az emberi értelmezés és döntéshozatal terébe. Még akkor sem történt ez meg, amikor a digitális rendszerek rendkívül összetetté váltak, alapvetően továbbra is végrehajtó szerepben maradtak, a kérdés mindig az volt, hogy az ember mit akar tőlük és nem fordítva. Ezzel szemben egy új típusú technológia megjelenésekor már nem kizárólag eszközökről beszélünk, hanem olyan rendszerekről, amelyek a gondolkodás bizonyos funkcióit imitálják vagy helyettesítik, ez a különbség nem fokozati, hanem minőségi változást hordoz magában. Nem arról van szó, hogy gyorsabbak vagy hatékonyabbak lettek az eszközeink, hanem arról, hogy más szerepet töltenek be.

Az infrastruktúra egyik legfontosabb tulajdonsága, hogy ideális esetben „láthatatlan": akkor működik jól, ha evidenciaként kezeljük a meglétét. A villamosenergia-hálózat, a vízi közmű vagy az internet mind ilyenek, jelen vannak és nélkülözhetetlenek, de nem vesznek részt aktívan a döntéseinkben. A kiber besorolhatóvá vált ezekbe kategóriákba; akkor is infrastruktúra maradt, amikor kritikus jelentőségűvé vált, még a biztonság vonatkozásában is rendszerek védelméről beszéltünk, nem pedig értelmező folyamatokról. Egy sikeres kibertámadás adatokat lopott, rendszereket bénított meg, vagy hozzáférést szerzett, de nem adott tanácsot, nem érvelt, nem alkotott alternatívákat. Ennek a passzív jellegnek az azonosítása és elfogadása fontos, mivel az infrastruktúra mindig valami mást szolgál, funkciója van és nem célja, akkor is, amikor rendkívül komplexszé válik, alárendelt szerepben marad az emberi szándéknak. Az a technológiai váltás, amellyel most szembesülünk, ott válik igazán érdekessé és az emberi elme számára riasztóvá, hogy ez a háttérszerep megbomlik. Egyre több olyan rendszer jelenik meg, amely nem pusztán végrehajt, hanem javasol, értelmez és összefüggéseket tár fel, a felhasználó nem utasításokat ad, hanem kérdez,

[5] Csepeli 2020.

a válasz pedig nem egy előre definiált kimenet, hanem kontextusfüggő értelmezés. Ez a váltás alapjaiban változtatja meg az ember és technológia viszonyát, a hangsúly áttevődik az irányításról az együttműködésre. Már nem az a kérdés, hogy a rendszer pontosan azt teszi-e, amit előírtunk neki, hanem az, hogy mennyire bízhatunk meg az általa adott válaszban, ez a bizalom nem technikai értelemben vett megbízhatóság, hanem kognitív bizalom. A most megfogalmazott kérdés már arról szól, hogy elfogadjuk-e egy rendszer értelmezését, érvelését vagy ajánlását, korábban ez a kérdés a kiber esetében soha nem merült fel ilyen formában.

Fontos különbséget tenni automatizmus és értelmezés között. Az automatizmus előre meghatározott szabályok alapján működik, még akkor is, ha ezek a szabályok rendkívül bonyolultak. Egy ilyen rendszer megbízhatósága mérhető, tesztelhető és formalizálható. Az értelmezés ezzel szemben mindig kontextusfüggő, nem pusztán szabályok alkalmazását jelenti, hanem jelentések közötti navigációt. Amikor egy technológiai rendszer ilyen funkciókat lát el, akkor már nem egyszerűen végrehajt, hanem közvetít a világ és az ember között. Ez a közvetítő szerep az, ami radikálisan megkülönbözteti az új technológiai helyzetet a korábbi kiberkorszak tapasztalataitól. Az infrastruktúra nem mondja meg, mit gondoljunk, egy értelmező rendszer viszont igen. Gyakran hangzik el megnyugtatásként, hogy ezek az új rendszerek „csak eszközök" – ez a kijelentés technikailag részben igaz, de társadalmi értelemben félrevezető. Egy kalapács vagy egy adatbázis valóban csak eszköz, nem formálja aktívan a gondolkodásunkat, legfeljebb lehetővé tesz bizonyos cselekvéseket. Egy olyan rendszer viszont, amely értelmez, összefoglal és javaslatot tesz, már részt vesz a kognitív folyamatban. Még akkor is, ha nincs tudata, szándéka vagy önálló célja, funkcionálisan betölti azt a szerepet, amelyet korábban emberek töltöttek be. Ez nem jelenti azt, hogy a rendszer „emberré válik", de azt igen, hogy az emberi gondolkodás ökoszisztémájának részese lesz.

Ahhoz, hogy ezt a változást pontosabban megértsük és vizsgálni tudjuk, érdemes megkülönböztetni a technikai és a kognitív infrastruktúrát. A technikai infrastruktúra a fizikai és digitális alapokat jelenti, amelyek lehetővé teszik a működést, a kognitív infrastruktúra ezzel szemben azokat az eszközöket és rendszereket foglalja magában, amelyek meghatározzák, hogyan értelmezünk információkat, hogyan hozunk döntéseket, és hogyan alkotunk jelentéseket. A könyvek, az írás, a nyomtatás és az oktatási intézmények mind ilyen kognitív infrastruktúrának tekinthetők.[6] Nem semlegesek, hanem strukturálják a gondolkodást, kiemelnek bizonyos formákat, háttérbe szorítanak másokat. Az új technológiai rendszerek ebbe a kategóriába illeszkednek, nem csupán adatot szolgáltatnak, hanem keretezik az értelmezést. Ez a szerep korábban mindig lassan, generációkon át alakult ki, most viszont rendkívüli sebességgel történik meg. A technológiai változások egyik leginkább alábecsült alkotóeleme a sebesség. Nemcsak arról van szó, hogy valami gyorsabban történik, hanem arról, hogy a gyorsaság önmagában minőségi különbséget hoz létre. Egy olyan kognitív infrastruktúra, amely pillanatok alatt válaszol, skálázható és mindig elérhető, egészen más hatást vált ki, mint egy lassan formálódó rendszer. A kiberkorszakban a sebesség főként az adatátvitelre és a feldolgozásra vonatkozott, jelenleg a sebesség az értelmezésre

[6] Berendt–Littlejohn–Blakemore 2020.

és a döntéstámogatásra is kiterjed. Ez azt jelenti, hogy a gondolkodás ritmusa maga is átalakul, ez az átalakulás pedig nem technikai részletkérdés, hanem kulturális változás. Meghatározza, mit tekintünk alapos mérlegelésnek, mit tartunk elfogadható válasznak, és hogyan viszonyulunk a bizonytalansághoz vagy maradvány kockázatokhoz. Az infrastruktúra egyik előnye az volt, hogy nem jelentett problémát annak semlegesnek tekintése, egy hálózat adatot továbbít, egy szerver kiszolgál és nem hat a kognitív tudatra. Egy értelmező rendszer esetében azonban az objektivitás illúziója sokkal veszélyesebb, mert amikor egy rendszer koherens, magabiztos válaszokat ad, könnyű elfelejteni, hogy ezek mögött választások, súlyozások és előfeltevések állnak. Ezek a választások nem feltétlenül rosszindulatúak, de sosem semlegesek. Ez a felismerés új típusú kritikai gondolkodást igényel, nem elég megérteni, hogyan működik egy rendszer technikailag, azt is érteni kell, hogyan strukturálja az összegzett adatokat.

Amikor a technológia „megszólal": szereplők, autoritás és bizalom

Ha az MI valóban túlmutat az infrastruktúra szerepén, akkor meg kell vizsgálni, hogyan változtatja meg az ember és technológia közötti bizalmi viszonyokat. A technológiák többsége hallgat, bár jelez, villog, sípol, de nem beszél, a felhasználó parancsokat ad, adatokat kap vissza, és a kettő közötti kapcsolat alapvetően ezen a szinten marad. Ez a hallgatás hosszú ideig természetesnek tűnt, és észrevétlenül meghatározta az ember-gép viszonyt, ez egyfajta biztonságérzetet is nyújtott az emberi tudat részére, nem kérdőjelezte meg felsőbbrendűségét, inkább pszichésen támogatta azt. Ez az idealista helyzet ott változik meg radikálisan, amikor a technológia megszólal, nem pusztán értesít, hanem válaszol, nem állapotot jelez, hanem állítást fogalmaz meg. A nyelvhasználat itt nem felszíni jelenség, hanem minőségi fordulópont, a nyelv ugyanis nem csupán információátadásra szolgál, hanem jelentést, szándékot és szakértelmet is közvetít. Amikor egy rendszer nyelvi formában lép kapcsolatba velünk, automatikusan más kategóriába kezdjük besorolni, nem infrastruktúraként érzékeljük, hanem interakciós partnerként. Ez a besorolás nagyrészt tudattalan, mégis rendkívül erős hatással van arra, hogyan viszonyulunk a technológiához. Az emberi elme hajlamos szereplőket látni ott is, ahol valójában csak folyamatok vannak, ez evolúciós örökség, amelynek alapja, hogy jobb volt tévesen szándékot feltételezni, mint elmulasztani egy valódi veszély felismerését. Ez a kialakult folyamat azonban nem kapcsol ki a modern technológiákkal szemben sem; amikor egy rendszer koherens mondatokban válaszol, érvel, sőt reflektál, az emberi agy automatikusan aktiválja azokat a sémákat, amelyeket más emberekkel való kommunikáció során használ. A hangsúly nem azon van, hogy a rendszer „valójában" ért-e, hanem azon, hogy a kommunikáció formája ezt sugallja. Figyeljük csak meg, hogyan kommunikálunk akaratlanul is a különböző MI-t használó alkalmazásokkal, ugyanazon interakciókat vetítjük át ösztönösen, amivel a mindennapi életben is kommunikálunk. Ez a megszemélyesítés nem naivitás, hanem kognitív reflex, akkor is működik, ha tudjuk, hogy egy algoritmussal van dolgunk. A tudás és az élmény itt gyakran szétválik, bár racionálisan tisztában vagyunk a technológia természetével, érzelmileg mégis másként reagálunk.

A nyelv nemcsak kapcsolatot teremt, hanem tekintélyt is közvetít. A magabiztos, strukturált és gördülékeny megszólalás az emberi kultúrában hagyományosan a kompetencia jele; aki jól és határozottan beszél, arról hajlamosak vagyunk feltételezni, hogy tudja, miről beszél. Ez a hatás különösen erős akkor, amikor egy rendszer gyorsan és következetesen válaszol, a válaszok ritmusa, formája és felépítése könnyen az objektivitás látszatát kelti. A felhasználó nem azt érzékeli, hogy egy statisztikai folyamat eredményét látja, hanem azt, hogy „valaki" megmondja, mi a valós helyzet. Senki nem mondja ki, hogy a rendszernek igaza van, mégis hajlamosak vagyunk annak tekinteni, ami különösen igaz olyan helyzetekben, ahol az ember maga bizonytalan, információhiányos vagy időnyomás alatt áll. A fenti szituáció fokozottan előkerülhet a katonai szakterület vonatkozásában, a mesterséges intelligencia már most is jelentős szerepet játszik a katonai műveletek tervezésében és végrehajtásában, ez a tendencia a jövőben tovább fog erősödni, mivel az MI képes hatalmas mennyiségű adatot gyorsan feldolgozni, például műholdképeket, hírszerzési jelentéseket és szenzoradatokat, a tervezési fázisban pedig segít az optimális stratégiák kidolgozásában különböző forgatókönyvek szimulálásával.[7] Az MI-modellek előre jelzik az ellenség várható lépéseit múltbeli minták és aktuális információk alapján, ezáltal a parancsnokok megalapozottabb döntéseket hozhatnak. A logisztikai tervezésben az MI optimalizálja az utánpótlási útvonalakat és erőforrás-elosztást, a valós idejű adatelemzés lehetővé teszi a gyors reagálást a változó harctéri helyzetekre, ez a digitalizációnak is az egyik alapfeltétele.[8] Az MI támogatja a célpontok azonosítását és priorizálását is, a végrehajtás során az autonóm rendszerek, például a drónok, képesek önállóan feladatokat végrehajtani. A kibervédelemben automatikusan felismeri és elhárítja a támadásokat, az MI-alapú döntéstámogató rendszerek folyamatos visszacsatolást adnak a műveletek során. Összességében a mesterséges intelligencia növeli a műveletek sebességét, pontosságát és hatékonyságát, miközben komoly etikai és biztonsági kérdéseket vet fel.[9]

Katonai rendszerekben történő megjelenés

A korábban elemzett folyamatok logikus következményeként a katonai alkalmazásban történő MI-használat elkerülhetetlen, de számos kockázatot hordoz magában. Mindenképpen kezelni szükséges a kialakult helyzetet annak érdekében, hogy a rendszerek alkalmazhatósága ne sérüljön. Szinte minden nemzet azonosította ezt a kihívást, a megoldást különböző formában képzelik el, számtalan esetben a nemzeti szuverenitás kérdéskörét előtérbe helyezve. A katonai alkalmazásban történő megjelenés iránymutató példája a már említett Project Maven, amely az Egyesült Államok egyik első olyan katonai kezdeményezése, amelyben MI-t alkalmaznak hadműveleti támogatásra. A program elsődleges célja, hogy a drónok által rögzített videófelvételeket automatikusan elemezze, ennek megfelelően a rendszer képes legyen felismerni különböző objektumokat, például járműveket és embereket is.

[7] Ertan et al. 2020.
[8] Weiss 2020.
[9] *Recommendation on the Ethics of Artificial Intelligence* 2021.

Ez jelentősen csökkentette az emberi elemzők terhelését, valamint az MI használata felgyorsította az információfeldolgozást, továbbá a technológia különösen hasznos volt a nagy mennyiségű adat feldolgozásában. A program ugyanakkor etikai kérdéseket is felvetett, több szakértő aggodalmát fejezte ki az automatizált megfigyelés következményei miatt, ezekről az etikai kérdésekről publikációmban később részletesen írok majd. Az etikai kérdések ellenére a projektet nem állították le, Steve Feinberg (az USA védelmiminiszter-helyettese) 2026. március 9-én a Pentagon vezetőinek és katonai parancsnokainak küldött tájékoztatásában megerősítette, hogy az amerikai Hadügyminisztérium (a Pentagon) döntése értelmében a Palantir Technologies által fejlesztett, Project Maven néven ismert harctéri mesterséges intelligenciát használó alkalmazást tartósan bevezetik a hadsereg egészében, a későbbiek során pedig már nem ideiglenes projektként határozzák meg.[10] Ez a döntés jelentősen befolyásolja a NATO jövőbeni képességfejlesztési irányait is, hiszen a harctéri kompatibilitás kérdésköre a szövetség előtt álló egyik legjelentősebb és folyamatosan jelentkező kihívás, továbbá precedenst is teremt az MI harctéri körülmények közötti alkalmazásával kapcsolatosan. Bár a NATO-n belül továbbra sem egységes a Maven projekt megítélése, a Supreme Headquarters Allied Powers Europe (SHAPE) mint a NATO stratégiai műveleti vezetési eleme aktívan bekapcsolódott a képesség tesztelésébe,[11] az új alkalmazás már messze túlmutat az eredetileg meghatározott célokon. Az MI használata tovább erősödik a parancsnoki döntéshozatal felgyorsításának érdekében, integrálják a különböző szenzorok által gyűjtött adatokat az egységes helyzetkép kialakításának céljából, az azokból készített elemzések megfelelő alapot teremthetnek a műveleti feladatok hatékony végrehajtásához. Fontos azonban kiemelni, hogy ezek az eljárások még tesztelési fázisban jelennek meg, a NATO szakértői számos fórumon kifejtették, hogy nem ismertek az MI használatának kockázatai, a megoldások használata műveleti, adott esetben minősített hálózatokon előre nem azonosítható következményekkel járhat. A technológia fejlődését nem lehet és nem is célszerű gátolni, azonban az információbiztonsági eljárások és folyamatok alkalmazásának alapvetésnek kell lennie a tesztelés és műveleti felhasználás során. A fenti példa jól mutatja, hogy a honvédelmi ágazat szintén szembesül a fejlődésből adódó kihívásokkal, azokat célszerű a saját igényeinek megfelelően formálni már a fejlesztések első fázisában. A kezdeti feltételezés, amely szerint az MI túlmutat a kiber fogalmán, ebben az esetben is jól érzékelhető, azt tovább elemezve látható lesz annak kognitív mivolta.

Munka, tudás és hatalom átrendeződése

A bizalom korábban hagyományosan személyekhez és intézményekhez kötődött. Egy katonai szakértőben, egy orvosban vagy egy tanárban nemcsak azért bíztunk, mert tudással rendelkezett, hanem azért is, mert felelősséget viselt. A bizalom mindig összekapcsolódott a számonkérhetőséggel, amikor azonban egy technológiai rendszer válik a tanács, az összefoglalás vagy az értelmezés forrásává, a bizalom természete

[10] Gordon 2025.
[11] SHAPE 2025.

megváltozik. Nem egy személyben bízunk, hanem egy működésben, nem morális integritást feltételezünk, hanem technikai megbízhatóságot, ez a váltás finom, de alapvető és mélyreható. A bizalom átalakul, miközben az interakció személyesnek hat. Ez a kettősség sajátos feszültséget hoz létre, mivel a rendszer „beszél", de nem vállal felelősséget abban az értelemben, ahogyan azt egy ember tenné. A kiberkorszak egyik jellemzője az volt, hogy a hatalom nagyrészt láthatatlan maradt. A hálózatok mögött intézmények és államok álltak, de a felhasználói élmény szintjén ezek ritkán jelentek meg, a technológia közvetített, de nem magyarázott. Az új helyzetben nem egy intézmény hivatkozik egy rendszerre, hanem a rendszer közvetlenül szólal meg. Ez a közvetlenség megkerüli azokat a hagyományos szűrőket, amelyek korábban legitimálták a tudást, szakmai közösségeket, vitákat, ellenőrzési mechanizmusokat. Ez nem feltétlenül rossz, de mindenképpen új, a tudás forrása kevésbé látható, miközben a tudás formája rendkívül meggyőző. Ez a kombináció különösen erős hatással van a döntéshozatalra, az egyik legérdekesebb jelenség az, hogy a rendszerek gyakran akkor is magabiztosnak tűnnek, amikor bizonytalanok. A nyelv ugyanis alapvetően kijelentő formában működik, egy válasz ritkán jelenik meg hezitálásként, inkább állításként fogalmazódik meg. Az emberi kommunikációban a bizonytalanságot gyakran jelzi a testbeszéd, a hangsúly vagy a szünet, ezek a jelek itt hiányoznak, ami megnehezíti annak felismerését, hogy egy válasz mennyire stabil alapokon nyugszik. A kiberinfrastruktúrák esetében a bizonytalanság technikai paraméterekben jelent meg, késleltetésben, hibaarányban, kiesésben, itt azonban a bizonytalanság értelmezési szinten jelenik meg, ami sokkal nehezebben észlelhető.

Egy másik fontos különbség az érzelmi reakciók intenzitása. A legtöbb infrastruktúrához érzelmileg semlegesen viszonyulunk, idegesek lehetünk, ha nem működik, de mélyebb kapcsolat nem alakul ki. Amikor azonban egy technológia nyelvi formában lép kapcsolatba velünk, könnyen kialakul valamiféle kötődés, nem feltétlenül erős érzelmi kapcsolatról beszélünk, de egyfajta megszokás és preferencia. Az ember elkezdi „ismerősnek" érezni a megszólalás módját, és ez önmagában bizalmat ébreszt. Ez a jelenség nem egyedi, hanem mélyen emberi, a nyelvhasználat mindig kapcsolatot teremt, még akkor is, ha tudjuk, hogy a másik oldalon nem ember ül. Amikor egy technológia szereplőként jelenik meg, az nemcsak pszichológiai, hanem társadalmi következményekkel is jár, a döntésekbe való bevonás, a tanácsadás és az értelmezés mind olyan funkciók, amelyek korábban emberekhez vagy intézményekhez kötődtek. Ez a szereplővé válás fokozatos, és éppen ezért nehéz pontos határokat meghatározni, nem egyik napról a másikra történik, hanem apró finomhangolásokon keresztül. Egyre több helyzetben válik természetessé, hogy először nem egy embert, hanem egy rendszert kérdezünk meg. Ez a természetesség az, ami igazán új, nem a technológia létezése, hanem az, hogy reflexszé válik számunkra a használata. Ezen a ponton válik igazán nyilvánvalóvá, miért korlátozott a kiberanalógia: a kiber soha nem beszélt, nem formált véleményt, nem adott tanácsot, nem jelent meg partnerként. Mindig háttérben maradt, még akkor is, amikor döntő fontosságú volt – egy olyan technológia viszont, amely megszólal, elkerülhetetlenül belép az emberi társas térbe, hat a kognitív tudatra. Nem azért, mert emberi lenne, hanem mert az emberi kommunikáció formáit használja. Ez a belépés alapjaiban változtatja meg a viszonyt, és új kérdéseket vet fel a felelősségről, a tekintélyről és az autonómiáról.

A társadalmak mindig is különböző típusú tudásra épültek. Egy kézműves, egy orvos, egy tudós vagy egy katonai tanácsadó értéke nem pusztán a fizikai munkában vagy a mechanikus tudásban rejlett, hanem abban, hogy rendelkezett olyan tapasztalattal és megértéssel, amelyet mások nem birtokoltak. A tudás és a hatalom között szoros kapcsolat állt fenn; aki tudott, annak a döntései súllyal bírtak, és akinek a döntései súllyal bírtak, annak társadalmi pozíciója volt. A digitális korszakban a kiberinfrastruktúrák ugyan megváltoztatták a tudáshoz való hozzáférés sebességét, de alapvetően nem tették feleslegessé az emberi szakértelmet. A számítógépek gyorsították az információfeldolgozást, tárolták az adatokat, de a jelentés és az értelmezés felelőssége továbbra is emberek kezében maradt. A hatalom így az ember és a technológia közös működéséből született, de mindig az ember irányította a döntést. Amikor egy technológia képes nemcsak adatot feldolgozni, hanem értelmezni és javaslatot adni, a helyzet radikálisan változik. A szakértelem ebben az esetben már részben a géppel való együttműködés képességén múlik, hiszen az, aki képes a rendszer által kínált információt értelmezni, ellenőrizni és beépíteni a döntéshozatalba, az előnyhöz jut. Ugyanakkor az, aki ezt a képességet nem sajátítja el, fokozatosan kiszorulhat. Ez a változás a munka és a tudás szerkezetét is átalakítja, a hagyományos szakértelem, amely évtizedek tapasztalatán alapult, most már kombinálódik a technológia által generált elemzéssel. Az új elvárás az, hogy az ember képes legyen együtt dolgozni a rendszerekkel, megérteni azok logikáját, kritikusan értelmezni a javaslatokat, és döntéseket hozni az automatizált tanácsok alapján.

A technológia szereplővé válása új típusú autonómiát igényel. Korábban a döntések felelőssége és a tudás birtoklása egyértelmű volt, az ember döntött, a gép végrehajtott. Most azonban a döntés folyamata hibriddé válik, a gép előkészít, javasol, előrevetít, az ember pedig értelmez, kiválaszt majd mérlegel. Ez a hibrid rendszer kihívást jelent: az embernek meg kell tanulnia, hogy ne automatikusan higgyen a rendszernek, de ne is tagadja annak jelentőségét. A hatalom és felelősség így eloszlik, részben a rendszer funkcionalitásán, részben az emberi döntésen múlik. A rendszerek által nyújtott gyors és széles körű hozzáférés látszólag közössé teszi a tudást, többen férhetnek hozzá elemzésekhez, tanácsokhoz és adatokhoz, mint valaha, ugyanakkor a hozzáférés nem jelenti automatikusan a megértést. Ez a kettősség – a hozzáférés demokratizálódása, a képesség szűk csoportokhoz kötődése – polarizációt hozhat létre.[12] A tudás új elitje azokból áll, akik képesek a rendszerekkel együtt dolgozni, a többiek pedig hátrányba kerülnek. A technológia gyorsasága és rugalmassága a munka világában egyértelmű előnyöket kínál, a döntések gyorsabban születnek, a problémák azonnal felismerhetők, a rendszerek képesek előre jelezni trendeket és kockázatokat. Ugyanakkor ennek az előnynek ára is van, mert a munkafolyamatok és a döntési logika részben kiszolgáltatottjává válik a rendszerek működésének. A rugalmasság és a gyorsaság paradox módon a kiszolgáltatottságot is növeli, mivel az emberi döntéshozónak egyre inkább a rendszer tempójához kell igazodnia, ráadásul úgy, hogy a folyamatok mögött rejlő mechanizmusokat gyakran nem látja teljesen át. A hatalom és a kompetencia így részben eltolódik a gépi rendszerek felé, miközben az emberi szerep továbbra is kritikus marad. Az új korszak szakértelme nemcsak a tudás birtoklását

[12] *Artificial Intelligence. Policy Paper on AI Foundation Models* 2023.

jelenti, hanem az alkalmazkodást, az együttműködést és a kritikai gondolkodást is. A tudás értékét nem pusztán az határozza meg, hogy mit tudunk, hanem az is, hogy hogyan használjuk fel a rendszerek által nyújtott eszközöket. Az új elit azokból a személyekből áll, akik képesek a technológia logikáját megérteni, az adatokat értelmezni, és a rendszert felelősen beépíteni a döntéshozatalba. Ez a kultúraváltás ugyan lassú, de elkerülhetetlen. A munka, a hatalom és a tudás új formái fokozatosan alakulnak ki, és a társadalmi struktúrák is ehhez igazodnak. Azok, akik felismerik és elsajátítják ezt a változást, előnyre tesznek szert, míg a többiek számára a megszokott keretek lassan elavulnak majd.

Végső soron a technológia szereplővé válása nemcsak a munka világát, hanem a társadalom egész szerkezetét átalakítja. Az új korszakban a kompetencia részben a gépi rendszerekhez való viszonyunkon múlik, részben pedig azon, hogy milyen mértékben tudjuk értelmezni, ellenőrizni és beépíteni az automatizált tanácsokat. Ez a változás mélyreható: nemcsak a szakértelem és a döntéshozatal formáját változtatja meg, hanem az emberi társadalmi kapcsolatok és intézmények működését is. A tudás elitje[13] és az információhoz való hozzáférés kérdése újraértelmeződik, miközben a hagyományos hatalmi struktúrák részben átalakulnak, részben pedig új hierarchiákra cserélődnek.[14]

Etika, normák és társadalmi keretek

A tanulmány eddigi részeiből világosan látható, hogy a technológia aktív szereplővé válik, értelmez, javasol, kommunikál. Ez felveti azt a kérdést, hogy egy ilyen rendszer viselkedését hogyan kell értelmezni etikai szempontból. Természetesen a technológia (ma még) nem rendelkezik tudattal, szándékkal vagy érzelmekkel, így morális felelőssége nincs, azonban a hatásai, az emberi döntésekre gyakorolt befolyása és a társadalmi következményei miatt az etikai megítélése nem elkerülhető. Az erkölcsi problémák itt nem a gép belső meggyőződéséből fakadnak, hanem abból, ahogyan a társadalom használja és értelmezi a rendszert. Minden javaslat, minden válasz befolyásolja az emberek döntéseit, és ezáltal kihat a gazdasági, politikai és kulturális viszonyokra. Az etika tehát nem a gépre vonatkozik, hanem a rendszer emberi felhasználására és annak következményeire, az új technológiai környezetben a normák fokozatosan alakulnak ki. Egy korábbi korszakban világos szabályok működtek, az emberi szakértelem, az intézmények és a társadalmi elvárások meghatározták a viselkedést, a döntések felelőssége egyértelmű volt, a hatalom és a tekintély struktúrái jól definiáltak voltak. Most azonban a normák is átalakulnak, a társadalomnak pedig fel kell ismernie, hogy a gépi javaslatok nem semlegesek, és hogy azok használata újfajta felelősséget igényel mindenki részéről. A szabályozásnak és a kulturális elvárásoknak egyaránt biztosítaniuk kell, hogy a technológia alkalmazása ne torzítsa a döntéshozatalt, ne növelje a társadalmi egyenlőtlenséget, és ne helyezze a felelősséget a felhasználó helyett a gépre.

[13] Borgesius 2018.
[14] Dabis–Csáki 2024.

Az egyik legfontosabb etikai követelménynek az átláthatóságnak kell lennie. Amikor egy rendszer javaslatot tesz, nem elég a meggyőző eredmény, hanem a lehetőségekhez mérten láthatóvá kell tenni azt is, hogy hogyan született. A felhasználónak értenie kell, hogy milyen adatok, milyen logika és milyen feltevések vezettek a válaszhoz. Ez nem pusztán tudományos kérdés, hanem etikai és társadalmi szempontból is alapvető, az átláthatóság hiánya könnyen téves bizalmat szülhet. Ha a felhasználó nem látja a döntés mögötti mechanizmust, hajlamos lehet elfogadni a javaslatot pusztán a kialakított forma vagy a koherencia alapján. Ez új típusú függőséget hoz létre, amely nem látható a hagyományos infrastruktúra-elemzésekben. A szereplővé vált technológia egy új etikai problémát is felvet, a felelősség eloszlásának kérdéskörét.[15] Korábban egy döntés vagy cselekedet egyértelműen emberekhez kötődött, most azonban a döntés folyamata részben gépi rendszerek által generált információkon alapul. Ezzel összhangban a felelősség is megosztottá válik, amelynek részese lesz a felhasználó, a rendszer tervezője és üzemeltetője, továbbá a használat módját meghatározó normák is. Ez a hibrid felelősség sokak számára új, nehezen értelmezhető fogalomként jelenik meg. Meg kell tanulnunk, hogy a gép javaslata nem csökkenti az ember felelősségét, a döntés továbbra is emberi döntés, a gép szerepe legfeljebb információt és értelmezési keretet nyújt. Az etikai kérdés az, hogy ezt a keretet hogyan használjuk, és milyen társadalmi garanciákat építünk be a folyamatba. A technológia etikai és társadalmi hatásainak kezelésére létrehozandó szabályozás kulcsfontosságú. Nem elegendő technikai előírásokat alkotni, társadalmi szinten is szabályozni kell a felhasználást, az átláthatóságot, a felelősségvállalást és a hozzáférést. Ennek célja nem a fejlődés megállítása, hanem annak irányítása és keretezése, hogy a társadalmi előnyök maximalizálódjanak, miközben a kockázatok minimalizálódnak. Fontos kiemelni, hogy maradvány kockázat minden esetben jelen lesz, ennek kezelése a felhasználó felelőssége. Az etikai keretek kialakítása nem egyszeri feladat, hanem állandó folyamat: ahogy a technológia fejlődik, úgy alakulnak a társadalmi normák és a jogi előírások is. Az együttműködés és a folyamatos reflexió kulcsfontosságú, hogy a rendszer ne torzítsa a hatalmi viszonyokat, és ne hozzon létre új egyenlőtlenségeket. A technológia szereplővé válása egyszerre hoz lehetőségeket és kockázatokat. A lehetőségek között szerepel a döntéshozatal gyorsítása, a tudás demokratizálása, az emberi hibák csökkentése és a komplex problémák hatékonyabb kezelése. Ugyanakkor kockázatot jelenthet a túlzott bizalom, az átláthatóság hiánya, a társadalmi rétegek széttöredezettségének kialakulása és a felelősségi határok elmosódása. Az etikai és szabályozási keretek célja, hogy a lehetőségek érvényesülhessenek, miközben a kockázatokat kontrollálni tudjuk. Ez nem egyszerű feladat, de nélkülözhetetlen ahhoz, hogy a technológia valóban a társadalom javát szolgálja, és ne váljon manipuláció vagy kiszolgáltatottság eszközévé.[16]

[15] Batool–Zowghi–Bano 2024.
[16] Vesnic-Alujevic – Nascimento – Pólvora 2020.

Hosszú távú ember-technológia együttműködés és fenntarthatóság

Az ember és a technológia közötti kapcsolat hosszú távú fenntarthatósága nem pusztán technikai kérdés, hanem kulcs és egyben cél is, hogy a rendszer és a felhasználó kölcsönösen értelmezhető, egységesnek tekinthető keretek között működjenek együtt. A fenntarthatóság azt jelenti, hogy a technológia nem uralja a döntéshozatalt, ugyanakkor támogatja a felhasználót abban, hogy hatékonyan és megalapozottan cselekedjen.[17] A fenntartható együttműködés három pillére a megértés, a kontroll és a tanulás.

A technológia gyors fejlődése folyamatos adaptációt követel meg, nem elég egyszer megtanulni a rendszer működését, a felhasználóknak folyamatosan összhangban kell lenniük a változásokkal és új funkciókkal, igazodniuk kell az új információs logikákhoz. Az adaptáció ugyanakkor nem csupán gyakorlati készségek kérdése, hanem mentális és érzelmi képesség is egyben, vagyis az embernek el kell fogadnia, hogy a döntési folyamatok részben gépi logikán alapulnak az új keretrendszerben. Ez az adaptáció kölcsönös: a rendszerek tervezőinek figyelembe kell venniük az emberi képességeket, korlátokat és szokásokat. Egy jól tervezett rendszer nemcsak információt szolgáltat, hanem segíti a felhasználót abban, hogy megértse, értékelje és alkalmazza az adatokat a saját döntéseiben.

Az együttműködés minőségét alapvetően a kommunikáció határozza meg, a rendszernek nem elég adatokat adnia, hanem világosan, keretrendszerben és érthetően kell közvetítenie az információt a felhasználó irányába. A visszajelzés kritikus fontosságú lesz, mivel a felhasználónak látnia kell, hogy a rendszer hogyan értelmezte a bemenetet, és hogyan jutott el a javaslatához. A visszajelzés kettős szerepet tölt be, egyrészt az ember számára ad támpontot, másrészt a rendszer is tanulhat a felhasználói interakciókból, ezeket szükségszerűen beépíti a jövőbeni válaszaiba. Ez a kölcsönhatás biztosítja, hogy a technológia ne csak statikus eszköz legyen, hanem dinamikusan fejlődő partnerré váljon a kognitív tudat számára.

Az együttműködés hosszú távú fenntarthatósága szorosan összefügg a bizalom és az autonómia kérdésével, a felhasználónak bíznia kell a rendszerben annyira, hogy a javaslatait figyelembe vegye, ugyanakkor meg kell őriznie saját döntési autonómiáját. Ez az egyensúly rendkívül finom, túlzott bizalom esetén a felhasználó kiszolgáltatottá válhat, túlzott szkepticizmus esetén a rendszer előnyei nem érvényesülnek kellőképpen. Az autonómia fenntartása érdekében a rendszereknek egyértelműen jelezniük kell a bizonytalansági szintet, a javaslatok korlátait és a lehetséges alternatívákat is, a felhasználónak pedig folyamatosan reagálnia kell a döntési folyamatra és felül kell vizsgálnia a gépi javaslatokat kritikus szempontok alapján.

A hosszú távú fenntarthatóság másik kulcseleme a képzés, a felhasználóknak új típusú kompetenciákat kell elsajátítaniuk, többek között az adatkritikát, a rendszer logikájának értelmezését és a hibrid döntéshozatal képességét. Nem elég passzívan elfogadni a gépi javaslatokat, tudatosan kell azokat beépíteni a döntési folyamatokba. A felhasználóknak érteniük kell a döntések társadalmi hatásait, a felelősség eloszlását és az etikai kereteket, ezáltal válhat a hibrid döntéshozatal nemcsak hatékonnyá, hanem

[17] *Artificial Intelligence Cybersecurity Challenges* 2020.

felelősségteljessé is. A fenntartható ember-technológia együttműködés nem valósulhat meg társadalmi keretek nélkül. Az intézményeknek szabályozniuk kell a hozzáférést, biztosítani kell az átláthatóságot, és védelmet kell nyújtani a visszaélések ellen.

Az intézmények feladata, hogy a technológia ezen fejlődését ne csak a gazdasági hatékonyság határozza meg, hanem a társadalmi jóllét, a szakterületek korábban kialakult kulturális keretei és az etikai normák is. A jól működő intézményi keretek lehetővé teszik, hogy a technológia ne csupán eszköz legyen, hanem aktív partner a társadalmi döntéshozatalban. Ez a partnerség a hosszú távú fenntarthatóság alapja, amely biztosítja, hogy a technológiai előnyök széles körben érvényesüljenek, miközben minimalizálódnak a kockázatok. Az új gondolatiság bevezetését, amennyiben rendelkezésre áll, nagymértékben felgyorsíthatja és támogathatja a szervezeten belül korábban kialakított oktatási keretrendszer új elemekkel történő kiegészítése. A Magyar Honvédség esetében ez a platform a Kiber- és Információs Műveleti Központ részeként működő Kiberakadémia lehet, amely jelenlegi oktatási tematikájának kiegészítésével szinte azonnal meg tudja kezdeni az érzékenyítési folyamatokat, majd ezt követően a tematikus felkészítéseket.

A hosszú távú együttműködés egyik legnagyobb kihívása tehát a technológia folyamatos fejlődése, amelynek részeként minden új funkció vagy képesség újabb követelményeket támaszt a felhasználóval szemben. Az adaptáció, a képzés, az etikai normák és a társadalmi szabályozás folyamatosan együtt kell hogy fejlődjenek a technológiával.[18] A másik kihívás az egyenlőtlenség kezelése, mivel nem minden felhasználó rendelkezik azonos képességekkel, tudással vagy hozzáféréssel. A hosszú távú fenntarthatóság érdekében a társadalomnak biztosítania kell, hogy a technológia előnyei ne koncentrálódjanak egy szűk elit kezében, hanem széles körben érvényesüljenek. Az ember és a technológia hibrid együttműködése a jövő társadalmának alapvető struktúráját formálja. A fenntarthatóság kulcsa – mint fentebb említettük – a megértés, az adaptáció, a visszajelzés, az autonómia és a képzés együttes érvényesítése, miközben a társadalmi intézmények biztosítják az etikai és normatív kereteket, ez az együttműködés nem csupán technikai kihívás, hanem kulturális és társadalmi átalakulás is. Azok a társadalmak és közösségek, amelyek képesek integrálni a technológiát a döntéshozatalba anélkül, hogy elveszítenék a felelősségüket és autonómiájukat, a jövő fenntartható, innovatív és igazságos szereplőivé válhatnak.

Összegzés és javaslatok a szervezetek számára az MI „új kiberszerepének" kezelése érdekében

A publikáció során részletesen elemeztem, hogy miként vált a technológia fokozatosan aktív szereplővé a társadalomban, a gazdaságban és a döntéshozatalban, és azt, hogy ez a folyamat természetesen hatással van az érzékeny adatokat kezelő rendszerekre, adatbázisokra, ideértve a katonai rendszereket is. Kezdetben a gépek csupán eszközök voltak, amelyek az ember munkavégzését gyorsították és egyszerűsítették.

[18] Bokor et al. 2022.

A számítástechnika, majd a digitális hálózatok elterjedésével fokozatosan átalakult a tudás és a hatalom szerkezete, és ez előrevetítette, hogy a technológia egyre nagyobb szerepet kap az emberi döntésekben. A hagyományos szakértelem integrálódik a gépi rendszerek által végrehajtott folyamatokba, az új kompetencia részben abból áll, hogy képesek vagyunk hatékonyan együttműködni ezekkel a rendszerekkel. Ez a változás etikai és társadalmi szempontból is kihívást jelent, mivel a felelősség eloszlása és a normák újraértelmezése elkerülhetetlen – a siker kulcsa pedig a megértés, az adaptáció, az autonómia, a visszajelzés és a megfelelő társadalmi szabályozás.

A tanulmányban végrehajtott elemzés eredménye alapján az alábbi szabályozási és fejlesztési javaslatok figyelembevétele és felhasználása esetén a szervezetek csökkenthetik kitettségüket az új típusú kihívásokkal szemben:

- Érthető működés és átláthatóság biztosítása: az MI-rendszerek egyre fontosabb szereplővé válnak a döntéshozatalban, ezért a szervezeteknek biztosítaniuk kell, hogy a működésük átlátható legyen. Ez magában foglalja a javaslatok logikájának, adatforrásainak és bizonytalansági szintjeinek egyértelmű kommunikálását, így biztosítva, hogy a felhasználók ne hozzanak téves feltételezések alapján döntéseket.[19]
- Kritikai kompetenciák fejlesztése: mivel az MI az „új kiber" párhuzamban a tudás és a hatalom új formáit hozza magával, a munkavállalóknak képessé kell válniuk a gépi javaslatok kritikus értelmezésére és a saját döntéshozatalba való integrálására. Ez hosszú távon biztosítja, hogy a szervezet ne váljon kiszolgáltatottá a gépi rendszereknek, azonban ez a kompetencia nem alakul ki magától, tudatosan kell felépíteni.
- Etikai keretek és felelősség tisztázása: mivel az MI-rendszerek befolyása megváltoztatja a felelősség eloszlását, a szervezeteknek világos etikai irányelveket kell kialakítaniuk, amelyek meghatározzák, mikor és hogyan használható a technológia, és ki vállalja a végső döntésért a felelősséget.[20] Amennyiben ezek a megoldások megjelennek a katonai rendszerekben, ott ezt a pontot kiemelt körültekintéssel kell alkalmazni.
- Rendszeres visszajelzés és ellenőrzés: ahhoz, hogy az MI valóban a korábban már integrálódott kiberhez hasonlóan hatékonyan és megbízhatóan működjön, a szervezeteknek folyamatosan ellenőrizniük kell a rendszerek hatékonyságát, és be kell építeniük a felhasználói visszajelzéseket a fejlesztésbe és működésbe. Amennyiben erre nem állnak rendelkezésre megfelelő anyagi, technikai és személyi erőforrások, akkor a teljes folyamat hatékonysága és sikere megkérdőjelezhető lesz.
- Egyenlő hozzáférés és képességek biztosítása: az MI előnyeinek széles körű érvényesítéséhez a szervezeteknek biztosítaniuk kell, hogy minden munkatárs hozzáférjen a rendszerekhez és rendelkezzen a megfelelő ismeretekkel, így elkerülhető, hogy a gépi rendszerek új elit réteget hozzanak létre. Bár mondhatjuk azt, hogy ez minden korban jellemző volt, most lehetőségünk van arra, hogy

[19] Andok 2025.
[20] Danzing 2025.

ettől eltérő módszert és rendszert alakítsunk ki, mivel ennek kezdeti alapköveit még most fektetjük le.

- Hosszú távú stratégiai tervezés: az MI „új kiberként" nem csupán eszköz, hanem stratégiai partner. A szervezeteknek figyelembe kell venniük a hosszú távú hatásokat, a változáskezelést és a fenntartható ember-gépi együttműködés kialakítását, hogy a technológia valóban a szervezet javát szolgálja.[21] Fontos a közös gondolkodás és tapasztalatmegosztás az erőforrások optimalizálásának érdekében, az egyéni megoldások bár számos esetben adott időpillanatban hatékonynak bizonyulnak, hosszú távon nem adnak valódi válaszokat.

Kockázatok kezelése és biztonsági mechanizmusok

Az MI-rendszerek új típusú kockázatokat hordoznak magukban, amelyek közül többet még nem sikerült beazonosítani, ezekre a fejlődési folyamat különböző fázisaiban fogunk ráeszmélni. Értelemszerűen előfordulnak majd félreértett és félremagyarázott javaslatok, előkerül a túlzott bizalom kérdésköre a rendszerrel szemben vagy a teljes tagadás lehetősége is. A lehetőségekhez mérten a szervezeteknek előre fel kell mérniük ezeket a kockázatokat, és már ebben a fázisban megfelelő ellenőrzési és védelmi mechanizmusokat kell kialakítaniuk.[22] A kockázatokat a lehető legmagasabb szinten szükséges megfogalmazni és kezelni, a fejlesztéseknek képesnek kell lenniük a stratégiai és politikai szinten megfogalmazott irányok támogatására.

Összességében elmondható, hogy a technológia nem csupán eszköz, hanem aktív partner a döntéshozatalban és a társadalmi fejlődésben. Az ember-technológia együttműködés jövője nem előre meghatározott, hanem attól függ, hogyan alakítjuk a normákat, a szabályozást és a kultúrát. A kihívások és kockázatok komolyak, de a lehetőségek is óriásiak; ha felelősségteljesen és fenntartható módon integráljuk a technológiát, új dimenziók nyílhatnak az emberi tudás, hatalom és közösségi élet számára. A jövő tehát nemcsak technológiai kérdés, hanem etikai, társadalmi és kulturális feladat is. Az, hogy képesek leszünk-e harmonikus, fenntartható és igazságos együttműködést kialakítani, attól függ, mennyire értjük meg a technológia szerepét, és mennyire tudjuk felelősségteljesen alakítani az ember-gépi hibrid világot.

A tanulmány elemzéseiből levonható következtetések azt mutatják, hogy a technológia szereplővé válása nem csupán a döntéshozatali folyamatokat gyorsítja és teszi hatékonyabbá, hanem alapvetően alakítja át a tudás, a hatalom és a felelősség szerkezetét a társadalomban. Kiderült, hogy azok a felhasználók, akik képesek együttműködni a rendszerekkel, kritikai módon értelmezni a javaslatokat, és integrálni azokat a saját döntéshozatalukba, jelentős előnyre tesznek szert, míg azok, akik nem rendelkeznek e képességekkel, fokozatosan kiszorulnak és lemaradnak. A kutatás rámutatott továbbá, hogy a fenntartható ember-technológia együttműködés kulcsa az átláthatóság, az adaptáció, a folyamatos tanulás és az etikai normák betartása, valamint a társadalmi intézmények megfelelő szabályozása. Ezek az eredmények

[21] Clarke–Knake 2019.
[22] *President Trumps Cyber Strategy for America* 2026.

azt sugallják, hogy a technológia fejlődése egyszerre kínál lehetőséget a társadalmi előnyök széles körű érvényesítésére és kihívást az egyenlőtlenségek és felelősségi kérdések kezelésében, így a jövőbeli fejlődés iránya nagymértékben azon múlik, hogyan integráljuk felelősségteljesen a gépi rendszereket a társadalmi és döntési folyamatokba. A feldolgozott irodalom és az azokból levont következtetések alapján kialakult 7 javaslat minden szervezeti struktúrára sikeresen adaptálható, függetlenül annak stratégiai vagy végrehajtói szerepkörétől, hogy civil, kormányzati vagy akár honvédelmi szerepkört látnak-e el.[23] A tanulmány eredményeként kijelenthető, hogy a tézis, miszerint az „MI az új kiber", nem igazolható, annak jellege és tartalma is eltérő.

