HADMÉRNÖK

Kiemelt közlemények

20. évf. (2025)
2. szám

ISSN 1788-1919 (elektronikus)

LUDOVIKA
EGYETEMI KIADÓ

IMPRESSZUM

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

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

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

Tartalom

Fórum

Kiképzés, felkészítés

Környezetbiztonság

HADMÉRNÖK
BIZTONSÁGTECHNIKA

20. évfolyam (2025) 2. szám 5–20.
DOI: 10.32567/hm.2025.2.1

Fráter-Szegedi Judit[1]

Veszélyes anyagokkal foglalkozó üzemek baleset-megelőzési lehetőségei a mesterséges intelligencia segítségével

Accident Prevention Opportunities for Plants Handling Hazardous Materials with the Help of Artificial Intelligence

Absztrakt

A mesterséges intelligencia nem új keletű technológia, széles körű alkalmazhatósága valamennyi gazdasági ágazatban ismertté tette. Az emberi gondolkodás alapján mintázott algoritmusok segítségével folyamatok automatizálhatók, a munkavállalók által nem kedvelt munkafázisok kiválthatók, a tevékenységek megkönnyíthetők. A gépi tanulás folyamatos, fejlődése nagymértékű és gyors. A mesterségesintelligencia-eszközök alkalmazása a megfelelő kereteken belül (etikusság, kellő kritikai szemlélet) hatékonyságnövelő, költséghatékony, és jelentős mértékben csökkentheti az emberi hibából eredő kockázatokat. Ez utóbbi kapcsán van a mesterséges intelligenciának létjogosultsága a munkavédelemben is. Főként azokban az esetekben, amikor egyes események kapcsán az összes lehetséges kimenet felvázolása, az emberi tényezők kiküszöbölése korlátozottan lehetséges. Kiváltképpen akkor, ha nem „hagyományos", hanem veszélyes anyagokkal foglalkozó üzemekről van szó. A mesterségesintelligencia-eszközök tudásának felmérése, a fejlesztési irányok kijelölése szükséges ahhoz, hogy ezekben az esetekben is jól alkalmazhatók legyenek, hatékonyan működjenek. A legfontosabb kérdés a téma kapcsán, hogy az AI-modellek képesek-e feltérképezni az események valamennyi lehetséges kimenetelét, az esetleges kockázatokat

[1] Tűz- és munkavédelmi szaktanácsadó, LEGO Manufacturing Kft.; doktori hallgató, Óbudai Egyetem Biztonságtudományi Doktori Iskola, e-mail: frater.szegedi.judit@uni-obuda.hu

olyan formán, hogy az emberi tényezőt sem hagyják ki, illetve képesek-e megfogalmazni az intézkedéseket az esetleges kockázatok megelőzése, csökkentése érdekében.

Kulcsszavak: mesterséges intelligencia, SEVESO, gépi tanítás, kockázatelemzés, fejlesztés

Abstract

Artificial intelligence is not a new technology, its wide applicability has made it known in all economic sectors. With the help of algorithms modelled on human thinking, processes can be automated, work phases that are not liked by employees can be replaced, and activities can be made easier. Machine learning is continuous, its development is large and rapid. The use of artificial intelligence tools within the appropriate framework (ethics, sufficient critical approach) can increase efficiency, be cost-effective and significantly reduce risks arising from human error. In connection with the latter, artificial intelligence also has a raison d'être in occupational safety. Especially in cases where it is limited to outline all possible outcomes in connection with certain events and eliminate human factors. Especially when it comes to plants that are not "traditional", but deal with hazardous materials. It is necessary to assess the knowledge of artificial intelligence tools and identify development directions so that they can be well applied in these cases and operate effectively. The most important question in this regard is whether AI models are able to map all possible outcomes of events, potential risks in a way that does not leave out the human factor, and whether they are able to formulate measures to prevent and reduce potential risks.

Keywords: artificial intelligence, SEVESO, machine learning, risk analysis, development

Bevezetés

Napjaink egyik leggyorsabban, legnagyobb mértékben fejlődő területe a mesterséges intelligencia (AI, MI). Valamennyi gazdasági ágazatban a működés szerves részét képezi az AI-technológia, amely a folyamatos tanításnak köszönhetően egyre több esetben, egyre mélyebben képes adott témakörökben adekvát választ adni a kérdésekre. Van azonban a tanulásnak egy jól meghatározott kerete, amelyen túl az AI sem rendelkezik, nem is rendelkezhet megfelelő szintű tudással tapasztalatok és egyéb információ híján, vagy mert bizonyos tényezők meghatározhatatlan együtthatását egyik algoritmussal sem lehet pontosan leírni, vagyis nem lehet az AI-t megtanítani rá. A munkabiztonság az egyik olyan terület, ahol az algoritmusokkal csupán keretet lehet adni a mesterséges intelligencia működésének. A köznyelvben véletlenek szerencsétlen sorozataként aposztrofált esetekben a mesterséges intelligencia sem feltétlenül képes az összes lehetséges kimenetelt, felmerülő kockázatot megfelelően prognosztizálni, vagy pedig megelőzni az esetlegesen bekövetkező eseményt. A veszélyes anyagokkal foglalkozó üzemek nem üzemszerű iparbiztonsághoz tartozó események, súlyos vagy katasztrofális kimenetelű balesetek a történések olyan láncolatát vázolhatják fel, amelyeket szinte lehetetlen megjósolni, a lehetséges kimeneteleket a teljesség igényével

rendszerbe dolgozni, a szükséges megelőző intézkedéseket egyfajta metódus alapján megadni. A beavatkozást végzők számára különösen fontos az, hogy minden eshetőséggel számolva rendelkezzenek megfelelő eszközökkel, egyéni védőeszközökkel. Az AI használata a munkavédelemben a jövő alternatívája lehet, felmerül azonban a kérdés, hogy mely program milyen algoritmus mentén tanítható, mi az az alap információkészlet, amelyre építkezhet.

Mesterséges intelligencia a munkavédelemben

A mesterséges intelligencia megjelenése a munkavédelemben determinált. A digitalizáció térnyerésével egyre több helyen jelennek meg AI-alkalmazások a munkavállalók tevékenységének megkönnyítése érdekében. Egyre több AI-megoldással lehet találkozni. Öngerjesztő a folyamat, hiszen tanul, reagál a környezet és a felhasználók visszajelzéseire, akik az újabb kérdésekkel tovább „ösztönzik" a tanulásra. A munkavédelemben az AI segítségével futtathatók különböző szimulációk, felgyorsítható a kockázatértékelés folyamata, az egyre növekvő adatbázisból részletesebben és mélyrehatóbban lehet az egyes kockázatokat elemezni, az adatokat gyorsabban vizsgálni. A valós idejű megfigyelésekhez ruhába, védőeszközbe, testbe ültetett digitális nyomon követő technológiák segítségével gyűjtött adatokat használhatnak, az adathalmazokból írt algoritmusokkal megfigyelhetik, felügyelhetik a munkavállalók életjeleit, stresszmutatóit. Ennek óriási szerepe van a katasztrófavédelem beavatkozást végző munkavállalóinak életvédelmében. Az egyéni védőeszközökbe ültetett érzékelők lehetővé teszik a vészhelyzetek valós idejű felismerését, figyelmeztetnek a kitettség káros szintjének elérésekor, a stressz-szint megnövekedésekor, egészségi problémák megjelenésekor, a fáradtság vagy egyéb, munkabiztonsági szempontból jelentős tényező fennállásakor. A munkavállaló biztonsága érdekében az eszköz valós időben befolyásolhatja a munkavállaló magatartását.[2] Új technológia, sok esetben megosztó az alkalmazása a jól szabályozható működés ellenére (a jogszabályi környezet nem teljes), hiszen adatokkal, adatokból dolgozik, a munkavédelem tekintetében mégsem az adatvédelem a legfontosabb kérdés. Sokkal inkább az, hogy olyan esetekben, amelyekben titkosították az adatokat, egyéb információ nem áll rendelkezésre, vagy tapasztalat útján nem szerezhetett tudást, hogyan határozható meg az adatbázisa, mi alapján lehet megtanítani a kockázatok felmérésére. Zákányi és munkatársai 127 fő bevonásával 16 kérdésből álló kérdőív segítségével vizsgálták a mesterséges intelligenciával kapcsolatos megítélést, valamint azt, hogy az AI-eszközök megfelelő jogi szabályozás mellett milyen szerepet tölthetnek be a vállalat életében a válaszadók szerint. Az eredményeik alapján az látszik, hogy a munkavédelemben is számos előnnyel járhat a mesterséges intelligencia alkalmazása:

- bármikor elérhető, mindenre kiterjedő oktatások;
- hatékonyabb kockázatvizsgálat;
- hatékonyabb baleset-megelőző programok;
- munkahelyi balesetek csökkenő száma.[3]

[2] Európai Munkahelyi Biztonsági és Egészségvédelmi Ügynökség 2020.
[3] Zákányi et al. 2024.

Az adatbányászat elterjedésével, a statisztikai feladatok és problémák mesterséges intelligencia segítségével történő megoldásának igényével jött a fellendülés. A munkavédelem területén két szakaszban fejlődött az MI alkalmazása. Az első szakaszban, az 1960-as években megjelent az MI a robotikában, létrehozták az első ***machine learning*** robotokat: SRI-t és Shakey-t.[4] Az automatizálás legfontosabb munkavédelmi hozadéka az volt, hogy a gép által elvégzett feladatokban nem volt emberi faktor, hiányzott a hibázás lehetősége, ezért jelentős mértékben lecsökkent a balesetek és sérülések esélye, vagyis a kockázatok száma és súlyosságának mértéke. 2015-ben a gépi tanulás és a *big data* kombinációjából létrejött ***deep learning*** fokozott térnyerése volt kiemelkedő jelentőségű a munkavédelem számára is. Megjelenhettek a mesterségesintelligencia-alapú munkavédelmi rendszerek. Funkcionalitásukat tekintve ezek a rendszerek az ergonómia területére koncentráltak. Az eszközökbe épített szenzorok segítségével nyertek adatokat a munkavállalók által végzett tevékenységekről. A későbbiekben már arra is lehetőséget adott, hogy az egyéni védőeszközök használatát megfigyeljék. A fejlődés folyamatos, de a mesterséges intelligencia kockázatértékelésben, baleset-megelőzésben még nem hódított teret magának. Jól funkcionálnak a MI-eszközök a termelékenység skálázásában, nagy adathalmazok anomáliáinak észlelésében, folyamatok automatizálásában, de az egészség- és biztonságvédelmi szektorban a dinamikus környezetben nehezebb a pozitív hatásokat detektálni egy-egy jó gyakorlat kapcsán. Jelenleg a gyártás, az építőipar, az ipar és a logisztika területén dolgozó munkavállalókat érintő legnagyobb veszélyek kapcsán mutatkozik előrelépés, a veszélyes üzemekkel kapcsolatosan nem.

A vizsgálat módszertana

A vizsgálat első része a fogalmi keretek meghatározása. A veszélyes anyagok gyártásához, felhasználásához, tárolásához, kezeléséhez kapcsolódó üzemek definiálása szerteágazó problémakört határoz meg. A katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény 3. §-a tartalmazza az értelmező rendelkezéseket a téma vonatkozásában. Ennek értelmében

„27. Veszélyes anyagokkal foglalkozó létesítmény: olyan, a veszélyes anyagokkal foglalkozó üzem területén lévő – föld alatti vagy föld feletti – technológiai vagy termelésszervezési okokból elkülönülő műszaki egység, ahol egy vagy több berendezésben (technológiai rendszerben) veszélyes anyagok előállítása, felhasználása, szállítása vagy tárolása történik, magában foglal minden olyan felszerelést, szerkezetet, csővezetéket, gépi berendezést, eszközt, iparvágányt, kikötőt, a létesítményt szolgáló rakpartot, kikötőgátat, raktárt vagy hasonló – úszó vagy egyéb – felépítményt, amely a létesítmény működéséhez szükséges.
28. Veszélyes anyagokkal foglalkozó üzem: egy adott üzemeltető irányítása alatt álló azon terület egésze, ahol egy vagy több veszélyes anyagokkal foglalkozó létesítményben – ideértve a közös vagy kapcsolódó infrastruktúrát is – veszélyes anyagok vannak jelen a törvény

[4] Bekey 2005.

végrehajtására kiadott jogszabályban meghatározott küszöbértéket elérő mennyiségben, és ennek alapján alsó vagy felső küszöbértékűnek minősül."[5]

A 28. pontban megadott alsó és felső küszöbérték fogalmát a 219/2011. (X. 20.) Korm. rendelet 1. §-a határozza meg az alábbiak szerint:

„1. Alsó küszöbértékű veszélyes anyagokkal foglalkozó üzem: ahol az 1. melléklet alapján meghatározható alsó küszöbértéket elérő vagy meghaladó, de a felső küszöbértéket el nem érő mennyiségben veszélyes anyagok vannak jelen. […]
2. Felső küszöbértékű veszélyes anyagokkal foglalkozó üzem: ahol a jelen lévő veszélyes anyagok mennyisége az 1. melléklet alapján meghatározható felső küszöbértéket eléri vagy meghaladja."[6]

Az atomerőművek a kormányrendelet értelmezésében nem minősülnek alsó vagy felső küszöbértékű üzemnek, a felhasznált hidrazin-hidrát miatt azonban felső küszöbérték feletti veszélyes üzemnek igen (az atomerőmű blokkjainak primer és szekunder köreiben felhasznált hidrazin a jogszabályváltozás miatt sorolandó a felső küszöbérték feletti üzemek közé). A vizsgálat azonban ebben az értelmezésben nem tesz különbséget az alsó és felső küszöbértékű, illetve különösen veszélyes üzemek között, hiszen az elsődleges cél a nem üzemszerű iparbiztonsági események elemzése (például nukleáris létesítményekben vagy a sugárzó anyag jelenlétében bekövetkező káresemény). Az alapvetés az, hogy a környezetre és/vagy az emberre kiemelt veszélyt jelentő üzemek kerülnek be a vizsgálatba. A bekövetkező események súlyossága és bekövetkezési valószínűsége tekintetében ugyanis nincs jelentősége a küszöbértékeknek. A szerző veszélyes üzemként kezel minden fokozott veszéllyel járó tevékenységet folytató, csekély mértékű rendellenesség bekövetkezésével is súlyos kárt okozó, fenyegető veszélyhelyzetet kialakító üzemet.

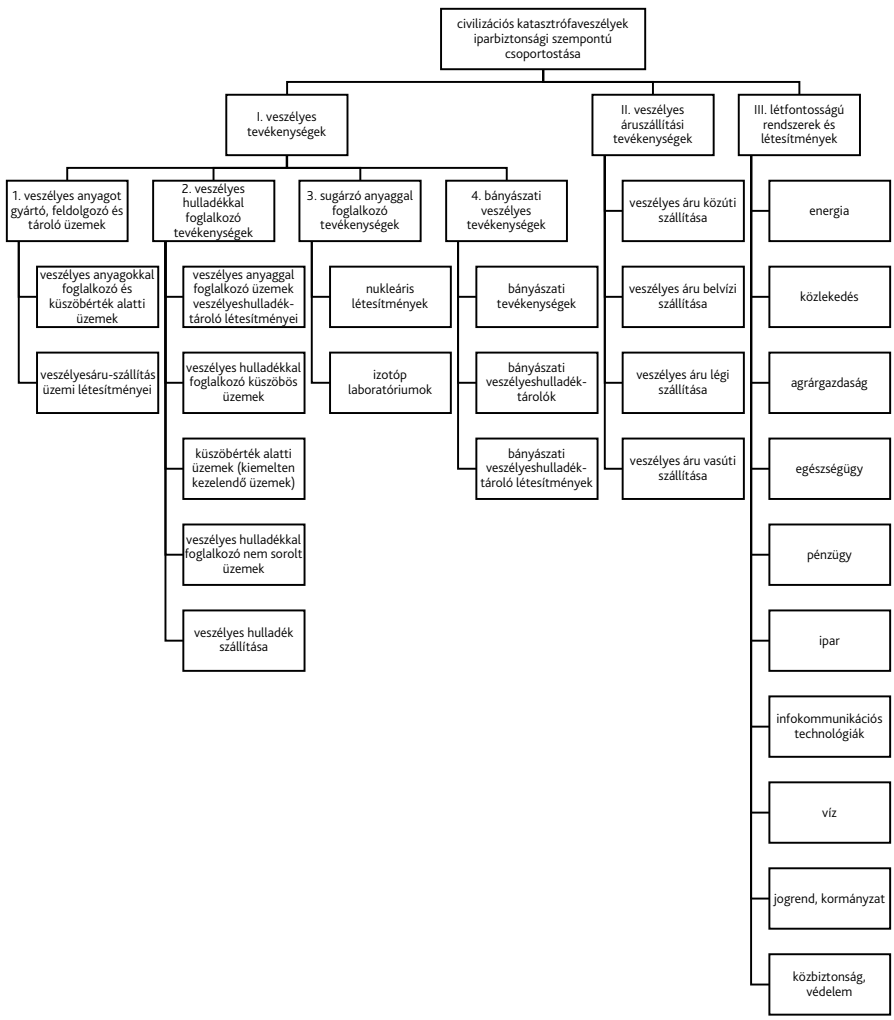
A vegyi anyagokkal kapcsolatban elengedhetetlen a veszélyes technológiák veszélyesanyag-kibocsátásait is elhatárolni: a normál üzemi kibocsátások hosszú lefolyású, nagy térséget érintő környezeti igénybevétellel, környezetterheléssel és szennyezéssel járó, hosszú távú környezetmódosító és környezetkárosító hatású veszélyes tevékenységekhez köthetők. Vészhelyzeti kibocsátásról akkor beszélünk, amikor jelentős mértékű káros (döntően mérgező) anyag kerül a környezetbe, tűzzel és/vagy robbanással járó esemény következik be, és a létesítményen belül vagy azon kívül közvetlenül vagy lassan hatóan veszélyezteti, károsítja az emberi életet, egészséget és/vagy környezeti elemeket. Ez utóbbi túlmutat a környezetvédelmen.[7] A vizsgálat elsődleges célja a nem normál üzemi kibocsátások kapcsán megjelenő, az emberi életet, egészséget, illetve a környezeti elemeket súlyosan károsító, veszélyeztető vészhelyzeti kibocsátások kockázatainak áttekintése.

[5] 2011. évi CXXVIII. törvény 3. § 27. és 28. pont.
[6] 219/2011. (X. 20.) Korm. rendelet 1. § 1. és 2. pont.
[7] Hoffmann et al. 2015.

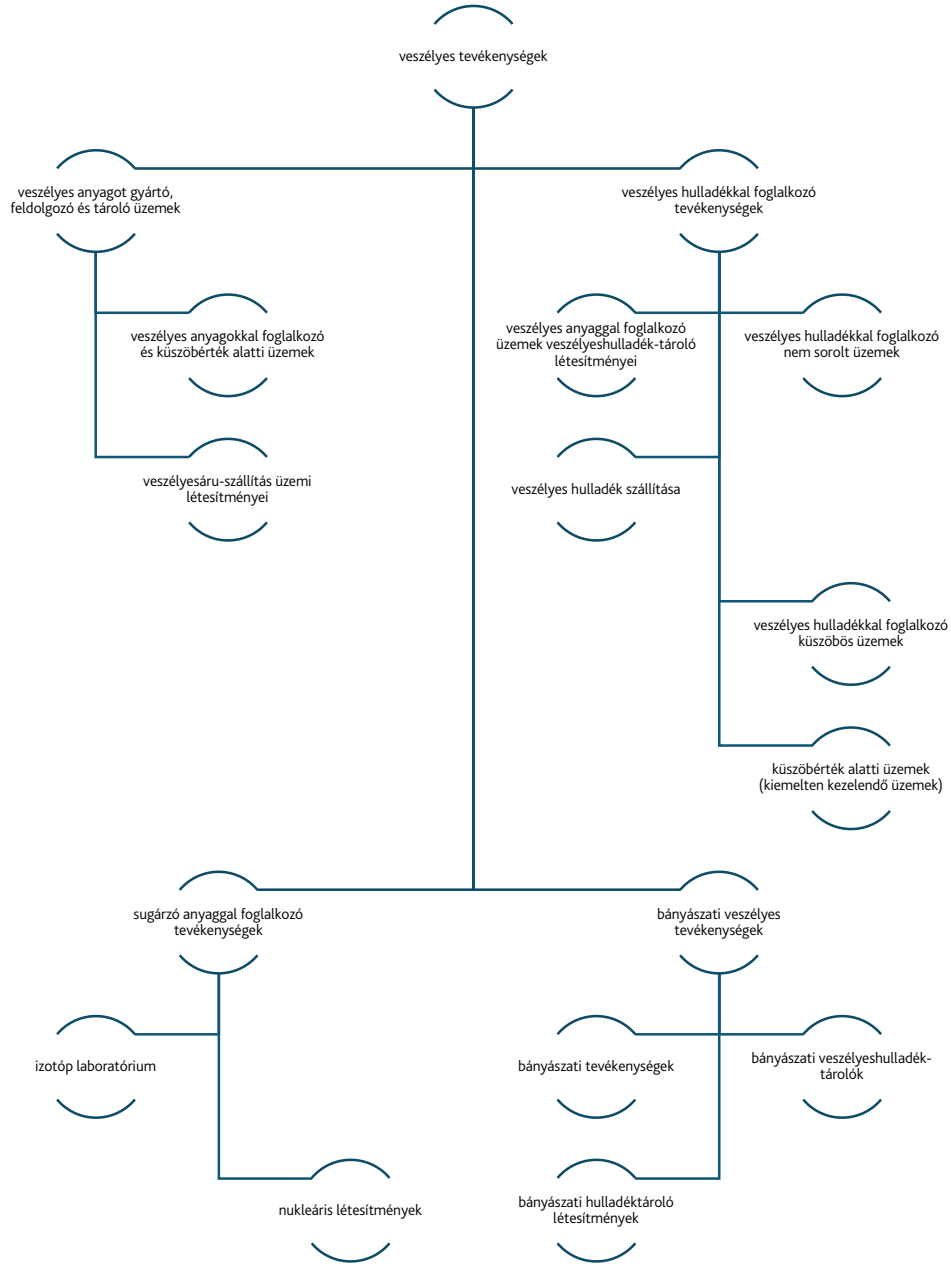
A civilizációs katasztrófaveszélyek kapcsolódhatnak veszélyes tevékenységekhez, veszélyesáru-szállítási tevékenységekhez és létfontosságú rendszerekhez/létesítményekhez. Az egyes csoportok elkülönítése segítséget nyújt az azonosításban.

A veszélyes anyagok gyártása, tárolása és feldolgozása során bekövetkező baleset lehet:

- tűz, amely a közvetlen környezetben okoz kárt;
- robbanás;
- egészségre, környezetre káros anyagok levegőbe vagy vízfolyásokba jutása – az anyag fajtájának, mennyiségének, fizikai mutatóinak, a terjedés meteorológiai, domborzati és más tényezőinek függvényében.



1. ábra: Civilizációs katasztrófahelyzetek
Forrás: Hoffmann et al. 2015



2. ábra: Veszélyes tevékenységek
Forrás: a szerző szerkesztése HOFFMANN *et al. 2015 alapján*

Ez utóbbi baleset több tíz kilométer távolságban is veszélyt okozhat, a lefolyása percek vagy órák alatt végbemehet, szélsőséges esetben akár több évtized időtartamra is elnyúlhat.[8] A civilizációs katasztrófaveszélyek iparbiztonsági szempontú csoportosítása az 1. ábrán látható.

A vizsgálat tárgya elsősorban a veszélyes tevékenységekre vonatkozik, így a veszélyes anyagokat gyártó, feldolgozó üzemeket, a veszélyes hulladékkal foglalkozó tevékenységeket, a sugárzó anyaggal foglalkozó tevékenységeket és a bányászati veszélyes tevékenységeket vizsgálom (2. ábra). Ennek létjogosultságát az adja, hogy a veszélyes anyagokkal foglalkozó üzemek működése kapcsán szerteágazó kockázatok határozhatók meg, a tevékenységek szállításra és egyéb tevékenységekre való kiterjesztése felaprózza a kockázatértékelést, kezelhetetlenné téve az adatbázist. Az alap adatbázis elkészültét, tesztelését követően lehet releváns annak kibővítése.

A vizsgálat tárgya az eseményekkel kapcsolatos prognózis, a látható és meg nem jósolható reakciók feltérképezése. A katasztrófavédelem folyamatosan bővülő listába rendezi a szóban forgó üzemeket, a nukleáris, kommunális és ipari hulladéklerakókat, a hulladékmegsemmisítőket, a lista azonban nem teljes. Az RSOE-EDIS Katasztrófa- és Vészhelyzeti Információs Szolgálat figyelemmel kíséri a földet veszélyeztető összes eseményt, feldolgozza az összegyűjtött információt, megjeleníti az eseményeket a felhasználók igényei alapján szűrhető formában, de az ő felsorolásuk sem mindenre kiterjedően szolgáltat információt.[9] A vizsgálat során (az RSOE-EDIS definíciói alapján) vizsgált események:

- veszélyes üzemek balesete (ipari és mezőgazdasági létesítmények, amelyekben alsó és felső küszöbértéket elérő mennyiségben vannak jelen veszélyes anyagok; az ezekkel való tevékenység során a folyamatok ellenőrizhetetlenné válása tömeges veszélyeztetést, emberi egészség-, környezet-, élet- és vagyonbiztonságot károsító eseményt okozhat; kiemelkedően jelentős mértékű kár, tömeges emberi sérülés vagy haláleset következhet be, a mentesítés, mentés elhúzódó);
- mérgező vagy vegyi anyagok kikerülése;
- izotópbaleset;
- nukleáriserőmű-baleset.[10]

Egyéb hazmat eseményeket[11] nem tekintek a vizsgálat tárgyának. A vizsgálat nem terjed ki továbbá a veszélyesáru-szállítással kapcsolatos balesetekre sem.

A mesterséges intelligencia fogalmi kereteinek meghatározása a teljesség igényével nehéz. Nincs egységes alapvetés a tekintetben, hogy a definíciónak pontosan mit kell tartalmaznia. Konkrét meghatározás nem létezik. A leglényegesebb eleme, hogy informatikai rendszer, feladatmegoldásra képes, és az emberi gondolkodáshoz hasonlóan működik.[12] Siba László (1989) a számítástudományok olyan területeként

[8] Hoffmann et al. 2015.
[9] RSOE-EDIS [é. n.].
[10] RSOE-EDIS [é. n.].
[11] Veszélyes anyagokkal kapcsolatos események, amelyek a veszélyes anyagokkal kapcsolatos általános kategóriákba nem illenek bele, vagy azok jellege vegyülve jelenik meg.
[12] Siba 1989.

aposztrofálja, amely emberi intelligenciát igénylő feladatokat megoldó számítógépes programok készítésével foglalkozik.[13] A definíció megjelenése a gépi tanulás virágkorának idejére (1980–1990) tehető. Az AI több ennél: nem előre meghatározott utasítások alapján, hanem adatokból tanulva végzi el a feladatokat, algoritmusokat, matematikai képleteket használ a döntéshozatalhoz, valamint a korábban tanult adatokat. Nem statikus, hanem autonóm működésű, és a legfontosabb tulajdonsága, amely a veszélyes üzemek kockázatkezelésében is jól alkalmazható, a tanulási képesség.

Önálló döntéshozatalra képes, reagálni tud a változásokra, valamint adaptálódni a környezethez. Ezek alapján az MI az emberi gondolkodás általános alapelveit alkalmazó, tanulási képességgel rendelkező, adatokból, matematikai képletekből és tanult adatokból önálló döntéshozatalra képes, autonóm működésű számítógépes rendszer, amely azonban emberi tulajdonságokkal nem ruházható fel, érzelmei, belátási képessége nincs, csupán emberhez hasonló képességei vannak (szemben azzal az alapvetéssel, amely szerint az MI elsősorban viselkedését tekintve nehezen különböztethető meg az embertől).[14] A vizsgálat szempontjából leginkább releváns az AI érzelmekre, belátási képességre vonatkozó hiányossága. Feltételezésem szerint ugyanis csak akkor képes a munkavállalókat érő kockázatokat megfelelően felismerni és kezelni, ha az ember egyéni sajátosságait is képes figyelembe venni, a kockázatok egy része ugyanis ebből fakad. Különös tekintettel a veszélyes üzemek működésére.

Az elemzés során olyan AI-eszközöket vizsgálok, amelyek betanított válaszológépek (a kép- és videógenerátorokat mellőzöm, az általuk létrehozott tartalmak nem relevánsak). A kiválasztás szempontja az, hogy ingyenes és Magyarországon is közvetlenül elérhető legyen, és valós idejű adatokban is keressen. A vizsgálati kérdések megfogalmazása magyar nyelven és három dimenzió (kockázatok, lehetséges kimenetelek és megoldási javaslatok) mentén történik. Az alapkoncepció szerint ugyanazokat a kérdéseket kapja valamennyi AI-asszisztens, de előfordulhat, hogy kiegészítő kérdésekre is szükség van a pontosítás érdekében.

A vizsgálandó események nem kizárólag a veszélyes anyagokkal kapcsolatos balesetekre korlátozódnak, a mesterségesintelligencia-eszközök feladata a veszélyes üzemek idővel történő fokozatos romlásából fakadó kockázatok értékelése.

A kérdések megfogalmazásakor az elsődleges szempont az volt, hogy az AI-eszközök nem feltétlenül ugyanazzal a nyelvi modellel dolgoznak, a megértés nagymértékben befolyásolhatja a kapott válaszokat. Figyelembe kellett venni azt is, hogy egyes AI-eszközök korlátozzák a feltehető kérdések és az ezekre adott válaszok számát.

Az AI-nak feltett alapkérdések:

1. Vázold fel az esemény kapcsán az összes lehetséges kimenetelt!
2. Milyen kockázatokkal kell számolni?
3. Az egyes kockázatok súlyosságát és bekövetkezési valószínűségét meg tudod jósolni?
4. Az emberi tényezőt figyelembe véve milyen kockázatokat tudnál felvázolni?
5. Van olyan emberi tulajdonság, amely súlyosbíthatja ezeket a kockázatokat?
6. Milyen intézkedéseket tennél a kockázatok csökkentése, megelőzése érdekében? Kockázatonként csoportosítva, ha lehet.

[13] Siba 1989.
[14] Fehér et al. 2020 értelmezésében: érvel, tanul, tervez.

A vizsgált események rövid leírása

A vizsgálat során olyan, megtörtént vagy elképzelhető eseményeket rögzítek az AI-eszközök számára, amelyek kimenetele többféle forgatókönyv mentén vázolható fel. Annak, hogy nem csupán valós események mentén vizsgálom az AI reakcióit, azért van relevanciája, mert feltételezésem szerint, ha nem rendelkezik valós tudással, akkor a meglévő alapján kell felépítenie a válaszait (tanul).

Az első esemény a paksi atomerőmű 2003-as, súlyosnak minősülő üzemzavarához kapcsolódik. Az AI-eszközöknek feltett kérdések egy lehetséges forgatókönyvhöz igazodnak, valós, megtörtént eseményekre alapozva. Eszerint nem működő reaktor melletti, attól leválasztott, vízzel teli, mély aknában végzik a fűtőelemek mosását (ami a hőtermelés során lerakódott, nemkívánatos és a hatékonyságot nagymértékben csökkentő szennyeződések eltávolítását jelenti).[15] A reaktorból eltávolított fűtőelemek nem lettek lehűtve, így kerültek az aknába. A nem megfelelő hűtés miatt a fűtőelemek túlhevültek, a tartály tetején a felforró víz buborékjai egyetlen nagy gőzbuborékká álltak össze. A nem áramló gőz hűtőközegként nem funkcionál, a fűtőelemek hőmérséklete még tovább emelkedett, burkolatuk megrepedt. A vízgőzzel kémiai reakcióba léptek. A fűtőelemek teljes hosszában kialakuló gőzbuborékba radioaktív nemesgázok és illékony hasadási termékek kerültek. A tartály teteje nem lett eltávolítva. A csarnokban olyan mértékűre nőtt a dózis, hogy csak speciális légzőkészülékkel lehetett bent tartózkodni.

A másik esemény petrolkémiai üzemhez kapcsolódik: egy csőtartó oszlop tetején 3 m magasságban 50 mm átmérőjű csővezeték hosszában felhasad és 10–12 cm hosszú nyíláson át 30 bar nyomással ömlik a pirogáz a szabadba. A hirtelen expanzió következtében erősen lehűlt gázfelhő gyűlik össze a talaj közelében, a mérsékelt szél miatt a szomszédos robbanásveszélyes üzemek felé sodródik. A gyári belső úthálózaton folyamatos a közlekedés. A nagy sebességgel örvénylő gázfelhő sztatikusan feltöltődik, a leföldelt acélszerkezetek között kisül, a szabadba kerülő gátfelhő berobban.

Vizsgált AI-programok

Gemini: Egyszerűbb válaszokat ad már ismert információk alapján vagy más forrásokra támaszkodva (más Google-szolgáltatásokból származó), vagy bonyolultabb válaszokat, nyelvi modellek szavait felhasználva. A nyelvet alkotó mintákat képes felismerni, a leggyakoribbak alapján válaszol. Az utasításokból, válaszokból és visszajelzésekből (is) tanul. Saját gondolatai, érzései nincsenek. Szavakból tanul, adott mintázat betanulását követően képes megjósolni a következő lehetséges szavakat. A válaszadásra a mintázatok alapján a kreativitás jellemző. A használat korlátja az adott időkeret, az ezen belül adható utasítások és beszélgetések száma. Ez Ex-Bardnak is tekinthető, a Google ChatGPT-re adott válasza.

[15] Szatmáry 2003.

Copilot: A Microsoft AI-eszköze. Bizonyos funkciók magyarul, ingyen, bármilyen eszközön használhatók. Komplex kérdéseket is fel lehet tenni neki. Beépülő modulok alkalmazhatók. Ugyanaz a funkciója, mint a ChatGPT-nek, az Open AI GPT 4 és GPT 4 Turbo nagy nyelvi modelljével dolgozik.
ChatGPT 4: Mesterségesintelligencia-alapú chatbot, az egyik legismertebb és leggyakrabban használt. Az Open AI fejlesztése, az általa gyűjtött és beprogramozott ismeretekből szerzett információk alapján válaszol a kérdésekre.
Bing AI: A Microsoft Edge keresőmotorjának AI-asszisztense. Kiszámíthatatlan viselkedése tette ismertté. Nem kizárólag szövegalkotásra képes, képgenerátor funkcióval is el van látva. Ingyenesen elérhető, de regisztrációhoz kötött.
Discord: Szöveges, képi, videó- és hangkommunikációra képes eszköz, hanggal vezérelhető, alapvetően gamereknek fejlesztették ki. Dinamikusan képes alakítani a beszélgetéseket, információk kérhetők, adott esetben játszani is lehet vele. Ingyenesen elérhető, de regisztrációhoz kötött. A felület jóval bonyolultabb, mint a többi chatbot esetében.
Google Bard: Képes a felhasználók kérdéseinek megválaszolására, információkat keres gyorsan és hatékonyan. A ChatGPT-hez hasonló alapfunkciója, hogy az emberi beszélgetéseket utánozza természetes nyelvi feldolgozással és gépi tanulással. Kezdetben a LaMDA (Language Model for Dialogue Applications) családjának nagy nyelvi modellje alapján működött (LLMS), ezt követően a PaLM- (Pathways Language Model 2) technológiát alkalmazták. Beszélgetésalapú chatbot, webes hozzáférésekből és LLM-ekből dolgozik (nagy nyelvi modellekből), szöveg- és kódadatbázison tanulnak. A mai Gemini (lásd korábban).
Perplexity: Mesterséges intelligenciával működő keresőmotor. A ChatGPT-hez hasonlóan információk keresésére alkalmazható. Ingyenesen elérhető verziója rendkívül korlátozott, egy kérdés feltételére ad lehetőséget.
Ask AI: GPT-4o és GPT-4 technológiára kifejlesztett chatbot, ajánlásokat, inspirációkat és információkat kínál minden témában. Ingyenesen elérhető verziója rendkívül korlátozott, egy kérdés feltételére ad lehetőséget.

SEVESO-üzemek – súlyos baleset, katasztrófahelyzet az AI szemével

Az egyik legfontosabb kérdés, hogy képes-e az AI a vészhelyzetekre való reagálás emberi vonatkozásait is figyelembe venni az elemzéskor. Ennek főként azért van létjogosultsága, mert a súlyos ipari balesetek csaknem fele emberi mulasztásra vezethető vissza. Statisztikai elemzések során levont következtetések szerint a magas szintű szakképzettség, a legfejlettebb technológia alkalmazása önmagában nem képes megakadályozni egy súlyos ipari baleset vagy valamely veszélyes anyaggal kapcsolatos esemény bekövetkezését, illetve a múlt tapasztalatai alapján tervezett, ipari körülmények között tesztelt, folyamatosan fejlesztett biztonsági rendszerek sem nyújthatnak százszázalékos védelmet minden esetben. A kérdésekre adott válaszok alapján az látszik, hogy valamennyi AI-eszköz egyazon adathalmazból, nyelvi modellből tanul és dolgozik. Az „ember" javarészt hiányzik belőlük.

A *Gemini* változatosan kezeli az alapszituációkat, hellyel-közzel jól átlátja a lehetséges kockázatokat, azonban nem részletezi a lehetséges összes szcenáriót. Jól látszik, hogy azokban az esetekben, amelyekben viszonylag sok adat fellelhető a webes

felületeken, értékelhetőbb válaszokat fogalmaz meg (például a lehetséges kimeneteleket időtartam – rövid távú események, közép- és hosszú távú kimenetelek – szerint kategorizálja), de konkrétumokat kizárólag kérésre, több kérdéssel rávezetve ad meg. A legrosszabb szcenáriót az ismert esetekben jól átlátja, a kitalált eseményeknél azonban elnagyolja a választ és általánosan fogalmaz. A kockázati mátrix elkészítéséhez saját bevallása szerint nem rendelkezik megfelelő mennyiségű és minőségű tudással, a paksi eset elemzésekor pedig jól összeszedett választ adott. A kockázatokat egyébként címszavakban adja meg, a technológiai és munkaköri, valamint a munkakörnyezetből fakadó kockázatokat nem tudja értékelni. Sok esetben megadja a lehetséges kiváltó okokat, a karbantartás hiánya szerepel a felsorolásban, azonban például az anyaghiba vagy anyagfáradás nem. És nem említi az embert magát sem, ha direkt kérdésben nem szerepel. A kockázatokhoz egyébként csatol egy intézkedést is, amellyel az adott kockázat csökkenthető, noha ez kérdésként nem szerepelt. Az emberi tényező esetében általában ugyanazok az elemek jelennek meg:

- képzetlenség;
- figyelmetlenség;
- nem megfelelő eszköz- és géphasználat;
- kommunikációs problémák;
- motiváció hiánya;
- biztonsági előírások figyelmen kívül hagyása;
- vészhelyzeti előírások nem megfelelő ismerete;
- hibás döntés.

Érdekes adathalmaz volt, ahogy a folyamatok eszkalálódását eredményező emberi tulajdonságokat kezeli.

1. Személyiségvonások:
   - Agresszivitás: Ha egy dolgozó agresszív személyiségjegyekkel rendelkezik, konfliktushelyzetekben hajlamosabb eszkalálni a helyzetet, akár fizikai erőszakkal is.
   - Impulzivitás: Az impulzív emberek gyakran gondolkodás nélkül cselekszenek, így könnyen hozhatnak olyan döntéseket, amelyek felerősítik a problémát.
   - Konfliktuskerülő magatartás: Paradox módon a konfliktus elől való menekülés is vezethet eszkalációhoz, ha a dolgozó nem mer szólni nemmegfelelőség esetén, a probléma viszont nem szűnik meg, hanem tovább gyűrűzik.
   - Perfekcionizmus: A túlzott tökéletességre való törekvés stresszt okoz, megnöveli a hibázás lehetőségét.
2. Érzelmi állapotok:
   - Félelem: A félelem, hogy büntetés jár a hibáért, vagy hogy elveszíti a munkáját, a dolgozót arra ösztönözheti, hogy eltitkolja a problémát, ami később nagyobb bajhoz vezethet.
   - Düh: A dühös dolgozó könnyen elveszíti a kontrollt, és olyan cselekedeteket hajthat végre, amelyek veszélyeztetik saját magát és másokat.
   - Frusztráció: A folyamatos frusztráció, a megoldhatatlannak tűnő problémák szintén agresszív viselkedéshez vezethetnek.

3. Kognitív torzítások:
    - Önbizalomhiány: Az önbizalomhiányos dolgozó hajlamosabb hibázni, és nehezebben kér segítséget, ami szintén eszkalációhoz vezethet. Ez a tényező talán a legkevésbé tudatos.
    - Állandó megfelelési kényszer: Az állandó megfelelési kényszer stresszt okoz, és hibákhoz vezethet.
    - • Felelősségvállalásra való képtelenség hiánya: Ha a dolgozó a problémákat mindig másoknak tulajdonítja, akkor nem hajlandó változtatni a saját viselkedésén, ami fenntartja a konfliktust.
4. A helyzethez kapcsolódó tényezők:
    - Időnyomás: Ha a dolgozó időnyomással dolgozik, akkor hajlamosabb hibázni és figyelmen kívül hagyni a biztonsági előírásokat.
    - Túlterheltség: A túlterhelt dolgozó nehezen tud koncentrálni, és könnyebben elkövet hibákat.
    - Rossz kommunikáció: A félreértések és a rossz kommunikáció könnyen vezethet konfliktusokhoz és eszkalációhoz.

A *Copilot* általánosságokat fogalmaz meg: személyi sérüléseket, környezeti károkat, tűzveszélyt, közösségi egészségügyi kockázatokat (szennyezett levegő, víz által okozott egészségügyi problémák – asztmás tünetek, allergiás reakciók, légzőszervi megbetegedések) és az egészségügyi költségek növekedését mint esetlegesen felmerülő kockázatot említi, az emberi tényezőből eredő kockázatokat nem önállóan, hanem direkt irányított kérdésre válaszolva adja meg a teljesség igénye nélkül (figyelmetlenség, képzetlenség, fáradtság, kommunikációs hibák, stressz, túlterheltség, munkavégzés megszokottá válása stb.), az egyéni sajátosságokat irányított kérdéssel sem veszi figyelembe (például azt, hogy adott szituációban minden ember másképp reagál vérmérséklettől, felkészültségtől, meglévő tapasztalattól, életkortól, nemtől stb. függően). A beszélgetés ezen a ponton megszakadt, a kockázatokat súlyosbító tényezőkre vonatkozó kérdésre nem érkezett válasz. Második alkalommal szépen végigvezette a kérdésekre adott válaszokat a kérésemnek megfelelően a paksi atomerőmű üzemzavara kapcsán, a lehetséges legrosszabb forgatókönyvet is figyelembe véve.

A *ChatGPT* az események megfogalmazásakor összefoglalta a legfontosabb tényezőket. Az esetlegesen bekövetkező eseményeket súlyosságuk szerint kategorizálta. Felvázolt egy katasztrofális szcenáriót, a következmények és utóhatások kapcsán a jogi következményekkel is foglalkozik, valamint az esetleges pénzügyi károkat is megemlíti. A kockázatokat személyi, környezetvédelmi, gazdasági, szabályozási és jogi, társadalmi, valamint technikai aspektusban vizsgálja. A kockázatok súlyossága és bekövetkezési valószínűsége kapcsán azonban saját bevallása szerint nem rendelkezik megfelelő tudással. Második alkalommal képes volt a számára releváns kockázatok súlyosságát és bekövetkezési valószínűségét megadni. Az emberi tényezőkre vonatkozó kérdés kapcsán ugyanazzal a készlettel dolgozik, mint amivel a többi AI-eszköz, csupán a megfogalmazás más. Az egyes kockázatokat súlyosbító emberi tulajdonságokat azonban másképp értelmezi, mint például a Gemini. Az adott tulajdonság által kiváltott hatás (például a túlzott magabiztosság miatt a dolgozók alábecsülhetik a helyzet kockázatait, vagy elhanyagolhatják a biztonsági intézkedéseket, mivel úgy érzik, hogy

már mindent jól tudnak) részletesen jelenik meg. Érdekes, hogy a rossz időgazdálkodást is súlyosbító tényezőként értékeli, szerinte ugyanis az időmenedzsment hiánya kényszerhelyzetet teremthet a dolgozók számára, aminek következményeként rossz döntéseket hozhatnak, hogy időt spórolhassanak. Ehhez kapcsolódik, hogy szerinte a munkavállalók közötti ellenséges viszony és rosszindulat jelentős mértékben csökkentheti a figyelmet, rontja a szabálykövető magatartást. Alapjaiban véve ugyanazokat a tulajdonságokat sorolta fel, mint a Gemini.

Összegzés

A mesterséges intelligencia az élet szinte minden területén, a legtöbb gazdasági ágazatban képes volt viszonylag rövid idő alatt teret hódítani magának, a munkavédelemben azonban kevésbé elterjedt. A dinamikusan változó környezeteket az AI-eszközök általában nem tudják (még) megfelelően kezelni. A veszélyes üzemekben a kockázatértékelések kapcsán ténylegesen van létjogosultsága a mesterséges intelligenciának, hiszen nagy mennyiségű strukturált és strukturálatlan adat feldolgozására képes, olyan mintákat és összefüggéseket azonosít, amelyek az emberi elemzők számra vagy nehezen, vagy egyáltalán nem észrevehetők. A mesterséges intelligencia képes modelleket alkotni, amelyek a jövőbeni eseményeket előre tudják jelezni, a proaktivitásban ennek kiemelten fontos szerepe van. A gyorsan változó körülményekre való reagálás képessége a valós idejű adatelemzésre való képesség függvénye. A mesterséges intelligencia alkalmazásával lehetőség nyílik erre. Ehhez azonban szükséges az AI-eszközök tudásának folyamatos bővítése, mélyítése. Az emberi tényezők vizsgálata rávilágított arra, hogy ez komoly hiányosság még, annak ellenére, hogy a veszélyes üzemekben megjelenő, munkavállalókat, szűkebb és tágabb környezetet stb. érintő kockázatok esetén súlyosbító tényező lehet egy-egy emberi tulajdonság.

A vizsgálat alapján az alábbi következtetések vonhatók le:

1. Az AI alkalmazása veszélyes anyagokkal foglalkozó üzemekben jelentősen növelheti a kockázatértékelés hatékonyságát, különösen nagy adathalmazokból származó mintázatok felismerésével és valós idejű elemzéssel.
2. Az AI-t olyan keretben érdemes használni, amely etikus, kritikai szemléletű és a humán tényező bevonását is biztosítja. Szükség van az emberi hibákból eredő kockázatok csökkentésére.
3. A veszélyes anyagokkal foglalkozó üzemek esetében problémát jelent a fogalmi keretek pontos megadása, az azonosítás és a határértékek kezelése, mivel a küszöbértékek nem feltétlenül befolyásolják a potenciális károkat; ezért a kockázatértékelésnél a környezetre és az emberre jelentős hatást gyakorló azonosított üzemek kerülnek előtérbe.
4. A mesterséges intelligencia fogalmi keretei és definíciói hiányosak és nem egységesek, ami megnehezíti a szabályozás és az összehasonlítható értékelések kialakítását.
5. A fenti problémakör és a jogi-szabályozási környezet hiányának, hiányosságainak összefüggései miatt szükség van a definíciók és az adatbázisok folyamatos bővítésére és naprakészen tartására.

Az MI jó eszköz lehet a kockázatértékelés gyorsítására, mintázatfelismerésre és az adatokból történő következtetések levonására, de nem helyettesítheti teljes mértékben az emberi szakértőket. A kockázatok megközelítése többszintű: technikai, emberi tényezők, környezeti hatások, jogi és gazdasági aspektusok együttes értékelése szükséges. A vizsgált források megerősítik, hogy a veszélyes üzemek kockázatkezelésében az adatalapú módszerek és az AI jelentős előnyöket kínálnak, különösen nagyszámú és strukturálatlan adatok esetén. Ugyanakkor a fogalmi keretek nem egyértelmű volta, az azonosítás bonyolult kérdésköre jelentős mértékben megnehezíti az alkalmazást. Az emberi tényezőket figyelembe kell venni, a releváns tényezők megadása azonban szintén széles körű elemzést igényel.

Az AI-alapú kockázatértékelő rendszerek kifejlesztése, AI-alapú szimulációk és interaktív oktatási modulok a mentesítési protokollok és vészhelyzeti eljárások jobb megértése, valamint kockázati mátrixok és események forgatókönyvei alapján működő döntéstámogatás irányába mutatnak.

További kutatási irányok:

- Uniós és nemzeti szabályozói keretek pontosításának vizsgálata a veszélyes anyagokkal foglalkozó üzemekre vonatkozóan; egységes fogalmi keretek és értékelési mutatók kidolgozása.
- AI-modellek kiértékelése a teljes kockázati spektrum lefedésére: képesek-e feltérképezni minden lehetséges kimenetelt és figyelembe venni az emberi tényezőket is?
- Szimulációalapú kutatások a vészhelyzeti kibocsátások és azok hosszú távú hatásainak modellezésére AI-támogatással.
- AI-alapú kockázatkezelő rendszerek integrálása a meglévő üzemirányítási rendszerekbe, valamint a humán-számítógép interfész javítása.

A veszélyes anyagokkal foglalkozó üzemek definíciója rendkívül összetett és sokténezős. A jogszabályok alapján alsó és felső küszöbértékű üzemek léteznek, de ezek a küszöbértékek nem feltétlenül korrelálnak a potenciális katasztrófakockázatok súlyosságával. Gyakran előfordul, hogy olyan üzemek minősülnek be, amelyekben a veszélyes anyagok jelenléte hosszú távon is kockázatot jelent, vagy olyan esetek, ahol a tevékenység nem hagyományos, mégis kiemelt kockázatot hordoz. Emiatt nehéz egységes, minden szcenáriót lefedő definíciót kialakítani, és az AI-alapú modellek számára is kihívást jelent a teljes körű és konzisztens fogalmi keret biztosítása. A definíciós bizonytalanság miatt fontos a rugalmas, kontextusérzékeny megközelítés és az interdiszciplináris értékelés.