Felhasznált irodalom

Artificial Intelligence Cybersecurity Challenges (2020). Brussels: European Union Agency for Cybersecurity (ENISA). Online: https://doi.org/10.2824/238222

Artificial Intelligence. Policy Paper on AI Foundation Models (2023). Paris: UNESCO. Online: www.unesco.org/en/articles/artificial-intelligence-unesco-publishes-policy-paper-ai-foundation-models

Andok Mónika (2025): Mesterségesintelligencia-jártasság. *Iustum Aequum Salutare,* 21(3), 43–60. Online: https://doi.org/10.69695/ias.2025.3.04

Batool, Amna – Zowghi, Didar – Bano, Muneera (2024): *Responsible AI Governance. A Systematic Literature Review.* arXiv. Online: https://arxiv.org/abs/2401.10896

Berendt, Bettina – Littlejohn, Allison – Blakemore, Mike (2020): AI in Education. Learner Choice and Fundamental Rights. *Learning Media and Technology,* 45(3), 312–324. Online: https://doi.org/10.1080/17439884.2020.1786399

Bokor Tamás et al. (2022): *Mi és az MI – Mesterséges intelligenciával kapcsolatos társadalmi attitűdök Magyarországon*. Budapest: MI LAB. Online: https://milab.tk.hu/uploads/files/MI_survey_report_final_doc.pdf

Borgesius, Frederik Zuiderveen (2018): *Discrimination, Artificial Intelligence and Algorithmic Decision-making.* Strasbourg: Council of Europe. Online: https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73

Clarke, Richard A. – Knake, Robert K. (2019): *The Fifth Domain.* New York: Penguin.

Csepeli György (2020): *Ember 2.0 – A mesterséges intelligencia gazdasági és társadalmi hatásai.* Budapest: Kossuth.

Dabis, Attila – Csáki, Csaba (2024): *AI and Ethics. Ethical Challenges of Generative AI in Higher Education.* London: Nature. Online: https://doi.org/10.1057/s41599-024-03526-z

Danzing, Richard (2025): *Artificial Intelligence, Cybersecurity, and National Security. The Fierce Urgency of Now.* Santa Monica: Rand. Online: www.rand.org/pubs/perspectives/PEA4079-1.html

[23] Magyarország Mesterséges Intelligencia Stratégiája [é. n.].

ERTAN, Aytekin et al. szerk. (2020): *Cyber Threats and NATO 2030. Horizon Scanning and Analysis.* Tallinn: NATO CCDCOE Publications. Online: https://ccdcoe.org/uploads/2020/12/Cyber-Threats-and-NATO-2030_Horizon-Scanning-and-Analysis.pdf

GIBSON, William (2004): *Neuromancer. 20th Anniversary Edition.* New York: Ace Books.

GORDON, Lisa (2025): Palantir Technologies Achieves Cybersecurity Maturity Model Certification (CMMC) Level 2. *Investors.palantir.com,* 2025. szeptember 17. Online: https://investors.palantir.com/news-details/2025/Palantir-Technologies-Achieves-Cybersecurity-Maturity-Model-Certification-CMMC-Level-2/

KOVÁCS László (2020): A kiberbiztonság és a kiberműveletek megjelenése Magyarország új Nemzeti Biztonsági Stratégiájában. *Honvédségi Szemle,* 148(5), 12–34. Online: https://doi.org/10.35926/HSZ.2020.5.1

Magyarország Mesterséges Intelligencia Stratégiája [é. n.]. https://cdn.kormany.hu/uploads/document/c/c0/c0d/c0dfdbd37cfa520ae37361a168d244c85e7295af.pdf

President Trump's Cyber Strategy for America (2026). Washington: White House. Online: www.whitehouse.gov/wp-content/uploads/2026/03/President-Trumps-Cyber-Strategy-for-America.pdf

Recommendation on the Ethics of Artificial Intelligence (2021). Paris: UNESCO. Online: www.unesco.org/en/legal-affairs/recommendation-ethics-artificial-intelligence

SHAPE Public Affairs Office (2025): NATO Acquires AI-enabled Warfighting System. *Shape.nato.int,* 2025. április 14. Online: https://shape.nato.int/news-releases/nato-acquires-aienabled-warfighting-system-

VESNIC-ALUJEVIC, Lucia – NASCIMENTO, Susana – PÓLVORA, Alexandre (2020): Societal and Ethical Impacts of Artificial Intelligence. Critical Notes on European Policy Frameworks. *Telecommunications Policy,* 44(6). Online: https://doi.org.10.1016/j.telpol.2020.10196

WEISS János (2020): *Digitalizáció és demokrácia*. Budapest: Goethe-Institut Magyarország. Online: www.goethe.de/ins/hu/hu/kul/sup/alg/ait/22035365.html

Jogi forrás

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

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG

21. évfolyam (2026) 3. szám 75–88.
DOI: 10.32567/hm.2026.3.5

Almási Csaba,[1] Cséplő Zoltán[2]

A nagy közbiztonsági kockázattal járó veszélyes áruk szállítását érintő szabályozás vizsgálata

Analysis of the Regulatory Framework Governing the Transport Security of High-Consequence Dangerous Goods

Absztrakt

A veszélyes árukkal kapcsolatos eltulajdonítás és visszaélések elleni védekezés jogi normarendszerének, valamint az ahhoz kapcsolódó műszaki és szervezési követelményeknek a vizsgálata alapvető fontosságú védelmi igazgatási szakfeladat. Jelen publikációban a nagy közbiztonsági kockázattal járó veszélyes árukra vonatkozó előírások elemzésével, az érintett áruk körének áttekintésével és a közbiztonsági tervek tartalmi követelményeinek rendszerezésével foglalkozunk. A módszertan alapját a vonatkozó nemzetközi és hazai jogszabályok, szakirodalmi források, valamint a veszélyesáru-szállítás gyakorlatának összehasonlító elemzése képezte. A közbiztonsági követelmények központi elemei a kockázatalapú tervezés, a személyi felkészítés, valamint a megelőző és védelmi intézkedések rendszere. A nemzetközi szabályozás keretjellegű előírásai mellett kiemelt szerepe van a nemzeti módszertani útmutatóknak, a képzési rendszerek fejlesztésének és a korszerű műszaki megoldások alkalmazásának a veszélyes árukkal kapcsolatos visszaélések megelőzésében.

Kulcsszavak: ADR, közbiztonság, közbiztonsági terv, kockázatalapú tervezés, veszélyesáru-szállítás

[1] Oktató, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Katonai Műszaki Doktori Iskola, e-mail: almasi.csaba@uni-nke.hu
[2] Iparbiztonsági főfelügyelő, Fővárosi Katasztrófavédelmi Igazgatóság, e-mail: zoltan.cseplo@katved.gov.hu

Abstract

The examination of the legal framework governing the prevention of theft and the misuse of dangerous goods, together with the related technical and organisational requirements, constitutes an important task within the field of security and defence administration. This paper focuses on the analysis of regulations applicable to high-consequence dangerous goods, the identification of the dangerous goods concerned, and the systematisation of the content requirements of transport security plans. The research methodology is based on a comparative analysis of relevant international and national legislation, scientific literature, and the practical implementation of dangerous goods transport security measures. The core elements of transport security requirements include risk-based planning, personnel preparedness, and the implementation of preventive and protective measures. In addition to the framework provisions established by international regulations, national methodological guidance, the development of training systems, and the application of modern technical solutions play a crucial role in preventing the theft and misuse of dangerous goods.

Keywords: ADR, public safety, security plan, risk-based planning, dangerous goods transportation

Bevezetés

A Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1163/2020. (IV. 21.) Korm. határozat (Nemzeti Biztonsági Stratégia) rögzíti, hogy a technológiai fejlődés terjedésével párhuzamosan nő azon nehezen ellenőrizhető, nem állami szereplők jelentősége, akik veszélyeztethetik a biztonságot. Ide tartoznak például a szervezett bűnözői csoportok, nemzetközi terrorszervezetek, kiberbűnözők, szélsőséges vallási mozgalmak, magánbiztonsági cégek, bizonyos civil szervezetek és más nemzetközi hálózatok. Kiemelt biztonsági kockázatként kell értékelni a magyarországi terrorcselekmények elkövetését, a külföldön magyar állampolgárok, magyar érdekeltségek elleni támadások lehetőségét, illetve a szomszédos országok ellen tömegpusztító fegyverekkel, nukleáris, radiológiai, biológiai vagy vegyi szennyező anyagokkal való akciókat. A dokumentum fontos védelmi célként tekint a terroristák által célba vehető helyszínek, különösen a lakosság és az ország kritikus infrastruktúráinak védelmére és a közlekedésbiztonságra. A veszélyhelyzetekre való felkészülés nemcsak az érintett szervezetek felkészítését, de a lakosság tájékoztatását is megköveteli.[3] A Nemzeti Biztonsági Stratégia 174. pontja szerint a katasztrófák megelőzéséhez szükséges képességeket – a lakosság életének, anyagi javainak védelme és a károk hatásainak minimalizálása céljából – szintén ki kell építeni valamennyi katasztrófakockázati típus esetében.

A veszélyesáru-szállítás közbiztonsági előírásainak vizsgálata illeszkedik a Nemzeti Biztonsági Stratégiában szereplő kihívásokkal kapcsolatos megelőzési-felkészülési feladatrendszerbe. A veszélyesáru-szállítással való visszaélések elleni védekezés hatékonyságának és megfelelőségének kockázatelemzésen alapuló ellenőrzése

[3] 1163/2020. (IV. 21.) Korm. határozat.

e cselekmények gyakoriságára vonatkozó információk hozzáférhetősége miatt jóval korlátozottabb, mint a nem szándékosan bekövetkező eseményekkel kapcsolatban.

A veszélyes áru közúti, vasúti és belvízi szállítása során felmerülő közbiztonsági tervezés nemzetközi szabályozásai – a szállítási módozatok technológiájától függően – szinte teljesen azonos rendelkezéseket tartalmaznak. 2005-től az Egyesült Nemzetek Szervezete Európai Gazdasági Bizottságának (ENSZ EGB) Veszélyesáru-szállítási Mintaszabályozásai[4] (ENSZ EGB mintaszabályozás) kiegészültek a közbiztonsági tervezés követelményeit meghatározó előírásokkal. A szabályozások célja a kereskedelmi forgalomban megjelenő veszélyes áruk jogosulatlan birtoklásának megelőzése, valamint az azokkal történő visszaélés elleni védekezés.[5] A veszélyes áru légi és tengeri szállításának nemzetközi szabályozása szintén a veszélyes áruk osztályozásának ENSZ-követelményeire épül. E szabályozás részletesen előírja, hogy mely anyagok szállíthatók, milyen csomagolásban, hogyan kell azokat jelölni, dokumentálni, és milyen biztonsági intézkedéseket kell alkalmazni. E biztonsági intézkedések valamennyi szállítási ágazatban egységes tartalommal jelennek meg.[6]

Jelen kutatásban a veszélyes áruk közúti szállítására vonatkozó ENSZ EGB-előírásokat vizsgáljuk meg részletesen, amely szabályzatot a Veszélyes Áruk Nemzetközi Közúti Szállításáról szóló Európai Megállapodás (European Agreement concerning the International Carriage of Dangerous Goods by Road, ADR) tartalmazza. Az Európai Unió tagállamaiban, így Magyarországon is A veszélyes áruk szárazföldi szállításáról szóló Európai Parlament és Tanács 2008/68/EK irányelve (2008. szeptember 24.) vezette be a közúti szállításokra vonatkozó közbiztonsági tervezés nemzetközi szabályozását. Magyarországon ezen előírásokat a kétévente megújuló szállítási ágazat szabályozása teremti meg kormányrendeleti szinten. A hatályos rendelkezéseket a Veszélyes Áruk Nemzetközi Közúti Szállításáról szóló Megállapodás „A" és „B" Melléklete kihirdetéséről, valamint a belföldi alkalmazásának egyes kérdéseiről szóló 165/2025. (VI. 24.) Korm. rendelet tartalmazza.[7]

Megítélésünk szerint a veszélyesáru-szállítás közbiztonsági megfelelőségének értékeléséhez szükséges megvizsgálni a nemzetközi jogi szabályozás előírásait, és azon kapcsolódó jogalkalmazási és feladat-végrehajtási jógyakorlatokat, amelyek kiindulópontok lehetnek a kapcsolódó műszaki fejlesztési lehetőségek, valamint a hazai oktatási, felkészítési és gyakoroltatási intézkedések műszaki feltételrendszerének megállapításában.

A veszélyesáru-szállítás közbiztonság-tervezési alapfogalmainak áttekintése

A veszélyesáru-szállítás jogszabályozásán belül a szállításban részt vevők részére előírt kötelezettségek és a hatósági jogosítványok megfelelő értelmezéséhez szükséges

[4] UN ECE 2023.
[5] Kátai-Urbán – Kozma – Vass 2015.
[6] Almási et al. 2023.
[7] Cséplő 2024.

a legfontosabb alapfogalmak vizsgálata. Az ADR[8] 1.2.1 fejezetében találhatók meg – többek között – a szabályozás alapfogalmai is, amelyek a következők:

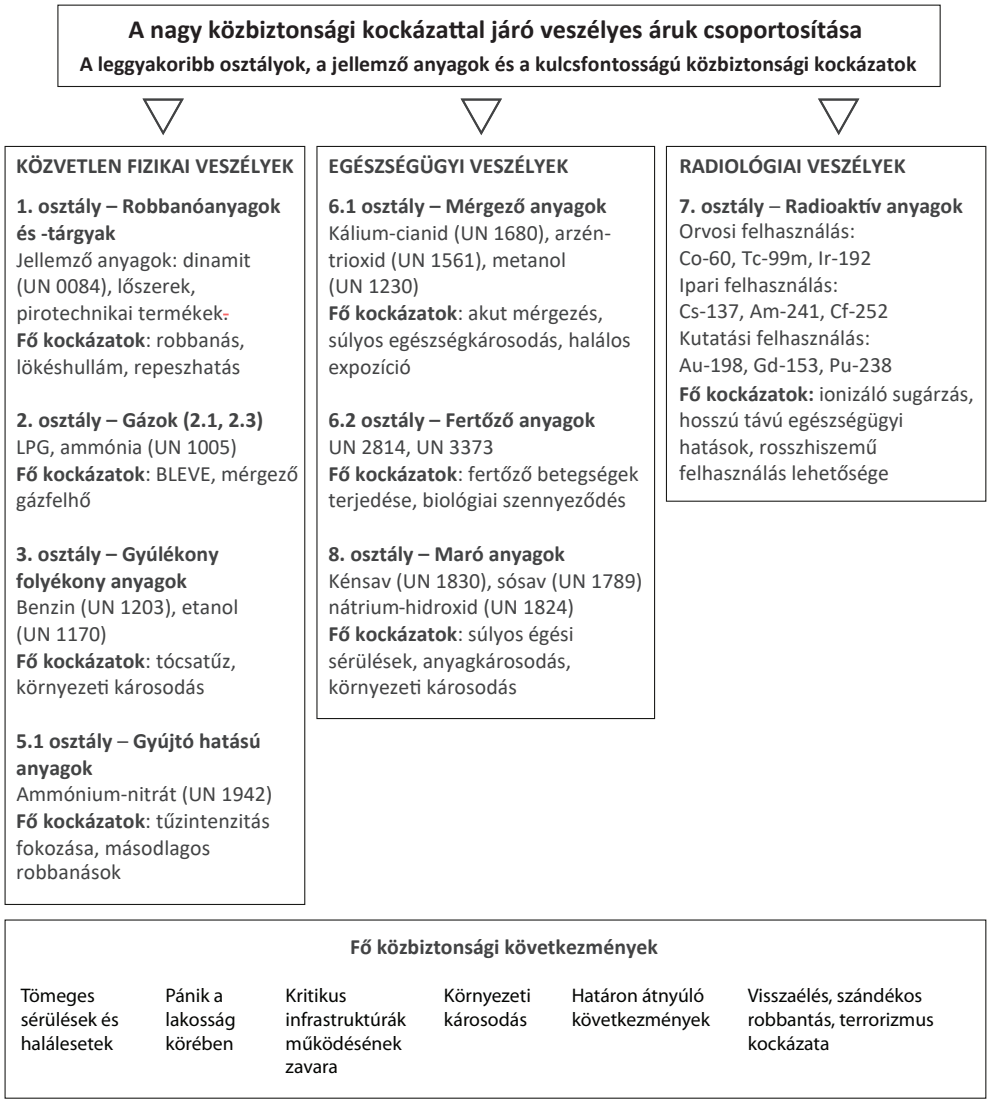
- A veszélyesáru-szállítási tevékenységek között megkülönböztetjük a veszélyes áru helyváltoztatását, a közlekedési okokból történő megállásokat, valamint minden olyan, a közlekedés szempontjából szükségessé vált, helyváltoztatás előtti, alatti és utáni időszakot, amely során a veszélyes áru a járműben, tartányban vagy konténerben van. A fogalom kiterjed a veszélyes áruk átmeneti tárolására is, amikor a közlekedési ágak (a közlekedési eszközök) cseréjénél (átrakásánál) a küldeménydarabokat vagy a tartányokat nem nyitják fel.
- A szabályozás értelmében szállítóeszköz lehet közúti jármű vagy vasúti kocsi, hajó, a hajó raktere vagy meghatározott fedélzeti területe. A jármű lehet battériás, fedett, nyitott, ponyvás és tartányjármű.
- A veszélyes áru szállításában részt vevők és egyéb, a biztonsági intézkedésekre kötelezettek lehetnek a csomagolók, a berakók, a töltők, a feladók, a szállítók, a fuvarozók, a címzettek és a kirakodók is. Közbiztonsági szempontból további felelőssége van magának a járművezetőnek, illetve azoknak, akik a járművezetőt biztonsági, közbiztonsági, oktatási vagy üzemi okból kísérik. Az illetékes hatóságok feladata a veszélyesáru-szállítási rendelkezések betartásának ellenőrzése.
- Az ADR közbiztonsági előírásokról szóló 1.10 fejezetében a „közbiztonság" fogalma alatt értendők „azok a rendszabályok és óvintézkedések, amelyek célja, hogy a lehető legkevesebbre csökkentsék a veszélyes áruk eltulajdonítását, illetve a velük való visszaéléseket, amelyek az embereket, az anyagi javakat vagy a környezetet veszélyeztethetik". A „közbiztonság" fogalomkörének értelmezéséhez azonban meg kell határozni a „veszélyes áruk" definícióját is. Az ADR szerint a veszélyes áru „olyan anyag, vagy tárgy, amely szállítását fenti megállapodások főszabályként tiltják, vagy csak rögzített feltételek mentén teszik lehetővé."

A nagy közbiztonsági kockázattal járó veszélyes áruk osztályai és egyes anyagai

Az alábbiakban az ADR, valamint szakmai tapasztalatunk alapján összefoglaljuk a nagy közbiztonsági kockázattal járó veszélyes anyagok és tárgyak érintett osztályainak főbb jellemzőit, alkalmazási körét, rendszerezve az egyes anyagok kockázati kérdéseit.

A nagy közbiztonsági kockázattal járó veszélyes áruk rendkívül sokféle fizikai, kémiai, biológiai és radiológiai tulajdonsággal rendelkeznek, amelyek eltérő veszélyeztető hatásokat eredményezhetnek. Bár az egyes anyagok különböző áruosztályba tartoznak, közbiztonsági szempontból – domináns veszélyjellemzőik alapján – jól elkülöníthető csoportokba sorolhatók. Az 1. ábra áttekintést ad a legfontosabb, nagy közbiztonsági kockázattal járó veszélyes áruk osztályairól, jellemző anyagairól és azok fő közbiztonsági kockázatairól.

[8] ADR: Accord européen relatif au transport international des marchandises dangereuses par route (fr.), azaz Veszélyes Áruk Nemzetközi Közúti Szállításáról szóló Európai Megállapodás.



1. ábra: A nagy közbiztonsági kockázattal járó veszélyes áruk rendszerezése és fő közbiztonsági kockázatai

Forrás: a szerzők szerkesztése

Az 1. ábra azt szemlélteti, hogy a nagy közbiztonsági kockázattal járó veszélyes áruk három fő veszélyességi csoportba sorolhatók: közvetlen fizikai, egészségügyi, valamint radiológiai veszélyt hordozó anyagokra. Bár az egyes osztályok veszélyjellemzői eltérők, közös sajátosságuk, hogy súlyos közbiztonsági következményekkel járó eseményeket idézhetnek elő, vagyis tömeges sérüléseket, kritikus infrastruktúrák működésének zavarát, környezeti károsodást vagy akár a szándékos visszaélés lehetőségét.

Az ADR 1. osztályába tartoznak azon robbanóanyagok és robbanóanyag-tartalmú tárgyak, amelyek kémiai reakció során nagy mennyiségű energia, hő és gáz hirtelen felszabadulásával robbanást idéznek elő. Az osztály 1.1–1.6 alosztályai a tömegrobbanás, a repeszhatás és egyéb robbanási jellemzők alapján különülnek el. Ide sorolhatók többek között a dinamit (UN 0084), a TNT (UN 0209), egyes ammónium-nitrát alapú robbanóanyagok (UN 0083), a feketelőpor (UN 0027), valamint különböző lőszerek és pirotechnikai termékek, mint például az UN 0336. Alkalmazásuk elsősorban a bányászatban, az építőiparban, a hadiiparban és a pirotechnikában jellemző. Kiemelkedő közbiztonsági kockázatukat a robbanásból eredő lökéshullám, a hőhatás és a repeszképződés adja.

Az ADR 2. osztálya a gázokat tartalmazza. Ide soroljuk mindazokat az anyagokat, amelyek 20 °C-on és 101,3 kPa nyomáson gáz halmazállapotúak, vagy amelyek ilyen körülmények között teljes egészében gázokká alakulnak. A gázok veszélye elsősorban fizikai és kémiai tulajdonságaikból fakad: lehetnek gyúlékonyak, nem gyúlékonyak, mérgezők vagy maró hatásúak. A gázok szállítása jellemzően nyomástartó edényekben vagy tartányjárművekben történik, a hőhatás és a nyomásváltozás elleni védelem biztosítása mellett. Tartányban szállítva elsődleges közbiztonsági kockázata a BLEVE (*boiling liquid expanding vapour explosion,* magyarul a forrásban lévő folyadék gőzének robbanása).

Az ADR 3. osztályába a gyúlékony folyadékok tartoznak, amelyek alacsony lobbanáspontjuk miatt könnyen gyúlékony gőzöket fejlesztenek. Jellemző képviselőik a benzin (UN 1203), az etanol (UN 1170), az aceton (UN 1090), a toluol (UN 1294), valamint a dízelolaj és a fűtőolaj (UN 1202). Ezek az egyik legnagyobb mennyiségben szállított veszélyes áruk csoportját alkotják. Fő veszélyüket a tűz- és robbanásveszély, valamint a jelentős környezeti kockázat jelenti. Tartányos szállításuk során a BLEVE és a tócsatűz kialakulásának lehetőségével is számolni kell.

Az ADR 4.1 osztályába tartoznak a gyúlékony szilárd anyagok, az önreaktív anyagok, az érzéketlenített szilárd robbanóanyagok és a polimerizálódó anyagok. Ezek hő, súrlódás, ütés vagy nyílt láng hatására könnyen meggyulladhatnak, égésük pedig gyors és intenzív lehet. Jellemző képviselőik a kén (UN 1350), a magnéziumpor (UN 1418), a gyufa (UN 1944 vagy UN 1331), valamint egyes önreaktív anyagok, például a dibenzoil-peroxid (UN 3104). Elsősorban az iparban és a vegyipari technológiákban alkalmazzák őket. Szállításuk során kiemelt jelentőségű a gyújtóforrások kizárása és a hőhatások elleni védelem, mivel közbiztonsági kockázatukat elsősorban gyúlékony tulajdonságuk adja.

Az ADR 4.2 osztályába az öngyulladásra hajlamos anyagok tartoznak, amelyek levegővel érintkezve vagy lassú oxidáció következtében külső gyújtóforrás nélkül is meggyulladhatnak. Jellemző képviselőik a fehér- (sárga-) foszfor (UN 1381), a dietil-cink (UN 1366) és a vas-szulfid (UN 1352). Ezeket elsősorban a vegyiparban, speciális kémiai technológiákban és egyes katonai alkalmazásokban használják. Tárolásuk és szállításuk során elengedhetetlen a levegőtől való elzárás és az inert környezet biztosítása. Közúti szállításuk viszonylag ritka, azonban spontán gyulladási hajlamuk miatt jelentős biztonsági kockázatot hordoznak.

Az ADR 4.3 osztályába a vízzel érintkezve gyúlékony gázokat fejlesztő anyagok tartoznak. Ezek víz vagy nedvesség hatására hidrogént vagy más gyúlékony gázokat

képeznek, amelyek a levegővel robbanásveszélyes elegyet alkothatnak. Jellemző képviselőik a nátrium (UN 1428), a kálium (UN 2257), a kalcium-karbid (UN 1402), a lítium (UN 1415) és az alumíniumpor (UN 1396). Alkalmazásuk elsősorban speciális ipari folyamatokhoz kapcsolódik. Tárolásuk és szállításuk során alapvető követelmény a nedvesség teljes kizárása, mivel már kis mennyiségű víz is veszélyes reakciót idézhet elő. Közúti szállításuk viszonylag ritka, azonban reakciókészségük miatt jelentős biztonsági kockázatot jelentenek.

Az ADR 5.1 osztályába a gyújtó hatású (oxidáló) anyagok tartoznak. Ezek önmagukban általában nem éghetők, azonban oxigén leadásával elősegítik más anyagok égését, ezáltal fokozzák a tűz intenzitását és terjedését. Jellemző képviselőik a kálium-nitrát (UN 1486), a nátrium-nitrát (UN 1498), az ammónium-nitrát (UN 1942), valamint a hidrogén-peroxid oldatok (UN 2014, UN 2015). Elsősorban a műtrágyagyártásban, a vegyiparban és a robbanóanyag-iparban alkalmazzák őket. Szállításuk során kiemelt jelentőségű az éghető anyagoktól való elkülönítés, mivel tűz esetén jelentősen növelhetik a káresemény súlyosságát. Gyakori közúti szállításuk miatt közbiztonsági kockázatuk is számottevő.

Az ADR 6.1 osztályába a mérgező anyagok tartoznak, amelyek belélegezve, lenyelve vagy bőrrel érintkezve már kis mennyiségben is súlyos egészségkárosodást vagy halált okozhatnak. Jellemző képviselőik a kálium-cianid (UN 1680), az arzén-trioxid (UN 1561), a metanol (UN 1230) és a diklór-etán (UN 1184). Ezek az anyagok a szervezetbe jutva toxikus hatást fejtenek ki, ezért különös veszélyt jelentenek a kezelőszemélyzetre és a környezetre. Elsősorban a vegyiparban, a növényvédőszer-gyártásban és laboratóriumi tevékenységek során használják ezeket. Közúti szállításuk gyakori, jellemzően küldeménydarabos formában.

Az ADR 6.2 osztályába a fertőző anyagok tartoznak, amelyek kórokozó mikroorganizmusokat vagy biológiai toxinokat tartalmaznak, és emberekben vagy állatokban betegséget okozhatnak. Jellemző példái a diagnosztikai minták (UN 3373), a humán vérminták és a laboratóriumi kórokozó-kultúrák (UN 2814). Szállításuk speciális, többrétegű és zárt csomagolásban történik, kezelőik számára pedig megfelelő védőfelszerelés alkalmazása szükséges. Az osztály elsődleges kockázata a fertőzés terjedése, ugyanakkor közbiztonsági szempontból a biológiai veszélyeztető képesség és a társadalmi hatások miatt is kiemelt jelentőségű.

A nagy közbiztonsági kockázattal járó radioaktív anyagok az ADR 7. osztályán belül azok a radioaktív küldemények, amelyek aktivitása eléri vagy meghaladja a meghatározott közbiztonsági küszöbértéket. A radioaktív anyagok instabil atommagjaik bomlása során ionizáló sugárzást bocsátanak ki, amely megfelelő védelem hiányában egészségkárosodást, sugárbetegséget vagy hosszú távú genetikai hatásokat okozhat.

Az ADR 7. osztályába tartoznak többek között az urán- és plutóniumizotópok, valamint a kobalt-60 és a cézium-137, amelyeket az energetikában, az orvostudományban, a kutatásban és az iparban alkalmaznak. Az anyagokat a sugárzási szint és a csomagolás alapján különböző kategóriákba sorolják, amelyek meghatározzák a szükséges biztonsági intézkedéseket. Közbiztonsági jelentőségük kiemelkedő, mivel a sugárforrásokkal való visszaélés vagy azok sérülése súlyos következményekkel járhat. A radionuklidok széles körű alkalmazása indokolja felhasználási területeik és hazai előfordulásuk áttekintését.

Orvosi és biológiai területen alkalmazzák például a Co-60 (kobalt-60) izotópot, mégpedig sugárterápiában, daganatos megbetegedések kezelésére, illetve ipari gammabesugárzó berendezésekben sterilizálásra. A Cs-137 (cézium-137) az orvosi besugárzókban, illetve sugárforrásként a radiográfiában és vastagságmérésnél jelenik meg. A Ir-192 (irídium-192) brachyterápiában (belső sugárkezelés) és ipari radiográfiában használatos.[9] Az olyan izotópok, mint az I-125, a Pd-103, a Ru-106 vagy az Sr-90, helyi sugárkezelésben használatosak (például prosztata-, szem- és egyéb daganatoknál).

A diagnosztikában alapvető anyag a Tc-99m, amely a leggyakrabban alkalmazott, képalkotó célú izotóp.[10] Emellett például a Tl-204, az Se-75, az Yb-169 is használatos sugárforrásként röntgenhelyettesítő ipari mérésekben és orvosi kutatásokban.[11]

Ipari és technológiai felhasználásúak az olyan izotópok, mint az Am-241 (amerícium-241), ipari füstérzékelőkben és sűrűségmérőkben jelennek meg, mint alfa-sugárzó források.[12] A Cf-252 (kalifornium-252) neutronforrásként használatos neutronaktivációs analízisben, robbanóanyag-detektálásban és reaktorkutatásban. Az előzőekben már említett Co-60 és Cs-137 ipari radiográfiában, például hegesztési varratok és fémstruktúrák hibáinak feltárására is szolgálnak. Más izotópok, mint a Kr-85 folyadékszintmérőkben és gázáramlás-vizsgálatokban, az Fe-55, valamint az Ni-63, röntgen-fluoreszcenciás spektroszkópiában és detektorok kalibrálására használatosak, a Po-210 pedig antisztatikus eszközökben, például műanyag- és textilipari alkalmazásokban jelenik meg.[13]

Tudományos és kutatási területen alkalmazzák az olyan izotópokat, mint az Au-198 (arany-198) aktivációs elemzésben és nyomjelzéses kísérletekben, különösen biológiai folyamatok és kémiai reakciók vizsgálatára szolgálnak.[14] A Cd-109 (kadmium-109) röntgen-fluoreszcenciás anyagvizsgálatban és érzékelők kalibrálásában használatos. A Gd-153 (gadolínium-153) denzitometriás mérésekben és tomográfiás kutatásokban, a Pm-147 (prométium-147) vékony rétegek vastagságának mérésére, illetve béta-forrásként energiamérő rendszerekben.[15] Az izotópok közé tartozik a Pu-238 (plutónium-238), amely radioizotópos termoelektromos generátorok (RTG) energiaforrása – például űrszondákban. Történelmileg a Ra-226 (rádium-226) orvosi kezelésekhez és világító festékekhez volt használatos, ma már főként kutatási célokra korlátozottan alkalmazzák.[16]

A környezetvédelmi és biztonságtechnikai alkalmazás területén meg kell említeni a Sr-90 (stroncium-90) izotópot, amely radioaktív szennyezések és környezeti minták (például talaj, víz, növények) vizsgálatára szolgál, mivel könnyen beépül a biológiai kalcium-ciklusba.[17] Az olyan források, mint az amerícium-241 és kalifornium-252, neutron- és gammamérésekben, a nukleáris hulladékok azonosításában is használatosak.

Magyarországon is működik olyan technológiai háttér és infrastruktúra, amely lehetővé teszi ezeknek az izotópoknak a gyártását, forgalmazását és alkalmazását.

[9] CDC 2026.
[10] Science Direct [é. n.].
[11] NRC 2026b.
[12] EPA 2026.
[13] NRC 2026a.
[14] Radiocode 2026.
[15] CDC 2026.
[16] NRC 2026b.
[17] National Academies of Sciences, Engineering, and Medicine 2008.

A Nemzetközi Atomenergia-ügynökség (International Atomic Energy Agency, IAEA) jelentése szerint Magyarország két kutatóreaktort is működtet, és izotóptermelés is folyik az országban, továbbá radioaktív forrásokat alkalmaznak ipari, orvosi és kutatási célokra.[18] Az 1959-ben üzembe helyezett, budapesti kutatóreaktor például kifejezetten célul tűzte ki az izotóptermelést orvosi és ipari felhasználásra.[19] Ez azt jelenti, hogy Magyarország nemcsak importál radionuklidokat, hanem hazai előállítás is folyik, különösen orvosi és ipari radioizotópok területén. Az Izotóp Intézet például hangsúlyozza, hogy ipari forrásokat (Co-60, Ir-192) is képes gyártani és szállítani.

Az ADR 8. osztályába a maró anyagok tartoznak, amelyek kémiai úton károsítják az élő szöveteket, valamint a fémek és más anyagok felületét. Jellemző képviselőik a kénsav (UN 1830), a sósav (UN 1789), a nátrium-hidroxid (UN 1823/1824), a kálium-hidroxid (UN 1813) és az ammónia-oldat (UN 2672). Ezeket széles körben alkalmazzák az iparban. Fő veszélyüket a súlyos szövetkárosító hatás és az irritáló gőzök jelentik, miközben jelentős szállítási mennyiségük miatt közbiztonsági szempontból is figyelmet érdemelnek.

Az ADR csomagolásban raktározott veszélyes áru általi veszélyeztetettség kezelésével a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről szóló szabályozás foglalkozik.[20] A raktárlogisztikai létesítmények szigorú tűzmegelőzési és a környezetvédelmi szabályozás hatálya alá tartoznak.[21]

A közbiztonsági tervezési kötelezettség

A nagy közbiztonsági kockázattal járó veszélyes árukkal foglalkozó szállítási szereplőknek közbiztonsági tervet kell készíteniük.

A közbiztonsági terv készítéséért a szállítók, fuvarozók, feladók és a többi résztvevő felelős. A terv elkészítéséhez az ADR konkrét, azonban általánosan megfogalmazott tartalmi követelményeket rendel, amelyek az alábbi elemekből állnak:

- A közbiztonsági rendszabályok és óvintézkedések végrehajtásáért felelős és megfelelő képesítéssel rendelkező személyek közötti feladatmegosztás.
- A veszélyes tevékenységben érintett veszélyes áruk és veszélyesáru-fajták nyilvántartása.
- A veszélyes tevékenységek közbiztonsági kockázatának értékelése. A szállítási műveletek vizsgálata, kitérve a veszélyes áruk járművön, tartányban vagy konténerben történő tárolására. A veszélyes áruk átmeneti tárolása az intermodális szállítás vagy az egységek közötti átrakás során.
- Az azonosított közbiztonsági kockázatok csökkentéséhez szükséges intézkedések, amelyek a következők lehetnek:
  - A szállítási folyamatban részt vevők képzésével kapcsolatos információ.

[18] IAEA 2022.
[19] Budapest Research Reactor Hungary 2026.
[20] Cimer et al. 2025.
[21] Kátai-Urbán et al. 2023.

  - A közbiztonsági intézkedések leírása, amelyek lehetnek többek között veszélyhelyzeti intézkedések, rezsimszabályok (új alkalmazottak biztonsági ellenőrzése).
  - Az üzemeltetési eljárások és intézkedések bevezetésének a meghatározása, mint például útvonal, átmeneti tárolóhelyek kiválasztása, érzékeny infrastruktúra-elemek kiválasztása.
  - A közbiztonsági rendkívüli események kezeléséhez és jelentéséhez szükséges hatékony eljárások és intézkedések kidolgozása.
- A közbiztonsági tervben foglaltak értékelésére, ellenőrzésére, valamint a rendszeres felülvizsgálatára és korszerűsítésére vonatkozó tevékenység rendjének meghatározása.
- A közbiztonsági tervben szereplő szállítási információk fizikai védelmének és hozzáférési rendjének biztosítására szolgáló intézkedések meghozatala. Ezek az intézkedések azonban nem akadályozhatják az ADR-ben máshol előírt információk megadását.

Az ADR az illetékes hatósággal történő együttműködési kötelezettséget ír elő a szállítónak, a fuvarozónak, a feladónak és a címzettnek a fenyegetésre vonatkozó információk kicserélésében, a megfelelő közbiztonsági intézkedések alkalmazásában és a közbiztonságot érintő rendkívüli események kezelésében. A jármű és rakománya eltulajdonításának megakadályozása érdekében a szabályzatok a készülékek, berendezések és megfelelő eljárásrendek alkalmazását írják elő. Az ADR a közlekedési telemetriai vagy egyéb nyomkövető módszerek alkalmazhatóságát is leírja.

A nagy közbiztonsági kockázattal járó radioaktív anyagok esetében az ADR előírja a Nukleáris anyagok fizikai védelméről szóló Egyezményben[22] és a Nemzetközi Atomenergia-ügynökség által kiadott *Nukleáris anyagok és nukleáris létesítmények fizikai védelme* című kiadványban megfogalmazottak használatát.[23] A kiadvány rendelkezéseit hazánkban az atomenergia alkalmazása körében a fizikai védelemről és a kapcsolódó engedélyezési, jelentési és ellenőrzési rendszerről szóló 190/2011. (IX. 19.) Korm. rendeletet hajtja végre. A nukleáris védettség megvalósulásához szükséges a fizikai védelmi intézkedések bevezetése mint az őrzés-védelmi, a monitoring és a visszaélések megakadályozásával kapcsolatos intézkedések bevezetése.[24] Az Országos Atomenergia Hivatal a nukleáris és radioaktív anyagokkal (7. osztály) kapcsolatos rendkívüli események megelőzésére és kezelésére módszertani útmutatókat dolgozott ki.[25]

A nukleáris védettség mindazon intézkedések, eszközök és eljárások összességét jelenti, amelyek azt szolgálják, hogy a nukleáris és egyéb radioaktív anyagokat, valamint a kapcsolódó létesítményeket ne tulajdoníthassák el, ne használják jogosulatlanul vagy ne éljenek ezekkel vissza. E rendszernek három alapvető területe van: a megelőzés, a detektálás és az elhárítás. A megelőzés magában foglalja a hatósági felügyeleti rendszert, a nukleáris biztosítékok és az exportellenőrzés szabályozását,

[22] A nukleáris anyagok fizikai védelméről szóló Egyezmény 1980.
[23] NAÜ 1999.
[24] Solymosi–Solymosi–Vass 2020.
[25] Országos Atomenergia Hivatal 2026.

a radioaktív anyagok pontos és naprakész nyilvántartását, valamint a nukleáris és más radioaktív anyagok megfelelő fizikai védelmét.[26]

A közbiztonsági tervezéshez közvetlenül kapcsolódó előírások vizsgálata

Az ADR az alábbi közbiztonsági tervezéssel kapcsolatos fontosabb előírásokat tartalmazza:

- Az ADR 1.3 fejezete alapján a veszélyes áruk szállításában részt vevő személyek képzése vonatkozásában a veszélyes árukkal kapcsolatos közbiztonsági előírásokról szóló 1.10 fejezet képzési követelményeit is figyelembe kell venni. A képzést a veszélyes áruk szállításával kapcsolatos munkakört ellátó személyeknek kell megkapniuk még a feladatok végrehajtása előtt. A képzésnek tehát többek között ki kell terjednie a közbiztonsági tervezési feladatok ellátására is.
- Az ADR részletesen tárgyalja a szállítási tevékenységben részt vevők biztonsággal kapcsolatos kötelezettségeit, amellyel kapcsolatosan az 1.4 fejezet előírja, hogy a közbiztonságot közvetlenül veszélyeztető eseménynél a szállításban részt vevőknek tájékoztatni kell a veszélyhelyzetet elhárító szolgálatokat, és rendelkezésükre kell bocsátaniuk a beavatkozáshoz szükséges információkat. Ezen túl a küldemény továbbítását meg kell szakítani – többek között – egy közbiztonságot érintő lehetséges veszély esetén, ha a küldemény nem felel meg az előírásoknak.
- A biztonsági követelmények betartását garantáló 1.8 fejezet szerint az illetékes hatóságnak ellenőriznie kell az 1.10.1.5 bekezdés szerinti közbiztonsági intézkedések betartását is. Ezzel kapcsolatosan a gazdálkodó szervezet (vállalkozás) biztonsági tanácsadójának feladata az 1.10.3.2 bekezdésben meghatározott közbiztonsági terv meglétének ellenőrzése.
- Az ADR 1.10 fejezete foglalja magában azon közbiztonsági előírásokat, amelyek tartalmazzák az általános előírásokat, a képzéssel kapcsolatos rendelkezéseket, a nagy közbiztonsági kockázattal járó veszélyes áruk azonosításának szabályait, valamint a közbiztonsági terv kötelező általános tartalmi elemeit.

A közbiztonsági tervezés általános előírásai között az alábbi rendelkezéseket találhatjuk:

- A veszélyes áru szállítása során biztosítani kell a megfelelően azonosított szállítót és fuvarozót.
- A veszélyes áruk átmeneti tárolóhelyein biztosítani kell azok megfelelő fizikai védelmét és megvilágítását.
- Fontos továbbá a járműszemélyzet fényképes személyazonosító okmányainak megléte, továbbá az illetékes hatóságnak naprakész nyilvántartást kell vezetnie az érvényes járművezetői oktatási bizonyítványokról.

[26] Horváth – Kátai-Urbán – Sebestyén 2016.

A közbiztonsági képzés során a következő szabályokat kell betartani:

- A képzésnek és ismeretfelújító oktatásnak részét kell képezze a közbiztonsági szempontok tudatosítása is, amelynek keretében foglalkozni kell a közbiztonsági kockázat jellegével, annak felismerésével, a kockázatkezelés és -csökkentés módszereivel és a közbiztonság megsértése esetén teendő intézkedésekkel. Ezen túl az érintetteknek meg kell ismerniük a közbiztonsági terv szerinti felelősségüknek megfelelő feladataikat is.
- A képzésnek – dokumentáltan – meg kell előznie a veszélyesáru-szállítói munkakör betöltését. Ezen túl a képzésben részesülőknek rendszeres időközönként ismeretfelújító oktatást kell biztosítani. A képzési iratokat az illetékes hatóság által meghatározott időtartamig meg kell őrizni.

A nagy közbiztonsági kockázattal járó veszélyes áruk tekintetében az ADR elsősorban a terroristacselekmények során alkalmazható árukat nevezi meg példákkal, a hatásuk között pedig megemlítik a tömeges baleseteket, a tömeges pusztató hatást, vagy – különösen a radioaktív anyagok esetében – a lehetséges társadalmi és gazdasági zavarokat.

Befejezés, következtetések

Jelen publikációban a veszélyes áru szállításához kapcsolódó közbiztonsági tervezés műszaki-technikai, valamint képzési elemeit vizsgáltuk.

A veszélyes áru szállítására vonatkozó jogi szabályozás közbiztonsági aspektusainak feltárását követően értelmeztük a témakör szempontjából meghatározó alapfogalmakat, majd részletesen elemeztük e szabályozásban rögzített közbiztonsági tervezési követelményeket.

Megállapítottuk, hogy a közbiztonsági előírások döntő többsége az ADR 1.10 fejezetében jelenik meg, ugyanakkor a képzéssel, az események bejelentésével és a hatósági ellenőrzésekkel kapcsolatos rendelkezések szintén fontos részét képezik a közbiztonsági követelményrendszernek.

A szabályozás alkalmazása szempontjából kiemelt jelentőségű a nagy közbiztonsági kockázattal járó veszélyes áruk körének meghatározása. Ennek keretében az ADR egyes osztályaihoz és alosztályaihoz tartozó, közbiztonsági szempontból releváns veszélyes anyagokat és anyagcsoportokat azok veszélyeztető hatásai alapján elemeztem és rendszereztem. Külön figyelmet fordítottunk a 7. osztályba tartozó radioaktív anyagokra, amelyek esetében megállapítottuk, hogy a hazai nukleáris védettségi szabályozás jelentős mértékben meghatározza a közbiztonsági tervezés eljárási és tartalmi követelményeit is.

A közbiztonsági tervek elkészítéséért a szállítási lánc különböző szereplői – így különösen a feladók, a fuvarozók, a szállítók és egyéb érintett résztvevők – együttes felelősséget viselnek. Bár a nemzetközi megállapodások meghatározzák a közbiztonsági tervek kötelező tartalmi elemeit, azok elsősorban keretjellegű követelményeket fogalmaznak meg. A részletes eljárási szabályok, módszertani útmutatások és gyakorlati alkalmazási feltételek kidolgozása ezért elsősorban a nemzeti szabályozás és a jogalkalmazást támogató szakmai dokumentumok feladata.

Megállapítható továbbá, hogy a közbiztonsági tervezés szabályozási rendszere dinamikusan fejlődő terület, amelynek alakulását jelentős mértékben befolyásolják a szállítási alágazatok technológiai változásai, valamint a veszélyes tevékenységekkel összefüggésben bekövetkezett balesetek társadalmi, gazdasági, politikai és szakmai hatásai. A szabályozás fejlődése ezért szoros kapcsolatban áll a közlekedési rendszerek biztonsági kihívásaival, valamint az ezekre adott nemzeti és nemzetközi válaszintézkedésekkel.

Felhasznált irodalom

Almási, Csaba et al. (2023): Security Planning in the Transport of Dangerous Goods by Road. *American Journal of Research Education and Development,* 4, 4–13. Online: https://red.devlart.hu/issues/2023_4.pdf

Budapest Research Reactor Hungary (2026): *Country Report RROG 2019 in Mainz, Germany 14–17 May.* Online: https://download.uni-mainz.de/fb09-kernchemie/RROG/Country_Report_Hungary.pdf

CDC (2026): *Radiation Emergencies.* Online: www.cdc.gov/radiation-emergencies/hcp/isotopes/cobalt-60.html

Cimer Zsolt et al. (2025): *Módszertani kézikönyv: veszélyes ipari védelmi ügyintézők részére*. Budapest: Hungária Veszélyesáru Mérnöki Iroda.

Cséplő, Zoltán (2024): Assessment of Public Security Planning Regulations and Guidelines related to Dangerous Goods Transportation Facilities. *American Journal of Research Education and Development,* (3), 60–73. Online: https://red.devlart.hu/issues/2024_3.pdf

Easy Access Rules for Air Operations (2026). *Easa.europa.eu,* 2026. március 27. Online: www.easa.europa.eu/en/document-library/easy-access-rules/easy-access-rules-air-operations

EPA (2026): *Americium in Ionization Smoke Detectors.* Online: www.epa.gov/radtown/americium-ionization-smoke-detectors

Horváth Kristóf – Kátai-Urbán Lajos – Sebestyén Zsolt (2016): Nukleáris biztonság és védettség hazai kutatási-fejlesztési eredményei. *Hadmérnök,* 11(4), 69–90. Online: http://hadmernok.hu/164_08_horvath.pdf

IAEA (2022): Mission Says Hungary Committed to Safe Management of Radioactive Waste, Sees Opportunities for Further Enhancement. *Iaea.org,* 2022. április 4. Online: www.iaea.org/newscenter/pressreleases/iaea-mission-says-hungary-committed-to-safe-management-of-radioactive-waste-sees-opportunities-for-further-enhancement

Kátai-Urbán Lajos – Kozma Sándor – Vass Gyula (2015): Veszélyes szállítmányok felügyeletével kapcsolatos jog- és intézményfejlesztési tapasztalatok értékelése. *Hadmérnök,* 10(3), 92–108.

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

National Academies of Sciences, Engineering, and Medicine (2008): *Industrial Radiography. Radiation Source Use and Replacement: Abbreviated Version.* Washington, DC: The National Academies Press. Online https://doi.org/10.17226/11976
NAÜ (1999): *Nukleáris anyagok és nukleáris létesítmények fizikai védelme.* INFCIRC/225/Rev.4, Vienna.
NRC (2026a): *Industrial Uses of Nuclear Materials.* Online: www.nrc.gov/materials/miau/industrial
NRC (2026b): *US Nuclear Regulatory Commission.* Online: www.nrc.gov
Országos Atomenergia Hivatal (2026): *Jogi szabályozás, útmutatók.* Online: www.haea.hu/web/v3/OAHPortal.nsf/web?openagent&menu=04&submenu=4_0
Radiocode (2025): *Au-198.* Online: www.radiacode.com/isotope/au-198?lang=en&utm
Science Direct [é. n.]: *Palladium 103.* Online: www.sciencedirect.com/topics/medicine-and-dentistry/palladium-103?utm
Solymosi Máté – Solymosi József – Vass Gyula (2020): A nukleáris biztonsági kultúra és a nukleáris védettségi kultúra történeti áttekintése és hazai alkalmazásai. *Védelem Tudomány,* 5(1), 181–191. Online: https://ojs.mtak.hu/index.php/vedelemtudomany/article/view/13395/10810
UN ECE (2023): *UN Model Regulations Rev. 23 (2023).* Online: https://unece.org/transport/dangerous-goods/un-model-regulations-rev-23

Jogi forrás

1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról
A nukleáris anyagok fizikai védelméről szóló Egyezmény, INFCIRC/274/Rev.1, IAEA, Vienna, 1980

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG

21. évfolyam (2026) 3. szám 89–103.
DOI: 10.32567/hm.2026.3.6

Cséplő Zoltán,[1] Kátai-Urbán Maxim,[2] Vass Gyula[3]

Az iparbiztonsági oktatás és képzés rendszerének vizsgálata

Examination of the System of Education and Training in Industrial Safety

Absztrakt

Az ország közigazgatásának, a gazdálkodó szervezeteknek és a lakosságnak a védelme érdekében működő iparbiztonság egyre nagyobb jelentőségű a civilizációs kihívásokkal teli világban. Következésképpen az iparbiztonsági üzemeltetők és a hatósági szakemberek oktatása és képzése egyre nagyobb prioritást élvez Magyarországon. Jelen tanulmány elkészítésének célja értékelni az iparbiztonsági felsőoktatási képzés kialakításának és fejlesztésének főbb eredményeit és tapasztalatait, amelynek alapján meghatározhatjuk a jövőbeni oktatásfejlesztési intézkedések célját és tartalmát.

Kulcsszavak: iparbiztonság, felsőoktatás, képzés, katasztrófavédelem, Magyarország

Abstract

Industrial safety has an increasing importance in a world full of civilisational challenges for the protection of the country's public administration, economic organisations and the population. Consequently, the education and training of industrial safety operators and government experts are becoming an increasingly high priority in Hungary. The aim of the present study is to evaluate the main results and experiences of the establishment and

[1] Iparbiztonsági főfelügyelő, Fővárosi Katasztrófavédelmi Igazgatóság, e-mail: zoltan.cseplo@katved.gov.hu
[2] Oktató, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Katonai Műszaki Doktori Iskola, e-mail: maximkatai@gmail.com
[3] Tanszékvezető egyetemi docens, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Katasztrófavédelmi Intézet Tűzvédelmi Műszaki Tanszék, e-mail: vass.gyula@uni-nke.hu

development of higher education in industrial safety, on the basis of which to determine the aim and content of future educational development measures.

Keywords: industrial safety, higher education, training, disaster management, Hungary

Bevezetés

A hazai iparbiztonság sajátos nemzetközi, európai uniós, illetve magyar jog- és intézményrendszerre épül, és jelentősen kapcsolódik a nemzetközi és európai uniós jogszabályok kialakulásához, Magyarország iparbiztonsági veszélyeztetettségéhez, a hazai biztonságkultúra kialakulásához. Az iparbiztonság megelőzési, felkészülési és baleset-elhárítási feladat- és hatáskörei kiterjednek a telepített veszélyes üzemekre, az azok közötti veszélyesáru-szállítási és logisztikai tevékenységre, a nukleáris létesítményekre és hulladéktárolókra, és azokra a kritikus szervezetekre és létesítményekre, amelyek magas fokú üzembiztonságának garantálása egyben az érintett lakosság és a környezeti elemek védelmét is jelenti. Az iparbiztonság területén dolgozó szakemberek a szabályozás hatálya alá tartozó üzemeltetők, hatóságok és önkormányzatok szervezeteiben látják el jogszabályban előírt feladataikat.

Az ágazati szakemberképzés célja, hogy az érintett végrehajtó szervezetek számára elegendő és a szükséges képesítéssel rendelkező, államtudományi és műszaki-mérnöki területen végzett, professzionális katasztrófavédelmi, tűzvédelmi és iparbiztonsági szakember álljon rendelkezésre, akik lépést tudnak tartani a természet és a technológia változásaival.

A következőkben – a releváns jogi szabályozás, szervezeti szabályozók és mértékadó szakirodalom feldolgozásának útján – a hazai felsőoktatási, szakképzési és felnőttképzési tapasztalatokat dolgozzák fel a szerzők összefoglaló módon.

Fogalmi áttekintés

A fogalmi vizsgálatunk az oktatás, a képzés és a továbbképzés fogalmi összetevőinek értékelésére terjed ki. Az oktatás tudományos fogalmát – a nevelés részeként – a Falus Iván szerkesztésében megjelent *Didaktika – Elméleti alapok a tanítás tanulásához* című kötet adja meg, amely szerint az oktatás olyan „komplex, tudatos, tervszerű, direkt és indirekt tevékenység, mely az ismeretszerzésnek, a jártasságok, a készségek kiépítésének, a gondolkodási funkcióknak, attitűdöknek, képességeknek, magatartás-, meggyőződésformálásnak az alapvető eszköze és legfontosabb törekvése az önszabályzó tanulás kialakítására”.[4] A *Közszolgálati Online Lexikon*ban található, Benedek András meghatározása alapján az oktatás „a tanulásra, a tartós tudásra, az ismeretek megszerzésére, megértésére, alkalmazására irányuló, a tananyag ismertetését, közvetítését, magyarázatát, rendszerezését, rögzítését, ismétlését, ellenőrzését, értékelését eredményező rendszeres irányítás, folyamatszerű pedagógiai tevékenység”.[5] A képzésen

[4] Falus 2003.
[5] Benedek 2006: 201.

pedig „azt a tevékenységet értjük, amelynek során az elsajátított ismeretek gyakorlati alkalmazása révén kifejlesztjük az adott területen szükséges jártasságokat, készségeket és képességeket. A képzés az oktatáshoz, az oktatási folyamathoz szorosan kapcsolódó kategória, amely lehetővé teszi az oktatás sajátos funkciójának, céljának kifejezését". [6]

A fogalmi értékelések leginkább autentikus bázisát véleményem szerint a hatályos jogi szabályozás adja. A 2011. évi CCIV. törvény a nemzeti felsőoktatásról (Nftv.) szerint a felsőoktatási intézményben folyó, egymásra épülő, felsőfokú végzettségi szintet biztosító képzési ciklusok az alapképzés, a mesterképzés és a doktori képzés. Emellett a felsőoktatási intézmény a 2013. évi LXXVII. törvény a felnőttképzésről (Fktv.) alapján tarthat – felsőfokú végzettséget nem biztosító – felsőoktatási szakképzést és szakirányú továbbképzést is. A felnőttképzési törvény megfogalmazásában a belső képzés „a munkáltató által saját munkavállalói részére saját munkaszervezetén belül, a munkáltató beszállítóinak munkavállalói részére vagy partner-, vagy kapcsolódó vállalkozások munkavállalói részére nem üzletszerűen szervezett képzés". A szakképzés fogalmát a 2019. évi LXXX. törvény a szakképzésről az alábbiakban adja meg: „a szakképzés felsőfokú szakképzettséget nem igénylő munkakör betöltéséhez vagy tevékenység végzéséhez szükséges a) szakmára felkészítő szakmai oktatás és b) szakképesítésre felkészítő szakmai képzés". Szakképzés a szakmajegyzékben való nyilvántartás, képzési és kimeneti követelmények, valamint szakmai program, programkövetelmény alapján végezhető, vizsgáztatást pedig az akkreditált szakképzési vizsgaközpont végezhet.

Az iparbiztonsági felsőoktatási képzések vizsgálata

Az iparbiztonsági felsőoktatás területén a Nemzeti Közszolgálati Egyetem (NKE) kiemelt szerepet tölt be hazánk közigazgatási felsőoktatásában. Az NKE Rendészettudományi Kar Katasztrófavédelmi Intézete (KVI) megfelelő számú, kiváló szakmai felkészültségű közszolgálati szakembert biztosít a magyar államigazgatás és önkormányzati igazgatás számára, akik tanulmányaik végeztével az egymásra épülő alapképzési és mesterképzési végzettséggel, illetve doktori PhD-fokozattal rendelkeznek.

Az NKE-n létesített és indított felsőoktatási szakok kurzusainak közös célja, hogy azonos alapértékek mentén szocializálják a közszolgálati, rendvédelmi, védelmi és biztonsági igazgatási pályára készülőket, és megkönnyítsék a különböző biztonsági szakterületek közötti mindennapi együttműködést.[7]

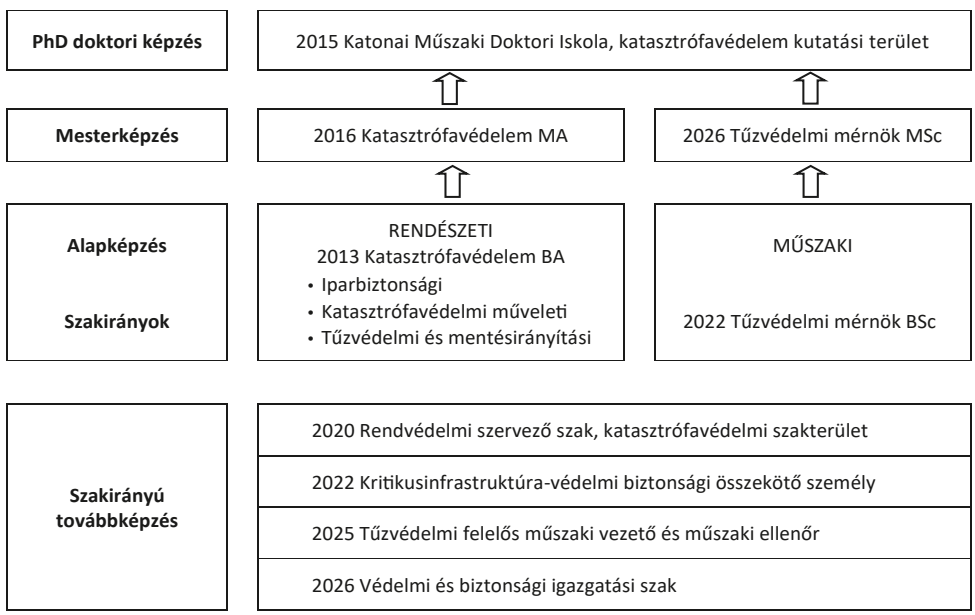
A KVI felsőoktatási képzéseinek célja, hogy a végzettek képesek legyenek az általános katasztrófavédelmi hatósági és egyéb szakfeladatok ellátására, különös tekintettel a katasztrófák megelőzésére, veszélyhelyzeti tervezésre, a katasztrófavédelem megszervezésére és műveleti feladatok ellátására, a helyreállítás, a polgárivédelem-felkészítés és a lakosságvédelem feladatainak végrehajtására. További kiemelt célkitűzés a hallgatók felkészítése a tüzek káros hatásai elleni védekezés keretében a tűzmegelőzési hatósági, a tűzoltási és műszaki mentési, a tűzvizsgálati, valamint az iparbiztonsággal kapcsolatos megelőzési, felkészítési, kárelhárítási és hatósági

[6] Benedek 2006: 198.
[7] Vass 2017.

feladatok ellátására. A végzettektől elvárás, hogy szakfeladataikat önállóan, megfelelő irányítás alatt végezzék, ugyanakkor jogosultak legyenek mesterszintű képzésre, valamint a megfelelő gyakorlati tapasztalat után vezetői feladatok ellátására is. Általánosságban kijelenthetjük, hogy a katasztrófavédelmi szervezetek szerepe a mai kihívásokkal teli világban egyre nagyobb elismerést kap, ami a képzési programok folyamatos fejlődésében is megnyilvánul.

A KVI oktatási tevékenysége bolognai rendszerben folyik, ahol a hallgatók a 6 féléves alapképzés elvégzése után 4 féléves mesterképzésben folytathatják tanulmányaikat. A katasztrófavédelem jogi és igazgatási jellegű alapképzése 2013 óta zajlik az NKE-n. A katasztrófavédelem alapképzés választható szakirányai: katasztrófavédelmi műveletek, tűzvédelmi és mentésirányítás, valamint iparbiztonság. A nappali és levelező tagozatos képzést az egyetemen 2012–2019 között önálló karközi intézetként, majd a Rendészettudományi Kar oktatási egységeként működő KVI szervezi. A három specializációnak megfelelően három szaktanszék foglalkozik az alapképzési szak oktatási tevékenységének szervezésével és lebonyolításával. A KVI és a BM Országos Katasztrófavédelmi Főigazgatóság (BM OKF) közötti jogviszony a két intézmény együttműködési megállapodásán alapul. A KVI által folytatott oktatás szakmai és személyzeti támogatását a BM OKF biztosítja, ami nagyban hozzájárul az oktatási és kutatási tevékenység további gyakorlatorientált fejlesztéséhez.[8]

Az 1. ábra mutatja be részletesen a KVI által gondozott szakok egymásra épülését, amely tartalmazza a szakok indításának időpontját is.



1. ábra: A KVI felsőoktatási portfóliója
Forrás: a szerzők szerkesztése

[8] Vass – Kátai-Urbán 2022.

A KVI által gondozott alap- és mesterképzési szakok két irányra oszlanak: az államtudományi képzési területben található rendészeti felsőoktatási területre, valamint a műszaki képzési területre. Az előbbi részei a következők: az államtudományi és közigazgatási felsőoktatási, a katonai, a nemzetbiztonsági, a nemzetközi és európai közszolgálati és a rendészeti felsőoktatási területek. A szakok KKK-inak utolsó megújítására 2023-ban került sor, amikor az NKE részt vett az RRF-2.1.1-21-2022-00001 azonosítószámú, *A felsőoktatási képzések ágazati modernizációja* című projektben. E munka keretében az államtudományi képzési terület alap-, osztatlan és mesterképzések KKK-inak megújítása valósult meg.[9] Az új KKK kiadása magával vonta többek között a rendészeti felsőoktatási szakok, így a katasztrófavédelem alap- és mesterképzés KKK-inak a felülvizsgálatát is, amelynek alapja a Magyar Képesítési Keretrendszer, illetve az Európai Képesítési Keretrendszer 6. szintjéhez tartozó kritériumok vizsgálata volt. Az egyik legfontosabb cél a tanulmányieredmény-specifikus KKK kialakítása, amelynek alapján megtörtént a képzéseken szerezhető kompetenciák felülvizsgálata (tudás, képesség, attitűd, autonómia és felelősség) is. Fontos volt továbbá a Kreatív Tanulási Program elemeinek a figyelembevétele is. Az előkészítő munka eredményeként a katasztrófavédelem alap- és mesterképzések KKK-i megjelentek az államtudományi képzési terület képzéseiről szóló 534/2023. (XII. 5.) Korm. rendeletben (KKK-rendelet).

A katasztrófavédelem alapképzési szakon végzettek a hivatásos katasztrófavédelmi szerveknél, az önkormányzati és létesítményi tűzoltóságoknál, az önkéntes tűzoltó egyesületeknél, valamint az ez irányú szakágazatokban foglalkoztatottak szakmai képesítési követelményeiről és szakmai képzéseiről szóló 9/2015. (III. 25.) BM rendelet szerint katasztrófavédelmi, polgári védelmi, hatósági, iparbiztonsági szakterületen felső szintű szakmai képesítést szereznek, de így van ez a gazdálkodó szervezetek vonatkozásában a katasztrófa- és polgári védelem szakágazatok esetében is. A tűzoltósági és ügyeleti szakterületen viszont felső szintű szakmai képesítést akkor biztosít a képzés, ha a végzett személy rendelkezik legalább középszintű tűzoltás, műszaki mentés vezetésére jogosító végzettséggel.

A hatályos iparbiztonsági jogi szabályozásban a következő képesítési jogosultságoknak és követelményeknek megfelelő képzések szerepelnek:

- A veszélyes üzemek létesítésével és üzemeltetésével kapcsolatos iparbiztonsági üzemeltetői és hatósági feladatok teljesítése, mégpedig a 219/2011. (X. 20.) Korm. rendelet a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről 7. melléklet 6. pont szerinti biztonsági dokumentációt készítő szervezettel és a veszélyes ipari védelmi ügyintézővel szemben támasztott képzési követelmények alapján. A hatósági területen a végzettek ismerik a kémiai biztonság, a biztonsági dokumentációk vizsgálatával és minősítésével, a veszélyeztetettségelemzéssel, a védelmi tervezéssel, a lakossági tájékoztatással és a településrendezéssel kapcsolatos eljárási és módszertani kompetenciákat.
- A veszélyes áruk szállításával kapcsolatos iparbiztonsági szakértői és hatósági tevékenység, mégpedig a veszélyes áru szállítási biztonsági tanácsadóról szóló 25/2014. (IV. 30.) NFM rendelet által előírt veszélyesáru-szállítási biztonsági tanácsadó alkalmazási kötelezettsége alapján. A vasúti szállítási biztonsági

[9] Christián–Keresztes 2024.

tanácsadói oktató alapképzési végzettség, amelyet a vasúti közlekedés biztonságával összefüggő munkakört betöltő munkavállalók szakmai képzésének és vizsgáztatásának, a vasúti vizsgaközpont és képzőszervezetek működésének, a képzési engedély kiadásának, továbbá a vasúti járművezetői gyakorlat szabályairól szóló 19/2011. (V. 10.) NFM rendelet 1. melléklete szerinti tevékenységet végzőknek kell megszerezni. A hatósági szakterületen a veszélyes áru közúti szállítási katasztrófavédelmi ellenőr szakképzettség megszerzése szükséges, amelyet vezetői szinten kiegészít a biztonsági tanácsadói végzettség megszerzésének az igénye is.[10]

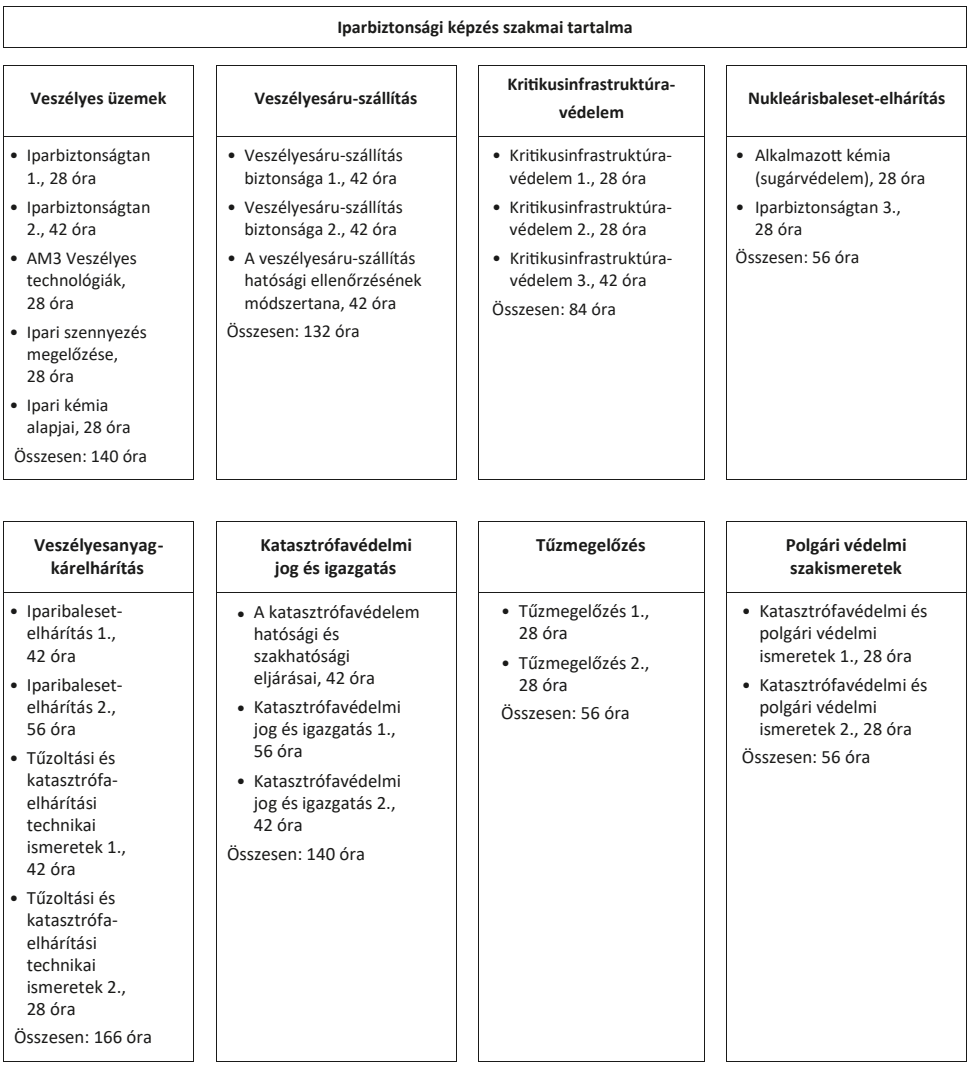
- A kritikus szervezetek ellenálló képességét biztosító feladatok végrehajtása: a kritikus szervezet ellenálló képességéért felelős vezetői beosztást a kritikus szervezetek ellenálló képességéről szóló 2024. évi LXXXIV. törvény (Kszetv.) 20. §-a alapján kell létesíteni, amelyet felsőoktatási intézmény kritikusinfrastruktúra-védelmi biztonsági összekötő személy szakirányú továbbképzési szakán lehet megszerezni. Az ellenálló képességért felelős vezető rendszeres továbbképzésére vonatkozó szabályokról szóló 59/2024. (XII. 3.) BM rendelet határozza meg a továbbképzés szabályait, amelyet a Katasztrófavédelmi Oktatási Központban (KOK) végeznek. A hatósági feladatokat ellátóknak célszerűen a fenti követelményeken túl megfelelő speciális hatósági feladatellátásra is fel kell készülni.
- A nukleárisbaleset-elhárítási szakfeladatok ellátása: A sugárvédelmi szakemberek képesítési követelményeit az ionizáló sugárzás elleni védelemről és a kapcsolódó engedélyezési, jelentési és ellenőrzési rendszerről szóló 2/2022. (IV. 29.) OAH rendelet 19. §-a írja elő. A képzés alap, bővített vagy átfogó fokozatú szaktanfolyamokon történik. A hatósági szakembereknek beosztástól függően bővített vagy átfogó szintű tanfolyami végzettség megszerzése indokolt.

A Katasztrófavédelem alapképzési szak KKK-jának megfelelően lett kimunkálva az a mintatanterv is, amelynek fontos része a tantárgyi programok leírása. A tantárgyi programokat két csoportra oszthatjuk: az első a törzsanyag tantárgyai, a második pedig a szakirányi ismeretek tantárgyai. A képzés törzsanyagához tartozó tárgyak csoportjai az államtudományi képzési területen minden egyes alapképzésben megtalálható Ludoviceum tantárgyak, a jogi és igazgatás jellegű tantárgyak és a katasztrófavédelmi alapozó tantárgyak.

Az alapozó képzések keretében a hallgatók elsajátítják többek között az iparbiztonsági szaktantárgyak megalapozásához szükséges természettudományi és műszaki alapismereteket is. A hatósági tevékenységhez a jogi és igazgatási ismeretek, míg a veszélyes anyagok azonosításához az alkalmazott kémia tantárgy ismerete elengedhetetlen.

A képzés gyakorlati jellegét, illetve a tudás és képesség kompetenciáinak alapját az iparbiztonsági szakirány szaktantárgyai adják, amelyek iparbiztonsági szakterületek szerinti felosztását a 2. ábra szemlélteti.

[10] Almási 2023.



2. ábra: Az iparbiztonsági képzés szakmai tartalma
Forrás: a szerzők szerkesztése

A 2. ábrán látható katasztrófavédelmi jogi és igazgatási tantárgyak, a tűzmegelőzési ismeretek és a polgári védelmi szakismeretek közvetlenül befolyásolják az iparbiztonság négy fő szakterületének képzési környezetét. Ugyanez mondható el a veszélyesanyag-károrelhárítási tantárgyakra is, amelyek között a tűzoltási és a katasztrófaelhárítási technikai ismeretek tantárgyak mellett megtalálhatjuk az iparibaleset-elhárítási tárgyakat is. Utóbbiak jelentik az iparbiztonsági szakterületek balesetelhárítási és károrelhárítási kapcsolódási pontjait is.

Az iparbiztonsági szakirányon tanuló hallgatók gyakorlati képzését az első és a második évfolyamokon lebonyolított szakmai gyakorlat jelentős mértékben támogatja. A nappali képzési rendben tanuló hallgatók lehetnek tűzoltó tisztjelöltek és állami ösztöndíjas vagy önköltséges képzésben részt vevő civil hallgatók. Fontos megállapítani, hogy az iparbiztonsági hatósági hatás- és feladatkörök miatt a kormányhivatali szervezeteknél is javasolt szakmai gyakorlatot szervezni a hallgatóknak. A BA-képzés tantárgyainak integrálása mellett a katasztrófavédelem mesterképzés kiterjeszti a hallgatók alapképzés során megszerzett tudását és képességeit, ahol a képző szervezet különös figyelmet fordít a katasztrófavédelmi vezetői képességek és készségeik fejlesztésére.

A KKK-rendelet tartalmazza a Katasztrófavédelem mesterképzési szak KKK-ját is. A végzettek okleveles katasztrófavédelmi vezető szakképzettséget kapnak, amely a 9/2015. (III. 25.) BM rendelet szerint katasztrófavédelmi, polgári védelmi, hatósági, iparbiztonsági szakterületen felső szintű szakmai képesítésnek felel meg. A gazdálkodó szerveztek vonatkozásában továbbá a katasztrófa- és polgári védelem, illetve a tűzvédelmi szakágazatok esetében is felső szintű szakmai végzettségnek számít. A tűzoltósági és ügyeleti szakterületen viszont a felső szintű szakmai képesítést akkor biztosítja a képzés, ha a végzett személy rendelkezik legalább középszintű tűzoltás, műszaki mentés vezetésére jogosító végzettséggel.

A katasztrófavédelem mesterképzési szak tantárgyait két csoportra oszthatjuk. A törzsanyag kurzusai között műszaki alapozó, humánpolitikai és vezetési, valamint a katasztrófavédelem jogi, szervezeti és intézkedési rendszerével foglalkozó tantárgyakat különböztethetünk meg. A differenciált szakmai ismeretek tantárgyak a katasztrófavédelem három fő szakterületéhez tartozó kurzusokat mint záróvizsgatantárgyakat foglalják magukba. Emellett a katasztrófavédelem funkcionális (logisztikai, nemzetközi és egészségügyi) szakmai feladataihoz tartozó kurzusokat is megkülönböztethetünk. A szabadon választható tantárgyak főként a tudományos kutatás és az angol nyelvű szakmai ismeretek ismeretanyagára koncentrálnak.

A katasztrófavédelem mesterképzésen belül levelező képzési rendben csak szűkített program szerint lehet főként rendszertani ismereteket közvetíteni a hallgatók felé. Az iparbiztonság 1. és az iparbiztonság 2. tantárgy az iparbiztonsági feladatokat érintő vezetési és irányítási feladatok eljárási és módszertani ismereteit tartalmazza. Ezen túl a képzésben van még két szabadon választható, főként elméleti ismereteket tartalmazó angol nyelvű iparbiztonsági tantárgy is.

A mesterképzés elvégzése után a legtehetségesebb hallgatók folytathatják doktori PhD-képzésüket az NKE Katonai Műszaki Doktori Iskolájában, amelynek 2015 óta működő katasztrófavédelem-kutatási területén 52 fő szerzett tudományos fokozatot.

A KVI szakirányú továbbképzési szakokat indított, amelyek közül iparbiztonsági szempontból a kritikusinfrastruktúra-védelmi biztonsági összekötő szakirányú továbbképzési szak emelhető ki. 2022 februárjában a BM OKF kezdeményezésére a KVI speciális, két féléves iparbiztonsági szakirányú továbbképzést indított a kritikus infrastruktúrák létesítményeinek és szolgáltatásainak biztonsága és védelme érdekében az érintett gazdálkodó szervezetek és államigazgatási szervek biztonsági szakemberei, többek között felső vezetői részére. A képzés a Kszetv. és a védelmi és biztonsági tevékenységek összehangolásáról szóló 2021. évi XCIII. törvény (Vbö. tv.)

jogalkalmazási ismereteinek feldolgozására szolgál. A kritikusinfrastruktúra-védelmi biztonsági összekötő személy szakképzettséget szerző végzettek felhatalmazást kapnak a Kszetv. és Vbö. törvény hatálya alá tartozó kritikus szervezeteknél úgynevezett ellenálló képességért felelős vezetői munkakör betöltésére.

Az előzőekben bemutatott elemzés tartalma alapján kellő bizonyossággal kijelenthetjük, hogy a KVI a 2012-es megalakulása óta elsődleges szerepet tölt be hazánkban a katasztrófavédelmi szakemberek felsőoktatási képzésében.[11]

A tűzvédelmi mérnökképzés iparbiztonsági mérnöki kompetenciáinak vizsgálata

A KVI 2017-ben megkezdte azoknak az oktatási és intézményfejlesztési intézkedéseknek a végrehajtását, amelyek elengedhetetlenek a tűzvédelmi mérnök alapképzés alapításához és elindításához. A képzés létesítése az alábbi képesítési jogkörökhöz kötött mérnöki (műszaki) tevékenység végzéséhez szükséges szakképzettség megszerzésére irányul:

- az építésügyi tűzvédelmi tervezői tevékenység folytatásához szükséges tűzvédelmi mérnöki felsőoktatási végzettség (tervezési jogosultság) megszerzését megalapozó ismeretek elsajátítása;
- a tűzvédelmi szakértői tevékenység végzéséhez szükséges ismeretek megszerzése a tűzvédelmi szakterületeken (építmények tűzvédelme, tűzoltó technikai eszközök, ipari tűzvédelem, tűzvizsgálat);
- a beépített tűzvédelmi berendezések tervezőire és kivitelezőire vonatkozó tűzvédelmi szakvizsga bizonyítvány megszerzéséhez kapcsolódó képesítési követelménynek való megfelelőség biztosítása;
- a gazdálkodó szervezetek tűzvédelmi szakágazataiban foglalkoztatott felsőfokú szakképesítéshez kötött katasztrófavédelmi, polgári védelmi, iparbiztonsági és tűzvédelmi beosztásokhoz tartozó műszaki tervezési, szervezési, elemzési és értékelési feladatok végrehajtása;
- a katasztrófavédelem tűzoltósági és ügyeleti szakterületén, az önkormányzati, a létesítményi tűzoltóságok, az önkéntes tűzoltó egyesületek tűzvédelmi szakbeosztásaiban végrehajtandó műszaki mérnöki feladatok ellátása.[12]

A szak a műszaki képzési terület alapképzései közé tartozik, amelyet a felsőoktatásban szerezhető képesítések jegyzékéről és az új képzések létesítéséről szóló 65/2021. (XII. 29.) ITM rendelet vett a szakképzettségek jegyzékébe. Az alapképzésekkel kapcsolatos európai követelményeket az úgynevezett ESCO- (European Skills, Competences, Qualifications and Occupations – készségek, kompetenciák, képesítések és foglalkozások) kompetencialeírások tartalmazzák. A képzési szakokkal szembeni fő elvárás az igényvezérelt képzés, a gyakorlatorientáltság és a rugalmas képzési szerkezet.[13]

[11] Kátai-Urbán – Varga – Vass 2023.
[12] Cséplő – Kátai-Urbán – Vass 2018.
[13] Bihari 2024.

A katasztrófavédelmi képzés műszaki feltételeinek és a hallgatók elhelyezési igényeinek kielégítését az NKE Ludovika Campuson létesítendő Katasztrófavédelmi Speciális Képzési Központ (KSKK) keretében tervezik. Az egyetem központi komplexuma ad majd otthont a KVI-nek, így az önálló működés feltételei a tervek szerint rendelkezésre fognak állni.

A tűzvédelmi mérnök alapképzésben összesen hét iparbiztonsági szaktantárgy szerepel, amelyek többségében egy-egy iparbiztonsági alapképzési tantárgynak felelnek meg összevont formában.

A tűzvédelmi mérnök alapképzést követi a tűzvédelmi mérnöki mesterképzés, amely a 2026–2027-es tanévben kezdődik meg két féléves levelező képzési rendben, és okleveles tűzvédelmi mérnök szakképzettséget ad. A szakon végzett szakemberek tűzvédelemmel foglalkozó gazdálkodó szervezeteknél, kormányhivataloknál, önkormányzatoknál és katasztrófavédelmi szervezeteknél fognak tudni elhelyezkedni. A szak ajánlott tanterve a tűzvédelmi mérnöki szakterület mesterszintű ismereteit tartalmazza, különös tekintettel a komplex tűzvédelmi menedzsmentre, az okosvárosok tűzvédelmére, a teljesítményalapú tűzvédelmi tervezésre, a kutatásmódszertanra, a digitális tervezési eszközök, mint például a BIM (*building information modeling* – épületinformációs modellezés) alkalmazására, a mesterséges intelligencia és az adatelemzés lehetőségeire.

A szak létesítése és indítása egyszerűsített rendben történik az Nft. szerint, amely alapján a hatályos intézményakkreditációval rendelkező felsőoktatási intézmény a KKK-t és az ajánlott tantervet szabadon készíti el azon a képzési területen, ahol korábban az alapképzés folytatására már jogosultságot szerzett. Az iparbiztonsági mérnöki kompetenciákhoz elsősorban a veszélyes technológiák tűzvédelme tantárgy kapcsolható, amelynek célja a hallgatók felkészítése az ipari létesítményekben alkalmazott, különleges kockázatot jelentő technológiák tűzvédelmi tervezésére. Ennek keretében foglalkoznak a tűz- és robbanásvédelmi kockázatok elemzésével, a robbanásveszélyes zónák besorolásával, a kapcsolódó tűzvédelmi dokumentáció elkészítésével, valamint a folyamatbiztonsági kockázatok értékelésével.

A tűzvédelmi mérnök alap- és mesterképzések tekintetében több korszerű mérnöki módszer is helyet kaphat, mint például a mesterséges intelligencia alkalmazása, különös tekintettel az intelligens észlelésre, a generatív tervezési optimalizációra és a hibrid szimulációs eljárások alkalmazására.[14]

Iparbiztonsági szakképzés és felnőttképzés Magyarországon

Magyarországon az iparbiztonsági szakképzés összekapcsolódik a KOK szervezeti fejlődéstörténetével, valamint az egységes és integrált katasztrófavédelmi szervezet kialakulásával. Az első katasztrófavédelmi törvény alkalmazásával a polgári védelmi képzések integrálódtak a KOK szakképzési tevékenységébe, majd a második katasztrófavédelmi törvény hatálybalépésével átalakult a tűzvédelmi képzési rendszer is a rendvédelmi moduláris képzési rendszer kialakulásával együtt. Az utóbbit befolyásolta

[14] Tóth et al. 2026.

az iparbiztonsági szakterület 2012. évi létrejötte, amely igényelte a vonatkozó szakképzések létrehozását is. A tűzoltó szakképzés az V. modulból tevődött össze (egységes rendvédelmi alapozó, tűzoltó II. és I. tűzoltó szerparancsnok, tűzoltósági referens).

A felső szintű szakmai képesítést nyújtó rendészeti szervező képzés keretében olyan hárommodulos képzést alakítottak ki, ahol a rendvédelmi alapozó modulra épült a katasztrófavédelmi közös modul, továbbá a szakmairányok moduljai a tűzvédelmi, a katasztrófavédelmi és az iparbiztonsági szakmairányokkal. A képzés az Országos Képzési Jegyzék szerint nyilvántartott oklevelet is adott. Az iparbiztonsági elágazás keretében a hallgatók az iparbiztonsági szakterületeken ellátandó hatósági és katasztrófavédelmi feladatokra készülnek fel. Ebben az időszakban indultak el olyan iparbiztonsági szaktanfolyamok, mint a katasztrófavédelmi mobil labor (KML) képzés, a veszélyesáru-szállítási ellenőri képzések a vasúti, belvízi, légi és közúti szállítási ágazatokban, továbbá a veszélyesáru-szállítási biztonsági tanácsadó képzés.

A 2021-től induló új szakmai képzési szerkezetben nyolcféle képzés található: tűzoltó, tűzoltó szerparancsnok, katasztrófavédelmi tisztképző, tűzvédelmi előadó, tűzvédelmi főelőadó, katasztrófavédelmi munkatárs (polgári védelmi és iparbiztonsági), katasztrófavédelmi ügyintéző (polgári védelmi és iparbiztonsági), kéményseprő. A felnőttképzés keretében a szakmai képzésekhez engedélyre, míg a belső képzésekhez bejelentésre volt szükség. Az új rendszerben elvált egymástól a képzés és a vizsgáztatás. Az utóbbi feladatokat a BM OKF-en működő Katasztrófavédelmi Vizsgaközpont látja el.[15]

A belső képzések közé tartoznak a veszélyesáru-szállítási ellenőröket felkészítő kurzusok, ezen belül a veszélyes áruk vasúti, belvízi, közúti, légi és tengeri szállítási katasztrófavédelmi ellenőröket képzők, valamint a KML-tanfolyam. A katasztrófavédelmi technikai eszközök kezelőinek képzései közül a műszaki mentő és vegyibaleset-elhárító gépjárműkezelői típustanfolyam, a vegyibaleset-elhárítás gépeit, berendezéseit kezelők típustanfolyama minősül iparbiztonsági tanfolyamnak.[16]

A KOK biztosítja az NKE KVI részére a KML-képzéshez, a vegyi és a sugárfelderítéshez, illetve az alkalmazott kémia laboratóriumi gyakorlati foglalkozásokhoz a képzési helyszínt és az oktatási eszközöket. A KOK az iparbiztonsági szabályozással érintett gazdálkodó szervezetek szakemberei részére időközönként veszélyes ipari védelmi ügyintéző és biztonsági összekötő személy képzéseket is indított.

A felnőttképzéssel foglalkozó civil képző szerveztek iparbiztonsági szempontból veszélyes ipari védelmi ügyintézői, veszélyesáru-szállítási ügyintézői és tanácsadói, biztonsági összekötő személy és sugárvédelmi szaktanfolyamokat indítottak.

Az iparbiztonsági gyakorlati képzések műszaki-technikai feltételeinek elemzése

A KVI katasztrófavédelmi és tűzvédelmi mérnöki felsőoktatási tevékenységét a 2026–2027-es tanév indításától az újonnan létesült KSKK fogja folytatni.

[15] Papp 2023.
[16] Papp 2021.

A veszélyesanyag-kárelhárítási képzés tulajdonképpen az iparbiztonsági szakterület kurzusaihoz tartozó műszaki-technikai feltételek biztosítása mentén fog tudni megfelelni a KKK-nak és a mintatantervekben rögzített képzési követelményeknek.

Az iparbiztonsági szaktantárgyak szakmai gyakorlati foglalkozásaihoz kapcsolódó módszertani és műszaki-technikai feltételek biztosításához kurzusonként fel kell mérni az egyes gyakorlati képzéshez szükséges műszaki-technikai eszközrendszert, amely a környezeti kockázatok felmérésére, az egyes események káros következményeinek elemzésére, illetve azok kezelésére épül.[17] Az ipari és környezeti katasztrófahelyzetek felszámolása a védekezés valamennyi időszakában a vezetés és az irányítás szoros összehangolását, az üzemeltetők hatóságokkal történő együttműködését, és komplex infokommunikációs rendszer létrehozását és működtetését igényli,[18] ezért az oktatásban és a képzésben alkalmazott módszereknek a valóságot visszatükröző magas műszaki tartalommal és gyakorlati képzési elemekkel kell rendelkezniük.

A katasztrófavédelmi és a tűzvédelmi alapképzésben az alkalmazott oktatási módszer szerint az alábbi gyakorlati foglalkozástípusokat lehet elkülöníteni:

- A laboratóriumi gyakorlatokat az alkalmazott kémia oktatásához szükséges megszervezni, amelyeket a KSKK tűzvédelmi laboratóriumában lehet megtartani. A hallgatók által elkészített eredménytermék ebben az esetben a laboratóriumi jegyzőkönyv.
- A számítási feladatokat jelentős számú gyakorlati foglalkozás esetén kell alkalmazni az iparbiztonsági szakfeladatok műszaki jellege miatt. A hallgatók számítási gyakorlati jegyzőkönyvet készítenek a foglalkozások keretében.
- A számítási gyakorlatok kiemelt formája a kockázat- és következményelemző szoftverek alkalmazása, amelyhez számítógépes infrastruktúra is szükséges.
- A szemináriumok szintén gyakorlati jellegű foglalkozások, amelyek valamely iparbiztonsági témakör elméleti anyagának egyéni vagy csoportos feldolgozására irányulnak, és ahol a hallgatók feladatlapokat töltenek ki.
- Az oktatás során kiemelt szerepet kapott a külső helyszíneken történő szakmai látogatások előkészítése és lebonyolítása, amelyek iparbiztonsági szakterületenként eltérők lehetnek, mégpedig:
  - veszélyes üzemekhez szervezett látogatások, amelyeket a közös tantárgynak számító veszélyhelyzeti ismeretek és szakmai alapismeretek tantárgyaknál külső helyszínen lehet megtartani. Az üzemlátogatások helyszínei: vegyipari, kőolaj- és gázipari, veszélyes anyaggal foglalkozó, radiológiai vagy nukleáris tevékenységgel foglalkozó üzem, valamint hőerőmű és gyógyszergyár.
  - A veszélyesáru-szállítás biztonsága tantárgyak keretében közúti, vasúti és légi szállítási hatósági ellenőrzési gyakorlatokon történő részvétel is be van tervezve, amelyeket az iparbiztonsági hatósággal egyeztetett módon szintén külső helyszínen tartunk.
  - Kritikusinfrastruktúra-védelem tantárgy esetében a katasztrófavédelem központi szerve által működtetett Iparbiztonsági Eseménykezelő Központ

[17] Kátai-Urbán et al. 2024.
[18] Farkas 2016.

bejárása, valamint a kritikusinfrastruktúra-üzemeltetőknél történő szakmai látogatások.
– A nukleáris balesetelhárítás vonatkozásában, a nukleáris létesítményekben és izotóplaboratóriumokban történő látogatások szervezése jelenthet fontos gyakorlati tapasztalatot a hallgatóknak.