Felhasznált irodalom

Bekey, George A. (2005): *Autonomous Robots: From Biological Inspiration to Implementation and Control*. Cambridge, MA: MIT Press.

Európai Munkahelyi Biztonsági és Egészségvédelmi Ügynökség (2020): *A digitalizáció és a munkavédelem. Az EU-OSHA kutatási programja.* Online: https://osha.europa.eu/sites/default/files/Digitalisation_and_OSH_HU.pdf

Fehér Krisztián – Kökényesi-Bartos Attila – Bártfai Barnabás (2020): *Mesterséges intelligencia, avagy Pandora digitális szelencéje.* Budapest: BBS-Info Kft.
Hoffmann Imre et al. (2015): Iparbiztonság Magyarországon. *Védelem Online,* 22(1), 1–12. Online: https://www.vedelem.hu/letoltes/anyagok/549-dr-hoffmann-imre-dr-levai-zoltan-dr-katai-urban-lajos-dr-vass-gyula.pdf
RSOE-EDIS [é. n.]: *Esemény definíciók.* Online: https://rsoe-edis.org/eventDefinitions
Siba László szerk. (1989): *Oxford számítástechnikai értelmező szótár.* Budapest: Novotrade Kiadó.
Szatmáry Zoltán (2003): Súlyos üzemzavar a Paksi Atomerőműben. *Fizikai Szemle,* 53(8), 266–271. Online: https://fizikaiszemle.elft.hu/archivum/fsz0308/szatmary0308.html
Zákányi Balázs – Fodor Ádám – Zákányiné Mészáros Renáta (2024): A munkavédelemben alkalmazható mesterséges intelligencia alkalmazásának morális és etikai kérdései. *Multidiszciplináris Tudományok,* 14(4), 353–367. Online: https://doi.org/10.35925/j.multi.2024.4.29

Jogi források

2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról. Online: https://net.jogtar.hu/jogszabaly?docid=a1100128.tv
219/2011. (X. 20.) Korm. rendelet a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről. Online: https://net.jogtar.hu/jogszabaly?docid=a1100219.kor

HADMÉRNÖK
BIZTONSÁGTECHNIKA

20. évfolyam (2025) 2. szám 21–36.
DOI: 10.32567/hm.2025.2.2

Tisza István[1]

A személyvédelem mechanikai eszközeinek vizsgálata, fejlesztési javaslatok

Examination of Mechanical Means of Personal Protection, Development Proposals

Absztrakt

A katasztrófavédelem beavatkozást végző munkavállalói számos alkalommal több súlyos kockázatnak vannak kitéve, amelyekkel szemben az egyéni védőeszközök sem minden esetben nyújtanak százszázalékos védelmet, noha a fejlesztések a védelmi szint maximalizálását célozzák. A kompromisszum a kényelem, a praktikum, a használhatóság és a maximális védelem között gyakran elengedhetetlen. A fejlesztési irányok az egyéni igényeknek megfelelően és ezektől függetlenül is jól meghatározhatók. A fejlődés üteme nem statikus állandó, dinamikusan változik eltérő intenzitással. Szükséges azonban összetett szempontrendszer alapján megadni azokat a lehetőségeket, amelyek mentén a fejlesztések minden igényt kielégítően elvégezhetők.A tanulmány legfontosabb célja a személyvédelem mechanikai eszközeinek, a tűzoltók egyéni védőeszközeinek vizsgálata az evolúció és a fejlesztési irányok tekintetében. A fejlesztésekkel kapcsolatban szükségszerű az azokra vonatkozó követelmények áttekintése, az optimális funkcionalitás, alkalmazhatóság és maximális védelmi szint meghatározása. A tanulmány célja továbbá a gyakorlati implementációra való javaslattétel.A vizsgálati módszer a vonatkozó szakirodalom áttekintése a teljesség igénye nélkül, az evolúciós ív megjelenítése, szemléltető elemzések készítése a jelenlegi védelmi képességekről és korlátokról a vegyi, hő- és mechanikai terhelések kapcsán, technológiai és anyagösszetételi vizsgálatok ismertetése a nanotechnológia és a korszerű textilanyagok felhasználásáról, jövőbeli fejlesztési irányok és követelmények meghatározása a mérnöki és gyártási folyamatokra vonatkozóan.

Kulcsszavak: egyéni védőeszköz, evolúció, nanotechnológia, fejlesztés, optimalizálás

[1] Tűzoltósági felügyelő, Fehérgyarmati Katasztrófavédelmi Kirendeltség, e-mail: Istvan.Tisza2@katved.gov.hu

Abstract

In many cases, emergency response workers are exposed to multiple, serious risks, against which personal protective equipment does not provide 100% protection in all cases, even though improvements are aimed at maximising the level of protection. A compromise between comfort, practicality, usability and maximum protection is often essential. Development directions can be well defined according to individual needs and independently of them. The rate of development is not static, it changes dynamically with different intensities. However, it is necessary to provide the options based on a complex system of criteria, according to which the developments can be carried out to the satisfaction of all needs. The main objective of the study is to examine the evolution and development directions of mechanical personal protection devices, personal protective equipment for firefighters. In connection with the developments, it is necessary to review the requirements for them, determine the optimal functionality, applicability and maximum protection level. The study also aims to make recommendations for practical implementation.The research method is a review of the relevant literature without claiming to be complete, to present the evolution curve, to prepare illustrative analyses of current protection capabilities and limitations in relation to chemical-thermal and mechanical loads, to present technological and material composition studies on the use of nanotechnology and modern textile materials, to determine future development directions and requirements for engineering and manufacturing processes.

Keywords: personal protective equipment, evolution, nanotechnology, development, optimisation

Bevezetés

A bevetések, beavatkozások során a tűzoltók számos veszélynek vannak kitéve, amely veszélyek a technológiai fejlődéssel egyre tágabb értelemben jellemzők és egyre súlyosabb következményekkel járhatnak akkor, ha nem alkalmazzák a rendszeresített egyéni védőeszközöket (a kollektív műszaki védelem a beavatkozások során nem kialakítható). Mivel egyre több veszéllyel szemben kell védeni a tűzoltókat, egyre nagyobb mértékű károsodásoktól, a védőeszközök folyamatos fejlesztése elengedhetetlen. Ezeknek az eszközöknek a sajátossága, hogy a védelmi szintek elérése mellett használhatónak is kell maradniuk, ez azonban a gyakorlatban sok esetben nem tud megvalósulni (például kesztyű).

Korábban végzett kutatási eredményeim abba az irányba mutatnak, hogy az eszközfejlesztés célja az egyéni védőeszközök terén elsősorban a védelmi szint elérése, nem a praktikum és a kényelem. A tűzoltóság olyan terület, ahol számos kockázat nagyon súlyos következménnyel, viszonylag gyakran következik be általában egy időben. Valamennyi kockázat figyelembevételére nincs lehetőség, ha mégis, akkor a korábban említett problémákkal szembesül az eszközt használó. A vizsgálat fő kérdése az volt, hogy oldhatók-e ezek az anomáliák, ha igen, milyen módon (a fejlesztések figyelembe veszik-e), ha nem, a biztonság vagy a használhatóság kerül-e előtérbe. A vizsgálat

eredményei alapján sem a biztonság, sem a kényelem nem szenved csorbát, a kompromisszumkészség elengedhetetlen, de a legfontosabb szempont valamennyi eszköz esetében a biztonság. Az egyéni igények figyelembevétele nem teljes, adott esetben sok a különbség a tűzoltók testfelépítése között. Ennek ellenére az eszközök használata egyértelműen a balesetek számának csökkenését eredményezte az elmúlt években, a fejlesztések során törekednek arra is, hogy használhatók is legyenek az eszközök (hiszen a használat jelentős többletkockázatot jelent, amennyiben nem megfelelő, megnövelve a súlyos sérülés esélyét). A tűzoltók összességében elégedettek az eszközök védelmi szintjével, valamint a komfortfokozatával.

Eszközönként vannak tulajdonságok, amelyek megosztják a használóikat, ezek jellemzően az egyéni tulajdonságok lekövetéséhez kapcsolódnak, a védelem magas fokú. Azt azonban nem szabad figyelmen kívül hagyni, hogy az egyes eszközök attól függően biztonságosak és kényelmesek, hogy mely gyártó forgalmazza őket. A hivatásos tűzoltó-parancsnokságok központi eszközbeszerzése kevésbé teszi lehetővé a drágább eszközök használatát, az önkénteseknek pedig végesek az anyagi erőforrásaik (habár megfelelő támogatói háttér esetén ez megoldott).

A korábbi kutatások hangsúlya jellemzően az egyéni védőruházatok fejlesztésére helyeződött. A nemzetközi irodalom bővelkedik a vonatkozó tanulmányokban, a hazai hiányos, korlátozott ezen a területen. Son Su-Young tanulmánya az egyenruhák anyaga és a mozgásszabadságra, izomtevékenységre gyakorolt hatások közötti kapcsolatot vizsgálja. Eredményei abba az irányba mutatnak, hogy a rugalmas és kompressziós ruházat a szabványos egyenruhához képest kismértékben növeli a mozgásszabadságot. A tanulmány a védőruházatok szabására, ergonómiájára fókuszál.[2] Wu a polifenilén-szulfid szövet alkalmazhatóságát vizsgálta. Eredményei szerint az anyag sűrűsége pozitívan befolyásolja a ruházat mechanikai tulajdonságát, szakítószilárdsága jobb értékeket hoz. Az éles környezetben való tesztelés azonban ez idáig nem valósult meg.[3]

A hőstressz csökkentése a hatékony és biztonságos munkavégzés egyik elsődleges támogatója. Az erre irányuló kezdeményezések a ruha kényelmi szintjét csökkentik, a hosszú távú alkalmazhatóság szempontjából többletkockázatot jelentenek.[4] Ezzel a ruha okozta többletterheléssel (kialakítás, tömeg) a Bodnár–Bérczi szerzőpáros foglalkozott tanulmányában.[5]

A fejlesztési irányokat annak megfelelően kell kijelölni, hogy a környezeti tényezők hogyan, milyen mértékben változnak. A körülmények folyamatos és nagymértékű változása indukálja, hogy a védőruházatok légáteresztők, kopásállók, vízhatlanok, kényelmesek legyenek, ugyanakkor a tűz ellen maximális védelmet nyújtsanak. A dekontaminációs módszerek összehasonlításával vizsgálta Polanczyk és munkatársai az egyes védőruházatok biológiai szennyeződésekkel szembeni ellenállását, ezen ellenálló képesség szintjének növelési lehetőségeit.[6]

[2] Son 2019.
[3] Wu 2019.
[4] Urbán–Restás 2017.
[5] Bodnár–Bérczi 2018.
[6] Polanczyk 2020.

Jogszabályi háttér

Az egyéni védőeszközök vonatkozó jogszabályi rendelkezéseinek vizsgálata szintén elengedhetetlen, tekintetbe véve, hogy azok változása nagymértékben befolyásolja, befolyásolhatja a fejlesztés irányait és lehetőségeit. Az egyéni védőeszközök munkahelyen történő használatának minimális egészségi és biztonsági követelményeit a 65/1999. (XII. 22.) EüM rendelet határozza meg. A munkavégzés során fellépő veszélyeket a rendelet 1., a funkcionalitás alapján történő felosztást a 2. számú melléklet tartalmazza. A 4. § (1) bekezdés *c)* pontja határozza meg azokat a feltételeket, amelyek az egyéni védőeszközök ergonómiájára vonatkoznak. A rendeletet módosító 77/2003. (XII. 23.) ESzCsM rendelet a védelmi funkció teljesítése vonatkozásában határozza meg az előírásokat, de csak általánosságban. A munkavédelemről szóló 1993. évi XCIII. törvény 1. § (2) pontja értelmében minden Magyarországon tevékenységet végző munkavállalónak joga van az egészséget nem veszélyeztető, biztonságos munkavégzési körülményekhez. A tűzoltók által végzett tevékenységek kapcsán a hagyományos munkavédelmi előírások korlátozott mértékben érvényesíthetők az előre nem látható, sok esetben nem pontosan körülhatárolható veszélyek, a gyorsan, jelentősen változó munkakörülmények miatt. Emellett az extrém fizikai és mentális megterhelés szükségszerűen magával hozza a speciális szabályozást. A tűzoltóságról szóló 1996. évi XXXI. törvény szabályozza a munkavégzési feltételeket, kiemelve a biztonságot és a védelmet. Az egyéni védőeszközök és védőruházatok vonatkozásában azonban nem tartalmaz rendelkezést. Az Európai Parlament és a Tanács (EU) 2016/425 rendelete definiálja az egyéni védőeszközt mint fogalmat. A rendelet idesorolja azokat a rendszereket is, amelyek a védelmi funkció betöltéséhez szükségesek és elengedhetetlenek, illetve amelyek a rögzítésben játszanak szerepet. A Belügyminisztérium Országos Katasztrófavédelmi Főigazgatósága az irányítása alatt álló területi jogállású szervek és helyi szervezetek esetében a személyi állomány egyéni védőeszközzel történő ellátásáról szóló 34/2021. számú főigazgatói intézkedéssel rendelkezik az egyéni védőeszközök beszerzéséről, használatáról, cseréjéről és karbantartásáról is. A hazai szabályozás általános használati keretet ad az egyéni védőeszközöknek, a specifikumok belső munkahelyi szabályzókban vannak megadva. A nemzetközi gyakorlat fejlesztésekkel, ergonómiai szempontokkal is foglalkozik. A védőeszközök fejlesztése, fejleszthetősége a nemzetközi irodalomra alapozva vizsgálható részletesebben.

A személyvédelem mechanikai eszközeinek evolúciója

A tűzoltóságnál rendszeresített védőfelszerelések közül a „legkevesebb" probléma a sisakkal van a tapasztalatok és a korábbi vizsgálati eredmények alapján. Az, hogy hosszabb viselés után a nyak és a vállak nehezen múló fájdalmát okozzák, nem feltétlenül a sisaknak tulajdonítható hiba, illetve hiányosság. A beavatkozást végzők jelentős része idősödő, a kisebb megterhelést is nehezebben viselik. A minél magasabb szintű védelmi képesség elérése érdekében más, több anyag van a sisakban (régebben kissé könnyebbek voltak a sisakok, azonban védelmi képességük is alacsonyabb volt).

Az új sisakbevizsgálási követelményeknek való megfeleléshez elengedhetetlen a gyártók számára az anyagfelhasználás módosítása. A hozzáadott réteg nagyjából 40 dkg súlytöbbletet eredményez a sisakoknál, ez önmagában azonban nem jelentene komoly problémát. A tűzoltók azonban idősebbek, a csontszerkezetük a kisebb pluszterhelést is nehezebben viseli. Emellett hosszú viselés alatt a 40 dkg is sokat számít. Komoly hiányossága, hibája a sisaknak, hogy akadályozza a hallást. Gépkocsivezetőknél ez kiemelten fontos szempont. Így az ő sisakjukat rövidített sisakhéjjal szerelik. Kevésbé akadályozza a hallást, azonban ezeknek a sisakoknak a védelmi képessége is alacsonyabb ezáltal. Ütés ellen jól védenek a sisakok, de a fejet felülről érő, nagy erejű ütések a nyakcsigolyák és a váll sérülését eredményezhetik.

Az 1990-es évek közepén rendszeresített kiskőrösi tűzoltó-védősisaknak lehajtható arcvédője volt. A héj üvegszállal erősített, a bélés pedig bőrből volt. Lehajtható arcvédelemmel rendelkezett, a kialakítása azonban műszaki mentésnél például komoly problémát jelentett, túl magas volt, beakadhatott. Viszont teljes egészében védte az arcot. Napjainkban a rendszeresített védősisakok az evolúcióban eljutottak arra a szintre, hogy ezt kiküszöbölték, integrált arcvédelemmel rendelkeznek. Kompromisszumot kellett azonban kötni: az integrált arcvédelem nem képes a teljes arcot elfedni, de cserébe nem okoz gondot a túl magas kialakítás. Egy jó magasan záródó kabátnyak kialakítása azonban valamelyest tudja ezt orvosolni. A Rosenbauer-sisakokba felülre építettek lámpát. Ez hasznos funkció. A Dräger-sisakokra oldalra szerelhető, itt azonban problémát jelent, hogy a plusz 20–30 dkg súly hosszú viselésnél egy irányba húzza a fejet.

A kesztyűvel kapcsolatos visszajelzések alapján a legnagyobb probléma, hogy túl vastag. Az lenne az optimális, hogy vékonyak legyenek, ugyanakkor a megfelelő védelmet nyújtsák beavatkozáskor. Ez azonban így nem működőképes elképzelés, kompromisszumokat kell kötni. A kesztyűk nehezek és vastagok, de megfelelő mértékben védik a beavatkozást végzők kezét bevetés során az esetleges veszélyhelyzetekben. Kötési feladatokat nem lehet benne megfelelően végezni, de a veszélyes övezeten kívül le lehet venni és a kötési feladatokat el lehet látni. A kesztyűvel kapcsolatos legfőbb probléma azonban az, hogy vastag, sok rétegű, a tűzoltó keze nagyon hamar és nagyon könnyen beleizzad, levételnél a belső réteg kifordul. Újbóli felvételnél a kihúzódott belsejébe a tűzoltó nem tudja a kezét visszadugni. Finommotorikus mozgásra a kesztyű egyáltalán nem alkalmas. A kompatibilitással kapcsolatban is vannak problémák: az új légzőkészülék kijelzője a mellkason van, egyébként is bonyolult feladat megnézni, de az energiahatékonyság miatt a kijelző kikapcsol, kesztyűben nem lehet az egyébként is apró gombot megnyomni, ha a tűzoltó leveszi a kesztyűt, akkor a visszavétel lesz problémás.

A tűzoltóságnál rendszeresített védőeszközök a fejlesztések ellenére a védőruhák területén nagyon gyengén teljesítenek, ezek kapják a legrosszabb értékeléseket. Volt egy minőségi ugrás az 1990-es évek végén, 2000-es évek elején, a Sattler után jött a Bristol. Az jó váltásnak bizonyult. Volt benne térdprotektor, jó volt a védőruházat védelmi képessége, lámpát és rádiót is lehetett rátenni, az első generációs ruháknak derékrészen volt tűz és hideg elleni védelme, oldalzsebe, és nagyon meleg volt. A bélését nem lehetett kivenni. A közvélekedés és a rossz nyelvek szerint az itt rendszeresített verzió a téli öltözet volt, és volt egy nyári változata, az azonban nálunk nem került

forgalomba. A Vektor magyar gyártás volt, hasonló a Bristolhoz, de a védelmi képessége nem volt olyan jó, mint annak. 2015 körül az R13 jött.

Az első garnitúra nagyon nem volt jó. Nem volt mérethelyes, a kabát, a nadrág a magasabb tűzoltók esetében túlságosan rövid volt. A védőruha alá beizzadva a légzőkészülék pántja alatt bőrpírt okozott a belső réteg. A kabát akkor jó, ha viszonylag bő, de nem túlságosan. A nadrágban a legfontosabb a térdprotektor, a tűzoltó a legtöbbször kúszik-mászik, törmelékben, szúrós tárgyakon térdel. Elengedhetetlen a gumírozott alj, a zsebes kialakítás, az erős, könnyen állítható kantárrész. A csatrész gyakran eltörik, a patentok kikapcsolódnak. A kabáton a mérőműszerek elhelyezésére alkalmas részeket kellene kialakítani, fémből készült karikákat, karabinereket elhelyezni a különböző kesztyűkhöz, hogy az egyes speciális műveletekhez kéznél legyen a megfelelő. A kabát legyen megfelelő hosszúságú (nyújtózkodva a mászóövből ne csússzon ki), de ne túlságosan, mert akkor könnyen beakadhat, nehezíti a beavatkozást végző mozgását. A kabátnál előnyös, ha a nyakrész biztonságosan és gyorsan felhúzható, hogy az integrált arcvédelmet kiegészítse.

Korábban a HAIX-csizmákat nagyon szerették a beavatkozást végzők, de nagyon drágák voltak. A Rosenberg fejlesztett gyorsfűzős csizmákat, de ezeknek a védelmi képessége nem 100%. A boka védelme ugyanis nem feltétlenül biztosított, könnyen kifordul, ha a tűzoltó valamilyen gödörbe lép. A gyorsfűzőst ugyan gyorsan fel lehet venni, de a bokát egyáltalán nem tartja. A talpátszúrás elleni védelem, a lábfej, lábujjak védelme a legfontosabb. A védelemnek azonban ára van, hosszú idő után kényelmetlen és nehéz a viselése, nem úgy hajlik, mint egy hagyományos cipő.

A kompozit erősítésű anyagok megjelenése könnyebbé, felhasználóbaráttá tette a légzőkészülékeket. T idom segítségével két palack helyezhető egymás mellé. Az aktuális felhasználás számításával jelzi a hátralévő bevetési időt, monitorozhatóvá váltak az értékek, a kijelzőn pedig nyomon követhetők. A hordkeret, a tépőzár, a kialakított palackhely, a tömlőszelepnél elhelyezett gyorscsatlakozó mind a jól használhatóságot biztosítja. Már nem kell a szelepet csavargatni. A véletlen elzárodás elleni védelem is ki lett alakítva, ahogyan a palackszeleptörés esetén a biztonsági rendszer, amely biztosítja, hogy ne tudjon az 1800 l levegő kiáramolni, fokozott veszélynek kitéve a beavatkozást végző tűzoltót. Kezdetben egy palack 14,7 kg volt, a kompozit palackok –5 kg-ot jelentettek, ez óriási előrelépés volt. Derékra adták a terhelést, de nem lehetett az autóra málházni, mert nem fért el. A légzőkészülékek evolúciójához hozzátartoznak az integrált bodyguard rendszerek, amelyek a kulcs kivétele és 20 másodperc passzivitás után bejeleznek. Magyarországon volt rádiós (táblán látható volt, hogy a bevetést végző hogyan áll levegővel, probléma esetén lehetett neki jelezni, hogy jöjjön ki), de drága és emberigényes volt a működtetés. A légzőálarc az ergonómiai kialakítás miatt a kifújt levegő nagy részét membránokon keresztül kiáramoltatja a szabadba, minimális mennyiség reked meg a sisak holtterében, amit visszaszív a tűzoltó, ebben nagyon sokat fejlődtek. Az álarcba beépíthető beszédváltó, mikrofon, a sisakba beépített hangszóró (főként a gáztömör védőruha esetén) megkönnyíti a külvilággal való kommunikációt. A tüdőautomata, a mentőálarc egy mozdulattal csatlakoztatható, már nincs az álarcba beépítve, sokkal költséghatékonyabb.

A magyar fejlesztések védelmi képességüket tekintve nem hozzák a várt eredményeket, viszont arányaiban drágák.

A jelen eszközei

A védősisakok új generációja (Rosenbauer Heros Xtreme) teljes kivitelű sisakhéjjal készült, a szabványi előírásokon messze túlmutató védelmi képességgel. Javították a viselési komfortot azért, hogy a viselőre kisebb járulékos terhelést rójon. Ehhez nagymértékben hozzájárul az új fejlesztés, ami egy sportosan bionikus formájú, könnyebb sisakhéjban manifesztálódik. A védőkesztyűben kívülről is könnyen állítható fejszalag mellett magas hőnek ellenálló arcvédő, középen elhelyezhető integrált LED-sisaklámpa biztosítja a még nagyobb kényelmet. Javítottak a sisak súlypontján és egyensúlyán, így a beállítás lehetősége is bővült. Integrálható műszaki szemüvegek, arcvédők, integrált sisakélvédő, teljesen rugalmas külső légzőkészülék, álarcrögzítő adapter és integrált hőkamera társulhat opcionálisan a sisakhoz. A kihordási idő a korábbiakhoz hasonlóan 15 év, kétévente felülvizsgálandó.[7]

Modellfrissített kivitelben és ergonomikusabb szabásminta alapján készül a Bristol Ergotech Action bevetési védőruha a CH2 védőkabát és a TCH2 típusú védőnadrág új generációjaként. A rétegrenden és a felhasznált anyagokon nem változtattak, a Nomex Delta T külső szövet, a NomexViscose-Isomex aramid nemez kevert szálas hőszigetelés és a Gore-Tex Fireblocker nedvességzáró és egyben lélegző rétegrend megfelel az előírásoknak. A viselési komforton igyekeztek javítani a szabással, a módosított elhelyezésű és záródó zsebekkel, magasabb kopásálló térdvédő betétekkel. A fejlesztések a védőkabát váll- és hátrészét célozták elsősorban a nagyobb mozgásszabadság érdekében (a karok mozgatása és a légzőkészülék viselése közben). A védelmi képesség nem változott, magasan megfelel az elvárt követelményeknek.[8]

A legújabb generációjú védőkesztyű a tenyérrészre szilikon bevonatú kétrétegű Nomex/Kevlart kapott. A fejlesztés legfontosabb célja a jó tapintási képesség, a nagy dörzsállóság, a vágás, átszúrás és vegyi anyagok elleni magas szintű védelem volt, a nagyobb viselési komfort és a kisebb járulékos terhelés. Ehhez Nomex/Gore-Tex/X-Trafit vízzáró-légáteresztő rétegeket kombináltak. A belső rész kevlár a vágás és hő elleni maximális védelemért. A kézfej részén mechanikai sérülés ellen védő protektor van. A jobb észlelhetőségért 3M Scotchlite fényvisszaverő csíkokat applikáltak a kesztyűre. A folyamatos fejlesztés ellenére sem oldható az ellentmondás, a mechanikai sérülés, hő, folyadékok áthatolása elleni védelem szükségszerűvé teszi a rétegrend alkalmazását, a finommechanikai munkákra azonban emiatt nem alkalmas. A műszaki mentő kesztyű elvileg képes a megfelelő tapintást biztosítani, a kézügyességet minimális szinten korlátozni, 5-ös besorolású a teljesítménye a vágás elleni védelem és a tapintás érzete tekintetében.

A Rosenbauer Österreich Neo tűzoltó védőcsizma legújabb fejlesztése a nitril-légpárnás talp, a speciális sarok és lábfej feletti hajlítási zónák, a nagy méretű fülek a jobb felhúzhatóság érdekében, a csizma súlyának csökkentése, valamint a Sympatex membrán a testnedv elvezetéséért.[9]

[7] Tulok 2016.
[8] Tulok 2016.
[9] Tulok 2016.

Az alkalmazott anyagok evolúciója

Az egyéni védőeszközök gyártása során alkalmazott anyagok evolúciós folyamata elválaszthatatlan az eszközök evolúciójától (hiszen az adott eszköz azért tudott könnyebb vagy ellenállóbb lenni, mert másfajta, korszerűbb, jobb, könnyebb stb. anyagokat fejlesztettek ki). Az anyagokkal kapcsolatos fejlesztések az eszközök fejlesztési irányát figyelembe véve szintén a feladat jellegéhez, a védendő kockázathoz igazodnak. A modern kor kihívásaihoz alkalmazkodó anyagok kiválasztásának elsődleges szempontja a maximális védelmi szint elérése. A folyamat elején az egyéni védőeszközök anyaga elsősorban a könnyen, nagy mennyiségben elérhető természetes bőr, gyapjú és pamut volt. A hőállóság és a vízállóság korlátozottan volt biztosított. A 20. század közepére érte el a fejlődés azt a szintet, hogy ezeket az anyagokat vegyileg kezelték annak érdekében, hogy növeljék a lángállóságot. A bevonat vagy a vegyi kezelés hatására azonban az eszköz nehéz vagy merev lett (például ruházat), jelentős mértékben korlátozta a mozgást. A modern kor hozta magával a Nomex, Kevlar, PBI (polibenzimidazol) és egyéb szintetikus szálak alkalmazását. Ezek az anyagok jóval nagyobb mozgásszabadságot biztosítanak, a korábbi eszközökhöz képest sokkal könnyebbek, rugalmasak, és az extrém hőhatásnak is ellenállnak. A többrétegű szerkezetnek köszönhetően három szinten is képes a ruházat megvédeni viselőjét: külsőleg hő és/vagy mechanikai behatás elleni védelem, a középső réteg nedvességzáró membrán, a belső pedig egy komfortréteg.

Napjaink legjellemzőbb alapanyagait az 1. táblázatban foglaltuk össze.

1. táblázat: Az egyéni védőeszközök anyaga

Anyag	**Felhasználási terület**
Fémek: alumínium, acél, titán	Lábvédelem – acélbetétes bakancsok, fejvédelem, egyes védőruházatok
Műanyagok: PVC, poliuretán, polipropilén	Védőszemüvegek, kesztyűk, védőruhák
Textilanyagok: pamut, poliészter, nylon, kevlár	Védőruházatok, kesztyűk, lábbelik, egyéb textilszármazékok
Gumi: különböző gumikeverékek	Kesztyűk, csizmák, légzésvédők
Kompozit anyagok: szénszál, üvegszál	Speciális sisakok, védőruházatok
Bőr	Védőkesztyűk, lábbelik, hegesztőruhák

Forrás: a szerző szerkesztése

Fejlesztési lehetőségek, javasolt irányok

A hatékonyság növelése, valamint a minél magasabb védelmi szint elérése érdekében a tűzoltók egyéni védőeszközei folyamatosan fejlesztendők. A lehetséges fejlesztési irányok több szempont alapján kijelölhetők. A védőeszközök evolúciója során a technikai fejlődés valamennyi mérföldköve jól detektálható. A fejlesztések a korábbi tapasztalatok és a témában végzett vizsgálat alapján az alábbiak szerint megvalósítandók:

- anyagtechnológia (hő- és lángálló anyagok; lélegző anyagok [a hőstressz elkerülése érdekében, nedvesség elvezetése, magasabb fokú kényelem]);
- beépített technológiák:
  - okoseszközök: védőruhába integrált érzékelők, amelyek valós idejű adatokat szolgáltatnak a tűzoltók állapotáról, például hőmérséklet, oxigénszint és szívritmus – valós idejű monitoring;
  - kommunikációs rendszerek: a sisakokba vagy védőmaszkokba beépített kommunikációs technológiák, amelyek lehetővé teszik a csapattagok közötti zökkenőmentes kapcsolattartást, még zajos környezetben is;
- ergonómiai fejlesztések:
  - könnyebb és kényelmesebb viselet (súlycsökkentés, ergonomikus viselet);
  - személyreszabhatóság;
- tartósság és karbantarthatóság:
  - hosszabb élettartam;
  - könnyebb tisztítás;
- víz- és szennyezésállóság;
- jobb láthatóság (reflektáló anyagok).

A tűzoltóság alapvető feladata a tűzoltás, a műszaki mentés és a tűzmegelőzés. A folyamatos fejlődés azonban azt eredményezi (lásd korábban), hogy a veszélyeztető tényezők köre bővülni, súlyosságuk nőni fog. A tevékenységekből az emberi tényező nem kivonható. Így a változásokkal együtt még fokozottabb figyelmet kell fordítani a védelemre. A változások leginkább gazdasági, technikai és technológiai jellegűek, ugyanakkor a környezet okozta vészhelyzeteknek is a köztudatban kell maradniuk.

Az iparosodás a számos pozitív hozadék mellett olyan anyagok és technológiák alkalmazását is jelenti, amelyek nem optimális esetben komoly veszélyforrások lehetnek. Ugyanakkor a technológia olyan módszerek kidolgozását, eszközök kifejlesztését is lehetővé teszi, amelyek a feladatokat ellátók védelmi szintjét képesek növelni, valamint maga a feladatellátás is jóval hatékonyabb lehet. A tűzoltóság egyik kiemelt fejlesztési iránya a személyi védelem megoldásainak változtatása.

A tűzoltóság tevékenysége során az emberi élet védelme elsődleges, függetlenül attól, hogy milyen irányú és mértékű a gazdasági, technológiai, technikai fejlődés. A mentendő és a mentést végrehajtó védelme egyaránt fontos, de az egyéni védőeszközök fejlesztése nagyobb arányban a mentést végrehajtók esetében jellemző. A fejlesztési lehetőségeknek abba az irányba kell mutatniuk, hogy

- maximális legyen a védelmi képesség;
- a ruházat csökkenjen a lehető legnagyobb mértékben úgy, hogy a védelmi képesség maximális maradjon;
- a viselhetőség és a komfortosság növelése az egyéni igények és szükségletek figyelembevételével történjen.

Mindezek mellett a jövő védőruházata már olyan anyagok megjelenését feltételezi, amelyek különböző szenzorok segítségével a beavatkozási környezet állapotának változásait is nyomon tudják követni, képesek akár a tűzoltó vitális funkcióit is figyelemmel kísérni, a beavatkozást végzőt érő káros hatások mértékét elemezni, majd

egyértelmű jelzést adni arra vonatkozóan, hogy képes-e a tűzoltó biztonságosan befejezni az adott feladatot, vagy vissza kell vonulnia. A sisakba beépíthető egy hőkamera is a rádió mellé.[10]

Nanotechnológia – a fejlesztések jövője

A fejlesztések során az elsődleges szempont a szabványoknak és az igényeknek megfelelő védelmi szint elérése, megtartása, növelése (amely igényt a megnövekedő, fokozatosan változó kockázatok, a veszélyes anyagok körének bővülése, a megnövekedett biológiai veszélyek hívták életre). A védelem azonban nem mehet teljes mértékben a viselhetőség, a kényelem, az ergonómia és a használhatóság rovására. Mindezek mellett a hosszabb élettartam is elérendő cél (fenntarthatóság, költséghatékonyság). Az új funkciók létjogosultságát szintén a megnövekedett igények adják: szenzorok és egyéb intelligens megoldások beépítésével, alkalmazásával új lehetőségek nyílnak meg a beavatkozást végzők védelmének maximalizálása érdekében.

A tűzoltó-védőfelszerelésekben több területen alkalmazható a nanotechnológia: hővédelem, víz-, olaj-, vegyszertaszítás, baktericid és vírusellenes tulajdonságok, erősítés, szenzorok. A számos nanorészecske-típus más-más tulajdonságokkal rendelkezik. Alkalmazhatóság és funkcionalitás alapján a 2. táblázatban bemutatott tulajdonságokkal rendelkező nanorészecskék kerülnek a figyelem középpontjába a tűzoltó az egyéni védőeszközök tekintetében.

2. táblázat: Nanorészecskék – védőfelszerelésekben való alkalmazás az egyes tulajdonságok alapján

Nanorészecske	**Tulajdonságok**	**Alkalmazás a védőfelszerelésben**
Grafén	Kiváló hővezető képesség, nagy szilárdság	Hővédelem, erősítés
Szilícium-karbid	Kiváló hőállóság, kopásállóság	Hővédelem, súrlódás-csökkentés
Bórax	Hőálló, olvadáspontja magas	Hővédelem, tűzállóság
Fluorpolimerek	Víz- és olajtaszítás	Védőruházat bevonata
Szilícium-dioxid	Víz- és olajtaszítás, átlátszóság	Sisakok, védőszemüveg bevonata
Ezüst	Baktericid, vírusellenes	Védőruházat bevonata
Réz	Baktericid, vírusellenes	Védőruházat bevonata
Titán-dioxid	Baktericid, vírusellenes, öntisztuló	Védőruházat bevonata
Szénszálas nanocsövek	Nagy szilárdság, könnyű súly	Erősítés, szenzorok

Forrás: a szerző szerkesztése Lázár 2025; Kutasi 2020a, 2020b, 2021, 2022 alapján

[10] Fülep 2020.

A beavatkozást végzők védőruhája esetében a legfontosabb szempont a hővédelem és a mechanikai védelem. Ez azonban sok esetben a viselhetőség és a jól használhatóság rovására megy. A különböző nanoszálak alkalmazásával ez az ellentmondás feloldható. A nanoszálak az emberi hajszálnál kétszázszor vékonyabbak. Folyékony polimerből állítják elő elektromos szálképzéssel. A folyamat végeredménye 500 nm-nél kisebb szál, amely nemszőtt jellegű szálrendszerben nagy fajlagos felülettel és kis pórusmérettel rendelkezik; az így keletkező anyagot nagy porozitás jellemzi. A textilanyagokra a védelmi képesség elérésére vagy növelésére funkciós anyagot juttatnak telítéssel vagy kenéssel. Az önfelépülő réteg(ek) nagyon vékony felületet képez(nek) a textilanyagon (1 nm-nél vékonyabb). A réteg kialakítása előtt a bevonandó anyagot töltéssel látják el (például a pamutszálat kationizálják, pozitívvá töltik), majd negatív töltésű ionokat tartalmazó polimerrel látják el nanotechnológia segítségével. Lehetőség van olyan réteg kialakítására a textileken, amely képes önmagát kijavítani, vagyis a bevonat hiányosságait pótolni. Speciális képességű réteg emellett a szálak felületén lévő saját részecskék célirányos nanotechnológiai rendezésével is létrehozható. A 10–30 nm-es réteg a tömbanyaghoz képest eltérő tulajdonságokkal rendelkezik.[11] A nanoszálakból elektromos eljárással képzett nemszőtt kelmék a baktériumok és vírusok áthaladását is képesek megakadályozni, így az ilyen jellegű kockázatok csökkentésében is jelentős szerep jut a nanoszálaknak.

A vegyi szálak vastagságának radikális csökkentése különleges tulajdonságokat kölcsönöz az anyagnak: rendkívüli szilárdsági jellemzők, nagy fokú vékonyság (áttetsző), nanométeres méretű üregecskék, pórusok, amelyek a vízmolekulákat és a levegőrészecskéket átengedik, a mikroorganizmusokat zömében nem.[12] A molekulaszerkezetükben módosított szálasanyagok és speciális, összetett kelmeszerkezetek hatékonyan elvezetik a test felszínéről a nedvességet, elpárologtatják azt (a tűzoltó esetében a védőruha alá jutott víz/verejték hő hatására nem okoz bőrsérülést), kopásállók, és az ibolyántúli sugárzásnak is ellenállnak.[13]

Fém-oxidok, korom, agyag alkalmazása nem ismeretlen a textilipar számára, a nanoméret azonban viszonylag új keletű. A poliészter, poliamid, poliolefinek bevitelével (mesterséges) szálakba az anyag elektromos vezetőképessége is javítható. Az acélhoz képest 15-szörös szilárdságú, egyhatod tömegű szén nanocsövek kiváló elektromos vezetők. Energiatároló, energiaátalakító berendezések előállítására is rendkívül alkalmasak. A szén nanocsövek különböző anyagokkal való kombinálása más-más különleges tulajdonság létrejöttét teszi lehetővé:

- polivinil-alkohol szállal merev, a hasonló dimenziójú acélhuzalnál hússzor szívósabb állítható elő;
- aromás poliamid szálakkal védőmellények, biztonsági hevederek, robbanásálló ponyvák készíthetők.

Agyag nanorészecskével növelhető az anyag elektromos vezetőképessége, a vegyszerállóság, égésgátlás biztosítható. A leglényegesebb és a tűzoltók szempontjából

[11] Kutasi 2021.
[12] Kutasi 2020b.
[13] Máthé–Orbán–Lázár 2015.

legrelevánsabb tulajdonság azonban az, hogy piezokerámia-részecskék felhordásakor az anyagot érő mechanikai jelet a ruha elektromos jellé alakíthatja. Ezzel a módszerrel a testen hordott ruházat közvetítésével monitorozhatók a beavatkozást végzők vitális funkciói.

A fejlesztéssel kapcsolatos nehézségek

Az okostechnológiával ellátott védőruhák kapcsán a fentiek mellett szükséges a működési akadályokat is áttekinteni a teljesség igénye nélkül: hőmérsékleti működési tartományok, elektromos eszközök hűtése, akkumulátorokból eredő egyéb kockázatok. A védőruházatokba beépített rendszereknek a tűzoltói terhelésnek megfelelően kell működniük (–20 °C és +60 °C közötti, de akár +70 °C fölötti hőmérsékleti tartományban). Az aktív elemek és szenzorok extrém nagy hőingadozásnak, hőmérséklet-robbanásnak kell hogy ellenálljanak, miközben a védelmet nem korlátozzák. A felhasznált anyagoknak külön-külön és együttesen is hatásosnak kell maradniuk, ugyanakkor figyelembe kell venni azokat a körülményeket is, amelyekben az egyes rendszerek robbanásbiztos közegben is biztonságosan működnek. A működőképesség érdekében célszerű az aktív hűtési modulok kialakítása, hogy az egyes részegységek túlmelegedését megakadályozzák. Az egyes részrendszerek egységbe rendezése, a fenti működési feltételek teljesíthetősége jelentős mértékben korlátozza az anyagfelhasználást. Az elektromos rendszerek (beépített érzékelők, kommunikációs modulok, AR-kijelzők vagy energiaellátó egységek) nagy energiát és hőt termelhetnek (noha épp a hőterhelés csökkentése az elsődleges cél a tűzoltók egyéni védőeszközei esetében), így passzív hűtést kell alkalmazni anélkül, hogy többletterhelést (extra réteget a ruházatban, merevebb anyagot, amely a mozgást akadályozza, korlátozza) okozna. Az aktív hűtés kizárólag akkor alkalmazható, ha a súlya és a kialakítása nem jelent nagyobb kockázatot, a viselhetőséget nem akadályozza, illetve nem csökkenti a védelmi szintet minimális mértékben sem. Hangsúlyos szerepe van az energiaellátás és a hűtés elválasztásának, hogy a hőterhelésnek esetlegesen kevésbé ellenálló részek a működésbiztonságot ne korlátozzák (redundáns tápellátás, vészhelyzeti kikapcsolási lehetőségek). Figyelembe kell venni a tűzoltók egyes körülményekre adott reakcióit, és gondoskodni arról, hogy a hűtés ne rontsa a mozgási rugalmasságot, ne legyen zavaró a beavatkozás során, ne csökkentse a láthatóságot és/vagy a kommunikációt.

Az akkumulátorok számos kockázatot hordoznak magukban:

- termikus futás;
- túlhevülés, amely könnyen átterjed a viselőre;
- nedves környezetben áramütés veszélye;
- elektromágneses interferencia és zavaró hatások a kommunikációs és szenzorrendszereknél. Ennek megelőzésére javasolt megoldások:
  - cella- és modulszintű monitoring: hőmérséklet, áram, feszültség valós idejű figyelése és automatikus lekapcsolás szükség esetén;
  - hő- és mechanikai védelem a tárolócsatlakozásoknál, tűzálló csatlakozók használata;

– érintésvédelmi és szigetelési normák betartása, valamint kompatibilitás a tűzoltó eszközökkel (hűtésálló huzalozás, nem gyúlékony anyagok);
– redundancia és gyorsan cserélhető modulok a szolgáltatásokban verhetetlen üzemidő biztosítására;
– egyszerű, érintésbarát kezelőfelületek és vészhelyzeti kikapcsolási lehetőségek.

Biztosítani kell a valós idejű interakciót a felhasználóval: a védőruhát és az eszközöket úgy kell kialakítani, hogy ne csökkenjen a helyzetfelismerés lehetősége, a döntéshozatal sebessége, ne zavarja a feladatvégzést:

- a vizuális és akusztikus visszajelzések legyenek érthetők és könnyen értelmezhetők zajos környezetben is;
- hozzáférés a létfontosságú adatokhoz (állapot, időzített funkciók, külső környezeti adatok), legyen gyors és megbízható;
- robusztus, könnyen tisztítható és impregnált felületek, amelyek ellenállnak a sűrű kátránynak, a koromnak és a nedvességnek;
- a karbantartási és ellenőrzési folyamatok egyszerűsítése: moduláris komponensek, gyors cserélhetőség, önellenőrző funkciók.

Tesztelés és megfelelőség: a darabokkal végzett teszteknek a valós körülményeket kell modellezniük:

- melegebb és hidegebb környezetben, poros és vizes körülmények között is működőképesnek kell lennie;
- tűzvédelmi és villamosbiztonsági előírások (például EN, NFPA, CE/DOT vagy helyi előírások) teljesítése;
- kompatibilitás a meglévő egyéni védőeszközökkel és a tűzoltó-bevetési-protokollokkal;
- felhasználó bevonása a tervezés korai fázisában.

Összegzés

A katasztrófavédelem beavatkozást végző munkavállalói számára különösen fontos az egyéni védőeszközök folyamatos fejlesztése. A technológia fejlődése, a körülmények folyamatos, nagymértékű, dinamikus változása szükségessé teszi a gyors alkalmazkodás képességét a használt eszközök terén is. A védelmi képesség elérése, megtartása, növelése sok esetben csak a használhatóság kárára tud megvalósulni, de mindenképpen kompromisszumot kell kötni a praktikum, a kényelem, a használhatóság és a maximális védelmi szint elérése érdekében. Korábbi vizsgálatok eredményei abba az irányba mutatnak, hogy a fejlődés útja egyértelműen ki van jelölve, de az igazán forradalmi megoldások a nanotechnológiához köthetők: lehetőséget kínál az anyagok hővédelmének növelésére, a különböző szenzorok beépítésére, különleges tulajdonságokkal „ruházza fel" az eszközöket. A cél olyan eszközök kifejlesztése lehet, amelyek a légzsákhoz hasonlóan „robbannak" a tűzoltó testére azokban az esetekben, amikor például szúróláng veszélyezteti a biztonságát: nanoanyag vagy nanoérzékelő segítségével közvetlen információátvitel történik. A tűzoltók egyéni védőeszközeinek

jövőképe ultrakönnyű anyagokat, érzékelőkkel ellátott ruházatot vízionál, amely a veszélyes helyzetek bekövetkezésének pillanatában képes a viselőt mindenre kiterjedő védelemmel ellátni.

A főbb következtetések a kutatás vonatkozó szakasza alapján: a védőeszközök teljesítménye dinamikusan változik a fejlesztések hatására; a „nagyobb védelem" feltétele a kényelem és a használhatóság kompromisszuma. A sisakok és védősisakok esetében a fejlesztések célja a redukált súly, a javított komfort, a jobb hallás- és látásbiztonság, valamint integrált kommunikációs lehetőségek. A védőruha anyagválasztásában a hő- és lángállóság mellett kiemelten fontos a rostok összetételéből adódó rugalmasság, a vízelvezetés és lélegzőkészség. A nanotechnológia alkalmazása lehetővé teszi a fejlettebb hővédelmet, a vízállóságot, valamint a baktérium- és vírusellenállást, miközben a technikai feldolgozásokat és költségeket figyelembe véve a használhatóság is javulhat. A fejlesztések során a védelmi szint és a használhatóság közötti kompromisszumok kiegyensúlyozása kulcsfontosságú; az olyan integrált megoldások, mint érzékelők és intelligens anyagok alkalmazása, segíthetik a valós idejű állapotkövetést és a gyors reakciót.

A gyakorlati használhatóságot az adja, hogy a vizsgált eszközök fejlesztése közvetlenül növeli a mentális és fizikai kockázatkezelés hatékonyságát a katasztrófavédelem és az ipari mentés területén, az intelligens rendszerek (érzékelők, LED-jelzések, kommunikációs csatornák) segítenek a csapatok közötti koordinációban és a sérült eszközök időben történő cseréjében, az anyag- és technológiai fejlesztések révén hosszabb élettartam, egyszerűbb karbantartás és költséghatékonyabb üzemeltetés érhető el. A jövőbeli kutatási irányok ennek megfelelően határozhatók meg:

- Nagyobb rugalmasság, hő- és ötvözeti ellenállás együttes megvalósítása különböző környezetekben (kemény fizikai munka, kültéri, extrém hőmérséklet).
- Nanotechnológiai anyagok hosszú távú viselhetőségének és a karbantartási költséghatékonyság részletes vizsgálata.
- Valós idejű monitoringrendszerek integrálása a védőruházatba (hőmérséklet, CO_2-szint, nyomás, mozgás érzékelése).
- Költséghatékonysági elemzések és szabványkövetelmények összehangolása a gyorsan fejlődő anyag- és technológiai területeken.
- Kiegészítő kockázat- és használhatósági vizsgálatok különböző munkavédelmi környezetekben.

Felhasznált irodalom

Bodnár László – Bérczi László (2018): Beavatkozói biztonság vizsgálata a nagy kiterjedésű erdőtüzek kapcsán. *Műszaki Katonai Közlöny,* 18(4), 102–110. Online: https://folyoirat.ludovika.hu/index.php/mkk/article/view/1521/840

Fülep Zoltán (2020): Elképzelés a jövő tűzoltóságáról a várható társadalmi és technikai változások szellemében. *Belügyi Szemle,* 68(8), 85–91. Online: https://doi.org/10.38146/BSZ.2020.8.5

Horváth Lilla (2025): *A tűzoltó egyéni védőeszközök szerepének, hatékonyságának, valamint védelmi-, és egyéb képességeinek növelésére elérhető aktuális lehetőségek kutatása.* PhD-értekezés-tervezet. Budapest: Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Katonai Műszaki Doktori Iskola. Online: https://kmdi.uni-nke.hu/document/kdmi-uni-nke-hu/Horv%C3%A1th%20Lilla%20Disszert%C3%A1ci%C3%B3%20tervezet%20250507.pdf

Kutasi Csaba (2020a): 60 éve kezdődött a nanokutatás, textilipari vonatkozások. *Kaleidoscope,* 10(21), 205–220. Online: https://doi.org/10.17107/KH.2020.21.205-220

Kutasi Csaba (2020b): A COVID-19 koronavírus elleni védelem textiles szemmel. *Magyar Kémikusok Lapja,* 75(5), 168–170.

Kutasi Csaba (2021): A nanokutatás textilipari alkalmazásai. *Magyar Kémikusok Lapja,* 76(2), 40–43. Online: https://doi.org/10.24364/MKL.2021.02

Kutasi Csaba (2022): Nemszőtt kelmék, mint arcvédő maszkok alapanyagai. *Magyar Textiltechnika,* 75(1), 9–13.

Lázár Károly (2025): A grafén alkalmazása textilruházatokban. *Magyar Textiltechnika,* 78(2), 33–35.

Máthé Csabáné – Orbán Istvánné – Lázár Károly (2015): Hírek a nagyvilágból. *Magyar Textiltechnika,* 67(1), 64–68.

Polanczyk, Andrzej et al. (2020): Analysis of the Effectiveness of Decontamination Fluids on the Level of Biological Contamination of Firefighter Suits. *International Journal of Environmental Research Public Health,* 17(8), 1–10. Online: https://doi.org/10.3390/ijerph17082815

Son, Su-Young (2019): Effect of Different Types of Firefighter Station Uniforms on Wearer Mobility Using Range of Motion and Electromyography Evidence. *Fashion & Textile Research Journal,* 21(2), 209–219. Online: https://doi.org/10.5805/SFTI.2019.21.2.209

Tulok Antal (2016): Korszerű egyéni védőeszközök és felszerelések. *Védelem Katasztrófavédelmi Szemle,* 16(5), 59–60.

Urbán, Anett – Restás, Ágoston (2017): Making Body Temperature Lower to Raise the Safety Level of Firefighter's Invention. *ECOTERRA: Journal of Environment Research and Protection,* 14(1), 47–51.

Wu, Chuansong (2019): Application of a New Firefighter Protective Clothing Material in Fire Rescue. *IOP Conference Series: Materials Science and Engineering,* 612(3), 1–5. Online: https://doi.org/10.1088/1757-899X/612/3/032009

Jogi források

1993. évi XCIII. törvény a munkavédelemről

1996. évi XXXI. törvény a tűz elleni védekezésről, a műszaki mentésről és a tűzoltóságról

65/1999. (XII. 22.) EüM rendelet a munkavállalók munkahelyen történő egyéni védőeszköz használatának minimális biztonsági és egészségvédelmi követelményeiről

77/2003. (XII. 23.) ESzCsM rendelet a munkavállalók munkahelyen történő egyéni védőeszköz használatának minimális biztonsági és egészségvédelmi követelményeiről szóló 65/1999. (XII. 22.) EüM rendelet módosításáról

A személyi állomány egyéni védőeszközzel történő ellátásáról szóló 34/2021. számú főigazgatói intézkedés

Az Európai Parlament és a Tanács (EU) 2016/425 rendelete (2016. március 9.) az egyéni védőeszközökről és a 89/686/EGK tanácsi irányelv hatályon kívül helyezéséről (EGT-vonatkozású szöveg)

HADMÉRNÖK
VÉDELEMINFORMATIKA
20. évfolyam (2025) 2. szám 37–53.
DOI: 10.32567/hm.2025.2.3

Gombás-Kása Éva[1]

A szárazföldi tábori híradó és informatikai rendszerek fejlesztésének kérdései a Magyar Honvédségben

Issues of Developing Land-Based Field Communications and IT Systems in the Hungarian Defence Forces

Absztrakt

A haderő fejlesztése az utóbbi években nagy hangsúlyt kapott a Magyar Honvédségben, amit a változó biztonságpolitikai környezet (2014-ben a Krím félsziget annektálása, 2022-ben az orosz–ukrán háború kitörése) idézett elő. Az elavult, több évtizedes üzemidővel rendelkező technikai eszközök fenntartása a továbbiakban már nem volt sem hatékony, sem gazdaságos, ezek nem feleltek meg a kor színvonalának sem. Ez a tanulmány a 2016-ban elindított Zrínyi Honvédelmi és Haderőfejlesztési Programban érintett, a vezetés-irányítási rendszert támogató szárazföldi tábori híradó és informatikai rendszerek fejlesztését mutatja be az orosz–ukrán háború tapasztalatainak tükrében.

Kulcsszavak: haderőfejlesztés, orosz–ukrán háború tapasztalatai, tábori híradó és informatikai rendszer, hálózatalapú képesség, interoperabilitás

Abstract

The development of the armed forces has received a high priority within the Hungarian Defence Forces in recent years, which was indicated by the changing security policy environment (the annexation of the Crimean Peninsula in 2014, the outbreak of the Russian–Ukrainian

[1] Alezredes, vezető, Híradó, Informatikai és Információvédelmi Csoportfőnökség, Telepíthető Rendszerek és Spektrumgazdálkodási Főnökség.

war in 2022). Maintaining outdated technical equipment with decades of service life was no longer efficient or economical, and they did not meet modern operational standards. This study presents the development of land-based deployable communications and information systems supporting the command and control system, as part of the Zrínyi Defence and Force Development Programme launched in 2016, in the light of the lessons learned from the Russian–Ukrainian war.

Keywords: armed forces development, lessons learned from the Russian–Ukrainian war, deployable communications and information systems, network-enabled capability, interoperability

Bevezetés

A Zrínyi Honvédelmi és Haderőfejlesztési Program (HHP) 2016-ban indult, kezdetben tízéves periódust ölelt fel, azonban ma már látható, hogy a haderőfejlesztés egy olyan téma, amely soha nem kerülhet le a napirendről a technika gyors fejlődése, illetve a világban zajló biztonságpolitikai események miatt.[2] A haderőfejlesztési program célja a modern haderővel szemben támasztott követelményeknek megfelelően felzárkóztatni a Magyar Honvédséget (MH) szervezeti, technikai, illetve infrastrukturális téren is. A szinte minden fegyvernemet érintő fejlesztésekkel párhuzamosan megindult a magyar hadiipar feltámasztása is. Időközben 2022-ben a program felülvizsgálata során már az első ukrán tapasztalatok is belekerültek. Magyarország Nemzeti Katonai Stratégiájának[3] kiadása a NATO-elvárásokhoz igazodó haderőfejlesztési program további pontosítását és bővítését indukálta, amely dokumentum leszögezte, hogy ugyan Magyarország nem tekint egyetlen államot sem lehetséges szemben álló félnek, a nemzetnek fel kell készülnie azokra a kihívásokra, amelyek a gyorsan változó biztonsági környezet hatására jelentkeznek. Nemcsak az orosz–ukrán háború, hanem a közel-keleti és észak-afrikai instabil államok, a folyamatosan jelen lévő polgárháborúk is új fenyegetést jelenthetnek Európára és Magyarországra egyaránt. Az Egyesült Államok és Kína közötti feszültség miatt a NATO főerejét adó amerikai fegyveres erők figyelme és erőforrásai is egyre inkább az ázsiai térségre koncentrálódnak, aminek következtében szükségessé vált, hogy Európa országai, köztük Magyarország is, önálló védelmi képességeiket fejlesszék.

Az utóbbi években tehát új biztonság- és védelempolitikai dokumentumok jelentek meg, amelyeknek része volt a 2020-ban kiadott Nemzeti Biztonsági Stratégia,[4] illetve a Nemzeti Katonai Stratégia is.[5] A HHP szorosan illeszkedik az új stratégiában megfogalmazott alapelvekhez, ennek keretében előtérbe helyezi a megelőzést, az ellenálló képességet, illetve a gyors és határozott válaszadás képességét. Az ehhez szükséges képességek kialakítása mentén szerezzük be az új technikai eszközöket és alakítjuk át a Magyar Honvédséget, ami minden területet érint, a tartalékos rendszer

[2] Szűcs 2016.
[3] 1393/2021. (VI. 24.) Korm. határozat.
[4] 1163/2020. (IV. 21.) Korm. határozat.
[5] Kálmánfi 2017.

megreformálásán keresztül a kibervédelmi képességek kialakításáig, a szárazföldi és a légierő képességeit, az űrszektort, illetve a hadiipart.[6] A HHP a Magyar Honvédség képességei és kiképzettsége tekintetében olyan átalakítást irányoz elő, amely a régió meghatározó haderejévé teszi.[7]

Magyarország geostratégiai elhelyezkedéséből adódó sebezhetősége, valamint kisállami jellemzőiből fakadó korlátozott képességei miatt fontosak azok a szövetségesi rendszerek, amelyeknek az ország jelenleg is tagja. Katonai szempontból a legfontosabb a NATO, amelynek a stratégiai törekvéseit figyelembe véve lett kialakítva Magyarország Fegyveres Védelmi Terve is. Szövetségesi kötelezettségeinkből fakadóan a NATO közös haderejébe történő nemzeti felajánlások a garanciái a NATO reagálóképessége fenntarthatóságának. Az egyik ilyen felajánlás az MH (közepes) Lövészdandár, amely 2023-ban érte el – a vonatkozó nemzeti korlátozásokkal – a teljes készenlétét. Jelenleg folyamatban van ennek átalakítása nehézdandárrá, amely a teljes műveleti készenlétét 2028-ban éri el a tervek szerint. Ennek elengedhetetlen hozzávalói azok a képességek, amelyek az új technikai eszközök beszerzésével válnak teljessé, így elmondhatjuk, hogy a HHP keretében folyamatosan bővül a nehézdandár eszközparkja.[8]

Tanulmányom célja annak bemutatása, hogy az orosz–ukrán háború híradó és informatikai tapasztalatai miként hatottak a Magyar Honvédség szárazföldi, tábori infokommunikációs rendszereinek fejlesztésére. Ennek keretében külön figyelmet fordítok az interoperabilitás, a hálózatalapú műveleti képességek, valamint a digitális hadszíntérrel szembeni követelmények teljesülésére.

A kutatás során a következő kérdésekre keresem a választ: Milyen technikai és strukturális irányváltásokat eredményeztek a háborús tapasztalatok a HHP keretében? Hogyan érvényesülnek a NATO FMN (*Federated Mission Networking* – Szövetségi Műveleti Hálózat) követelményei a Magyar Honvédség híradó-informatikai rendszerében? Milyen típusú eszközök és megoldások járulnak hozzá a biztonságos, minősített adatátvitel biztosításához tábori környezetben?

Módszertani szempontból a tanulmány leíró és elemző jellegű, és alapvetően másodlagos forrásokra (szakirodalom, doktrínák, nemzetközi gyakorlatok, honvédelmi dokumentumok) épül. A kutatás nem tartalmaz empirikus adatgyűjtést, célja a rendelkezésre álló források alapján a szintetizálás és a következtetések levonása a Magyar Honvédség technikai fejlesztési irányairól.

A híradó és informatikai rendszerekkel szemben támasztott követelmények

A fejlesztések egyik területét jelentik a vezetés-irányítást (C2) támogató híradó és informatikai rendszerek. A Magyar Honvédség Összhaderőnemi Híradó és Informatikai Doktrínájában (Hír/4) foglaltak szerint a katonai vezetés alapvető eszköze a híradó és informatikai rendszer, amely biztosítja az alárendeltek vezetését, valamint azok

[6] Csiki Varga – Tálas 2020: 89–112.
[7] Elengedhetetlen a magyar haderő fejlesztése 2024.
[8] Bányász 2024.

irányításának, a feladatok meghatározásának, a szervezetek és személyek együttműködésének a technikai feltételeit. Ez a tevékenység a harci támogatás részét képezi, a katonai vezetés működőképességét tehát a híradó és informatikai támogatás biztosítja, amely egyben a csapatvezetés végrehajtásának nélkülözhetetlen eleme. Az információ és annak birtoklása napjainkban stratégiai fontosságú előnyt biztosít a hadszíntéren. Az információs fölény (előny) a vezetési fölény alapvető feltételeként a katonai műveletek eredményességét befolyásoló tényező. A megszerzett információ továbbítása, feldolgozása, tárolása, rendelkezésre bocsátása korszerű híradó és informatikai rendszerek alkalmazásával valósul meg.[9] Ezen rendszerek kialakításánál mindenkor érvényesülni kell a következő alapelveknek: rendelkezésre állás, megbízhatóság, szabványosság, kompatibilitás, interoperabilitás, felcserélhetőség, azonosság.

A fenti alapelvek érvényesüléséhez a kor színvonalának megfelelő távközlési és információtechnológia szükséges. Hiába állnak rendelkezésre a harc megvívásához szükséges modern harcjárművek, lövegek, harckocsik vagy felderítő rendszerek, ha a feltételek hiánya miatt a szükséges információ eljuttatása az alárendeltekhez nem lehetséges, illetve nincs olyan technikai háttér, amelynek segítségével az összegyűjtött információk kezelése megvalósulhat. Ebben az esetben az átfogó helyzetkép kialakítása sem kivitelezhető, amely a parancsnok döntéshozatalát segítené.

A műveletek híradó és informatikai támogatásánál figyelembe kell venni azt is, hogy a szervezeti hierarchia és az információ kezelésének szintjei nem mindig esnek egybe. A híradó és informatikai rendszereknek biztosítaniuk kell, hogy a különböző vezetési szintekhez tartozó információs rendszerek összekapcsolása megvalósuljon úgy, hogy a felhasználók a számukra szükséges információt jogosultságuknak megfelelően a rendszerből ki tudják nyerni azon az eszközön keresztül, amely a rendelkezésükre áll. Ezen szemlélet alapján alakult ki a NATO-ban a hálózat nyújtotta képesség (NATO Network-Enabled Capability, NNEC)[10] – magyar megfelelője a Hálózatalapú Műveleti Képesség (HAMK)[11] –, amelyhez elengedhetetlen a korszerű információs és kommunikációs technológia alkalmazása.[12]

Ezen alapelveknek megfelelően dolgozta ki a híradó és informatikai szakterület a HHP-programba a tábori szárazföldi híradó és informatikai rendszerek vonatkozásában a követelményeket, amelyek érintik a rádió-, a műholdas, a mikrohullámú, a troposzféra- és a vezetékes híradást, illetve a vezetési pontok kialakítását is. A biztosított C2-rendszereken keresztül ma már nemcsak nyílt, hanem minősített információ továbbítását is meg kell oldani tábori körülmények között is, ami rendkívül nagy kihívást jelent, elsősorban a biztonság kialakítása szempontjából. Erre is megoldást kellett

[9] Haig–Várhegyi 2005: 160–164.

[10] NNEC: Olyan hadműveleti koncepció, amely a korszerű információs és kommunikációs technológiák alkalmazásával biztosítja a különböző katonai szervezetek, szenzorok, vezetési pontok és fegyverrendszerek valós idejű, hálózatba szervezett együttműködését. Célja a helyzetismeret, a döntéshozatal és a műveleti hatékonyság fokozása az információ gyors megosztása és feldolgozása révén. A koncepció alapját a rendszerbe integrált, interoperábilis és biztonságos adatáramlás képezi, amely előnyt biztosít a hadszíntéren.

[11] HAMK: A Magyar Honvédség sajátosságaihoz, szervezeti felépítéséhez és műveleti követelményeihez igazítva alkalmazza az NNEC elveit. A HAMK célja a műveleti környezetben fellépő információs túlsúly biztosítása, a közös helyzetértékelés és a vezetési képességek javítása, valamint a különböző haderőnemek közötti hatékony együttműködés megteremtése.

[12] Hír/4 2013: 1–14.

találni a HHP keretében annak érdekében, hogy az elektronikus információvédelem, valamint az infokommunikációs rendszerek és az adatátvitel biztonsága megvalósuljon.

Másik fontos kérdés, amellyel a szövetségesi kötelezettségekből fakadóan mindenképpen foglalkoznunk kell, az interoperabilitás, amelynek során a híradó és informatikai rendszerek szükséges mértékű összekapcsolásának technikai, illetve műszaki feltételeit meg kell határozni. Ehhez közös, azonosan értelmezett elvek és eljárásrendek kialakítása szükséges.[13] A katonai híradó és informatikai rendszerek közötti együttműködés szintjeinek specifikációját NATO-szabványok, valamint az AJP-6 NATO-kiadvány tartalmazza. Összesen hat szintet azonosítanak, ahol a 6. szint szerinti követelmények teljesülésekor már a két rendszer úgy kapcsolódik össze, hogy az a felhasználó részére nem észrevehető, mivel a két rendszer teljesen nyitott egymás irányába, és nincsenek korlátozásai az információhoz férésnek. Ezzel szemben az 1. szinten a rendszerek egymás felé zártak, nincs fizikai kapcsolat a két rendszer között, az információcsere emberi beavatkozást igényel. A két véglet között helyezkedik el a többi szint. Mindenesetre az látható, hogy a 6. szint igényli a legtöbb forrást, előkészületet és feladatot, ezért a racionális keretek között tartás érdekében szükséges annak meghatározása, hogy melyik rendszernek milyen szinten kell kapcsolódnia egy másik rendszerhez a hatékony feladat-végrehajtás érdekében.[14]

A Magyar Honvédség 2016-ban csatlakozott az FMN-közösséghez, amely tulajdonképpen az egyes nemzetek által alkalmazott Összevont Műveleti Hálózatok „szabványaként" értelmezhető. Azok az infokommunikációs eszközrendszerek, amelyek képesek teljesíteni ezen szabványokat, illetve a szakállomány kiképzettsége eléri ezt a szintet, integrálhatók a NATO vezetés-irányítási struktúráját kiszolgáló technikai rendszerekbe, más technológiák és tudásszintek pedig nem. Az úgynevezett FMN Spiral specifikációban meghatározott követelmények kétévente frissülnek új verzióra.[15]

Az FMN nem egy állandó eszközparkot és egy szolgáltatáscsomagot jelent, azaz nem csak a megfelelő hardver beszerzése szükséges a képesség eléréséhez. Az FMN-készenlét (FMN Readiness) egy részletesen szabályozott validációs folyamat eredményeként érhető el, amelynek feltétele a validálásra tervezett szintű Spiral képességnek valamely többnemzeti interoperabilitási, úgynevezett FMN validációs gyakorlaton (FMN Readiness Certification Exercise) való tesztelése. A sikeres validációt követően adják ki az FMN Ready tanúsítványt.[16]

Az orosz–ukrán háború híradó-informatikai tapasztalatai

A híradó és informatikai rendszerek fejlesztésének kérdésénél nem hagyhatjuk figyelmen kívül a közelünkben zajló konfliktus, az orosz–ukrán háború tapasztalatait sem. A HHP 2022-es felülvizsgálata során ezek a tapasztalatok már beépültek, de érdemes továbbra is folyamatosan figyelemmel kísérni a technológiában, illetve az eljárásokban

[13] Munk 2024.
[14] Hír/4 2013: 31–40.
[15] NATO [é. n.].
[16] NATO Communications and Information Agency [é. n.].

bekövetkező innovációkat a minél hatékonyabb képességfejlesztési koncepció kialakítása érdekében.

Az orosz–ukrán háborúban a két fél más-más híradó struktúrát alkalmaz, ami fakad az eltérő technikai fejlettségből, illetve az eltérő stratégiai prioritásból is. Az orosz fél erősen centralizált rendszert valósított meg, ami kedvez a nagyobb katonai műveletek koordinálásának, de megnehezíti a gyors reagálást. Az ukrán fél az adatok valós idejű továbbításával, illetve a decentralizált struktúrából fakadóan gyors döntéshozatalt képes megvalósítani, amely hatékonyabb a kisebb, önálló műveletek végrehajtása során. Megállapítható továbbá, hogy az elektronikai hadviselési rendszerek, valamint a kiberképességek alkalmazása kulcsfontosságú elem a katonai műveleteknél mindkét fél részéről. Ukrajna rugalmasabb, innovatív eszközökkel válaszol az orosz műveletek során jelentkező kihívásokra. Jellemző, hogy a polgári életben alkalmazott technológiákat adaptálja a híradó és informatikai rendszerébe, amellyel adott esetben az oroszok infokommunikációs képességeit is képes túlszárnyalni.[17] A valós idejű adatátvitel, illetve a nagy sebességű kommunikáció elengedhetetlen feltétel a gyors, hatékony döntéshozatal, illetve a katonai műveletek végrehajtása szempontjából. Az orosz fél sok esetben elavultnak tekinthető rádiórendszerei nem biztosítják ezt a kritériumot. Az elektronikai hadviselés ellen alig védettek, kevésbé felelnek meg a kor színvonalának, illetve a titkosítási eljárások hiánya is problémát okoz. Az ukrán fél a nyugati támogatásból származó műholdas és dróntechnológiák felhasználásával képes a rádióhíradás lehallgatására, amellyel fontos információkhoz jut a tervezett tevékenységekről.[18]

Összességében az orosz rádiók a modern technológiákhoz képest elmaradottak, illetve a centralizált struktúra miatt a híradó és informatikai rendszereik sebezhetők, aminek következtében a csomóponti eszköz kiesése esetén az adat- és hangkapcsolat annak pótlásáig megbénulhat.[19] Az ukránok egyrészt a nyugati támogatásból származó, másrészt a polgári életben használt, a piacon könnyen és olcsón elérhető civil eszközöket is alkalmazzák, amelyek gyorsan telepíthetők, de kevésbé biztonságosak. A fejlett nyugati technikai eszközök felhasználásával titkosított rádiókommunikációt alkalmaznak, amely a zavarás és a lehallgatás ellen védettebb, ezáltal biztonságosabbnak tekinthető. Gyorsan áthelyezhető mobil rádióállomások alkalmazásával valósítják meg azt a rugalmasságot, amely lehetővé teszi a gyors reagálást. A civilek által kezelt polgári technológiák (amatőr rádiók, polgári szolgáltatók hálózati infrastruktúrája stb.) alkalmazása jól kiegészíti vagy pótolja a katonai híradó és informatikai rendszerek elemeit, amennyiben azok nem állnak rendelkezésre. Ezenkívül segítik a területvédelmi erők tevékenységét is, amelyek technikai eszközökkel történő ellátása jelentősen alulmarad a harcoló erőkével szemben. Általánosan megfigyelhető, hogy a rádiókommunikációban is egyre nagyobb hangsúlyt kap a hangalapú kommunikáció ellenében az adatalapú kommunikáció, amely egyre szélesebb körű informatikai megoldásokkal valósítható meg.[20]

A mikrohullámú technológiát mindkét fél alkalmazza, gyors és megbízható adatátvitelt tesz lehetővé közepes távolságon. Rácspontokba szervezve akár az egész műveleti terület lefedésére használható, könnyen telepíthető, illetve mobilállomások révén

[17] Savage 2023.
[18] Babu–Williams 2022.
[19] Marins 2023.
[20] Demarest 2022.

alkalmazása rugalmas. Az adatátviteli sávszélesség elegendő videó- és adatátvitelre is. Tábori mikrohullámú állomások esetén más technológiákkal (műholdas, illetve rádiófrekvenciás rendszerek) létrejövő integrációval a hatótávolság is tovább növelhető, valamint redundáns hálózatalapú kommunikáció kialakítása is megvalósítható. Megoldást jelenthet más hagyományos technológiák (például vezetékes rendszerek) kiváltására annak hiánya vagy sérülése esetén. Alkalmazásánál azonban figyelembe kell venni, hogy az elektromágneses zavarokra, illetve az ellenséges zavaró tevékenységre érzékeny, valamint az időjárás és a terep befolyásolja a teljesítményét.[21]

A Drone Relay alkalmazása újdonságként jelent meg a háborúban, ezáltal a drónba integrált mikrohullámú átviteli modulok segítségével a nehezen elérhető területeken is sikerült biztosítani az adatátvitelt.[22] Az orosz haderő ezzel ellentétben a hagyományos katonai kivitelű tábori mikrohullámú komplexumokat alkalmazza, amelyek a toronymagasság és az adóteljesítmény miatt már nagy távolságú kommunikációra és titkosított adatátvitelre képesek, azonban az elektronikai zavarásra érzékenyek, ami ellen a frekvenciaugratásos technológia alkalmazásával védekeznek. A mikrohullámú rendszerek esetében a jövőben a zavarás elleni védelem megoldása kulcsfontosságú kérdés, új üzemmódok és hullámformák fejlesztése, valamint a frekvenciaugratásos rendszerek tökéletesítése révén.

A műholdas technológiák szerepe is felértékelődött az elmúlt időszakban, ma már nélkülözhetetlenek a kommunikáció, a felderítés, valamint a precíziós fegyverek alkalmazása, a valós idejű helymeghatározás terén. Kiválóan alkalmazható a földi kommunikációs infrastruktúrák rombolása, sérülése esetén, illetve redundáns kapcsolatot biztosít a folyamatos és robusztus kommunikáció érdekében.[23]

Ukrán oldalon nagy áttörést jelentett, hogy az alacsony pályás műholdrendszer, a Starlink hozzáférhetővé vált a kommunikáció biztosítására olyan területeken, ahol más eszközökkel, illetve infrastruktúrával az nem volt szavatolt. A műholdas kommunikáció előnye a nagy sávszélesség, a kis idejű késleltetés, valamint az, hogy a végpontok közötti titkosítás miatt az elektronikus lehallgatásnak való kitettsége alacsony, illetve a decentralizált struktúrának köszönhetően nehezen zavarható. Jól alkalmazható a drónok vezetésére és adatainak továbbítására is.[24] Az orosz haderő a saját műholdas rendszerére támaszkodik mind a kommunikáció, mind a helymeghatározás, valamint a fegyverirányítás területén. Az orosz műholdak függetlenek a nyugati rendszerektől, azonban technikai állapotuk miatt kevésbé megbízhatók, illetve könnyebben zavarhatók. A saját műholdas rendszer mellett alkalmaznak kereskedelmi műholdakat, valamint rendelkezésre áll a Starlinkhez hasonló alacsony pályás műholdrendszer is, amely védett adat- és hangkapcsolatot biztosít.

Ukrán oldalról prioritás a műholdas rendszerek zavarásának megakadályozása titkosítási módszerek, illetve gyors áttelepítések alkalmazásával, valamint saját műholdképesség kifejlesztése a stratégiai függetlenség elérése céljából. Az orosz oldal a meglévő műholdas rendszerét igyekszik modernizálni új és technológiailag fejlettebb műholdak pályára állításával.

[21] Johnson 2024.
[22] Kushnikov 2022.
[23] Armada International 2024.
[24] Harper 2023.

A HHP híradó-informatikai tartalma

A HHP keretében kiemelt szerepet kapott a híradó és informatikai képességek korszerűsítése, különös tekintettel a digitális hadszíntér elvárásaira. A modern hadviselésben a valós idejű információáramlás, a vezetés-irányítás biztosítása, valamint az adatbiztonság és a hálózati védelem megteremtése elengedhetetlenné vált. A 2022-ben kirobbant orosz–ukrán háború tapasztalatai különösen rávilágítottak az infokommunikációs rendszerek szerepére és sebezhetőségére, ami hatással volt a magyar fejlesztési irányok kijelölésére is. Az alábbiakban a HHP híradó-informatikai komponenseinek főbb elemeit, fejlesztési célkitűzéseit és ezek műveleti jelentőségét ismertetem.

Műveleti Hálózati Készlet (MHK), a minősített műveleti informatikai hálózat alapja

Az orosz gyártmányú tábori híradóközpontokat 2008-ban a Rába H-18 alvázon lévő HIK/G híradó és informatikai komplexum váltotta fel, amelyből jelenleg csak kevés áll rendelkezésre a Magyar Honvédségben, így inkább átmeneti eszköznek tekinthető. Többségében technikailag az előző generációhoz tartozó informatikai hálózati eszközökkel felszerelt, amelyek a mai igényeknek már nem felelnek meg, beleértve az FMN-képességet is, amely a szövetségesi feladatok ellátása során már elengedhetetlen követelmény. Ez az eszköz a Magyar Honvédség stacioner hálózata nyílt szolgáltatásainak tábori körülmények közötti kiterjesztésére készült (a minősített képességnek csak a fizikai biztonsága és a passzív hálózata előkészített), így azonban a híradó és informatikai szolgáltatásokat csak nyílt hálózaton képes biztosítani.

Hasonló képességekkel rendelkezik a békefenntartó missziók kiszolgálását végző, konténeres kialakítású Békefenntartó Híradó és Informatikai Központ (BHIK). A HIK/G híradó és informatikai komplexum „kistestvére" a HIK/S modulkészlet, amely ládázott formában tartalmazza a szükséges szervereket, aktív eszközöket és kábeleket, illetve a munkaállomásokat.

2017-ben elkészült a prototípusa egy olyan hordozható minősített informatikai készletnek (*Top Secret Local Area Network Kit,* TLAN), amely „Titkos" szintű minősített hálózathoz csatlakoztatható, rendelkezik tempest képes aktív eszközökkel és minimális számú végberendezéssel, azonban a készlet bővíthető. A készlet akkreditáció után képes két minősített hálózathoz csatlakozni. Az eszközkészlet a CWIX-2019 gyakorlaton már bemutatkozott többnemzeti környezetben is. Az informatikai képességei alapján aktív eszközökkel kiegészítve az FMN Spiral 2 és részben Spiral 3 követelményeknek feleltethető meg. A CWIX-2023-as gyakorlaton FMN-környezetben validálták a HUNOPNET (*Hungarian Operation Network* – Nemzeti Műveleti Hálózat) rendszer hardverkörnyezeteként.

A képességfejlesztés folytatásaként megtervezték a műveleti hálózati készletcsaládot (a NATO-terminológiában a megnevezés lehet PoP – *Point of Presence* vagy DCIS – *Deployable Communications and Information System*), amely a HIK/G komplexumhoz hasonlóan alvázon helyezkedik el, de attól eltérően nem egy felépítmény belsejében telepített, hanem ládázott modulkészletekből áll, amelyek üzemeltetéséhez nem

szükséges azokat a gépjárműről letelepíteni. Az informatikai és távbeszélő-szolgáltatások biztosítása érdekében gyorsan telepíthető, komplex átviteli utat (műhold, LAN, optika) fogadni képes eszköz, amellyel minősített és nyílt hálózatok is kiszolgálhatók. Készletébe tartoznak a szerverek, a szükséges aktív eszközök, vezetékes anyagok, aggregátor, szünetmentes tápegységek, illetve a járműre épített VSAT[25] *(Very Small Aperture Terminal)* antenna, amely a gyors áttelepíthetőséget támogatja. Folyamatos üzemkészségének biztosításához a laktanyai „online" tárolás feltételeinek megteremtése szükséges, ennek során a szerverek, illetve a munkaállomások szoftverei folyamatosan frissülnek, ami jelentősen lerövidíti a rendszerek telepítéséhez szükséges időt. Az MHK különböző konfigurációkban tervezett a kiszolgálandó szervezet méretétől, a felhasználók, illetve a domainek számától függően.

Kétféle telepítési mód lehetséges. Az egyik változatban hosszabb idejű kiszolgálás esetén modulárisan, ládákból összeépíthető rendszerként a hordozó járműtől függetlenül épületben/konténerben vagy sátorban elhelyezve, onnan kiszolgálva a törzsmunkahelyeket. A másik változatban egy vagy több hordozó jármű speciális felépítményében, a kialakított rekeszekben helyezik el, és az előre kiépített kábelrendszerekkel kötik össze őket, ezzel biztosítva a gyors telepíthetőséget.

Hungarian Operation Network (HUNOPNET)

A HUNOPNET koncepció az MND-C (*Multinational Division Center* – Közép-európai Többnemzeti Hadosztály) szerepvállalással 2021-ben indult el. Ez az első olyan tábori (telepíthető) műveleti hálózat, amely minősített adat továbbítására alkalmas „NATO Secret" szintig.

Az eltelt időszakban a rendszer folyamatosan fejlődött, jelenleg egy NATO-alárendeltségben működő parancsnokság igényeinek megfelelően képes futtatni a törzsmunkához szükséges funkcionális szolgáltatásokat, illetve az automatizált vezetés-irányítási rendszert, a HUNTACCIS (*Hungarian Tactical Command and Control Information System* – MH Tábori Vezetés-Irányítási Rendszer) szoftverrendszert.

Az MND-C az alárendelt katonai szervezetei érdekében infokommunikációs képességgel rendelkező technikai csoportot fog működtetni, hogy a teljes interoperabilitás biztosítva legyen. Ez a kidolgozott koncepció a HUNOPNET Digital Liaison Team (Digitális Összekötő Csoport), amelyet a hadműveleti területen bevált amerikai mintára alkottak meg. A csoportszintű képesség rendelkezik a minősített informatikai rendszer telepítésének képességével a hozzá tartozó műholdas átviteli út biztosítását is beleértve. Ennek a képességcsomagnak a beszerzése a közeljövőben várható.

A rádiókommunikáció

A rádiókommunikáció a harcászati szint alapvető és elsődleges vezetési eszköze az alegységek közötti gyors és megbízható információcsere érdekében. A Magyar

[25] VSAT: műholdas szolgáltatás igénybevételéhez szükséges eszköz.

Honvédség a régi típusú orosz rádiókat 2008–2014 között cserélte le a Kongsberg MRR (*Multi Role Radio* – többcélú rádió) rádiócsalád kézi, hordozható és járműbe épített rádióira, valamint a HARRIS típuscsaládból is vásárolt eszközöket, aminek célja az interoperabilitás biztosítása volt. Ezen eszközök még elsődlegesen a hangalapú kommunikációra alkalmasak, habár az adattovábbítás is lehetséges, azonban az jellemzően csak másodlagos funkcióként jelenik meg. Nagy mennyiségű és méretű adatok átvitelére ezek nem használhatók hatékonyan.

Már ez a váltás is nagy előrelépést jelentett a magyar katonai rádióhíradás történetében, azonban a jelenlegi HHP keretében beszerzett rádiók olyan technológiai és üzemeltetésbeli különbséget jelentenek, amelyhez elengedhetetlen a jól felkészült, magas szakmai ismeretekkel rendelkező szakállomány megléte. Az új technikai eszközökbe (Leopard 2A7 HU harckocsi, PzH 2000 HU önjáró löveg, Lynx páncélozott gyalogsági harcjármű, Gidrán páncélozott harcjármű) már az Elbit Systems Deutschland GmbH & Co. E-Lynx harcászati rádiócsalád rövidhullámú és ultrarövid-hullámú rádióit szerelik be. Ezek az eszközök Internet Protocol (IP) alapú, hálózatcentrikus, szoftvervezérelt rádiók, széles sávú adatátviteli képességgel. Az Elbit saját fejlesztésű digitális üzemmódjai képesek hang, adat és BFT- (*Blue Force Tracking* – saját erők követése) jelek párhuzamos, egyidejű továbbítására. Az átvitt adatok titkosítását az AES-256 szimmetrikus kulcsú titkosítás látja el.

A rádiócsaládból a HF,[26] a VHF[27]/UHF[28] és az L[29] frekvenciatartományban működő rádiókat szerezték be. A Magyar Honvédség E-Lynx rádiói:

- E-Lynx MP-VS50 (egycsatornás) járműfedélzeti rádió (VHF/UHF, L);
- E-Lynx MP-VD55 (kétcsatornás) járműfedélzeti rádió (VHF/UHF, L);
- E-Lynx PNR-1000 személyi rádió (*soldier radio,* UHF);
- E-Lynx MCTR-7200HH kézi rádió (*handheld,* VHF/UHF);
- E-Lynx MCTR-7200MP hordozható rádiók (*manpack,* VHF/UHF);
- HRM 9125 (125 W) járműfedélzeti rádió (HF);
- HRM 9400 (400 W) járműfedélzeti rádió (HF).[30]

A szövetségesi rendben végrehajtott feladatok során továbbra is fontos tényező az interoperabilitás, amely a különböző rádiótípusok miatt jelenleg is kihívást jelent annak ellenére, hogy a NATO is prioritásként kezeli ezt a területet. Azonban az interoperabilitást szolgáló NATO-szabványok hiányában, illetve az egyes gyártók egyéni érdekei miatt ez egyelőre nem valósult meg. A szárazföldi erők részére gyártott, földfelszíni alkalmazáshoz optimalizált, különböző gyártóktól származó rádiók hiába működnek egy frekvenciasávban, az eltérő moduláció és információvédelmi algoritmusok miatt kizárólag nyílt hang üzemmódban képesek egymással kommunikálni, amivel a jelenlegi követelmények nem teljesíthetők. Általánosan elmondható, hogy szövetségesi környezetben a Harris rádiótípusokkal oldható meg ez a feladat, amelyekkel szinte minden szövetséges állam hadereje rendelkezik.

[26] HF: *High Frequency* – rövidhullám (3–30 MHz).
[27] UHF: *Ultra High Frequency* – mikrohullám (300 MHz – 3 GHz).
[28] VHF: *Very High Frequency* – ultrarövidhullám (30–300 MHz).
[29] L sáv: 1–2 GHz.
[30] Kovács 2022: 187–203.

A Magyar Honvédségben tervezetten az interoperabilitást továbbra is az L3Harris Technologies Inc. AN/PRC-117 G típusú rádiója fogja biztosítani, amely szoftveralapú hang-, kép-, illetve adattovábbításra is képes eszköz.

A dandár- és zászlóaljszintű vezetési pontok működtetéséhez kulcsfontosságúak a rádióállomások, amelyek integráltan képesek több rádióirányhoz vagy rádióhálóhoz (az elöljáró és/vagy az alárendeltek/együttműködők felé) csatlakozni. Dandár- és zászlóaljszinten az orosz típusú rádióállomásokat a 2008–2014 közötti fejlesztési ciklusban csak korlátozottan váltották ki a PK-1, PK-2, PK-3, PK-4 kódú eszközök, amelyekbe Kongsberg MRR/MV-300 és Harris AN/PRC-150C rádiókat építettek be. Az eszközök mennyisége azonban a Magyar Honvédség alakulatainak teljes körű ellátását nem tette lehetővé. A HHP keretében betervezték a Gidrán alvázon kialakított különböző rádiós képességekkel rendelkező páncélozott eszközök többféle konfigurációját, amelyek jelenleg elsősorban a tüzérképességet erősítik, hiszen az első beszerzések a vitéz Barankay József 1. Önjáró Tüzérosztály állományába kerültek. Jelenleg is zajlik ezen eszközökben az IC2 (Integrated Command and Control System) integrált tűzvezető rendszer, valamint a HUNTACCIS vezetés-irányítási rendszer integrációja, amelyekben már az Elbit E-Lynx, valamint a Harris AN/PRC-117/G rádiók biztosítják a hang- és az adatátvitelt. Azonban ezek az eszközök sem állnak rendelkezésre jelenleg olyan mennyiségben, amely biztosítaná a dandár vezetési pontjának rádiókommunikációját.

Középtávon szükséges egy olyan megoldás, amely a jelenleg alkalmazott három rádiótípust magában foglalja, ezzel biztosítva a különböző rádiórendszerek homogén rádióforgalmi rendszerbe szervezését. Átmeneti megoldásként a PK-1/G-M és az R-142 M3 integrált rádióállomás és központ áll rendelkezésre, amellyel tervezetten a harckocsi- és tüzéralegység integrálása a dandár híradó rendszerébe lehetségessé válik. A két eszköz hasonló képességekkel rendelkezik kisebb eltérésekkel. A PK-1/G-M-et RÁBA H-18 alvázra, az R-142 M3-at Unimog-alvázra telepítik. Általánosságban úgy értelmezhető, hogy a PK-1 M/G dandárszintű, az R-142 M3 zászlóaljszintű eszköz. Ezek a rádióállomások két VHF és egy HF rádiócsatornát biztosítanak nyílt vagy zárt, rejtjelezett üzemmódban. Rendelkeznek integrált laptopokkal, amelyeken a HUNTACCIS vezetés-irányítási rendszer is futhat. Ennek a képességnek a vezetési pontra történő kiterjesztése érdekében a PK-1/G-M rádióállomás egy 50" méretű érintőképernyős monitorral is rendelkezik. Az állomást úgy alakították ki, hogy az egyik Kongsberg-rádió a későbbiek folyamán kicserélhető legyen Elbit MCTR egycsatornás 50W-os rádióra.

Újdonság, hogy ezekbe az eszközökbe informatikai szegmens is került, amellyel a megfelelő gerinchálózatra csatlakozást követően a Magyar Honvédség Kormányzati Célú Elkülönült Hálózata (MH KCEHH) is elérhető, így az MH Intranet hálózat, valamint az IP-alapú hangkommunikáció elérése is biztosítható. A felcsatlakozás több átviteli út alkalmazásával is történhet, tábori mikrohullámú állomás, VSAT, optikai kábel alkalmazásával, illetve a rádióállomás készletébe tartoznak a szükséges informatikai aktív eszközök is. A PK-1/G-M és az R-142 M3 felépítmények közötti méretkülönbségekből fakadóan az informatikai készlet az R-142 M3 rádióállomásban ládázott kivitelben áll rendelkezésre. Egy másik innováció a rádióállomásban a vezetési pont tábori őrzés-védelmét segítő telepíthető kamerarendszer, amely azonban csak a PK-1/G-M rádióállomás készletében található meg.

Tábori távközlési átviteli utat biztosító eszközök

A Magyar Honvédségben az elmúlt évtizedek során szintén kritikus képességhiány alakult ki nagy adatátviteli kapacitású eszközök terén, amelyekhez a műholdas, a troposzféra-, illetve a mikrohullámú eszközök tartoznak. Ez kulcsfontosságú kérdés a NATO/EU-feladatok, a missziók híradó és informatikai támogatásának területén, de nemzeti alkalmazás során a stacioner hálózathoz (MH KCEHH) történő felcsatlakozási pontok korlátozott rendelkezésre állása esetén is ezen eszközök biztosítanának széles sávú átviteli utakat a tábori vezetési pontok részére. Az alábbiakban azokat az átviteli utat biztosító rendszereket ismertetem, amelyek a haderőfejlesztési koncepcióban szerepelnek.

Műholdas átviteli képesség

A Magyar Honvédségnek 2025 decemberében nem volt saját katonai műholdas képessége, így a műholdas szolgáltatásokat és a végponti terminálokat polgári szolgáltatótól, jelenleg a Nemzeti Infokommunikációs Szolgáltató Zrt.-től bérlik, illetve az átviteli út is polgári műsorszóró műholdon keresztül szavatolt. A műholdas átviteli képesség keretében rendelkezésre álló VSAT-terminálok részére biztosított rendszerszintű adatsebesség azonban nem teszi lehetővé a terminálok maximumának kihasználhatóságát. Alkalmazásánál figyelembe kell venni, hogy a civil műhold igénybevétele több kockázatot is hordoz. A polgári szolgáltató földi állomásainak kialakítása a katonai biztonsági szempontok érvényesülését tekintve nem előnyös, valamint a polgári műhold zavarvédettsége és frekvenciatartománya sem biztosítja a katonai alkalmazáshoz elvárt paramétereket. Figyelembe kell venni azt is, hogy a polgári szolgáltató tulajdonában lévő műhold adott esetben bármikor deaktiválható. A HHP keretében tervben van az MH VSAT rendszer kialakítása, azonban a feladat indítása a szükséges forrásallokáció hiánya miatt csak 2027-ben kezdődhet majd meg. A szolgáltatás kialakítása a beszerzésen kívül infrastrukturális beruházást és kiképzést, illetve szervezetfejlesztést is igényel.

A harcászati rádiók SATCOM (*Satellite Communication* – műholdas hírközlés) képessége műholdhozzáférés hiányában az MH feladatainak érdekében nem kihasználható, ezért a VSAT-hoz hasonló módon lesz biztosítva a műholdkapacitás a kiképzés, illetve a gyakorlatok támogatása érdekében. Áthidaló megoldásként a Magyar Honvédség idén bérel szolgáltatásként Starlink-antennákat, amely projektet a SpaceX amerikai űrkutatási vállalat a globális internetszolgáltatás biztosítása céljából indította el. Alkalmazásával lényegesen nagyobb adatsebesség érhető el, könnyen telepíthető és kis méretű. A polgári kivitelezés, valamint a polgári szolgáltatóból fakadó problémák azonban itt is fennállnak.

Troposzféra-átviteli képesség

A troposzféra-szóródáson alapuló kommunikációs rendszerek technológiája, amely optikai rálátás nélkül, a hullámok troposzféráról történő visszaverődése által képes összeköttetést biztosítani, az elmúlt évtizedekben nagyon látványosan fejlődött. A korszerű eszközök mérete, adatsebessége, teljesítményigénye a korábbiaknál sokkal jobban alkalmazhatóvá teszi azt. A rendszer beszerzése ugyan költségesebb, mint egy hagyományos rádiórelé, azonban az általa biztosítható hatótávolság, az antennaárbóc nélkülözhetősége (nagy előnye a telepítési idő csökkenése), illetve a szükséges kezelőszemélyzet kisebb létszáma alapján indokolt ezen technológia alkalmazása.

A Magyar Honvédség troposzféra-rádiórelé (*Beyond Line of Sight,* BLOS – optikai rálátás nélkül) híradás képességét a 2000-es évek elején felszámolták, annak pótlására eddig nem került sor. A HHP keretében kialakult egy elképzelés arra, hogy az orosz–ukrán háború tapasztalatainak megfelelően ennek a képességnek az újjáépítése megtörténjen. A troposzféra-eszközökkel a rádiórelénél nagyobb távolságban biztosítható az átviteli út. Az MH KCEHH stacioner rendszerének szolgáltatásátadási pontjaihoz csatlakozva vagy attól függetlenül biztosítanak átviteli utat a híradó és informatikai készletek részére. Alkalmazásához nem szükséges antennaárbóc, hanem tányérantennával rendszeresítik, illetve létezik ládázott vagy utánfutóra épített változata is. Az MH KCEHH kiesése esetén annak pótlására alkalmazható, illetve a műholdképességet is helyettesítheti. Stratégiai képességnek tekinthető maximum 250 km-es hatótávolsága, valamint maximum 100 Mbps-os adatátviteli sebessége miatt.

Tábori mikrohullámú képesség

A 2018-ban elkészült rádiórelé, az RR-1/G tábori digitális mikrohullámú állomás az első alternatíva, amely a régi orosz típusú analóg rádiórelék modern utódjának tekinthető a Magyar Honvédségben. Az eszköz megjelenése a híradó és informatikai eszközök sorában így mérföldkőnek számít, azonban a rendelkezésre álló készletek száma még messze nem fedi le a jelentkező igényeket. A Magyar Honvédség 2025 decemberében 4 db mikrohullámú állomással rendelkezett, a flotta bővülése 2027-től folytatódik.

A rádiórelé (*Line of Sight,* LOS – optikai rálátással) alapvetően dandár-, illetve zászlóaljszintű eszköz, amely maximálisan 35 km távolságot tud áthidalni, és maximum 95 Mbps adatátviteli sebességet nyújt. Egyszerre két irány kiszolgálására alkalmas, amely tovább bővíthető, illetve nyílt és minősített hang- és adatátviteli képességgel is rendelkezik. Új technikai megoldásként vízburkos szupercsendes aggregátorral, pneumatikus antennaárbóccal, valamint távvezérelt antennaforgató rendszerrel szerelték fel. A mikrohullámú kommunikáció alapfeltétele a stacioner mikrohullámú gerinchálózathoz felcsatlakozási pontok rendelkezésre állása, amelyek kiépítése szintén szerepel a HHP tervében. Az RR-1/G nemcsak átjátszó állomás, hanem csomóponti eszköz is, amely IP-telefóniával, valamint tábori hálózatmenedzsment-képességgel is rendelkezik, illetve az országos hálózatfelügyeleti rendszerbe integrálható.

Complex Transzportkiterjesztési Rendszer (CTR)

A CTR egy olyan rugalmas transzportkiterjesztési rendszer, amellyel a központi híradó és informatikai szolgáltatások elérhetők, illetve a célrendszerek adattovábbítása kiépített stacioner infrastruktúra nélkül biztosítható tábori körülmények között. A gyors telepíthetőség érdekében ládázott kialakításban tartalmazza a szükséges aktív eszközöket, tűzfalat, illetve antennát. Nagy előnye, hogy különböző hálózatokról üzemeltethető (internet, mobil 5G, VSAT, Starlink, SATCOM-képes rádió, mikrohullám, Nemzeti Távközlési Gerinchálózat), emellett rendelkezik az automatikus hálózatválasztás képességével. Alapvetően stacioner hálózatok kisalegység szintű kiterjesztésére alkalmas, amelynek eredményeképpen a szerverszolgáltatás az adatközpontban valósul meg, központi kiszolgálás keretében. Az alapkészlet a tervek szerint tartalmazza az IP-telefonkészülékeket, valamint a katonai kivitelű laptopokat is. A készlettel biztosított nyílt MH KCEHH hálózat felhasználható a minősített hálózat felhordó hálózataként is. A készlethez kiegészítésként alkalmazható az LTE-450[31] hálózati csatlakozáshoz szükséges modem és antenna. Az LTE-450 hálózatot 2024-től a vonatkozó kormányhatározat[32] értelmében a Honvédelmi Minisztérium a Magyar Honvédség érdekében átvette, és a HM EI Zrt. üzemelteti.

Összegzés

A mindenütt jelen lévő információs és kommunikációs technológia kritikus fontosságú a jövőbeli konfliktusokban. A Magyar Honvédségnek alapvető érdeke, hogy csatlakozzon azon országokhoz, amelyek ezt felismerve folyamatosan fejlesztik, „digitalizálják" a haderejüket. Úgy gondolom, hogy elindultunk mi is ezen az úton, amely azonban még göröngyös és hosszú. Az előzőkben leírtakból kitűnik, hogy jó elképzelésekkel és tervekkel rendelkezik a szakterület. Ezeknek a megvalósításához viszont elengedhetetlen a megfelelő finanszírozás, amely más, szintén a haderőfejlesztés keretében zajló projekt miatt nem mindig valósul meg megfelelően.

NATO-tagállamként és az EU tagjaként elsődleges az együttműködés erősítése, ezen belül a híradó és informatikai interoperabilitási képességek fejlesztése, amely a HHP fókuszpontjában is áll. Egyúttal előtérbe kerülnek a könnyen telepíthető, gyorsan mozgatható híradó és informatikai rendszerek. A távközlési utak, a vezeték nélküli hálózatok, a mobil, a mikrohullámú és a műholdas kapcsolati rendszerek alapvetően határozzák meg a valós idejű információmegosztást, a műveletek koordinálását, a célpontok pontos azonosítását. A hálózatalapú hadviselés a gyors döntéshozatalt, valamint a helyzetre adott rugalmas és dinamikus válaszokat teszi lehetővé. Ez elképzelhetetlen technológiailag fejlett, robusztus és dinamikus híradó és informatikai rendszerek nélkül.

[31] LTE-450: Negyedik generációs (4G) mobil távközlési technológia 450 MHz-es frekvenciasávon működő változata, amely különösen alkalmas nagy lefedettséget igénylő, alacsony sűrűségű területeken történő alkalmazásra. A frekvenciasáv sajátosságai miatt jól használható katonai és katasztrófavédelmi célokra, mivel kedvező rádióterjedési tulajdonságai vannak, a rendszerek gyorsan telepíthetők, megbízható adat- és hangkommunikációs képességet biztosítanak tábori körülmények között is.