A külső helyszíni szakmai látogatásokról a hallgatók beszámolót készítenek. A veszélyesanyag-kárelhárítási tevékenység területén a technológiai fejlődéssel együtt járó kemizáció következtében a hatósági tevékenység mellett kiemelt szerepet kap a műszaki szemlélet, amely különösen a veszélyesanyag-káreseményeknél végzett helyzetértékeléseknél kaphat szerepet.[19] Az ipari balesetelhárítás tantárgyak esetében fontos szempont a radiológiai, a biológiai és a vegyi (RBV) felderítési, mintavételi eszközök és mérőműszerek használatának elsajátítása, amely történhet gyakorlati foglalkozás keretében az Iparbiztonsági Eseménykezelő Kabinetben vagy gyakorló KML-szerrel a gyakorlótéren. A veszélyesanyag-kárelhárítási gyakorlat helyszíne szintén a gyakorlótér.

A KSKK-n belül az Iparbiztonsági Eseménykezelő Kabinet lesz a legfontosabb szakmai oktatási helyszín, amelynek alapvetően négy képzési és oktatási funkciója lehet:

- *Iparbiztonsági kockázat- és következményelemző alkalmazások funkció:* a civilizációs katasztrófák megelőzését célzó kockázat- és következményelemzési számítógépes rendszer alkalmazásának gyakorlóhelye.
- *Iparbiztonsági eseménykezelő funkció:* az iparbiztonsági szakmai és hatósági jogalkalmazási feladatok végrehajtásánál felhasznált, mérnöki módszereken és eljárásokon alapuló prognóziskészítő szimulációs rendszerek megelőzési, felkészülési és baleset-elhárítási célú alkalmazása, valamint a veszélyesanyag-kárelhárítási műszaki-technikai eszközök alkalmazásának biztosítása.
- *A telepített veszélyesanyag-monitoringrendszer alkalmazásának funkciója:* a katasztrófavédelem telepített veszélyesanyag-monitoringrendszereihez tartozó, vezetői döntéstámogató alkalmazások oktatási verzióinak felhasználása.
- *Mobil veszélyesanyag-felderítő eszközök és műszerek (műszerterem) funkció:* Itt kapnak helyet az iparbiztonsági események kezelésénél felhasznált vegyi és sugárzóanyagok felderítésének oktatási eszközei és műszerei is.

Következtetések

Az iparbiztonsági felsőoktatás, képzés és továbbképzés rendszerének vizsgálata során az alábbi főbb következtetések vonhatók le:

- Az iparbiztonság rendszere a katasztrófavédelem létrejöttének és fejlődésének időszakában épült ki véglegesen, az ehhez kapcsolódó oktatási és képzési rendszer az NKE bázisán kialakult katasztrófavédelmi és tűzvédelmi mérnöki képzés központjában fejlődhet tovább. A tanulmányban elvégzett fogalmi

[19] Nagy 2024.

értékelés hozzájárulhat az iparbiztonsági oktatás, képzés, illetve továbbképzési rendszer és képzési portfólió vizsgálatához.

- Az oktatás és a képzés bázisa a KVI, ahol várhatóan műszaki technikai jellegű fejlődést jelentő eredményeket fog hozni a Katasztrófavédelmi Speciális Képzési Központ létesítményeinek kiépítése és alkalmazása.
- A KKK-k gyakorlati képzéséhez tartozó iparbiztonsági tudás és képesség követelményeit érintő technikai feltételek teljes mértékben a KSKK által nyújtott eszközökkel és szolgálatásokkal biztosíthatók az átadást követő években.
- Az iparbiztonsági gyakorlati képzések műszaki-technikai feltételeinek fejlesztése területén négy fő funkció létrehozása szükséges, ahol a kockázat- és következményelemző alkalmazás funkcióra épül az iparbiztonsági eseménykezelő, a telepített veszélyes anyag monitoringja, valamint a gyakorló katasztrófavédelmi mobil laboratóriumi képzési funkció.

Felhasznált irodalom

Almási, Csaba Sándor (2023): Evolution of the Regulation of the Transport of Dangerous Goods by Road. *Műszaki Katonai Közlöny,* 33(2), 113–122. Online: https://doi.org/10.32562/mkk.2023.2.9

Bihari Péter (2024): A műszaki képzési terület újításai. In Tolnai Ágnes (szerk.): *Felsőoktatási képzések ágazati modernizációja.* Budapest: Magyar Felsőoktatási Akkreditációs Bizottság, 69–74. Online: www.mab.hu/wp-content/uploads/a_felsooktatasi_kepzesek_agazati_modernizacioja.pdf

Christián László – Keresztes Judit (2024): Képzések átalakítása az államtudományi képzés területén. In Tolnai Ágnes (szerk.): *Felsőoktatási képzések ágazati modernizációja.* Budapest: Magyar Felsőoktatási Akkreditációs Bizottság, 60–68. Online: www.mab.hu/wp-content/uploads/a_felsooktatasi_kepzesek_agazati_modernizacioja.pdf

Cséplő Zoltán – Kátai-Urbán Lajos – Vass Gyula (2018): A tűzvédelmi mérnöki képzéshez szükséges szakmai feltételek vizsgálata. *Hadmérnök,* 13(1), 153–167. Online: www.hadmernok.hu/181_12_cseplo.pdf

Falus Iván szerk. (2003): *Didaktika. Elméleti alapok a tanítás tanulásához.* Budapest: Nemzeti Tankönyvkiadó.

Farkas Tibor (2016): A katasztrófavédelmi és válságkezelési tevékenységek általános elemzése az irányítás és az infokommunikációs támogatás tükrében. *Hadmérnök,* 11(3), 135–148. Online: http://hadmernok.hu/163_11_farkas.pdf

Kátai-Urbán Lajos – Vass Gyula – Cséplő Zoltán (2015): Iparbiztonsági képzés a Nemzeti Közszolgálati Egyetemen. *Védelem Online,* 22, 1–16. Online: www.vedelem.hu/letoltes/anyagok/727-iparbiztonsagi-kepzes-a-nemzeti-kozszolgalati-egyetemen.pdf

Kátai-Urbán, Lajos – Varga, Ferenc – Vass, Gyula (2023): Disaster Management Higher Education in Hungary. *Science for Population Protection,* 15(1), 51–57. Online: www.population-protection.eu/prilohy/casopis/46/406.pdf

Kátai-Urbán Maxim et al. (2024): A veszélyes üzemek környezeti kárelhárítási műszaki követelményeinek vizsgálata. *Hadmérnök,* 19(2), 63–76. Online: https://doi.org/10.32567/hm.2024.2.5

Nagy Rudolf (2024): Vegyi haváriák vizsgálata a kárterület kialakulásának tükrében. *Biztonságtudományi Szemle,* 6(4), 99–111. Online: https://doi.org/10.12700/btsz.2024.6.4.99
Papp Antal (2021): A szakképzés megújítása – napjaink változásai. *Katasztrófavédelmi Szemle,* 28(4), 14–18. Online: www.vedelem.hu/letoltes/ujsag/v202108.pdf?12
Papp Antal (2023): Iparbiztonsági képzések helyzete és fejlődésének iránya a KOK képzési rendszerében. *Védelem Tudomány,* 4(1), 83–98. Online: https://ojs.mtak.hu/index.php/vedelemtudomany/article/view/13304
Tóth, Rita et al. (2026): Integrating Artificial Intelligence (AI) Into Performance-based Fire Protection Design: Challenges, Methods and Vision. *Polgári Védelmi Szemle,* 18, 380–390. Online: https://mpvsz.hu/pv_szemlek/pvszemle2026/index.html?search=380
Vass Gyula (2017): Gondolatok a katasztrófavédelmi felsőoktatásról. *Védelem Tudomány,* 2(1), 188–203. Online: https://ojs.mtak.hu/index.php/vedelemtudomany/article/view/13078
Vass Gyula – Kátai-Urbán Lajos (2022): A katasztrófavédelmi felsőoktatási képzés fejlődése és jövője. *Belügyi Szemle,* 70(10), 2135–2152. Online: https://doi.org/10.38146/BSZ.2022.10.12

Jogi források

2011. évi CCIV. törvény a nemzeti felsőoktatásról
2013. évi LXXVII. törvény a felnőttképzésről
2019. évi LXXX. törvény a szakképzésről
2021. évi XCIII. törvény a védelmi és biztonsági tevékenységek összehangolásáról
2024. évi LXXXIV. törvény a kritikus szervezetek ellenálló képességéről
19/2011. (V. 10.) NFM rendelet a vasúti közlekedés biztonságával összefüggő munkakört betöltő munkavállalók szakmai képzésének és vizsgáztatásának, a vasúti vizsgaközpont és képzőszervezetek működésének, a képzési engedély kiadásának, továbbá a vasúti járművezetői gyakorlat szabályairól
219/2011. (X. 20.) Korm. rendelet a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről
25/2014. (IV. 30.) NFM rendelet a veszélyes áru szállítási biztonsági tanácsadóról
9/2015. (III. 25.) BM rendelet a hivatásos katasztrófavédelmi szerveknél, az önkormányzati és létesítményi tűzoltóságoknál, az önkéntes tűzoltó egyesületeknél, valamint az ez irányú szakágazatokban foglalkoztatottak szakmai képesítési követelményeiről és szakmai képzéseiről
65/2021. (XII. 29.) ITM rendelet a felsőoktatásban szerezhető képesítések jegyzékéről és az új képzések létesítéséről
2/2022. (IV. 29.) OAH rendelet az ionizáló sugárzás elleni védelemről és a kapcsolódó engedélyezési, jelentési és ellenőrzési rendszerről
534/2023. (XII. 5.) Korm. rendelet az államtudományi képzési terület képzéseiről
59/2024. (XII. 23.) BM rendelet az ellenálló képességéért felelős vezető rendszeres továbbképzésére vonatkozó szabályokról

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG

21. évfolyam (2026) 3. szám 105–117.
DOI: 10.32567/hm.2026.3.7

Földes Tibor[1]

A működésfolytonosság mint stratégiai képesség a kritikus infrastruktúrák védelmében

Continuity of Operations as a Strategic Capability for the Protection of Critical Infrastructures

Absztrakt

A kritikus infrastruktúrák védelme azért vált kiemelt biztonsági feladattá, mert például az energia-, a közlekedési és az informatikai rendszerek közötti függőségek ma már közvetlen, gyorsan terjedő zavarokat eredményezhetnek. A digitalizáció, a globális ellátási láncok sérülékenysége és a hibrid fenyegetések olyan környezetet teremtettek, ahol a működésfolytonosság biztosítása stratégiai jelentőségű. A működésfolytonosság-tervezés és annak kormányzati-honvédelmi megfelelője, a működés folytonossága olyan vezetési és operatív rendszerek összessége, amelyek biztosítják, hogy a kritikus szolgáltatások jelentős zavar esetén is fennmaradjanak. A NATO doktrínái a katonai működés biztonságos tervezési elveit határozzák meg, míg a NIST-keretrendszerek a civil és kiberbiztonsági folytonosság technikai standardjait rögzítik. A tanulmány bemutatja, hogyan egészítik ki egymást a NATO doktrinális iránymutatásai és a NIST technikai keretrendszerei a működésfolytonosság megteremtésében. Rámutat, hogy a működésfolytonosság-tervezés és a működés folytonossága nem kizárólag adminisztratív tevékenységként értelmezhető, hanem a szervezeti működés irányításának egyik alapvető eleme, amely a megelőzés, észlelés, reagálás és helyreállítás egységes rendszerére épül.

Kulcsszavak: biztonság, kritikus infrastruktúra, működésfolytonosság, stratégia

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

Abstract

The protection of critical infrastructures has become a priority security task because the dependencies between systems such as energy, transportation, and information technology can now result in direct and rapidly spreading disruptions. Digitalisation, the vulnerability of global supply chains, and the rise of hybrid threats have created an environment in which ensuring continuity of operations has strategic significance. Business continuity planning and its governmental–military counterpart, continuity of operations, represent a set of leadership and operational systems that ensure critical services remain functional even under significant disruption. NATO doctrines define the planning principles required for the secure continuation of military operations, while NIST frameworks establish the technical standards for civil and cybersecurity continuity. This study demonstrates how NATO's doctrinal guidance and NIST's technical frameworks complement each other in building resilience. It emphasises that business continuity planning and the continuity of operations cannot be interpreted solely as an administrative activity, but rather as a fundamental element of organisational governance, built on an integrated system of prevention, detection, response, and recovery.

Keywords: security, critical infrastructure, continuity of operations, strategy

Bevezetés

A kritikus infrastruktúra fogalma alatt a tanulmány azokat az állami, gazdasági és társadalmi szempontból alapvető szolgáltatásokat és rendszereket érti, amelyek működésének zavara jelentős hatással lenne az állami működésre, a közbiztonságra vagy a társadalom alapvető szükségleteinek kielégítésére. A fogalom értelmezése az Európai Unió kritikus szervezeteinek rezilienciájáról szóló irányelvére, valamint annak nemzeti megfelelőire támaszkodik, kiegészítve a NATO rezilienciamegközelítésével. A kritikus infrastruktúrák (KI) védelme a 21. századra kiemelten kezelendő szakterületté vált, védelme egyre nagyobb figyelmet kap.[2] A modern társadalmak működését biztosító kritikus infrastruktúrák egyre szorosabb kölcsönhatásban állnak egymással.[3] A KI-k – például energia-, víz-, közlekedési, egészségügyi és információs rendszerek – olyan mértékben épülnek egymásra, hogy működésük zavara nem csupán egy adott ágazat problémája, hanem rövid időn belül társadalmi és nemzetbiztonsági következményekkel járhat. A tudományos felfedezések, az innovációban rejlő képességek és lehetőségek szinte folyamatosan változtatták és változtatják a biztonsági környezetet.[4] A technológiai gyorsulás és a digitalizáció mellett a globális ellátási láncok sérülékenysége és a hibrid fenyegetések[5] terjedése együtt alakítja ki azt a környezetet, amelyben a KI-k védelme már rendszerszintű kihívássá vált. Ebben

[2] Szénási 2024: 19.
[3] Bakos–Kovács 2025: 111.
[4] Földes 2025: 146.
[5] Hibrid fenyegetés: a katonai, információs, kiber-, gazdasági és politikai eszközök összehangolt alkalmazása, amelynek célja a társadalmi működés megzavarása vagy befolyásolása. A fizikai és digitális támadások egyszerre, egymást erősítve jelenhetnek meg.

a környezetben a biztonság nem statikus állapotként értelmezhető, hanem gyorsan változó, gyakran előre nem jelezhető kockázati környezet. A technológia ma már kettős természetű: egyszerre növeli a hatékonyságot, miközben új, gyakran nehezen felismerhető kockázatokat is létrehoz. A működésfolytonosság-tervezés (BCP[6]), valamint annak kormányzati és honvédelmi megfelelője, a működés folytonossága (COOP) vezetői felelősség és műveleti képesség. Különösen igaz ez azokra az ágazatokra, rendszerekre, ahol a működés elvárt rendelkezésre állása a nap 24 órájában közel teljes, és ahol egy rövid leállás is kárt okozhat. Egy kórház esetében ez konkrétan azt jelenti, hogy egy áramszünet során a sürgősségi ellátás csak akkor biztosítható, ha a tartalék energiaellátás azonnal és megszakítás nélkül átveszi a működést.

Magyarországon a KI-k védelme elsődlegesen állami feladat, amelyet a szövetségesi elvárások és iránymutatások alapján kialakított nemzeti jogszabályok határoznak meg. Tekintettel arra, hogy az alapvető szolgáltatások[7] jelentős részét nem állami, hanem piaci szereplők működtetik, elengedhetetlenné vált a világos és kötelező előírások megfogalmazása. Ez óhatatlanul szoros együttműködést kíván meg az állami, honvédelmi, katasztrófavédelmi és magánszektorhoz tartozó szervezetek között, hiszen az alapvető szolgáltatások folytonossága csak összehangolt módon biztosítható.

A működésfolytonosság egy olyan mechanizmust, intézkedésegyüttest jelent, amellyel egy szervezet vagy rendszer különleges körülmények között, jelentős zavar esetén is elfogadható szinten tud működni, majd tervezetten vissza tud állni a normál üzemre. A jelen publikáció a KI-k védelmének összefüggésrendszerében a működésfolytonosság-tervezés szerepét és módszertani megközelítéseit mutatja be, elsősorban a NATO-doktrínák és a NIST által meghatározott keretrendszerek alapján. A NATO-doktrínák a katonai és stratégiai működésfolytonosság alapelveit rögzítik, míg a NIST-keretrendszerek a civil, technikai és kiberbiztonsági folyamatok részletes követelményeit határozzák meg. A két megközelítés együtt ad teljes képet arról, hogyan tartható fenn a kritikus szolgáltatások működőképessége összetett, többdoménű környezetben.

A BCP olyan szervezeti tervezési és működtetési folyamat, amelynek célja, hogy zavar esetén is fennmaradjanak a kritikus működési képességek. A COOP ugyanezt a megközelítést követi a kormányzati és honvédelmi szervezetek körében. A működésfolytonosság azt jelenti, hogy a rendszer a zavarokat követően gyorsan helyre tud állni. A NATO-doktrínák a katonai műveletek folytonosságát támogatják, míg a NIST-keretrendszerek a civil, szervezeti és informatikai folytonosság technikai szabványait adják. A kutatás módszertana kvalitatív, összehasonlító és normatív elemzésre épül, amely a vonatkozó NATO-doktrínák, NIST-ajánlások és uniós, valamint hazai jogszabályok rendszerszintű feldolgozását végzi el. Az elemzés célja nem új szabályozási elemek létrehozása, hanem annak feltárása, hogy a különböző szabályozási és doktrinális keretrendszerek miként egészítik ki egymást a működésfolytonosság biztosításában. A módszertan lehetővé teszi a stratégiai, szervezeti és technikai szintek közötti összefüggések azonosítását, valamint a működésfolytonosság mint integrált szervezeti képesség értelmezését.

[6] A rövidítések jegyzéke a dokumentum végén található.

[7] A kritikus szervezetek ellenálló képességéről szóló 2024. évi LXXXIV. törvény 1. számú melléklet „C" oszlopban meghatározott és a védelmi és biztonsági tevékenységekről szóló 2021. évi XCIII. törvény 5. számú melléklet „C" oszlopban meghatározott szolgáltatások.

A működésfolytonosság stratégiai jelentősége

A KI-k működésfolytonosságának biztosítása multidiszciplináris keretrendszerben értelmezhető. Egyszerre alkalmazandó a NATO katonai doktrínája, a nemzetközi működésfolytonossági és kiberbiztonsági szabványok, valamint az európai és a hazai szabályozás. Ezen három pillér – doktrína, szabvány, jogszabály – teremti meg azt a keretet, amely nélkülözhetetlen az alapvető szolgáltatások folytonosságának fenntartásához.

A NATO doktrinális rendszere – a vizsgált témát illetően – az AJP-01[8] és az AJP-3-as[9] doktrínacsalád. Az AJP-01 doktrína központi szerepet játszik a hadműveletek tervezésének és végrehajtásának szabályozásában. Ezt egészíti ki az AJP-3 doktrínacsalád, amely részletes útmutatást ad a védelem, logisztikai támogatás, a kommunikációs rendszerek működtetésére és az információmegosztás fenntartására, amely egyben a BCP/COOP-rendszerek alapját is képezi. A műszaki követelményeket részletező AJP-3.12.1[10] doktrína az ideiglenes energiaellátás, a hálózati helyreállítás és a mobil képességek szerepét hangsúlyozza, amelyek a katonai és civil működésfolytonossági megoldások technikai alapját adják, adhatják. Az AJP-3.14[11] lefekteti a haderővédelem alapelveit és működési rendjét. Meghatározza, hogyan kell a fenyegetések, veszélyek és sebezhetőségek elemzését beépíteni a műveleti tervezésbe, és bemutatja, hogy az aktív, passzív és helyreállító védelmi intézkedések együtt hogyan biztosítják a katonai erők folyamatos működőképességét. Az AJP-3.28[12] doktrína a stabilizációs és válságkezelési műveletek[13] során elvárt civil infrastruktúra-támogatási feladatokat határozza meg, kiemelve a kritikus szolgáltatások ideiglenes biztosításának és helyreállításának jelentőségét.

A nemzetközi működésfolytonossági és kiberbiztonsági szabványok – különösen a NIST és az ENISA keretrendszerei – elsősorban azt a célt szolgálják, hogy a szervezetek működése a különféle zavaró események ellenére is fennmaradjon. A NIST SP 800-34 r1[14] egy jól felépített, PDCA-logikára épülő COOP-életciklust kínál, amely segít a felkészüléstől kezdve a válaszadáson át egészen a helyreállításig egységes rendszerben kezelni a folyamatokat. A NIST SP 800-61 r3[15] azt mutatja meg, hogyan érdemes felépíteni és működtetni egy CSIRT-et vagy SOC-ot: milyen protokollok támogatják a kiberincidensek időben történő felismerését, kezelését és koordinált lezárását. A NIST SP 800-53 r5[16] egy átfogó kontrollkatalógust biztosít, amelyben a technikai, szervezeti és folyamatszintű biztonsági és folytonossági intézkedések egy egységes keretrendszerként jelennek meg.

[8] AJP-01: szövetségesi Összhaderőnemi Alap Doktrína.
[9] AJP-3: szövetségi Összhaderőnemi Doktrína a Műveletek Végrehajtásáról.
[10] AJP-3.12.1: szövetségi Összhaderőnemi Doktrína a Katonai műszaki tevékenységekhez.
[11] AJP-3.14: szövetségi Összhaderőnemi Doktrína a Haderővédelemről.
[12] AJP-3.28: szövetségi Összhaderőnemi Doktrína a a Stabilizációhoz való Katonai Hozzájárulásról.
[13] Stabilizációs és válságkezelési műveletek: olyan tevékenységek, amelyek célja az alapvető civil szolgáltatások helyreállítása, fenntartása és a társadalmi rend stabilizálása katonai támogatással.
[14] NIST SP 800-34 r1: Vészhelyzeti és működésfolytonossági tervezési útmutató szövetségi információs rendszerek számára.
[15] NIST SP 800-61 r3: Ajánlások és megfontolások a kiberbiztonsági kockázatkezeléshez kapcsolódó incidenskezeléshez.
[16] NIST SP 800-53 r5: Biztonsági és adatvédelmi kontrollok információs rendszerek és szervezetek számára.

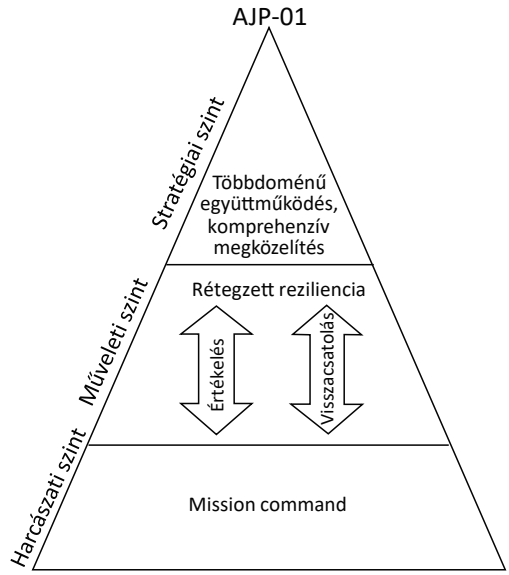
A magyar működésfolytonossági szabályozás az NIS2-[17] és a CER-irányelvekhez[18] igazodva jogszabályi szinten[19] határozta meg a kritikusinfrastruktúra-szereplők szervezeti, jelentési, incidenskezelési és gyakoroltatási kötelezettségeit. A vonatkozó mellékletek egyértelműen nevesítik azokat a szektorokat és alágazatokat, amelyek esetében a BCP/COOP tervezésének és működtetésének megléte elengedhetetlen, továbbá keretrendszert biztosítanak az interdependenciák vizsgálatának standardizált végrehajtásához. A megfelelés így nem pusztán formális jogi kötelezettség, hanem a működésfolytonosság-tervezés minőségének és a szervezeti működésfolytonosság tényleges szintjének egyik legfontosabb meghatározó tényezője.

A működésfolytonosság jelentősége ma már jóval túlmutat a hagyományos üzletmenet-biztonsági megközelítésen. A kommunikációs, energetikai, logisztikai és – egyre inkább – az informatikai rendszerek olyan szorosan összekapcsolódó hálózatot alkotnak, hogy egyetlen elem meghibásodása vagy kiesése is könnyen láncreakciót idézhet elő. Ez nemcsak technikai fennakadásokat okozhat, hanem a társadalmi működés zavarához, gazdasági károkhoz és komoly reputációs veszteségekhez is vezethet. Míg a piaci szereplők esetében a működésfolytonosság megszilárdítása versenyelőnyt és üzleti stabilitást jelent, addig a kritikus infrastruktúrák terén mindez a közérdek védelméről, a lakosság biztonságáról és az állami működés zavartalanságáról szól – vagyis elengedhetetlen alapfeltétel. Például egy regionális áramszolgáltató esetében egy alállomás kiesése nemcsak az energiaellátást érinti, hanem a távközlési szolgáltatásokat és a közlekedési irányítórendszereket is. Egy ilyen esemény során a BCP-tervnek tartalmaznia kell az alternatív energiaforrások aktiválását és a prioritási sorrendben történő visszakapcsolást.

A működésfolytonosság rendszerszintű megközelítése

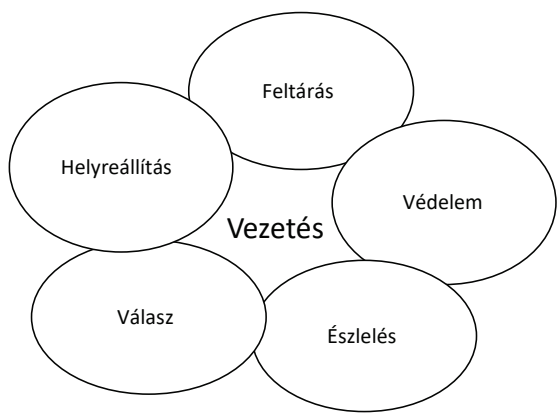
A BCP/COOP-életciklus intézményi nézőpontból mindig a stratégiai keretek kijelölésével indul. A működésfolytonosság nem pusztán a dokumentumok és eljárások együttese, hanem az erők, erőforrások és felelősségi körök olyan rendszere, amely a váratlan helyzetekben is képes fenntartani és helyreállítani a működést. A NATO-doktrínák – kiemelten az AJP-01 – ezt a rendszerszemléletet a komprehenzív megközelítés,[20] a rétegzett működésfolytonosság,[21] a *mission command*[22] és a többdoménű együttműködés alapelveire építik. A gyors regenerációt és döntésképességet az alapelvek mentén összehangolt stratégiai, műveleti és harcászati szintű tervezés, valamint az értékelés és a visszacsatolás biztosíthatja. Az alapelvi összefüggéseket az 1. ábra szimbolizálja.

[17] NIS2: az Európai Parlament és a Tanács 2022/2555 számú irányelve, amely az EU területén egységesen magas szintű kiberbiztonságot ír elő a kritikus és fontos ágazatok számára.
[18] CER: az Európai Parlament és a Tanács (EU) 2022/2557 irányelve a kritikus szervezetek rezilienciájáról.
[19] Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény, a kritikus szervezetek ellenálló képességéről szóló 2024. évi LXXXIV. törvény, a védelmi és biztonsági tevékenységek összehangolásáról szóló 2021. évi XCIII. törvény.
[20] Komprehenzív megközelítés: összetett, többdimenziós döntés- és műveletirányítási szemlélet, amely összehangolja a különböző szereplők, szervezetek és képességek tevékenységét.
[21] Rétegzett működésfolytonosság: egy rendszer ellenálló képessége több, egymásra épülő védelmi, működési és helyreállítási komponensből áll.
[22] *Mission command:* küldetésorientált vezetés vagy küldetésalapú irányítás.



1. ábra: Az AJP-01 alapelveinek rendszerszemlélete
Forrás: a szerző szerkesztése

A technikai-szervezeti oldalon a NIST által ajánlott a működésbe integrált állandó visszacsatolás, amelynek keretét a vezetés–feltárás–védelem–észlelés–válasz–helyreállítás hat funkció adja meg. A folyamatok a szerepkörök, a hatáskörök és a felelősségek egyértelmű rögzítésével folytatódik. A folyamatok összefüggéseit a 2. ábra mutatja be.



2. ábra: A NIST biztonsági keretrendszere
Forrás: a szerző szerkesztése

A NATO-műveleti logika szerint a működésfolytonosság feltétele a stabil C2-rendszer, a világos felelősségmegosztás és a *unity of effort,*[23] mert válsághelyzetben a felelősségi zavar vagy a döntések késlekedése önmagában is kockázatnövelő tényező. A NIST-ajánlások ezt már kötelező elvárásként határozzák meg: az incidenskezeléshez kapcsolódó szerepek, jogosultságok, döntési jogok és folyamati utak előre rögzített, egyértelmű dokumentálása teremti meg azt a szervezeti alapot, amelyre a műszaki és üzemeltetési kontrollok biztonsággal épülhetnek. Ez az alap azonban csak akkor működik valódi képességként, ha a szervezeten belüli függőségeket és a kritikus erőforrásokat részletesen ismerjük. Nemcsak a saját folyamataikat és rendszereiket kell feltérképezni, hanem azokat a szolgáltatókat, beszállítókat, közmű- és felhőszolgáltatókat, stratégiai partnereket is, amelyek közvetlenül vagy közvetve befolyásolják a működés folytonosságát. Például egy felhőszolgáltató kiesése esetén egy szervezet működése csak akkor tartható fenn, ha előzetesen kialakított alternatív szolgáltatói kapcsolatokkal vagy több szolgáltatót alkalmazó architektúrával rendelkezik. A reális kockázatértékeléshez ezek aktív bevonása a tervezés alapvető feltétele. A BCP/COOP technikai alapja a kritikus eszközök és erőforrások azonosítása, a rájuk ható fenyegetések és sérülékenységek feltárása – a fizikai, az informatikai és a kommunikációs infrastruktúrák teljes spektrumán –, hogy a releváns kockázatokat időben észleljük és kezelni tudjuk.

A korai észlelés mind a NATO-, mind a NIST-megközelítésben kiemelt jelentőségű. A NATO-doktrínák ezt többdoménű érzékeléssel és egységesen működő hírszerzési-kommunikációs láncokkal támogatják. A NIST ugyanezt műszaki oldalról bontja ki: a folyamatos hálózati és szolgáltatói megfigyelés, a rendellenes mintázatok elemzése, valamint a riasztási és incidensbejelentési feltételek egyértelmű meghatározása teremti meg azt a helyzetképet, amelyre a gyors reagálás épül. Egy zsarolóvírus-támadás során például a szervezet először leválasztja az érintett rendszereket a hálózatról, ezt követően elemzi a naplóállományokat a behatolás azonosítására, majd biztonsági mentésekből állítja helyre a működést, ami jól leképezi az észlelés–válasz–helyreállítás folyamatát.

A NATO-oldali reagálás kockázatközpontú, és erősen támaszkodik a vezetésirányítási rendszerre. Katonai környezetben ez például azt jelenti, hogy egy kommunikációs rendszer kiesése esetén mobil kommunikációs egységeket telepítenek a parancsnoki lánc fenntartása érdekében. A megközelítés lényege a gyors helyzetértékelés, a világos prioritások kijelölése, az erőforrások összehangolása és a kritikus szolgáltatások átmeneti fenntartása, miközben szükség esetén az alternatív megoldások is azonnal aktiválhatók. A NIST ugyanezt részletes, lépésről lépésre követhető folyamatokban írja le: az incidensek első vizsgálatától és továbbításától kezdve a helyzet elemzésén és a bizonyítékok kezelésén át egészen a belső és külső kommunikáció összehangolásáig, a célzott beavatkozások végrehajtásáig. A helyreállítás célja a működőképesség ellenőrzött és biztonságos visszaállítása. Ez a gyakorlatban jelentheti például egy informatikai rendszer fokozatos újraindítását priorizált szolgáltatások mentén, miközben folyamatosan ellenőrzik az adatintegritást és a rendszerbiztonságot. A NATO ezt műveleti követelményként határozza meg, míg a NIST ennek részletes,

[23] *Unity of effort:* erőfeszítések egysége, különböző szervezetek összehangoltan, közös cél irányába dolgoznak.

technikai folyamatleírást ad. Mindkét megközelítés közös eleme, hogy a tanulságok és a bizonyítékok visszacsatolása indítja el a következő életciklusszakaszt, ezáltal válik a működésfolytonosság valóban tanuló és önjavító képességgé.

A kritikus infrastruktúrák működésfolytonosságának gyakorlati értelmezését jól szemlélteti egy olyan forgatókönyv, amelyben egy állami működés szempontjából kiemelt, digitalizált szolgáltatás – például egy központi adminisztratív vagy logisztikai rendszer – külső, felhőalapú szolgáltató infrastruktúrájára támaszkodik. Egy ilyen környezetben egy szolgáltatói oldalon bekövetkező incidens – például kiberbiztonsági esemény, hálózati kiesés vagy ellátási láncot érintő zavar – közvetlen hatással lehet a kritikus szolgáltatás rendelkezésre állására, miközben maga az érintett szervezet objektumszintű védelmi intézkedései változatlanul fennállnak. A működésfolytonosság biztosítása ilyen esetben kizárólag integrált megközelítéssel valósítható meg. NATO-doktrinális szempontból a vezetés és irányítás folyamatossága, a döntési ciklus fenntartása és az erőforrások újrapriorálása biztosítja a szervezeti működőképesség fenntartását. Ezzel párhuzamosan a NIST által meghatározott incidenskezelési életciklus – az észlelés, elemzés, reagálás és helyreállítás egymást követő lépéseivel – a technikai válaszintézkedések végrehajtását strukturálja. A példában a szolgáltatás helyreállításának sikeressége nem kizárólag a technikai redundanciától függ, hanem attól is, hogy a szervezet előzetesen meghatározta-e az elfogadható helyreállítási idő- és adatvesztési célértékeket, valamint képes-e együttműködni a külső szolgáltatóval a válsághelyzet kezelésében. Ez a megközelítés jól szemlélteti, hogy a működésfolytonosság napjainkban nem statikus tervdokumentumként, hanem a szervezeti irányítás, a technikai védelem és a szabályozási megfelelés szerves egységeként értelmezhető.

A működésfolytonosság és a biztonsági érettség egységes megközelítése

Az ajánlás szerint a biztonsági környezet gyorsan, nem lineáris módon változik, ezért a szervezetnek tudatosan felépített, mérhető és folyamatosan fejleszthető biztonsági szintet kell elérnie és fenntartania. Ez nem egyetlen intézkedésen múlik: a megelőzés, az észlelés, a reagálás és a helyreállítás együtt adhat stabil működést. A cél nemcsak az üzemeltetés és a rendelkezésre állás védelme, hanem az ártó szándékú befolyásolásból eredő incidensek kezelése is. Ez a képesség végigkíséri a teljes tervezési és végrehajtási ciklust, és érdemben erősíti a rendszer BCP/COOP-dokumentációját. Mivel a szervezetüzemeltetési eszközökön kívül számos infokommunikációs eszközt használnak – akár integráltan is –, a kiberbiztonsági kockázatok mellett adatvédelmi, beszállítói láncbeli, hírnévi, technológiai és fizikai kockázatokkal is számolni kell. A kockázatkezelésnek folyamatos – nem kampányszerű – tevékenységnek kell lennie. A folyamatos működés alapja az ajánlás szerint a felelősök kijelölése a hat fő funkció mentén. A szerepek a szervezet méretétől és a kockázati profiltól[24] függően összevonhatók, de a felelősség és az elszámoltathatóság – különösen a jogi kötelezettségek miatt – nem csökkenthető, a szerepek összevonása sem eredményezheti ezeknek a követelményeknek a gyengülését.

[24] Kockázati profil: rendszer vagy folyamat egyedi kockázati jellemzőinek összessége.

- A *vezetés* kialakítja, jóváhagyja és kommunikálja a biztonsági stratégiát, összeköti a funkciókat, és láthatóvá teszi a képességeket, hiányokat, beszállítói kitettségeket és beavatkozási pontokat.
- A *feltárás* a valós kockázati kép vizualizálása: eszköz- és szolgáltatásleltár, az adatáramlás megértése és ábrázolása, kritikussági besorolás, sérülékenységek és fenyegetések azonosítása, az eredendő kockázat becslése és a válaszok rangsorolása.
- A *védelem* az arányos, célzott megelőző és következménycsökkentő intézkedésekről szól: azonosítás- és hozzáférés-kezelés, fizikai védelem, tudatosság és képzés, adatbiztonság, konfigurációkezelés, gondozott szoftver- és hardveréletciklus, szabályozott válaszok a környezeti fenyegetésekre.
- Az *észlelés* a hálózatok, szolgáltatások, a fizikai környezet és – amennyire a beszállítói átláthatóság engedi – a partnerek folyamatos nyomon követése. Feladata az anomáliák értelmezése, a „zaj" kiszűrése és a cselekvésre kész döntési információk előállítása.
- A *válasz* a tényleges lépések összehangolását jelenti, vagyis az incidensek osztályozását és hitelesítését, az objektív belépési pont kijelölését a helyreállítási folyamatba, az eseti elemzések elkészítését a kiváltó okok és a terjedés feltárására, a bizonyítékszintű dokumentálást, a kár és a további események valószínűségének becslését, valamint a belső és külső érintettek időszerű és hiteles tájékoztatását.
- A *helyreállítás* pedig a működőképesség ellenőrzött visszaállítása. A lépések kiválasztása és rangsorolása, a zárási feltételek teljesítése, az esemény- és helyreállítási dokumentáció lezárása, a tanulságok beépítése a terveinkbe és szabályzatainkba. A megvalósítást rendszeres visszamérés és a tanulságok tudatos beépítése követi, így a folyamatos működés egy dinamikus, önmagát erősítő folyamattá válik.

Az AJP-01 szemlélete szerint a szervezet működőképességének fenntartása nemcsak technikai vagy eljárási kérdés, hanem vezetési és együttműködési gyakorlat, amely a teljes életciklust átszövi. A gyorsan változó környezetben a vezetőknek nemcsak irányt kell mutatniuk, hanem olyan bizalmi és együttműködési kultúrát is teremteniük, amelyben minden szereplő tisztán látja a saját feladatát, hatáskörét és az együttműködés kereteit. Ez teremti meg azt a működési alapot, amelyre a folytonossági és helyreállítási képességek épülhetnek. A tevékenységek koordinációját támogatja a helyzetértékelés folyamatos, több forrásból történő frissítése: az információk hitelességének vizsgálata, a működési képességek állapotának értékelése és a rendelkezésre álló erőforrások valós idejű átlátása. Az ajánlás hangsúlyozza, hogy a megelőzés, a felkészülés, a reagálás és a helyreállítás nem elszigetelt funkciók, hanem egymást erősítő, ciklikusan ismétlődő tevékenységek, amelyeknek a parancsnoki döntések és a végrehajtó szintek között zavartalanul kell áramolniuk. A dokumentum rámutat, hogy a folyamatos működés nem tartható fenn pusztán erőforrásoldalról, szükség van a kommunikáció, a feladatmegosztás, a felelősségi viszonyok és a partnerségi kapcsolatok összehangolt, átlátható kezelésére is. A működésfolytonosság humán oldala ugyanilyen meghatározó: a szerepek, a felelősségek és az együttműködési szabályok

egyértelmű meghatározása, valamint a feladatellátás személyi feltételeinek biztosítása döntően befolyásolja, hogy egy válsághelyzetben a tervek valóban végrehajthatók-e. Ez különösen fontos olyan helyzetekben, amikor a szervezet egyszerre több működési területen tevékenykedik, és a feladatok összehangolásához több beszállítóval és számos érintett féllel kell együttműködnie. Amennyiben ez az összhang működik, a folytonosság nem külön gyakorlat, hanem a mindennapi vezetés részévé válik, amely a BCP/COOP-dokumentációt élővé, a döntéseket következetessé, a helyreállítást pedig gyorsabbá és bizonyítékokon nyugvóvá teszi.

Ezek a vezetési és együttműködési alapok teremtik meg azt a ritmust, amelyben a folytonosság és a helyreállítás már nem külön feladat, hanem a szervezet működésének szerves része. Ez a működés természetes ritmusa a BCP/COOP-életciklusnak, ahol a stratégiai irányok és a műszaki-eljárási kontrollok kölcsönösen támogatják egymást, és a szervezet kritikus képességei folyamatosan finomodnak a tervezés, a végrehajtás, az ellenőrzés és a beavatkozás köré épülő gyakorlatnak köszönhetően. Ebben a keretben a NATO-szemlélet stratégiai és műveleti megközelítése összhangba kerül a NIST részletes végrehajtási nyelvével. A NATO oldaláról érkezik a több szintre és doménre kiterjedő, felelősségalapú együttműködés iránya, míg a NIST biztosítja a gyakorlati megvalósítás eszközeit. A NATO–NIST összehasonlító kereteit az 1. táblázat mutatja.

1. táblázat: A NATO–NIST összehasonlító keretei

NATO: Stratégia, művelet	**NIST: Technika, eljárás**
C2, együttműködés	Detektálás, válasz, kontrollok
Mission command	Életciklus
többdoménű működés	CSIRT-, SOC-folyamatok

Forrás: a szerző szerkesztése

Összegzés

Amennyiben ez a két megközelítés valóban találkozik, akkor a működésfolytonosság gyakorlati értelemben azt jelenti, hogy egy szervezet egy esemény után módosítja az eljárásait, például frissíti a helyreállítási terveit vagy átalakítja a beszállítói struktúráját. A szervezet képes érzékelni a helyzeteket, értelmezni az összefüggéseket, döntéseket hozni, cselekedni és helyreállítani, mindezt bizonyítékokra támaszkodva és a saját valós kitettségeihez igazítva. A NATO stratégiai gondolkodásmódja és a NIST részletes végrehajtási logikája egymás mellett nem kettős terhet jelentenek, hanem közösen létrehoznak egy olyan keretet, amelyben a vezetők és a végrehajtó szereplők egyaránt tisztán látják, hogy mikor, mivel és hogyan kell beavatkozni. Ebben a modellben a működésfolytonosság nem egyszeri projekt, nem kampányszerű feladat, hanem a szervezet kollektív tanulási folyamata, amelyben a hibákból nyert tapasztalat, a visszajelzések elemzése és az előretekintő tervezés egyaránt helyet kap.

Ez a megközelítés lehetővé teszi, hogy a szervezet ne csupán reagáljon a zavarokra, hanem előre felismerje a gyenge pontokat, és még az események bekövetkezése előtt

kialakítsa a megfelelő alternatívákat. A felkészültség és a gyors alkalmazkodóképesség így nemcsak technikai, hanem kulturális tényezővé válik. A döntéshozók és a működtetésben érintettek közösen alakítanak ki egy olyan működési környezetet, ahol a problémák nyíltan felszínre kerülhetnek, és a megoldások keresése nem büntetéshez, hanem fejlődéshez kapcsolódik.

Ennek eredményeképpen a BCP/COOP nem különálló dokumentum vagy „külön dosszié" lesz, hanem a vezetési és üzemeltetési gyakorlat szerves része, ahol a stratégiai elvek a műszaki kontrollokon és az operatív rutinokon keresztül tényleges túlélőképességgé formálódnak. A működésfolytonosság így válik valódi szervezeti kompetenciává. Olyan képességgé, amely nemcsak válsághelyzetben véd, hanem a mindennapi működés stabilitását, a szolgáltatások minőségét és a társadalmi bizalom fennmaradását is támogatja.

A két megközelítés összeérése tehát nem adminisztratív kötelezettség teljesítését jelenti, hanem azt a felismerést, hogy az ellenálló képesség egy olyan befektetés, amely mérhetően csökkenti az üzemszünetek idejét és a helyreállítás költségeit. A bemutatott megközelítés egy integrált működésfolytonossági modellt körvonalaz, amely egyaránt illeszkedik a katonai-doktrinális, a technikai-eljárási és a szabályozási követelményekhez.

Felhasznált irodalom

Jogszabályok és uniós dokumentumok

Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről (2022). Brüsszel, Az Európai Unió Hivatalos Lapja, L 333/164, 2022. december 27. Online: https://publications.europa.eu/resource/cellar/c4d36f49-85bc-11ed-9887-01aa75ed71a1.0012.01/DOC_1

Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve a hálózat- és információbiztonságról (2016). Brüsszel: Az Európai Unió Hivatalos Lapja, L 194, 2016. július 19. Online: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32016L1148

Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve a hálózat- és információbiztonságról (2022). Brüsszel: Az Európai Unió Hivatalos Lapja, L 333, 2022. december 27. Online: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32022L2555

2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről. Online: https://mkogy.jogtar.hu/jogszabaly?docid=a1200166.TV

NATO-doktrinális dokumentumok

North Atlantic Treaty Organization – NATO Standardization Office (2021): AJP-3.14 Allied Joint Doctrine for Force Protection. Online: www.coemed.org/files/stanags/01_AJP/AJP-3.14_EDA_V1_E_2528.pdf

North Atlantic Treaty Organization – NATO Standardization Office (2022. december 19): NATO Standard AJP-01 Allied Joint Doctrine (Edition F, Version 1). Online: www.coemed.org/files/stanags/01_AJP/AJP-01_EDF_V1_E_(1)_2437.pdf

North Atlantic Treaty Organization – NATO Standardization Office (2020): AJP-3 Allied Joint Doctrine for Operations. Online: www.coemed.org/files/stanags/01_AJP/AJP-3_EDC_V1_E_2490.pdf

North Atlantic Treaty Organization – NATO Standardization Office (2021): AJP-3.28 Allied Joint Doctrine for Stability Policing. Online: https://assets.publishing.service.gov.uk/media/63d7b111e90e0773d50c7530/AJP-3.28_web_accessible.pdf

NIST- és technikai keretrendszerek

National Institute of Standards and Technology (2018): Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. Gaithersburg, MD.