[32] 88/2024. (IV. 23.) Korm. rendelet.

A HHP további tervezése során kiemelt szempontként kell érvényesülnie a fejlesztések hosszú távú fenntarthatóságának, mivel a technológiai innováció folyamatos, és annak ütemével a haderőnek lépést kell tartania. A beszerzett rendszerek alkalmazási tapasztalatainak rendszeres értékelése és annak visszacsatolása alapvető feltétele a rugalmas, adaptív képességfejlesztésnek.

A HHP megvalósítását azonban nehezíti, hogy a Magyar Honvédség szervezeti felépítése is változik, ez magával vonja a vezetés-irányítással, ezáltal a tábori híradó és informatikai rendszerrel szemben támasztott követelmények módosulását is, amely folyamatos felülvizsgálatot, áttervezést igényel. Ennek során azonban figyelembe kell venni a hibrid rendszerek (régi és új) együttes üzemeltetéséből fakadó nehézségeket is, ami átmeneti megoldásokat igényel a szakterület részéről.

Az elemzés során bemutatott fejlesztések világosan rámutatnak arra, hogy a Magyar Honvédség infokommunikációs képességeinek modernizációja elengedhetetlen a 21. századi hadviselés követelményeinek való megfeleléshez. A tanulmány célkitűzése az volt, hogy feltárja az orosz–ukrán háború hatását a HHP keretében zajló híradó és informatikai fejlesztések irányvonalára. A vizsgálat leíró, forrásalapú módszertanra épült, ami lehetőséget adott a rendszerszintű változások és trendek értelmezésére.

A kutatási kérdések alapján megállapítható, hogy az adaptált tapasztalatok elsősorban a hálózatalapú műveleti képességek, az információvédelem, valamint a többnemzeti interoperabilitás fejlesztésében érvényesülnek. A tanulmány rámutatott arra is, hogy a biztonságos és gyors információáramlás képessége döntő tényező a modern műveleti környezetben, amely a stratégiai döntéshozatal sikerességét közvetlenül befolyásolja.

A bemutatott eszközök és technológiák (például TLAN, HUNOPNET) olyan alaprendszerek, amelyeknek az integrálása a NATO-követelmények mentén folyik, ugyanakkor a hazai sajátosságokra és kapacitásokra is épít. A tanulmány tehát hozzájárul a meglévő szakirodalom bővítéséhez a híradó és informatikai fejlesztések dokumentálásával, és megalapozza a későbbi, empirikus alapú kutatásokat ezen a területen.

További kutatások indokoltak lehetnek az új generációs technológiák alkalmazhatóságának, a hibrid rendszerek kompatibilitásának, valamint a NATO-követelmények teljesítésének elemzése terén. A híradó és informatikai rendszerek fejlesztése tehát nem csupán technikai kérdés, hanem stratégiai képességépítés, amelynek tudományos vizsgálata a jövőben is indokolt marad.

Felhasznált irodalom

Armada International (2024): How MilSatCom Has Transformed Warfare and Continues to Shape the Battlefield. *Armada International,* 2024. október 4. Online: https://www.armadainternational.com/2024/10/how-milsatcom-has-transformed-warfare-and-continues-to-shape-the-battlefield/

Babu, Sunil JB – Williams, Huw (2022): Ukraine Conflict: Ukraine's Electronic Warfare Systems in Focus. *Janes,* 2022. március 4. Online: https://www.janes.com/osint-insights/defence-news/c4isr/ukraine-conflict-ukraines-electronic-warfare-systems-in-focus

Bányász Eszter (2024): Minden új eszközzel növekszik Magyarország biztonsága. *Honvedelem.hu,* 2024. november 6. Online: https://honvedelem.hu/hirek/minden-uj-eszkozzel-novekszik-magyarorszag-biztonsaga.html

Csiki Varga Tamás – Tálas Péter (2020): Magyarország új nemzeti biztonsági stratégiájáról. *Nemzet és Biztonság,* 13(3), 89–112. Online: https://doi.org/10.32576/nb.2020.3.7

Demarest, Colin (2022): Ukraine to Get Thousands of Secure Radios in Latest US Package. *Defense News,* 2022. június 16. Online: https://www.defensenews.com/battlefield-tech/c2-comms/2022/06/16/ukraine-to-get-thousands-of-secure-radios-in-latest-us-package/

Elengedhetetlen a magyar haderő fejlesztése. *Honvedelem.hu,* 2024. február 16. Online: https://honvedelem.hu/hirek/elengedhetetlen-a-magyar-hadero-fejlesztese.html

Haig Zsolt – Várhegyi István (2005): *Hadviselés az információs hadszíntéren.* Budapest: Zrínyi Kiadó.

Harper, Jon (2023): Pentagon Contracting With SpaceX's Starlink to Provide Satellite Communication Capabilities for Ukraine. *Defensescoop,* 2023. június 1. Online: https://defensescoop.com/2023/06/01/pentagon-contracting-with-spacexs-starlink-to-provide-satellite-communication-capabilities-for-ukraine/?utm_source=chatgpt.com

HÍR/4 Magyar Honvédség Összhaderőnemi Híradó és Informatikai Doktrína (2013). A Magyar Honvédség kiadványa.

Johnson, Nicholas (2024): Back to the Future of Comms. *RAND,* 2024. július 30. Online: https://www.rand.org/pubs/commentary/2024/07/back-to-the-future-of-comms.html

Kálmánfi Gábor (2017): Európának meg kell védenie magát. *Honvedelem.hu,* 2017. április 4. Online: https://honvedelem.hu/hatter/biztonsagpolitika/europanak-meg-kell-vedenie-magat.html

Kovács Zoltán (2022): A Magyar Honvédség harcászati rádiócsalád fejlesztésének helyzete a Zrínyi Honvédelmi és Haderőfejlesztési Program tükrében. *Hadmérnök,* 17(2), 187–203. Online: https://doi.org/10.32567/hm.2022.2.13

Kushnikov, Vadim (2025): Brave1 Tests Tools to Increase Drone Communication Range. *Militarnyi,* 2025. január 22. Online: https://militarnyi.com/en/news/brave1-tests-tools-to-increase-drone-communication-range/

Marins, Patricia (2023): The Russian Army's Communication Challenges. *Defense Arabia,* 2023. július 18. Online: https://english.defensearabia.com/the-russian-armys-communication-challenges/

Munk Sándor (2024): Részleges interoperabilitás, szükséges-e tudományos vizsgálata? *Hadtudomány,* 34(E-szám), 115–132. Online: https://doi.org/10.17047/Hadtud.2024.34.E.115

NATO [é. n.]: *Federated Mission Networking.* Online: https://www.act.nato.int/activities/federated-mission-networking/

NATO Communications and Information Agency [é. n.]: *What is FMN?* Online: https://coi.nato.int/FMNPublic/SitePages/Home.aspx

Savage, Olivia (2023): Ukraine Conflict: Ukraine Develops Jam-Resistant Radio. *Janes,* 2023. október 18. Online: https://www.janes.com/osint-insights/defence-news/defence/ukraine-conflict-ukraine-develops-jam-resistant-radio
Szűcs László (2016): Honvédelmi és haderőfejlesztési program kezdődik. *Honvedelem.hu,* 2016. december 20. Online: https://honvedelem.hu/hirek/hazai-hirek/honvedelmi-es-haderofejlesztesi-program-kezdodik.html

Jogi források

1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról
1393/2021. (VI. 24.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról
88/2024. (IV. 23.) Korm. rendelet az LTE-450 MHz-es mobil adatkommunikációs hálózat honvédelmi célú átvételével kapcsolatos rendelkezésekről, valamint a kormányzati célú hálózatokról szóló 346/2010. (XII. 28.) Korm. rendelet módosításáról

HADMÉRNÖK
VÉDELEMINFORMATIKA

20. évfolyam (2025) 2. szám 55–73.
DOI: 10.32567/hm.2025.2.4

Mátyás Ináncsi,[1] Péter Bányász,[2]
Péter Kugler,[3] Máté Dub[4]

Empirical Studies of Russian–Ukrainian War Related Fake News, Part 3[5]

Abstract

The Russian–Ukrainian war, which broke out on 24 February 2022, resulted in several paradigm shifts in cyber warfare. One aspect of these changes is psychological operations. Russia and Ukraine have conducted extensive psychological operations campaigns to fulfil their war objectives, which have since been intense along modified objectives. This series of studies examines the impact of war-related fake news through various empirical research. In the first part of the paper, the authors examine the emergence of psychological operations and related terms in the international academic literature using network analysis methodology. In the second part of the paper, the authors use sentiment and network analysis to investigate the spread of different fake news. In the third study, the authors measure the attitudes toward the perception of the Hungarian Defence Forces from the perspective of the war in the neighbouring country.

Keywords: Russian–Ukrainian war, PSYOPS, cyberwarfare, network analysis, sentiment analysis

[1] PhD student, Ludovika University of Public Service, Department of Cyber Security, Doctoral School of Military Sciences, e-mail: inancsi.matyas@uni-nke.hu
[2] Associate Professor, Ludovika University of Public Service, Faculty of Political Science and International Studies, Department of Cyber Security, e-mail: banyasz.peter@uni-nke.hu
[3] Ludovika University of Public Service, Faculty of Military Science and Officer Training, e-mail: kugler.peti@protonmail.com
[4] PhD student, Ludovika University of Public Service, Doctoral School of Military Science, e-mail: dub.mate@uni-nke.hu
[5] Supported by the ÚNKP-22-2-II-NKE-11, ÚNKP-22-2-I-NKE-79 and ÚNKP-22-1-I-NKE-14 New National Excellence Programmes of the Ministry of Innovation and Technology financed from the National Research, Development and Innovation Fund.

Introduction

"In a volatile world, making Hungary secure and successful in the long run requires the efforts and cooperation of the nation as a whole, including the preservation of the Hungarian language and culture – both within and beyond our borders" states the National Security Strategy of Hungary. A Secure Hungary in a Volatile World in 2020.[6] Of course, a significant part of this task falls to law enforcement agencies and the Hungarian Defence Forces (hereinafter referred to as HDF). National security relies strongly on the security of the world. As we have seen in the past years, a conflict in the Middle East could very easily spread to Europe as an immigration disaster. Hungary, as a Schengen border nation, is in a challenging position. While securing our borders and enforcing legal entry requirements to Hungary and, by extension, Europe is essential in ensuring national security, we cannot overlook the fact that our safety is intrinsically linked to the safety of others. When others are secure, crises are less likely to spill over to us, making global peace essential for our protection.

Notably, although wars have steadily declined since World War II, becoming historically unprecedentedly rare now, hybrid warfare is a significant threat to national security. Moreover, this has been accompanied by a rise in the number of conflicts below the threshold of war and the number of frozen conflicts. Table 1 presents the status quo of frozen conflicts around Europe, allowing us to note how frozen conflicts surround us.

Table 1: The status quo of "frozen conflicts" in 2024

	Azerbaijan	**Moldova**	**Georgia**	**Ukraine**
Type of conflict	Frozen conflict	Frozen conflict	Frozen conflict(s)	"Hot war"
Status-quo	Solved	Frozen	Frozen	Ongoing
Russian military presence	Temporary	Weakened	Stable	Attacking
EU peace-oriented involvement	None	Trade facilitation	Administrative border monitoring	Multidimensional military aid

Source: Cenusa 2024

The situation remains worrying at the global level. Between 1946 and 2011, there were 42 cases of frozen conflicts.[7] Some of these frozen conflicts have been ongoing for such a long time (to give some examples: India–Pakistan, Egypt–Israel, North Korea – South Korea) that we can assume – without outside assistance or significant changes in government and social structure – they might be permanent.

[6] The Government of Hungary 2020.
[7] Klosek et al. 2021: 849.

One of the reasons of this rise in the number of frozen conflicts is caused by the increasing complexity of global affairs, leading to more unexpected events, both in terms of sudden weather changes triggered by global warming and the actions of some actors in international politics. For example, Russia's unexpected annexation of Crimea in 2014 and the Russian–Ukrainian war, which started as a hybrid conflict and escalated into an all-out war in 2022, will be a prolonged conflict, even if a peace agreement officially ends the war. After that, international peacekeeping forces will likely be required in Ukraine as independent observers and to prevent further conflict escalation. It is also more practical for an independent actor to coordinate the international community's assistance in the reconstruction process to maximise the efficient use of resources. In addition, in connection with the threat of hybrid warfare, we must emphasise that public support is a critical element of the defence against hybrid warfare in the current era.

Before continuing from this perspective, we must shift our attention towards cyberspace. At a time of post-truth, does it make sense to ask people's opinions? The essence of the post-truth "syndrome" is that instead of facts and logic, people make decisions based on the emotions aroused by a given topic or event, leaving a wide margin for manipulation. In cyberspace, it is increasingly filled and divided by accelerating information bubbles; how useful and possible is it to get an accurate picture of what the general public thinks?

Ordinary citizens are likely to inform themselves about the HDF's activities mainly on the internet, so the perception of the HDF and peacekeeping operations can be very diverse due to the different credibility of websites. Depending on the information bubble in which they "stay" in cyberspace, they may be more supportive, more averse to the topic, or not concerned about it at all, thus adopting a neutral attitude.

Our research aims to establish and support with empirical data the current level of public support and trust in the HDF and its capabilities to defend Hungary. Additionally, it examines public opinion on our NATO membership and the potential expansion of NATO.

The last public survey regarding public trust in the HDF was collected during the 2016 Microcensus of the Hungarian Central Statistical Office, which has taken place in October of 2016. The census took place in 2,148 municipalities across the country at approximately 440,000 addresses, sampling around 10% of the Hungarian households.[8] In 2018 Attila Rácz published his article about the results; at that time the HDF enjoyed a medium level of public trust, on the scale of 0 (totally untrusted) to 10 (fully trusted), the average trust level was 5.44.[9]

We believe that the 2015 migration crisis, the Covid–19 epidemic period, and the war fought in Ukraine will significantly increase the HDF's prestige among the population in general. The Zrínyi Defence and Force Development Programme started in 2017, the aim of which is the general modernisation of the whole HDF, bringing it to the standard of a modern 21st century army, and the related equipment purchases

[8] Central Statistical Office of Hungary 2016.
[9] Rácz 2018: 4–9.

will contribute to this cause, as well. In addition, the HDF's more active use of social media will also support this trend.

Disinformation has always been part of war; this is also true for the Russian–Ukrainian war. There have been some disinformation campaigns regarding Hungary as well, the most memorable is perhaps the rumour that Putin offered Transcarpathia for Orbán's support. This alleged offer was never confirmed by reliable sources and was denied by Putin himself in the Tucker Carlson interview.[10]

There has been no major HDF-related disinformation campaign in this war, the Russian narrative targets the political leaders of Hungary and the unity of the alliances standing against them (in their narrative), the EU and NATO. If we browse the EUvsDisinfo Project, no HDF related news exist. We think that one sign to look for in the future is whether there will be a disinformation campaign attempting one of the following: discrediting the HDF, increasing the tension between the political and military leadership, or undermine the social recognition of soldiers.

In the everyday news, the HDF is mainly mentioned in three contexts: new military hardware arrived because of the ongoing Zrínyi Defence and Force Development Programme; HDF has rebuild a capability long lost or added a new modern one; HDF is successful in a peacekeeping mission. We wanted to gauge the level of engagement among the Hungarian population. We collected all active HDF missions and used SentiOne to measure online engagement and sentiments.

Based on a comprehensive review of the existing literature, we identified and formulated the key hypotheses guiding our research:

H1: The awareness level of the HDF-related news is a deciding factor in the population when it comes to sentiments regarding: a) the HDF's capabilities to defend Hungary on its own; b) defending together with allied forces; c) the support of Hungary's NATO membership and; d) the support on the expansion of NATO.
H2: The Hungarian people's public preference for crisis management type varies by demographic factors such as age, gender, or education level.
H3: The socioeconomic background has an impact on the individuals' views regarding the question if NATO membership or the expansion of NATO lies in the interest of Hungary.

Methods

Our research is structured in two parts. First, we conducted sentiment analysis using the SentiOne social media listening platform. We analysed the online content concerning the HDF's missionary engagement based on keywords. A message, tweet, etc., can be classified into three categories based on sentiment value: positive, neutral and hostile.

In the second part of our study series, we explained in detail the methodology used by the SentiOne platform, so we will not repeat it here but briefly summarise it. SentiOne (sentione.com) is a content-based web analytics platform that covers and

[10] Carlson 2024.

recognises 70 languages all across the globe. It crawls and analyses content presented and perceived in social media and other online channels. The SentiOne monitoring tool currently monitors over 20,000,000,000 mentions and gathers data from 8 different types of sources, namely portals, blogs, Twitter, Facebook, Instagram, video, forums and review sites. The mentions are divided into statements and articles, automatically classified as positive, neutral, or negative using SentiOne's unique, proprietary algorithm. The interactive platform is built upon user-provided keywords and key phrases to look for the specific mentions that, either in themselves or within their context, contain those pre-given phrases that interest the user. The system gathers data in almost real time yet has a memory that can go back up to 3 years. For quantitative research, data is structured by different focus points and research parameters and is visualised interactively. This technology also supports qualitative research, enabling in-depth analysis and categorisation of all the indexed web content.

Our second method was publishing a questionnaire survey. It was based on the one compiled in Fang and Sun's 2019 article Gauging Chinese Public Support for China's Role in Peacekeeping[11] translated into Hungarian and removing Chinese specificities. We also changed some questions and added new ones to reflect the Hungarian social and geographical circumstances. The response to the questions was based on a 5-point Likert scale, which is a psychometric scale commonly used in research to measure attitudes, perceptions, or subjective evaluations. It is a structured ordinal scale designed to capture a respondent's attitude or opinion by providing a range of fixed-choice responses. The scale generally includes five points, with levels of agreement ranging from 'completely disagree' (1) to 'completely agree' (5), often including a neutral midpoint ('Neither Agree nor Disagree'). This scale quantifies subjective data, facilitating statistical comparison and analysis. The questionnaire also included the respondents' socioeconomic and demographic data. The data obtained from the questionnaire were processed by statistical analysis using the Python libraries scipy.stats[12] and scikit-posthocs.[13] For data handling we used the pandas library.[14]

The data collection period was from 11 March 2023 to 11 April 2023. We received 116 responses to our questionnaire; one record was removed during the cleaning up process. The remaining sample of 115 was analysed. It is important to acknowledge that our dataset is not representative of the entire Hungarian population, particularly with respect to age distribution and educational attainment, which we consider the most critical factors. Consequently, the results obtained from our analysis should not be generalised to the broader population, as a substantially larger, more diverse sample would be required for such extrapolation. Therefore, the findings presented are applicable solely to the respondents of this specific questionnaire and should be interpreted with caution in this context.

[11] Fang–Sun 2019.

[12] Part of the broader SciPy library, scipy.stats is a module focused on providing a wide array of statistical functions, tests and probability distributions.

[13] A specialised library designed for performing post-hoc tests after non-parametric statistical tests like Kruskal–Wallis. It fills a gap left by scipy.stats, which does not offer built-in post-hoc test functionality.

[14] Pandas is a highly popular open-source data analysis and manipulation library for Python. It provides flexible and powerful data structures for efficient management of structured data, such as time series, tables and matrices.

Another limitation of this study is that the responses were collected through self-reported questionnaires, which may introduce a form of bias known as response bias. This bias occurs when respondents do not provide entirely accurate answers due to factors such as social desirability, recall issues, or the desire to conform to perceived norms. As a result, the validity of the findings may be affected by the inherent inaccuracies in self-reported data.[15]

The Kruskal–Wallis H test is a rank-based non-parametric test that can determine whether there are statistically significant differences between two or more groups of an independent variable for a continuous or ordinal dependent variable. It is considered a non-parametric alternative to one-way ANOVA and is an extension of the Mann–Whitney U test that allows comparisons between more than two independent groups. For example, it can be used to understand whether attitudes about a workplace problem – where attitudes are measured on an ordinal scale – differ by job position. The Kruskal–Wallis H test is an omnibus test statistic that cannot tell which specific groups of its independent variable are statistically significantly different; it can only tell whether at least two groups are different.[16]

Dunn's test is a post-hoc test used after a Kruskal–Wallis H test to determine which specific groups differ from each other. It performs pairwise comparisons and calculates a Z test statistic to show statistically significant differences between groups. To control the family-wise error rate (which increases with multiple comparisons), adjustments like Bonferroni or Sidak can be applied to the p values. We used the Bonferroni correction and calculated the results using Python's scikit-posthocs[17] library.[18]

The chi-square test is a non-parametric statistical method employed to evaluate the presence of a statistically significant association between categorical variables. It assesses whether the observed frequency distribution deviates from the expected distribution under the assumption of independence. This test is widely utilised in hypothesis testing to examine the independence of two categorical variables or to determine the goodness of fit between empirical data and a theoretical model.[19]

Mann–Whitney U test, as a non-parametric test, is designed to analyse data without assuming a specific distribution. It is particularly useful when: sample sizes are small, data is ordinal, can analyse ranked variables. Another of its advantages is that it does not require data to follow a normal distribution.[20]

15 Furnham 1986: 1–2.
16 Kruskal–Wallis 1952.
17 The scikit-posthocs library is a Python package designed for performing multiple post-hoc tests after non-parametric statistical tests like the Kruskal–Wallis test. It supports various tests such as Dunn's test, Conover's test, and the Nemenyi test. Additionally, it offers several methods for correcting p values for multiple comparisons, such as the Bonferroni correction.
18 Dunn 1964.
19 The University of Utah s. a.
20 Mann–Whitney 1947.

Results

Using the SentiOne social media monitoring platform, we examined the posts on each social media platform about missions with Hungarian participation, using the shortened or full English names of the missions as keywords. Since SentiOne can estimate the language of a given piece of content with 99% accuracy, we used this data instead of the much less reliable country/position, which SentiOne can only estimate without this information. The sentiment value was calculated using an appropriate Excel function for Hungarian content. The results are summarised in Table 2. A topic's sentiment can be harmful, neutral, or positive. A lack of sentiment gives an empty result, as shown in Table 2.

Table 2: Sentiment values of Hungarian peacekeeping missions

Mission	Negative	Neutral	Positive	Empty	Summary
EUFOR-Althea	3	5	0	65	73
EUMM	17	41	4	49	111
EUNAV-FOR-IRINI	0	7	1	5	13
EUTM-MALI	11	42	3	49	105
KFOR	2,501	9,720	1,527	2,602	16,350
MINURSO	1	8	0	15	24
International Coalition (Iraq)	0	0	0	0	0
NMI	0	1	0	5	6
UNFYCIP	0	1	0	5	6
UNIFIL	38	201	18	223	480
Overall	2,571	10,026	1,553	3,018	17,168

Source: compiled by the authors based on SentiOne

Perhaps unsurprisingly, the KFOR mission, as the most significant (and probably the best-known) peacekeeping mission, has the most hits. Altogether, the various missions show slightly negative perceptions where there is enough data available to make it worthwhile to look at. Only one entry with at least 100 records is worth examining, and there are only 4.

Overall, the Hungarian social media sentiment toward Hungarian peacekeeping missions was neutral. Around 58.3% of the sentiment showed neutral feelings towards missions; this means people or other sources talked about the missions in a factual, empirical way. However, if we compare the negative and positive sentiments, the negatives exceeded the positive views.

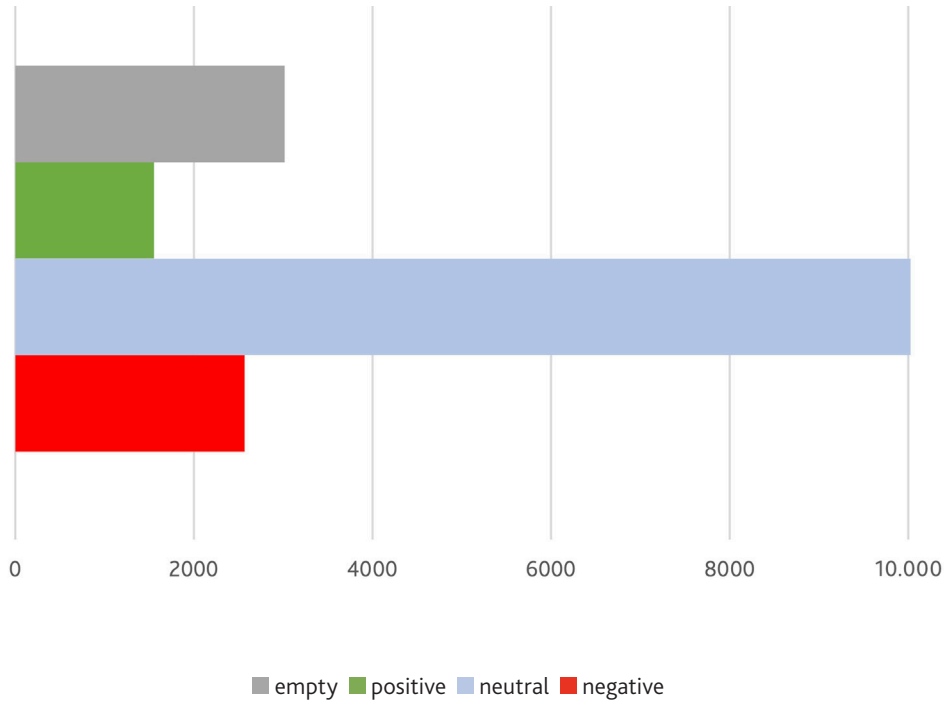


Figure 1: The share of sentiment values of Hungarian peacekeeping missions
Source: compiled by the authors based on SentiOne

As seen in Figure 1, neutral sentiment overwhelmingly dominates, with minimal positive feedback and a noticeable negative sentiment. As mentioned earlier, we suspect that a high amount of neutral sentiment can be noted toward factual reporting, where users share stories in a non-emotional reporting manner. SentiOne is capable to browse three years of data, so if we take into account this long timespan and the lack of engagement, we can see that there is room for improvement from the HDF's side to get closer to the Hungarian population.

H1: The awareness level of the HDF-related news is a deciding factor in the population when it comes to sentiments regarding: a) the HDF's capabilities to defend Hungary on its own; b) defending together with allied forces; c) the support of Hungary's NATO membership and; d) the support on the expansion of NATO.

If we visualise answers on the grouping variable "awareness level", the results can be seen in Figure 2.

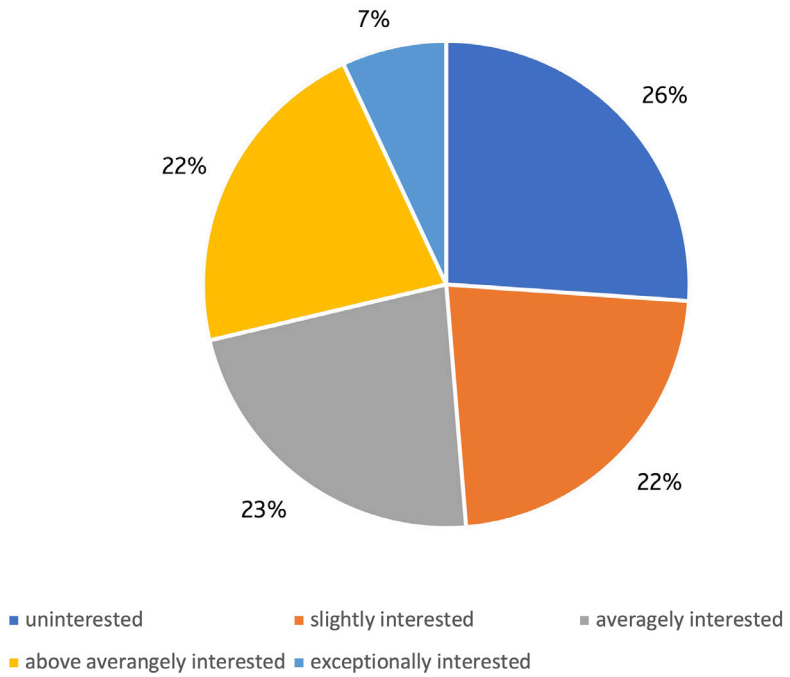


Figure 2: Distribution of answers regarding awareness level
Source: compiled by the authors based on the abovementioned questionnaire

Table 3: The Kruskal–Wallis H test results on HDF self-defence capabilities and NATO attitude

Variable	H statistic	P value
v28_self	2.583	0.6298
v29_ally	18.3475	0.0011
v30_NATO_mem	15.2985	0.0041
v31_NATO_ext	8.4666	0.0759

Source: compiled by the authors

Statistically significant differences were found in v29_ally and v30_NATO_mem, suggesting that awareness levels influence opinions on these topics.

Dunn's test was conducted as a post-hoc analysis following the Kruskal–Wallis H test, which showed a statistically significant difference for v29_ally. The Bonferroni correction was applied as control for multiple comparisons.

Table 4: Dunn's test with Bonferroni correction

	1	2	3	4	5
1	1.0	1.0	0.1607	0.0003	0.7796
2	1.0	1.0	1.0	0.0645	1.0
3	0.1607	1.0	1.0	0.75	1.0
4	0.0003	0.0645	0.75	1.0	1.0
5	0.7796	1.0	1.0	1.0	1.0

Source: compiled by the authors

Group 1, as those participants, who are uninterested in HDF news and Group 4, who show above average interest in this kind of news have significantly different views on whether the HDF can defend Hungary with the assistance of allies. No other groups exhibit strong statistical differences.

A Dunn's post-hoc test with Bonferroni correction was conducted after the Kruskal–Wallis H test, which found that awareness level significantly influences opinions on NATO membership. The results can be found in Table 4.

Table 5: Dunn's test with Bonferroni correction

	1	2	3	4	5
1	1.0	0.1461	0.0128	0.0407	0.0359
2	0.1461	1.0	1.0	1.0	1.0
3	0.0128	1.0	1.0	1.0	1.0
4	0.0407	1.0	1.0	1.0	1.0
5	0.0359	1.0	1.0	1.0	1.0

Source: compiled by the authors

Group 1, who are uninterested in HDF news differs significantly from Groups 3, 4 and 5, who are averagely or above interested in HDF news, meaning that awareness level strongly impacts NATO membership views for these groups. Groups 3, 4 and 5 also do not show significant differences among themselves, indicating similar opinions in these groups.

As this hypothesis was only partially true, we rejected it.

H2: The Hungarian people's public preference for crisis management type varies by demographic factors such as age, gender, or education level.

We have chosen to investigate the connection between demographic factors and crisis management type because we believe that at the end of the Russian–Ukrainian war there will be great need for volunteer nations to send crisis response teams to Ukraine. We wanted to see if the Hungarian people are showing any kind of preference regarding the methods, in order to better understand what kind of factors may play

in this preference. We asked this question in a neutral way, so the results do not get influenced (so much) by the ongoing war.

From the 5 categories 3 involved sending personnel, military support and medical contingent (which in the Hungarian tradition means military medical troops), but there was the civilian expert option as a more neutral choice.

The financial support category referred to assisting in the form of monetary donation, grants or low-interest loans. The military support category encompasses support provided for peace operations through military means, including the deployment of armed forces, provision of defence equipment and tactical assistance. This support aims to enhance stability, ensure security, and reinforce peacekeeping efforts through structured military involvement. The civilian expert category means sending civilian experts as consultants, to restore basic governmental or infrastructural networks and capabilities. The humanitarian aid category provides essential aid to alleviate immediate suffering and support basic needs, such as food, water, shelter and emergency relief supplies. This assistance addresses urgent crises, protects vulnerable populations and fosters community resilience. The medical contingent category focuses on delivering medical support, including deploying healthcare professionals, medical supplies and facilities. This assistance aims to ensure essential health services, manage medical emergencies, and contribute to the well-being and recovery of communities in crisis.

In the questionnaire the test takers had to input their priorities on crisis management, and rank the five options from 1 to 5, where 1 was the kind of support they would prefer the most, and 5 the least preferred. Every option needed to be given a rank.

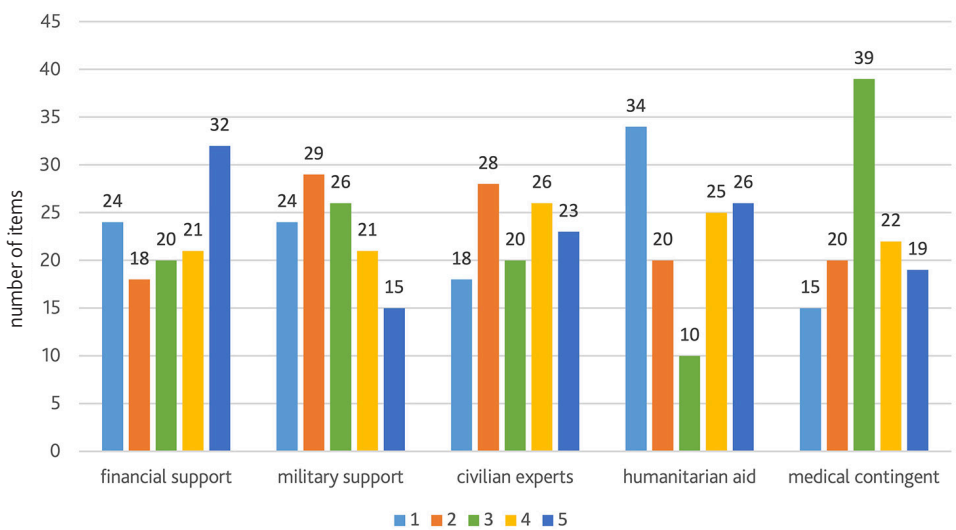


Figure 3: Prioritisation of different types of crisis management
Source: compiled by the authors based on the abovementioned questionnaire

We tested our hypothesis using the chi-square test for different crisis management types and the demographic variables gender, age and highest education.

Table 6: Chi-square test results

Variable 1	Variable 2	Chi-square	Degree of freedom	P value
v18_fin_sup	gender	3.1099	4	0.5396
v18_fin_sup	v1_age	26.1933	24	0.3434
v18_fin_sup	v3_degree	15.1355	24	0.9167
v19_mil_sup	gender	10.1937	4	0.0373
v19_mil_sup	v1_age	20.675	24	0.6578
v19_mil_sup	v3_degree	28.6828	24	0.2323
v20_civ_sup	gender	3.8767	4	0.423
v20_civ_sup	v1_age	18.6153	24	0.7722
v20_civ_sup	v3_degree	24.8124	24	0.416
v21_hum_aid	gender	2.0838	4	0.7203
v21_hum_aid	v1_age	25.2373	24	0.393
v21_hum_aid	v3_degree	27.8248	24	0.2675
v22_med_sup	gender	18.6218	4	0.0009
v22_med_sup	v1_age	40.2863	24	0.0199
v22_med_sup	v3_degree	36.4695	24	0.0494

Source: compiled by the authors

The results show that military support (v19_mil_sup) is statistically influenced by gender; there is a difference of preferences regarding military aid among the genders. Medical contingent as support type (v22_med_sup) is significantly affected by the following variables: gender, age and education; these factors seem to play a role in how people prioritise medical assistance.

Preferences for financial aid, civilian expert assistance and humanitarian aid are not significantly influenced by gender, age, or education among our responders. People's opinion on these forms of crisis management appears to be independent of their demographic background.

As in our survey gender was a binary choice (and mandatory as well), we used the Mann–Whitney U test to compare the differences between the genders regarding military support (v19_mil_sup) and medical contingent (v22_med_sup). For military support, the Mann–Whitney U result was 1,409, with a p value of 0.1801, so statistically seen, the difference between the genders is insignificant. Medical support had the Mann–Whitney U score of 2,058.5 and a p value of 0.0164, which is a statistically significant difference.

For the rest of the variables, which had a significant difference in the chi-square test, we did a Kruskal–Wallis H test with the following results to see if there is a group difference.

Table 7: Kruskal–Wallis H test

Variable 1	Variable 2	Kruskal–Wallis H	P value
v21_hum_aid	v3_degree	14.9987	0.0203
v22_med_sup	v1_age	6.4767	0.372
v22_med_sup	v3_degree	13.0179	0.0428

Source: compiled by the authors

This shows that the support for medical contingent does not show any significant difference between the age groups. For the other two support types, we did a Dunn's post-hoc test with Bonferroni correction, with the following results.

Table 8: Dunn's test with Bonferroni correction

	1	2	3	4	5	6	7
1	1.0	1.0	1.0	0.8918	1.0	1.0	1.0
2	1.0	1.0	1.0	1.0	0.4975	1.0	1.0
3	1.0	1.0	1.0	1.0	0.1631	1.0	0.6484
4	0.8918	1.0	1.0	1.0	0.1559	1.0	0.1844
5	1.0	0.4975	0.1631	0.1559	1.0	1.0	1.0
6	1.0	1.0	1.0	1.0	1.0	1.0	1.0
7	1.0	1.0	0.6484	0.1844	1.0	1.0	1.0

Source: compiled by the authors

Table 9: Dunn's test with Bonferroni correction

	1	2	3	4	5	6	7
1	1.0	0.4377	1.0	0.8552	1.0	1.0	1.0
2	0.4377	1.0	1.0	1.0	1.0	0.3261	1.0
3	1.0	1.0	1.0	1.0	1.0	1.0	1.0
4	0.8552	1.0	1.0	1.0	1.0	0.3128	1.0
5	1.0	1.0	1.0	1.0	1.0	1.0	1.0
6	1.0	0.3262	1.0	0.3128	1.0	1.0	1.0
7	1.0	1.0	1.0	1.0	1.0	1.0	1.0

Source: compiled by the authors

Seeing the results, they show that there is no significant difference among any of the groups.

As a final conclusion we rejected H2, because only for the medical contingent was there a difference of genders for support. For any other crisis management types using the demographic variables age, gender and highest education level we did not find any preference.

H3: The socioeconomic background has an impact on the individuals' views regarding the question if NATO membership or the expansion of NATO lies in the interest of Hungary.

Using the variables v30_NATO_membership_support, v31_NATO_extension_support, v3_highest_degree and v11_financial_situation we did a chi-square analysis.

Table 10: Chi-square analysis results

Variable 1	Variable 2	Chi-square	Degree of freedom	P value
v30_NATO_mem	v31_NATO_ext	118.9375	16	0.0
v30_NATO_mem	v3_degree	20.1331	24	0.6892
v30_NATO_mem	v11_fin_sit	69.554	36	0.0007
v31_NATO_ext	v3_degree	23.2235	24	0.5066
v31_NATO_ext	v11_fin_sit	50.9422	36	0.0505
v3_degree	v11_fin_sit	46.1222	54	0.7683

Source: compiled by the authors

We used Cramer's V analysis, which measures the association strength between two categorical variables. It ranges from no association 0 value to strong association value 1.

Table 11: Cramer's V results

Variable 1	Variable 2	Cramer's V
v30_NATO_mem	v31_NATO_ext	0.5085
v30_NATO_mem	v11_fin_sit	0.3889

Source: compiled by the authors

Strong association is found between NATO membership and NATO expansion, suggesting that individuals' stance on NATO membership is closely tied to their views on its enlargement. A moderate association was found between NATO membership support and financial situation, this indicates that economic background has an impact on an individual's opinion about NATO membership, but the connection is not as strong as in the case above.

As a next step Bonferroni correction was applied to the Dunn's post-hoc test, which is used to identify which specific groups within v30_NATO_mem and v31_NATO_ext significantly differ from each other.

Table 12: Dunn's test with Bonferroni correction

	1	2	3	4	5
1	1.000000	1.000000	0.939203	0.390864	0.000277
2	1.000000	1.000000	1.000000	1.000000	0.000672
3	0.939203	1.000000	1.000000	1.000000	0.000362
4	0.390864	1.000000	1.000000	1.000000	0.003772
5	0.000277	0.000672	0.000362	0.003772	1.000000

Source: compiled by the authors

Group 5 whose stance is that they support NATO membership differs significantly from all other groups, meaning individuals in this category have a statistically distinct opinion compared to the rest, as they also support NATO expansion. All the other groups have relatively similar perspectives, as indicated by their non-significant p values. The strongest statistical difference is observed between Group 1 and Group 5 suggesting polarised opinions, which is true, as these groups are NATO non-supporters and supporters.

The Bonferroni correction was applied to the Dunn's post-hoc test, which is used to determine which specific categories of v30_NATO_mem and v11_fin_sit significantly differ from each other. Please note that the variable showing the participants financial situation (v11_fin_sit) has been set up identically to the Hungarian Central Statistical Office's Microcensus, on a scale from 1–10, where 10 is the richest category.

Table 13: Dunn's test with Bonferroni correction

	1	2	3	4	5	6	7	8	9	10
1	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
2	1.0	1.0	1.0	1.0	1.0	1.0	0.969	1.0	1.0	1.0
3	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
4	1.0	1.0	1.0	1.0	1.0	1.0	0.937	1.0	1.0	1.0
5	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
6	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
7	1.0	0.969	1.0	0.937	1.0	1.0	1.0	1.0	1.0	1.0
8	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
9	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0
10	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0	1.0

Source: compiled by the authors

This suggests that people with different financial situations do not have significantly different views on NATO membership or the economic situation does not influence this preference.

The Cramer's V and Dunn's post-hoc test may look contradictory but we must consider that Cramer's V looks at the overall association, if there is some level of relationship between the variables, but in the end, the Dunn–Bonferroni test confirms that no individual financial category differs significantly in a way that passes the strict statistical threshold.

As this hypothesis was only partially true, we rejected it.

Discussion

As mentioned previously, our results are limited by the sample size of the survey. In general, a random sampling method may give a margin of error that is mathematically exact, but because of practical reasons (e.g. limited resources) most of the surveys use non-probability sampling, where the participating population is adjusted according to the larger target population's distribution.

NATO usually conducts a public opinion survey among the Alliance Members twice a year: one before the yearly summit, the other in around November. They use a sample size of 1,000 persons per country (or in smaller countries 500 persons), and non-probability sampling. Instead of random selection, the survey uses a method where respondents are chosen based (weighted) according to the latest population statistics. At the writing of this article, the newest survey is the NATO Annual Tracking Research 2022, where field work was done in November of 2022.

As another widely recognised survey, the Eurobarometer surveys typically conduct 1,000 interviews per country. In smaller countries, such as Luxembourg, Malta and Cyprus, the sample size is usually 500 interviews.

According to this practice we can say that for a more reliable result a sample size of 500–1,000 would be needed, if possible weighted for the Hungarian population census results of 2022.

The John Lukacs Institute of Ludovika University of Public Service (formerly known as the Institute for Strategic and Defence Studies) has a more focused series of studies, where starting from 2019 every odd year they publish an analysis about the threat and security perceptions in the Central and Eastern European Region. In the Czech Republic, Poland, Hungary, Romania and Slovakia as former satellite states of the Soviet Union, the perspective on today's Russia differs from the rest of the NATO members. Here the sample size was also 1,000 per country.

As we lack public data on the HDF and citizen engagement, or regarding how citizens see HDF and soldiers in general, accurate disinformation remedies are hard to find. We recommend educating the next generation regarding this topic as part of the Fundamentals of National Defence course and in Civics and Social Studies classes.

Summary

In our first article we explored the concept of hybrid warfare, the new art of war of the 21st century. By using psychological operations and disinformation campaigns they have a strategic role in influencing public perception and undermining military operations. We highlighted the difficulty of addressing such campaigns due their cost efficiency, the anonymity of sources and the international nature of online platforms. Moreover, based on the literature review of this new concept, we analysed scientific trends of misinformation and disinformation. It is not surprising that academic discourse increasingly focuses on misinformation and disinformation at the global level, especially regarding global events like the Covid–19 pandemic and the Russian–Ukrainian war. But this trend clearly started to accelerate slowly around 2013. We believe that this will remain an ongoing challenge in the future, and one whose importance will continue to grow. Following up these results, we have collected the top one hundred keywords in connection with disinformation and misinformation. We choose network analysis, because with this method we have the opportunity to highlight strong connections between keywords. With disinformation keyword connections there was a strong connection between disinformation and fake news, social media and misinformation. This was expected since these keywords often go hand in hand. Unexpectedly, the human element also took centre stage in the network. This means that the researchers focus on the human side of disinformation. The same analysis was done with the keyword misinformation. Compared to disinformation, Covid–19 related keywords were more present and more connected; especially vaccine related. The human keyword also took a central position in the network with the same dominancy compared to the previous results. Overall researches were somewhat different related to these two keywords, to disinformation the focus was wider, while misinformation had a smaller Covid–19 related focus.

In our second article we found that based on network research, sentiment analysis suggests that Hungary's stance regarding the Russian–Ukrainian war and the narratives surrounding it can give cause for concern. The divergence between Hungarian society and the narratives and perceptions of Hungary's allies and global public opinion poses significant risks. Hungarian-speakers may be more exposed to psychological operations, particularly due to the tendency of the individuals to align with perspectives that oppose issues they also perceive negatively – often without realising the underlying intent of cognitive influence behind them. We also found that Hungarian social media usage patterns tend to reduce exposure to global discourse, as they differ from the more diverse news consuming habits and tendencies of the international communities. Additionally, negative perceptions of Hungary may harm her bilateral relations with other countries, affecting cooperations on a large scale. The consequences of influencing operations are almost impossible to predict. In addition to harming international relations or just by simply eroding trust in government and media credibility, the increasing societal tensions could undermine the democratic governance system and values. The trend of rising extremism in Europe could continue and could lead to fracture in the EU.

In conclusion, Hungary must prepare herself for psychological operations mainly by raising public awareness. The risks posed by them is immense and recognising them is crucial to the national interest. With international cooperation and the effective allocation of resources, appropriate countermeasures can be developed to detect and counter such operations in a short timeframe. Ensuring resilience hinges on public awareness regarding influence campaigns, so risk mitigation should begin here.

In our last article we attempted to identify the most important factors influencing NATO and crisis management, whether demographic or socioeconomic, or simply awareness regarding the HDF's activities. Because of the comparatively small sample size of the respondents, we were unable to find a definite factor for the abovementioned attitudes. We believe that after the war ends, some kind of peacekeeping force will be needed to prevent the situation in Ukraine from escalating again, so it is necessary to prevent disinformation initiatives seeking to discourage the Hungarian population from supporting any kind of crisis management.

In the ongoing Russian–Ukrainian war, the HDF was not targeted by disinformation campaigns, only attacks on Hungary on the political level were performed. The HDF's peacekeeping missions are Hungary's biggest contribution to our allies in NATO and the EU, and professionally seen the biggest success, but sadly, as we have seen, it falls short of expectations in online presence. Hopefully, this trend will improve in the future, as the defence of Hungary relies on the entire society, and this requires trust in the HDF's capabilities and the support of citizens.

In our article series we highlighted the security challenges posed by information operations. These operations use the dissemination of misinformation, disinformation and malinformation to manipulate the public's political will, while destroying trust in the government and public institutions. Worse still, freedom of expression, the "cornerstone" of traditional democracy, is being used to amplify this effect. While addressing the topic of fake news is a complex problem, it is important to recognise the colossal impact social media platforms can have, as they offer an easy to use and low-cost medium for disinformation campaigns. It also makes us ask the question: To what extent is an individual accountable for spreading misinformation online? Where can we, as a society, draw the line to protect ourselves against this?

Since political leaders in democratic societies determine military objectives and operations, this kind of operation can pose a serious threat to national security, hindering or multiplying the costs and risks of military operations. We explored the divergence of Hungarian public sentiment, particularly the trends of being susceptible to foreign influence through disinformation campaigns. It is a fact that the HDF's international peacekeeping operation contributions and cooperation with allies in NATO and the EU can be regarded as a professional success. However, their online presence remains limited and this also shows that societal support needs to be enhanced. Trust in the HDF's self-defence capability is critical to national defence, as well as societal resilience.

In conclusion, our research advocates for enhanced international cooperation, and proactive measures to mitigate the risk posed by information operations. To heighten the general public's awareness, a more effective education and strategy are needed to combat this challenge. We believe this is vital to safeguard the security of Hungary and our allies.

References

Carlson, Tucker (2024): *The Vladimir Putin Interview.* Online: https://tuckercarlson.com/the-vladimir-putin-interview

Central Statistical Office of Hungary (2016): *Mikrocenzus* 2016 [Microcensus 2016]. Online: https://www.ksh.hu/mikrocenzus2016/

Cenusa, Denis (2024): *Review of "Frozen Conflicts" in the EU Neighbourhood: Rearrangement of the Regional Security Chessboard.* Online: https://www.eesc.lt/en/publication/review-of-frozen-conflicts-in-the-eu-neighbourhood-rearrangement-of-the-regional-security-chessboard/

Deák, András György – Felméry, Zoltán (2023): Biztonságpercepció a kelet-közép-európai régió országaiban. Egy komparatív vizsgálat elsődleges tanulságai [Perceptions of Security in the Countries of the Central and Eastern European Region. Key Findings of a Comparative Study]. *ISDS Analyses,* 2023/16.

Dunn, Olive J. (1964): Multiple Comparisons Using Rank Sums. *Technometrics,* 6(3), 241–252. Online: https://doi.org/10.1080/00401706.1964.10490181

Fang, Songying – Sun, Fanglu (2019): Gauging Chinese Public Support for China's Role in Peacekeeping. *The Chinese Journal of International Politics,* 12(2), 179–201. Online: https://doi.org/10.1093/cjip/poz006

Furnham, Adrian (1986): Response Bias, Social Desirability and Dissimulation. *Personality and Individual Differences,* 7(3), 385–400. Online: https://doi.org/10.1016/0191-8869(86)90014-0

Klosek, Kamil Christoph – Bahenský, Vojtěch – Smetana, Michal – Ludvík, Jan (2021): Frozen Conflicts in World Politics: A New Dataset. *Journal of Peace Research,* 58(4), 849–858. Online: https://doi.org/10.1177/0022343320929726

Kruskal, William H. – Wallis, Allen W. (1952): Use of Ranks in One-Criterion Variance Analysis. *Journal of the American Statistical Association,* 47(260), 583–621. Online: Online: https://doi.org/10.1080/01621459.1952.10483441

Mann, Henry B. – Whitney, Donald R. (1947): On a Test of Whether One of Two Random Variables Is Stochastically Larger than the Other. *The Annals of Mathematical Statistics,* 18(1), 50–60. Online: https://doi.org/10.1214/aoms/1177730491

Rácz, Attila (2018): A magyar honvédség lakossági megítélése a 2016-os mikrocenzus és más reprezentatív adatfelvételek tükrében [The Public Perception of the Hungarian Defence Forces in Light of the 2016 Microcensus and Other Representative Surveys]. *Honvédségi Szemle – Hungarian Defence Review,* 146(6), 4–9. Online: https://kiadvany.magyarhonvedseg.hu/index.php/honvszemle/article/view/322

The Government of Hungary (2020): *Hungary's National Security Strategy. A Secure Hungary in a Volatile World.* Online: https://honvedelem.hu/hirek/government-resolution-1163-2020-21st-april.html

The University of Utah [s. a.]: The Chi-Square Test for Independence. *Sociology 3112.* Department of Sociology. Online: https://soc.utah.edu/sociology3112/chi-square.php

HADMÉRNÖK
VÉDELEMINFORMATIKA
20. évfolyam (2025) 2. szám 75–91.
DOI: 10.32567/hm.2025.2.5

Karsa Róbert[1], Négyesi Imre[2]

Nagy nyelvi modellek és zárt információs rendszerek a védelmi szférában

Large Language Models and Closed Information Systems in the Defence Sector

Absztrakt

A mesterséges intelligencia, különösen a nagy nyelvi modellek és a gépilátás-rendszerek jelentős változásokat hoznak a mindennapi életünkben. Ez a tanulmány feltárja a mesterséges intelligencia védelmi szférában történő alkalmazásának lehetőségeit és kihívásait. Bemutatjuk a nyelvi modellek működését, képzési folyamatait, a generatív modellek képességeit és korlátait, valamint a képfeldolgozás terén elért eredményeket, beleértve a vizuális nagy nyelvi modelleket. Kiemeljük a vektorbeágyazások és vektoradatbázisok fontosságát az információkeresésben, valamint az adatlekérésre alapozott szöveggenerálás szerepét a hallucinációk csökkentésében. Vizsgáljuk a nyelvi modellek képzésének költségeit és a magyarországi lehetőségeket is. A tanulmány rámutat, hogy a nagy nyelvi modellek hadtudományban való alkalmazása jelentős potenciált rejt, de a bizalmas adatok védelme érdekében elengedhetetlen a saját, biztonságos informatikai infrastruktúra kiépítése. Egy zárt információs rendszer segítségével bemutatjuk, hogy a védelmi szektor hogyan tudja kihasználni a technológia előnyeit a biztonságos információkezelés érdekében. Következtetésként hangsúlyozzuk a hosszú távú beruházás és a folyamatos innováció szükségességét a védelmi szektor számára.

Kulcsszavak: mesterséges intelligencia, nagy nyelvi modell, hallucináció, vektoradatbázis, hadtudomány

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola; egyetemi tanársegéd, Pécsi Tudományegyetem Természettudományi Kar Matematikai és Informatikai Intézet, e-mail: karsa.robert@pte.hu
[2] Egyetemi docens, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar, e-mail: negyesi.imre@uni-nke.hu

Abstract

Artificial intelligence, especially large language models and machine vision systems, are bringing major changes to our everyday lives. This paper explores the opportunities and challenges of applying AI in the defence domain. We present the operation and training processes of language models, the capabilities and limitations of generative models, and advances in image processing, including visual large language models. We highlight the importance of vector embeddings and vector databases in information retrieval, and the role of data query-based text generation in reducing hallucinations. We also examine the costs of training language models and the opportunities in Hungary. The paper shows that the use of large language models in military science has a significant potential, but that it is essential to build a dedicated, secure IT infrastructure to protect confidential data. By demonstrating a closed information system, we show how the defence sector can take advantage of the technology to ensure secure information management. In conclusion, we emphasise the need for long-term investment and continuous innovation in the defence sector.

Keywords: artificial intelligence, large language model, hallucination, vector database, military science

Bevezetés

A mesterséges intelligencia (MI) és ezen belül a nagy nyelvi modellek (LLM-ek) jelentős változásokat hoznak mindennapi életünkben és a hadtudomány területén is. Új készségeket, lehetőségeket kell megtanulnunk, megismernünk. A védelmi szférának ezekhez a változásokhoz alkalmazkodnia kell, sőt a gyors technológiai felzárkózással előnyt kell kovácsolnia a lehetőségekből. A kockázatkerülő háborúk korában, ahol a kibereszközök, az autonóm fegyverrendszerek és a katonai képességfejlesztés dominál, az MI központi szerepet játszik a harctéri kockázatok minimalizálásában és a hatékonyság növelésében. Az LLM-ekkel kapcsolatos kutatásunk elsősorban a katasztrófavédelmi hatósági információk feldolgozásával foglalkozik, de az elérhető eredmények túlmutatnak a katasztrófavédelmi területen, és olyan komplex védelmi rendszerek fejlesztéséhez vezetnek, amelyek segítségével új honvédelmi és rendvédelmi képességek jöhetnek létre. Az MI alkalmazása a hadtudományban több területen is megfigyelhető. A kiberhadviselés során az MI jelentősen növeli annak hatékonyságát mind a támadó, mind a védekező oldalon. Képes gyorsabban felismerni a szokatlan tevékenységeket, valamint automatizált válaszokat adni a fenyegetésekre. Az MI kulcsfontosságú az autonóm fegyverrendszerek, például a drónok működésében, lehetővé téve számukra az önálló döntéshozatalt és a célok hatékonyabb elérését. Az MI a katonák képességfejlesztésében is fontos szerepet játszhat, segítheti az agy-számítógép interfészek fejlesztését, ami javíthatja a tanulást, a kiképzést és a döntéshozatalt, továbbá az MI képes a taktikai döntések támogatására, csökkentve a bizonytalanságot a harctéren. Az MI alkalmazásakor be kell tartani az igazságos háború elméletének elveit, és az emberi kontrollt minden esetben biztosítani kell. Célunk, hogy bemutassuk azokat a módszereket és technológiákat, amelyek jelenleg a modern információs infrastruktúrák adatfeldolgozási részének belső alapköveit

képezik, valamint rámutassunk a zárt információkereső rendszerek egy lehetséges változatának védelmi célú alkalmazására. Az új eredmény ezen alkalmazások lehetséges fejlesztésének és a technológiai háttér összefüggéseinek bemutatásában rejlik.

Adatfeldolgozási infrastruktúrák

LLM-ek

Amikor számítógépek segítségével próbálunk meg leírni egy folyamatot, akkor modelleket készítünk, amelyek reményeink szerint egy elvárt viselkedést mutatnak. A nyelvi modell matematikai értelemben olyan valószínűségi eloszlás a szavak sorozatai között, ahol a modell minden egyes szóhoz valószínűségi értéket rendel egy szekvenciában, azaz a szövegben a következő szót jelzi előre az előtte lévő szavak alapján. Az LLM már olyan típusú nyelvi modell, amelynek hátterében egy neurális hálózat van. Ez a neurális hálózat architektúráját tekintve jellemzően egy transzformer, amely jelentős számítási kapacitás igénybevételével hatalmas szövegkorpuszon tanul; egyik legismertebb típusa a GPT-3 vagy éppen a Llama. Ezek a neurális hálózatok az információkat a paramétereikben (számok) tárolják az általánosan megszokott dokumentumok helyett. Ezt a tudást paraméteres tudásnak is hívjuk. Az LLM-ek esetén ezeknek a paramétereknek a száma több milliárdos nagyságrendet is elérhet. A modellek nevében található számok és a B jelölés általában a paraméterszámra utalnak milliárdban kifejezve.

Az LLM-ek képzése

A modellek képzése rendszerint két vagy három lépésből áll. Az első az előképzés, amely során a modell megszerzi az alapvető tudását és képességeit a világunkkal kapcsolatban. Ez a tanulás önfelügyelt tanulás, amelyben a modell maga generálja a tanuláshoz szükséges címkéket. Ez azt jelenti, hogy a tanulási folyamatban nem szükséges emberi közreműködés (kézi címkézés), mivel a modell saját magának hoz létre célokat a tanulás során, ami rendszerint a tanulandó szöveg következő szótöredéke. A képzés során a modellnek mindig a következő szót kell kitalálnia, a képzés alatt a modellnek nincs információja a kitalálandó szó utáni szavakról. A képzés során a modell megtanulja a nyelv mintázatait, és reprezentációkat fejleszt ki a szavak és a szövegkörnyezet közötti kapcsolatokra. A modell megérti a kontextust és képes előrejelzéseket tenni a szövegben következő szavakra vagy mondatokra vonatkozóan.

Ez a tudás a tanítóadatokat tartalmazó akár több milliárd szavas korpusz felett értelmezhető, tehát a modell ismeretei és az ismeretek mélysége egy témában elsősorban a témához kapcsolódó tanítóadatok mennyiségén alapszik. A képzés második szakaszában felügyelt finomhangolás történik, amely már jóval kevesebb erőforrást igényel, mint az előképzés. A felhasználói szándék általában túlmutat azon, hogy egy szöveghez a következő szót előre jelezzük, vagyis egy szöveg írását folytassa. A problémának a megoldására fejlesztették ki a modell-finomhangolási technikát. Ennek során a modellt előre gondosan összeállított utasítás-válasz párokkal

tanítják tovább, amelynek eredményeképpen a modell képes lesz utasítások, kérdések megválaszolására, és annak általánosító képessége is javul. A finomhangolás során az utasítás-válasz párokból feladattól függően a néhány ezertől akár sok százezeres mennyiséget is használhatunk.

A finomhangolás azt is jelenti, hogy egy általános képességekkel rendelkező nyelvi alapmodellt továbbképzünk tartományspecifikus adatokkal, és az adott tartomány szakértőjévé válhat a nyelvi modell.

A képzés opcionális harmadik szakaszában a hangsúlyt arra helyezik, hogy a válaszok jobban kövessék az emberi preferenciákat. Ilyenkor a képzés során emberi visszajelzéseket is felhasználnak; egyik legismertebb ilyen képzési módszer az RLHF, amely során megerősítéses tanulást alkalmaznak felhasználva az emberi visszajelzéseket. Ennek eredményeképpen a modell megtanulja az emberi preferenciákat, és válaszai sokkal „emberibbnek" tűnnek.

Képzési költségek

Az LLM-ek képzése rendkívül költségigényes feladat, ezért nagyon kevés cég képes arra, hogy saját modellt fejlesszen. A fejlesztési költségek a modell növekedésével (a paraméter számának növekedésével) skálázódnak. A BLOOM nevű, 176 milliárd paraméterrel rendelkező nyelvi modell előképzése nagyjából 118 napig tartott és 433 196 kWh áramfogyasztással járt. Az előképzést 384 NVIDIA A100 GPU-val, 48 számítási egység segítségével végezték el. Magyarországon jelenleg csak a Komondor nevű szuperszámítógép képes hasonló feladatok elvégzésére. A Komondor specifikációja szerint a GPU partíciója 232 db NVIDIA A100-as GPU-val rendelkezik, és a fenti BLOOM-modell képzése számításaink szerint több mint 190 napig tartana, amennyiben a szuperszámítógép csak az LLM képzésével foglalkozna.

Hazánkban jelenleg a legnagyobb nyilvánosan elérhető és magyar nyelvű adatokon képzett modell a Nyelvtudományi Kutatóközpont által készített PULI modellcsalád.

Generatív modellek

A legismertebb ilyen modell a GPT nevezetű LLM, amelyet az OpenAI fejlesztett ki. A GPT-modell előzetes tanítása szintén hatalmas mennyiségű szöveges adattal történt. A GPT-modell generatív jellege azt jelenti, hogy képes új szöveget generálni, amely a tanítóadatokból tanult nyelvi szerkezeteket és jellemzőket követi. A GPT modellek sokoldalúak, és széles körben alkalmazhatók szöveggenerálásra, ember és gép közötti párbeszéd megvalósítására. A GPT előnye, hogy kontextuális reprezentációkat készít az előző szövegrészletek figyelembevételével, és így képes értelmes és koherens szöveg generálására. A 2018-ban megjelent GPT-modell újabb verziókkal bővült, mint a GPT-2, a GPT-3 és a GPT-4o. Ezek egyre nagyobb méretűek és jobbak lettek. A GPT-típusú modellek ma a legjelentősebb és legfejlettebb nyelvi modellek közé tartoznak, és a természetes nyelvfeldolgozással kapcsolatos alkalmazások széles körben használják őket.

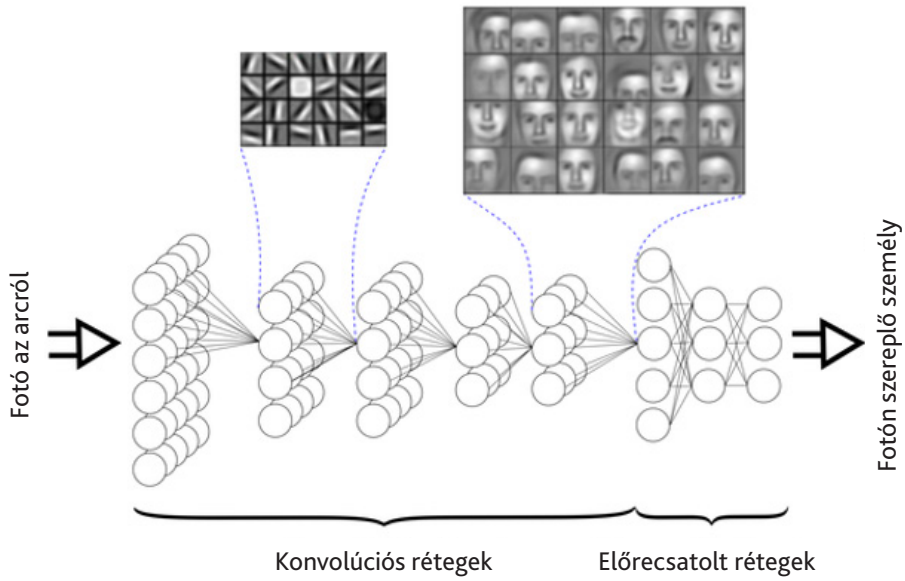
Az LLM-ek segítségével a számítógéppel emberi nyelven tudunk kommunikálni, ami olyan távlatokat nyit meg az ember-gép kommunikációban, amelyek néhány éve még teljesen elképzelhetetlennek tűntek.

Hallucináció

Az LLM-ek többnyire helyes és jó információkat adnak vissza köszönhetően a nagy paraméteres tudásbázisuknak, azonban időnként előfordul, hogy olyan tényeket állítanak, amelyek hihetőnek tűnnek, de ellentmondásosak, vagy éppen nincsenek összhangban a valós tényekkel. A hallucináció fogalma a patológia és a pszichológia területéről ered, és olyan észlelést jelent, amelyben egy entitás vagy esemény jelenik meg, miközben az valójában nem létezik. Az LLM-ek esetén a hallucináció egy olyan jelenség, amikor a generált szöveg értelmetlen, hibás vagy félrevezető. A hallucinációkat két fő csoportra bonthatjuk. Az első a ténybeli ellentmondás, amely során egy állítás valós információkra alapozható, azonban ellentmondásokat tartalmaz. Ilyen például az, amikor egy modellt az izzó feltalálójáról kérdeznek, és az helytelenül Thomas Edisont adja válaszként, aki nem a feltaláló volt, de kapcsolódott az izzóhoz, hiszen tökéletesítette az addigi tervezési eljárást. A másik hallucinációtípus a tények gyártása, amikor a modell olyan tényeket állít, amelyek nem ellenőrizhetők a meglévő tudásunk szerint. Ilyen például, amikor az „Eiffel-torony építésének főbb környezeti hatásairól" kérdezték a modellt, az helytelenül azt állította, hogy „az építkezés a párizsi tigris kihalásához vezetett", pedig ez a faj nem létezik, így ezt az állítást semmilyen történelmi vagy biológiai feljegyzés nem támasztja alá. A hallucináció enyhítésének egyik módja a lekérdezésalapú szöveggenerálás, a RAG, amikor a nyelvi modell nemcsak a belső paraméteres tudására támaszkodik, hanem külső adatforrásokból is felhasznál információkat a válasz generálásához.

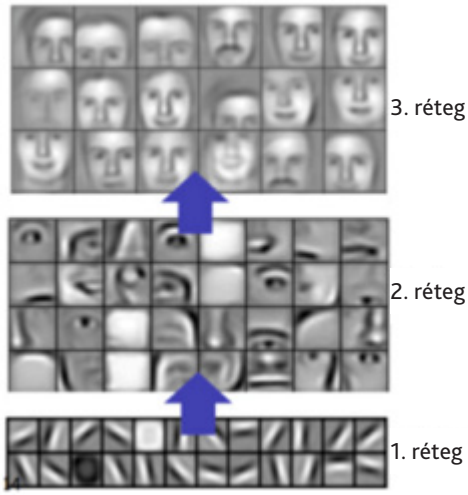
Gépi látás konvolúciós neurális hálózatok segítségével

A számítógépes képfeldolgozási feladatokhoz fejlesztették ki az úgynevezett konvolúciós neurális hálózatokat (CNN), amelyek azon az ötleten alapulnak, hogy a hálózat különböző rétegei a kép egyes vonásait tanulják meg, és ezeket kombinálva annak egyre bonyolultabb részleteit képesek felismerni.



1. ábra: Konvolúciós neurális hálózat
Forrás: Tóth 2016: 945

Ez a folyamat látható az 1. ábrán. A CNN első része a kép tulajdonságait tanulja meg, majd a CNN második része végzi az osztályozási feladatot. A CNN rétegekből áll, és az adatoknak a rétegeken kell keresztülmenni, ami egyben az adatok feldolgozását is jelenti. A CNN első rétege a bemeneti réteg, itt adjuk át az információt a hálózatnak, ami esetünkben egy kép. Az első rétegek még csak egyenes, ferde vonalakat ismernek fel, majd a következő réteg az előzőkből összeálló magasabb szintű jellemzőket képes kinyerni. A konvolúció az információk speciális kivonása a képből. Ezt a folyamatot figyelhetjük meg a 2. ábrán. Általánosságban elmondható, hogy minél több konvolúciós lépést alkalmazunk, annál összetettebb funkciókat képes megtanulni a hálózat. Az egyes rétegek által kinyert funkciókat a későbbiekben a hálózat képes kombinálni, és felismer bonyolult formákat a kép tetszőleges részén. A CNN egyes rétegei a képnek egy sajátos reprezentációját tárolják és tanulják meg.



2. ábra: Konvolúciós neurális hálózat rétegeinek vizualizációja
Forrás: Albawi – Mohammed – Al-Zawi 2017: 1

A gépi látásban is megjelentek a transzformer architektúrák, amit a szakirodalomban *Vision Transformer*nek (ViT) neveznek. Ezek olyan neurális hálózatok, amelyek a transzformer architektúrát alkalmazzák képek elemzésére. A ViT-ek működése és képzése hasonló az LLM-ekhez, azzal a különbséggel, hogy itt a modell bemenetét nem szavak alkotják, hanem a feldolgozandó kép kis részletei. A bemeneti képet kis, nem átfedő téglalapokra bontják. Például ha a kép 224 × 224 pixeles, és egy részlet mérete 16 × 16, akkor a kép 196 részletre lesz felbontva. Analógiát keresve a kép- és szövegfeldolgozás között, ami a szövegfeldolgozásnál egy nagyobb szövegrészlet, az a képfeldolgozásnál a teljes kép, a szavaknak, pontosabban a tokeneknek pedig a kis képrészletek felelnek meg.

Vizuális nagy nyelvi modellek

A vizuális nagy nyelvi modellek (VLLM) olyan transzformeralapú neurális hálózatok, amelyek képesek a képek és szövegek közötti multimodális kapcsolatokat modellezni. Ezek a modellek nagyban hozzájárultak a gépi látás és a természetesnyelv-feldolgozás fejlődéséhez, összekapcsolásához. A VLLM-ek képesek kombinálni és integrálni képi és szöveges adatokat, így képesek az egyik modalitás információinak felhasználására a másik modalitás értelmezésében. A VLLM-ek általában külön egységeket használnak a képek és a szövegek feldolgozására, majd ezeket a reprezentációkat kombinálják. A működésük során a képeket kis részekre bontják, amelyeket beágyaznak, a szövegeket pedig tokenekre (szótöredékekre), amelyeket szintén beágyaznak. Felhasználásuk sokrétű, alkalmasak képeket értelmezni és azokról leiratokat készíteni, kérdésekre válaszolni egy adott kép alapján, képek és szövegek kombinált felhasználásával

osztályozási döntéseket hozni. A VLLM tulajdonképpen a hagyományos nyelvi modell kiegészítése a képi modalitással.

Beágyazások

Szöveges adatok beágyazása: a modern nyelvi modellek egyik közös tulajdonsága a szóbeágyazások használata, ahol szavakat vagy csak szórészleteket sokdimenziós matematikai vektorokká alakítunk át úgy, hogy a vektortérben egymáshoz közel eső szavak jelentése hasonló legyen. A szóbeágyazásnak egyik ismert megvalósítása a Word2Vec eljárás. A Word2Vec mögött meghúzódó alapötlet az, hogy a korpuszban minden szót egyetlen vektor reprezentál, amely az összes kontextus (a közeli szavak) alapján lesz kiszámítva, amelyben a szó előfordul. Ennek a megközelítésnek az intuíciója az, hogy a hasonló jelentésű szavak hasonló kontextusban fordulnak elő. A szavakat reprezentáló beágyazott vektorok nemcsak a szavak jelentését, hanem a szót körülvevő szavak kontextusának a jelentését is megragadják. Amikor dokumentumosztályozást végzünk, tulajdonképpen ezt a beágyazási technikát használjuk fel. Mondatokat vagy akár egész dokumentumokat alakítunk át sokdimenziós vektorokká, és azokat osztályozzuk. A transzformeralapú modellek erőssége, hogy az egyes tokenek (szótöredékek) belső ábrázolása, reprezentálása függ a tokent megelőző tokenektől is. A kódolt reprezentációk így szemantikai és kontextuális információt is hordoznak.

A beágyazás segítségével hatékony keresési megoldásokat lehet készíteni, hiszen a beágyazás révén nemcsak szavak, hanem mondatok, nagyobb szövegegységek közötti jelentésbeli hasonlóságot is tudunk mérni.

Képi adatok beágyazása: a képbeágyazások tulajdonképpen a képek olyan reprezentációi, amelyeket gépi tanulási modellek, például CNN-ek segítségével generálnak. Ezek a vektorok információkat tartalmaznak a képek tartalmáról, stílusáról és struktúrájáról. A CNN-ek szűrők használatával nyerik ki a képek jellemzőit, és ezeket a jellemzőket vektorokká alakítják. A ViT-ek esetében az előbbiekhez hasonlóan a transzformer architektúrából nyerjük ki a beágyazási vektorokat. A képi beágyazásoknál is igaz, hogy hasonló tartalmú képek a vektortérben egymáshoz közel helyezkednek el. Ez teszi lehetővé például a képekkel történő keresést.

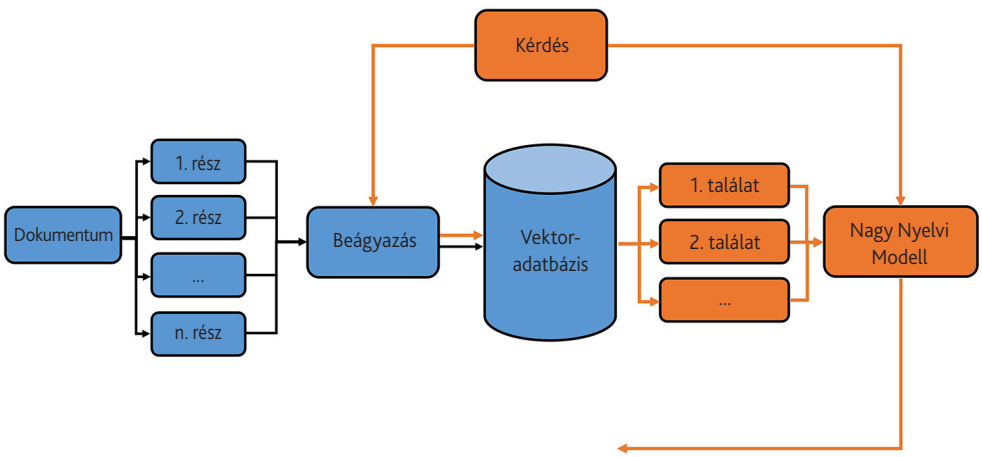
Vektoradatbázisok

A vektoradatbázisok olyan adatbázisrendszerek, amelyek képesek nagy mennyiségű vektoralakú adatot tárolni és hatékonyan lekérdezni. Ezek a rendszerek a gépi tanulás fejlődésével, a beágyazási technikák megjelenésével terjedtek el. Egyik erősségük a szemantikus keresésben rejlik, ahol a hagyományos kulcsszóalapú keresést felváltja a vektorok közötti hasonlóságon alapuló keresés. A hasonlóságot a vektorok közötti távolság (például euklideszi távolság, renuszhasonlóság) alapján határozzuk meg. A vektorok a beágyazásuknál fogva sokkal több információt reprezentálnak, mint a kulcsszavak, ezért a keresés hatékonyabbá vált. A hagyományos keresők csak a pontos egyezéseket találják meg, míg a vektoradatbázisok a keresés során képesek

olyan elemeket is azonosítani, amelyek tartalmilag hasonlók a keresési kifejezéshez, még akkor is, ha a pontos kulcsszavak nem szerepelnek bennük. Ez a módszertan hatalmas előrelépést jelent az olyan területeken, ahol a pontos kulcsszavak meghatározása nehézkes, például a képfelismerésben vagy a komplex szöveges adatok elemzésében. A vektoradatbázisok felhasználási területe ma már széles: képkeresés, hangalapú keresés, szemantikus keresés, témák felderítése, szövegek csoportosítása.

Adatlekérésre alapozott szöveggenerálás

A hallucinációk csökkentésének egyik lehetséges megoldása olyan eljárás, amikor a keresett információt nem a nyelvi modell tanult paraméteres tudásbázisából nyerjük ki, hanem más módszerrel a prompthoz, azaz a nyelvi modell részére átadott szöveghez csatolunk információkat egy külső tudásbázisból. Ezt az eljárást nevezzük adatlekérésre alapozott szöveggenerálásnak, az angol terminológiában RAG-nak. A továbbiakban mi is ezt a RAG elnevezést fogjuk használni.



3. ábra: A RAG folyamata
Forrás: a szerzők szerkesztése

A 3. ábrán láthatjuk a RAG-rendszer működési folyamatait. A feldolgozandó dokumentumokat először részekre tördeljük, egy rész jellemzően néhány száz szót tartalmaz. Az így keletkezett szövegrészleteket beágyazással átalakítjuk sokdimenziós vektorokká, és eltároljuk azokat egy vektoradatbázisban. Amikor kérdést teszünk fel a RAG-rendszernek, akkor a kérdést átalakítjuk a beágyazás segítségével egy nagydimenziós vektor formájába. Ezt követően a kérdésvektorhoz hasonló vektorokat keresünk a vektoradatbázisban. Az így kapott hasonló vektorokat, amelyek egy-egy szövegrészt

reprezentálnak, visszaalakítjuk szöveggé, ezek lesznek a találatok. Amennyiben a kereső jól működik, a visszakapott találatok ténylegesen kapcsolódnak a kérdéshez. Ezeket a találatokat pedig átadjuk az eredeti kérdéssel együtt a nyelvi modellnek, amely választ generál a kérdésünkre. Egy RAG segítségével felépített rendszer esetén az LLM-nek azt a tudását használjuk elsősorban, amely a promptból képes információkat feldolgozni. Erre lehet egy példa, amikor a Wikipediát mint külső tudásbázist használjuk például Zrínyi Miklóssal kapcsolatos kérdés megválaszolására. Első lépésben a Wikipediát le kell tölteni, fel kell darabolni, és a szövegrészleteket be kell ágyazni, majd eltárolni egy vektoradatbázisban. A RAG-rendszer a kérdésből („Mikor született Zrínyi Miklós?") megkeresi a számára elérhető adatokat Zrínyi Miklósról a vektoradatbázisból, majd ezeket az információkat becsomagolja a promptba. A nyelvi modellnek pedig a kérdésből és a Zrínyi Miklósról átadott információkból kell választ generálnia.[3]

Egy gyakorlati alkalmazás bemutatása hadtudományi témában

LLM-ek a védelmi szférában

A műveletek támogatása kapcsán paradigmaváltás zajlik, hiszen a mesterséges intelligencia olyan adatokon alapuló döntés-előkészítési lehetőségekkel bír, amelyek korábban elképzelhetetlenek voltak. A védelmi szférában nagyon sok írott szöveges formában elérhető dokumentum keletkezik. Ezek a dokumentumok rendkívül jelentős tudást és rengeteg értékes információt reprezentálnak. A dokumentumok jelentős része a védelmi és biztonsági megfontolások alapján nyilvánosan nem elérhető. Ezeknek az adatoknak a feldolgozása, tudásreprezentációk kialakítása kizárólag teljesen ellenőrzött körülmények között lehetséges, azaz nem engedélyezhető, hogy az interneten elérhető – például Chat GPT, Gemini vagy más hasonló – rendszerek részére ezekből az adatokból bármi is átadható legyen. Amennyiben ezt a megszorítást elfogadjuk, úgy kénytelenek vagyunk saját, a védelmi szféra egyes résztvevői számára külön-külön megoldásokat létrehozni.

Gyakorlati alkalmazás

Képzeljünk el egy olyan szituációt, ahol nagy mennyiségű szöveges, képi és akár hanginformációt, például rádióüzeneteket, műholdfelvételeket, drónfelvételeket és jelentéseket kell feldolgozni. Ezek az adatok különböző forrásokból származnak, különböző formátumban érkeznek, és gyors feldolgozásuk kritikus a döntéshozatali folyamatban.

A feldolgozás lépései: Adatfeldolgozás során a különböző formátumú adatokat (szöveg, kép) egységes formátumba kell konvertálni. Az adatokból vektoros reprezentációkat kell létrehozni és tárolni egy nagy teljesítményű vektoradatbázisban. Ez lehetővé teszi a gyors és hatékony keresést a hasonlóságon alapuló lekérdezések segítségével.

[3] Ram 2023.

RAG-alkalmazási példa lehet, ahol az értékelő-elemző egy komplex kérdést tesz fel: „Milyen katonai tevékenységet észleltek az elmúlt 24 órában X település környékén, figyelembe véve a rendelkezésre álló műhold- és drónfelvételeket, valamint a lehallgatott rádióüzeneteket?" A RAG-rendszer a kérdést vektorizálja, és a vektoradatbázisban megkeresi a legrelevánsabb szöveges és képi információkat. Ezeket az információkat összegyűjti, és egy LLM-nek adja át, amely egy koherens és informatív jelentést generál az elemző számára. A RAG-rendszer minimalizálja a hallucináció kockázatát, mivel a válasz közvetlenül az adatokon alapul.

LLM-ek a hadtudományban

A hadtudományban nagyon jelentős szerepe van az írásbeliségnek, hiszen a hadtudományhoz szorosan köthető a dokumentálás mint az ismeretek felhalmozásának egyik formája. Ez a jelentős írásbeli tudásanyag, amennyiben digitalizált formában is elérhető, kiváló alapot adhat egy nyelvi modell finomhangolásához egy adott szakterületen.

Az MI katonai alkalmazása számos etikai kérdést is felvet. Kiemelt figyelmet kell fordítanunk az emberi kontroll biztosítására, a dehumanizáció elkerülésére és az igazságos háború elmélete elveinek betartására. Az MI alkalmazásának átláthatónak és indokoltnak kell lennie, és az MI-t irányító embereknek kell felelősséget vállalniuk az MI által végrehajtott műveletekért. A kockázatkerülő háború fogalmi rendszere is összefügg az MI-vel, hiszen a technológia egyik célja a katonákra leselkedő kockázatok csökkentése, a veszteségek minimalizálása.[4]

A rendelkezésünkre álló hadtudománnyal kapcsolatos szövegek segítségével a nyelvi modell szert tehet olyan ismeretekre, amelyek erre a tudásbázisra épülnek. Egy kellően nagy nyelvi modellben[5] már kialakultak bizonyos érvelési képességek, amelyek a tanult tudásbázis alapján képesek lehetnek koherens és következetes válaszokat adni bizonyos kérdésekre. Az ilyen modellek nagyon gyorsan képesek releváns információk összegyűjtésére és azokból stratégiai, taktikai döntéseket előkészítő anyagok létrehozására.

A védelmi szektorban gyakran előfordulnak olyan „Szigorúan titkos", „Titkos", „Bizalmas" vagy „Korlátozott terjesztésű" dokumentumok, amelyeknek a tudásanyagára támaszkodnunk kell, azonban nem lehetséges azokat vagy azoknak valamely részhalmazát egy külső fél tudomására hozni. Gondolhatunk stratégiai tervdokumentációkra, védelmi folyamatleírásokra stb. Ezekben az esetekben teljesen zárt és hozzáférés-kontrollált rendszerekben kell gondolkodnunk.

A fentiek alapján az MI és az LLM-ek nem csupán a hadtudomány elméleti megközelítését változtatják meg, hanem a gyakorlati alkalmazásokban is forradalmi újításokat hoznak.

[4] Boda 2024.
[5] Wei 2022.

Zárt információkereső rendszer

A védelmi szférában is működőképes rendszer kialakítása megköveteli, hogy akár hálózati kapcsolat nélkül is működő okos információkereső rendszert alakítsunk ki. Az információk visszakeresése túlmutat egy egyszerű keresőmotoron, amely a kérdésre csak találatokat ad. A mai technológiai lehetőségek lehetővé teszik, hogy a kérdésekre válaszokat kapjunk, ami felgyorsítja a munkafolyamatainkat azáltal, hogy a keresést és az eredmények szintetizálását egy program elvégzi helyettünk.

Egy zárt információs rendszert készítettünk el teljesen nyílt forráskódú szoftverekkel, és a *Hadtudomány* folyóirat 29–34. évfolyamok közötti számaiból 234 cikket használtunk fel a vektoros adatbázis készítéséhez. A cél az volt, hogy modellezzük nagy mennyiségű tudásanyag feldolgozását és tárolását egy zárt környezetben, majd abból kérdések alapján releváns információkat nyerjünk ki RAG segítségével, és válaszokat készítsünk nyelvi modellek felhasználásával.

A rendszert a GitHub[6] kódtárban is elérhető Open-WebUI[7] keretrendszerre építettük fel. A szövegek beágyazására használt modult magyar nyelvű szövegeken finomhangoltuk,[8] generálásukhoz pedig a LLama 3.1 8B[9] utasításkövető modelljét használtuk. A teljes rendszert Ubuntu Linux[10] operációs rendszerre telepítettük. A megfelelő sebességű működéshez szükséges egy GPU[11] is, Nvidia RTX 3090-est használtunk a projekthez.

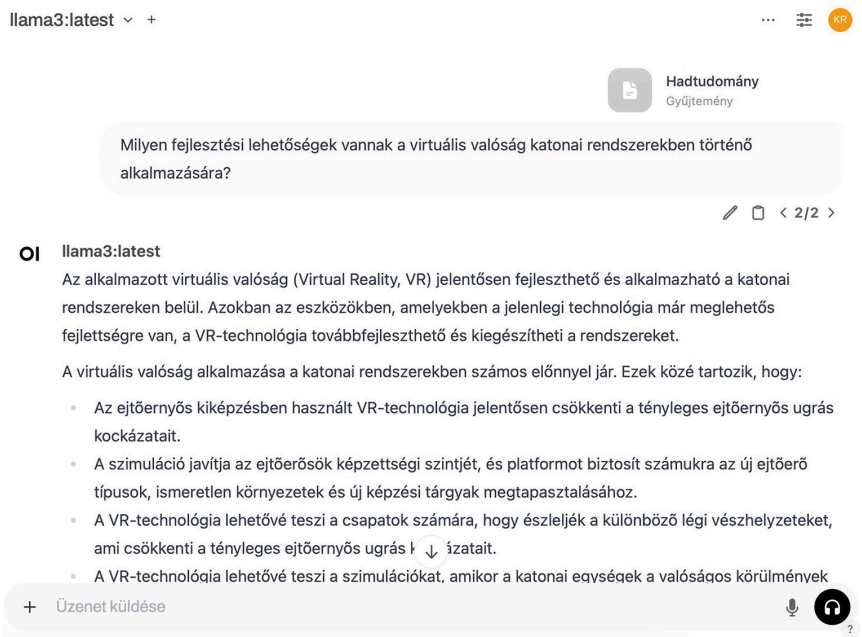
Az így létrejött rendszer az internettől teljesen függetlenül is képes működni és releváns válaszokat adni teljesen specifikus kérdésekben is, amelyekre a válaszadáshoz szükséges tudásanyag csak helyi gépen található meg. A válaszadáshoz semmilyen információ nem kerülhet ki, hiszen a választ generáló nyelvi modell is a helyi gépen fut.

A 4. ábrán láthatjuk a keresőrendszer felületét, ahol a keresőbe beírt kérdést, utasítást válaszolja meg, hajtja végre a rendszer. A válaszát a RAG rendszerbe feltöltött dokumentumok alapján készíti el, megadva a válaszhoz felhasznált dokumentumokat.

A kérdés a következő volt: „Milyen fejlesztési lehetőségek vannak a virtuális valóság katonai rendszerekben történő alkalmazására?"

Válasz: „Az alkalmazott virtuális valóság (Virtual Reality, VR) jelentősen fejleszthető és alkalmazható a katonai rendszereken belül. Azokban az eszközökben, amelyekben a jelenlegi technológia már meglehetős fejlettségre van, a VR-technológia továbbfejleszthető és kiegészítheti a rendszereket.

[6] Lásd: https://github.com
[7] Lásd: https://github.com/open-webui/open-webui
[8] Lásd: https://huggingface.co/karsar/paraphrase-multilingual-MiniLM-L12-hu-v2
[9] Lásd: https://huggingface.co/meta-llama/Llama-3.1-8B-Instruct
[10] Lásd: https://ubuntu.com/
[11] Graphics Processing Unit.



4. ábra: Zárt információkereső rendszer
Forrás: a szerzők felvétele

A virtuális valóság alkalmazása a katonai rendszerekben számos előnnyel jár. Ezek közé tartozik, hogy:

- Az ejtőernyős kiképzésben használt VR-technológia jelentősen csökkenti a tényleges ejtőernyős ugrás kockázatait.
- A szimuláció javítja az ejtőerősök képzettségi szintjét, és platformot biztosít számukra az új ejtőerő típusok, ismeretlen környezetek és új képzési tárgyak megtapasztalásához.
- A VR-technológia lehetővé teszi a csapatok számára, hogy észleljék a különböző légi vészhelyzeteket, ami csökkenti a tényleges ejtőernyős ugrás kockázatait.
- A VR-technológia lehetővé teszi a szimulációkat, amikor a katonai egységek a valóságos körülmények között gyakorolnak.

Ezek mellett a virtuális valóság alkalmazása a katonai rendszerekben továbbfejleszthető és kiegészítheti a rendszereket, például:

- A digitális katona program, amely a honvédek egyéni felszerelésének átfogó modernizálását célozza.
- A robototechnológia, amely a robotoknak olyan képességeket ad, hogy meg tudják oldani bizonyos feladatokat, például a szimulációban.
- Az autonóm csapásmérő eszközök, amelyek olyan képességekkel rendelkeznek, hogy megszerezhetik a céljaikat a valóságos körülmények között.

A virtuális valóság alkalmazása a katonai rendszerekben számos lehetőség és előnyt tartalmaz. Azonban, ahhoz, hogy ezt a fejlesztését megvalósítsuk, szüksége van olyan erőforrásokra, amelyekkel a rendszereket kiegészítik és fejlesztik tovább."

A válasz elkészítéséhez a következő forrásanyagokat használta fel a rendszer:

1. forrás: 12266-Cikk szövege-52251-1-10-20230804.pdf
Relevancia: 66.18%(0.6618)
Tartalom: „HADMÛVÉSZET Négyesi Imre/c71 A virtuális valóság technológia alkalmazásának lehetőségei a katonai készségfejlesztésben* DOI 10.17047/HADTUD.2023.33.2.3 …"
2. forrás: 9734-Cikk szövege-44567-1-10-20230207.pdf(oldal 6)
Relevancia: 56.52%(0.5652)
Tartalom: „–robothadviselés és robottechnológia; –digitális katona program; –autonóm csapásmérő eszközök; –kvantum számítástechnika; –szimulációs, virtuális és kiterjesztett valóság. …"
3. forrás: 6780-Cikk szövege-28285-1-10-20210713.pdf(oldal 16)
Relevancia: 56.12%(0.5612)
Tartalom: „A Digitális Katona Program a honvédek egyéni felszerelésének átfogó modernizálását célozza. Kiemelkedõen fontos eleme a programnak, hogy ahol kivitelezhetõ, ott a rendszerelemek kutatás -fejlesztése és gyártása a hazai védelmi ipar bevonás ával valósuljon meg. …"

A források tartalmi elemei nem teljes körűek a fenti idézetekben.

A kérdésre adott válasz nem tökéletes, csak egy résszel foglalkozik, illetve számos helyesírási hibát is tartalmaz. A válasz nagyban függ a rendszer beállításaitól, hogy hány forráscikket használjon, milyen hosszú legyen a válasz, illetve fontos paraméterek a vektros adatbázis létrehozásánál a kontextusméret, átfedés. A bemutatott kérdés-válasz páros hoz tartozó válasz további beállításokkal finomítható, változtatható.

Összefoglalás, következtetések

Összefoglalás

Ez a tanulmány a mesterséges intelligencia, különösen az LLM-ek és a gépilátásrendszerek alkalmazásának lehetőségeit és kihívásait vizsgálta a védelmi szférában. Részletesen bemutattuk a nyelvi modellek működését, képzési folyamatait, valamint a generatív modellek képességeit és korlátait, mint például a hallucináció jelensége. A képfeldolgozás terén a legkorszerűbb modellek, valamint a VLLM-ek lehetőségeit elemeztük. Kitértünk a vektorbeágyazások és vektoradatbázisok jelentőségére a hatékony információkeresés és feldolgozás szempontjából, valamint az adatlekérésre alapozott szöveggenerálás technikájának szerepére a hallucinációk csökkentésében. Tanulmányunk rámutatott az LLM-ek képzésének jelentős költségigényére és a jelenlegi magyarországi

lehetőségekre. Az LLM-ek alkalmazása nemcsak az általános szöveges feladatokban, hanem a speciális területeken, például a hadtudományban is komoly potenciált rejt. Konklúzióként kijelenthetjük, hogy az LLM-ek és a gépilátás-rendszerek alkalmazása paradigmaváltást hozhat a katonai műveletek támogatásában, azonban a bizalmas adatok védelme érdekében elengedhetetlen egy saját, biztonságos, zárt informatikai infrastruktúra kiépítése, a megfelelő szakértelem fejlesztése és a folyamatos innováció. A védelmi szektor számára tehát egy hosszú távú, jelentős beruházást igénylő projekt megvalósítása válik szükségessé a biztonság érdekében.

Következtetések

A műveletek támogatása kapcsán paradigmaváltás zajlik, hiszen a mesterséges intelligencia olyan adatokon alapuló döntés-előkészítési lehetőségekkel bír, amelyek korábban elképzelhetetlenek voltak. A védelmi szférában nagyon sok írott szöveges és képi formában elérhető dokumentum keletkezik. Ezek a dokumentumok jelentős tudást és rengeteg értékes információt reprezentálnak. A dokumentumok jelentős része a védelmi és biztonsági megfontolások alapján nyilvánosan nem elérhető. Ezeknek az adatoknak a feldolgozása, tudásreprezentációk kialakítása kizárólag teljesen ellenőrzött körülmények között lehetséges, azaz nem engedélyezhető, hogy az interneten elérhető rendszerek (például Chat GPT, Gemini stb.) ezekből az adatokból bármihez is hozzáférjenek. Amennyiben ezt a megszorítást elfogadjuk, úgy kénytelenek vagyunk saját, a védelmi szféra egyes résztvevői számára külön-külön megoldásokat létrehozni.

Véleményünk szerint el kell kezdenünk kiépíteni azokat a saját védelmi informatikai infrastruktúrákat, amelyek képesek feldolgozni és kezelni a védelmi szektorban található adatokat. Ez a kiépítés több szempontból is komplex feladat. Első lépésben egy olyan biztonságos, zárt környezetet kell létrehoznunk, amely megfelel a legmagasabb szintű adatvédelmi és biztonsági előírásoknak. Ez magában foglalja a fizikai biztonságot, a hálózati biztonságot, valamint az adat titkosítását és hozzáférés-szabályozását. A rendszernek skálázhatónak kell lennie, hogy képes legyen kezelni a folyamatosan növekvő adatmennyiséget, és rugalmasnak, hogy alkalmazkodni tudjon a változó igényekhez. A technológiai infrastruktúra mellett elengedhetetlen a megfelelő szakértelem biztosítása is. Képzett adattudósokra, biztonsági szakértőkre és rendszergazdákra van szükség, akik képesek a rendszer üzemeltetésére, karbantartására és folyamatos fejlesztésére. Ezenfelül a különböző védelmi szervek közötti együttműködés és adatmegosztás is kritikus fontosságú, ami standardizált adatformátumok és protokollok bevezetését követeli meg. A különböző rendszerek integrációja is jelentős kihívás lehet, és gondos tervezést igényel. Hosszú távon pedig a folyamatos fejlesztés és innováció biztosítása a legfontosabb. A mesterséges intelligencia gyors fejlődése miatt folyamatosan figyelemmel kell kísérni az új technológiákat, és be kell építeni azokat a rendszerbe, amennyiben növelik a hatékonyságot és a biztonságot. Ez a folyamatos fejlesztés azonban csak megfelelő finanszírozás és szakmai támogatás mellett valósulhat meg. A védelmi szféra számára tehát egy hosszú távú, jelentős beruházást igénylő projekt elindítása válik szükségessé, amelynek sikeressége a nemzeti biztonság szempontjából is rendkívül fontos.

Felhasznált irodalom

Albawi, Saad – Mohammed, Tareq Abed – Al-Zawi, Saad (2017): Understanding of a Convolutional Neural Network. *2017 International Conference on Engineering and Technology (ICET),* Antalya, Turkey, 1–6. Online: https://doi.org/10.1109/ICEngTechnol.2017.8308186

Birhane, Abeba et al. (2021): Science in the Age of Large Language Models. *Nature Reviews Physics,* 5, 277–280. Online: https://doi.org/10.1038/s42254-023-00581-4

Boda Mihály (2024): A kockázatkerülő háború és a bátorság a 20–21. század fordulóján. *Honvédségi Szemle,* 152(3), 113–125. Online: https://doi.org/10.35926/HSZ.2024.3.9

Brown, Tom B. et al. (2020): *Language Models are Few-Shot Learners.* Online: https://doi.org/10.48550/arXiv.2005.14165

Devlin, Jacob et al. (2018): BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding. Online: https://arxiv.org/abs/1810.04805

Filippova, Katja (2020): Controlled Hallucinations: Learning to Generate Faithfully from Noisy Data. In Cohn, Trevor – He, Yulan – Liu, Yang (szerk.): *Findings of the Association for Computational Linguistics EMNLP 2020.* [H. n.]: Association for Computational Linguistics, 864–870. Online: https://doi.org/10.18653/v1/2020.findings-emnlp.76

Huang, Lei et al. (2025): A Survey on Hallucination in Large Language Models: Principles, Taxonomy, Challenges, and Open Questions. *ACM Transactions on Office Information Systems,* 43(2), 1–55. Online: https://doi.org/10.1145/3703155

Jurafsky, Daniel – Martin, James H. (2023): N-gram Language Models. In Jurafsky, Daniel – Martin, James H.: *Speech and Language Processing: An Introduction to Natural Language Processing, Computational Linguistics, and Speech Recognition.* Third Edition draft. [H. n.]: [k. n.], 31–57. Online: https://web.stanford.edu/~jurafsky/slp3/3.pdf

Kukreja, Sanjaj et al. (2023): Vector Databases and Vector Embeddings-Review. In *2023 International Workshop on Artificial Intelligence and Image Processing (IWAIIP).* Online: https://doi.org/10.1109/IWAIIP58158.2023.10462847

Lewis, Patrick (2020): Retrieval-Augmented Generation for Knowledge-Intensive NLP Tasks. In Larochelle H. et al. (szerk): *Advances in Neural Information Processing Systems 33 (NeurIPS 2020).* Online: https://arxiv.org/pdf/2005.11401

Luccioni, Aleksandra Sasha – Viguier, Sylvain – Ligozat, Anne-Laure (2023): Estimating the Carbon Footprint of BLOOM, a 176B Parameter Language Model. *Journal of Machine Learning Research,* 24, 1–15. Online: https://doi.org/10.48550/arXiv.2211.02001

Mikolov, Thomas et al. (2013): *Efficient Estimation of Word Representations in Vector Space.* Online: https://arxiv.org/pdf/1301.3781

Pan, James Jie et al. (2024): Vector Database Management Techniques and Systems. In *SIGMOD '24: Companion of the 2024 International Conference on Management of Data.* New York: Association for Computing Machinery, 597–604. Online: https://doi.org/10.1145/3626246.3654691

Ram, Ori et al. (2023): *In-Context Retrieval-Augmented Language Models.* Online: https://doi.org/10.1162/tacl_a_00605
Stiennon, Nisan et al. (2020): *Learning to Summarize From Human Feedback.* Online: https://arxiv.org/pdf/2009.01325
Tóth Bálint Pál (2016): Beszélő számítógépek mély gondolatokkal. Neurális hálózatok. *Élet és Tudomány,* 71(30), 944–946.
Touvron, Hugo et al. (2023): *LLaMA: Open and Efficient Foundation Language Models.* Online: https://doi.org/10.48550/arXiv.2302.13971
Vaswani, Ashish et al. (2017): Attention Is All You Need. *Advances in Neural Information Processing Systems,* 5998–6008. Online: https://arxiv.org/pdf/1706.03762.pdf
Wei, Jason et al. (2022): *Emergent Abilities of Large Language Models.* Online: https://doi.org/10.48550/arxiv.2206.07682
Yang, Min et al. (2021): DOLG: Single-Stage Image Retrieval With Deep Orthogonal Fusion of Local and Global Features. In *Proceedings of the IEEE/CVF International Conference on Computer Vision.* 11772–11781. Online: https://doi.org/10.1109/ICCV48922.2021.01156
Yang Zijian Győző et al. (2023): Jönnek a nagyok! BERT-Large, GPT-2 és GPT-3 nyelvmodellek magyar nyelvre. In *XIX. Magyar Számítógépes Nyelvészeti Konferencia,* 247–262. Online: https://acta.bibl.u-szeged.hu/78417/1/msznykonf_019_247-262..pdf
Zhang, Shengyu et al. (2023): *Instruction Tuning for Large Language Models: A Survey.* Online: https://doi.org/10.48550/arXiv.2308.10792
Zhou, Chunting et al. (2023): *LIMA: Less Is More for Alignment.* Online: https://doi.org/10.48550/arXiv.2305.11206

HADMÉRNÖK
VÉDELEMINFORMATIKA
20. évfolyam (2025) 2. szám 93–111.
DOI: 10.32567/hm.2025.2.6

Krasznay Csaba[1]

Az űr és a kibertér mint műveleti terek konvergenciája az orosz–ukrán háború tükrében[2]

The Convergence of Space and Cyberspace as Operational Domains in the Light of the Russian–Ukrainian War

Absztrakt

A világűr és a kibertér egyre szorosabb összefonódása jelentős kiberbiztonsági kihívásokat eredményez mind az állami, mind a magánszereplők számára. Jelen tanulmány 47 tudományos publikáció szisztematikus elemzésével azonosítja az űrkiberbiztonság fő tematikus klasztereit. A szövegalapú klaszterezés eredményeként hat meghatározó kutatási terület körvonalazódik: 1) kiberbiztonsági irányítás és stratégia; 2) jogi és szabályozási keretek; 3) az űr mint hadszíntér; 4) az orosz–ukrán háború tanulságai; 5) a magánszektor szerepe az űrkiberbiztonságban; valamint 6) technikai kiberfenyegetések és kiberreziliencia. Az elemzés rávilágít arra, hogy míg a nemzetközi kutatások száma növekszik, a témában magyar nyelven még nem jelent meg mélyreható tudományos publikáció. Tekintettel arra, hogy Magyarország és egyes magyar vállalatok deklaráltan rendelkeznek űrtechnológiai ambíciókkal, a jelen téma hazai kutatása indokolt. A tanulmány hozzájárul ennek a hiánynak a pótlásához, valamint rendszerezett áttekintést nyújt az űrkiberbiztonság kutatási trendjeiről és a további vizsgálatokat igénylő területekről.