National Institute of Standards and Technology (2012): Computer Security Incident Handling Guide (NIST Special Publication 800-61 Revision 2). Gaithersburg, MD.

National Institute of Standards and Technology (2018): Risk Management Framework for Information Systems and Organizations (NIST Special Publication 800-37 Revision 2). Gaithersburg, MD.

Szabványok és módszertani források

International Organization for Standardization (2019): ISO 22301:2019 – Security and resilience – Business continuity management systems – Requirements. Geneva: ISO.

International Organization for Standardization (2022): ISO/IEC 27001:2022 – Information security management systems – Requirements. Geneva: ISO.

Folyóiratcikkek

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

Földes Tibor (2025): A biztonság szerepe és fontossága a szövetségesi kritikus infrastruktúra szabályozásának kialakításában. *Szakmai Szemle,* 23(1), 146–163. Online: https://ojs.knbsz.gov.hu/index.php/szakmai/article/view/234/130

Szénási Imre (2024): Kritikus rendszerelemek jellemzői, azok kijelölése, valamint azok védelme; *Nemzetbiztonsági Szemle,* 12(2), 18–37. Online: https://doi.org/10.32561/nsz.2024.2.2

Rövidítések jegyzéke

Rövidítés	**Angol megnevezés**	**Magyar jelentés**
AJP	Allied Joint Publication	Szövetséges összhaderőnemi kiadvány
ATP	Allied Tactical Publication	Szövetséges harcászati (taktikai) kiadvány
BCP	Business Continuity Planning	Üzletmenet-folytonosság tervezése
BIA	Business Impact Analysis	Üzleti hatáselemzés
C2	Command and Control	Vezetés és irányítás
COOP	Continuity of Operations	A szervezeti működés folytonossága
CI	Critical Infrastructure	Kritikus infrastruktúra
CSIRT	Computer Security Incident Response Team	Informatikai Biztonsági Incidens-kezelő Csapat
CER	Critical Entities Resilience	Kritikus szervezetek ellenállóképessége
NIS / NIS2	Network and Information Security Directive	Hálózat- és információbiztonsági irányelv / NIS2
NIST	National Institute of Standards and Technology	Amerikai Nemzeti Szabványügyi és Technológiai Intézet
IR	Incident Response	Incidenskezelés
SOC	Security Operations Center	Információbiztonsági Műveleti Központ
RTO	Recovery Time Objective	Helyreállítási időcél
RPO	Recovery Point Objective	Helyreállítási pontcél
PDCA	Plan–Do–Check–Act	Tervezés, végrehajtás, ellenőrzés, beavatkozás

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG

21. évfolyam (2026) 3. szám 119–135.
DOI: 10.32567/hm.2026.3.8

Takács Dániel,[1] Négyesi Imre[2]

A nukleáris energia hasznosításának új korszaka

SMR – a megszelídített atombomba

A New Era in Nuclear Energy Utilisation

SMR – The Tamed Atomic Bomb

Absztrakt

A tanulmány a nukleáris technológia fejlődését a nukleáris háború fenyegetésének, a bipoláris világrend sajátosságainak és a jellemző háborúforma alakulásának összefüggésében vizsgálja, különös tekintettel a katonai nukleáris fegyverek geopolitikai hatásaira és a fegyverkezés, valamint az energiatermelés dualitására. Elemzi a kiégett fűtőanyagok hosszú távú kezelésének környezeti és biztonsági kockázatait, valamint azt, hogy a kis moduláris reaktorok (small modular reactor, SMR) decentralizált, szigetüzemű működésükkel hogyan járulnak hozzá az energiafüggetlenséghez, az ellátásbiztonsághoz és a fosszilis energiahordozóktól való függés csökkentéséhez. A fűtőelemek fogyasztásának optimalizálása, az üzemanyagciklusok meghosszabbítása és a moduláris felépítés révén az SMR-ek csökkentik az üzemeltetési költségeket, növelik a rendszer rugalmasságát, miközben méretük, rövidebb telepítési idejük és időjárástól független termelésük stabil, tervezhető energiaellátást biztosít a nagyfogyasztók és a kritikus (különösen a katonai és a kritikus információs) infrastruktúrák számára. A „megszelídített atombomba" metaforáján keresztül a nukleáris technológia olyan kontrollált, precíziós energiamegoldásként jelenik meg, amely a hideg háború nukleáris elrettentésének logikájától eltérően a fenntartható fejlődés, a nemzetbiztonság és a globális stabilitás metszéspontjában helyezkedik el, ugyanakkor a radioaktív hulladékkezelés,

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola, e-mail: takacs.daniel@uni-nke.hu
[2] Egyetemi tanár, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Katonai Infokommunikációs Intézet Informatikai Tanszék, e-mail: negyesi.imre@uni-nke.hu

a potenciális balesetek és a szabályozási-felügyeleti követelmények továbbra is meghatározó korlátokat jelentenek.

Kulcsszavak: nukleáris energia, small modular reactor, szigetüzemű energiaellátás, energiafüggetlenség, kritikus infrastruktúra

Abstract

This study examines the evolution of nuclear technology in the context of the threat of nuclear war, the characteristics of the bipolar world order, and the development of modern warfare, with a particular focus on the geopolitical impacts of nuclear weapons and the dual nature of weaponisation and energy production. It analyses the environmental and security risks of the long-term management of spent nuclear fuel, as well as how small modular reactors (SMRs), through their decentralised, island-mode operation, contribute to energy independence, security of supply, and the reduction of reliance on fossil fuels. By optimising fuel consumption, extending fuel cycles, and leveraging a modular design, SMRs reduce operating costs and increase system flexibility. Meanwhile, their compact size, shorter deployment times, and weather-independent generation ensure a stable, predictable energy supply for large-scale consumers and critical (especially military and information) infrastructures. Through the metaphor of the "tamed atomic bomb", nuclear technology is presented as a controlled, precision energy solution that – diverging from the logic of Cold War nuclear deterrence – lies at the intersection of sustainable development, national security, and global stability, even as radioactive waste management, potential accidents, and regulatory oversight requirements continue to represent significant constraint.

Keywords: nuclear energy, small modular reactor, island-mode energy supply, energy independence, critical infrastructure

Bevezetés

A modern háború folyamatosan változó jelenség, amely a technológiai fejlődés hatására kaméleonszerűen alkalmazkodik a politikai és társadalmi környezethez.[3] A fegyverzetek, harcmodorok és stratégiai megfontolások nem izoláltak, hanem szoros kölcsönhatásban állnak a korszak technológiai újításaival, így a háború és a politika kapcsolata állandó újraértelmezést igényel. A nukleáris technológia és a mesterséges intelligencia megjelenése radikálisan átalakította a biztonsági stratégiákat, különösen egy bipoláris világrend fényében, ahol a kockázatkerülő háború és a technológiai bátorság egyensúlya dominál.[4] Ebben a komplex rendszerben a nukleáris energia kettős szerepe – a békés energetikai alkalmazások és katonai célok – egyaránt kulcsfontosságú a geopolitikai dinamikák alakításában.

[3] Boda 2024a.
[4] Boda 2024b.

Az utóbbi évtizedekben a kis moduláris reaktorok technológiája új horizontokat nyit az energiaellátás decentralizációja és rugalmassága terén, miközben a nukleáris fegyverek fenyegetése mellett a fenntartható és stabil energiatermelés elengedhetetlen kritériummá vált. Ez a tanulmány a nukleáris háború, a katonai technológia fejlődése és az energetikai innovációk összefüggéseit elemzi, kiemelve a modern háború információvezérelt, technológiailag komplex természetét, amely a hagyományos hatalmi és bátorságfogalmakat új keretek közé helyezi. Az elemzés során különös figyelmet kap a nukleáris technológiák dualitása, a biztonsági kockázatok és a nemzetbiztonsági kihívások, valamint az SMR-ek[5] mint a 21. századi hadviselés és energiaellátás kulcsfontosságú elemei. E kutatás célja hozzájárulni a modern háború interdiszciplináris megértéséhez, és iránymutatást nyújtani a fenntartható és biztonságos jövő felé vezető úton.

Módszertan

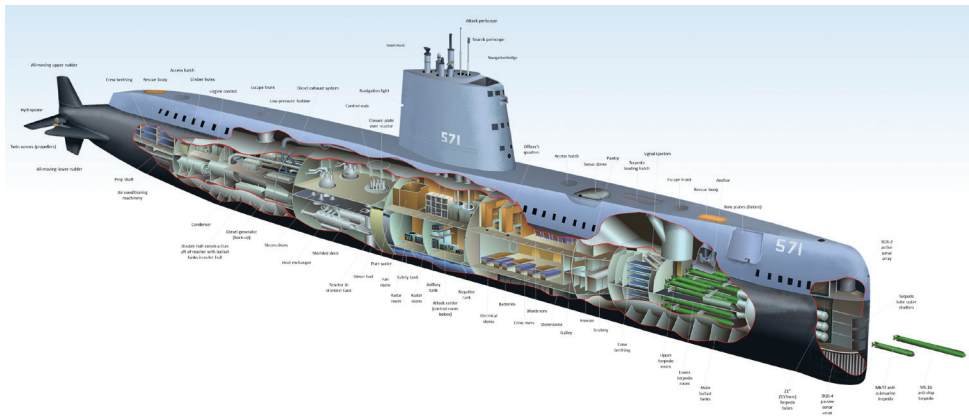
Ebben a tanulmányban primer kutatást nem végeztem, az adatokat és információkat elsősorban nyílt forrásokból, tudományos folyóiratokból, akadémiai publikációkból, hivatalos kormányzati és nemzetközi szervezetek jelentéseiből gyűjtöttem össze. Emellett széles körű irodalmi áttekintést végeztem könyvek, tanulmányok és szakirodalmi összefoglalók alapján, amelyek a nukleáris technológia, a hadiipar, a geopolitika, valamint az energetikai innovációk témaköreit ölelik fel. A források megbízhatóságát és hitelességét kiemelten kezeltem, párhuzamosan értékelve a különböző nézőpontokat és módszertani megközelítéseket, hogy átfogó és objektív képet kapjak a modern háború és a nukleáris technológia összefüggéseiről.

A minőségi és mennyiségi elemzés fókuszába a szövegelemzés, összehasonlító történeti adatok, valamint a technológiai fejlesztések és geopolitikai események kvantitatív mutatóinak figyelembevétele került. Különös hangsúlyt fektettem a hagyományos, illetve a kis moduláris reaktorok összehasonlítására teljesítmény, tüzelőanyag-felhasználás, beszerzési források, valamint a keletkező hulladék mennyisége szerint, történelmi áttekintéssel kiegészítve.

Történelmi áttekintés

Az SMR technológiájának gyökerei a hidegháborús korszakig nyúlnak vissza, amikor a nukleáris energia katonai alkalmazásai, elsősorban az atom-tengeralattjárók hajtóműveiben, ösztönözték a kompakt, nagy teljesítményű reaktorok fejlesztését. Az első működő példa az amerikai USS Nautilus (SSN-571) volt 1954-ben (1. ábra), amely a világ első nukleáris meghajtású tengeralattjárójaként forradalmasította a tengeri hadviselést: a kis méretű, magas dúsítású urán-235-öt használó reaktora akár 60 000 tengeri mérföldet is megtett oxigén nélkül, lehetővé téve a hónapokig tartó álcázott műveleteket a bipoláris világrend konfliktusaiban.

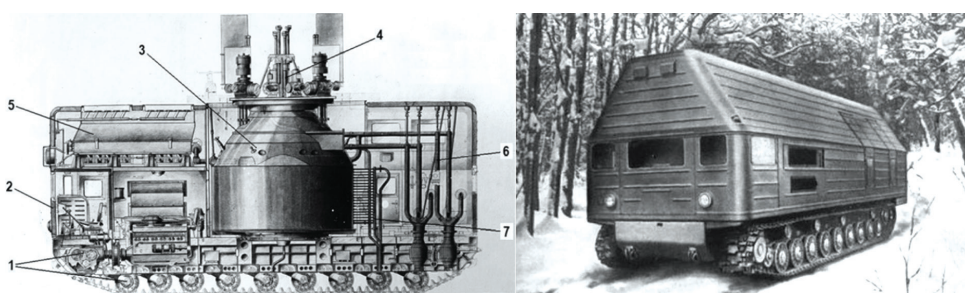
[5] Adorján–Rétfalvi 2022.



1. ábra: USS Nautilus (SSN-571)
Forrás: www.hisutton.com/USS-Naultius-First-Nuclear-Submarine.html

A szovjet válasz a K–3 Leninszkij Komszomol (Project 627A) tengeralattjáró volt 1958-ban, amely hasonló kompakt VM-A reaktort használt.

A szovjet mérnökök további fejlesztéseket végeztek. Kifejlesztették a TESZ-3 (Транспортная Электростанция 3, Transportable Electric Station 3) mobil erőművet (2. ábra). Ez a Szovjetunió egyik legambiciózusabb hidegháborús projektje volt, amelyet 1957-ben rendelt meg a Közepes Gépegyesítés Minisztériuma távoli, elérhetetlen területek energiaellátására, elsősorban katonai célokra. A leningrádi Kirov gyárban fejlesztették ki, és 1961-ben sikeresen tesztelték szibériai terepen, ahol 1,5 MW villamos teljesítményt termelt körülbelül 250 napig, napi 14 g U-235 fogyasztással.[6] Érdekessége, hogy a modulokat egy-egy nehéz harckocsi (T–10) megnyújtott alvázára építették, így szinte teljes körű szárazföldi mobilitással rendelkeztek.



2. ábra: A TESZ-3 erőmű egy modulja
Forrás: https://nucet.pensoft.net/article/89356

[6] Naumenko–Mokhireva 2022.

A T–10 alvázat úgy alakították át, hogy a futóművet 10 támogatógörgőre bővítették (a standard 7 helyett), a láncszélességet növelték a talajnyomás csökkentése érdekében, és két 750 lóerős dízelmotort szereltek be a közel 200 tonnás összsúly mozgatásához. A maximális sebességük 15 km/h volt.[7]

Egy működőképes reaktor telepítéséhez 4 egységre volt szükség, amelyből az első két modul egy kéthurkos, vízhűtéses nukleáris reaktor volt a kapcsolódó berendezésekkel (hűtés, vezérlés), a másik két modulban volt a gőzturbina-generátor, irányítórendszerek és segédberendezések.

Természetesen gondoltak a sugárzásvédelemre is, ezért háromszintű árnyékolás jellemezte:

1. szint: ólomtartály a reaktor körül
   Az aktív zónát (ahol a maghasadás zajlik) vastag ólomtartály vette körül, amely a gamma-sugárzást abszorbeálta. Az ólom a sűrűsége (11,34 g/cm³) miatt kiválóan alkalmas erre, akár már 10–20 cm vastagsággal elnyelheti a dózis 99%-át.
2. szint: bórsavval töltött tartály
   A reaktor körül bórsavoldattal töltött víztartály helyezkedett el, amely neutronmérséklőként működött: a bórium-10 izotóp neutronokat fog el, megakadályozva a további láncreakciót és csökkentve a neutronfluxust.[8]
3. szint: földbe ásás vasbeton lefedéssel
   Üzembe helyezés előtt a modulokat gödörbe süllyesztették (kb. 2–3 m mélyre), majd vasbetonnal zárták le: a földréteg szerves neutronmérséklő (hidrogén), a beton tartós gamma-védelem, így a felszíni sugárzást a minimálisra csökkentették.

A TESZ-3 sikeres tesztjei ellenére az 1960-as évek közepén a szovjet kormány költségvetési okokból leállította a fejlesztést, de egyik modulját ma is Obnyinszkben őrzik. Ez a projekt előrevetítette a modern SMR-ek decentralizált, katonai alkalmazásait.

Még radikálisabb volt a szovjet atomautó-kísérlet legendája: egyes források szerint az 1958–1960 közötti NM-2 prototípus egy kis méretű, folyékonyfém-hűtésű reaktort tartalmazott, amely 6 kW teljesítményű, de akár 50 évig működőképes lett volna egyetlen töltettel. Valóban létezett-e, vagy csak egy városi legenda volt? Internetes források egy 1965-ös szovjet atommeghajtású autóról írnak, amelyet egy Volga alapjaira építettek (3. ábra). Több forrás technikai paramétereket is tartalmaz, de a jármű létezése inkább anekdotikus, mint valóságos.

[7] Retro Transport 2024.
[8] Neutronfluxus: a sugárzás intenzitásának mérőszáma, amely a tér egy adott pontján áthaladó neutronok mennyiségét jelöli.



3. ábra: „Atom Volga" (Ядерная „Волга")
Forrás: https://russian7.ru/post/yadernaya-volga-kak-v-sssr-postroili-a/

Az ihletet minden bizonnyal a nagy versenytárs, az USA adta, ahol már 1957-ben bemutatták a Ford Nucleont[9] (4. ábra). Természetesen csak egy 3/8 arányú modellig jutottak el, de így is megadták a pontos fogyasztási adatokat, amelyek szerint nagyjából 8000 km-t tudna megtenni egy urániumpellettel, amelyet a kiégés után a benzinkutakon cseréltek volna.



4. ábra: Ford Nucleon atomautó
Forrás: https://medium.com/@KDKR/nuclear-cars-a-futuristic-dream-of-the-1950s-bb426876cd97

[9] The 1958 Ford Nucleon 2021.

Mint a példák mutatják, a hidegháború alatt a nukleáris ipar nem korlátozódott az atombomba-kísérletekre, mint a Trinity-teszt (1945, USA, 21 kt), valamint a szovjet RDSZ–1 (amerikai kódneve „Joe–1", 1949, 22 kt) vagy a Cár-bomba (1961, 50 Mt), hanem párhuzamosan dübörgött a békés és katonai energiatermelés. Az USA-ban az Atoms for Peace program (1953) keretében épült az első kereskedelmi reaktor, a Shippingport (1957, 60 MW), míg a Szovjetunió RBMK-prototípusa (1954) gyorsította az áramtermelést. Repülőgéphajtómű-kísérletekben az USA NB-36H (1955–1957) hordozott működő reaktort, a szovjet Tu–95LAL pedig 1961-ig tesztelte a technológiát. Tengerhajózásban az NS Savannah (1962, USA, 74 MW) konténerhajóként kereskedelmi útra indult, szemben a szovjet Leninszkij Komszomol jégtörővel (1959, 30 MW).

Ezzel párhuzamosan űrprogramok is indultak: az USA SNAP-10A (1965) első, űrben működő reaktora 500 W teljesítménnyel termelt orbitális energiát (sajnos csak 42 órán át működött), a reaktor még 4000 évig pályán marad 1300 km magasságban,[10] míg a szovjet RORSZAT műholdak (1967–) BES-5 reaktorral 3–10 kW-ot biztosítottak a működéshez. Mobil erőművekben a kanadai WR-1 (1962) kísérleti reaktora mellett a francia Pamir projekt (1962–1968) 25 kW-os egysége támogatta az Antarktisz-kutatást. Haditengerészeti hordozókban az USA Enterprise repülőgép-hordozó (1961, 8 reaktor) 280 MW-ot adott, míg a szovjet Kirov osztály (1978–) KN-3 reaktorai 300 MW felettit. Ezek a projektek azt mutatják, hogy a nukleáris ipar robbanásszerűen terjeszkedett, a fegyverkezés mellett az energiatermelést, a közlekedést és a kutatást szolgálva, megalapozva a mai SMR-eket. Ezek a fejlesztések a bipoláris világrend háborúformáinak válasza volt: az elrettentés és a proxykonfliktusok igényelték a rugalmas, önellátó energiát, ami ma polgári SMR-ekben éled újjá.

Az SMR-ek műszaki paraméterei és összehasonlítása

A kis moduláris reaktorok napjaink egyik legígéretesebb nukleáris energetikai innovációját képviselik,[11] különösen a rugalmas telepíthetőség, a magas biztonsági szint és a gazdaságosság miatt. Teljesítményük tipikusan 10 és 300 MW között mozog, így többszörösen kisebbek, mint a hagyományos nagy teljesítményű atomerőművek, amelyeket gyakran gigawattos kategóriában mérnek. Ez lehetővé teszi a moduláris felépítést, azaz több egység sorba vagy párhuzamosan kapcsolható, optimalizálva az energiaigényhez való alkalmazkodást és minimalizálva az üzemeltetési kockázatokat.

Az SMR-ek egyik kulcsfontosságú eleme a tüzelőanyag típusa: általánosan használtak a magas próbaértékű alacsony dúsítású urán (HALEU[12]), valamint a fejlettebb, TRISO[13] (TRi-structural ISOtropic) kerámiával bevont részecskék, amelyek jelentősen növelik a reaktorbiztonságot és az üzemanyag élettartamát.

[10] *System for Nuclear Auxiliary Power* 2025.

[11] Adorján–Rétfalvi 2022.

[12] A HALEU *(high-assay low-enriched uranium)* egy speciális uránüzemanyag-kategória, amelynek neve paradoxonnak tűnik, de pontosan írja le a tulajdonságait: „magas próbaértékű alacsony dúsítású urán", vagyis a hasadóképesebb urán-235 (U-235) izotóp aránya magasabb a szokásosnál, de még mindig az alacsony dúsítású (LEU) tartományban marad (<20%).

[13] Fejlett nukleáris üzemanyagtípus, amely mákszem méretű (kb. 1 mm átmérőjű) gömböcskékből áll, kifejezetten magas hőmérsékletű, gázhűtésű reaktorokhoz, SMR-ekhez (például Xe-100, HTGR) fejlesztve.

1. táblázat: A nukleáris üzemanyagok típusai

Üzemanyag-típus	U-235 dúsítottság (%)	Átlagos égésfok (%)	Hőmérséklettűrés (°C)	Hulladéktermelés	Biztonsági jellemzők	Hol használják?
Természetes urán (NU)	~0,7	0,5–1	~800	Magas	Korlátozott	CANDU (Kanada: Bruce), Magnox (UK: Sizewell A)
Alacsony dúsítású urán (LEU)	<5	3–5	1200	Közepes	Szabványos PWR-biztonság	Paks (VVER-440, 30–4,95% UO_2), PWR (USA: Vogtle), BWR (Japán: Fukusima)
HALEU	5–19,75	10–20	1200–1400	Alacsony	Nagyobb hatékonyság, kevesebb hulladék	NuScale SMR (77 MW, <5% LEU/HALEU), Natrium (TerraPower)
Nagy dúsítású urán (HEU)	>20	20–90	1400–1600	Magas	Katonai, proliferációs kockázat	Atom-tengeralattjárók (USS Nautilus, K-3), fegyverek
TRISO gömböcskék	10–20 (HALEU alapú)	30–99	>1600	Nagyon alacsony	Önzáró, extrém sugárzásállóság	Xe-100 (X-energy), HTGR (UK: HTR-PM, Kína)
Urán-oxid (UO_2)	3–5	40–50	1200	Közepes	Standard pálcák	Paks (UO_2 tabletták), Westinghouse PWR
Urán-oxikarbid (UCO)	3–5	40–60	1500	Kisebb mint UO_2	Hőállóbb, sűrűbb	Fejlett SMR-ek (NuScale prototípusok), HTGR-ek
MOX (kevert-oxid)	4–7 (Pu-val)	5–8	1200	Közepes (újrahasznosított)	Plutóniumtartalmú, biztonsági protokollok	Paks kísérleti kazetták, EDF (Franciaország)

Forrás: a szerzők szerkesztése

Érdemes megemlíteni, hogy a paksi atomerőmű többféle üzemanyagot használ (és használhat) a VVER-440 reaktorokban.[14] Tesztelik az új generációs üzemanyagokat is a hatékonyság növelése érdekében, miközben a fő típus a standard LEU/UO_2 marad.

Az SMR-ek katonai alkalmazásokban rejlő potenciálját jól mutatja a Project Pele (USA) – amely egy mobil, gyors telepítésű, így akár hadszíntéri energiaellátást is képes biztosítani –, valamint az amerikai haditengerészet és a NATO érdeklődése a moduláris energiaforrások iránt. A technológiai fejlődés egyre inkább előtérbe helyezi a biztonságos, környezetbarát és decentralizált nukleáris energia szerepét a 21. századi energiarendszerekben.

[14] *Hogyan működik* 2021.

Az SMR-ek hulladéktermelése, kezelése és költséghatékonysága

A hulladéktermelés terén az SMR-ek akár 30–40%-kal kevesebb kiégett üzemanyagot termelhetnek az ugyanolyan villamos energia előállítása mellett, mivel nagyobb üzemanyag-hatékonyságot tesznek lehetővé. Egy hagyományos PWR (nyomásvízkazános reaktor) blokk, mint a paksi 4×1000 MW egység, évente kb. 25–30 tonna kiégett kazettát termel 1 GWe-nyi[15] termelés mellett, ahol az urán-235-ös égésfok mindössze 4-5% (a maradék 95% U-238 és hasadási termékek). Ezzel szemben az SMR-ek – különösen a TRISO- vagy HALEU-alapúak – 10–20%-os égésfokot érnek el, így 1 GWe-re vetítve csak 15–20 tonna hulladék keletkezik, radikálisan csökkentve a tárolási igényt.

Hogy mindez nagyságrendileg érzékelhető legyen: egy 300 MW-os BWRX-300 SMR (GE-Hitachi) 40 év alatt kb. 200–250 m^3 hulladékot termel, szemben egy AP1000 (1100 MW) 800–1000 m^3-jével – ez egy focipályányi terület 3 m magasságban szemben a kétszer akkora mennyiséggel. A TRISO-gömböcskék különösen hatékonyak: 99%-os égésfok mellett a radioaktív frakció <1%, főleg rövid felezési idejű izotópok (Cs-137: 30 év, Sr-90: 29 év), míg a hagyományos UO_2-pálcákban 5–10% hosszú élettartamú (például Pu-239: 24 000 év, Am-241: 432 év) izotópok találhatók, amelyek sokkal tovább terhelik a környezetet.

A hulladékkezelés megoldásai az SMR-eknél diverzifikáltak:

- Átmeneti tárolás: szárazkazetta-rendszerek (VASCO, Holtec), ahol a kazettákat hűtött, passzív légkeringtetésű konténerekben tartják 10–20 évig, amíg a hőtermelés 90%-a elmúlik.
- Újrafeldolgozás: PUREX-eljárással (La Hague, Franciaország) a Pu és U kinyerhető és 96%-ban újrahasznosítható – SMR-eknél ez 50–70%-ra növelhető HALEU-visszanyeréssel.
- Geológiai elhelyezés: mélyfúrásos *repositoryk*[16] (például Yucca Mountain koncepció, 500–1000 m kvarcitban), ahol a hulladékot réz/vitrifikált üveg konténerekben zárják el 100 000 évre.
- Transzmutáció: gyorsreaktorokban (például Natrium) neutronbombázással a hosszú élettartamú aktinoidákat (Np-237, Am-243) rövidebb feleződésűvé alakítják.
- Sugárzási időtartam: az SMR-hulladék 90%-a 300 év alatt <1 mSv/órára csökken (természetes háttérszint), a maradék 10% (aktinoidok) 10 000 évig jelent kockázatot, de vitrifikációval ez 1% alá csökkenthet. Összehasonlítva: a szénalapú erőművek évente 100 000 tonna hamut termelnek nehézfémekkel (arzén, higany), sugárzása 100-szorosa az atomerőmű hulladékának térfogatára vetítve.

A szén, mivel a földből bányásszák, nyomokban mindig tartalmaz természetes radioaktív elemeket (urán, tórium, kálium-40), valamint ezek bomlástermékeit (például rádium, radon). Ezek az anyagok a földkéregben mindenhol ott vannak, így a szénben

[15] GWe (Gigawatt-electric): elektromos teljesítmény-mértékegység. Az erőmű által a villamosenergia-hálózatba táplált hasznos elektromos teljesítményt jelöli, megkülönböztetve a reaktorban keletkező hőteljesítménytől.

[16] *Repository* (végleges tároló): a radioaktív hulladékok hosszú távú, biztonságos elhelyezésére és a környezettől való elszigetelésére szolgáló létesítmény.

is. Amikor a szenet elégetik, az éghető szerves anyag (a szén maga) elég és CO_2 formájában távozik. A radioaktív elemek azonban nem égnek el, hanem visszamaradnak a hamuban és a pernyében. Mivel a szén térfogata az égés során drasztikusan lecsökken, e maradványban pedig ezen radioaktív anyagok koncentrációja akár a 10-szerese is lehet az eredeti szénének.

2. táblázat: SMR és „hagyományos" atomerőművek összehasonlítása

Paraméter	**Hagyományos atomerőmű (PWR/VVER, 1000 MW)**	**SMR (SMR, 60–300 MW)**	**Hatékonyság és megjegyzések**
Teljesítmény (MW)	1000	60–300	SMR kisebb egységekben, moduláris bővítés
Személyzet	600–800 fő	20–50 fő	SMR automatizált, kisebb személyzet, 75–95% költségmegtakarítás személyzeti téren
Hulladéktermelés	25–30 tonna/év/GWe	15–20 tonna/év/GWe	SMR akár 30–40%-kal kevesebb hulladék, hatékonyabb üzemanyag-felhasználás
Üzemanyag-dúsítás	301505% U-235	5–20% (HALEU)	Magasabb dúsítás SMR-eknél növeli a hatékonyságot és csökkenti hulladékot
Bekerülési költség	6–9 milliárd USD/GWe	4–6 milliárd USD/GWe	SMR gyorsabb telepítés, moduláris, kevesebb újraegyesítés, alacsonyabb kockázat
Üzemanyagköltség	5–7 USD/gj	4–6 USD/gj	SMR kevesebb üzemanyagot használ, de a HALEU drágább
Területigény	2–4 km²	0,1–0,5 km²	SMR sokkal kisebb, jobb telepítési rugalmasság
Telepítési idő	10–15 év	2–4 év	SMR lényegesen gyorsabb kapacitásnövelést tesz lehetővé
Üzemanyagégési hatékonyság	4–5%	10–20%	SMR magasabb égésfok, kevesebb hulladék
LCOE *(levelized cost of electricity)*	70–95 USD/MWh	40–60 USD/MWh	SMR költséghatékonyabb, különösen a kisebb méret és automatizálás miatt

Forrás: a szerzők szerkesztése

A telepítési idő lényegesen rövidebb, míg egy hagyományos atomerőmű (például Vogtle-3/4, USA) megépítése 10–15 évet (és kb. 30 milliárd USD-t) vesz igénybe engedélyezéssel, tervezéssel, építéssel együtt, addig egy SMR 2–4 év alatt telepíthető – gyári előgyártott modulokból (a NuScale gyártási kapacitása 12 modul/év), gyors hatósági jóváhagyással (NRC: 18 hónap). Ez különösen fontos a gyors energetikai válaszlépések szempontjából, például háborús helyzetben (ukrán mintára) vagy klímaváltozási katasztrófák utáni helyreállításban.

Üzemeltetési költségeik akár 30–40%-kal alacsonyabbak is lehetnek a moduláris felépítés, az automatizált rendszerek és az egyszerűbb karbantartás miatt: az LCOE[17] 40–60 USD/MWh, míg a hagyományos 70–90 USD/MWh (2025-ös becslés). A kisebb személyzet (20–50 fő vs. 800), a passzív biztonsági rendszerek (termoszifonhűtés, nincs aktív pumpa) és hosszabb üzemanyagciklus (8–12 év vs. 18 hónap) mind csökkentik a kiadásokat, miközben a modulcserével *plug-and-play* karbantartás lehetséges.

Nukleáris hulladék kezelése: Újrahasznosítás és innovatív megoldások az SMR-eknél

A nukleáris hulladék nem csupán „mélyre ásás" kérdése – a hagyományos geológiai elhelyezés (például olyan 500–1000 m mély kvarcit repositoryk, mint a finn Onkalo vagy a tervezett Yucca Mountain) mellett számos fejlett technológia létezik, amelyek akár 96%-os újrahasznosítási arányt tesznek lehetővé, különösen az SMR-ek esetében. A kiégett üzemanyag nem homogén: 94–96%-a újrahasznosítható urán (U-238 → U-235 dúsításra), 1% plutónium (újrahasznosítható MOX üzemanyagként), és csak 4–5% valódi hosszú élettartamú hulladék (minor aktinoidok: americium, neptunium). Az SMR-eknél ez az arány még kedvezőbb: magasabb égésfok (10–20% vs. 4–5%) miatt kevesebb hulladék keletkezik kezdetben, és a TRISO-gömböcskék önzáró mikrokapszulái extrém biztonságot nyújtanak olvadás vagy baleset esetén.

A következő újrahasznosítási technológiákat használják a leggyakrabban:

- PUREX eljárás (Franciaország, La Hague): a kiégett kazettákat nitrilsavval oldják fel, majd oldószeres extrakcióval választják szét az uránt (96% visszanyerés), a plutóniumot (1%) és a hulladékot. Az újrahasznosított U/Pu MOX-ként kerül vissza a reaktorokba – Franciaország 30 éve működik ezel a modellel, évente 1100 tonna hulladékból 1000 tonna új üzemanyag készül. Az SMR-eknél ez különösen hatékony: a HALEU visszanyerése olcsóbb, mivel kisebb dúsítási lépcső kell (5–19% vs. 3–5%).
- Transzmutáció gyorsreaktorokban: a hosszú élettartamú izotópokat (Pu-239: 24 000 év, Am-241: 432 év) neutronbombázással rövidebb feleződésűvé alakítják. Az USA Natrium SMR-je (TerraPower) nátriumhűtésű gyorsreaktor, amely hagyományos hulladékot „eszik": 60 év alatt 90%-át transzmutálja, maradékát 300 évre csökkenti. Oroszország BN-800-ja ugyanezt teszi, és Paks is feldolgozhatná a hulladékát.
- Pirometallurgia (elektrolízis): száraz eljárás, ahol a fémhulladékot olvadt sóban (chlorkálium) elektrolízissel választják szét, amellyel a plutóniumot úgy módosítják, hogy ne legyen felhasználható fegyvergyártásra.
- Vitrifikáció: a maradék 4% hulladékot (hasadási termékek: Cs-137, Sr-90) bórszilikát üvegbe olvasztják 1100 °C-on, titánium konténerekbe zárva. A boroszilikát üveg 500 000 évig stabil.

[17] *Levelized cost of electricity:* fajlagos energiatermelési költség. Egy erőmű teljes élettartamára vetített összes költségének (beruházás, üzemeltetés, tüzelőanyag, finanszírozás) és az ezalatt megtermelt összes villamos energiának a hányadosa. Azt az átlagárat jelöli, amelynél a beruházás a teljes életciklus alatt megtérül.

3. táblázat: Nukleárishulladék-feldolgozási módszerek

Módszer	Hatékonyság	Időtartam-csökkentés	SMR-előny	Példa
PUREX újrahasz-nosítás	96%	–	HALEU-vissza-nyerés	La Hague
Transzmutáció	90%	10 000 → 300 év	Kis volumen	Natrium
Vitrifikáció	100% stabil	500 000 év	Kompakt	Onkalo
Piroprocesszus	99%	–	Fegyverbiztonság	Dél-Korea

Forrás: a szerzők szerkesztése

SMR-specifikus hulladékkezelés: miért hatékonyabb?

Az SMR-eknél a hulladékmennyiség 30–40%-kal kisebb GWe-re vetítve a magasabb égésfokú üzemanyag-használat miatt. Egy NuScale 77 MW modul 40 év alatt 50 m^3 hulladékot termel, míg egy 1000 MW-os PWR 500 m^3-t. Ez tízszeres térfogatcsökkenés, ami logisztikai és költségelőnyök sorozatát eredményezi.

Mennyiségi összehasonlítás részletesen, példaszámítás 1 GWe/év termelésnél:

- PWR: 25 tonna kiégett kazetta → PUREX után 1 m^3 vitrifikált hulladék;
- NuScale SMR: 15 tonna → 0,6 m^3 vitrifikált hulladék;
- 40 évre vetítve: 40 m^3 vs. 24 m^3 (focipálya 10 cm vs. 6 cm magas halom);
- sugárzás 300 év után természetes háttérszint (<0,1 mSv/h) mindkettőnél, de az SMR kisebb volumene 10-szer olcsóbb tárolást jelent (500 m mély repositoryként).

4. táblázat: Nukleáris hulladék termelése hagyományos vs. SMR reaktorokban 1 GWe-re vetítve

Paraméter	PWR (1000 MW)	NuScale SMR (77 MW)	Hatékonyság, előny
Hulladék/GWe/év (tonna)	25–30	15–20	30–40%
Égésfok (%)	4–5	10–20 (TRISO: 99)	2–4-szer magasabb
40 év hulladék (m^3)	500	50	10-szer kisebb térfogat
Vitrifikált végtermék (m^3)	40	2,4	16-szer kompaktabb
Tárolási költség (MUSD)	100–150	10–15	90% megtakarítás
Sugárzási idő (effektív)	300+ év	300 év (<1% marad)	Ugyanaz, kisebb volumen

Forrás: a szerzők szerkesztése

TRISO[18]-kapszulák alkalmazása SMR-ekben: előnyök és hátrányok

A TRISO-gömböcskék használata kis moduláris reaktorokban drámaian fokozza a biztonságot, mivel a mákszem méretű mikrokapszulák négyszeres kerámia páncéllal (puffer-szén-SiC-szén) körülzárják a radioaktív részecskéket, megakadályozva a kioldódást még 2000 °C feletti hőmérsékleten is. Ez a passzív biztonsági paradigma lehetővé teszi a *walk-away safe* üzemmódot: teljes áramkimaradás esetén a termoszifonhűtés mellett a TRISO önzáró tulajdonsága garantálja, hogy semmilyen radioaktív anyag ne jusson a környezetbe, a dózisküszöb <0,01 mSv/h marad. Az üzemeltetés jelentősen egyszerűsödik, mert a 99%-os égésfok miatt 40 évig elhanyagolható töltéscserére van szükség, a személyzetigény 35 főre csökken, a karbantartás a modulcserére korlátozódik. Előnyök: kiváló proliferációellenes[19] tulajdonság (fegyverminőségű plutónium előállítása gyakorlatilag lehetetlen), 10-szer kisebb hulladékmennyiség, magasabb termikus hatékonyság (45–50%), balesetbiztos működés. Hátrányok: gyártási költség 2-3-szor magasabb, HALEU-beszállítói lánc korlátozott (Oroszország-dominancia), gyári infrastruktúra-fejlesztés szükséges (például X-energy Oak Ridge üzem – 2025),[20] a kezdeti licencelési procedúrák pedig elhúzódnak. Összességében a TRISO az SMR-ek stratégiai biztonsági magja, amely a polgári és katonai alkalmazásokban egyaránt paradigmaváltást jelent, hosszú távon kompenzálva a magasabb kezdeti befektetést.

Kockázatok, nemzetbiztonsági alkalmazások és geopolitikai dimenziók

Az SMR-eket mint nemzetbiztonsági eszközt érdemes bemutatni. Európában elsősorban az energiaszuverenitás, Magyarországon az ellátásbiztonság, a Magyar Honvédségnél pedig a harctéri és kritikusinfrastruktúra-ellátás[21] szempontjából lehetnek kulcsfontosságúak ezek a megoldások.[22]

Európai energiaszuverenitás és kritikus[23] infrastruktúra

Európában az SMR-eket nem elsősorban katonai, hanem stratégiai energetikai eszközként kezelik: cél az orosz fosszilis forrásokról való leválás, a gázfüggőség csökkentése és a megújuló energiaforrások ingadozásának kiegyenlítése. A kockázat főként

[18] TRISO-mikrokapszulák technológiája. A TRISO-gömböcskék önzáró mikrokapszulái a nukleáris biztonság csúcsa: 10^{12} gömböcske/modul, mindegyik négyrétegű páncélban:
- pórusos szénpuffer: fissziós gázok (Xe, Kr) befogására;
- pirolitikus szén (PyC): mechanikai védelem;
- szilícium-karbid (SiC): 2000 °C-ig olvadásbiztos kerámia;
- külső PyC: végső tömítés.

[19] Azt a célt szolgáló műszaki vagy jogi megoldás, amely megakadályozza, hogy a polgári nukleáris technológiát és anyagokat atomfegyverek előállítására használják fel.

[20] Újfajta nukleáris termék gyártására készül az USA 2025.

[21] Munk 2002.

[22] Végvári 2016.

[23] Kovács 2007; Haig 2007.

szabályozási (engedélyezés, társadalmi elfogadottság) és pénzügyi (kezdeti magas CAPEX,[24] piaci bizonytalanság), nem pedig technológiai jellegű.

Magyarországi SMR-ek mint nemzetstratégiai tartalék

Magyarország középtávon 2030 utáni üzembe helyezésre készül, akár több SMR-rel is, 10–20 milliárd dolláros beruházási sávban, részben amerikai technológiára támaszkodva.

A fő célok:

- villamosenergia-ellátás diverzifikálása Paks I–II mellett;
- regionális exportképesség;
- nagyipari fogyasztók (például hadiipari, akkumulátor- és hidrogénüzemek) lokális nukleáris ellátása.

Az Országos Atomenergia Hivatal már részt vesz az EU SMR-hatósági munkacsoportban, ami jelzi, hogy már zajlik a jogi-szabályozási előkészítés. Kockázatot jelent azonban a beszállítói függőség (HALEU, nyugati–orosz üzemanyag-szétválás), társadalmi kommunikáció, valamint az, hogy a hazai hálózati és ipari struktúrát időben adaptálni kell.

Magyar Honvédség: energialogisztika és harctéri ellátás

A Magyar Honvédség békeidőszaki energiaköltsége a teljes magyar villamosenergia-felhasználás kevesebb mint 0,2%-a, ugyanakkor az infrastruktúra (laktanyák, logisztikai központok, bázisok, kommunikációs és irányítóközpontok) nagy mértékben függnek a civil hálózattól. Ezek sebezhetősége (például kibertámadás, hálózati zavar, regionális áramszünet) erősen veszélyeztetheti a katonai képességeket.

Egy vagy több, honvédségi területen telepített SMR:

- szigetüzemű, önálló támaszpont-energiaellátást biztosíthat (radarok, vezetési pontok, UAV-bázisok, híradó hálózat);
- kiválthatja a nagy mennyiségű dízelüzemanyag-tárolást és konvojlogisztikát, csökkentve a támadási felületet;
- integrálható harctéri energiaellátó koncepciókkal (konténeres SMR-projektekhez hasonlóan, Project Pele-analógia[25]).

A rendvédelmi és katasztrófavédelmi szervek számára az SMR-ek a kritikus infrastruktúrák (ivóvíz, kommunikáció, egészségügy, irányítóközpontok) szünetmentes ellátását jelenthetik nagyobb katasztrófák (árvíz, hosszú idejű hálózati zavar, regionális konfliktus) esetén.

[24] Tőkeberuházási költség: a létesítmény megépítéséhez szükséges egyszeri, kezdeti kiadások (tervezés, építés, technológia) összessége.

[25] Az Egyesült Államok Védelmi Minisztériumának (DoD SCO) fejlesztési programja, amelynek célja egy szabványos konténerekben szállítható, közúton és légi úton is mozgatható, 1–5 MWe teljesítményű, biztonságos (TRISO-tüzelőanyagot használó) nukleáris mikroreaktor kifejlesztése katonai bázisok energiaellátására.

5. táblázat: Kockázatok és honvédelmi szempontok

Dimenzió	Hagyományos nagyerőmű	SMR hazai/katonai telepítése	Magyar Honvédség szempontja
Ellátás függése a civil hálózattól	Nagyfokú	Részlegesen függetleníthető	Kritikus bázisok leválaszthatók
Harctéri/logisztikai sérülékenység	Magas (üzemanyag-konvojok)	Alacsonyabb (helyben termelés)	Kevesebb konvoj, kisebb támadási felület
Telepítési rugalmasság	Korlátozott (fix telephely)	Magas (moduláris, regionális)	Tábori és állandó bázisok differenciált ellátása
Szabályozási/jogi komplexitás	Bejáratott	Növekvő, kevés precedens	Honvédelmi kivételek + polgári keretek összehangolása
Célpontkockázat *(strike value)*	Nagyon magas	Kisebb, szétszórt modulok	Decentralizált, nehezen bénítható energiarendszer

Forrás: a szerzők szerkesztése

Következtetések, ajánlások, javaslatok

Bár az SMR-ek képesek szigetüzemű, helyi áramtermelésre, a termelt energia elosztása további kihívásokat jelent. A meglévő hálózatokat bővíteni és korszerűsíteni kell, hogy befogadják és kezelni tudják a decentralizált forrásokból érkező energiát. Fontos hangsúlyozni, hogy az SMR-ek csak villamos energiát termelnek, így nem pótolják a katonai vagy ipari szektorokban jelenleg használt gázolajat vagy más üzemanyagokat. Emellett a villamosenergia-tárolás jelenleg még nem optimális a szélerőművek vagy naperőművek területén is ismert problémák miatt, amelyek az SMR-eknél is jelentkezhetnek. Különösen problémás, hogy az SMR-ek termelése általában egy minimális kapacitás alá nem csökkenthető, így előfordulhat, hogy időszakosan jóval kevesebb energia szükséges, mint amennyit az SMR képes előállítani, ezáltal a felesleget a hálózatba kell táplálni. Ez hasonló helyzetet teremt, mint a nyári időszakokban a lakossági naperőművek esetén, amikor az energiafelesleg eladása kritikus kérdés.