Kulcsszavak: űrkiberbiztonság, orosz–ukrán háború, kiberműveletek, kiberreziliencia

[1] Egyetemi docens, Nemzeti Közszolgálati Egyetem ÁNTK Kiberbiztonsági és E-közigazgatási Tanszék, e-mail: krasznay.csaba@uni-nke.hu

[2] A tanulmány a Bolyai János Kutatási Ösztöndíj támogatásával készült.

Abstract

The increasing integration of space and cyberspace has led to significant cybersecurity challenges for both governmental and commercial actors. This study systematically analyses 47 academic publications to identify the key thematic clusters in space cybersecurity research. Through text-based clustering, six distinct research domains emerge: (1) cybersecurity governance and strategy, (2) legal and regulatory frameworks, (3) space as a theater of war, (4) cybersecurity lessons from the Russia–Ukraine war, (5) private sector involvement in space cybersecurity, and (6) technical cyber threats and resilience. The analysis highlights that while international research on space cybersecurity is growing, there is a notable absence of Hungarian-language academic publications on this topic. However, given the declared ambitions of Hungary and some Hungarian companies in space technology, domestic research on this topic is justified. The study contributes to bridging this gap by providing a structured overview of space cybersecurity research trends and identifying key areas for future investigations.

Keywords: space cybersecurity, Russia–Ukraine war, cyber operations, cyber resilience

Bevezetés

Az orosz–ukrán háború 2022. február 24-i nyílt fegyveres összecsapását számos kibertéri művelet előzte meg, illetve ezek a támadások azóta is folyamatosan megjelennek mindkét hadviselő fél oldalán. Az offenzív műveletek kiemelt célpontjai az egyes kritikus információs infrastruktúrák, amelyek közül az egyik példa az űrtávközlést megvalósító információs rendszerek, azaz a műholdak és az azokkal kommunikáló földi állomások, legyenek azok akár irányítóközpontok, akár végpontok. Habár az űreszközök kiemelt szerepe a hadviselésben nem újdonság, ez az első olyan háború, ahol az űreszközök biztonsága kiberbiztonsági szempontból kérdőjeleződik meg. A függés pedig kölcsönös, hiszen a harctéren használt informatikai eszközök működése igen gyakran az űrtávközlést megvalósító eszközöktől függ. Ez tehát azt jelenti, hogy a katonai kiberműveleteknek hatása van az űrben levő, katonai célokat is támogató eszközökre, példát mutatva a multidomén-műveletek egy, a magyar nyelvű szakirodalomban kevéssé tárgyalt esetére.

Míg a tengerészeti rendszerek (tehát a tenger mint műveleti tér) és a légi közlekedés (tehát a légtér mint műveleti tér) kiberfüggősége már évek óta vizsgált terület, az űr és a kibertér műveleti tér konvergenciájára aránylag kevés figyelmet fordítottak eddig a kutatók és a műveleti tervezők. Kutatási kérdésem, hogy a hadtudományban mérvadó szakirodalom milyen összefüggéseket állapított meg a két műveleti térrel kapcsolatban, mi a jelenlegi *state-of-the-art* ezen a területen az orosz–ukrán háború tapasztalatai alapján. Hipotézisem szerint a háborús tapasztalatok olyan új impulzusokat adtak a tudományos diskurzusnak, amelyek következtében új, jól körülhatárolható, korábban nem, vagy csak kevéssé kutatott tudományos tématerületek jöttek létre. Kutatásom során tudományos módszertanként szakirodalmi kutatást végzek, amelynek során feltárom a releváns tanulmányokat, és azok klaszterelemzésével támasztom alá a hipotézisemet.

Esettanulmányok az orosz–ukrán háborúból

Az űr és a kibertér konvergenciájának fontossága három jól dokumentált esettanulmányon keresztül mutatható be az orosz–ukrán háború kapcsán. Ezek a ViaSat műholdas szolgáltató elleni támadás, a Starlink műholdas távközlési rendszer felhasználása az ukrán védelmi műveletek során, illetve a GPS-jelek zavarása nemcsak a műveleti területen, hanem a Baltikum jelentős részén is.

A ViaSat szolgáltató elleni kibertámadást 2022. február 24-én, közvetlenül az orosz–ukrán háború kezdete előtt hajtották végre. A kiberművelet következtében jelentős hálózati kiesés történt, amely az ukrán katonai kommunikációt is érintette. A támadás célpontja a KA-SAT műholdhálózat földi szegmense volt, amelyet a támadók kompromittáltak. Az incidens több ezer, nem csak katonai védelmi rendszerben használt végfelhasználói modemet érintett, amelyek a támadás következtében használhatatlanná váltak. Az Európai Űrügynökség és az amerikai hírszerző ügynökségek vizsgálatai megállapították, hogy a támadás egy előre megtervezett kiberművelet része volt, amelyet az orosz összhaderőnemi támadás részeként kell értelmezni.

A támadás technikai aspektusait vizsgálva kiderült, hogy egy úgynevezett *wiper,* azaz adattörlő típusú rosszindulatú szoftvert használtak, amely a KA-SAT modemek memóriáját törölte, így azok újraindítás után sem tudtak csatlakozni a hálózathoz. A támadók a földi hálózati infrastruktúrát kompromittálták, és egy frissítési csatornán keresztül terjesztették a kártékony szoftvert. A támadás során nem közvetlenül a műholdakat vették célba, hanem azokat az eszközöket, amelyek a felhasználók és a műholdak közötti kapcsolatot biztosították.[3]

A támadás elsődleges tanulsága az volt, hogy noha közismert tény, hogy a műholdas kommunikáció kulcsfontosságú infrastruktúra, amely sérülékeny lehet kibertámadásokkal szemben, különösen katonai konfliktusok esetén, a szolgáltatók nem rendelkeznek megfelelő kibervédelemmel. Az incidens egyben rávilágított a műholdas rendszerek biztonságának és a beszállítói lánc védelmének fontosságára, rámutatva, hogy a saját űrképességekkel nem rendelkező országok mennyire kitettek a polgári űrtávközlésnek. A támadás után több szervezet, köztük a NATO, az EU és az amerikai kormány, fokozta a műholdas kommunikáció biztonságára vonatkozó intézkedéseit, hogy csökkentse a jövőbeni hasonló fenyegetések kockázatát, ezek megvalósítása azonban több évet vesz igénybe.

A ViaSat-támadás után a Starlink műholdas internetrendszere kulcsszerepet játszott az ukrajnai háborúban, amikor 2022 februárjában, az orosz invázió kezdetén az ukrán kormány sürgős segítséget kért a kommunikációs infrastruktúra fenntartására. Elon Musk vállalata, a SpaceX rövid időn belül több ezer Starlink-terminált biztosított Ukrajna számára, lehetővé téve az ország katonai, kormányzati és civil szervezetei számára a folyamatos internet-hozzáférést. Az első egységek néhány napon belül megérkeztek, és a hálózat gyors telepítésével az ukrán hadsereg sikeresen fenntartotta a műveleti kommunikációt, miközben az orosz csapatok megsemmisítették vagy zavarták a hagyományos telekommunikációs infrastruktúrát.

[3] Boschetti–Gordon–Falco 2022.

A Starlink rendszere különösen a harctéren bizonyult nélkülözhetetlennek, mivel biztosította a drónműveletek vezérlését, a titkosított katonai kommunikációt és az ukrán erők koordinációját. A rendszer egyik előnye a hagyományos infrastruktúrával szemben az volt, hogy decentralizált és nehezebben támadható. Habár az orosz hadsereg több alkalommal is megpróbálta zavarni a Starlink műholdjeleit és kibertámadásokat indított a földi terminálok ellen, a SpaceX folyamatos frissítésekkel gyorsan reagált a fenyegetésekre. 2022 májusára több mint 10 000 Starlink-egységet használtak Ukrajnában, és ez a szám tovább növekedett a háború során.[4]

A Starlink katonai alkalmazása geopolitikai kérdéseket is felvetett, mivel egy magánvállalat közvetlen hatással volt egy háborús konfliktus menetére. 2023-ban Elon Musk elismerte, hogy a SpaceX korlátozott hozzáférést vezetett be a Starlink használatára bizonyos hadműveleteknél, például a Krím közelében végrehajtott támadások során. Ez rávilágított arra, hogy a kritikus kommunikációs infrastruktúra egy magánvállalat kezében stratégiai döntéseket befolyásolhat. Az ukrajnai eset tanulságai alapján egyre nagyobb figyelem irányul arra, hogy a modern hadviselésben milyen szerepet játszanak a magántulajdonban lévő technológiák, és milyen szabályozásokra lehet szükség a jövőben.

A GPS-jelek zavarása rendszeres problémává vált konfliktuszónákban, különösen az orosz–ukrán háborúban. Orosz egységek különböző elektronikai hadviselési eszközökkel bocsátanak ki elektromágneses impulzusokat, amelyek rontják a GPS-jel minőségét. Noha a GPS-alapú amerikai katonai műveletekre ez nem gyakorolt jelentős hatást, az Egyesült Államok dollármilliókat költött arra, hogy megvédje kommunikációs infrastruktúráját az orosz kibertámadásokkal és GPS-zavarásokkal szemben.

A GPS-alapú ukrán drónműveletek szintén kevéssé érintettek, mivel ezek képesek olyan területeken támadni, ahol nincsenek aktív orosz földi zavaróeszközök, illetve egyre jobban elterjednek a mesterséges intelligencia által vezérelt autonóm csapások, valamint sok esetben optikai szállal vezetik a drónokat. Az ukrán erők emellett a Starlink műholdrendszeren keresztül hatékonyan kommunikálnak és koordinálják csapásaikat. Ezzel szemben a polgári GPS-jelek zavara különösen nagy hatással érinti a légi közlekedést, és már előfordult, hogy repülőgépeket más repülőtérre kellett átirányítani, mert nem tudták biztonságosan végrehajtani a leszállást. Az Európai Repülésbiztonsági Ügynökség (EASA) 2022. március 17-én figyelmeztetést adott ki a műholdas navigációs zavarok miatt, és négy érintett régiót azonosított: Kalinyingrád, Kelet-Finnország, a Fekete-tenger és Észak-Irak.

A GPS-zavarás a régióban nem új jelenség, Oroszország már a 2014-es krími konfliktus óta alkalmazza ezt a taktikát, különösen kelet-ukrajnai területeken. 2017-ben a Fekete-tengeren 20 hajó fedélzeti rendszere mutatott hamis helyzetadatokat, és egy 2016 óta végzett elemzés szerint több mint 9800 esetben manipulálták a jeleket, érintve 1300 kereskedelmi hajót. Az ilyen beavatkozások nemcsak katonai műveleteket, hanem kereskedelmi és humanitárius feladatokat, például kutató-mentő műveleteket is akadályozhatnak. Az Egyesült Államok és

[4] Abels 2024.

az Európai Unió egyaránt aggódik a GPS-alapú rendszerek biztonsága miatt, különösen a Galileo rendszer 2019-es részleges leállása óta, ami rávilágított a műholdas infrastruktúra védelmének fontosságára.[5]

Szakirodalmi áttekintés és klaszterelemzés

A kiberbiztonság és az űrtevékenységek metszéspontja egyre nagyobb figyelmet kap a szakirodalomban. Annak érdekében, hogy látható legyen, milyen módon reagált a tudományos közösség az orosz–ukrán háború tapasztalataira, tematikus irodalomkutatást végeztem. Ennek során a célom az volt, hogy a mérvadó tudományos forrásokból felleljem a 2022 és 2025 közötti azon publikációkat, amelyek ezzel a témával foglalkoznak. Kulcsszavas keresés segítségével ezért átnéztem a Magyar Tudományos Művek Tárát, a Google Scholart, a ResearchGate-et, valamint a Nemzeti Közszolgálati Egyetem által előfizetett tudományos adatbázisok közül az IEEE, a Sage, a Scopus, a Springer és a Taylor & Francis listáit. Az adatbázisok kiválasztása során arra törekedtem, hogy a lehető legteljesebb merítést tudjam végezni az esetleges publikációk területén, így nagyobb listából szűrhettem le a mértékadó publikációkat. Ezek mellett az olyan mérvadó tudományos műhelyek kiadványait is átnéztem, mint a NATO Cooperative Cyber Defence Center of Excellence és az ETH Zürich. Keresőszavaim rendre a *cybersecurity, space, Ukraine-Russia, war, satellite* keresőszavak voltak. Emellett áttekintettem a fellelt források hivatkozási listáit is, bízva abban, hogy ezzel újabb, a kritériumoknak megfelelő szakirodalmat találok. A kiválasztás során minden esetben elolvastam az absztraktokat is, így ki tudtam zárni azokat a cikkeket, amelyek ugyan a keresőszavaknak megfeleltek, de tartalmukat tekintve nem voltak relevánsak. A kiterjedt keresés eredményeképp 47 releváns forrást találtam, amelyek teljesítik a tudományos publikációkkal kapcsolatos kritériumokat, tehát nem sajtóhírek vagy piaci cégek publikációi, valamint a kibertér és az űr konvergenciájának biztonsági vetületeiről szólnak. Elfogadtam viszont azokat a kiadványokat, amelyeket tudományos műhelyek, jellemzően egyetemek adtak ki jelentés formájában. A kiválasztott szakcikkek szerzői körét érdekes módon nem lehet klaszterezni, sem affiliációban, sem földrajzi értelemben nincsen meghatározó köre azoknak, akik a témában publikálnak. Ez is mutatja, hogy a választott téma egyelőre inkább csak partikuláris érdeklődésre tart számot.

A forrásokat ezután mélyelemzésnek vetettem alá, amelynek célja az volt, hogy tematikus klaszterelemzéssel feltárjam a megadott 47 publikáció főbb témacsoportjait a teljes szövegük alapján. A dokumentumklaszterezés lényege, hogy a hasonló tartalmú szövegeket közös csoportba rendezzük, így megkönnyítve a rejtett témák és mintázatok azonosítását. Ennek érdekében NLP-alapú szöveganalízist és gépi tanulási módszereket alkalmaztam a szövegek feldolgozására és a klaszterek kialakítására. Az optimális klaszterszámot előzetes elemzések alapján 5-6-ra becsültem, és végül hat tematikus klasztert azonosítottam. A tematikus klaszterelemzéshez mesterségesintelligencia-alapú megközelítést alkalmaztam, a ChatGPT mélyelemzés funkciójának

[5] Kolovos 2022.

segítségével azonosítva a fő témákat és strukturálva a besorolási folyamatot. Az NLP-alapú szövegelemzés lehetővé tette a dokumentumok tartalmi csoportosítását a TF–IDF vektorizáció és a *k-means* klaszterezési algoritmus alkalmazásával. Az alábbiakban részletesen bemutatom a klaszterezés módszertanát, majd ismertetem a kapott klasztereket azok főbb témái, jellemzői és egymáshoz fűződő szemantikai kapcsolatai szerint. Ennek az eszköznek a megbízhatóságát számos tanulmány vizsgálja,[6] amelyek alapján a ChatGPT megfelelő a feladat elvégzéséhez, de mint minden esetben, szakértői validációra van szükség. Ezt jelen esetben úgy tettem meg, hogy az alkalmazott elemzési módszereket részletesen dokumentáltattam a mesterséges intelligenciával, a kapott eredményeket pedig manuálisan visszaellenőriztem, azaz a cikkek teljes szövegének ismeretében meggyőződtem a klaszterezés megfelelőségéről.

Kutatási módszertan

Első lépésben a korábban említettek szerint elvégeztem az adatgyűjtést és előkészítettem a publikációkat a további vizsgálatra. A vizsgálatban szereplő 47 publikáció 2022–2025 között jelent meg, és mind az űr (világűr) és a kibertér metszetében felmerülő biztonsági kérdésekkel foglalkozik. A klaszterelemzéshez a cikkek teljes szövegét (vagy elérhetőség hiányában absztraktját és címét) használtam fel. A szövegeket az algoritmus előfeldolgozta: eltávolította a felesleges írásjeleket, *stopword*öket és normalizálta a szavakat (kisbetűs alakra hozva, szükség esetén szótövekre csonkolva). E lépések célja a nyelvtani alakulatok egységesítése és a zaj csökkentése, hogy a klaszterező algoritmus a tartalmi hasonlóságokra koncentrálhasson.

Második lépésben történt a szövegvektorizáció. Az előkészített dokumentumokat az algoritmus numerikus vektorként reprezentálta a tartalmuk alapján. Ehhez az elemzés TF–IDF *(Term Frequency – Inverse Document Frequency)* módszert alkalmazott, amely minden dokumentumhoz egy egyedi szóvektort rendel. A vektor elemei a szavak fontosságát tükrözik: magasabb érték jelzi, hogy az adott kifejezés gyakori az adott szövegben, de ritkább az összes dokumentum között, így jól jellemzi a tartalmat. Ez a megközelítés segít kiemelni az egyes cikkekre jellemző kulcsszavakat, és mérsékli az általános jelentésű szavak hatását. Alternatív megoldásként szóbeágyazási *(embedding)* technikák is szóba jöhetnek a szemantikai hasonlóság jobb megragadására – például egy pretrénelt nyelvi modell segítségével –, de a TF–IDF-alapú megközelítés is bevált a tematikus különbségek feltárására.

A harmadik lépés a klaszterező algoritmus futtatása volt. A dokumentumvektorok alapján az algoritmus *k-means* algoritmussal csoportosította a cikkeket. A *k-means* egy gyakran használt partícionáló klaszterezési eljárás, amelynek lényege, hogy előre meghatározott k klaszterközéppont köré rendezi a pontokat iteratív módon. Az algoritmus addig finomítja a klasztereket, amíg a dokumentumok a legközelebbi középpontjukhoz tartoznak. A *k-means* hatékony és jól skálázható módszer, amely elegendő információt ad a témák szétválasztásához. Emellett kísérletképpen az algoritmus a hierarchikus klaszterezést is megvizsgálta, amely fastruktúrát eredményez a dokumentumok között – ez részletesebb betekintést nyújthat a klaszterek alstruktúráiba, viszont nagyobb számítási igényű. Jelen elemzésben a *k-means* eredményeit

[6] Lásd például Natarajan–Verma–Kumar 2025.

használtam fel, mivel ezek jól értelmezhető, elkülönülő témacsoportokat adtak. Minden cikket egyetlen klaszterbe soroltam *(hard clustering),* így a klaszterek nem fedik át egymást, hanem diszjunkt tématerületeket reprezentálnak.

Ezután következett a klaszterszám meghatározása. Az optimális klaszterszámot több szempont figyelembevételével 5 és 6 közé állítottam be. Egyrészt a szakirodalmi témák ismeretében feltételeztem, hogy nagyjából öt-hat jól elkülöníthető tematikus csoport jelenhet meg (például jogi kérdések, katonai vonatkozások, technikai fenyegetések stb.). Másrészt kvantitatív módon is megvizsgáltam több klaszterszám mellett a modell kimenetét – például a sziluettmutató értékét –, illetve a klaszterek értelmezhetőségét. Az 5-6 klaszter közötti tartományban kaptam a legkoherensebb eredményeket. Végül a hatklaszteres megoldás bizonyult a legjobban értelmezhetőnek: ebben az esetben egyik klaszter sem volt túl kicsi vagy tartalmilag heterogén, és a csoportok jól leírható, összetartozó témákat fedtek le. Az alábbiakban a hat azonosított klasztert ismertetem, megnevezve fő témájukat és jellemzőiket. Ezen túl kitérek arra is, milyen szemantikai kapcsolatok fedezhetők fel a klaszterek között.

Eredmények: klaszterek és főbb témák

Az elemzés tehát hat tematikus klasztert eredményezett, amelyek az alábbi fő témakörökbe csoportosítják a publikációkat. Minden klaszternél megadom a jellemző tartalmi fókuszt, néhány kulcskifejezést és példaként egy-két idetartozó publikációt. Fontos megjegyezni, hogy noha a klaszterek különálló csoportokat alkotnak, közöttük vannak átfedések és kapcsolódási pontok is – ezeket a későbbiekben részletezem.

1. klaszter: Kiberbiztonsági irányítás (governance) és stratégia az űrben

Az első klaszter az űrbeli kiberbiztonság szabályozási, irányítási és stratégiai kérdéseire fókuszál. Idetartoznak azok a munkák, amelyek átfogóan tárgyalják, hogyan lehet biztosítani a kibertér biztonságát a világűrben, illetve milyen globális együttműködésre és szabványokra van szükség. Gyakoriak a *regulatory framework, governance, strategy* jellegű kulcsszavak, ami jelzi, hogy ez a klaszter a szabályozási kihívásokkal és megoldásokkal foglalkozik.

A publikációk ebben a klaszterben rendszerint rámutatnak, hogy az űr és a kibertér szorosan összefonódó globális közeg, amelyre egységes stratégiákat kell kidolgozni. Kiemelik a nemzetközi összefogás és terminológiai összehangolás fontosságát egy hatékony kiberbiztonsági szabvány vagy politika megalkotásához. Több munka hangsúlyozza a *final frontier* jellegű gondolatot, miszerint az űr a kibertér új határterülete, ahol a kihívások kezelése proaktív szabályozást igényel.

E klaszterbe tartozik például *Drafting a Cybersecurity Standard for Outer Space Missions: On Critical Infrastructure, China, and the Indispensability of a Global Inclusive Approach*[7] című cikk, amely egy globális, inkluzív kiberbiztonsági szabvány

[7] Segate 2024.

kidolgozásának szükségességét taglalja az űrmissziók számára. Szintén idesorolható az *Understanding Cybersecurity in Outer Space*[8] című publikáció, amely az alapvető kihívásokat és stratégiai megfontolásokat tekinti át az űrbéli kiberbiztonság területén. Ezen munkák közös nevezője, hogy átfogó képet adnak a kiberbiztonsági irányításról és stratégiai keretekről az űrtevékenységek kapcsán.

2. klaszter: Jogi és szabályozási keretek az űrkiberbiztonságban

A második klaszter középpontjában az űrtevékenységek kiberbiztonságának jogi vonatkozásai állnak. Idesoroltam azokat a publikációkat, amelyek nemzetközi és nemzeti jogi kereteket, szabályozásokat, illetve politikai irányelveket vizsgálnak a kibertér és a világűr metszetében. A klaszterre jellemző kulcsszavak: *international law, legal framework, policy, orbit,* utalva arra, hogy gyakran szó esik az űrszabályozás nemzetközi jogi aspektusairól és az orbitális rendszerek védelméről.

E klaszter publikációi részletesen elemzik, hogyan alkalmazhatók a meglévő nemzetközi jogszabályok (például az űrjog és a kiberhadviselés joganyaga) az olyan új kihívásokra, mint a műholdak elleni kibertámadások. Több tanulmány foglalkozik a jogi hézagokkal és dilemmákkal is – például hogy miként lehet felelősségre vonni egy államot vagy nem állami szereplőt egy műhold meghekkeléséért, illetve milyen önvédelemi lehetőségek (például *self-defence*) adottak egy kibertámadás esetén az űrben. Emellett felmerül a nemzeti szintű szabályozás kérdése is, például az EU és az USA eltérő megközelítéseinek összehasonlítása a műholdak kiberbiztonsági előírásaiban.

Ebbe a klaszterbe tartozik például a *Law in Orbit: International Legal Perspectives on Cyberattacks Targeting Space Systems*[9] című tanulmány, amely az űrrendszerek elleni kibertámadások nemzetközi jogi értelmezését tárgyalja. Szintén idesorolható a *Developing a Cybersecurity Policy for Low Earth Orbit Satellite Broadband – an International Law Perspective,*[10] amely az alacsony Föld körüli pályán működő műholdhálózatok (például műholdas internet) kiberbiztonsági szabályozását vizsgálja nemzetközi jogi szempontból. Továbbá az *Anti-Satellite Weapons and Self-Defence: Law and Limitations*[11] című munka is, amely a műholdak elleni fegyverek és a jogos önvédelem kérdését feszegeti. E klaszter minden munkája a szabályozási kihívások és jogértelmezések kérdéseit boncolgatja, biztosítandó az űrbeli rendszerek kiberbiztonságát.

3. klaszter: Az űr mint hadszíntér – kiberveszélyek és hadműveleti dimenzió

A harmadik klaszterbe azok a publikációk kerültek, amelyek az űr mint műveleti terület szerepét és az ott megjelenő kiberveszélyeket tárgyalják általános, nem egy konkrét konfliktusra korlátozódó módon. Idetartoznak a *warfighting domain, space warfare, threats in space* témájú munkák, amelyek azt vizsgálják, hogyan válik a világűr

[8] Poirier 2024a.
[9] Bace–Gökce–Tatar 2024.
[10] Kulesza – Akcali Gur 2023.
[11] O'meara 2024.

a hagyományos szárazföldi, tengeri, lég- és kibertér mellett a hadviselés egy új dimenziójává. A klaszter kulcsszavai közé tartozik a *domain* (domén vagy hadszíntér), *warfare, threats* és *security challenges.*

A klaszter publikációi arra mutatnak rá, hogy az űrbéli infrastruktúrák (műholdak, űreszközök) elleni kibertámadások és zavaró tevékenységek (például zavarás, APT-támadás) katonai szempontból stratégiai jelentőségűvé válnak. Több tanulmány foglalkozik a koncepcionális kérdésekkel, például hogy az űr- és kibertartomány mennyiben olvad össze *(space-cyber nexus),* és hogyan lehet kormányozni vagy szabályozni ezt az új hadszínteret. Idesorolhatók olyan munkák, amelyek a hatodik hadviselési domén gondolatát vetik fel – utalva arra, hogy a kibertér után az űr lehet a következő hadszíntér, vagy épp a kettő kombinációja. Emellett a klaszterbe tartozó cikkek érintik a fenyegetések típusait is (például *malicious cyber activities against space assets*) és ezek kezelésének elvi kérdéseit.

Ebben a klaszterben található az *On the Threshold of Space Warfare*[12] című publikáció, amely az űrháború küszöbén álló technológiai és stratégiai változásokat tekinti át. Szintén idesorolható a *The Sixth Warfighting Domain? Governing The Space-Cyber Nexus*[13] is, amely azt vizsgálja, miként lehet irányítani és szabályozni az űr-kiberhadműveleti területet. További példa a *Security Challenges When Space Merges with Cyberspace*[14] című cikk, amely a kibertér és a világűr összefonódásából eredő biztonsági kihívásokat térképezi fel. Összességében e klaszter anyagai az űrhadviselés általános elméleti és fenyegetésbeli aspektusait járják körül, megalapozva a konkrét konfliktusokra vonatkozó elemzéseket.

4. *klaszter: Az orosz–ukrán háború tanulságai és esetei az űr-kiberhadviselés*ben

A negyedik klaszter kifejezetten az orosz–ukrán háborúval és annak űrbeli kiberbiztonsági vonatkozásaival foglalkozik. Ez a klaszter gyűjti össze azokat a publikációkat, amelyek az Ukrajnában 2022-ben kirobbant háború során szerzett tapasztalatokat elemzik, különös tekintettel a műholdak és az űrinfrastruktúra szerepére, valamint a konfliktusban alkalmazott vagy észlelt kibertámadásokra. A klaszter leggyakoribb kulcsszavai: *War in Ukraine, Russian-Ukrainian conflict, military operations, space assets, satellites.* Ezek jól mutatják, hogy a csoport témája a valós háborús esetek és tapasztalatok feldolgozása.

Az idesorolt tanulmányok részletesen dokumentálják, hogyan jelentek meg a kibertérbeli műveletek a fizikai konfliktus részeként. Több publikáció hangsúlyozza, hogy az orosz–ukrán konfliktus volt az első, ahol a kereskedelmi műholdak (például Starlink) és a hozzájuk kapcsolódó kibervonatkozások kiemelt szerepet kaptak – egyesek „az első kereskedelmi űrháborúként" is hivatkoznak rá. E klaszter munkái sorra veszik a háború során tapasztalt kibertámadásokat, például a ViaSat műholdhálózat elleni támadást a konfliktus kezdetén, illetve azt, miként használták az űralapú

[12] Pražák 2022.
[13] Tepper et al. 2023.
[14] Varadharajan–Suri 2024.

szolgáltatásokat (navigáció, kommunikáció, felderítés) a harcoló felek. A tanulmányok elemeznek konkrét incidenseket és azok hatását a hadműveletekre, valamint levonják a stratégiai tanulságokat arról, hogyan kell felkészülni hasonló jövőbeni konfliktusokra.

Ebbe a klaszterbe tartozik a *Hacking the Cosmos: Cyber Operations Against the Space Sector – A Case Study From the War in Ukraine*[15] című tanulmány, amely konkrét esettanulmányként mutatja be, hogyan támadták meg a háború során az űrszektort (ilyen volt például a ViaSat műholdas hálózat elleni kibertámadás). Idesorolható a *The Space Domain and the Russia-Ukraine War*[16] is, amely átfogóan elemzi, hogyan vált a világűr a háború egyik hadszínterévé, és milyen műveletek történtek ebben a doménben. További példa a *Starlink's Role in Ukraine: Portent of a Space War?*[17] című publikáció, amely kifejezetten a Starlink műholdas internet szerepét vizsgálja a konfliktusban, felvetve, hogy ez előrevetíti-e az űrháborúk új korszakát. Ezek a publikációk mind az orosz–ukrán háború tapasztalatait dolgozzák fel, rávilágítva arra, hogy a modern fegyveres konfliktusokban az űrbéli kiberfaktor immár megkerülhetetlen.

5. klaszter: Kereskedelmi és magánszereplők a digitális hadszíntéren

Az ötödik klaszter az űrbeli kiberbiztonság kereskedelmi és civil vonatkozásait emeli ki, különös tekintettel a magánszektor szereplőire (például kereskedelmi műhold-üzemeltetők) és a „digitális hadszíntér" koncepciójára. A klaszter kulcsszavai – mint *commercial, operators, digital battlefield, lessons learned* – arra utalnak, hogy ezek a munkák azt vizsgálják, miként vonódnak be a nem állami szereplők (vállalatok, magán-infrastruktúrák) a konfliktusokba, és milyen tanulságok adódnak ebből.

A publikációk rámutatnak, hogy napjaink fegyveres konfliktusaiban a magántulajdonú űreszközök és rendszerek (például kereskedelmi, távközlési vagy földmegfigyelő műholdak) is célpontokká, illetve stratégiai erőforrásokká válnak. Ez új kihívásokat hoz a nemzetbiztonság és a kibervédelem terén, hiszen a hadviselés immár kiterjed a kereskedelmi szolgáltatók hálózataira is. Több tanulmány ebben a klaszterben azt emeli ki, hogy a magánszektor bevonása miatt a hadszíntér „digitalizálódik", azaz az információs infrastruktúrák és a kibertámadások ugyanolyan fontossá váltak, mint a hagyományos fegyverek. Emellett szó esik a konfliktusokból levonható technikai és szervezeti tanulságokról is *(lessons learned),* amelyek segíthetnek a jövőbeni együttműködésben az állami és magánszereplők között.

A *Commercial Space Operators on the Digital Battlefield*[18] című tanulmány ebben a klaszterben azt vizsgálja, hogyan válnak a kereskedelmi űrcégek (például műholdas kommunikációt nyújtó vállalatok) a modern háborúk digitális hadszínterének részévé. Hasonló témát érint a *Russian-Ukraine Armed Conflict: Lessons Learned on the Digital Ecosystem,*[19] amely az orosz–ukrán háború kapcsán szerzett tapasztalatokat elemzi a digitális infrastruktúrák (beleértve a magánhálózatokat) vonatkozásában. Habár

[15] Poirier 2024b.
[16] Peperkamp–Bolder 2024.
[17] Ray–Selvamurthy 2023.
[18] Cesari 2023.
[19] Aviv–Ferri 2023.

tartalmilag átfedés van az előző klaszterrel a háborús kontextus miatt, ezek a művek kifejezetten a civil szféra és a katonai műveletek összefonódására koncentrálnak. Kiemelendő továbbá a *Cyber Orbits: The Digital Revolution of Space Security*[20] című cikk, amely átfogóbban tekint a digitális átalakulásra az űrbiztonság terén – ideértve a kereskedelmi és védelmi szféra kapcsolatát is. Ez a klaszter tehát rámutat a köz- és magánszféra közötti együttműködés szükségességére az űrkiberbiztonság területén.

6. klaszter: Technikai kiberfenyegetések és rendszerszintű ellenálló képesség

A hatodik klaszter központi témája az űrrendszerek elleni kiberfenyegetések technikai jellege és az ezekkel szembeni kibervédelmi mechanizmusok, reziliencia. Idesorolhatók azok a tanulmányok, amelyek konkrét technikai sebezhetőségeket, támadási módszereket, valamint a védekezés műszaki és szervezeti aspektusait taglalják. A klaszter kulcsszavai: *cyber attacks, critical infrastructure, resilience, communications, defence.* Ezek jelzik, hogy a csoport középpontjában a kritikus űrinfrastruktúrák (például műhold-kommunikációs rendszerek) védelme és a kibertámadások kezelése áll.

Az ebbe a klaszterbe tartozó publikációk részletesen bemutatják a fenyegetési képet: milyen jellegű kibertámadások érhetik az űreszközöket (például zavarás, adatlopás, szolgáltatásmegtagadás), és ezek milyen hatással lehetnek a rendszer működésére és a földi szolgáltatásokra. Több tanulmány foglalkozik a kiberreziliencia fogalmával, vagyis hogy az űrrendszerek tervezésénél és üzemeltetésénél miként lehet biztosítani a támadásokkal szembeni ellenálló képességet és a gyors helyreállítást. Idetartoznak továbbá olyan átfogó elemzések, amelyek rendszerszinten vizsgálják a sebezhetőségeket és a védekezési stratégiákat – például egyes munkák szakirodalmi felmérést nyújtanak az űrkiberbiztonság témájában, rávilágítva a technikai kihívásokra és a jelenlegi felkészültségi szintre. Emellett felmerül az interdiszciplináris megközelítés igénye: a műszaki megoldások mellett a stratégiai és szabályozási szempontok figyelembevétele is szükséges a hatékony védelemhez (ezt jelzi, hogy például egyes klaszterbeli dokumentumok az ESPI-jelentés[21] keretében tárgyalják a *space-cyberdefence* kihívásokat).

Példaként említhető a *Cyber Resilience Limitations in Space Systems Design Process: Insights from Space Designers*[22] című publikáció, amely űripari szakemberek bevonásával elemzi, hol vannak a tervezési folyamatban gyenge pontok a kiberreziliencia szempontjából. További idesorolható munka a *Cyber Attacks on Critical Infrastructures and Satellite Communications*[23] című elemzés, amely konkrétan a műholdas kommunikációs infrastruktúrák elleni támadások típusait és az azok elleni védekezés lehetőségeit tekinti át. Szintén érdekes az *ESPI Report – Space, Cyber and Defence: Navigating Interdisciplinary Challenges,* a már említett kiadvány, amely európai szemszögből, interdiszciplinárisan vizsgálja az űrkiberbiztonságot, beleértve a technikai és védelmi dimenziókat is. E klaszter tehát a technológiai kihívásokra és a védelmi válaszokra helyezi a hangsúlyt az űrkiberbiztonság területén.

[20] Botezatu–Vevera 2024.
[21] European Space Policy Institute 2023.
[22] Shahzad et al. 2024.
[23] Carlo–Obergfaell 2024.

Szemantikai kapcsolatok a klaszterek között

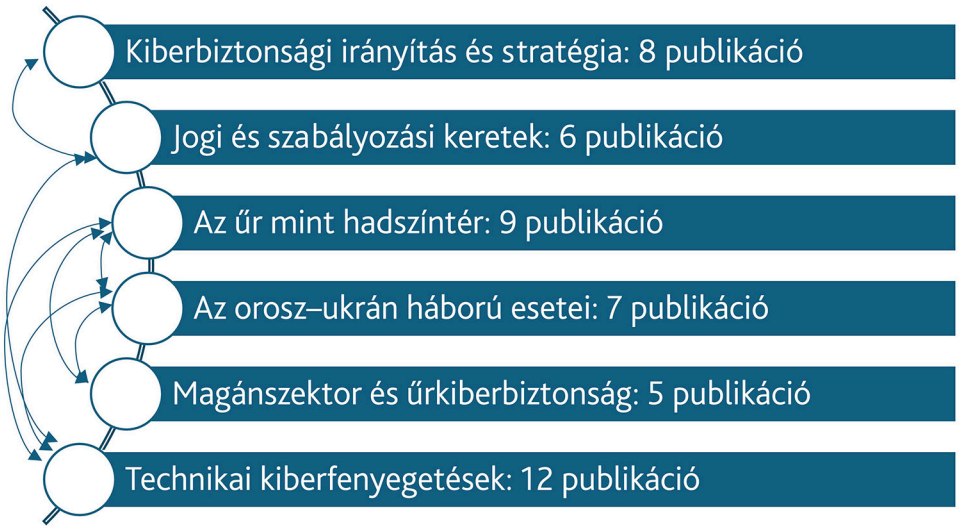
A már említett klaszterek jól elkülöníthető témaköröket jelölnek, ugyanakkor nem függetlenek teljesen egymástól (1. ábra). Figyelemre méltó, hogy több klaszter is a fegyveres konfliktusok köré szerveződik (különösen a 3., 4. és 5. klaszter), jelezve, hogy a katonai vonatkozás az űrkiberbiztonsági szakirodalomban kiemelt szerepet kap, nem függetlenül az orosz–ukrán háború tapasztalataitól. Ez a megállapítás egyben alátámasztja a hipotézisemet, és igazolja, hogy ezek a klaszterek új irányokat mutatnak a tudományos diskurzusban. A 3. klaszter az elméleti keretet adja meg ahhoz, hogy az űrt mint hadszínteret kezeljük, míg a 4. klaszter ennek a gyakorlati megnyilvánulását mutatja be az orosz–ukrán háború példáján. Az 5. klaszter ehhez kapcsolódva a konfliktusok egy speciális aspektusára, a magánszektor bevonására fókuszál, így szorosan kapcsolódik a 4. klaszterhez (hiszen az ukrán háborúban vizsgálja a Starlink és egyéb kereskedelmi infrastruktúrák szerepét). Valójában több publikáció is említhető lenne egyszerre a 4. és az 5. klaszterben – például a Starlinkről szóló tanulmány joggal illeszkedik a háborús és a kereskedelmi témájú klaszterbe is. Jelen tanulmányban azonban minden művet a fő fókusza alapján soroltam be egy klaszterbe.

Hasonló átfedés figyelhető meg a jogi-politikai (2. klaszter) és a stratégiai-irányítási (1. klaszter) témák között. Mindkettő a szabályozás és az irányítás kérdéskörével foglalkozik, csak eltérő szinten: az 1. klaszter általános stratégiai víziókat és koordinációs igényt fogalmaz meg, míg a 2. klaszter konkrét jogi kereteket és normákat elemez. E két klaszter együtt ad átfogó képet a kiberbiztonsági *governance*-ről: az egyik inkább politikai-stratégiai, a másik jogi végrehajtási nézőpontból. A közöttük lévő szemantikai kapcsolat abban rejlik, hogy a hatékony kiberbiztonsági stratégia kidolgozása (1. klaszter témája) megköveteli a megfelelő jogi háttér meglétét (2. klaszter témája), és *vice versa:* a jogi szabályozásnak igazodnia kell a stratégiai realitásokhoz. Ez a két kutatási területe semmiképpen sem nevezhető újdonságnak, több évtizedre visszamenő múltja van a témába vágó publikációknak. Az orosz–ukrán háború azonban olyan gyakorlati esettanulmány, amely miatt ennek a két klaszternek a finomhangolása szükséges.

A technikai kihívások klasztere (6. klaszter) szintén kapcsolódik a többiekhez, hiszen a műszaki sebezhetőségek és támadások ismerete alapozza meg mind a szabályozási/jogi válaszlépéseket, mind a katonai stratégiát. Például a 6. klaszterben tárgyalt sérülékenységek és védelmi mechanizmusok jelentik azt a valóságot, amelyre a 3. klaszterben vázolt hadműveleti stratégiáknak reagálniuk kell, és amelyeket a 2. klaszter jogi keretei szerint kell kezelni (például felelősség, nemzetközi együttműködés kérdése). Ugyanez igaz fordítva is: a 4. klaszter háborús esettanulmányai rávilágítanak olyan konkrét technikai problémákra (mint a ViaSat-incidens), amelyek a 6. klaszter általános technikai témái közé illeszkednek. A technikai aspektus vizsgálata szintén nem újdonság, azonban a konkrét támadások tapasztalatai alapján a műszaki védelem irányai tovább finomíthatók.

Összességében a klaszterek között erős szemantikai összefüggésrendszer bontakozik ki, ami természetes egy ilyen interdiszciplináris területen. Az űrkiberbiztonság témaköre komplex: magában foglalja a nemzetközi jogot és politikát, a katonai stratégiát, a technológiát és a gazdasági-kereskedelmi aspektusokat is. A klaszterelemzés eredményei azt tükrözik, hogy a szakirodalom fő áramlatai is e dimenziók mentén szerveződnek,

ugyanakkor együtt alkotnak egy koherens egészet. A külön klaszterekbe rendezett témák valójában egymásra épülnek és egymást kiegészítik: a háborús tapasztalatok informálják a jövőbeli szabályozást és technikai fejlesztéseket; a jogi keretek meghatározzák a katonai és kereskedelmi szereplők mozgásterét; a technikai újítások pedig új kihívásokat teremtenek a stratégák és a jogalkotók számára.



1. ábra: A megvizsgált publikációk száma klaszterenként és a klaszterek közötti szemantikai kapcsolat
Forrás: a szerző szerkesztése

Következtetések

A 47 publikáció tematikus klaszterelemzése révén öt-hat markáns tématerületet sikerült azonosítani az űrkiberbiztonság diskurzusában. Jelen esetben hat klaszter körvonalazódott: 1) kiberbiztonsági kormányzás és globális stratégia az űrben; 2) jogi és szabályozási keretek; 3) az űr mint új hadszíntér és a kiberveszélyek általános kérdései; 4) az orosz–ukrán konfliktus tapasztalatai és esettanulmányai; 5) a magánszektor és a digitális hadszíntér szerepe; valamint 6) technikai kihívások és rendszerszintű kiberbiztonsági ellenálló képesség. A klaszterek feltárása rávilágított, hogy a téma rendkívül szerteágazó, de az egyes almotívumok mentén jól strukturálható. Egyben alátámasztotta a hipotézisemet, és igazolta, hogy egyrészt vannak olyan tématerületek, amelyek korábban nem, vagy csak kis mértékben voltak kutatottak (2, 3, 4), míg a régóta kutatott területeken az orosz–ukrán háború tapasztalatai alapján finomhangolások történnek (1, 5, 6).

Az ilyen jellegű klaszterezés hasznos a kutatók számára, mert segít rendszerezni a tudásbázist, illetve azonosítani, hol koncentrálódik a kutatás. Látható például, hogy az orosz–ukrán háború témája kiemelt figyelmet kapott (számos publikáció tartozik ide), ami azt jelzi, hogy a valós események erősen formálták a diskurzust. Ugyanakkor a szabályozási és technikai klaszterek léte azt mutatja, hogy a hosszú távú kihívások – úgymint nemzetközi jogi mechanizmusok kialakítása, illetve a rendszerek biztonságos tervezése – szintén központi kérdések. A klaszterelemzés eredményei alapján a kutatásban esetlegesen hiányos vagy kevésbé feldolgozott területek is azonosíthatók. Ha például azt találtam volna, hogy alig van publikáció a kereskedelmi szereplők vonatkozásában, az egy lehetséges kutatási hézagra utalna – jelen esetben azonban minden fő aspektusra találtam több példát is.

Összefoglalva, a klaszterezés rámutatott az űrkiberbiztonsági szakirodalom fő sodorvonalaira. Az eredmények strukturáltan bemutatva segíthetnek egy készülő publikáció előkészítésében. A szerzők hivatkozhatnak arra, hogy mely fő témakörökbe csoportosul a téma irodalma, és hol helyezkedik el a saját kutatásuk ezen a térképen. Tekintettel arra, hogy a magyar űrambíciók hatására az űrrel kapcsolatos hazai tudományos kutatás a reneszánszát éli, klaszterelemzésem segítheti a témával foglalkozó kutatók orientációját. A részletes módszertani leírás pedig biztosítja az elemzés megismételhetőségét és átláthatóságát, ami a tudományos minőség szempontjából elengedhetetlen. A tematikus klaszterek bemutatása emellett összefoglaló képet nyújt az olvasóknak az űrkiberbiztonság jelenlegi tudásanyagának tagolódásáról és a különböző témák közötti kapcsolatokról.

Az űrkiberbiztonság tehát egy dinamikusan fejlődő kutatási terület, amely az űreszközök, a műholdak és a világűrben alkalmazott informatikai rendszerek sebezhetőségeit, valamint azok védelmi megoldásait vizsgálja. Noha a nemzetközi szakirodalomban az előző fejezetekben bemutatott módon egyre növekvő figyelem irányul az űrkiberbiztonság stratégiai, jogi és technikai aspektusaira, a magyar nyelvű tudományos diskurzusban ez a téma még feldolgozatlan. A 2022 utáni magyar nyelvű szakirodalom áttekintése során megállapítottam, hogy jelenleg nem áll rendelkezésre olyan magyar nyelvű tudományos publikáció, amely kifejezetten az űrkiberbiztonságot vizsgálná, és amely tematikus rendszerezéssel segítené a terület hazai kutatóinak és döntéshozóinak munkáját. A témával kapcsolatos magyar nyelvű anyagok jellemzően szakmai blogokban, híroldalakon és előadások formájában jelentek meg, amelyek ugyan fontos megállapításokat tartalmaznak, de nem biztosítanak mélyreható tudományos elemzést vagy rendszerezett módszertani megközelítést.

Jelen tanulmány segítségével lehetővé válik ennek a hiánynak a pótlása. Miután tudományos keretbe helyezve bemutattam az űrkiberbiztonság legfontosabb tématerületeit egy átfogó tematikus klaszterezési elemzés segítségével, az eredmények hozzájárulhatnak a magyar nyelvű szakirodalom bővítéséhez, valamint irányt mutathatnak a döntéshozók és a kutatók számára a jövőbeli űrbiztonsági kihívások megértéséhez és kezeléséhez.

Felhasznált irodalom

Abels, Joscha (2024): Private Infrastructure in Geopolitical Conflicts: The Case of Starlink and the War in Ukraine. *European Journal of International Relations,* 30(4), 842–866. Online: https://doi.org/10.1177/13540661241260653

Aviv, Itzhak – Ferri, Uri (2023): Russian-Ukraine Armed Conflict: Lessons Learned on the Digital Ecosystem. *International Journal of Critical Infrastructure Protection,* 43, 100637. Online: https://doi.org/10.1016/j.ijcip.2023.100637

Bace, Brianna – Gökce, Yasir – Tatar, Unal (2024): Law in Orbit: International Legal Perspectives on Cyberattacks Targeting Space Systems. *Telecommunications Policy,* 48(4), 102739. Online: https://doi.org/10.1016/j.telpol.2024.102739

Boschetti, Nicolò – Gordon, Nathaniel G. – Falco, Gregory (2022): Space Cybersecurity Lessons Learned from the ViaSat Cyberattack. *ASCEND 2022.* American Institute of Aeronautics and Astronautics. Online: https://doi.org/10.2514/6.2022-4380

Botezatu, Ulpia-Elena – Vevera, Adrian-Victor (2024): Cyber Orbits: The Digital Revolution of Space Security. In Burt, Sally: *National Security in the Digital and Information Age.* IntechOpen. Online: https://doi.org/10.5772/intechopen.1005235

Carlo, Antonio – Obergfaell, Kim (2024): Cyber Attacks on Critical Infrastructures and Satellite Communications. *International Journal of Critical Infrastructure Protection,* 46, 100701. Online: https://doi.org/10.1016/j.ijcip.2024.100701

Cesari, Laetitia (2023): *Commercial Space Operators on the Digital Battlefield. HAL Open Science. Online:* https://hal.science/hal-04491357/document

European Space Policy Institute (2023): *ESPI+ Report. Space, Cyber and Defence: Navigating Interdisciplinary Challenges.* Vienna: ESPI. Online: https://www.espi.or.at/wp-content/uploads/2023/11/ESPI-Report_-Space-Cyber-and-Defence-Navigating-Interdisciplinary-Challenges.pdf

Kolovos, Alexandros K. (2022): *Commercial Satellites in Crisis and War: The Case of the Russian-Ukrainian Conflict.* Online: https://kolydas.eu/wp-content/uploads/2023/05/CommercialSatellitesincrisisandwar.pdf

Kulesza, Joanna – Akcali Gur, Berna (2023): *Developing a Cybersecurity Policy for Low Earth Orbit Satellite Broadband – an International Law Perspective.* Online: https://doi.org/10.2139/ssrn.4424148

Natarajan, K. – Verma, Srikar – Kumar, Dheeraj (2025): Enhanced Interpretation of Novel Datasets by Summarizing Clustering Results Using Deep-Learning Based Linguistic Models. *Applied Intelligence,* 55, 317. Online: https://doi.org/10.1007/s10489-025-06250-6

O'Meara, Chris (2024): Anti-Satellite Weapons and Self-Defence: Law and Limitations. In Kwan, Claire et al.: *CyCon 2024: Over the Horizon. 16th International Conference on Cyber Conflict.* Tallinn: NATO CCDCOE, 249–262. Online: https://doi.org/10.23919/CyCon62501.2024.10685637

Peperkamp, Lonneke – Bolder, Patrick (2024): The Space Domain and the Russia-Ukraine War. In Rothman, Maarten – Peperkamp, Lonneke – Rietjens, Sebastiaan: *Reflections on the Russia-Ukraine War.* Leiden: Leiden University Press, 257–273. Online: https://doi.org/10.24415/9789400604742-014

Poirier, Clémence (2024a): Understanding Cybersecurity in Outer Space. *CSS Analyses in Security Policy,* 343, 1–4. Online: https://doi.org/10.3929/ETHZ-B-000675292
Poirier, Clémence (2024b): Hacking the Cosmos: Cyber Operations Against the Space Sector. A Case Study from the War in Ukraine. *CSS Cyberdefense Reports.* Online: https://doi.org/10.3929/ethz-b-000697348
Pražák, Jakub (2022): On the Threshold of Space Warfare. *Astropolitics,* 20(2–3), 175–191. Online: https://doi.org/10.1080/14777622.2022.2142351
Ray, Kaushik – Selvamurthy, William (2023): Starlink's Role in Ukraine. Portent of a Space War? *Journal of Defence Studies,* 17(1), 25–44. Online: https://www.idsa.in/publisher/journal-of-defence-studies/starlinks-role-in-ukraine-portent-of-a-space-war/
Segate, Riccardo Vecellio (2024): Drafting a Cybersecurity Standard for Outer Space Missions: On Critical Infrastructure, China, and the Indispensability of a Global Inclusive Approach. *Journal of Asian Security and International Affairs,* 11(3), 345–375. Online: https://doi.org/10.1177/23477970241261432
Shahzad, Syed et al. (2024): Cyber Resilience Limitations in Space Systems Design Process: Insights from Space Designers. *Systems,* 12(10), 434. Online: https://doi.org/10.3390/systems12100434
Tepper, Eytan et al. (2023): The Sixth Warfighting Domain? Governing The Space-Cyber Nexus. *Georgia Law Review,* 59. Online: https://ssrn.com/abstract=4791739
Varadharajan, Vijay – Suri, Neeraj (2024): Security Challenges when Space Merges with Cyberspace. *Space Policy*, 67, 101600. Online: https://doi.org/10.1016/j.spacepol.2023.101600

Függelék: Az elemzés során felhasznált források listája

Klaszter	Megjelenés éve	Szerzők	Cím
Az űr mint hadszíntér	2024	Ahumada, Abraham; Del Canto Viterale, Francisco	Securing the Final Frontier: United States Space Force Cybersecurity Capabilities
Az űr mint hadszíntér	2024	Botezatu, Ulpia-Elena	Cybersecurity in the Era of Space Domain Awareness
Az űr mint hadszíntér	2024	Botezatu, Ulpia-Elena; Vevera, Adrian-Victor	Cyber Orbits: The Digital Revolution of Space Security
Az űr mint hadszíntér	2023	Chabert, Valentina	The Outer-Space Dimension of the Ukraine Conflict: Toward a New Paradigm for Orbits as a War Domain?
Az űr mint hadszíntér	2024	de Zoysa, Sayonara; Siriwardana, Deemantha	Final Frontier of Strategic Information Warfare and Cybersecurity Challenges to Satellites and Space Infrastructure
Az űr mint hadszíntér	2023	Heinl, Caitríona	Outer Space as a Growing Security and Defence Domain: Strategic Lessons on Cyber Disruption

Klaszter	Megjelenés éve	Szerzők	Cím
Az űr mint hadszíntér	2022	Pražák, Jakub	On the Threshold of Space Warfare
Az űr mint hadszíntér	2023	Tepper, Eytan; Shackelford, Scott J.; Romano, James B.; Dmitriachev, Sergei	The Sixth Warfighting Domain? Governing The Space-Cyber Nexus
Az űr mint hadszíntér	2024	Blechová, Anna; Harašta, Jakub; Kasl, František	From Space Debris to Space Weaponry: A Legal Examination of Space Debris as a Weapon
Jogi és szabályozási keretek	2024	Bace, Brianna; Gökce, Yasir; Tatar, Unal	Law in Orbit: International Legal Perspectives on Cyberattacks Targeting Space Systems
Jogi és szabályozási keretek	2024	De Sousa, Bruno Reynaud	Cyber Operations Targeting Space Systems. Legal Questions and the Context of Privatisation
Jogi és szabályozási keretek	2023	Li, Du	Legal Dilemma for Combatting Malicious Cyber Activities Against Space Activities
Jogi és szabályozási keretek	2023	Martin, Anne-Sophie	Outer Space, the Final Frontier of Cyberspace: Regulating Cybersecurity Issues in Two Interwoven Domains
Jogi és szabályozási keretek	2024	O'Meara, Chris	Anti-Satellite Weapons and Self-Defence: Law and Limitations
Jogi és szabályozási keretek	2022	Omelyanenko, Vitaliy; Huts, Nataliia; Melnyk, Lina	Space Law in Ukraine: Current Status and Future Development
Kiberbiztonsági irányítás és stratégia	2022	Dilworth, Seth W.; Osborne, D. Daniel	Cyber Threats Against and in the Space Domain: Legal Remedies
Kiberbiztonsági irányítás és stratégia	2023	Febbraro, Daniella	The Need for Cyber Resilience of Space Assets: Law and Policy Considerations of Ensuring Cybersecurity in Outer Space
Kiberbiztonsági irányítás és stratégia	2023	Jacobs, Bas	A Comparative Study of EU and US Regulatory Approaches to Cybersecurity in Space
Kiberbiztonsági irányítás és stratégia	2024	Mattila, Juha Kai	Arranging the Defence of the Cyber Environment as a Part of Military Affairs: Tactical, Operational and Strategic Approach in Retrospect of The Russian-Ukrainian War 2022
Kiberbiztonsági irányítás és stratégia	2024	Poirier, Clémence	Understanding Cybersecurity in Outer Space

Klaszter	Megjelenés éve	Szerzők	Cím
Kiberbiztonsági irányítás és stratégia	2024	Racionero-Garcia, Juan; Shaikh, Siraj Ahmed	Space and Cybersecurity: Challenges and Opportunities Emerging from National Strategy Narratives
Kiberbiztonsági irányítás és stratégia	2024	Segate, Riccardo Vecellio	Drafting a Cybersecurity Standard for Outer Space Missions: On Critical Infrastructure, China, and the Indispensability of a Global Inclusive Approach
Kiberbiztonsági irányítás és stratégia	2024	Shahzad, Syed; Joiner, Keith; Qiao, Li; Deane, Felicity; Plested, Jo	Cyber Resilience Limitations in Space Systems Design Process: Insights from Space Designers
Magánszektor és űrkiberbiztonság	2023	Kulesza, Joanna; Akcali Gur, Berna	Developing a Cybersecurity Policy for Low Earth Orbit Satellite Broadband – an International Law Perspective
Magánszektor és űrkiberbiztonság	2024	Abels, Joscha	Private Infrastructure in Geopolitical Conflicts: The Case of Starlink and the War in Ukraine
Magánszektor és űrkiberbiztonság	2023	Cesari, Laetitia	Commercial Space Operators on the Digital Battlefield
Magánszektor és űrkiberbiztonság	2022	Kolovos, Alexandros K.	Commercial Satellites in Crisis and War: The Case of the Russian-Ukrainian Conflict
Magánszektor és űrkiberbiztonság	2023	Ray, Kaushik; Selvamurthy, William	Starlink's Role In Ukraine: Portent of a Space War?
Az orosz–ukrán háború esetei	2022	Sokiran, Maksym; Zubko, Oksana; Levchenko, Diana	Space Information and Technologies in the Military Activity of Ukraine: Legal Aspect
Az orosz–ukrán háború esetei	2023	Aoki, Setsuko	International Law of the Military Uses of Outer Space in Light of the War in Ukraine as the First Commercial Space War
Az orosz–ukrán háború esetei	2024	Bataille, Mathieu	The Impact and Consequences of the War in Ukraine on Military Space Policies and Operations
Az orosz–ukrán háború esetei	2024	Chadwick, Steven L.	Russia-Ukraine War Lessons for Multidomain Operations
Az orosz–ukrán háború esetei	2022	Choi, Seonghwan	Analysis and Aspects of Space Warfare in the Russia-Ukraine War (Russian Invasion of Ukraine) and Considerations for Space Technology Development
Az orosz–ukrán háború esetei	2024	Gurantz, Ron	Satellites in the Russia-Ukraine War

Klaszter	Megjelenés éve	Szerzők	Cím
Az orosz–ukrán háború esetei	2024	Peperkamp, Lonneke; Bolder, Patrick	The Space Domain and the Russia-Ukraine War
Technikai kiberfenyegetések	2024	Nichols, Randall K.; Mumm, Hans C.; Lonstein, Wayne D.; Ryan, Julie J. C. H.; Carter, Candice M.; Open Textbook Library	Cyber-Human Systems, Space Technologies, and Threats
Technikai kiberfenyegetések	2024	Poirier, Clémence	Hacking the Cosmos: Cyber Operations Against the Space Sector: A Case Study from the War in Ukraine
Technikai kiberfenyegetések	2023	Aviv, Itzhak; Ferri, Uri	Russian-Ukraine Armed Conflict: Lessons Learned on the Digital Ecosystem
Technikai kiberfenyegetések	2022	Boschetti, Nicolò; Gordon, Nathaniel G.; Falco, Gregory	Space Cybersecurity Lessons Learned from the ViaSat Cyberattack
Technikai kiberfenyegetések	2024	Carlo, Antonio; Obergfaell, Kim	Cyber Attacks on Critical Infrastructures and Satellite Communications
Technikai kiberfenyegetések	2024	Jones, Rachel C.	Survey of Space Professionals' Perception of Satellite Cybersecurity from 2012 to 2022: Decision-Makers' Thoughts on Satellite Cybersecurity Evolving
Technikai kiberfenyegetések	2023	Kavallieratos, Georgios; Katsikas, Sokratis	An Exploratory Analysis of the Last Frontier: A Systematic Literature Review of Cybersecurity in Space
Technikai kiberfenyegetések	2024	Khan, Shah Khalid; Shiwakoti, Nirajan; Diro, Abebe; Molla, Alemayehu; Gondal, Iqbal; Warren, Matthew	Space Cybersecurity Challenges, Mitigation Techniques, Anticipated Readiness, and Future Directions
Technikai kiberfenyegetések	2024	Lin, Patrick; Abney, Keith; DeBruhl, Bruce; Abercromby, Kira; Danielson, Henry; Jenkins, Ryan	Outer Space Cyberattacks: Generating Novel Scenarios to Avoid Surprise
Technikai kiberfenyegetések	2022	Thangavel, Kathiravan; Plotnek, Jordan Joseph; Gardi, Alessandro; Sabatini, Roberto	Understanding and Investigating Adversary Threats and Countermeasures in the Context of Space Cybersecurity
Technikai kiberfenyegetések	2024	Varadharajan, Vijay; Suri, Neeraj	Security Challenges when Space Merges with Cyberspace
Technikai kiberfenyegetések	2023	European Space Policy Institute (ESPI)	ESPI+ Report. Space, Cyber and Defence: Navigating Interdisciplinary Challenges

HADMÉRNÖK
VÉDELEMINFORMATIKA
20. évfolyam (2025) 2. szám 113–128.
DOI: 10.32567/hm.2025.2.7

Molnár Ákos Ádám[1]

A mesterséges intelligenciával kapcsolatos befogadóképesség és a különböző érzékelések empirikus vizsgálata

Empirical Examination of Receptivity to Artificial Intelligence and Different Perceptions

Absztrakt

A mesterséges intelligencia rohamos terjedése újfajta társadalmi és szabályozási kihívásokat teremt. Kutatásom a technológia penetrációjának és jogi kereteinek vizsgálatára irányult, különös tekintettel a ChatGPT mint jelenség feltűnésére. A vegyes módszertanú vizsgálat kérdőíves felmérést és online keresési trendek elemzését kombinálta a technológiaelfogadás UTAUT2 modelljének alkalmazásával, így elemezve a Google Trends platform adatait különböző témákban a ChatGPT nyilvánosságra kerülését követően mind hazai, mind nemzetközi szinten. A kérdőíves felmérés során megvizsgálva a kitöltők informáltságát, tudatosságát és észleléseit különböző statisztikai eljárásokkal, az informáltság és a kockázatészlelés közötti kapcsolat összetett képet rajzolt ki, ahol csak bizonyos aggodalmak esetén volt kimutatható szignifikáns összefüggés. A kutatás rávilágított arra, hogy a tudatos technológiahasználat és a jövőbeli kockázatok észlelése között nincs egyértelmű kapcsolat, ami fontos kérdéseket vet fel a technológiai fejlődés társadalmi megítélésével kapcsolatban.

Kulcsszavak: MI, érzékelések, kérdőíves felmérés, UTAUT2

[1] Hallgató, Közszolgálati Egyetem Államtudományi és Nemzetközi Tanulmányok Kar, e-mail: molnar.akos.adam@uni-nke.hu

Abstract

The rapid spread of artificial intelligence creates new social and regulatory challenges. My research focused on examining the penetration of technology and its legal framework, with particular emphasis on the emergence of ChatGPT as a phenomenon. The mixed-methods study combined a questionnaire survey and analysis of online search trends using the UTAUT2 model of technology adoption, analysing data from the Google Trends platform on various topics following the release of ChatGPT, both domestically and internationally. The questionnaire survey examined the respondents' level of information, awareness, and various perceptions using different statistical methods, revealing a complex picture of the relationship between information and risk perception, with a significant correlation only in the case of certain concerns. The research highlighted that there is no clear relationship between conscious technology use and the perception of future risks, which raises important questions about the social perception of technological development.

Keywords: AI, perceptions, survey, UTAUT2

Bevezetés

A mesterséges intelligencia (MI) fogalmi meghatározása komplex tudományos kihívást jelent, mivel több diszciplínát átfogó technológiát ölel fel. Az Európai Unió az MI-t olyan rendszerekként definiálja, amelyek intelligens viselkedést mutatnak környezetük elemzése és célirányos cselekvés révén,[2] míg az Egyesült Államok végrehajtási rendelete gépi alapú, ember által irányított döntéshozó rendszerekre utal.[3] Az MI fejlődése a régi korok automatái után (Platón mechanikus galambja, Leonardo da Vinci lovagja) az 1950-es években vált forradalmivá: Alan Turing tesztje megalapozta a gépi gondolkodás értékelését, John McCarthy 1955-ben alkotta meg a mesterséges intelligencia kifejezést, majd az 1970-es években megjelentek az első antropomorf robotok. A ChatGPT 2022-es nyilvánosságra hozatala *tipping point*ot jelentett, mivel a tömeges tudatosság növekedését okozta, amit a Google Trends adatai igazolnak – a magyar *mesterséges intelligencia* és *chatgpt* keresések 2022 novemberétől 75–100%-os növekedést mutattak, hasonlóan a globális *AI* és *deep learning* kifejezésekhez.

Empirikus kutatásom részeként 2024. január 8–24. között 127 válaszadót (59% nő, 57% 14–22 éves) kérdőíves felmérés útján vizsgáltam. A kitöltők 80%-a használt már tudatosan MI-t, főként ChatGPT-t. A UTAUT2 modell alapján végzett korrelációelemzés kimutatta, hogy a korábbi MI-használók szignifikánsan negatívabb kapcsolatot mutattak a technológia teljesítményjavító hatásával ($r = -0{,}42$), az elősegítő feltételekkel ($r = -0{,}38$) és a hedonista motivációval ($r = -0{,}41$) kapcsolatban. Az informáltság és az észlelések vizsgálatánál klaszterelemzés során két homogén csoportot azonosítottam, de a Kruskal–Wallis-teszt csak az MI hatásaira ($p = 0{,}009$) és a megfigyelési technológiákra ($p = 0{,}001$) vonatkozó aggodalom esetén mutatott

[2] European Parliament 2021.
[3] ISO [é. n.].

szignifikáns kapcsolatot. A második hipotézist (MI-használat és kockázatpercepció kapcsolata) a statisztikai elemzés nem támasztotta alá ($p > 0.05$ minden változónál). Empirikus kutatásaim során online kulcsszóelemzést alkalmazok a Google Trends platform segítségével, amely a *google.com* keresőmotor adatbázisa alapján mutatja meg a keresési adatokat. A kulcsszóelemzés mellett kérdőíves felmérést végeztem a Google Forms platformon, az eredményeit az IBM SPSS statisztikai szoftver segítségével elemzem ki.

H1: A mesterséges intelligenciával kapcsolatos informáltság és az aggodalom, fenyegetés és fogékonyság kérdések között kapcsolat van.

H2: A ChatGPT nyílt használatával felerősödött a mesterséges intelligenciával kapcsolatos kifejezések online megjelenése.

Az empirikus kutatás bemutatása és módszertana

Google Trends

A Google Trends egy hatékony eszköz, amely közel valós idejű betekintést nyújt az emberek Google általi kereséseibe. Ezek az adatok felhasználhatók egy adott téma, helyszín vagy időpont iránti keresés felmérésére. Az eszköz felfedezés funkciója pedig témák szerint csoportosítja az adatokat, átfogó képet nyújtva a keresési trendekről. A Trends népszerűségi grafikonjának értelmezése kulcsfontosságú. A helyalapú adatok a Google Trends egy másik aspektusa, amely országonként, régiónként és városonként mutatja be a keresési érdeklődést, amelyben a sötétebb árnyalatok magasabb érdeklődési szintet jeleznek. A felhasználók válthatnak a térkép- és listanézetek között, kiválasztva a kívánt bontást.

A normalizált érdeklődési értékek 1 és 100 között mozognak, a 100-as érték a legnagyobb érdeklődést jelzi. Fontos megjegyezni, hogy az értékek az érdeklődési szintet jelölik, a legmagasabb ponthoz viszonyítva az adott intervallumon belül. Amennyiben az érték 0, akkor nincs elég adat ahhoz, hogy meg tudja jeleníteni azt a diagramon. Az eszközzel egészen 2004. január 1-ig visszamenőleg lehet keresni, különböző időintervallumokat megadva. Az emelkedő adatok olyan témákat vagy lekérdezéseket tükröznek, amelyekben a keresési érdeklődés jelentősen megnőtt, és gyakran jelzik a kialakulóban lévő trendeket is. A top keresések a legnagyobb keresési volumenű lekérdezéseket emelik ki. Jelen esetben az eredményeket 2020. január 1-től vizsgálom, habár nyilvánosan csak 2022 novemberétől volt elérhető a ChatGPT.[4]

[4] Walsh 2025.

Kérdőíves felmérés

A kérdőív több részből épül fel: az első részben a demográfiai adatokat vizsgálom. Ilyen adatok voltak a nem, az életkor és az iskolai végzettség. A második szekcióban a kitöltők MI-vel kapcsolatos ismereteit vizsgálom, illetve hogy használtak-e már MI-t tudatosan. Ebben a szekcióban 6 állítást is megfogalmazok a technológiával kapcsolatban – ezek közül 3 darab igaz és 3 darab hamis állítás –, amelyekre egy háromértékű Likert-skálán válaszolhattak, egyáltalán nem ért egyet, részben egyetért és teljes mértékben egyetért válaszok közül válogatva. A Likert-skálák olyan skálák, amelyek az egyén attitűdjét vizsgálják egy kérdés kapcsán. A válaszlehetőségeket kitáblázva, majd 1-től 3-ig számokat rendelve hozzájuk, minden kitöltőnél kapok egy eredményt 6 és 18 között.

A harmadik szekció az MI-vel kapcsolatos észleléseket vizsgálja. Ezt a fejezetet további 3 részre osztom, ezekre a kérdésekre egy ötös skálán válaszolhattak a kitöltők. Az első részben az arra vonatkozó észlelt fogékonyságot vizsgálom, hogy a jövőben az MI jelentősen befolyásolni fogja-e az illető jelenlegi/leendő munkakörét. Ebben a részben 5 kérdésre összesen 5 és 25 között lehetett pontot elérni. A második egysége a kérdőíves résznek az észlelt fenyegetés, amelynek lényege megtudni, hogy az adott kitöltő mennyire tartja veszélyesnek a technológiát magára és környezetére tekintve. A kérdőív ezen részének utolsó előtti blokkjában kutatom a válaszadó aggodalmát az MI-vel kapcsolatban. Utóbbi két szekcióban szintén 5-5 kérdés alapján 5 válaszlehetőségből összesen 5 és 25 közötti pontszámot érhettek el a kitöltők.

Az utolsó kérdéskörben a technológiával kapcsolatos elfogadottságot vizsgálom az UTAUT2-modell mentén. A technológia elfogadásának és használatának egységes elmélete (*Unified Theory of Acceptance and Use of Technology,* UTAUT2) modell széles körben elismert és átfogó keretrendszer az információs rendszerek elfogadásának és használatának tanulmányozására. Ez a modell azt sugallja, hogy több kulcsfontosságú tényező, köztük a teljesítményelvárások, az erőforrás-elvárások, a társadalmi befolyás és a megfelelőség alapvető szerepet játszik az egyén technológia elfogadására és használatára irányuló szándékának alakításában. Emellett az UTAUT2 modell kibővíti ezt a keretrendszert az érzelmek és tapasztalatok dimenzióinak bevonásával, felismerve azok jelentőségét az elfogadásra és használatra vonatkozó döntésekben.[5] Ennek során 18 kérdést tettem fel, 2-2 kérdést csoportonként, mint a hedonista motiváció vagy a társadalmi befolyásolás. A kérdésekre szintén ötfokú Likert-skálán lehetett válaszolni.

A kérdőívemre kapott válaszokat először Excel-táblázatokban összegeztem, megtisztítottam és szeparáltam. Ezt követően feltöltöttem a világ egyik vezető statisztikai és adatelemző vállalatának, az IBM-nek az SPSS nevű szoftverébe. Erre a vállalatra és technológiájára világszerte támaszkodnak kutatók és egyéb szakmai felhasználók.[6] A szoftverben a különböző válaszokhoz különböző számkódokat párosítottam a gördülékenység érdekében (például nő = 1, férfi = 2), majd a változókat csoportosítottam attól függően, hogy azok nominálisak, ordinálisak vagy intervallumalapúak. Nominális skála az, amelynél a válaszok között nincs értékváltozás (például nem, nemzetiség),

[5] Ain–Kaur–Waheed 2016.
[6] Sajtos–Mitev 2007.

ordinális skála esetében van rangsor a válaszok tekintetében, azonban nem tudni, mekkora (például egy betegség előrehaladtának mérése). Intervallumskáláról pedig akkor beszélhetünk, ha az értékek közti különbséget tudjuk értelmezni is (például testmagasság, hőmérséklet).[7] A kérdések és válaszok betöltése után, illetve a kódolás befejeztével elkezdtem a különböző statisztikai módszerek használatát. A szoftver ezeket a bonyolult matematikai módszereket magától futtatja le, nekünk csak a megfelelő elemeket kell kijelölni hozzá.[8]

A kereszttábla egy adattáblázat, amelynek segítségével az adatokat, a sorokban és oszlopokban lévő különböző eredményeket egymással összevetve, egyesével tudom megvizsgálni. A két változó közti összefüggések vizsgálata azonban csak százalék- és számértékeket ad meg. A kereszttábla-elemzésen belül ezért használtam még a khi-négyzet-próbát. A próba során kapjuk meg a szignifikanciaszintet. Ha ez az érték 0,05 alá esik ($s < 0,05$), akkor beszélhetünk szignifikáns összefüggésről, tehát van kapcsolat két változó között. Viszont ha ez a szám egyenlő vagy nagyobb, mint 0,05 ($s = 0,05$ vagy $s > 0,05$), akkor nem beszélhetünk szignifikáns összefüggésről, tehát megállapíthatjuk, hogy nincs kapcsolat a változók között. Fontos kitétel ugyanakkor, hogy a kereszttábla mátrixának celláiban 5-nél több értéknek kell lennie. Amennyiben a cellák minimum 20%-ában a mennyiségre utaló adatok nem érik el az 5 darab/főt, akkor a khi-négyzet-próba adatait nem vehetjük figyelembe a magas hibaráta miatt. A kereszttáblán belül használom még a Cramer-féle V-tesztet, amely a legmegbízhatóbb mutató a szignifikanciaszint erősségének vizsgálatára. A teszt megmutatja, hogy milyen erős két változó közötti szignifikáns kapcsolat. Az értéke 0 és 1 között terjedhet, amennyiben az értéke 0,5 alatti, akkor gyenge kapcsolatról, 0,5-ös értéknél közepes erősségű kapcsolatról, míg 0,5 és 1 között erős kapcsolatról beszélhetünk.[9]

Kruskal–Wallis-tesztet alkalmaztam továbbá különböző csoportok és egyéb Likert-skálán mért változók közti kapcsolatok elemzésére. Ezt az attitűdöt később számértékkel láttam el a mérés lefuttatása érdekében.[10] A teszt alapján két dolgot vizsgáltam, először is a csoportok és változók közötti szignifikanciaszintet, másodszor pedig a rangátlagokat. A rangátlagok esetünkben azt jelzik, hogy a csoporthoz való tartozás milyen magatartást mutat a vizsgált kérdések tekintetében (például minél magasabb, annál inkább értenek egyet az adott kérdéssel a csoport tagjai).[11]

Mindezek mellett klaszterelemzéssel csoportokat alkottam, a csoportok számát Ward-féle eljárással határoztam meg, így megkapva a számomra legoptimálisabb csoportszámot. A klaszterelemzés során különböző homogén csoportokat hoztam létre az elemzésbe bevont kérdések és az azokra adott válaszok alapján.[12] Ezeket a csoportokat azonban a Kruskal–Wallis-teszt során elvégzett egyéb változókkal való összevetés után tudtam elnevezni a kapott rangátlagok segítségével (például

[7] Sajtos–Mitev 2007.
[8] Csallner 2015.
[9] Sajtos–Mitev 2007; Csallner 2015.
[10] Laerd Statistics [é. n.].
[11] Laerd Statistics [é. n.].
[12] Sajtos–Mitev 2007.

jól informáltak, kevésbé informáltak stb.). A teszt során az elnevezett csoportokat vizsgáltam tovább egyéb kérdésekre adott válaszokkal és demográfiai adatokkal.[13]

Korrelációelemzés során az adatok közötti összefüggést, annak szorosságát és erősségét vizsgáltam. Első lépésként gyűjtjük az adatokat két vagy több változóról. Fontos, hogy az adatokat alaposan ellenőrizzük, hogy biztosak lehessünk pontosságukban és megbízhatóságukban. Ezután kiszámítjuk a korrelációs együtthatót, a Pearson korrelációs együtthatót használva, hogy mérjük az adatok közötti lineáris kapcsolatot. A korreláció értéke pozitív vagy negatív előjellel jellemezhető, amely alapján értékeljük a kapcsolat erősségét és irányát, így maga az érték –1 és 1 között terjed. Fontos, hogy ellenőrizzük a korreláció statisztikai szignifikanciáját, hogy megállapítsuk, hogy a talált kapcsolat valóban jelentős-e, vagy csak véletlen. Emellett más tényezőket is figyelembe kell venni, amelyek befolyásolhatják a kapcsolatot.

Az MI-vel kapcsolatos keresések online megjelenése (H2)

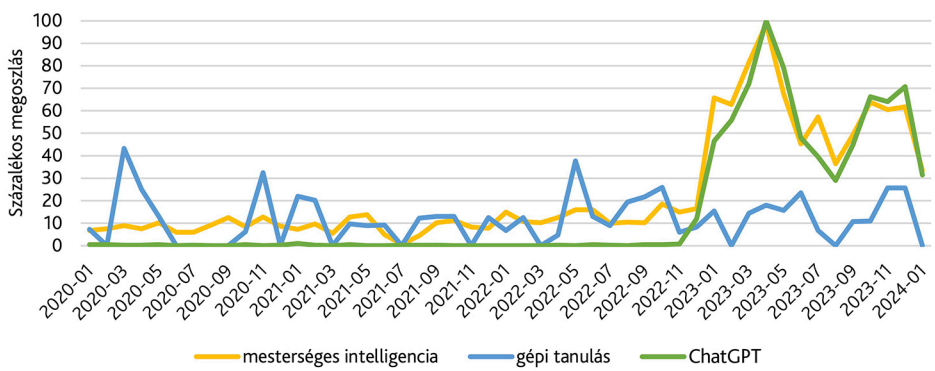
Második hipotézisemben azt állítottam, hogy a ChatGPT megjelenésével és tömeges használatával megerősödtek az MI-vel kapcsolatos kifejezések online megjelenései. Természetesen felmerül a kérdés, hogy pontosan mi is az OpenAI által fejlesztett ChatGPT, és jelen esetben miért tartom fontosnak ennek a vizsgálatát. Maga a ChatGPT egy olyan MI-alapú chatbot, amely a technológia több aspektusát felhasználva, mint például a természetesnyelv-feldolgozás, a gépi tanulás és a *Generative Pre-trained Transformer* (GPT) segítségével képes megválaszolni kérdéseinket, szövegeket összefoglalni, megírni vagy akár kódokat generálni. Maga a GPT a nagy nyelvi modellek egyik típusa, amely a nyelvi feldolgozást segíti elő. 2023 decemberében a szoftver a GPT-3.5-öt használja az ingyenes alkalmazásnál, és a 4.0-t az előfizető felhasználók számára.[14] Magát a ChatGPT-t azért tartom fontosnak a kutatás során, mert úgy vélem, hogy ez volt az a szoftver, amely a mindennapi felhasználókhoz eljuttatta az MI-t (annak ellenére, hogy évtizedek óta velünk van) úgy, hogy az emberek tudtak róla, hogy valóban ilyen technológiát használnak. Korábban az MI olyan problémákra irányult, amelyek esetén a kudarc, mint olyan, költséges volt, mint egy önvezető jármű esetén. Manapság azonban a legkisebb problémáinkra is ott van a ChatGPT vagy több száz egyéb alkalmazás, platform, amelyek hasonló módon akár a bevásárlólistámat vagy a nyaralásomat is megtervezik (persze a bevásárlólistám elrontása is jelentős kudarc).[15]

Az OpenAI-t 2015-ben alapították, egy MI-t kutató szervezetként indult, és 2018-ban mutatta be a GPT-1 modelljét mint az első transzformatív alapú nyelvi modellt. Ezt követően 2019-ben bemutatták a 2-es verziót, amely 1,5 milliárd paraméterrel rendelkezett a korábbi 117 millióhoz képest, és feladatok széles körét tudta elvégezni. Az igazi nagy robbanást a GPT-3 modell hozta, amely 175 milliárd paraméterrel rendelkezett.[16]

[13] Sajtos–Mitev 2007.
[14] Hetler 2023.
[15] Mollick 2022.
[16] Yosifova 2023.

Vizsgálatom során több kifejezésre is rákerestem a Google Trends segítségével, világszintű keresés során az *AI, deep learning, machine learning, artificial intelligence* és *chatgpt* kifejezéseket vizsgálom. Továbbá Magyarországon belül kerestem több magyar kifejezést is, mint *mesterséges intelligencia, gépi tanulás, chatgpt* és *mélytanulás*. Utóbbi esetben azonban nem volt elegendő adat ahhoz, hogy a szoftver diagrammá tudja azt alakítani.

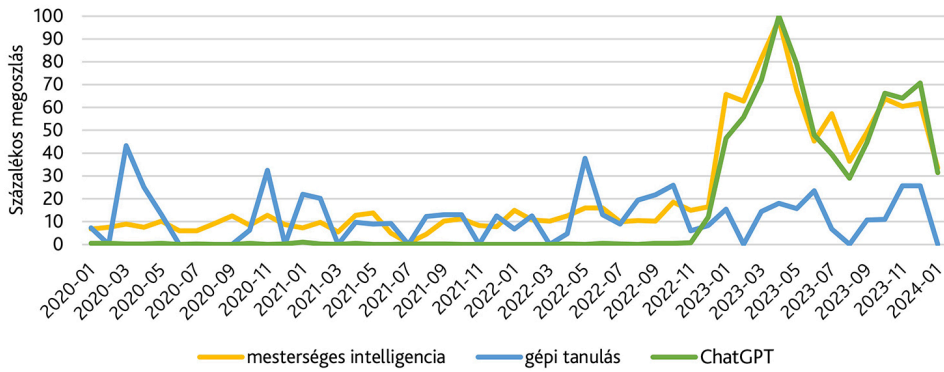
Megvizsgálva az adatokat a magyar kifejezések esetén, valamint az ezek alapján képzett diagramot (1. ábra), látható, hogy a *mesterséges intelligencia* és a *chatgpt* kifejezések 2022. november előtt stagnálnak. Míg a zöld színnel jelölt *chatgpt* keresés eredményeit nem tudta értelmezni a kereső, ami a kevés adatra utal, addig a mesterséges intelligencia is jellemzően 0–25%-os intenzitás között mozog. Ezzel egyidejűleg a ChatGPT megjelenésekor mindkét kifejezés százalékos keresése növekedni kezdett 2022 novembere után, és csúcspontjukat 2023 márciusában érték el. Ezzel egyidejűleg a *gépi tanulás* kifejezés kiugró adatokat produkált, és nincs a korábbi két görbéhez kapcsolható hasonlóság benne.



1. ábra: A mesterséges intelligenciával kapcsolatos kifejezések online keresésének változása Magyarországon

Forrás: a szerző szerkesztése a Google Trends adatai alapján

Nemzetközi szinten vizsgálva a kifejezéseket a korábbiakhoz hasonló eredményeket kaptam. Ahogy a 2. ábrán látható, a kifejezések jellemzően azonos értékeket mutatnak. Ez alól kivétel a *deep learning* és a *machine learning* kifejezések, amelyek nagyobb tartományban ugranak ki már 2022 novembere előtt, továbbá a két kifejezésnek 2022 januárjában is megnövekszik a keresési aránya, ugyanakkor sajnos nem sikerült ezeket a kiugrásokat semmilyen nagyobb eseményhez vagy hírhez kötnöm. Ami azonban itt is megfigyelhető, az az, hogy minden általam vizsgált kifejezés esetében, a ChatGPT nyilvánossá tételével, majd annak a köztudatban való elterjedésével, 2022 novembere után növekedésnek indult, és szintén jellemzően 2023 márciusában érték el a maximális keresési értéküket, a 100%-ot. Fontos azonban megjegyezni, hogy ezeknek a keresése az elmúlt 1 évben nem csökkent jelentősen, azóta is 60% felett, de jellemzően 75–100% között mozog.



2. ábra: A mesterséges intelligenciával kapcsolatos kifejezések online keresésének változása világszinten
Forrás: a szerző szerkesztése a Google Trends adatai alapján

A kapott eredmények alapján második hipotézisemet, miszerint a ChatGPT nyílt használatával felerősödtek az MI-vel kapcsolatos kifejezések online megjelenései, alátámasztom mind nemzetközi szinten, mind Magyarországon, tekintve, hogy a kapott eredmények mind azt igazolják, hogy a technológia nyílt használata, majd elterjedése után ezeknek a kifejezéseknek a keresése megemelkedett, továbbá nemzetközi szinten azóta is kimagasló.

A kérdőíves felmérés főbb eredményei

Maga a kérdőív 2024. január 8–24. között volt elérhető, és ez alatt az idő alatt összesen 127-en töltötték ki, akiknek több mint a fele, 59%-a volt nő. A válaszadók jelentős része 14 és 22 év közötti volt, azonban 29%-uk 23 és 30 év közötti, illetve 14 kitöltő ennél idősebb. Az iskolai végzettséget tekintve a kitöltők 34%-a rendelkezik felsőfokú diplomával, míg 10% csupán általános iskolai bizonyítvánnyal, a kitöltők legnagyobb részének a középfokú végzettség a legmagasabb (71 fő). A tanulói vagy munkavállalói státusz esetében egyszerre több opciót is megjelölhettek. Ez esetben nyugdíjas kitöltő nem volt, és csupán 4% volt munkakereső. A kitöltők legnagyobb része, 75%-a tanuló vagy hallgató, míg 39%-uk munkavállaló. A kérdőívben több MI-technológiával kapcsolatos általános kérdést is feltettem. Ezen eredmények alapján a kitöltők közel 80%-a használt már tudatosan MI-technológiát, és jelentős részük, 25 fő jelölte meg a ChatGPT-t. Vizsgálom továbbá a tájékozottságot és a szkepticizmust a technológiával kapcsolatban, amely kérdésekre háromfokú Likert-skálán lehetett válaszolni. A tájékozottságot vizsgálva a kitöltők 70%-a közepesen tartja magát tájékozottnak, míg az egynegyede nagyon tájékozottnak. Ezt összevetem az MI-vel kapcsolatos állításokkal. Az MI jövőjét tekintve ugyanakkor a kitöltők közel fele optimista, és csupán 16% az, aki pesszimista. Ezeket az eredményeket az 1. táblázat számszerűsítve és százalékos megoszlásban is jól mutatja.

1. táblázat: A kérdőívet kitöltők általános adatai

		Fő	Megoszlás (%)
Nem	Nő	75	59%
	Férfi	52	41%
Életkor	23 évesnél fiatalabb	76	60%
	23–30 éves	37	29%
	31 éves vagy idősebb	14	11%
Iskolai végzettség	Általános iskolai bizonyítvánnyal rendelkezik	13	10%
	Középfokú végzettséggel rendelkezik	71	56%
	Felsőfokú végzettséggel rendelkezik	43	34%
Munkavállalói/hallgatói státusz	Tanuló/hallgató	95	75%
	Munkakereső	5	4%
	Munkavállaló	50	39%
Használt-e már korábban MI-t?	Igen	96	75,6%
	Nem	31	24,4%
Mennyire tartja magát tájékozottnak az MI-vel kapcsolatban?	Nagyon	30	23,6%
	Kevésbé	89	70,1%
	Egyáltalán nem	8	6,3%
Az MI jövőjével kapcsolatos szkepticizmus	Optimista	59	46,5%
	Közömbös	48	37,8%
	Pesszimista	20	15,7%

Forrás: a szerző szerkesztése a kérdőív eredményei alapján

A kérdőívben 6 darab MI-vel kapcsolatos állítást fogalmaztam meg, amelyek közül 3 igaz és 3 hamis állítás volt. Az első állítás, amely szerint az MI minden tevékenységben felülmúlja az embert, valótlan volt, azonban a kitöltők jelentős része inkább vagy teljes mértékben egyetértett az állítással. A nagy adatmennyiséggel kapcsolatos kérdés

szintén hamis volt, azonban itt a kitöltők jelentős része már egyáltalán nem értett egyet az állítással. A természeti katasztrófákat tekintve, a kitöltők csupán 7%-a szerint képes az MI megjósolni és megakadályozni a különböző természeti katasztrófákat, és 39%-uk egyáltalán nem hiszi, hogy ilyenre képes. A természetesnyelv-feldolgozás köztudottan egyik részterülete az MI-technológiának, és a kitöltők jelentős része egyet is értett ezzel az állítással. A jogszabályi keretek közé szorított MI a kitöltőket megosztotta, és szinte 1/3 arányban adták meg a válaszaikat. Az önvezető járművekkel kapcsolatban is nagyjából hasonló arányokról beszélhetünk, azonban ezzel az állítással inkább nem értettek egyet a kitöltők.

2. táblázat: A kitöltők MI-vel kapcsolatos válaszai

MI-vel kapcsolatos állítások	**Egyáltalán nem ért egyet**		**Részben egyetért**		**Teljes mértékben egyetért**	
A mesterséges intelligencia minden feladatban és tevékenységben felülmúlja az emberi intelligenciát	42 fő	33%	79 fő	62%	6 fő	5%
Az MI-rendszereknek jellemzően nincs szükségük nagy mennyiségű adatra a hatékony működéshez	85 fő	67%	28 fő	22%	14 fő	11%
Az MI képes előre jelezni és megakadályozni természeti katasztrófákat	50 fő	39%	68 fő	54%	9 fő	7%
A természetesnyelv-feldolgozás a mesterséges intelligencia egyik részterülete	10 fő	8%	66 fő	52%	51 fő	40%
Az MI különböző területei világszerte jogszabályi keretek közé vannak szorítva	34 fő	27%	53 fő	42%	40 fő	31%
Az önvezető autók már képesek teljesen önállóan közlekedni városi környezetben is	48 fő	38%	52 fő	41%	27 fő	21%

Forrás: a szerző szerkesztése a kérdőív eredményei alapján

A különböző észleléseket vizsgálva, mint fogékonyság, fenyegetés és aggodalom, 5-5 kérdésre a kitöltők egy ötfokú Likert-skálán válaszolhattak az egyáltalán nem és a nagyon szélsőértékek között. A fogékonyságot tekintve, hogy hatással lesz az életükre, befolyásolni fogja a munkaköreiket, a döntéseiket, illetve hogy az MI megreformálja az oktatást és munkahelyek megszűnéséhez fog vezetni, a kitöltők több mint fele lát rá esélyt, jellemzően 80% feletti részük gondolja így.

Abban a tekintetben, hogy mennyire tartják fenyegetésnek az MI-t, annak hibáit, fejlődését, rosszindulatú alkalmazását és az MI-t használó járműveket, a kitöltők már jobban megosztottak. A *nem tudom* köztes lehetőséget viszonylag kevesen választották,

és magától az MI-től, illetve az ezt használó járművektől jellemzően kevésbé tartanak. Ebben az esetben legnagyobb arányban a középső értékek, mint a *nem igazán veszélyes, nem tudom* és *veszélyes* opciókat választották. Ugyanakkor az MI hibáit, fejlődési kockázatait már a kitöltők nagy része veszélyesnek találta, a rosszindulatú felhasználást pedig közel 90%-a sorolta a veszélyes és nagyon veszélyes kategóriákba.

Az észlelt aggodalmat vizsgálva, hogy mennyire aggódik az MI hatásai, az MI-vezérelt megfigyelési technológiák, a növekvő energiafelhasználás környezeti hatásai, a társadalmi és gazdasági egyenlőtlenségre tett hatásai és az álhírek miatt, a válaszok jobban megoszlottak. Az MI hatásai, az MI által vezérelt megfigyelési technológiák, valamint a társadalmi és gazdasági hatásai miatti aggodalom nagyjából egyenlő arányban, két táborra osztotta a kitöltőket, az energiafogyasztás kérdésében közel egyenlő arányban oszlott szét a kitöltők aránya a válaszlehetőségek között. Ugyanakkor az MI által készített *deepfake* és álhírek a kitöltők 75%-át aggodalommal tölti el.

3. táblázat: A kitöltők észlelésekre adott válaszai

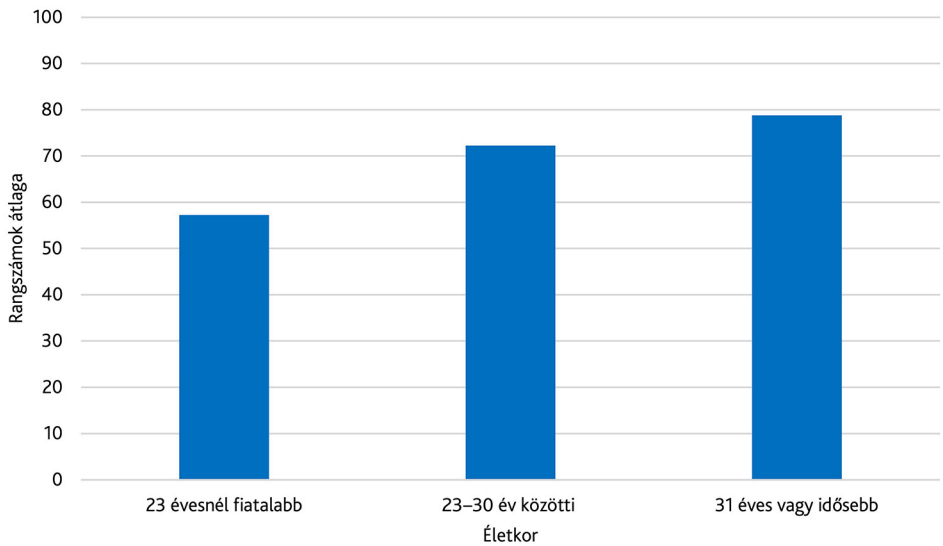
Észlelt fogékonyság	**Nem lát rá esélyt**		**Kevésbé lát rá esélyt**		**Nem tudom**		**Lát rá esélyt**		**Nagy esélyt lát rá**	
A jövőben az MI jelentősen befolyásolni fogja a jelenlegi/leendő munkakörét	8 fő	6%	16 fő	13%	6 fő	5%	63 fő	50%	34 fő	27%
Az elkövetkezendő 1–2 évben az MI hatással lesz az ön személyes adatbiztonságára és magánéletére	5 fő	4%	9 fő	7%	21 fő	17%	62 fő	49%	30 fő	24%
Az MI-algoritmusok befolyásolni fogják önt a jövőben meghozandó döntéseiben	17 fő	13%	28 fő	22%	17 fő	13%	48 fő	38%	17 fő	13%
Az MI jelentős változásokat fog hozni az oktatás területén	1 fő	1%	8 fő	6%	5 fő	4%	54 fő	43%	59 fő	46%
A következő 1–2 évben az MI munkahelyek megszűnéséhez fog vezetni	11 fő	9%	16 fő	13%	11 fő	9%	50 fő	39%	39 fő	31%

Észlelt fenyegetés	Egyáltalán nem veszélyes		Nem igazán veszélyes		Nem tudom		Veszélyes		Nagyon veszélyes	
A mesterséges intelligencia	10 fő	8%	38 fő	30%	29 fő	23%	42 fő	33%	8 fő	6%
Az MI hibái vagy hibáinak lehetséges következményei	4 fő	3%	15 fő	12%	17 fő	13%	66 fő	52%	25 fő	20%
Az MI fejlődésével kapcsolatos lehetséges kockázatok	6 fő	5%	15 fő	12%	26 fő	20%	65 fő	51%	15 fő	12%
Az MI rosszindulatú felhasználása	3 fő	2%	6 fő	5%	4 fő	3%	36 fő	28%	78 fő	61%
A különböző MI-vel működő önvezető járművek	9 fő	7%	32 fő	25%	24 fő	19%	41 fő	32%	21 fő	17%
Észlelt aggodalom	**Egyáltalán nem aggódik**		**Kevésbé aggódik**		**Nem tudom**		**Aggódik**		**Nagyon aggódik**	
Az MI hatásai miatt	17 fő	13%	53	42%	14	11%	36	28%	7	6%
Az MI által vezérelt megfigyelési technológiák miatt	12 fő	9%	31	24%	15	12%	53	42%	16	13%
A mesterséges intelligencia a megnövekedett energiafogyasztás miatt negatív hatással lehet a környezetre	23 fő	18%	35	28%	35	28%	23	18%	11	9%
Az MI társadalmi és gazdasági egyenlőtlenségekre gyakorolt hatása miatt	14 fő	11%	36	28%	30	24%	39	31%	8	6%
Az MI által generált mélyen hamisított tartalmak és álhírek	7 fő	6%	15	12%	13	10%	43	34%	49	39%

Forrás: a szerző szerkesztése a kérdőív eredményei alapján

A kapott adatok alapján kereszttábla-elemzéssel megvizsgálom, hogy van-e szignifikáns különbség a nemhez tartozás tekintetében és abban, hogy használt-e már korábban tudatosan MI-hez kapcsolódó technológiát az illető. A kapott eredmények alapján a teszt sikeresen lefutott a hibaráta alatt (0%), azonban eredményként az mondható el, hogy nincs a változók között összefüggés, ugyanis a szignifikanciaszint magasabb, mint 0,05 (s = 0,121), tehát a nemhez tartozástól függetlenül használtak már ilyen technológiát.