Az SMR-technológia széles körű társadalmi elfogadása és támogatása nélkülözhetetlen a sikeres bevezetés és alkalmazás szempontjából. Ehhez a legfontosabb a hiteles, folyamatos és nyitott kommunikáció a lakosság és a civil szervezetek felé. Részletesen be kell mutatni, hogyan működik az SMR, milyen passzív biztonsági rendszerei vannak, és miként képesek megakadályozni a hagyományos erőműveknél előforduló baleseteket. Be kell mutatni a nukleáris hulladék hosszú távú biztonságos kezelésének módszereit. Fontos hangsúlyozni, hogy az SMR-ek üzemanyagként használják a TRISO-kapszulákat, amelyek rendkívül ellenállók, és jelentősen csökkentik a radioaktív anyagok kiszabadulásának veszélyét még extrém körülmények között is.

Fontos a szoros együttműködés az oktatási intézményekkel és médiaorgánumokkal, hogy a tudományos alapokon nyugvó tényeket széles körben terjesszék. A közösségi

részvétel és a párbeszéd elősegíti a bizalomépítést, csökkenti a technológiával kapcsolatos ellenállást.

Nem elhanyagolható az sem, hogy az SMR-ek telepítése előtt a helyi lakosságot alaposan tájékoztassák az üzemeltetés környezeti és biztonsági aspektusairól, valamint a vészhelyzeti protokollokról. A transzparens információáramlás mellett a technológia sikeressége érdekében szükséges az állami és nemzetközi szabályozók által előírt szigorú ellenőrzés és független auditálás. Ez nemcsak a biztonságot garantálja, hanem a társadalmi elfogadást is. Összességében tehát a megfelelő kommunikáció és oktatás egyaránt előfeltétele az SMR-technológia társadalmi elfogadottságának és a sikeres energetikai átmenetnek.

Felhasznált irodalom

Adorján Ferenc – Rétfalvi Eszter (2022): A kisméretű moduláris atomerőművek (SMR), mint a klímavédelem ígéretes eszközei. *Nukleon,* 15(1), 1–11. Online: https://nuklearis.hu/sites/default/files/nukleon/15_1_243_Adorjan.pdf

Boda Mihály (2024a): A háború mint kaméleon. A fegyvertechnika fejlődésének hatása a háború és a politika viszonyára a kezdetektől a mesterséges intelligenciáig. *Hadtudomány,* 34(3), 99–113. Online: https://doi.org/10.17047/HADTUD.2024.34.3.99

Boda Mihály (2024b): A kockázatkerülő háború és a bátorság a 20–21. század fordulóján. *Honvédségi Szemle,* 152(3), 113–115. Online: https://real-j.mtak.hu/26962/13/HSz_2024_3.pdf

Haig Zsolt (2007): Az információs társadalmat fenyegető információlapú veszélyforrások. *Hadtudomány,* 17(3), 37–56. Online: https://real-j.mtak.hu/29477/3/Hadtudomany_2007_3.pdf

Hogyan működik (2021). Online: https://atomeromu.mvm.hu/Tudastar/HogyanMukodik

Kovács László (2007): Kritikus információs infrastruktúrák Magyarországon. *Hadmérnök,* 2007. november 27. Online: http://hadmernok.hu/kulonszamok/robothadviseles7/kovacs_rw7.html

Munk Sándor (2002): Információs színtér, információs környezet, információs infrastruktúra. *Nemzetvédelmi Egyetemi Közlemények,* 6(2).

Naumenko, Natalia Yu – Mokhireva, Inna M. (2022): TES-3 – Transportable Nuclear Power Plant Mounted on Self-propelled Tracked Vehicles. *Nuclear Energy and Technology,* 8(2), 139–142. Online: https://doi.org/10.3897/nucet.8.89356

Retro Transport [@RetroTransport] (2024) TES-3: The Soviet Nuclear Monster on T-10 Tank Chassis. *YouTube,* 2024. november 16. Online: www.youtube.com/watch?v=KJqo2PEqHm8

System for Nuclear Auxiliary Power (SNAP) Overview (2025). Online: www.energy.gov/etec/system-nuclear-auxiliary-power-snap-overview

The 1958 Ford Nucleon: An Idea That's Still ahead of Its Time. *Nuclear Newswire,* 2021. július 12. Online: www.ans.org/news/article-3058

Újfajta nukleáris termék gyártására készül az USA – van egy erős magyar szál a történetben (2025). *VG.hu,* 2025. november 19. Online: www.vg.hu/nemzetkozi-gazdasag/2025/11/smr-x-energy-triso-uzemanyag

Végvári Zsolt (2016): Harctéri villamosenergia-ellátás. Új energetikai megoldások kutatásának szükségessége és a fejlesztési lehetőségek összevetése. *Katonai Logisztika,* 24(2), 52–74. Online: https://epa.oszk.hu/02700/02735/00082/pdf/EPA02735_katonai_logisztika_2016_2_052-074.pdf

HADMÉRNÖK
KATONAI LOGISZTIKA

21. évfolyam (2026) 3. szám 137–147.
DOI: 10.32567/hm.2026.3.9

Norbert Daruka,[1] Kálmán Dénes,[2] Zoltán Kovács,[3]
Róbert Vég,[4] István Ember[5]

The Impact of Additive Manufacturing Used in the Russo–Ukrainian Conflict on Decentralised Manufacturing[6]

Abstract

3D printing is one of the most widespread disruptive technologies today. It also plays a significant role in wartime, especially when the appropriate background and system are available. By combining this technology with digital warehousing and decentralised manufacturing, we can identify the most important cornerstones in the operational environment and challenges of the Russo–Ukrainian conflict. Since we conducted our analysis using data obtained from an active war environment that can be considered reliable, we can state that we have successfully identified the most important elements and categories of decentralised manufacturing associated with this technology.

Keywords: decentralised manufacturing, 3D printing, additive manufacturing, digital warehouse

[1] Explosives industrial engineer, e-mail: daruka.norbi@gmail.com
[2] Civil engineer, e-mail: denes.kalman.1975@gmail.com
[3] Associate Professor, Ludovika University of Public Service, Department of Combat Support, e-mail: kovacs.zoltan@uni-nke.hu
[4] Associate Professor, Ludovika University of Public Service, Department of Military Technology, e-mail: vegh.robert@uni-nke.hu
[5] Assistant Professor, Ludovika University of Public Service, Department of Combat Support, e-mail: ember.istvan@uni-nke.hu
[6] This paper was supported by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences.

Introduction

Today, armed forces face a series of challenges that pose significant difficulties. These can be global problems, such as ongoing environmental and climate change,[7] the appropriate and secure integration of artificial intelligence into current systems,[8] or local problems, such as an armed conflict that pits two or more nations against each other.

No matter how we look at these issues, one thing is certain. There are disruptive technologies available that play a significant role in these processes or can help manage negative developments. Additive manufacturing is such a technology. It is developing rapidly, has become part of everyday life, and is gaining an increasingly large share of the industrial segment.

This technology is capable of processing both simple polymers and specialised raw materials[9] for the production of customised items. It can be used to produce both simple components and complex structures, and in the event of an armed conflict, it can ensure part of our supply of spare parts,[10] or parts of offensive weapons can be manufactured using it. This segment may include drones that simply collect and transmit data[11] but versions designed to destroy the enemy also belong here.

The Russo–Ukrainian war provides us with a picture of the real-world application of 3D printing and the unique circumstances surrounding it, which are linked to digital warehousing and decentralised manufacturing. The aim of this publication is to identify the cornerstones of this symbiosis, analyse the way it works, and categorise its elements in order to obtain a comprehensive and detailed picture of the situation that has developed.

3D printing in the Russo–Ukrainian war

One of the most decisive weapons in the Russo–Ukrainian war are unmanned aerial vehicles (hereinafter: UAVs). Both sides use this technology thousands of times a day on the eastern front. One of the key weapons in Russia's deep strikes is the Geran–2 (a clone of the Iranian-developed Shahed–136), of which, according to some sources, thousands have already been manufactured and used in deep distance strikes. This is a situation that could not go unanswered, so the Ukrainian side naturally stepped up the production of interceptor drones. All this is already happening on a mass production scale, which could reach as many as 10,000 units.[12]

In case of drone warfare, a war competition between so-called 3D printing farms equipped with 3D printers is unfolding. These units are capable of producing a significant number of plastic parts for these UAVs, such as frames (Figure 1), covers, control

[7] Padányi 2022; Padányi 2024.
[8] Négyesi–Fazekas 2022; Fazekas 2023.
[9] Halinka et al. 2023; Vég 2023: 86.
[10] Gávay 2024; Gyarmati et al. 2025.
[11] Szilágyi et al. 2024.
[12] Tyrer-Jones 2025.

surfaces, propellers, mechanical parts, etc. This method is fast and efficient, but not necessarily cheap. In case of one-way attack (hereinafter: OWA) UAVs, it is not necessary to manufacture them to a high standard of durability, as these first-person view (hereinafter: FPV) devices usually only carry out a single combat mission during their lifetime. This means that even lower-quality devices and components may be acceptable, although this is a sensitive issue when human lives may depend on it.

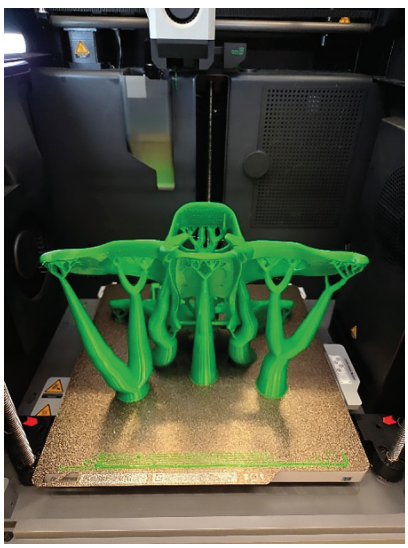


Figure 1: Drone frame during 3D printing
Source: compiled by the authors

3D printing is an effective method for manufacturing explosive components. It is important to note that the technology is not yet capable of producing shaped charge using explosives as printing materials, so plastic or liquid explosives must be used for their final production. It is not necessary to manufacture all components, as the latest explosive devices are only partially improvised. The armed forces modify and supplement these otherwise standard devices to make them more effective or to enable them to be deployed from completely different weapon platforms, even UAVs.

Ukrainian forces are also using devices known as "Candy Bombs" against Russian troops. These consist of casings manufactured using additive manufacturing, which are filled with conventional plastic explosives and covered with fragments. These are mostly manufactured not by professional factories, but by volunteers, in close cooperation with users. Of course, there are no official data on their number, but the number of devices imported into Ukraine so far can be estimated at several tens of thousands. There are two other special features of this activity. Production is not carried out by professional specialists, but artificial intelligence (hereinafter: AI) based software is now used for design tasks. It is important to note that the components arrive in the recipient country as children's toys during customs clearance,

thus concealing their original purpose. Since they are made of plastic, the latter fact may not be apparent to the untrained eye.[13]

As a specific example, Ukrainian force trainees have converted RKG–3 anti-tank grenades in this way. The final result is an aerial bomb that can be effectively deployed using commercially available drones. According to some sources, the accuracy of the converted offensive weapons is within a 1-metre radius from a height of 300 metres. This successful development is underscored by the fact that today every Ukrainian brigade has some amount of additive manufacturing capacity.[14]

In addition to all this, Ukraine receives a great deal of support from Western countries, including 3D printers. Some of these are capable of operating reliably in operational areas. The device developed for the production of metal parts the size of shipping containers, for example, is unique in its kind and capable of producing parts weighing up to 40 kg.[15] Of course, spare parts supply is a key issue in wartime. One of the most important tools for relieving the burden on supply chains and becoming independent of them is 3D printing,[16] and there is perhaps no simpler solution for manufacturing spare parts or replacement parts, although there is a downside to everything. As we mentioned earlier, in case of equipment and parts that are exposed to heavy loads, their service life may be significantly reduced, and maintenance cycles may be shortened. This can be compensated for with appropriate engineering expertise and material selection, and in some cases can even be improved compared to the original part.

Of course, the Russian side also uses this disruptive technology, although significantly less information is available about it on the Internet and other sources. However, even in the absence of information, it can be strongly assumed that they also exploit the combat advantages inherent in additive manufacturing, which can even reach a strategic level.

According to the available information, the Russian army also uses fixed farms where specially trained units manufacture drone components using additive manufacturing tools. Of course, based on what has been said, they are able to satisfy anyone's needs with their tools, including the manufacture of components for explosive devices.[17]

Digital warehouses

Digital repositories (databases or libraries) are structured data storage systems that are suitable for storing, managing, organising and searching large amounts of information (mainly design documentation). These interfaces do not function solely as information storage locations, but can also be dynamic platforms for information flow, knowledge sharing, learning and collaboration. These digital interfaces are

[13] Dass 2024.
[14] Dass 2024.
[15] Verdict 2024; XSPEE3D s. a.
[16] Saber et al. 2025: 52.
[17] Sputnik International 2024.

mostly accessible online, which can have numerous advantages if cybersecurity is also emphasised during their development.[18]

These advantages include, but are not limited to, the following:[19]

- Global, unlimited access. Online access without opening hours allows users to access digital materials stored in the database anytime, anywhere, provided they have the appropriate technical equipment and network access.
- Search and filter function. The registration, search, and filter functions in digital warehouses enable you to find the information you need quickly and efficiently.
- Significant storage capacity. Digital warehouses can store and manage huge amounts of information in digital form.
- Provision of interactive content. Digital databases offer access to interactive content (e.g. instructional videos, interactive maps, assembly instructions) and other multimedia elements.
- Easy management of changes. The content of digital warehouses can be easily updated, modified and maintained, ensuring that users always have access to up-to-date data and information.

With the advantages listed above, such a platform provides faster, more efficient, more flexible and more convenient access to information online, far surpassing traditional methods (traditional libraries, education, reading, etc.). Although databases are vulnerable to security risks, they have proven their worth in manufacturing areas.[20]

In order to ensure that the physical conditions for 3D-printing are met in a well-organised infrastructure, the personnel operating the technical equipment, technicians and engineers must have access to the relevant information, data and files stored in the appropriate digital format. Such a platform ensures that staff do not need design expertise; excellent management of the manufacturing equipment is sufficient to produce parts of the required quality. There are currently several open-access websites where files suitable for 3D printing can be downloaded free of charge or for a fee. The files on these sites vary, ranging from simple household items to more complex structures. The biggest disadvantage of using these files is that special military components, parts and structures cannot be found there, as in many cases they are protected and restricted from the public by law, and the professional design and material selection of the parts cannot be adequately verified.[21]

According to Ukrainian officials, they already have a digital warehouse filled with digital documentation for more than 170 domestically designed components and plan to expand it radically in the future. The platform not only provides access to personnel, but also offers manufacturing services, most of which are, of course, advanced additive manufacturing capabilities. This interface connects the defence industry more closely and helps reduce dependence on supply chains. In technical terms, the repository is an online database. Only verified Ukrainian manufacturers can upload their documentation and obtain designs produced by others. Currently

[18] Daruka et al. 2024: 76.
[19] Daruka et al. 2024: 76–77.
[20] Daruka et al. 2024: 77.
[21] Daruka et al. 2024: 77.

available items include antennas, drone frames, propellers and special modules. A significant advantage is that it provides access to 11 different services (casting, 3D printing, etc.). These options allow manufacturers to respond to emerging needs with advanced solutions.[22]

In parallel with the operational advantages of digital warehouses, cybersecurity and information assurance emerge as critical enabling factors. As these repositories contain sensitive design data, production parameters, and in some cases classified military components, they constitute high-value targets for cyber espionage and sabotage. Compromise of such systems may result not only in the loss of intellectual property but also in the deliberate manipulation of design files, potentially leading to the production of faulty or unsafe components. Consequently, the protection of digital warehouses must extend beyond traditional access control and encryption measures and include integrity verification mechanisms, version control and secure authentication of uploaded files. In a decentralised manufacturing environment, trust in digital design data becomes a decisive operational factor.

Decentralised manufacturing

Centralised manufacturing capacity is not a strategy that is destined to succeed in today's warfare. Of course, this can be nuanced if the production units are located in a country that is legally protected, not directly involved in the conflict, or if the company has significant defence and countermeasure capabilities. However, these are special situations. In general, it can be said that almost the entire territory of a country involved in an armed conflict can be attacked with advanced weapons, although only the major powers have the military capacity and technological background for this. However, even more accessible deep strike systems are capable of causing significant damage to these types of facilities.

An often-underestimated element of decentralised manufacturing is the human factor. The effectiveness of additive manufacturing in combat environments does not solely depend on technological availability but also on the rapid transfer of practical knowledge to operators with limited formal engineering backgrounds. The Russo–Ukrainian conflict demonstrates that short, task-oriented training modules, standardised workflows, and intuitive manufacturing interfaces can compensate for the lack of traditional industrial expertise. In this context, digital warehouses serve not only as repositories of design files but also as platforms for accelerated learning, enabling soldiers and volunteers to adapt manufacturing processes to rapidly changing operational requirements.

From a strategic perspective, decentralised additive manufacturing significantly enhances system-level resilience. By distributing production capabilities across multiple geographically separated nodes, armed forces reduce their vulnerability to single-point failures caused by kinetic strikes or supply chain disruptions. Even limited-capacity manufacturing cells can maintain operational continuity by producing

[22] K. 2025.

mission-critical components locally. This resilience-oriented approach aligns with modern concepts of adaptive warfare, where survivability and flexibility are prioritised over economies of scale.

Decentralisation, on the other hand, has a significant advantage. Crowdfunding manufacturing is a new trend in this segment, but it works surprisingly well. One outstanding example of manufacturing financed by donations and community support is WildHornets. This Ukrainian military company uses the revenue generated in the manner described above to manufacture, among other things, FPV drones carrying various weapons, drone-hunting FPV UAVs, batteries, and ground control units on a 3D printing farm. They do all this using Bambulab 3D printers (Figure 2) and produce 65% of the UAVs themselves. According to their public statistics, Ukrainian troops have destroyed 151 tanks, 613 vehicles, 448 UAVs, 220 armoured vehicles, 122 artillery or MLRS units, 4 air defence units, and killed 818 soldiers. This resulted in a total loss of USD 1.69 billion for the Russian Federation.[23]



Figure 2: Drone parts made with a Bambulab X1E 3D printer
Source: compiled by the authors

Of course, other manufacturers also operate such hidden factories, and as mentioned above, products are also supplied from outside Ukraine, and military units also have self-sufficient capacity.

Taking all this into account, we can comprehensively interpret decentralised manufacturing, which has both a state-organised and a voluntary branch. Both the organised and voluntary versions can be integrated into the digital warehousing system, thus facilitating the production of the tools needed for the tasks and known to the soldiers.

[23] Tyrer-Jones 2025; Wild Hornets s. a.

However, it is worth further dividing the elements of production according to location, because we can distinguish between plants operating in a protected environment and plants located in conflict zones, which are usually technically hidden. In case of protected plants, the possibility of illegal, covert attacks or sabotage, even using secret service methods, must of course be taken into account.

It is also worth discussing state-organised manufacturing in order to get a complete picture of this ecosystem. This refers not only to the activities of players in the defence industry as part of traditional industry, but also to maintaining the army's self-sufficiency. Each component plays an important role, as it ensures that equipment and spare parts are available at all times. One of the keys to the success and efficiency of this system is its coordination with digital warehouses, so that all stakeholders can deliver fresh, high-quality products.

However, there are issues that need to be clarified. The right to manufacture spare parts is not unrestricted in all cases, although in case of old equipment that is no longer supplied, this is not an issue. However, in case of new, modern equipment, it is not always possible for the army to carry out repairs itself, and in some cases the manufacturing of replacement parts may result in serious industrial property rights infringements. A similar situation may arise if intellectual property (hereinafter: IP), designs, information and expertise are transferred to partners via digital warehouses without the consent of the copyright holder. These legal challenges are currently the biggest known limitations of the decentralised manufacturing ecosystem,[24] and the simplest solution is a royalty-based compensation system. In principle, the number of manufactured devices can be tracked, and a fee agreed in advance between the parties is paid to the rights holder, unless they explicitly waive this right.

Beyond legal and industrial property concerns, the widespread use of additive manufacturing in armed conflicts raises ethical and international humanitarian law-related questions. The low entry threshold of 3D printing technologies blurs the traditional distinction between state and non-state actors involved in weapons production.[25] Volunteer-based manufacturing initiatives, while operationally effective, challenge established accountability frameworks. These developments necessitate a reassessment of existing regulatory approaches to weapon manufacturing and highlight the need for updated international norms addressing digitally enabled decentralised production.

Another challenge is the process of quality assurance and standardisation. Military standards set high benchmarks that ensure reliable operation under difficult conditions. However, this is worth reconsidering, especially in case of OWA devices, because in many cases the technological solutions used to manufacture the products result in unreasonably high prices.

Although this is just one example, it is definitely worth storing the documents necessary for quality assurance in a digital repository so that the organisation can filter the finished products through self-checking.

[24] Chan et al. 2018: 156–162.
[25] Suckau 2025: 25–26.

This alone does not replace the importance of military acceptance. In case of standardisation, especially for UAVs, it is also worth considering the processes and defining technology circles rather than specific devices, and classifying the devices that fall within them as applicable. Obviously, this is only if they meet the predefined parameters and the expected quality.

Summary

The Russo–Ukrainian conflict offers valuable lessons for future military planning regarding the integration of additive manufacturing, digital warehousing and decentralised production. These practices are not limited to high-intensity conflicts but can be adapted to crisis response, peacekeeping operations and disaster relief scenarios. The rapid scalability, flexibility and cost-efficiency of such systems suggest that decentralised manufacturing will become a permanent element of modern military logistics rather than a temporary wartime solution.

Overall, we have managed to review and summarise – albeit not exhaustively – the practices used during the Russo–Ukrainian conflict in the context of 3D printing, digital warehousing and decentralised manufacturing.

The results show that, technically, decentralised manufacturing could also become a possibility for proxy financing, where supporting states and market players could enter an armed conflict covertly or even openly as non-belligerents. Regardless, this system, which is often built on community funding and donations, can be an excellent foundation for a country's self-defence. It requires organisation and preparation, but the benefits it provides become significantly more valuable as the intensity of operations increases.

There are still obstacles to overcome in order for this symbiosis between the three areas to function with maximum efficiency, but a solution is in sight. Moreover, once legal and quality assurance issues have been clarified, all parties can strive with increased intensity to achieve mutual success in such a system.

References

Chan, Hing K. – Griffin, James – Lim, Jia Jia – Zeng, Fangli – Chiu, Anthony S. F. (2018): The Impact of 3D Printing Technology on the Supply Chain: Manufacturing and Legal Perspectives. *International Journal of Production Economics,* 205(Special Issue), 156–162. Online: https://doi.org/10.1016/j.ijpe.2018.09.009

Daruka, Norbert – Dénes, Kálmán – Ember, István – Kovács, Zoltán – Vég, Róbert (2024): Digitális adatbázis létrehozásának lehetőségei a magyar honvédségben a 3D-nyomtatási képesség támogatására. *Honvédségi Szemle,* 152(4), 72–81. Online: https://doi.org/10.35926/HSZ.2024.4.6

Dass, Rueben (2024): 3D-Printing in Conflict Zones: A Game-Changer? *Global Network on Extremism and Technology,* 14 October 2014. Online: https://gnet-research.org/2024/10/14/3d-printing-in-conflict-zones-a-game-changer/?utm_source=chatgpt.com

Fazekas, Ferenc (2023): Mission Command and Artificial Intelligence. *Land Forces Academy Review,* 28(2), 69–79. Online: https://doi.org/10.2478/raft-2023-0010

Gávay, György (2024): Honvédségi járművek kezelőszerveinek pótlása, módosítása 3D-nyomtatási technológia alkalmazásával. *Műszaki Katonai Közlöny,* 34(3), 25–38. Online: https://doi.org/10.32562/mkk.2024.3.3

Gyarmati, József – Gávay, György – Hegedűs, Ernő (2025): Potential Applications of Different 3D Printing Technologies in Military Logistics. *International Scientific Conference VojNa 2025,* Belgrade. Online: www.researchgate.net/publication/399444603_Potential_applications_of_different_3D_printing_technologies_in_military_logistics

Hlinka, József – Erőss, László D. – Fendrik, Ármin – Bán, Krisztián (2023): Changes in Mechanical Properties Due to Heat Treatment on Additive Manufactured Ti-64AI-4V. *Communications – Scientific Letters of the University of Zilina,* 25(1), B1–B6. Online: https://doi.org/10.26552/com.C.2023.001

K., Joseph (2025): Ukraine Integrates 3D Printing into Secure Military Supply Platform. *3D Natives,* 7 October 2025. Online: www.3dnatives.com/en/ukraine-integrates-3d-printing-into-secure-military-supply-platform-07102025/

Négyesi, Imre – Fazekas, Ferenc (2022): A mesterséges intelligencia integrálásának lehetőségei a vezetési pontok feladatrendszerébe. *Hadtudományi Szemle,* 15(3), 145–159. Online: https://doi.org/10.32563/hsz.2022.3.9

Padányi, József (2022): *Kihívások, kockázatok, válaszok. Az éghajlatváltozás okozta kihívások és azok hatása a katonai erőre.* Budapest: Ludovika Egyetemi Kiadó.

Padányi, József (2024): *The Effects of Climate Change on the Military. Risks, Challenges and Answers.* Budapest: Ludovika University Press. Online: https://doi.org/10.36250/01185

Saber, Dalia et al. (2025): Additive Manufacturing (3D printing) and the Future of Supply Chains: Opportunities, Challenges, and Trends. *Global Journal of Engineering and Technology Advances,* 25(3), 51–64. Online: https://doi.org/10.30574/gjeta.2025.25.3.0336

Suckau, Liska (2025): Additive Manufacturing in the Military Technology Sector: Applications and Proliferations of an Emerged Technology. *PRIF Report,* (3). Peace Research Institute Frankfurt. Online: https://doi.org/10.48809/prifrep2503

Sputnik International (2024): *Russian Soldiers Use 3D Printers to Print Spare Drones and Ammunition Parts in Special Op Zone.* Online: https://sputnikglobe.com/20240310/russian-soldiers-use-3d-printers-to-print-spare-drones-and-ammunition-parts-in-special-op-zone-1117245366.html?utm_source=chatgpt.com

Szilágyi, Dávid – Sziroczák, Dávid – Rohács, Dániel – Fendrik, Ármin (2024): Feasibility of a Drone-Based Road Network Inspection System. *Engineering Proceedings,* 79(1). Online: https://doi.org/10.3390/engproc2024079076

Tyrer-Jones, Alex (2025): Ukraine Deploys 3D Printed Drones to Combat Russian Shahed Swarms. *3D Printing Industry,* 25 July 2025. Online: https://3dprintingindustry.com/news/ukraine-deploys-3d-printed-drones-to-combat-russian-shahed-swarms-242362/

Verdict (2024): 3D Battlefield Printing in Ukraine. *Verdict,* 15 January 2024. Online: www.verdict.co.uk/3d-printing-ukraine-battlefield/?cf-view&cf-closed

Vég, Róbert L. (2023): A 4D nyomtatás és az okosanyagok alkalmazásának lehetőségei. *Műszaki Katonai Közlöny,* 33(4), 77–89. Online: https://doi.org/10.32562/mkk.2023.4.6

Wild Hornets (s. a.): *Who We Are.* Online: https://wildhornets.com/en/who-we-are

XSPEE3D (s. a.): *Make Metal Anywhere. Containerised Metal 3D Printer.* Online: www.spee3d.com/wp-content/uploads/2023/11/SPEE3D_Consolidated_Corporate-Brochure_A4_4pp_V8.pdf

HADMÉRNÖK
KATONAI LOGISZTIKA

21. évfolyam (2026) 3. szám 149–164.
DOI: 10.32567/hm.2026.3.10

Szajkó Gyula,[1] Lévai Zsolt[2]

A közúti infrastruktúrák katonai megfelelőségi vizsgálata a logisztikai felderítés végrehajtásakor, 2. rész

The Military Suitability Assessment of Road Infrastructure During Logistic Reconnaissance, Part 2

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 kiemelt figyelmet kell fordítani a logisztikai szervezeteknek 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 mozgatási-szállítási feladatainak tervezésekor és szervezésekor. A cikkel a szerzők

[1] Adjunktus, 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

célja az, hogy 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 sector plays an important role in the integrated transportation system, and its operation and maintenance also have significant importance for the Hungarian Defence Forces (HDF), as it provides a connecting link between the bases of military organisations, airports, seaports and river ports, and railway stations. The movement of forces including military equipment, and personnel – between unloading ports (sea, air, and rail unloading ports) and the receiving operational areas – is carried out through road transport. Moreover, the largest volume of theater movement are carried out by road transportation. 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, logistics 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 gathering of information, it is advisable to use checklists and to define requirements for each feature of the 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 assessments of road infrastructure.

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

Cikksorozatunk első részében bemutattuk az útpálya és a csomópontok szempontjait és a hozzájuk rendelt követelményeket. A második részben elemezzük a műtárgyakra és az útpálya környezetére kialakított kritériumokat, majd meghatározzuk a megfelelőségi intervallumokat, amelyeket alkalmazva gyorsíthatóvá válhat a közúti infrastruktúrák logisztikai felderítése.

A követelmények meghatározására alkalmazott módszer

A tanulmánysorozatban összesen 4 fő infrastruktúra-elem szempontrendszerét mutatjuk be. A táblázatokba foglalt közutak elemeit (útpálya, csomópont, műtárgy, útpálya környezete) külön pontozzuk, súlyozzuk és értékeljük. A táblázat követelményeihez rendszerint 0,5; 1; illetve 1,5 pontértékeket rendeltünk, amelyek az adott infrastruktúra-jellemző katonai szempontú megfelelőségének mértékét fejezik ki. A magasabb

pontszám a haditechnikai eszközökkel történő közlekedés kedvezőbb feltételeit és a kisebb mértékű korlátozottságot jelzi. Az 1 pont közepes megfelelőséget fejez ki, amelynek során az infrastruktúra-elem alapvetően lehetővé teszi a haditechnikai eszközök közlekedését, ugyanakkor bizonyos korlátozásokkal, előkészítő intézkedésekkel vagy fokozott körültekintéssel kell számolni. A legalacsonyabb, vagyis a 0,5 pont olyan adottságot jelöl, amely jelentős mértékben korlátozza a katonai járművek közlekedését, ezért az adott infrastruktúra-elem csak szűk körben vagy jelentős szervezési, műszaki, illetve forgalomszabályozási intézkedések mellett vehető igénybe.

Az így kialakított háromfokozatú értékelési skála egyszerűen alkalmazható a szemrevételezés során, ugyanakkor megfelelő részletezettséget biztosít az infrastruktúra-elemek közötti különbségek számszerű kifejezésére és összehasonlítására.

A közúti infrastruktúrák logisztikai felderítéséhez használható szempontlista

A cikkben szereplő szempontrendszert egy korábban készített értekezés[3] és egy megjelent publikáció[4] már részletesen elemezte, ezért jelen tanulmányban kizárólag a kialakított követelményekre térünk ki. A kritériumok meghatározásához elsősorban a NATO által kiadott *Criteria and standards for the zones of the reinforcement and sustainment network*[5] című dokumentumot vettük figyelembe, valamint a Bizottságnak (EU) a kettős felhasználású infrastruktúrával kapcsolatos intézkedések egyes kategóriáira alkalmazandó infrastrukturális követelmények meghatározásáról[6] szóló 2021/1328 végrehajtási rendeletét. Az általunk kidolgozott listában 4 fő szemponthoz határoztunk meg követelményeket, amelyek közül a műtárgyakat és az útpálya környezetét elemezzük a következőképpen (1. táblázat).

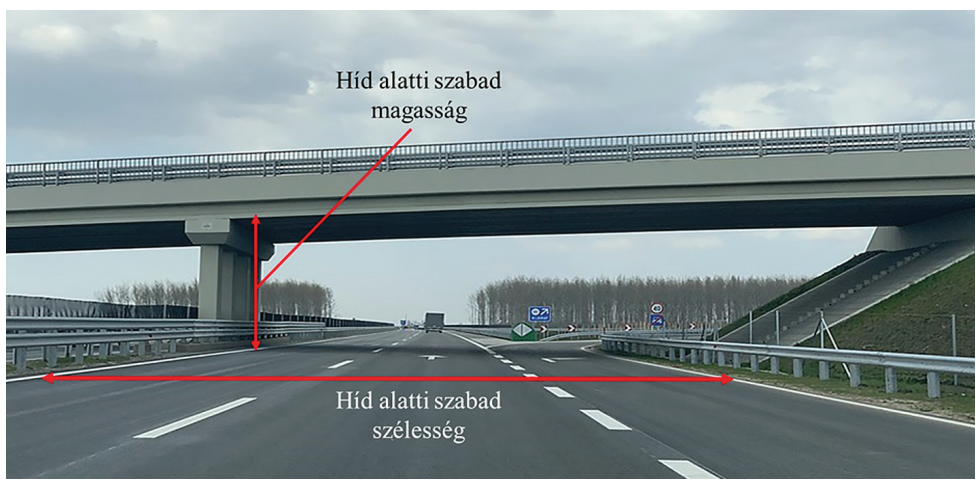
Az 1. pontot figyelembe véve a katonai járművek rendelkezésére álló szabad magasság a műveleti mobilitás és az átcsoportosítási képesség biztosítása szempontjából meghatározó tényező. A katonai szállítójárművek és a speciális eszközszállítók (például a harckocsikat szállító alacsonyágyas félpótkocsik) jellemzően az átlagos közúti járműveknél nagyobb magasságú rakománnyal közlekednek, így a korlátozott szabad magasság nagyfokú akadályt képezhet számukra.[7] Amennyiben a rendelkezésre álló szabad magasság nem éri el a 4,0 métert, az jelentősen befolyásolhatja a harcjárművek, a műszaki eszközök és egyéb katonai felszerelések sikeres mozgatását. A 4,1–4,5 méter közötti tartomány már részben kielégíti a követelményeket, azonban nagyobb méretű eszközök számára még mindig korlátozó tényező lehet. Megfelelőnek a 4,5 métert meghaladó szabad magasság tekinthető, mivel ez biztosítja a legtöbb katonai szállítójármű és rakományának akadálymentes áthaladását.

[3] Szajkó 2025: 71.
[4] Szajkó 2019: 61–77.
[5] ACO Directive 084-004 2024.
[6] A Bizottság (EU) 2021/1328 végrehajtási rendelete.
[7] AASHTO 2018.

1. táblázat: A műtárgyak szempontjai és a hozzájuk rendelt követelmények

Ssz.	Szempontok	Megjegyzés	
Részletezett adatok – műtárgyak			
1.	Járművek rakománnyal rendelkezésre álló szabad magassága súlyozás: 2x	≤4 m	0,5 pont
		4,1–4,5 m	1 pont
		4,5 m<	1,5 pont
2.	Járművek rakománnyal rendelkezésre álló szabad szélessége súlyozás: 2x	3,5–5,5 m	0,5 pont
		5,6–7,2 m	1 pont
		7,2 m≤	1,5 pont
3.	Műtárgy (például híd, áteresz, felüljáró) teherbírása, ha nincs MLC-besorolása súlyozás: 2x	<130 t	1 pont
		=130 t	1,5 pont
4.	A műtárgy MLC-besorolása, ha van súlyozás: 2x	MLC4–MLC40	0,5 pont
		MLC41–MLC99	1 pont
		MLC100≤	1,5 pont
5.	Műtárgy (például hidak, átereszek) szabad szélessége súlyozás: 2x	2,55–5 m	1 pont
		5 m ≤	1,5 pont
6.	A műtárgyak esetleges hibáinak, korlátozásainak hatása a forgalomra súlyozás: 1x	nagy hatás	0,5 pont
		közepes hatás	1 pont
		kis hatás	1,5 pont
7.	A korlátozások várható időtartama súlyozás: 1x	30 nap ≤	0,5 pont
		14–30 nap	1 pont
		≤14 nap	1,5 pont

Forrás: a szerzők szerkesztése Szajkó 2019: 75 alapján



1. ábra: Műtárgy alatti szabad magasság és szélesség
Forrás: a szerzők szerkesztése

Az értékelési pontszámok meghatározása az említett lehetséges korlátozások szempontjaihoz igazodik. Ennek megfelelően a ≤4,0 méteres szabad magasságra adott 0,5 pont azt tükrözi, hogy az útszakasz jelentős korlátozásokkal használható, és csak korlátozott számú, alacsonyabb felépítményű katonai jármű számára biztosít átjárhatóságot. A 4,1–4,5 méter közötti tartományra adott 1 pont közepes megfelelőséget jelez, ahol a legtöbb általános katonai jármű már közlekedhet, de speciális vagy túlméretes eszközök, szállítmányok mozgatásakor még fennállhatnak akadályok. A 4,5 métert meghaladó szabad magasságért járó 1,5 pont a kedvező, közel korlátozásmentes állapotot fejezi ki, amely a katonai szállítások széles spektrumát támogatja.

A szempont kétszeres súlyozása hangsúlyozza a szempont jelentőségét a katonai alkalmazhatóság összesített értékelése során. A műtárgyak alatti megfelelő szabad magasság biztosítása kulcsfontosságú tényező a járművek biztonságos közlekedtetéséhez. A műtárgy alatti szabad magasság és szélesség illusztrációja az 1. ábrán látható.

A rakománnyal együtt figyelembe vett járművek szabad szélessége közvetlen hatással van az oldalirányú mozgástérre, a közlekedés biztonságára és az útvonal átbocsátóképességére.

A 3,5–5,5 méter közötti szabad szélesség azt mutatja, hogy az áthaladás jelentősen korlátozott.[8] Ebben a tartományban a túlméretes eszközök számára a rendelkezésre álló oldaltávolság minimális, ami növeli a tartószerkezeti elemekkel vagy más járművekkel való ütközésveszélyt. A biztonságos haladás érdekében szükségessé válhat a forgalom egyirányúsítása, ideiglenes korlátozása, ezek miatt ehhez a kategóriához 0,5 pontot rendeltünk.

Az 5,6–7,2 méter közötti szabad szélesség már kedvezőbb közlekedési feltételeket biztosít. Az ilyen keresztmetszeti méretekkel rendelkező műtárgyak alatt a technikai eszközök többsége biztonságosan áthaladhat, jellemzően forgalomszervezési beavatkozás nélkül. A megfelelő oldaltávolság csökkenti a baleseti kockázatot, és lehetővé teszi a folyamatos (akár a kétirányú) forgalmat, ezért ezt a tartományt 1 ponttal célszerű értékelni a logisztikai felderítés végrehajtásakor.

A 7,2 métert meghaladó szabad szélesség a legkedvezőbb állapotot jelenti, amely elegendő helyet biztosít akár szélesebb, túlméretes eszközök számára is. A nagyobb szabad tér növeli a biztonságot, valamint – az adott szakaszon – a forgalom rugalmasságát és az út kapacitását, ennek megfelelően a kategóriához 1,5 pontot rendeltünk.

A 2. pont kétszeres súlyozása arra utal, hogy a műtárgy alatti szabad szélesség (ennél a szakasznál) kritikus tényező lehet a katonai szállítások tervezésekor. A nem megfelelő szélességi paraméter szűk keresztmetszetet képezhet, ami akadályozza a túlméretes vagy speciális haditechnikai eszközök mozgását, és közvetlen hatással van az útvonalválasztásra, a szállítási időre, valamint az üzemeltetési biztonságra.

A műtárgyak teherbíró képessége (3. pont) kulcsfontosságú tényező a katonai műveleti mobilitás és a nehéz eszközök átcsoportosításának biztosítása szempontjából. Amennyiben a műtárgyak – különösen a hidak vagy a felüljárók – nem rendelkeznek katonai, azaz *military load classification*[9] (MLC-) besorolással, úgy a teherbírás

[8] A Bizottság (EU) 2021/1328 végrehajtási rendelete.
[9] *Military load classification:* katonai járműteherbírási osztályok.

meghatározását tömeg- (tonna-) alapú megközelítéssel célszerű megvalósítani. A határértékek meghatározásához a Bizottság (EU) 2021/1328 végrehajtási rendeletét vettük alapul, amely szerint a műtárgyak 130 tonnás teherbírása az útfelületek azon képességét jelenti, hogy alkalmi jelleggel ellenálljanak a túlsúlyos katonai eszközök áthaladásából vagy szállításából eredő terheléseknek.[10] Ennek megfelelően a 130 tonna alatti teherbírással rendelkező műtárgyak vonatkozásában az átbocsátóképesség korlátozott a nehéz katonai járművek részére. A modern harckocsik, önjáró tüzérségi eszközök, valamint azok szállítására szolgáló alacsonyágyas szerelvények össztömege gyakran megközelíti vagy meghaladja ezt az értéket. Ennek következtében az ilyen teherbírású műtárgyak kerülőutak kijelölését tehetik szükségessé vagy speciális műszaki biztosítást igényelhetnek. Ezért ezt a kategóriát célszerű 1 ponttal értékelni.

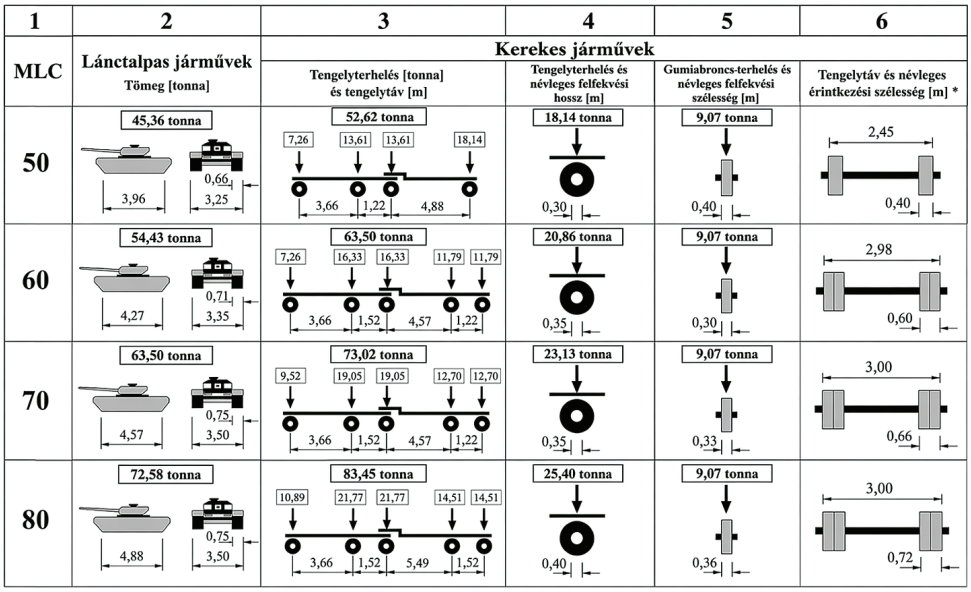
A 130 tonna teherbírású műtárgyak már képesek biztosítani a legtöbb korszerű (túlsúlyos) katonai jármű és szállítóeszköz biztonságos áthaladását. Ennek megfelelően az ilyen műtárgyak alkalmazhatósága szélesebb körű, és jelentősen hozzájárul a műveleti rugalmassághoz, így 1,5 ponttal értékelhetők.

Az 1. táblázat 4. pontjában a kétszeres súlyozás azt tükrözi, hogy a műtárgyak teherbírása komoly hatással van a katonai szállítások tervezésére (például az útvonalak kijelölésekor), ezért is szükséges kiemelt figyelmet fordítani erre a szempontra a szemrevételezések végrehajtásakor és az eredmények kiértékelésekor.

A műtárgyak MLC besorolásával azok értékelése könnyebben elvégezhető a felderítő csoportok számára, mivel ez a rendszer kifejezetten az infrastruktúrák (például a hidak) katonai alkalmazhatóságát fejezi ki.[11] A NATO Stanag 2021 alapján az MLC-érték közelítőleg megfeleltethető a jármű tömegének tonnában *(short ton)* kifejezett értékének, ugyanakkor fontosnak tartjuk kiemelni, hogy ez nem közvetlen tömegazonosság, hanem egy komplex terhelési mutató, amely figyelembe veszi a tengelyelrendezést és a terheléseloszlást is (az MLC50-től MLC80-ig terjedő mutatókra vonatkozó értékeket példaként a 2. ábra szemlélteti).

A kategóriákat figyelembe véve az MLC 4–MLC 40 tartomány megközelítőleg 4–40 tonna közötti teherbírást jelöl, amely elsősorban könnyű és közepes tömegű katonai járművek – könnyű szállítójárművek és egyes páncélozott eszközök (például a teljes harcképes állapotban 16,7 tonna súlyú Gidrán[12]) – áthaladását teszi lehetővé. Az MLC 41–MLC 99 kategória közepes teherbírási szintet képvisel, amely már alkalmas a legtöbb általános katonai szállítójármű, valamint több nehéz harcjármű közlekedésére, ugyanakkor néhány nagy tömegű eszköz – például a harckocsikkal terhelt járműszerelvények – számára még korlátozó tényező lehet. Az MLC 100 vagy annál magasabb besorolású műtárgyak magas teherbírásúnak tekinthetők, amelyek biztosítják a nehéz harcjárművek és teljes terhelésű szállítószerelvények akadálymentes áthaladását.

[10] A Bizottság (EU) 2021/1328 végrehajtási rendelete: 44.
[11] Hajós 2025: 52–55.
[12] Ocskay–Vágner 2021: 47–54.



* A névleges felfekvési hossz a 4. oszlopban van meghatározva.

2. ábra: A műtárgyak MLC szerinti teherbírásának és a járműterhelési jellemzők szemléltetése
Forrás: a szerzők szerkesztése NATO Stanag 2021 alapján

Az értékelési rendszerben alkalmazott pontozás közvetlenül ezen kategóriák katonai megfelelőségét veszi figyelembe. Az MLC 4–MLC 40 tartományra adott 0,5 pont az alacsony teherbírásból adódó jelentős korlátozottságot fejezi ki, mivel ezek a műtárgyak nem teszik lehetővé a nehéz haditechnikai eszközök átcsoportosítását. Az MLC 41–MLC 99 kategóriára adott 1 pont közepes megfelelőséget jelez, amely a katonai forgalom jelentős részét képes kiszolgálni, de nem biztosít teljes körű alkalmazhatóságot. Az MLC 100 vagy annál magasabb értékhez rendelt 1,5 pont a kedvező, közel korlátozásmentes állapotot tükrözi, amely lehetővé teszi a katonai szállítások biztonságos végrehajtását. A szempont kétszeres súlyozása fejezi ki (az előző szemponthoz hasonlóan), hogy a műtárgy teherbírása az infrastruktúra katonai értékelése során kiemelt jelentőségű, és nagyobb súllyal célszerű figyelembe venni, mint egyes más tényezőket, például a műtárgy forgalmi korlátozásait. A teherbírás ugyanis elsődleges, fizikai korlátozó tényezőként jelenik meg, amely közvetlenül meghatározza az adott útszakasz használhatóságát.

Az 5. pontban szereplő műtárgyak szabad szélessége szintén fontos tényező a közúti infrastruktúrák logisztikai felderítésekor, mivel közvetlenül befolyásolja a járművek biztonságos és folyamatos áthaladását. A szabad szélesség meghatározza a járművek „fizikai átférhetőségét", a manőverezési lehetőségeket és a forgalom folyamatosságát is, amely különösen lényeges jellemző akkor, ha a konvojokat a műtárgyakon keresztül kell mozgatni.

A 2,55–5 méter közötti szabad szélesség minimálisan elegendő a járművek részére, ugyanakkor ebben a tartományban a katonai járművek – különösen a szélesebb páncélozott eszközök – áthaladása fokozott figyelmet igényel, és gyakran korlátozott

manőverezési lehetőségekkel jár. Ezért ez a kategória jellemzően egyirányú vagy váltakozó irányú áthaladást tehet szükségessé, amely tovább csökkentheti a katonai mozgások hatékonyságát és növelheti a sérülés vagy baleset kockázatát. Az 5 métert elérő vagy meghaladó szabad szélesség már jobb feltételeket biztosíthat, mivel lehetővé teszi a szélesebb katonai járművek részére a biztonságosabb közlekedést. Ennek megfelelően a 2,55–5 méteres tartományra adott 1 pont közepes megfelelőséget jelez, míg az 5 métert meghaladó szabad szélességért járó 1,5 pont a legkedvezőbb állapotot fejezi ki. A szempont kétszeres súlyozása arra utal, hogy a műtárgyak keresztmetszeti korlátai alapvetően határozzák meg a katonai járművek mozgási lehetőségeit. A nem megfelelő szabad szélesség torlódásokat, forgalomszervezési nehézségeket és fokozott baleseti kockázatot jelenthet, amelyek különösen kritikusak lehetnek a menetek végrehajtásakor.

A műtárgyak esetleges hibáinak és korlátozásainak (6. pont) forgalomra gyakorolt hatását is célszerű megvizsgálni az infrastruktúra-elemek katonai célú értékelése során. Ide tartoznak mindazon állapotromlások, szerkezeti hiányosságok vagy ideiglenes forgalmi korlátozások, amelyek befolyásolják a technikai eszközök biztonságos közlekedését. Ilyen tényezők lehetnek például a sebességkorlátozások, a sávszűkítések vagy az időszakos lezárások.

A forgalomra gyakorolt nagy hatás és a hozzá rendelt 0,5 pont azt szemlélteti, hogy a műtárgy hibái vagy korlátozásai jelentősen akadályozzák a forgalmat, akár kerülőutak igénybevételét is szükségessé tehetik.

A közepes hatásra adott 1 pontnál a forgalom fenntartható, azonban különböző szabályozások (például forgalomirányítás) mellett, amelyek lassítják a mozgást és növelik a szervezési igényt. A kis hatásra meghatározott 1,5 pont azt fejezi ki, hogy a műtárgy állapota és az esetleges korlátozások csak minimális mértékben befolyásolják a forgalmat, így a katonai járművek áthaladása alapvetően zavartalanul biztosítható.

A szempont egyszeres súlyozása arra utal, hogy bár a műtárgyak állapotából adódó korlátozások befolyásolják a közlekedést, ezek hatása általában kisebb jelentőségű, mint a táblázatban korábban említett szempontok.

Az 1. táblázat utolsó pontjánál (7. pont) az ideiglenes vagy tartós forgalmi korlátozások időtartama meghatározhatja, hogy az adott műtárgy milyen mértékben képes biztosítani a folyamatos katonai mozgásokat, valamint szükségessé válik-e alternatív útvonalak kijelölése. A 30 napot meghaladó korlátozások – amelyekhez 0,5 pont tartozik – tartós akadályt jelentenek, és ebből a szempontból jelentős mértékben korlátozzák az útvonal katonai alkalmazhatóságát. Ilyen helyzetben a forgalom átterelése vagy kerülőutak igénybevétele válhat szükségessé, ami növeli a menetidőt és az erők leterheltségét. A 14–30 nap közötti időtartamot (1 pont) közepes hatásúnak tekintjük, mivel ezek a korlátozások ugyan átmenetiek, de még érdemben befolyásolhatják a csapatmozgások szervezését. A 14 napnál rövidebb időtartamú korlátozások (1,5 pont) általában csak kisebb mértékben zavarják a forgalmat, és megfelelő szervezéssel jól kezelhetők.

A szempontrendszer következő és egyben utolsó része az útpálya környezetéhez rendelt jellemzőkkel folytatódik (2. táblázat).

2. táblázat: Az útpálya környezetének szempontjai és a hozzájuk rendelt követelmények

Fsz.	Szempontok	Megjegyzés	
Részletezett adatok – útpálya környezete			
8.	Lehetséges rövid vagy hosszú pihenő helye, mérete súlyozás: 2x	4000–5000 m²	1 pont
		5000 m²≤	1,5 pont
9.	Lehetséges pihenő infrastruktúrája (például vízvételi lehetőség, illemhely) súlyozás: 2x	nincs vagy korlátozott	1 pont
		van megfelelő	1,5 pont
10.	Konvojfordítási lehetőség súlyozás: 1x	nincs lehetőség	1 pont
		van lehetőség	1,5 pont
11.	Konvojfordítási lehetőség forgalmi irányai súlyozás: 1x	egymás utáni Y fordulás	0,5 pont
		egyszerre Y fordulás	1 pont
		egyszerre hurokban fordulás	1,5 pont
12.	Üzemanyag-vételezési pont, parkoló alkalmazhatósága súlyozás: 1x	4000–5000 m² min. 2 töltőpisztoly	1 pont
		5000 m²≤ és több mint 2 töltőpisztoly	1,5 pont
13.	Az út környezetében lévő veszélyes objektum helye, földrajzi koordinátái (például petárdagyár, vízmű), esetleges hatása a forgalomra súlyozás: 1x	nagy hatás	0,5 pont
		közepes hatás	1 pont
		kis hatás	1,5 pont
14.	Az útpálya forgalmát korlátozó növényzet (mérete, jellemzői) hatása a forgalomra súlyozás: 1x	nagy hatás	0,5 pont
		közepes hatás	1 pont
		kis hatás	1,5 pont

Forrás: a szerzők szerkesztése Szajkó *2019: 75 alapján*

A 8. pontot figyelembe véve a pihenőhelyek lehetséges helyének és méretének felderítése, értékelése fontos lehet akkor, ha többórás menetekkel kell számolni az erők átcsoportosításakor. A közúti szállítások végrehajtásakor (a menetoszlopok számára az elkészített menetszámvetések alapján) menetvonalakat jelölnek ki és rendeznek be, amelyekbe rövid és hosszú pihenők is beletartoznak. A konvojmozgások tervezése során a pihenőidők ütemezése jellemzően 3-4 órás menetidőkhöz igazodik, amelyet egy körülbelül 1 órás pihenő követ, míg a napi menet második felében egy hosszabb, megközelítőleg 2 órás pihenési periódust ütemeznek be a parancsnokok.[13] A megfelelő alapterület és infrastruktúra biztosíthatja a menetoszlopok ideiglenes megállását, csoportosítását, így lehetőség adódik a személyi állomány pihentetésére, élelmezési ellátásra, a technikai eszközök szükségszerű karbantartására, ellenőrzésére, valamint üzemanyag kiszolgálására. A 4000–5000 m² közötti terület (az értékelési rendszerben 1 pont) egy 20 járműből álló konvojra vonatkozóan minimálisan megfelelőnek

[13] Ált/54 A Magyar Honvédség szárazföldi haderőnemének harcszabályzata 2014.

tekinthető,[14] mivel biztosítja a járművek rövid idejű megállását, ugyanakkor a manőverezési lehetőségek és a biztonsági távolságok korlátozottak lehetnek.

Az 5000 m²-t meghaladó terület ezzel szemben kedvezőbb feltételeket (1,5 pont) biztosít, lehetővé téve a járművek rendezett elhelyezését, a biztonságos mozgást, a menet közbeni üzemanyag-feltöltést, a műszaki ellenőrzések elvégzését vagy a szükségszerű javítások végrehajtását. A szempont kétszeres súlyozása arra utal, hogy a menetek szervezése során a pihenőhelyek megléte és mérete sokkal jelentősebb, mint a táblázatban szereplő 12-es és 13-as pontok.

A pihenőhelyek infrastruktúrájának kapacitásai (9. pont) szintén fontosak, mivel közvetlenül hatással lehetnek a személyi állomány ellátására vagy a katonai eszközök üzemeltetési feltételeire. Az olyan alapvető létesítmények, mint a vízvételi lehetőség, az illemhelyek vagy egyéb kiszolgáló elemek (például üzemanyagtöltő állomások) hozzájárulnak a pihenőhely jobb használhatóságához. Amennyiben ezek az infrastruktúra-elemek hiányoznak, vagy csak korlátozottan állnak rendelkezésre, az csökkenti a „megálláskor" elvégzendő feladatok hatékonyságát, különösen akkor, ha hosszabb idejű pihenőt tart a menetoszlop parancsnoka. Ennek megfelelően a 9. ponthoz tartozó szempont kritériumát az infrastruktúrák meglétének vagy hiányának figyelembevételével határoztuk meg, ahol az 1 pont a korlátozott, míg az 1,5 pont a megfelelő állapotot jelenti. A kétszeres súlyozás azt fejezi ki, hogy a pihenőhelyek megfelelő infrastruktúrájával, azok igénybevételével lehet biztosítani a „megálláskor" jelentkező feladatok kényelmesebb, hatékonyabb végrehajtását.

A konvojfordítási lehetőségek megléte (10. pont) tovább növelheti az egyes pihenők alkalmazhatóságát, mivel biztosíthatja az irányváltás lehetőségét szükséghelyzetben (például váratlan útlezárás során vagy az utak rombolása, meghibásodása miatt). Amennyiben nem áll rendelkezésre megfelelő fordítási lehetőség, úgy a menetoszlopok jellemzően csak hosszabb kerülőutak igénybevételével vagy bonyolult manőverekkel képesek irányt változtatni. A felderítés során a fordítási lehetőség meglétét 1,5 ponttal, míg a hiányát 1 ponttal célszerű értékelni, amelynek kialakításakor figyelembe vettük azt a szempontot is, hogy egy megálló (az infrastruktúrájával együtt) alkalmas lehet a konvojok pihentetésére még akkor is, ha nincs lehetőség a menetoszlopok visszafordítására. A 2. táblázat 10. pontjának egyszeres súlyozása továbbá azt jelzi, hogy a szempont bár fontos, de nem kritikus tényező.

A konvojfordítási lehetőség forgalmi irányai (amennyiben van) további elemzést igényelnek, mivel ezáltal ki lehet jelölni az irányváltoztatásra leginkább alkalmas pihenőhelyet (11. pont). Az egymás után végrehajtható Y fordulás a legkedvezőtlenebb megoldást jelenti, mivel jelentős időráfordítást kíván, ezért 0,5 ponttal célszerű értékelni. Az egyszerre történő Y fordulás már sokkal hatékonyabb a végrehajtási időt tekintve, azonban továbbra is helyigényes folyamat, amelyet 1 ponttal értékeltünk. A legkedvezőbb megoldást a hurokban végrehajtható fordulás jelenti, hiszen lehetővé teszi a katonai járművek biztonságos és folyamatos mozgását, ezért a szemponthoz 1,5 pontot rendeltünk. Az egyszeres súlyozás – hasonlóan a 10. ponthoz – arra utal,

[14] Tervezési alapadatnak egy 20 db katonai járműből álló konvojt tekintettünk. Egy katonai járműre átlagosan (kb. 8–12 m hosszú és 2,5–3 m széles) kb. 150–250 m² területigénnyel számoltunk, amelynek meghatározásához figyelembe vettük a járművek közötti biztonsági távolságot és a manőverezési sávokat is.

hogy bár a fordulási mód befolyásolja a menetoszlopok visszafordítási lehetőségeit, hatása kisebb, mint például annak, hogy van megfelelő pihenőhely a vizsgált útszakaszon vagy nincs ilyen lehetőség.

Az üzemanyag-vételezési pontok és a hozzájuk kapcsolódó parkolóterületek (12. pont) biztosíthatják a katonai eszközök szükségszerű üzemanyag-feltöltését, valamint az állomány (rövid idejű) pihentetését. A 4000–5000 m² közötti terület, legalább két töltőpisztollyal, minimálisan elegendő egy 20 járműből álló konvoj számára, ugyanakkor nagyobb forgalomnál már torlódásokhoz és a várakozási idő növekedéséhez vezethet. Az 5000 m² feletti terület és a több töltőpisztoly megléte jobb feltételeket tesz lehetővé a menetoszlopok részére, biztosítva több jármű egyidejű kiszolgálását. Az általunk alkalmazott értékelési rendszer ezt a különbséget tükrözi az 1 és 1,5 pontos kategóriákkal.

Az út környezetében található veszélyes objektumok jelenléte és azok forgalomra gyakorolt hatása (13. pont) lényeges biztonsági szempont a katonai útvonalak értékelése során. Ilyen objektumok lehetnek például ipari létesítmények, robbanásveszélyes üzemek vagy kritikus infrastruktúrák, amelyek működésükből adódóan akár forgalmi korlátozások bevezetését is indokolhatják, illetve üzemzavar vagy rendkívüli esemény bekövetkezésekor az adott útszakasz ideiglenes lezárását eredményezhetik. Ennek megfelelően a jelentős hatással bíró objektumokat 0,5 pontra, a közepes kockázatú létesítményeket 1 pontra értékeltük. Az adott útszakasz forgalmára minimális hatást gyakorló objektumokhoz 1,5 pontot rendeltünk. A szempont egyszeres súlyozása arra utal, hogy ezek a tényezők alapvetően kockázati jellegűek, amelyek bekövetkezési valószínűsége általában alacsony és hatásuk eseti jellegű.

Az útpálya környezetében található növényzet (14. pont) szintén befolyásolhatja a közlekedés biztonságát és hatékonyságát. A túlzott vagy nem megfelelően karbantartott növényzet korlátozhatja a látási viszonyokat, csökkentheti az igénybe vehető pálya szélességét, így akadályozhatja a katonai járművek mozgását. A nagymértékű hatást kiváltó tényezőket, amelyek jelentős forgalmi korlátozást okozhatnak, 0,5 ponttal, a közepes hatást (részleges zavarokat) eredményező növényzetet 1 ponttal, míg a kis hatású (minimális befolyással bíró) akadályokat 1,5 ponttal célszerű értékelni a szemrevételezések végrehajtását követően. A növényzet hatása a forgalomra egyszeres súlyozása szintén azt jelzi, hogy bár fontos környezeti tényező, hatása általában kisebb mértékű és jól kezelhető a táblázatban kétszeres súlyozással szereplő szempontokhoz képest.

A szempontlista és a meghatározott követelmények alapján gyűjtött adatok kiértékelése

A szemrevételezési szempontlista követelményeihez – hasonlóan a cikk első részében értékelt tényezőkhöz – előre definiált, diszkrét pontértékeket (0,5; 1 és 1,5 pont) rendeltünk, amelyek az adott jellemző katonai, forgalmi és/vagy geometriai megfelelőségét fejezik ki. A pontértékekhez kapcsolódó súlyozást (1× vagy 2×) úgy alakítottuk ki, hogy a vizsgált szempontok egymáshoz viszonyított jelentőségét tükrözze.

Az értékelés során első lépésként az összpontszámot határoztuk meg, amely az alábbi módon számítható:

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

ahol:

- P = az adott útvonal értékelési pontszáma,
- 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 képlet alkalmazásával a nagyobb jelentőségű paraméterek – például a műtárgyaknál az infrastruktúra-elem MLC-besorolása – nagyobb súllyal jelennek meg az összesített értékelésben. A kapott összpontszámok értelmezése nem abszolút küszöbértékek alapján történik, hanem a teljes mintára jellemző ponteloszlás statisztikai jellemzőinek figyelembevételével.

Ennek érdekében meghatároztuk az összpontszámok átlagát és szórását, amely lehetővé teszi az infrastruktúra-elemek összehasonlítását és besorolását.

A műtárgyak és az útpálya környezetének alkalmassági kategóriáit az átlag és a szórás figyelembevételével jelöltük ki, az alábbi képlet alapján:[15]

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

ahol:

σ = az adott infrastruktúra-elem pontértékeinek szórása,
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 a műtárgyak és az útpálya környezetére vonatkozóan:

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

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

[15] Spiegel–Stephens 2018.

3. táblázat: A műtárgyak és az útpálya környezetének szempontjai és a hozzájuk rendelt követelmények kiértékelése

Ssz.	Infrastruktúra-elem	Súlypont	Osztályozás	Megjegyzés
1.	Műtárgy	18–16	Korlátozás nélkül alkalmas a haditechnikai eszközök számára	A műtárgy még akkor is alkalmas lehet minden eszköz közlekedésére, ha az értékelés során a maximális pontszámhoz képest kisebb eltérés mutatkozik. Ez különösen a műtárgy korlátozásaira és azok időtartamára vonatkozik[16]
		15,5–10,5	Korlátozással alkalmas a haditechnikai eszközök számára	A műtárgy a megadott intervallum alapján csak korlátozással, de a legtöbb haditechnikai eszköz számára alkalmas közlekedtetésre
		10–8	Csak meghatározott eszközök számára vagy egyáltalán nem alkalmas közlekedésre	A túlméretes vagy túlsúlyos eszközök számára vagy rosszabb esetben az összes jármű számára alkalmatlan közlekedésre
2.	Útpálya környezete	13,5–11,5	Korlátozás nélkül használható (például pihentetésre)	Az útpálya környezete akkor is alkalmas lehet a konvojok pihentetésére, ha két ponttal kevesebbre értékeljük a maximális értékhez képest. Ez vonatkozhat az üzemanyag vételezési pontra
		11–7,5	Korlátozással alkalmas	Az útpálya környezete a megadott intervallum alapján csak korlátozással alkalmas például pihentetésre
		7–5,5	Csak meghatározott eszközök számára vagy egyáltalán nem alkalmas használatra	Csak meghatározott összetételű konvojok számára (például amelyeknek összetétele 10 eszköznél kevesebb) vagy egyáltalán nem alkalmas közlekedésre és pihentetésre

Forrás: a szerzők szerkesztése

A műtárgyak vonatkozásában a 16 pont feletti, korlátozás nélkül alkalmas haditechnikai eszközök közlekedtetésére elnevezésű ponttartomány az átlag feletti, illetve az átlag + szórás környezetében elhelyezkedő értékeket foglalja magában. Az ide sorolt műtárgyak teherbírása, geometriai kialakítása lehetővé teszik a haditechnikai eszközök számára a zavartalan áthaladást. Az elemzés során arra a következtetésre jutottunk, hogy ezen kategóriába tartozó műtárgyak akkor is alkalmasak a legtöbb haditechnikai eszköz közlekedtetésére, ha egyes kisebb jelentőségű tényezők – például az ideiglenes korlátozások vagy azok időtartama – miatt mérsékelt pontcsökkenés következik be. Ezt alátámasztja, hogy a műtárgyak katonai megfelelőségét elsősorban

[16] A műtárgy alkalmas lehet minden eszköz közlekedtetésére, amennyiben a korlátozás ideiglenesen (14 és 30 nap közötti intervallumra) vonatkozik, és maximum közepes hatást gyakorol a forgalomra. A közepes hatásnak tekinthető például az ideiglenesen egy forgalmi sávra szűkített közlekedés vagy az ideiglenes méret és súlykorlátozás.

a nagyobb súlyszorzóval rendelkező paraméterek, különösen a teherbírás és a szabad szélesség, valamint magasság határozzák meg.

A 15,5–10,5 közötti ponttartomány a korlátozással alkalmas haditechnikai eszközök közlekedtetésére kategóriát jelöli, amely az átlag környezetében elhelyezkedő értékeket tartalmazza. Az ide tartozó műtárgyak alapvetően biztosítják a katonai járművek áthaladását, azonban egyes jellemzők – például a szabad szélesség vagy a szabad magasság – korlátozó tényezőként jelenhetnek meg. Ilyen jellemzők és adatok mellett a katonai eszközök közlekedése alapvetően szervezési intézkedésekhez kötött, például tengelyterhelés-korlátozás, sebességcsökkentés vagy egyirányú forgalom alkalmazása válhat szükségessé. A legtöbb haditechnikai eszköz közlekedése ugyanakkor megfelelő előkészítés mellett biztosítható.

A 10–8 pont közötti intervallum a csak meghatározott haditechnikai eszközök számára alkalmas közlekedtetésre kategóriát jelenti, amely az átlag alatti, illetve az átlag szórás környezetében elhelyezkedő értékeket fedi le. Az ebbe a kategóriába tartozó műtárgyak jellemzően a teherbírás, a geometriai kialakítás vagy a forgalmi feltételek miatt jelentős mértékben korlátozzák a közlekedést. Ennek megfelelően csak kisebb tömegű, alacsonyabb tengelyterhelésű vagy normál méretű haditechnikai eszközök közlekedtetése lehetséges.

A táblázat következő része az útpálya környezetének pontértékeit tartalmazza. Az osztályozás szerint a 13,5–11,5 pont közötti, korlátozás nélkül alkalmas haditechnikai eszközök közlekedtetésére az átlag feletti, illetve az átlag + szórás környezetében elhelyezkedő értékeket foglalja magában. Az ide sorolt infrastruktúra-elemek feltételei – beleértve a pihenőhelyek méretét és infrastruktúráját, az üzemanyag-vételezési lehetőségeket, valamint a konvojfordítási feltételeket – együttesen biztosítják a menetoszlopok folyamatos és biztonságos mozgatását.

A 11–7,5 pont közötti tartomány a korlátozással alkalmas haditechnikai eszközök közlekedtetésére kategóriát jelöli, amely az átlag környezetében elhelyezkedő értékeket tartalmazza. Az ebbe a kategóriába tartozó infrastruktúrákkal alapvetően lehet támogatni adott útszakaszon a konvojok mozgatását, azonban néhány tényező, például a pihenőhelyek mérete vagy a konvojfordítási lehetőségek korlátozottsága miatt a menetoszlopok vezetése és irányítása fokozott figyelmet igényel.

A 7–5,5 pont közötti intervallum csak meghatározott haditechnikai eszközök számára alkalmas közlekedtetésre kategóriát jelenti, amely az átlag alatti, illetve az átlag szórás környezetében elhelyezkedő értékeket fedi le. Az ide tartozó útpálya-környezeti feltételek csak korlátozott mértékben vagy egyáltalán nem támogatják konvojok mozgatását, pihentetését vagy a visszafordítások kivitelezését. Ezeken a szakaszokon jellemzően csak kisebb összetételű menetoszlopok közlekedtetése biztonságos, fokozott tervezési és végrehajtási feltételek mellett.

Összegzés

A tanulmánysorozat célja olyan szemrevételezési és értékelési módszer kidolgozása volt, amely támogatja a közúti infrastruktúrák katonai szempontú, logisztikai felderítés során történő gyors és egységes vizsgálatát. A közúti alágazat kiemelt szerepet

tölt be az erők mozgatás-szállítási feladatainak végrehajtásában,[17] különösen akkor, amikor a vasúti, légi vagy vízi szállítási kapacitások korlátozottan állnak rendelkezésre, illetve amikor a kirakó pontok és az alkalmazási körletek közötti összeköttetést kell biztosítani.[18] A cikksorozatban négy fő infrastruktúra-elemet – az útpályát, a csomópontot, a műtárgyat és az útpálya környezetét – külön-külön vizsgáltuk, mivel ezek eltérő módon és súllyal befolyásolják a haditechnikai eszközök biztonságos közlekedésének lehetőségét.

A kidolgozott értékelési módszer egyik lényeges eredménye, hogy az egyes infrastruktúra-elemekhez előre meghatározott követelményeket és pontértékeket rendeltünk. A 0,5; 1 és 1,5 pontos értékelési kategóriák, valamint az 1-szeres és 2-szeres súlyszorzók alkalmazása lehetővé teszi, hogy a katonai alkalmazhatóság szempontjából meghatározóbb tényezők – például az útpálya burkolatszélessége, a tengelyterhelése, a műtárgyak MLC-besorolása, teherbírása – nagyobb hatással jelenjenek meg az összesített értékelésben. A módszer előnye, hogy nem csupán leíró jellegű adatgyűjtést tesz lehetővé, hanem számszerűsíthető és összehasonlítható eredményeket biztosít.

A pontozási rendszerhez kapcsolódó statisztikai kiértékelés – az átlag és a szórás figyelembevételével – alkalmas arra, hogy az útpályát, a csomópontokat, a műtárgyakat és az útpálya környezetét alkalmassági kategóriákba sorolja. Ennek alapján elkülöníthetők a korlátozás nélkül alkalmas, a korlátozással alkalmas, valamint a csak meghatározott haditechnikai eszközök számára használható infrastruktúra-elemek. Ez különösen fontos a katonai döntéshozatalban, mert az útvonalak alkalmazhatósága nem kizárólag egyetlen paramétertől függ, hanem több, például geometriai, teherbírási, forgalmi és környezeti tényező együttes értékelésétől.

Kijelenthető, hogy a tanulmányban rögzített követelmények és a hozzájuk rendelt pontértékek lehetővé teszik a felderítő csoportok számára a közúti infrastruktúra-elemek felmérését, értékelését, valamint az elemek egzakt besorolását a megfelelő alkalmassági csoportokba. Ezzel gyorsítható és hatékonyabbá tehető a közutak szemrevételezése és az adatok alapján az elemek kiértékelése.

Összességében megállapítható, hogy a cikksorozatban bemutatott követelményrendszer hozzájárul a logisztikai felderítés egységesítéséhez, a közúti infrastruktúrák gyorsabb kiértékeléséhez, valamint az erők mozgatás-szállítási feladatainak megalapozottabb tervezéséhez. A módszer alkalmazása elősegítheti a katonai szervezetek számára az infrastruktúra-elemek azonosítását, az útvonalak közötti rangsorolást, valamint a szükséges korlátozó vagy kiegészítő intézkedések meghatározását.

Felhasznált irodalom

AASHTO (2018): *A Policy on Geometric Design of Highways and Streets.* Washington D.C.: American Association of State Highway and Transportation Officials. Online: https://store.transportation.org/Item/PublicationDetail?ID=4415

[17] Szászi 2018: 41–136.
[18] Fábos 2018.

ACO Directive 084-004: Criteria and Standards for the Zones of the Reinforcement and Sustainment Network (2024). Mons: Supreme Headquarters Allied Powers Europe.

Ált/54 A Magyar Honvédség szárazföldi haderőnemének harcszabályzata, II. rész, Zászlóalj (2014). Budapest: Magyar Honvédség.

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 infrastrukturális követelmények meghatározásáról. Online: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32021R1328

Fábos Róbert (2018): *A katonai közúti szállítások alapjai.* Budapest: Dialóg Campus. Online: https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/13097/480_Katonai%20kozuti%20szallitasok%20alpjai_e.pdf?sequence=1

Hajós Bence (2025): Közúti híd kísérleti célú próbaterhelése Leopard 2A7HU harckocsival. *Haditechnika,* 59(3), 52–55. Online: https://doi.org/10.23713/HT.59.3.10

Ocskay István – Vágner Szabolcs (2021): Gidrán – egy növelt aknavédelemmel rendelkező harcjármű megjelenése a Magyar Honvédségben: II. rész. *Haditechnika,* 55(4), 47–54. Online: https://doi.org/10.23713/HT.55.4.09

Spiegel, Murray R. – Stephens, Larry J. (2018): *Statistics*. New York: McGraw-Hill Education. Online: https://dl.icdst.org/pdfs/files4/7e065b450295a78731ae9a88b40bb8c7.pdf

STANAG 2021 – Standardization Agreement, Military Load Classification of Bridges, Ferries, Rafts and Vehicles (2024). Edition B, Version 1, 26.11.2024. NSO(NAAG)1402 (2024) MILENG/2021.

Szajkó Gyula (2019): Az út és úthálózatok értékelése a hadszíntéri logisztikai felderítés végrehajtásakor. *Hadmérnök,* 14(4), 61–77. Online: http://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: NKE, Katonai Műszaki Doktori Iskola. Online: https://doi.org/10.17625/NKE.2025.033

Szászi Gábor (2018): A közlekedés ágazatai. In Siposné Kecskeméthy Klára – Szászi Gábor (szerk.): *Közlekedési hálózatok.* Budapest: Ludovika Egyetemi Kiadó, 41–136. Online: https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/13096/Kozlekedesi_halozatok_e.pdf?sequence=1&isAllowed=y1&isAllowed=y

HADMÉRNÖK
KATONAI LOGISZTIKA

21. évfolyam (2026) 3. szám 165–183.
DOI: 10.32567/hm.2026.3.11

Szajkó Gyula,[1] Pap Andrea,[2] Vég Róbert László[3]

A 3D-nyomtatással készült üzemanyag-szaktechnikai eszköz felhasználása a katonai felsőoktatásban

Application of 3D-Printed Specialised Fuel Equipment in Military Higher Education

Absztrakt

A Magyar Honvédség (MH) számára kiemelten fontos, hogy küldetésorientált vezetőket, leendő tiszteket képezzenek a Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar katonai alapképzési szakjain. Ez a követelmény megjelenik a katonai logisztika alapképzési szakon tanulmányokat folytató honvédtisztjelöltekkel szemben is, akiknek nem csupán elméleti ismeretekkel kell rendelkezniük, hanem magas szintű gyakorlati kompetenciákat is el kell sajátítaniuk. A modern hadviselés és a katonai logisztika komplexitása, valamint a technológiai fejlődés gyors üteme új kihívások elé állítja a katonai felsőoktatást, amelynek egyik kulcskérdése az innovatív oktatási módszerek és eszközök integrálása. Ehhez kapcsolódóan a tanulmány középpontjába egy 3D-nyomtatással készített üzemanyag-szaktechnikai eszköz oktatási célú alkalmazásának lehetősége kerül. Az additív gyártástechnológia az elmúlt évtizedben jelentős fejlődésen ment keresztül, és egyre szélesebb körben jelenik meg mind az ipari, mind az oktatási környezetben. A technológia egyik legfontosabb előnye a gyors prototípusgyártás, a költséghatékonyság, valamint az a képesség,

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

[2] Egyetemi docens, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Katonai Logisztikai Intézet Hadtáp, Pénzügyi és Katonai Közlekedési Tanszék, e-mail: pap.andrea@uni-nke.hu

[3] Doktori hallgató, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Hadtáp, Pénzügyi és Katonai Közlekedési Tanszék; tanársegéd, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Hadtudományi Doktori Iskola, e-mail: vegh.robert@uni-nke.hu

hogy komplex geometriai formák is könnyen előállíthatók vele. Ezek a tulajdonságok különösen alkalmassá teszik a 3D-nyomtatást olyan speciális üzemanyag-szaktechnikai eszközök modelljeinek létrehozására, amelyek hagyományos módszerekkel nehezen, drágán vagy egyáltalán nem lennének hozzáférhetők az oktatás számára. A tanulmány ismerteti, hogy miként alkalmazhatók ezek az eszközök demonstrációs és magyarázó segédeszközként az oktatásban.

Kulcsszavak: 3D-nyomtatás, üzemanyag-szaktechnikai eszköz, átfolyásmérő, katonai felsőoktatás, alkalmazhatóság

Abstract

It is of paramount importance for the Hungarian Defence Forces (HDF) to train mission-oriented leaders and future officers across all undergraduate programmes at the Faculty of Military Science and Officer Training of the Ludovika University of Public Service. This requirement also applies to cadets enrolled in the Military Logistics Bachelor's programme, who are expected to acquire not only theoretical knowledge but also a high level of practical competencies. The complexity of modern warfare, the increasing sophistication of military logistics, and the rapid pace of technological development pose new challenges for military higher education. One of the key issues in this context is the integration of innovative teaching methods and tools into the educational process. This study focuses on the potential application of 3D-printed specialised fuel-handling equipment for educational purposes in military higher education. Additive manufacturing technology has undergone significant development in recent decades and is increasingly utilised in both industrial and educational environments. Its main advantages include rapid prototyping, cost-effectiveness, and the ability to produce complex geometrical structures with relative ease. These characteristics make 3D printing particularly suitable for producing models of specialised fuel-handling equipment that would otherwise be difficult, expensive, or impossible to access using traditional methods in an educational context. The study demonstrates how such tools can be effectively used as demonstrative and explanatory teaching aids in military higher education.

Keywords: 3D printing, specialised fuel-handling equipment, fuel flow meter, military higher education, application

Bevezetés

A 21. század biztonságpolitikai és védelmi ipari környezete jelentős változásokon megy keresztül, ami alapvetően új követelményeket támaszt a modern fegyveres erőkkel, valamint a katonai felsőoktatással szemben. A korszerű hadviselés egyik meghatározó jellemzője a technológiai fejlődés felgyorsulása, amely nemcsak a harceljárásokat vagy a műveletek intenzitását, hanem a logisztikai rendszerek működését és fejlesztését is nagymértékben befolyásolja. Ennek következtében a katonai felsőoktatási intézményeknek olyan korszerű oktatási módszereket és innovatív technológiai

megoldásokat kell alkalmazniuk, amelyek elősegítik a hallgatók gyakorlatorientált képzését és a haditechnikai rendszerek mélyebb megértését.

A Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar egyik kiemelt feladata olyan honvédtisztjelöltek képzése, akik képesek megfelelni a Magyar Honvédség előtt álló összetett szakmai és vezetői kihívásoknak. A katonai logisztika alapképzési szak honvédtisztjelöltjei számára különösen fontos a technikai eszközök működésének, alkalmazási lehetőségeinek megismerése és az üzemeltetésükkel kapcsolatos tapasztaltok feldolgozása. Az üzemanyag biztosítása és az ahhoz kapcsolódó szaktechnikai rendszerek a katonai logisztika, azon belül a hadtáptámogatás egyik meghatározó területét képezik, mivel a műveleti képességek fenntartásának alapvető feltétele a megfelelő mennyiségű és minőségű hajtóanyagkészletek biztosítása.[4] A technikai eszközök (például az üzemanyagtöltő gépjárművek, a motoros hajtóanyag-szivattyúk, az átfolyásmérő berendezések) azonban jellemzően olyan méretűek, valamint olyan magas beszerzési és fenntartási költséggel rendelkeznek, hogy csak korlátozottan állnak rendelkezésre az oktatási környezetben. A probléma kezelésének egyik lehetséges megoldását jelentheti az additív gyártástechnológia és azon belül a 3D-nyomtatás, amely az elmúlt években egyre jelentősebb szerepet kapott mind az ipari, mind az oktatási szektorban.[5]

A 3D-nyomtatás gyűjtőfogalma több, egymással párhuzamosan fejlődő additív gyártási eljárást foglal magában, amelyek sajátosságaik révén lehetővé teszik különféle alkatrészek, modellek és prototípusok[6] gyors, pontos és költséghatékony előállítását. Emellett a technológia komplex geometriai formák – például különleges töltetek[7] vagy pilóta nélküli légijárművek alkatrészeinek – gyártására is alkalmas.[8] Rugalmasságából és helyszíni alkalmazhatóságából adódóan a 3D-nyomtatás a műveleti logisztika területén is jelentős lehetőségeket kínál, különösen a gyors alkatrész-utánpótlás és a helyben történő gyártás támogatásában. A 3D-nyomtatási eljárás a munkadarabot nulla helyzetből kiindulva, rétegről rétegre állítja elő, azaz a munkadarab anyagának hozzáadása és a munkadarab kialakítása azonos időben történik. Lehetőséget biztosíthat továbbá az „alkatrész az alkatrészben" konstrukciók kivitelezésére, illetve megfelelő 3D-modellező szoftver alkalmazásával a generatív tervezésre.[9]

Ezzel párhuzamosan az ingyenesen hozzáférhetővé váló ismeretanyagok, a nyílt forráskódú mozgalom, valamint az *open-source* eszközök és az alapanyagok árának csökkenése megteremtette annak a feltételeit, hogy ezek a technológiák integrálódjanak a kreatív, projektközpontú oktatás és a problémaalapú tanulás módszertanába.[10] A 3D-nyomtatás egyik legnagyobb előnye az oktatásban, hogy segítségével olyan szemléltető modellek készíthetők, amelyek támogatják az elméleti ismeretek gyakorlati megértését, valamint lehetőséget teremtenek az interaktív oktatás és a kreatív tanulási módszerek megvalósítására.[11]

[4] Ált/217 Magyar Honvédség Összhaderőnemi Logisztikai Támogatás Doktrína 2015.
[5] Pap–Vég 2025: 59–83.
[6] Ember 2023: 7–9.
[7] Ember 2022: 64–66; Ember–Ádám 2022: 109.
[8] Gál–Németh 2019.
[9] Gávay 2024.
[10] Szabó–Németh 2019; Németh–Szabó 2022.
[11] Végvári 2023.

A katonai tiszképzésben alkalmazott hagyományos demonstrációs eszközök korlátozott funkcionalitással rendelkeznek, valamint nagyobb objektumok, infrastruktúrák alkalmazását, kiépítését teszik szükségessé (például javító műhelyek, üzemanyag-kiszolgáló állomások létesítését). Ezzel szemben a 3D-nyomtatással előállított modellek képesek szemléletesen bemutatni az egyes szaktechnikai eszközök szerkezeti felépítését, működési elvét és kapcsolatrendszerét. Az üzemanyag-szaktechnikai eszközök vonatkozásában ez különösen fontos, mivel a honvédtisztjelöltek számára nehézséget jelent a komplex rendszerek működésének pusztán elméleti alapú értelmezése. Egy oktatási célú modell kialakítása meghibásodott vagy tartalék alkatrészek felhasználásával is lehetséges, ugyanakkor a 20–40 éves eszközök alkatrész-utánpótlása nemzetközi szinten is jelentős logisztikai kihívást jelent.[12] Ennek megfelelően a tanulmány célja annak a vizsgálata, hogy 3D-nyomtatással előállítható-e olyan átfolyásmérő modell, amelyet alkalmazni lehet a katonai felsőoktatásban demonstrációs és oktatást támogató eszközként. A kutatás bemutatja az additív gyártástechnológia oktatási célú alkalmazhatóságát, valamint az átfolyásmérő modell tervezésének és előállításának folyamatát.

Az üzemanyag-kiszolgálás során alkalmazott átfolyásmérők és a PPO-25 típusú mérőberendezés

A haditechnikai eszközök működésének egyik alapvető feltétele az üzemanyagkészletek folyamatos biztosítása. A különböző harc- és gépjárműtechnikai eszközök üzemeltetése jelentős mennyiségű hajtóanyag felhasználását igényli, amelynek tárolása, szállítása és kiadása összetett ellátási feladatot jelent.[13] A hajtóanyag-ellátás során meghatározó jelentőségű a pontos mennyiségmérés, mivel általa lehet nyilvántartani a felhasznált készleteket, valamint ellenőrizni a tartályok közötti üzemanyag-átfejtések volumenét. A pontatlan mérés nemcsak a technikai eszközökbe kiadott mennyiség hibás nyilvántartásához vezethet, hanem a tároló tartályok feltöltésekor vagy lefejtésekor csökkentheti a feladatok végrehajtásának hatékonyságát is (például a tartályok túltöltésén keresztül).

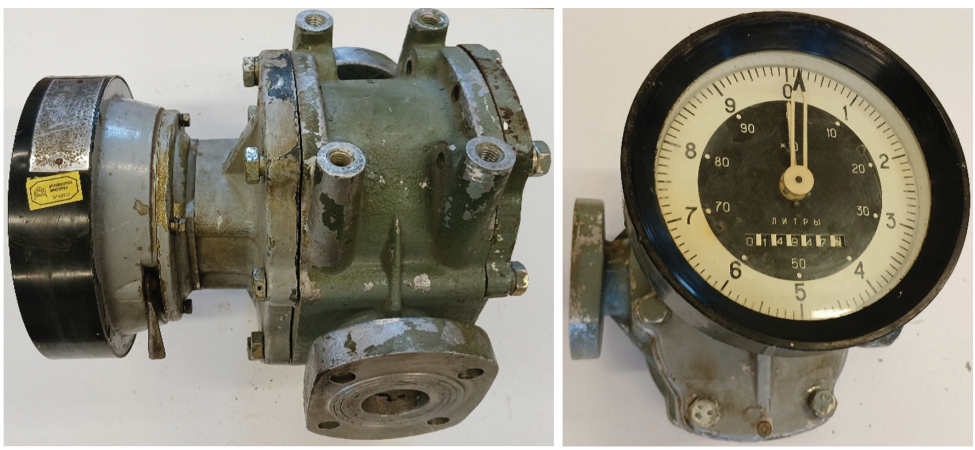
A hajtóanyagok kiadására szolgáló rendszerekben alkalmazott átfolyásmérőknek – az említett probléma elkerülése érdekében – az a legfontosabb feladata, hogy az átáramló folyadék mennyiségét pontosan meghatározza. A mérés történhet térfogat- vagy tömegáram alapján. A katonai üzemanyag-kiszolgáló rendszerekben leggyakrabban térfogatáram-mérőket alkalmaznak. Ennek oka, hogy ezek a rendszerek robusztus kialakításúak, egyszerűbb karbantartást igényelnek, valamint mobil környezetben is megbízhatóan üzemeltethetők. A mérőeszközöknek ugyanakkor meg kell felelniük a fokozott mechanikai és biztonságtechnikai követelményeknek, mivel a folyékony hajtóanyagok tűz- és robbanásveszélyes közeget képeznek.[14]

[12] Gávay 2023.
[13] Szajkó 2024.
[14] Miller 1996.

A hajtóanyagok kiadása során többféle mérési technológiát lehet használni. A legelterjedtebb megoldások közé tartoznak a térfogat-kiszorításos (*positive displacement,* PD), a turbinás, a Coriolis-elven működő, valamint az ultrahangos átfolyásmérők. A különböző technológiák eltérő pontossági, szerkezeti és üzemeltetési tulajdonságokkal rendelkeznek, ezért alkalmazásuk mindig az adott rendszer követelményeitől függ.

A katonai üzemanyag-kiszolgáló rendszerekben jellemzően a térfogat-kiszorításos átfolyásmérőket alkalmazzák. Ezeknek a működése azon alapul, hogy az átáramló folyadék mechanikusan elkülönített mérőkamrákat tölt meg, majd a kamrák ismétlődő térfogatváltozása alapján a rendszer meghatározza az átáramlott folyadék mennyiségét.[15] A technológia előnye, hogy már alacsony átfolyási sebesség mellett is nagy pontosságú, és kevésbé érzékeny a viszkozitás változására.

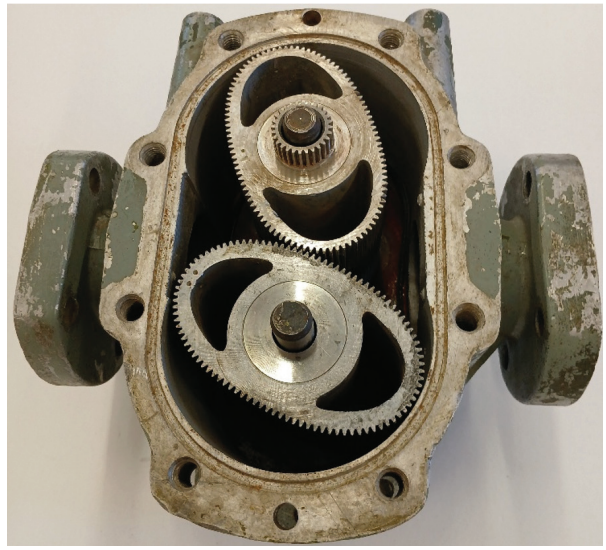
A tanulmányunkban vizsgált mérőberendezés egy PPO-25 típusú ovális fogaskerekes átfolyásmérő, amelyet az URAL–4320 alvázra épített üzemanyag-kiszolgáló rendszerekben is működtetnek (1. ábra).



1. ábra: PPO-25 típusú ovális fogaskerekes átfolyásmérő
Forrás: a szerzők felvétele

Az URAL–4320 katonai tehergépjármű-család a szovjet, majd később az orosz katonai rendszerek egyik meghatározó platformja, amelyet széles körben alkalmaztak üzemanyag-szállító és kiszolgáló járművek alapjaként is.[16] Az ilyen rendszerek feladata a különböző harc- és gépjárművek, valamint a technikai eszközök mobil módon történő hajtóanyag-kiszolgálása, amelynek végrehajtásakor elengedhetetlen a kiadott mennyiség pontos mérése. A PPO-25 típusú mérőberendezés működési elve a térfogat-kiszorításos mérők csoportjába tartozik. A mérő belsejében két egymással kapcsolatban álló ovális keresztmetszetű fogaskerék helyezkedik el (2. ábra).

[15] Overview of Positive Displacement Flow Meters 2023.
[16] Farkas 2026.



2. ábra: PPO-25 típusú ovális fogaskerekes átfolyásmérő ovális keresztmetszetű fogaskerekei a házban
Forrás: a szerzők felvétele

Az átáramló folyadék nyomása forgómozgást hoz létre, amelynek hatására a fogaskerekek és a mérőház közötti kamrák meghatározott térfogatú folyadékrészeket választanak le egymásról. A fogaskerekek minden teljes fordulata ismert mennyiségű folyadék továbbítását jelenti, így a forgási ciklusok száma alapján meghatározható az átáramlott teljes térfogat.

A térfogatáram az alábbi képlettel fejezhető ki:[17]

$$Q = n \cdot Vc$$

ahol:
Q – térfogatáram,
n – a mérőkamrák ciklusszáma időegység alatt,
Vc – az egy ciklus során továbbított térfogat.

Az ovális fogaskerekes kialakítás egyik legfontosabb előnye a magas mérési pontosság és ismételhetőség. A PPO-25 típusú mérők jellemző pontossága 0,25–0,5% közötti, amely megfelel az üzemanyag-kiszolgáló rendszerekkel szemben támasztott követelményeknek.[18] A rendszer további előnye, hogy mechanikus kijelzővel is üzemeltethető, így működése nem minden esetben igényel külső elektromosenergia-ellátást. Ez különösen lényeges szempont a katonai alkalmazási környezetben, ahol a villamosenergia-szolgáltatás korlátozott vagy egyáltalán nem biztosított.

[17] Daku–Vad 2024.
[18] Titan Enterprises Ltd. [é. n.].

A mérőberendezés robusztus szerkezeti kialakítása lehetővé teszi a hosszú távú üzemeltetést. A mérőház jellemzően öntött alumínium- vagy acélszerkezetből készül, amely ellenáll a mechanikai igénybevételeknek és az üzemanyagok kémiai hatásainak. A belső mozgó alkatrészek nagy pontosságú megmunkálása alapvető feltétele a megfelelő mérési pontosság fenntartásának. A fogaskerekek és a ház közötti minimális illesztési hézag biztosítja, hogy a szivárgási veszteség minimális maradjon, ezáltal javítva a mérési precizitást (3. ábra).[19]



3. ábra: A fogaskerék és a ház közötti minimális illesztési hézag
Forrás: a szerzők felvétele

A katonai felsőoktatásban ugyanakkor az ilyen eszközök működésének szemléltetése jelentős nehézségekbe ütközik. Az eredeti berendezések mérete, tömege és működtetési követelményei miatt azok oktatási célú alkalmazása viszonylag korlátozott. A valós hajtóanyag-kiszolgálás fokozott biztonságtechnikai előírásokat tesz szükségessé, amelyek hagyományos tantermi környezetben szintén nehezen biztosíthatók. E problémák kezelésére kínál korszerű megoldást a 3D-nyomtatási technológia.

A PPO-25 típusú mérőberendezés 3D-modellje

Az additív gyártástechnológia lehetőséget biztosít a PPO-25 típusú átfolyásmérő méretarányos vagy metszeti modelljének elkészítésére. A 3D-modell segítségével a honvédtisztjelöltek közvetlenül tanulmányozhatják a mérő belső szerkezeti felépítését, az ovális fogaskerekek kapcsolódását, valamint a térfogat-kiszorításos működési elvet. A szemléltető modell különösen előnyös lehet a katonai logisztikai képzés során, mivel lehetővé teszi az elméleti ismeretek és a gyakorlati bemutató összekapcsolását, és alkalmazásával a hallgatók könnyebben megérthetik az üzemanyag-kiadó rendszerek működését, miközben a demonstráció biztonságosan, valós hajtóanyag alkalmazása nélkül végezhető el.

A 3D-nyomtatott modell további előnye, hogy lehetőséget biztosít a szerkezeti elemek részleges átláthatóságára vagy metszeti kialakítására, amely hagyományos oktatási eszközökkel nehezen valósítható meg. Ez különösen fontos a belső mechanikai

[19] Magyar Honvédség 1985.

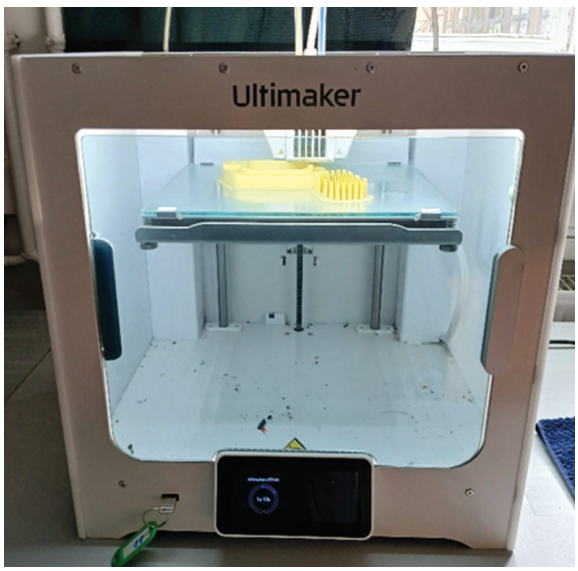
folyamatok szemléltetése során, hiszen az eredeti mérőberendezés működése zárt házban történik, így annak belső mozgásai normál üzemi körülmények között nem figyelhetők meg.

A 3D-nyomtatási technológia alkalmazása nemcsak az oktatási szemléltetés hatékonyságát növeli, hanem lehetőséget biztosít a komplex műszaki rendszerek költséghatékony reprodukálására is. A PPO-25 típusú átfolyásmérő modelljének gyártása során különösen fontos szempont volt, hogy az megőrizze az eredeti szerkezeti kialakítás főbb geometriai jellemzőit, miközben alkalmas legyen az oktatási célú demonstrációra. A tervezés során figyelembe kellett venni a 3D-nyomtatási technológia sajátosságait, valamint azokat a szerkezeti módosításokat, amelyek lehetővé tették a belső mechanikai elemek láthatóvá tételét. Az oktatási célú modell kialakításának egyik legfontosabb követelménye az volt, hogy a honvédtisztjelöltek számára szemléletes módon mutassa be az ovális fogaskerekek mozgását és a térfogat-kiszorításos mérési elv működését. Emellett lényeges szempontként jelentkezett a megfelelő mechanikai stabilitás és a nyomtatási idő optimalizálása is, mivel ezek jelentősen befolyásolják az additív gyártási folyamat gazdaságosságát. A tervezési folyamat során ezért szükségessé vált az eredeti mérőberendezés szerkezeti elemzése, a méretarány meghatározása, valamint a nyomtatható alkatrészekre történő bontás. A digitális modell elkészítését követően megkezdődhetett a megfelelő nyomtatási paraméterek kiválasztása és a prototípus gyártása. Mivel az NKE HHK Katonai Logisztikai Intézetének Haditechnikai Tanszéke rendelkezik olyan 3D-nyomtatókkal, amelyekkel műanyag, szálerősítéses műanyag és fém alkatrészek nyomtatását is el lehet végezni, adódott a lehetőség, hogy ezen technológiákat felhasználjuk az oktatást segítő makett előállítására.[20] A kivitelezésre elegendőnek találtuk a műanyagnyomtató alkalmazását, mert a cél az volt, hogy az eredetivel megegyező, de attól méretben kisebb és lényegesen könnyebb oktatási segédeszköz készüljön el. A fémnyomtatás jelentős idő- és költségráfordítással jár, valamint az elkészült végtermék tömege lényegében megegyezik az eredeti munkadarabbal, így annak a használatát kizártuk. A Markforged kompozitnyomtatót az Onyx nyomtatószállal, amelyhez még folyamatos húzású üvegszál-erősítést is lehet alkalmazni, oktatási makett előállítására nem célszerű felhasználni – bár az ebből készült tárgyak felülete különösen sima és egyenletes, és a hőállóságuk is kiemelkedő –, mert a nyomtatószál jelentős költséggel jár (110 414 Ft / tekercs, ami 800 cm^3).[21] A tanszéken meglévő Ultimaker S3 nyomtató (4. ábra) is alkalmas arra, hogy különféle olcsóbb műanyagokból előállíthassuk a makettet.

Természetesen a nyomtató tálcájának mérete nem teszi lehetővé a pontos méretarányos alkatrész kinyomtatását, de nem is ez volt cél, ezért megfelelőnek bizonyult a 60%-os méretben történő nyomtatás. Ebben a nagyságban még kellően pontos és részletgazdag a végtermék, ugyanakkor a mérete még nem túlságosan nagy, így az oktató könnyen el tudja vinni magával a megfelelő tanórára. A produktum felhasználási célja egyértelműen meghatározta az alkalmazandó alapanyagot is. Mivel az eszköz oktatási célra készült, aminek nincs semmilyen speciális szilárdsági

[20] Gyarmati et al. 2026.
[21] Admasys.

követelménye, így elegendő olyan mértékű erősséget biztosítani, hogy az emberi kézben – miközben a hallgatók forgatják, adogatják egymásnak – ne roppanjon össze, vagy ne törjön el.

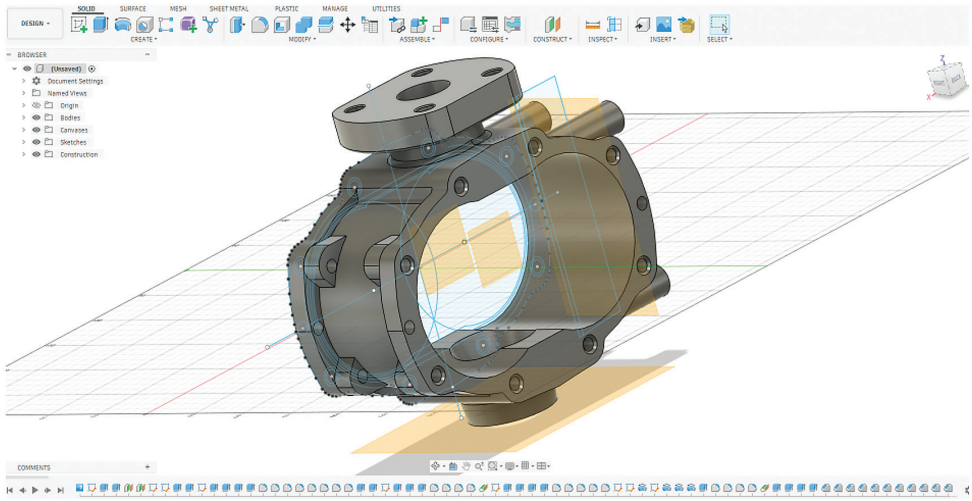


4. ábra: Ultimaker S3 nyomtató nyomtatás közben
Forrás: a szerzők felvétele

Az anyagnak nem kell hő- vagy időjárásállónak lennie, így elsőbbséget élveztek azok a filamentek, amelyek könnyen kezelhetők, viszonylag alacsony olvadási hőmérséklettel rendelkeznek, és nem utolsósorban csekély költségvonzattal bírnak. Az oktatási makett előállításához megfelelőnek találtuk a PLA-t (*polylactic acid* – politejsav), mert ez alacsonyabb hőmérsékleten is feldolgozható és a többi műanyaghoz képest kevésbé hajlamos a vetemedésre. Hátránya, hogy a levegőből való párafelvétele magas, ami a nyomtatásnál hibát okozhat, ez főként akkor fordul elő, ha már régebben felbontottuk a filamenttekercset. A PLA jó UV-állósággal és rétegtapadással rendelkező, merev és erős műanyag, amit magas keményítőtartalmú gabonafélékből állítanak elő. Biológiailag lebomló polimer, vagyis kijelenthetjük, hogy a többi műanyaghoz képest a környezetet kevésbé károsítjuk vele.[22] A színválasztás viszont számos lehetőséget biztosít a jobb megértésre, mivel a különböző részeket más és más színű filamentből lehet előállítani. Azért, hogy az egyes részek jól elkülönüljenek egymástól, a fogaskerekeket sárga, a házat pedig fekete alapanyagból nyomtattuk.

Az oktatási makett megtervezése és a 3D-modell megrajzolása az AutoDesk Fusion 360 szoftver segítségével történt (5. ábra).

[22] Faidallah–Szakál–Oldal 2021; Vég 2024.



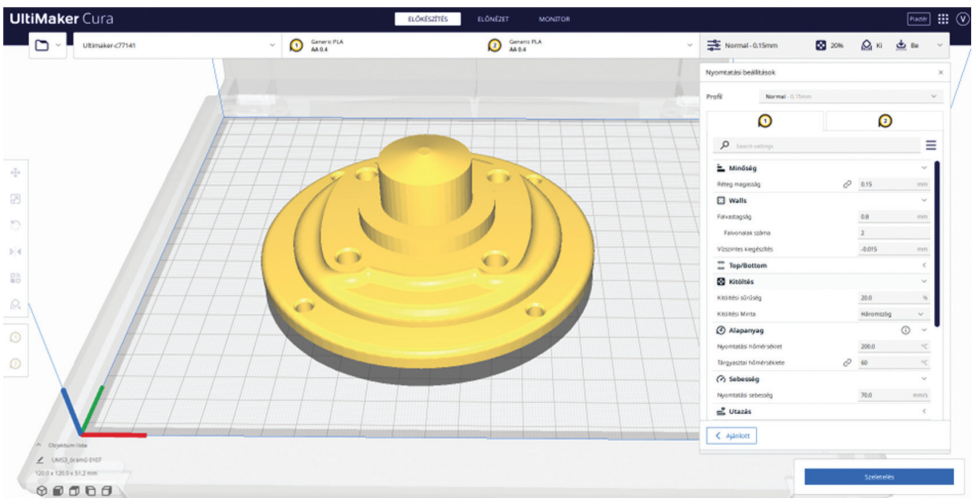
5. ábra: 3D-modell készítése AutoDesk Fusion 360 szoftverben
Forrás: a szerzők felvétele

A program felhasználóbarát felületet és sokoldalú eszközkészletet kínál, támogatja az összetett geometriák és szerkezetek könnyű kialakítását, ami nagyobb precizitást tesz lehetővé. Emellett az integrált szimulációs és elemzési funkciói segítenek a tervek tesztelésében és optimalizálásában, így időt és költséget takarít meg. A Fusion 360 felhőalapú működése megkönnyíti az együttműködést és a fájlok kezelését több felhasználó között. A rendszeres frissítések és a közösségi támogatás révén folyamatosan fejleszthető, és nem utolsósorban a jogtiszta verzió rendelkezésre áll a munkához a Haditechnikai Tanszéken.

A modell létrehozása az eredeti alkatrész geometria-méreteinek a meghatározásával kezdődött. A mérési folyamat során tolómérőt, különböző hosszúságú vonalzókat és szögmérő eszközöket használtunk, amelyekkel meghatározhatók voltak az alkatrész különböző átmérői, hosszméretei, falvastagsága, valamint az egyes szakaszok egymáshoz viszonyított dőlésszögei. A felmérés eredményeként az alkatrész minden lényeges geometriai méretét meghatároztuk. A modellezés célja nem a fizikai alkatrész teljes, mérethű lemásolása volt, hanem annak szerkezeti és funkcionális jellemzőinek megőrzése. Ennek megfelelően a fő méreteket, valamint a furatok elhelyezkedését és méreteit pontosan átvettük, így a modell konstrukciós szempontból pontosan megegyezik az eredeti alkatrésszel. A rajzolás során figyelembe kellett venni a 3D-nyomtatás sajátosságait is, vagyis a könnyebb nyomtathatóság érdekében bizonyos módosításokat, egyszerűsítéseket kellett elvégezni.

A digitális modell kialakítása referenciasíkokra készített vázlatok alapján, fokozatosan valósult meg. A modellezés során többféle módszert alkalmaztunk: egyrészt síkban megrajzolva és ebből elkészítve a térbeli modellt, valamint közvetlenül úgynevezett testprimitívek felhasználásával építettük fel az egyes alkatrészeket. A tervezés alatt figyelembe kellett venni a használt anyag tulajdonságait, a nyomtatási módszert és a késztermék felhasználási célját.

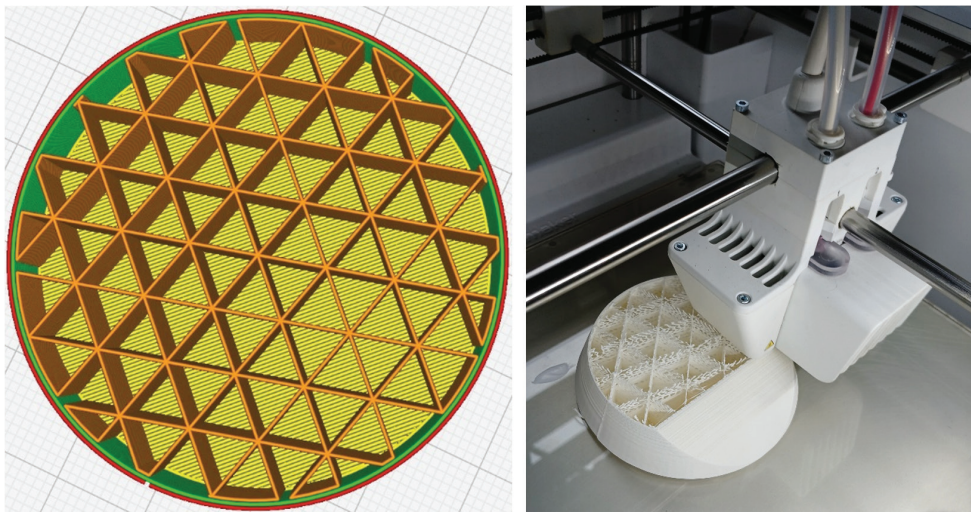
Természetesen a digitális modell (STL, vagyis *standard triangle language* formátum, amely tartalmazza a 3D-nyomtatáshoz szükséges geometriai adatokat) önmagában még nem alkalmas a nyomtatásra, ezért azt előzetesen fel kell dolgozni egy szeletelőprogram segítségével. A szeletelés során a modellt rétegekre bontjuk, vagyis elkészítjük a szerszámpályákat, jelen esetben a nyomtatófej mozgáspályáját. Ehhez több program áll rendelkezésre, általában vannak gyári szeletelőprogramok a különböző 3D-nyomtatókhoz, de használhatók univerzális, ingyenesen elérhető online verziók is, mint például az Ultimaker Cura, amelyet mi is használtunk (6. ábra).



6. ábra: Alkatrész szeletelése Ultimaker Cura programmal
Forrás: a szerzők felvétele

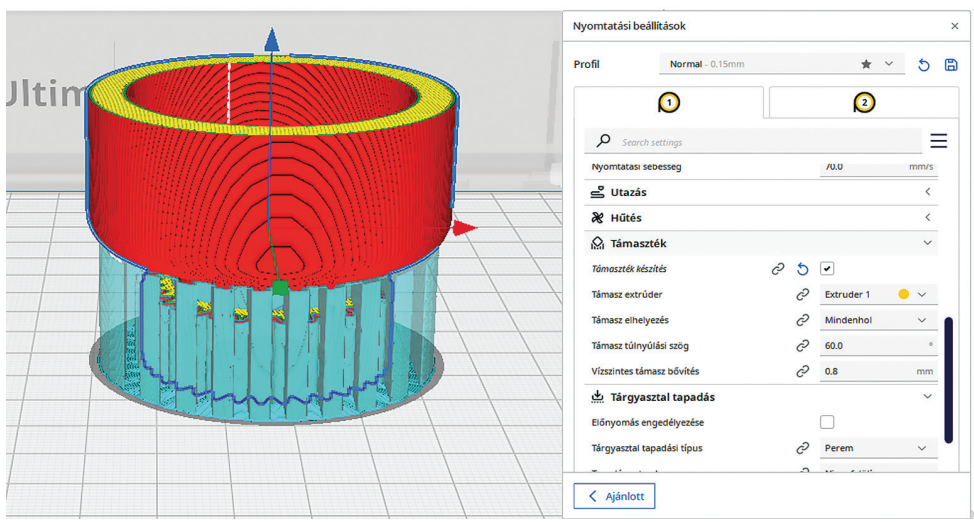
A nyomtatáshoz számos paraméter beállítható, mint például a rétegvastagság, a támasztékok használata, a kitöltési minta és sűrűség, a nyomtatási és tálcahőmérséklet, a nyomtatási sebesség, a tárgyasztal tapadási jellemzői stb. Rétegvastagságként a 0,1 mm-est alkalmaztuk, mivel ez biztosítja a legjobb felbontást az adott nyomtató esetében, és kiváló minőségű sima felületet eredményez. Természetesen a 0,2 mm is megfelelő lenne a gyártási feladatok végrehajtásához és elfogadható minőséget is adna, ugyanakkor most nem volt szempont a rövidebb nyomtatási idő.

A kitöltési minta és a kitöltési sűrűség meghatározó szerepet játszik a nyomtatott modell belső szerkezetének kialakításában, ezáltal jelentősen befolyásolja annak mechanikai szilárdságát, valamint a felhasznált alapanyag mennyiségét. Mivel a készített modell elsődlegesen oktatási és szemléltetési célokat szolgál, nem volt szükség a maximális szilárdság biztosítására. Ennek megfelelően egy egyszerűbb, háromszög alakú kitöltési mintát alkalmaztunk, míg a kitöltési sűrűséget viszonylag alacsony, 40%-os értékre állítottuk. A 7. ábrán a háromszög kitöltési minta képe és a kitöltési sűrűség nagysága látható.



7. ábra: Háromszög kitöltési minta nézete és nyomtatása
Forrás: a szerzők felvétele

Bizonyos esetekben szükséges a nyomtatás során támasztékok alkalmazása. A síkfelületek nyomtatásával általában nincs probléma, és adott meredekségű, általában 45°-os szögeket is problémamentesen fel tud építeni a nyomtató (gyakorlati tapasztalatból adódóan tudjuk, hogy akár 70–80°-os szögeket is be lehet állítani, és úgy is megfelelő lesz a kész darab minősége), ugyanakkor a levegőben nem tud nyomtatni. A kiugró részeket csak úgy képes felépíteni, ha alatta olyan támasztékokat épít be, amelyek a későbbiek során eltávolíthatók (8. ábra).



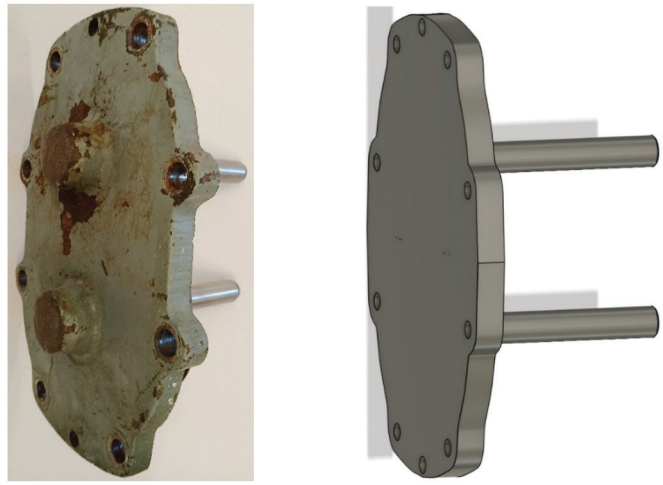
8. ábra: Nyomtatási támaszték nézete és beállítási paraméterei
Forrás: a szerzők felvétele

Az ábrán a Cura program kék színnel jelöli a támasztékot, amelynek paraméterei széles skálában beállíthatók az adott modell és a nyomtatási igények függvényében. A kétfejes nyomtató esetében lehetőség van arra, hogy a támasztékot más alapanyagból vagy színből nyomtassuk ki, így könnyebben megkülönböztethetők, hogy mi az eredeti vagy a támasz, de akár oldható támaszanyagot is lehet (az oktatási makett készítéséhez nem volt szükség rá) alkalmazni. A felhasznált PLA anyagról az utólagos megmunkálás során tökéletesen, kézzel is el lehetett távolítani a támasztékot, ezért ezt a megoldást választottuk.

A nyomtatási hőmérséklet beállítására lehetőség van, de ezt meghatározza az alkalmazott filament anyaga és a gyári ajánlások, amelyek többnyire elfogadhatók. A nyomtatások során előfordul, hogy célszerű változtatni az ajánlásokon a tökéletesebb végeredmény érdekében, de most erre nem volt szükség. A tárgyasztal tapadása viszont mindig problémás egy új anyag alkalmazása esetén, illetve nagymértékben meghatározza, hogy milyen a nyomtatandó tárgy felfekvése. Több sikertelen nyomtatásunk adódott az alkatrészek előállításánál, mire kialakult az a tapasztalat, hogy mekkora legyen a tárgyasztal hőmérséklete, és hogy milyen mértékben alkalmazzunk ragasztást is.

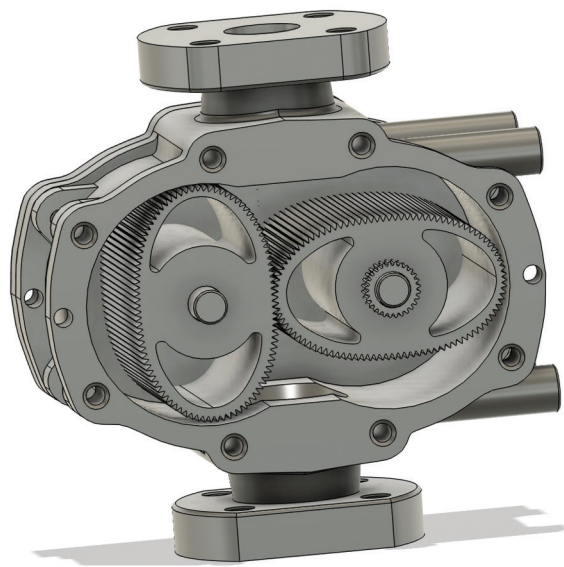
A nyomtatási sebességre nem állandó értéket állítottuk be, hanem azt az egyes alkatrészek tulajdonságaihoz igazítottuk. Az olyan elemek esetében, amelyek precízebb kivitelezést igényeltek – például a kis méretű fogakkal rendelkező fogaskerekeknél –, 50 mm/s nyomtatási sebességet alkalmaztunk. A nagyobb méretű, egyszerűbb geometriájú alkatrészeknél, mint például a ház, 70 mm/s sebességet használtunk. Az egyes darabok nyomtatási ideje igen változó volt, a mérő középrészének nyomtatása közel két napig tartott. A nagyobb nyomtatási sebesség minőségromlással járhat, ezért nem emeltük 70 mm/s fölé, és nem is volt rá szükség, mivel nem volt számunkra fontos tényező az elkészülési idő.

A tervezés során több esetben egyszerűsítésekkel kellett élnünk, amelyek a makett gyakorlati használhatóságát nem érintették, viszont a 3D-nyomtatásnál jelentős előnyöket lehetett elérni vele. Jó példa erre a 9. ábra bal oldalán látható eredeti alkatrész, amelynek fedelén két kiemelkedés figyelhető meg. Az első 3D-modell elkészítésénél ezeket ugyanígy megterveztük, de nyomtatáskor – mivel a síkfelületet kellett bázisnak felhasználni – ez jelentős támaszanyag-felhasználással járt, ugyanakkor a támaszanyag feletti síkfelület minősége erősen megkérdőjelezhető volt. A módosítás utáni (9. ábra jobb képe) változatnál viszont a bázisfelületet teljesen síkra alakítottuk, így nem volt szükség támasztékra, ezáltal csökkent a nyomtatási idő és a felhasznált anyag mennyisége, ugyanakkor a felülete kifogástalan minőségű lett.



9. ábra: Eredeti alkatrész (bal oldali) és az áttervezett (egyszerűsített) modell (jobb oldali)
Forrás: a szerzők felvétele

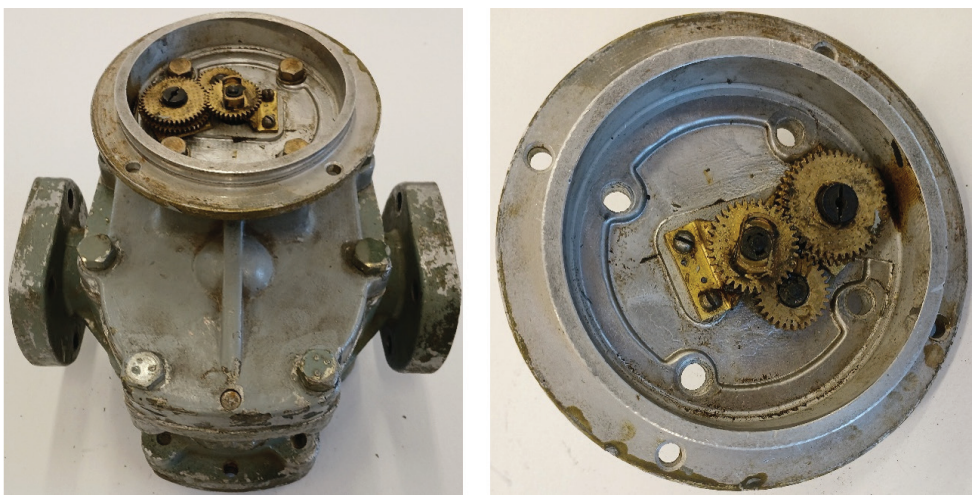
A tervezés és a nyomtatás legproblémásabb része a ház, a fedlap és a fogaskerekek elkészítése (fogaskerekes hajtómű) volt (10. ábra).



10. ábra: Az üzemanyagmérő fogaskerekes hajtóműve
Forrás: a szerzők felvétele

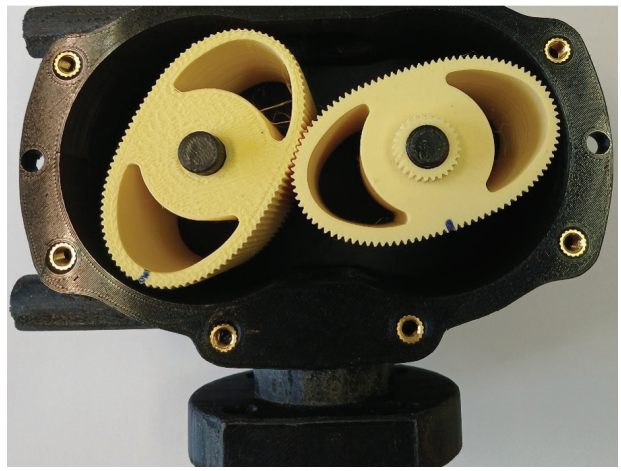
A fogaskerekek kialakítása különösen nagy kihívást jelentett, mivel nagyon kicsi fogakkal rendelkeztek, amit nehéz volt közvetlenül mérni, ezáltal többszöri módosítás (és nyomtatás) vált szükségessé, hogy a végleges méret kialakuljon, valamint a makett működőképes legyen, vagyis a fogaskerekek kis ellenállással kapcsolódjanak egymáshoz és végig legördüljenek egymáson, miközben a fogaskerekek és a ház közötti hézag is minimális maradt.

Az üzemanyagmérő mérőrészének maketten történő kialakítása – a kisméretű fogaskerekek miatt – nem volt megvalósítható. Az alkatrész eredeti méretben elkészítve sem lett volna működőképes, a 60%-os kicsinyítés alkalmazásával pedig a geometriai méretek olyan mértékben csökkentek volna, hogy azok a rendelkezésre álló 3D-nyomtatási technológiával műanyagból már nem voltak legyárthatók (11. ábra). Az óra számlapjánál szintén egyszerűsítést kellett elvégezni, mivel nincs olyan fogaskerekes hajtóműve, ami a mutatót és a számlálót meghajtaná, ezért elegendőnek bizonyult 3D-nyomtatással az óra házának az elkészítése és fénykép alapján a számlap.

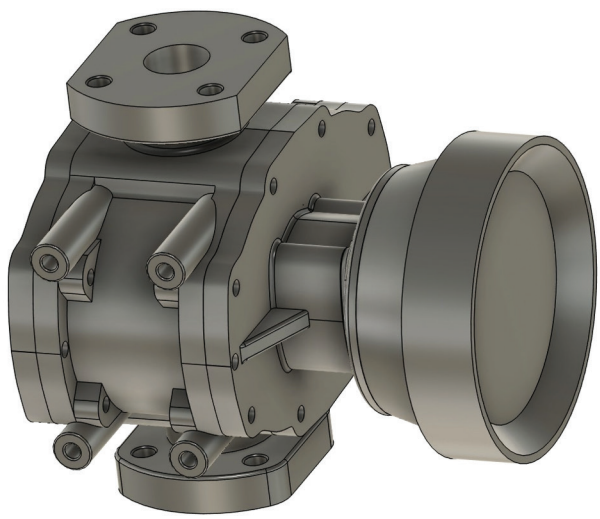


11. ábra: Az üzemanyagmérő óraműrésze
Forrás: a szerzők felvétele

Mivel az üzemanyagmérő több alkatrészből épül fel, ezért fontos volt annak a biztosítása, hogy a teljes makett könnyen szerelhető legyen. Ennek érdekében menetbetéteket építettünk be, amelyek lehetővé tették az alkatrészek csavaros rögzítését. Ez a megoldás nemcsak a szerelési folyamatot teszi megbízhatóvá és többször ismételhetővé, hanem az eredeti berendezés szerkezeti kialakítását is hűen tükrözi. Mindezek mellett a szerelési műveletek tanórán is egyszerűen és gyorsan végrehajthatók, ezáltal segítve a tanagyag könnyebb és pontosabb elsajátítását és az oktatási célok elérését. A 12. ábrán láthatók a házba beültetett menetbetétek, a 13. ábrán pedig az elkészült modell rajza.



12. ábra: Menetbetétek beültetése a maketten
Forrás: a szerzők felvétele



13. ábra: Üzemanyagmérő oktatási makettjének rajza
Forrás: a szerzők felvétele

A PPO-25 típusú átfolyásmérőről készített makett sikeresen alkalmazható volt szemléltető eszközként a Hadtáp szaktechnikai eszközök kurzus oktatása során. A késztermék lehetővé tette, hogy a honvédtisztjelöltek első alkalommal közvetlenül, „testközelből" is megismerhessenek egy olyan üzemanyag-szaktechnikai eszközt, amelynek működését korábban jellemzően csak elméleti formában tanulmányozhatták. Az eszköz különösen hasznosnak bizonyult az átfolyásmérő működési elvének bemutatásában, mivel a belső szerkezeti elemek és azok kapcsolatai jól láthatóvá váltak a hallgatók

számára. Az alkalmazott szemléltető makett jelentősen megkönnyítette az oktató magyarázó tevékenységét, miközben hozzájárult az összetett műszaki folyamatok könnyebb megértéséhez is.

Összegzés

A katonai felsőoktatás egyik fontos feladata, hogy a honvédtisztjelöltek számára az elméleti ismeretek mellett megfelelő gyakorlati tapasztalatokat és szemléltetési lehetőségeket is biztosítson. Az üzemanyag-szaktechnikai eszközök oktatása során ugyanakkor számos nehézség merül fel, mivel az alkalmazott berendezések méretükből, tömegükből, valamint speciális üzemeltetési és biztonságtechnikai követelményeikből adódóan csak korlátozott mértékben vonhatók be a „tantermi" oktatásba. Ezeknek a problémáknak a kezelésére kínál korszerű és költséghatékony megoldást a 3D-nyomtatási technológia.

A tanulmány célja annak vizsgálata volt, hogy a PPO-25 típusú ovális fogaskerekes átfolyásmérő alapján előállítható-e olyan 3D-nyomtatott modell, amely demonstrációs és oktatástámogató eszközként alkalmazható a katonai felsőoktatásban. A cikkben bemutattuk az eredeti berendezés működési elvét, a digitális modell elkészítésének folyamatát, valamint a nyomtatási paraméterek és technológiai megoldások kiválasztásának szempontjait. A modellezés és a gyártás során több esetben egyszerűsítések alkalmazására volt szükség, amelyek nem befolyásolták a működési elv bemutathatóságát, ugyanakkor jelentősen javították a nyomtathatóságot, csökkentették az anyagfelhasználást és a gyártási időt.

A gyakorlati tapasztalatok alapján megállapítható, hogy a rendelkezésre álló FDM-technológiával és PLA alapanyag alkalmazásával olyan oktatási célú makett állítható elő, amely megfelelően szemlélteti az átfolyásmérő szerkezeti felépítését és működési elvét. A modell külön előnye, hogy lehetőséget biztosít a belső szerkezeti elemek és azok kapcsolatainak megfigyelésére, ami az eredeti berendezés esetében a zárt kialakítás miatt nem, vagy csak korlátozottan valósítható meg.

Az eredmények rámutattak arra is, hogy a 3D-nyomtatási technológia alkalmazása nem csupán az oktatási segédeszközök előállításában, hanem a régebbi hadtápszaktechnikai eszközök dokumentálásában és digitális megőrzésében is jelentős lehetőségeket kínál. A digitális modellek létrehozása hozzájárulhat olyan eszközök műszaki adatainak megőrzéséhez, amelyek a jövőben egyre nehezebben lesznek hozzáférhetők. A modellezési folyamat során szerzett tapasztalatok azt mutatták, hogy a hagyományos műszaki ismeretek és a korszerű additív gyártástechnológiák hatékonyan kombinálhatók egymással. A cikkben bemutatott eljárás igazolta, hogy megfelelő tervezési és gyártási paraméterek alkalmazásával a 3D-nyomtatott modellek alkalmasak lehetnek összetett műszaki rendszerek szerkezeti és működési sajátosságainak szemléltetésére. A létrehozott digitális állományok további módosítások és fejlesztések alapjául is szolgálhatnak, így újabb oktatási célú változatok gyorsan és költséghatékonyan készíthetők el. A módszer egyik legnagyobb előnye, hogy az elkészült modellek szükség esetén egyszerűen reprodukálhatók. A cikk eredményei alapján megállapítható, hogy a technológia alkalmazása lehetőséget teremt

a hadtápszaktechnikai eszközök és berendezések oktatási modelljeinek elkészítésére, ezáltal hozzájárulva a gyakorlatorientált tisztképzés fejlesztéséhez és a honvédtisztjelöltek szakmai felkészítésének hatékonyságához. Emellett a 3D-nyomtatás lehetőséget biztosít arra is, hogy a hallgatók már képzésük során megismerkedjenek a modern digitális tervezési és gyártási eljárások alapjaival is.

Felhasznált irodalom

Ált/217 Magyar Honvédség Összhaderőnemi Logisztikai Támogatás Doktrína (2015). Budapest: Magyar Honvédség.

Az Ural-4320 tehergépkocsi és típusváltozatai, anyagismereti és igénybevételi szakutasítás (1985). Szekszárd: Honvédelmi Minisztérium.

Daku Gábor – Vad János (2024): *Áramlástan*. Budapest: Akadémiai Kiadó. Online: https://doi.org/10.1556/9789636640163

Ember István – Ádám Balázs (2022): Béléstestek készítésének technikai lehetőségei alacsony sűrűségű anyagból. *Műszaki Katonai Közlöny,* 32(3), 101–111. Online: https://doi.org/10.32562/mkk.2022.3.6

Ember István (2022): 3D nyomtatott lyukasztó töltetek hatásvizsgálata. *Hadmérnök,* 17(4), 63–73. Online: https://doi.org/10.32567/hm.2022.4.5

Ember István (2023): Additív eljárással készült lineáris vágótöltetek működésének vizsgálata. *Hadmérnök,* 18(3), 5–17. Online: https://doi.org/10.32567/hm.2023.3.1

Faidallah, Rawabe Fatima – Szakál, Zoltán – Oldal, István (2021): Introduction to 3D Printing. Techniques, Materials and Agricultural Applications. *Hungarian Agricultural Engineering,* (40), 47–58. Online: https://doi.org/10.17676/HAE.2021.40.47

Farkas Zoltán (2026): Logisztikai szaktechnikai eszközök egykor és napjainkban V. rész. Üzemanyag-szállító és -töltő gépkocsik. *Haditechnika,* 60(1), 13–20. Online: https://doi.org/10.23713/HT.60.1.02

Gál Bence – Németh András (2019): Additív gyártástechnológiák katonai alkalmazásának vizsgálata, különös tekintettel a katonai elektronika területére. *Hadmérnök,* 14(1), 231–249. Online: https://doi.org/10.32567/hm.2019.1.19

Gávay György Viktor (2023): Logisztikai járművek alkatrészpótlása 3D-nyomtatási technológia alkalmazásával. *Katonai Logisztika,* 31(3–4), 208–232. https://doi.org/10.30583/2023-3-4-208

Gávay György Viktor (2024): Honvédségi járművek kezelőszerveinek pótlása, módosítása 3D-nyomtatási technológia alkalmazásával. *Műszaki Katonai Közlöny,* 34(3), 25–38. Online: https://doi.org/10.32562/mkk.2024.3.3

Gyarmati, József – Gávay, György– Hegedűs, Ernő (2026): Potential Applications of Different 3D Printing Technologies In Military Logistics. In *VojNa 2025. International Scientific Conference on Military Sciences.* Belgrade: Military Academy, University of Defence, 938–946. Online: www.researchgate.net/publication/399444603_Potential_applications_of_different_3D_printing_technologies_in_military_logistics

Miller, Richard W. (1996): *Flow Measurement Engineering Handbook*. New York: McGraw-Hill.

Németh András – Szabó András (2022): Zrínyi-Újvár hadszíntérkutatási eredményeinek hasznosulása a katonai műszaki oktatásban. In Hausner Gábor (szerk.): *Zrínyi Miklós és öröksége*. Budapest: Ludovika Egyetemi Kiadó, 149–178. Online: https://openaccess.ludovika.hu/nke/catalog/view/152/1338/3267

Overview of Positive Displacement Flow Meters (2023). Online: https://instrumentationtools.com/positive-displacement-flowmeters/

Pap Andrea – Vég Róbert László (2025): Térszemlélet fejlesztése a katonai logisztikában 3D-nyomtatás és számítógéppel támogatott műszaki modellezés (CAD) által – 1. rész. *Műszaki Katonai Közlöny,* 35(3–4), 69–83. Online: https://doi.org/10.32562/mkk.2025.3-4.5

Szabó András – Németh András (2019): A katonai műszaki képzés rendszerének kihívásai és lehetséges fejlesztési irányai. *Hadtudományi Szemle,* 12(ksz.), 261–288. Online: https://doi.org/10.32563/hsz.2019.1.ksz.19

Szajkó Gyula (2024): A béketámogató műveletek üzemanyagszükséglet-tervezéséhez használt számvetési módszerek. In Gőcze István – Padányi József (szerk.): *Szemelvények a katonai műszaki tudományok eredményeiből IV.: Hallgatói kötet*. Budapest: Ludovika Egyetemi Kiadó, 183–203. Online: https://doi.org/10.36250/01202_10

Titan Enterprises Ltd. [é. n.]: *Oval Gear Flow Meters Overview – Technical Product Data Sheet*. Online: https://flowmeters.co.uk/wp-content/uploads/pdfs/tech-data/data-sheet-oval-gear-meters-overview-06-25.pdf

Vég Róbert László (2024): Forgó dugattyús befecskendezőszivattyúk a harc- és gépjárműtechnikában 2. Befecskendező szivattyú tehermentesítő szelep oktatási célú modell kialakítása 3D-nyomtatási technológiával. *Műszaki Katonai Közlöny,* 34(ksz.), 115–128. Online: https://doi.org/10.32562/mkk.2024.ksz.10

Végvári Zsolt (2023): A 3D-nyomtatás felhasználási lehetőségei a műveleti logisztikában. *Katonai Logisztika,* 31(1–2), 177–198. Online: https://doi.org/10.30583/2023-1-2-177

Tartalom

VÉDELEMINFORMATIKA

Farkas Athéné: *A mesterséges intelligencia alkalmazási lehetőségei a kiberbiztonsági auditok gyakorlatában* 5

Olga Lavro-Gazdag: *Doxxing as an Information Operation* 21

Ferenc Nyizsnyik: *Crowdsourcing Intelligence* 43

Pozderka Gábor: *Kibertől az MI-ig: A mesterséges intelligencia az új kiber?* 55

KÖRNYEZETBIZTONSÁG

Almási Csaba, Cséplő Zoltán: *A nagy közbiztonsági kockázattal járó veszélyes áruk szállítását érintő szabályozás vizsgálata* 75

Cséplő Zoltán, Kátai-Urbán Maxim, Vass Gyula: *Az iparbiztonsági oktatás és képzés rendszerének vizsgálata* 89

Földes Tibor: *A működésfolytonosság mint stratégiai képesség a kritikus infrastruktúrák védelmében* 105

Takács Dániel, Négyesi Imre: *A nukleáris energia hasznosításának új korszaka* 119

KATONAI LOGISZTIKA

Norbert Daruka, Kálmán Dénes, Zoltán Kovács, Róbert Vég, István Ember: *The Impact of Additive Manufacturing Used in the Russo–Ukrainian Conflict on Decentralised Manufacturing* 137

Szajkó Gyula, Lévai Zsolt: *A közúti infrastruktúrák katonai megfelelőségi vizsgálata a logisztikai felderítés végrehajtásakor, 2. rész* 149

Szajkó Gyula, Pap Andrea, Vég Róbert László: *A 3D-nyomtatással készült üzemanyag-szaktechnikai eszköz felhasználása a katonai felsőoktatásban* 165