Az életkor és az informáltság kérdéskörét tekintve, Kruskal–Wallis-teszttel vetettem össze a változókat, és a hat informáltsággal kapcsolatos kérdésnél összesen egy esetben van szignifikáns különbség, mégpedig annál, hogy *az MI különböző területei világszerte jogszabályi keretek közé vannak szorítva*. A kérdésekre adott válaszok és a rangszámok átlaga alapján elmondható, hogy minél idősebb korosztályba tartozik egy illető, jellemzően annál jobban volt tisztában azzal, hogy a kérdőív kitöltésekor még egy jellemzően szabályozatlan területről beszélhettünk. Ezt a 3. ábra is jól mutatja.



3. ábra: Az életkor és az informáltság vizsgálata „az MI különböző területei világszerte jogszabályi keretek közé van szorítva" kérdéssel kapcsolatban
Forrás: a szerző szerkesztése a kérdőív eredményei alapján

Az informáltságot tovább vizsgáltam, miszerint a végzettség és az, hogy mennyire érzi magát tájékozottnak egy adott személy, vajon kapcsolatban állnak-e. Azonban mindkét változó esetén a szignifikanciaszint meghaladta az 5%-ot, így elmondható, hogy nincs szignifikáns különbség a végzettség és az informáltság között, továbbá aközött, hogy mennyire ítéli meg magát tájékozottnak egy adott személy.

A kérdőíves felmérés során korrelációelemzéssel vizsgáltam az UTAUT2 modell mentén a kitöltők új technológiához való hozzáállását. Ennek során 9, a modell alapján befolyásoló témakör szerint 2-2 állítást hoztam, összesen 18-at. Ezekre az *egyáltalán nem ért egyet* opciótól a *teljesen egyetért*ig ötfokú Likert-skálán lehetett válaszolni. A kérdőívben feltettem a kérdést, hogy korábban használt-e már MI-alapú technológiai megoldást, és az erre adott válaszokat elemeztem az UTAUT2 modell állításaira adott feleletekkel. A teszt során a kapott válaszok eredményeit értékekkel láttam el 1-től 5-ig, majd ezeknek vettem a kerekített átlagait, így megkapva a tudatosság, fogékonyság, fenyegetés, aggodalom,

teljesítményvárakozás, erőfeszítés-várakozás, társadalmi befolyás, elősegítő feltételek, hedonista motiváció, ár-érték, szokás, magatartási szándék, használói magatartás átlagait.

Az eredményeket megvizsgálva, a tudatosság és észlelések kérdéskört tekintve nem volt szignifikáns különbség a változók között, így elmondható, hogy nincs rá bizonyíték, hogy a technológiához való hozzáállást befolyásolná a tudatosság és a különböző általam vizsgált észlelések, mint az aggodalom, a fogékonyság és a fenyegetettség. Tovább vizsgálva az UTAUT2-es kérdésköröket, egyedül a társadalmi befolyásolás és az erőfeszítés-várakozás esetén nincs szignifikáns különbség (s = 0,131, 0,117), azonban az összes többi esetén rendben vannak az értékek (4. táblázat).

4. táblázat: A korrelációs teszt eredményei

	Pearson-féle korreláció	**Szignifikanciaszint**
Tudatosságátlag	–0,024	0,785
Fogékonyságátlag	–0,024	0,785
Fenyegetésátlag	0,033	0,710
Észlelt aggodalom átlaga	–0,046	0,606
Teljesítményvárakozás	–0,377	0,000
Erőfeszítés-várakozás	–0,140	0,117
Társadalmi befolyás	–0,135	0,131
Elősegítő feltételek	–0,505	0,000
Hedonista motiváció	–0,281	0,001
Ár-érték	–0,289	0,001
Szokás	–0,377	0,000
Magatartási szándék	–0,452	0,000
Használói magatartás	–0,513	0,000

Forrás: a szerző szerkesztése a kérdőív eredményei alapján

A kapott korrelációs eredmények minden esetben közepes negatív értéket kaptak ($-0,7 < r \leq -0,2$). Ezek alapján elmondható, hogy teljesítményvárakozás, elősegítő feltételek, hedonista motiváció, ár-érték, szokás, magatartási szándék, használói magatartás negatív kapcsolatot mutat a használattal. Tehát megállapítható, hogy akik korábban már használtak MI-alapú technológiát, azok jellemzően:

1. kevésbé látják úgy, hogy az segíti őket a teljesítményük javításában;
2. kevésbé érzik azt, hogy a szükséges feltételek és támogatás rendelkezésre állnak az új technológia használatához;
3. kevésbé motiváltak arra, hogy kipróbálják vagy elfogadják az új technológiát;
4. kevésbé érzik azt, hogy az új technológia értéke meghaladja annak költségeit;
5. kevésbé alakítottak ki szokást a technológia használatában;

6. kevésbé hajlamosak új szokásokat kialakítani az új technológia használatában;
7. kevésbé elégedettek a technológia által elért eredményekkel, nem szívesen bátorítanának mást annak a használatára.

A kérdőíves felméréssel kapcsolatos hipotézis vizsgálata (H1)

A kérdőívhez kapcsolódóan 1 hipotézist fogalmaztam meg. Első hipotézisemben az MI-vel kapcsolatos informáltság és az aggodalom, fenyegetés és fogékonyság kérdések közötti szignifikáns különbséget vizsgáltam. A vizsgálat során homogén csoportokat, azaz klasztereket hoztam létre az informáltságra adott válaszok alapján. A Ward-féle eljárással képzett dendrogram alapján kétklaszteres eljárást választottam, továbbá Kruskal–Wallis-eljárással a rangszámok átlaga alapján az első csoportba tartozó személyek jellemzően azok, akik informáltabbak a technológiával kapcsolatban.[17] Jelen esetben minél magasabb a rangszámok átlaga, annál inkább informált egy csoport, és az első klaszternél ez a szám jellemzően magasabb.

Ezeket az informáltság alapján képzett klasztereket összevetettem a Kruskal–Wallis-teszt során a különböző érzelmekre adott válaszokkal. Elmondható, hogy a klaszterek nem mutatnak szignifikáns különbséget a fogékonyság és fenyegetés kérdéskörökre adott válaszokkal, azonban az aggodalom esetén két kérdésnél volt kapcsolat. Az MI hatásai és az MI által vezérelt megfigyelési technológiák miatti aggodalom esetén a szignifikanciaszint alacsonyabb volt, mint 5% (0,009, 0,001). Így elmondható, hogy az informáltság alapján képzett klaszterek és az MI-vel kapcsolatos aggodalom bizonyos esetekben összefügg, azonban jellemzően nincs szignifikáns különbség a változók között, így az első hipotézisemet megcáfolom.

Összegzés

A kutatásban több hipotézist megvizsgáltam, amelynek során primer kutatást végeztem. A Google Trends platform segítségével az online kereséseket vizsgáltam, és az ebben kialakult trendeket elemeztem, miközben H2 hipotézisemet alátámasztom, miszerint a ChatGPT megjelenésével az MI-vel kapcsolatos keresések száma megnövekedett. Azt vizsgálni nem volt lehetőségem, hogy pontosan a ChatGPT volt-e az oka a kiugrásoknak, azonban azt sikerült megállapítani, hogy a publikálást követő időszakban a keresések magasabb számban voltak jelen a Google platformjain, és ez napjainkra is jellemző. Azt is megállapítottam, hogy a platform elérhetővé tételével a keresések száma hirtelen kiugró értékeket ért el, ezek alapján pedig második hipotézisemet igazolom. Ezt követően a kérdőíves elemzésem módszertani részét mutattam be, mint a használt felületet és módszereket, illetve a szerkezetét, majd a kérdőívvel kapcsolatos kitöltéseket és eredményeket. Ezt követően több elemzést is elvégeztem, főként az informáltság vizsgálatát, és megállapítottam, hogy az általam összevetett változók jellemzően nincsenek vele kapcsolatban. Kivétel volt ez alól az életkor és

[17] Sajtos–Mitev 2007.

az informáltság, ahol egy kérdés esetében elmondható, hogy minél idősebb korosztályba tartozik valaki, annál inkább van tisztában az MI jogszabályi kereteivel.

A H1 hipotézisem során vizsgáltam az informáltság és az észlelések kapcsolatát, több eljárást is végrehajtottam az elemzés érdekében. Az általam képzett klaszterek azonban két aggodalom körében adott válaszok alapján voltak kapcsolatban, így ezt a hipotézist elvetettem, jellemzően nincsenek kapcsolatban az informáltság és az észlelésekre adott válaszok. Az első hipotézisem bizonyítása megbukott a szignifikanciaszint hiányában, és elmondható, hogy nincs kapcsolat aközött, hogy használt-e már valaki MI-technológiát, és aközött, hogy mennyire tart a jövőbeli következményeitől.

Felhasznált irodalom

Ain, NooUi – Kaur, Kiran – Waheed, Mehwish (2016): The Influence of Learning Value on Learning Management System Use: An Extension of UTAUT2. *Information Development,* 32(5), 1306–1321. Online: https://doi.org/10.1177/0266666915597546

Csallner András Erik (2015): *Bevezetés az SPSS statisztikai programcsomag használatába.* Jegyzet. Szeged: SZTE Juhász Gyula Pedagógusképző Kar. Online: http://www.inf.u-szeged.hu/~banhelyi/okt/SPSS_2021tavasz/csallner-spss-javitott.pdf

European Parliament (2021): *Artificial Intelligence Act.* Online: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf

Hetler, Amanda (2023): What is ChatGPT? *TechTarget,* 2025. március 4. Online: https://www.techtarget.com/whatis/definition/ChatGPT

ISO [é. n.]: *What is Artificial Intelligence (AI)?* Online: https://www.iso.org/artificial-intelligence/what-is-ai

Laerd Statistics [é. n.]: *Kruskal-Wallis H Test Using in SPSS Statistics.* Online: https://statistics.laerd.com/spss-tutorials/kruskal-wallis-h-test-using-spss-statistics.php

Mollick, Ethan (2022): ChatGPT Is a Tipping Point for AI. *Harvard Business Review,* 2022. december 14. Online: https://hbr.org/2022/12/chatgpt-is-a-tipping-point-for-ai

Sajtos László – Mitev Ariel (2007): *SPSS kutatási és adatelemzési kézikönyv.* Budapest: Alinea Kiadó.

Walsh, Shelley (2025): Timeline of ChatGPT Updates & Key Events. *Search Engine Journal,* 2025. október 9. Online: https://www.searchenginejournal.com/history-of-chatgpt-timeline/488370/

Yosifova, Aleksandra (2023): The Evolution of ChatGPT: History and Future. *365 DataScience,* 2023. augusztus 14. Online: https://365datascience.com/trending/the-evolution-of-chatgpt-history-and-future/

HADMÉRNÖK
VÉDELEMINFORMATIKA

20. évfolyam (2025) 2. szám 129–142.
DOI: 10.32567/hm.2025.2.8

Szabó Gergő[1]

A generatív mesterséges intelligencia használata a kibertudatosítási képzésekben, 1. rész

The Use of Generative Artificial Intelligence in Cybersecurity Awareness Training, Part 1

Absztrakt

A tanulmány célja annak vizsgálata, hogy miként alkalmazható a generatív mesterséges intelligencia (GenMI) a kibertudatossági képzésekben, különös tekintettel az oktatás személyreszabhatóságára, hatékonyságára és elfogadottságára. A kutatás elméleti része az ADDIE-modell mentén tárgyalja a GenMI szerepét az oktatástervezésben, bemutatva annak lehetőségeit a tananyagfejlesztés, a személyre szabás és a visszacsatolás területén. Részletesen ismerteti a RAG-technológia szerepét is, különösen a tartalmi pontosság és az adatbiztonság aspektusaira fókuszálva. Az empirikus kutatás egy 109 fő részvételével végzett kérdőíves vizsgálatra épül, amelyet a Technology Acceptance Model (TAM) keretrendszere szerint szerkesztettem. A kérdőív többek között phishing szimulációkat, egy generált szcenáriót, valamint attitűdkérdéseket tartalmazott.

Kulcsszavak: mesterséges intelligencia, kibertér, kibertámadás

Abstract

This study examines how generative artificial intelligence (GenAI) can be applied in cybersecurity awareness training, with particular emphasis on personalisation, effectiveness, and user acceptance. The theoretical section follows the ADDIE instructional design model and explores the role of GenAI in educational planning, highlighting its potential in content development, adaptive learning, and feedback mechanisms. Special attention is given to

[1] Hallgató, Nemzeti Közszolgálati Egyetem, e-mail: sz.gergo628@gmail.com

Retrieval-Augmented Generation (RAG) technologies, focusing on content accuracy and data protection considerations.

The empirical part of the research is based on a questionnaire survey conducted with 109 participants and designed according to the Technology Acceptance Model (TAM). The questionnaire included phishing simulations, an AI-generated cybersecurity scenario, and attitude-based questions. The aim of the study is to assess how non-expert users perceive and evaluate cybersecurity training materials generated by artificial intelligence, and to identify key factors influencing their acceptance and perceived usefulness.

Keywords: artificial intelligence, cybersecurity, awareness training, phishing

Bevezetés

A digitális technológiák fokozódó jelenléte a munkahelyi és a magánélet területén egyre inkább indokolttá teszi a kiberbiztonsági tudatosság fejlesztését. Az olyan fenyegetések, mint az adathalászat, a célzott támadások vagy a social engineering,[2] gyakran nem technikai sebezhetőségeken, hanem emberi tényezőkön keresztül érik el céljukat.

A SlashNext 2023-ról készült jelentése szerint a ChatGPT megjelenését követő évben 1265%-kal nőtt a rosszindulatú adathalász-e-mailek száma, különösen a hitelesítő adatokat célzó támadásokban. Ugyanebben az időszakban a magyar nyelv védőhatása is megszűnni látszik, a generatív mesterséges intelligencia (GenMI) eszközeinek segítségével már anyanyelvi szintű adathalász-üzeneteket is lehet készíteni, megszüntetve ezzel a korábbi figyelmeztető nyelvi hibákat.[3]

A leghatékonyabb védekezést ebben az esetben a megfelelő ismeretanyag és felkészültség biztosítja, amelyet célzott oktatási programok révén lehet fejleszteni.

A GenMI, különösen a nagy nyelvi modellek (Large Language Modells, LLM) megjelenésével új távlatok nyíltak az oktatás személyre szabása terén. Az ilyen rendszerek képesek az egyéni tudásszinthez, tanulási stílushoz vagy motivációhoz illeszkedő szcenáriók, példák és magyarázatok generálására, így támogatva az adaptív tanulást. Ez a megközelítés különösen ígéretes a kiberbiztonsághoz hasonló, dinamikusan változó területeken, ahol az oktatási tartalmak gyors elavulása állandó kihívást jelent.

Ugyanakkor a GenMI által generált tartalmak használata etikai, minőségi és elfogadottsági kérdéseket is felvet: vajon megbízhatók-e ezek az anyagok? Mennyire tanulnak belőlük az emberek? És milyen mértékben fogadják el az ilyen típusú oktatást azok, akik nem rendelkeznek mélyebb technológiai ismeretekkel?

A kutatás ezekre a kérdésekre keresi a választ, az elméleti háttér áttekintése mellett pedig egy kérdőíves vizsgálatot is tartalmaz. A vizsgálat célja, hogy felmérje a generatív mesterséges intelligenciával létrehozott kiberbiztonsági

[2] Olyan manipulációs technikák összessége, amelyeket arra használnak, hogy az embereket bizalmas információk, például jelszavak, pénzügyi adatok vagy hozzáférési jogosultságok önkéntes kiadására vegyék rá, gyakran azzal, hogy megbízható forrásnak álcázzák magukat a támadók. Lásd: Shaw et al. 2009.

[3] SlashNext 2023.

oktatási szcenáriók elfogadottságát és értékelését nem szakmabeli felhasználók körében. A cikksorozat első részében az elméleti háttér és a rendelkezésre álló technológiai megoldások áttekintéséről lesz szó, míg a második rész a kutatási kérdéseket és a kérdésekhez kapcsolódó hipotézisek tesztelését mutatja be.

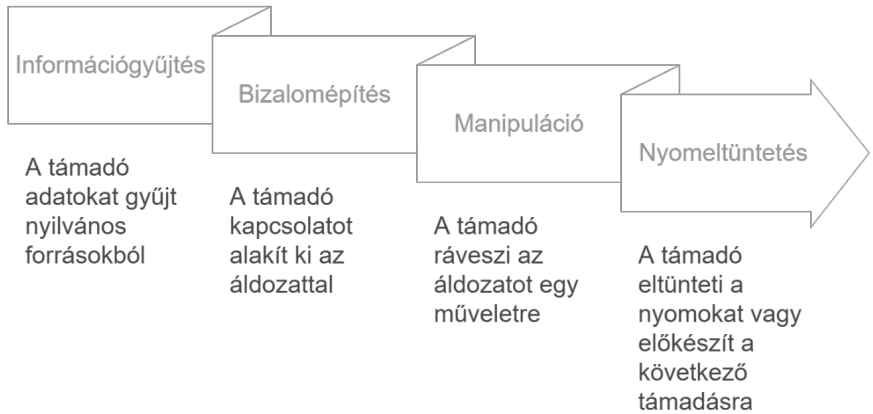
A generatív mesterséges intelligencia szerepe a kiberbiztonsági oktatásban

A fejezet tárgyalása előtt fontos röviden tisztázni néhány gyakran egymás helyett használt, de tartalmilag eltérő fogalmat. Az információvédelem az információk védelmét jelenti a jogosulatlan hozzáféréstől, függetlenül attól, hogy azok digitális vagy fizikai formában léteznek. Ennek egy szűkebb, technológiai fókuszú része az informatikai biztonság, amely az információkat kezelő rendszerek, hálózatok és szerverek védelmére koncentrál. Ezzel szemben a kiberbiztonság már kifejezetten a hálózati környezetben megjelenő fenyegetések, például adathalászat és zsarolóvírusok elleni védelmet helyezi előtérbe. Végül a kibervédelem elsősorban a nemzeti vagy kritikus infrastruktúrák védelmére használt fogalom, amely magában foglalja a technikai mellett a stratégiai, jogi és szervezeti védekezési mechanizmusokat.[4]

A kibervédelem napjainkban dinamikusan fejlődő szakterület, hiszen folyamatosan jelennek meg újabb támadási vektorok és kritikus sérülékenységek. Az egyik legrégebb óta jelen lévő, ugyanakkor máig kiemelten veszélyes támadási forma a social engineering, ezen belül is az adathalászat. A social engineering célja, hogy a támadó a felhasználó jóhiszeműségét kihasználva szerezzen hozzáférést védett rendszerekhez, vagy szivárogtasson ki érzékeny személyes, üzleti vagy piaci adatokat, jellemzően haszonszerzés céljából.

A támadások sokszor egy jól felépített manipulációs folyamatra épülnek. Ezt a folyamatot jól modellezi a Social Engineering Attack Framework (social engineering támadási keretrendszer, SEAF),[5] amely négy fő fázisból áll. Első lépés az információgyűjtés, amikor a támadó a célpontról adatokat gyűjt nyilvános forrásokból vagy közösségi médiából. Második lépésként a támadó interakcióba lép az áldozattal, és bizalmi kapcsolatot alakít ki. Harmadik lépésként a támadó a megszerzett bizalom révén rábírja az áldozatot valamilyen műveletre, például linkre kattintásra vagy adatok átadására. Végezetül a támadás befejeződik, a támadó eltünteti a nyomokat, vagy további támadásokat készít elő (1. ábra).

[4] Merritt 2024.
[5] Mouton et al. 2014.



1. ábra: A SEAF fázisai
Forrás: a szerző szerkesztése

Ez a támadási módszer elsősorban az alkalmazottakat célozza, hiszen minden munkavállalónak szüksége van valamilyen fokú jogosultságra feladatai ellátásához. Az ő megtévesztésük révén a támadók képesek megkerülni a technikai védelmi rendszereket is, ezért terjedt el a kibervédelmi szakmában az a mondás, hogy „a kiberbiztonság leggyengébb láncszeme maga az ember".

A kiberfenyegetések változó természete és az oktatás szükségessége

A Verizon adatai szerint az adatszivárgások több mint 74%-a közvetlenül az emberi tényezőre vezethető vissza,[6] beleértve a hibás döntéshozatalt, a gyenge jelszavak használatát vagy a figyelmetlen linkkattintást. Ezzel párhuzamosan a Proofpoint kutatása arra figyelmeztet, hogy a szervezetek 90%-a nem technikai áttörések, hanem social engineering és célzott adathalászat révén kerül veszélybe.[7] Ezt a képet erősíti az ENISA Threat Landscape 2024 is, amely alapján a válaszadók 31%-a szerint a felhasználói hiba volt az incidens kiváltó oka, míg 17% a többlépcsős hitelesítés (multi-factor authentication, MFA) hiányát nevezte meg a támadás fő tényezőjeként, tehát az incidensek legalább 48%-a emberi mulasztásra vagy hiányosságra vezethető vissza.[8]

A helyzetet tovább súlyosbítja a generatív mesterséges intelligencia gyors térnyerése, amely a támadók kezében is hatékony eszközzé vált. A SlashNext jelentése szerint a ChatGPT nyilvános megjelenését követő egy éven belül az MI által támogatott adathalászkampányok száma 1265%-kal nőtt. Ez különösen az e-mailek nyelvi hitelességét és személyre szabását érinti: a támadók ma már képesek anyanyelvi

[6] Verizon 2024.
[7] Proofpoint 2023.
[8] European Union Agency for Cybersecurity 2024.

szintű, kontextushoz illesztett és pszichológiailag célzott üzeneteket generálni, ez pedig a felhasználók számára rendkívül megnehezíti a megtévesztés felismerését.[9]

Mindez világosan rámutat arra, hogy a hagyományos, évente egyszer tartott kibertudatossági képzés már nem elegendő a mai fenyegetettségi környezetben. Az oktatásnak alkalmazkodnia kell a gyorsan változó támadási technikákhoz, figyelembe kell vennie a résztvevők eltérő előismereteit, és folyamatos, valós idejű visszacsatolással kell támogatnia a tanulási folyamatot.

A generatív mesterséges intelligencia e téren új lehetőségeket kínál, képes valósághű, egyénre szabott szcenáriók generálására, amelyek lehetővé teszik, hogy a tanulók biztonságos környezetben tapasztalják meg a különböző támadások működését és következményeit. Ezáltal nemcsak az elméleti tudás mélyül, hanem a gyakorlati felkészültség és a helyzetfelismerési készség is fejlődik.

Ez a trend azonban túlmutat a technológiai újításokon, stratégiai jelentőségű. A képzések személyre szabása, különösen a kiberbiztonság területén, a szervezeti reziliencia egyik kulcsfontosságú tényezőjévé válik. A generatív mesterséges intelligencia ebben a kontextusban nem csupán egy új eszközként, hanem új oktatási paradigma előfutáraként jelenik meg.

A generatív mesterséges intelligencia támogatási lehetőségei a NIST CPLP keretrendszerben

A kibertudatossági oktatási tervet minden szervezetnek saját kockázatelemzése és értékelése alapján kell kialakítania. Nem létezik univerzálisan alkalmazható sablon, amely minden környezetben módosítás nélkül használható lenne. A kockázatértékelés eredményei határozzák meg azokat a stratégiai szempontokat és prioritásokat, amelyek mentén az oktatási célok kijelölhetők. Ezek figyelembevételével alakítható ki egy olyan tanulási program, amely illeszkedik a szervezet fenyegetettségi profiljához és kockázattűrő képességéhez.

Ezt a megközelítést a National Institute of Standards and Technology Cybersecurity and Privacy Learning Program (Szabványügyi és Technológiai Nemzeti Intézet Kiberbiztonsági és Adatvédelmi Tanulási Programja, NIST CPLP) szerzői is hangsúlyozzák, a kiberbiztonság nem kizárólag technológiai vagy IT-feladat, hanem szervezeti szintű felelősség, amelyben minden szereplőnek, az első számú vezetőtől a beosztott munkatársakig, van szerepe.[10]

Ami minden jól működő kibertudatossági oktatási terv közös vonása, az a biztonsági kultúra kialakítása iránti igény. A szervezeten belül minden szinten meg kell hogy jelenjen az a szemlélet, amely támogatja, ösztönzi és fenntartja a biztonságtudatos viselkedést. A biztonsági kultúra kialakításának igénye azonban nem alulról, hanem felülről kell hogy induljon, a felső vezetés részéről, stratégiai szintről kell érkeznie annak az elköteleződésnek, amely megalapozza a célok megfogalmazását, és biztosítja az oktatási program végrehajtásához szükséges jogosítványokat.

[9] SlashNext 2023.
[10] Merritt et al. 2024.

A stratégiai tervben a vállalat vezetésének világosan meg kell határoznia azokat az alapelveket és irányvonalakat, amelyek mentén a kibertudatossági képzés kialakítható. Idetartozik a szervezet víziója és küldetése, a stratégiai célok és feladatok, az oktatás megközelítése és résztervei, az alkalmazandó eljárásrendek, valamint azok a mérőszámok és jelentési rendszerek, amelyekkel a program hatékonysága mérhető.

A stratégiai irányvonalak részét képezi a szervezet kockázatkezelési eljárásrendje is. A kialakított biztonsági kultúra lehetőséget teremt arra, hogy az alkalmazottak a saját kockázatértékelésük alapján hozhassanak döntéseket.[11]

A képzések elsődleges célja a tudásbeli és készségszintű hiányosságok azonosítása és pótlása. A NIST CPLP ebben a kontextusban kifejezetten javasolja a generatív mesterséges intelligencián alapuló tananyagok és szerepkör-specifikus képzések alkalmazását. Ennek köszönhetően minden alkalmazott olyan, a saját munkakörére szabott biztonsági ismereteket szerezhet, amelyek közvetlenül hozzájárulnak a szervezet átfogó kiberbiztonságához és kockázatkezelési stratégiájához.

A képzési programoknak szorosan illeszkedniük kell a stratégiai tervben rögzített vállalati célkitűzésekhez, valamint a kockázatkezelési elvekhez és a hatályos adatvédelmi és megfelelőségi *(compliance)* előírásokhoz. A képzések hatékonyságát folyamatosan monitorozni szükséges, például az alkalmazottak viselkedésének változása vagy az incidensek számának alakulása alapján, így lehetőség nyílik az oktatási program folyamatos fejlesztésére.

A kibertudatossági oktatás másik alappillérét a vállalati szabályzatok és eljárásrendek képezik. Ezek világosan megfogalmazzák a szervezet elvárásait az alkalmazottak felé: mit és hogyan kell végrehajtani. A szabályoknak egyszerű, közérthető állításoknak kell lenniük, amelyek az elvárt viselkedést határozzák meg. Az eljárásrendek rögzítik, hogyan történik a szabályok gyakorlati végrehajtása, meghatározzák az egyes szereplők felelősségi köreit, a végrehajtás lépéseit és fázisait, valamint a kapcsolódó dokumentációkat.

Fontos, hogy ezek a szabályzatok és eljárásrendek összhangban legyenek a vállalat más, nem kiberbiztonsági területeken alkalmazott belső irányelveivel. Ez garantálja, hogy az alkalmazottak számára érthető, elfogadható és teljesíthető napi elvárások szülessenek. Idetartozhat például az üzletfolytonossági terv vagy a katasztrófaelhárítási protokoll is.

Ezek összessége adja meg azt a stabil alapot, amelyre egy hatékony kibertudatossági oktatási terv épülhet. Az alkalmazottaknak éppen ezeket a szabályokat és eljárásrendeket kell megismerniük, és ezek végrehajtására kell őket felkészíteni a képzés során. Ezután kezdődhet meg az oktatási terv kidolgozása az ADDIE-modell mentén, amelyet a következőkben kiberbiztonsági szempontból elemzek.

Elemzés

A generatív mesterséges intelligencia ebben a szakaszban jelentős támogatást nyújthat az oktatási tervet készítők számára. A GenMI képes gyorsan elvégezni az adatgyűjtést és a trendanalízist, például a legfrissebb közismert sebezhetőségek és kitettségek

[11] Merritt et al. 2024.

adatbázisának (Common Vulnerabilities and Exposures, CVE[12]) feldolgozásával. Mivel ezek az adatbázisok a legkritikusabb sebezhetőségeket listázzák, figyelmen kívül hagyásuk jelentősen növeli a szervezeti kockázatot. A GenMI ezenkívül képes szakcikkek, iparági jelentések és kiberbiztonsági kutatások gyors áttekintésére is, és az ezekből kinyert tudást képes összevetni a szervezet korábbi biztonsági eseményeivel. Ennek eredményeképp azonosíthatók azok a kihívások és fenyegetések, amelyekre az oktatási tervnek reagálnia kell.

A fenti adatokra építve a GenMI segíthet a tananyag összeállításában, biztosítva annak naprakészségét, különösen akkor, ha új támadási vektorok jelennek meg. A vállalat stratégiai célkitűzéseinek figyelembevételével az MI javaslatokat tehet a fenyegetések rangsorolására is, így a képzés a legrelevánsabb és legsürgetőbb problémákra összpontosíthat.

Amennyiben a vállalat korábban már tartott kibertudatossági tréningeket, a mesterséges intelligencia képes feldolgozni az ezekből származó visszacsatolásokat, beleértve a nyílt szöveges válaszokat is. A természetesnyelv-feldolgozás technológiájával az MI képes elemezni a kulcskifejezéseket, problémás tartalmakat, és ezáltal segítheti a tréningfejlesztőket abban, hogy a hibásan értelmezett vagy alulteljesített területeket javítsák.

Tervezés és fejlesztés

A GenMI képes a munkavállalók korábbi tréningjeiből vagy előzetes felmérésekből származó eredmények alapján azonosítani az egyéni hiányosságokat és erősségeket. Ezek alapján tanulói profilokat alakít ki, amelyekre építve különböző nehézségi szintű oktatási tartalmak állíthatók össze. A kezdők számára az alapfogalmak és a gyakorlati példák kapnak nagyobb hangsúlyt, míg a haladó szintű felhasználók számára technikai elemzéseket, esettanulmányokat és szimulációkat kínál a rendszer.

A generatív mesterséges intelligencia az oktatás gyakorlati dimenziójában is kulcsszerepet játszik. Lehetővé teszi interaktív, valósághű szimulációk generálását, amelyek során a dolgozók a megszerzett kiberbiztonsági ismereteket biztonságos környezetben alkalmazhatják. Ilyen például a HacWare által fejlesztett MI-eszköz, amely minden munkavállaló számára egyedi adathalász-e-maileket generál a valós támadási mintázatok alapján. Nem egységes kampányok futnak tehát, hanem személyre szabott, dinamikusan változó tartalmakat küld ki a rendszer.[13] Fontos ugyanakkor megjegyezni, hogy kormányzati vagy magasabb biztonsági osztályba sorolt rendszerek esetében az ilyen „teszttámadások" generálása különösen körültekintő tervezést, valamint előzetes engedélyezést igényelhet.

A GenMI emellett képes valós incidensek elemzésére, és azok alapján olyan szimulációs forgatókönyvek előállítására, amelyek tükrözik az adott szervezet valóságos működését. Ezek a forgatókönyvek könnyen paraméterezhetők, így a különböző

[12] CVE: Egy nyilvános, szabványosított elnevezést és azonosítót biztosító adatbázis az ismert szoftveres és hardveres sebezhetőségek számára. A CVE-azonosító célja, hogy a különböző biztonsági eszközök és szolgáltatások ugyanarra a sebezhetőségre egységes hivatkozással tudjanak utalni. Lásd CVE [é. n.].

[13] AI-Generated Phishing Simulations Are a Game Changer for MSPs 2023.

szervezeti egységek, például az IT, a kiberbiztonsági részleg vagy a marketingosztály tudásszintjéhez és feladataihoz igazodó szituációk generálhatók. A szimulációk csoportos formában is megvalósíthatók, ezzel is szemléltetve, hogyan képes egy ártalmatlannak tűnő incidens gyorsan eszkalálódni.

A multimédiás tartalmak integrálása szintén hozzájárul az élményszerű tanuláshoz. A GenMI képes infografikákat, oktatóvideókat vagy interaktív vizuális elemeket létrehozni, amelyek például bemutatják az adathalász-támadások evolúcióját. A deepfake technológia, amelyet a kiberbűnözők is egyre gyakrabban használnak, visszafordítható az oktatás szolgálatába. A Breacher.ai például deepfake videókkal és hangfelvételekkel támogatja a szimulációs tréningeket: ezek révén a dolgozók valósághű, megtévesztő MI-tartalmakkal találkozhatnak, amelyeket biztonságos környezetben tanulnak felismerni.[14]

Egy empirikus kutatásban Brito és munkatársai egy rövid, elméleti és gyakorlati elemeket is tartalmazó, mesterséges intelligenciát bemutató modult illesztettek be hat kiberbiztonsági kurzusba, amelyet kérdőíves módszerrel mértek előtte és utána. A résztvevők 30%-os tudásszint-növekedésről számoltak be, a válaszok 84%-os egyezést mutattak a tananyag tartalmi elemeivel, az általános vélekedés pozitív volt (átlagos sentiment score: +0,50).[15] Ez a példa jól mutatja, hogy a GenMI-alapú tartalomfejlesztés nemcsak technológiai, hanem pedagógiai szempontból is képes hozzáadott értéket teremteni a képzések során. A tanulmány megerősíti, hogy a generatív mesterséges intelligencia szerepe nem csupán elméletben, hanem a gyakorlatban is releváns és hatékony a kiberbiztonsági tananyagok fejlesztésében.[16]

Fontos azonban hangsúlyozni, hogy a GenMI által készített oktatási tartalmakat minden esetben szakmai validációnak kell alávetni. A mesterséges intelligencia nem válthatja ki teljes mértékben az emberi szereplőket: az oktatási célok és a vállalat belső szabályozási környezetének összehangolása továbbra is az oktatásszervező feladata marad. A GenMI tehát nem autonóm megoldás, hanem egy intelligens támogató eszköz, amely a megfelelő kontroll mellett jelentősen növelheti a képzések hatékonyságát és relevanciáját.

Megvalósítás

A GenMI-chatbotok szimulált támadási szituációkban is bevethetők, például szerepjáték-alapú gyakorlatokon keresztül. Egy ilyen rendszer képes „támadóként" viselkedni: például egy technikai támogatást végző munkatárs szerepében próbálja rávenni a felhasználót arra, hogy bizalmas információkat osszon meg vele, például jelszót. A gyakorlat végén azonban a chatbot „átalakul" oktatóvá, és visszajelzést ad arra vonatkozóan, hogy milyen jelek utalhattak volna a megtévesztő szándékra. Ilyen módon működött a ChatGPT is a New Jersey állami kiberbiztonsági központ belső

[14] Breacher.ai 2025.
[15] Brito et al. 2025.
[16] Brito et al. 2025.

képzési folyamatában, ahol kérdezz-felelek típusú támogatóként segítette a dolgozók tájékozódását.[17]

A képzés részeként a GenMI automatizált módon képes különböző típusú tesztek és vizsgák előállítására. Ezek a felmérések lefedhetik az egyszerű feleletválasztós kérdésektől kezdve a nyílt végű kérdések értékelésén át az interaktív, multimédiás tesztekig terjedő spektrumot. A tanulók egyéni előrehaladásához igazodva a rendszer képes adaptív módon nehezíteni vagy egyszerűsíteni a feladatokat, ezzel is támogatva a hatékony tanulási folyamatot.

A tanulási élmény javítása érdekében a generatív mesterséges intelligencia gamifikációs elemek integrálására is alkalmas. Valós idejű szimulációkkal, pontgyűjtő rendszerekkel vagy versenyszerű kihívásokkal növelhető a tanulói elköteleződés és motiváció. A tanulási folyamat ezáltal nemcsak hatékonyabbá, hanem élményszerűbbé is válik, így hosszabb távon is hozzájárul a megszerzett tudás mélyebb rögzüléséhez.

Értékelés

Az oktatási programok hatékonyságának mérése és értékelése elengedhetetlen a folyamatos fejlesztés érdekében. A GenMI-alapú rendszerek ebben a folyamatban kulcsszerepet játszanak, nem csupán objektív teljesítményértékelést tesznek lehetővé, hanem személyre szabott, azonnali visszacsatolást is biztosítanak a képzésben részt vevő alkalmazottak számára. Ezáltal a tanulók gyorsabban felismerhetik saját hiányosságaikat, és célzottabban fejleszthetik készségeiket.

A GenMI-rendszerek nem csupán értékelnek, hanem pedagógiai támogatást is nyújtanak, a helyes megoldás mellett azonnali, közérthető magyarázatot is képesek adni. Ez különösen fontos a hibák értelmezése és a tanulási folyamat elmélyítése szempontjából. A visszacsatolás tartalma ráadásul összekapcsolható a tanuló egyéni profiljával, például korábbi eredményeivel vagy tanulási preferenciáival, így a képzési anyag még jobban személyre szabható.

Összességében az értékelés GenMI által támogatott módja nem csupán hatékonyabbá, hanem adaptívabbá és még inkább tanulóközpontúvá is teszi a képzési folyamatot. A visszacsatolás azonnalisága és relevanciája lehetőséget teremt arra, hogy a kiberbiztonsági oktatás valóban dinamikusan reagáljon a tanulók fejlődési szükségleteire és a folyamatosan változó fenyegetettségi környezetre. A hatékonyság mérése során az önértékelésen túl objektív metrikák, például a szimulált támadásokra adott reakcióidő, a hibaarány vagy az incidensek számának változása is fontos visszajelzést adhatnak.

Etikai kihívások a generatív mesterséges intelligencia használata során

Fontos azonban hangsúlyozni, hogy az ingyenes verziók hatékonysága erősen függ a felhasználó által megfogalmazott kérdések (promptok) minőségétől. Ahhoz, hogy

[17] New Jersey Cybersecurity & Communications Integration Cell [é. n.].

ezek az eszközök valóban figyelembe vegyék a szervezet specifikus szabályzatait és eljárásrendjeit, a promptoknak pontosan és szakszerűen kell megfogalmazniuk az elvárt kontextust, ami a nem szakmai felhasználók számára kihívást jelenthet.

A fizetős, vállalati verziók, például a ChatGPT Enterprise, lényegesen alkalmasabbak a teljes oktatási életciklus támogatására. Ezek a megoldások lehetővé teszik a vállalatspecifikus tudásbázis integrálását, így az MI relevánsabb és kontextusérzékenyebb válaszokat tud adni. Ugyanakkor a költségek is magasabbak, a ChatGPT vállalati verziója például alkalmazottanként havi 20 dolláros előfizetési díjjal jár. E megoldások azonban nem kizárólag a kiberbiztonsági képzésekben alkalmazhatók, hanem számos más belső tudásmenedzsment-feladatban is értékes támogatást nyújthatnak.

A személyre szabott tanulási utak megvalósításához nemcsak pedagógiai, hanem technológiai eszközökre is szükség van. A Cognitive CyTutor nevű rendszer[18] jól illusztrálja, hogyan támogatható a NIST CPLP tanulási ciklusának személyre szabott komponense egy federált, megerősítéses tanulást alkalmazó MI-platformmal. A tanulói viselkedést és előrehaladást elemző modellek lehetővé teszik, hogy a rendszer automatikusan módosítsa az oktatási stratégiákat, miközben a tanulók adatai helyben maradnak.[19]

Egy jó példája a GenMI NIST CPLP keretrendszer szerinti alkalmazásának a SENSAI (scalable, embedded, natural-language system for AI instruction, skálázható, beágyazott, természetes nyelvű mesterségesintelligencia-alapú oktatórendszer), amelyet egy amerikai egyetemen fejlesztettek ki és alkalmaztak. A rendszer bevezetése több ezer hallgató bevonásával történt, és a visszajelzések alapján jelentősen javult a problémamegoldási hatékonyság és a tanulói elégedettség. A rendszer egyetlen tanársegéd költségéhez mérhető anyagi ráfordítással volt működtethető, miközben lényegesen nagyobb tanulói kört szolgált ki.[20]

Mindezek mellett elengedhetetlen számolni a GenMI-rendszerek inherens kockázataival is. A nagy nyelvi modellek, mint a GPT, központi tanítási adatokon alapulnak, amelyek torzításokat hordozhatnak. Emellett a hallucináció jelensége is fennáll, a modell akkor is generálhat magabiztosnak tűnő válaszokat, ha nem rendelkezik megbízható háttértudással az adott kérdésről. Ez különösen kritikus lehet olyan érzékeny területeken, mint a védelemre vagy biztonsági eljárásokra vonatkozó tanácsadás, ahol a téves információ akár súlyos következményekkel is járhat.

A problémák kezelése érdekében elengedhetetlen a rendszeres emberi jóváhagyás, a GenMI által generált tananyagokat és válaszokat az oktatók részéről folyamatosan ellenőrizni kell. Emellett célszerű a belső szabályzatok integrálása az MI-rendszerek működésébe, hogy a generált tartalom illeszkedjen a szervezet elvárásaihoz. Az irányelvek és a határok világos meghatározásával jelentősen csökkenthető a félrevezető vagy téves válaszok esélye. E kockázat csökkentésére szolgálhatnak a Retrieval-Augmented Generation (visszakereséssel támogatott szövegalkotás, RAG-) rendszerek, amelyek a válaszokat megbízható, külső forrásokkal egészítik ki, növelve ezzel a tartalmi pontosságot.

[18] Yogarajah–Hossain 2025.
[19] Yogarajah–Hossain 2025.
[20] Nelson–Doupé–Shoshitaishvili 2025.

Külön figyelmet érdemel a hitelesség és az aktualitás kérdése is. A GenMI-modellek, még ha technológiailag fejlettek is, nem feltétlenül rendelkeznek a legfrissebb információkkal, például a naprakész CVE-adatbázisok tartalmával. Ezért az ilyen típusú kritikus információk értelmezésében és alkalmazásában az MI nem helyettesítheti az emberi szakértelmet.

Emellett fontos szerepe van a felhasználók felkészítésének is, a mesterséges intelligencia akkor működik igazán hatékonyan, ha a munkavállalók képesek strukturált és célzott kérdéseket megfogalmazni. A prompt engineering, azaz a helyes kérdésfeltevés elsajátítása tehát önálló tanulási céllá válik, nemcsak a kiberbiztonsági oktatás, hanem más vállalati folyamatok szempontjából is hasznos készségként. A hatékony promptolás része a célirányos utasításadás, a kontextus világos meghatározása, valamint a kívánt választípusok előzetes rögzítése, ami különösen fontos a kiberbiztonsági fogalmak torzulásmentes átadásához.

Nem elhanyagolható szempont az adatvédelem sem. A vállalati belső képzések során alkalmazott GenMI-megoldások komoly adatbiztonsági kockázatokat hordozhatnak, különösen, ha azok nyílt, internetes platformokon futnak. A Samsung 2023-as esete intő példa: több mérnök véletlenül szenzitív céges adatokat, köztük félvezetőgyártó eszközök forráskódját töltötte fel a ChatGPT-be, ami súlyos adatvédelmi incidenst eredményezett.[21]

További támadástípusok, mint a *prompt injection* vagy a *data poisoning,* szintén torzíthatják a GenMI-rendszerek válaszait, különösen, ha azok nem megfelelően védett vagy nyílt környezetben működnek. 2023 márciusában az OpenAI szolgáltatásában egy technikai hiba következtében a felhasználók idegen beszélgetések címeit és egyes számlázási adatait is láthatták, ami jól mutatja: az MI-rendszerek nem csupán adatkezelők, hanem potenciális adatforrások is a támadók számára.[22]

Ez különösen problémás egy olyan vállalati oktatási platform vonatkozásában, ahol a rendszer a cég belső tudásbázisából merít (például a NIST által említett eljárásrendek és szabályzatok), vagy esetleg a vállalat maga kormányzati entitás, és minősített adatokkal dolgozik. Amennyiben a GenMI-t szabályozás és felügyelet nélkül használjuk, érzékeny üzleti információk, minősített vagy személyes adatok is kiszivároghatnak a generált tartalmakon keresztül.

Számos vállalat felhőszolgáltatásként veszi igénybe a GenMI segítségével támogatott oktatási rendszereket, ami további adatvédelmi aggályokat vet fel. A harmadik fél által üzemeltetett, felhőben tárolt adatok potenciálisan hozzáférhetők illetéktelen személyek vagy támadók számára, ha a felhőszolgáltató kiberbiztonsága sérül. További problémát jelenthet a nyílt API-ok használata, elképzelhető, hogy a vállalati rendszerek túl sok adatot osztanak meg az MI-szolgáltatóval. Továbbá a felhőalapú MI-szolgáltatók is naplózhatják a felhasználói interakciókat, amelyeknek a kiszivárgása esetén bizalmas adatok tömegesen kerülnek az internetre.[23]

Vállalati környezetben kritikus, hogy a generatív MI használata megfeleljen a GDPR és a hamarosan várható EU AI Act előírásainak. Ez főként azt jelenti, hogy a rendszerbe bevitt érzékeny adatok ne kerüljenek illetéktelen kezekbe, és ne használják fel azokat

[21] Petkauskas 2023.
[22] Petkauskas 2023.
[23] Solving the Security Challenges of Retrieval-Augmented Generation (RAG) 2025.

a szolgáltatók más célra, például a nyelvi modell újratanítására a cég engedélye nélkül. A nagy felhős MI-szolgáltatók reagáltak erre, az OpenAI ChatGPT Enterprise verziója kifejezetten hangsúlyozza, hogy „az ügyfél adata az ügyfélé marad, nem használjuk a beszélgetéseket a modell tanítására", továbbá a szolgáltatás SOC 2 megfelelőséggel rendelkezik, és a kommunikáció titkosított.[24] Hasonlóképpen a Microsoft Security Copilot is úgy lett kialakítva, hogy a vállalati adatok kontrollja az ügyfélnél maradjon, a Microsoft nyilatkozata szerint a Security Copilot által feldolgozott adatok nem kerülnek be az OpenAI alapmodell további tanításába, és a rendszer teljesen zárt, megfelel a Microsoft vállalati biztonsági és megfelelőségi követelményeinek.[25] Ezek fontos szempontok például a pénzügyi vagy az egészségügyi szektorban, ahol tiltott lehet külső felhőbe személyes adatot küldeni.

Összességében a GenMI számos ponton képes támogatni a kiberbiztonsági oktatási folyamatokat, az elemzéstől kezdve a személyre szabott tananyagfejlesztésen át a szimulációk és értékelések automatizálásáig. Ugyanakkor mind a tartalmi hitelesség, mind az adatvédelmi kockázatok szempontjából világossá vált, hogy a generatív rendszerek használata csak megfelelő kontroll és szabályozás mellett lehet biztonságos. Különösen érzékeny környezetben, például a kormányzati, a pénzügyi vagy az egészségügyi szektorban, olyan megoldásokra van szükség, amelyek képesek egyesíteni a GenMI előnyeit a belső tudásbázisok védelmével. A felelős mesterséges intelligencia (Responsible AI) elvei, mint az átláthatóság, méltányosság, elszámoltathatóság, szintén alkalmazhatók a GenMI-rendszerekre, különösen érzékeny környezetekben, mint a pénzügyi vagy a kormányzati szektor.

Összegzés

A tanulmány első részében áttekintettem a GenMI szerepét a kibertudatossági képzések oktatástervezési folyamatában. Bemutattam, hogyan képes a GenMI támogatni az oktatókat az oktatási tartalom létrehozásának különböző fázisaiban, az elemzéstől az értékelésig. A tanulásszervezés klasszikus modelljein túl (például ADDIE) a viselkedésbefolyásoló elméleteket is megvizsgáltam, különös tekintettel a tudatosságnövelési célokat szolgáló keretrendszerekre, mint a NIST CPLP modell.

A tanulmány második részében a GenMI-rendszerek által generált kihívásokra kifejlesztett RAG modell bemutatásán felül, már egy kvantitatív kutatás eredményeit ismertettem, amelynek célja, hogy feltérképezze, miként viszonyulnak a felhasználók a generatív mesterséges intelligencia által létrehozott kiberbiztonsági oktatási tartalmakhoz.

[24] Introducing ChatGPT Enterprise 2023.
[25] Jakkal 2023.

Felhasznált irodalom

AI-Generated Phishing Simulations Are a Game Changer for MSPs (2023). ConnectWise Marketplace, 2023. július 11. Online: https://marketplace.connectwise.com/blogs/ai-generated-phishing-simulations-are-a-game-changer-for-msps/

Breacher.ai (2025): *Deepfake Archives.* Online: https://breacher.ai/solutions/deepfake-simulation/

Brito, Fernando et al. (2025): Enhancing Cybersecurity Education With Artificial Intelligence Content. *In Proceedings of the 56th ACM Technical Symposium on Computer Science Education 1.* New York: Association for Computing Machinery, 158–164. Online: https://doi.org/10.1145/3641554.3701958

CVE [é. n.]: Frequently Asked Questions (FAQs). Online: https://www.cve.org/ResourcesSupport/FAQs

EU Artificial Intelligence Act. Online: https://artificialintelligenceact.eu/ai-act-explorer/

European Union Agency for Cybersecurity (2024): *ENISA Threat Landscape 2024: July 2023 to June 2024.* Online: https://data.europa.eu/doi/10.2824/0710888

Jakkal, Vasu (2023): Introducing Microsoft Security Copilot: Empowering Defenders at the Speed of AI. *Official Microsoft Blog,* 2023. március 28. Online: https://blogs.microsoft.com/blog/2023/03/28/introducing-microsoft-security-copilot-empowering-defenders-at-the-speed-of-ai/

Merritt, Marian et al. (2024): *Building a Cybersecurity and Privacy Learning Program. NIST SP 800-50r1.* Gaithersburg: National Institute of Standards and Technology. Online: https://doi.org/10.6028/NIST.SP.800-50r1

Mouton, Francios et al. (2014): Social Engineering Attack Framework. In *2014 Information Security for South Africa.* 1–9. Online: https://doi.org/10.1109/ISSA.2014.6950510

Nelson, Connor – Doupé, Adam – Shoshitaishvili, Yan (2025). SENSAI: Large Language Models as Applied Cybersecurity Tutors. In *Proceedings of the 56th ACM Technical Symposium on Computer Science Education 1.* New York: Association for Computing Machinery, 833–839. Online: https://doi.org/10.1145/3641554.3701801

New Jersey Cybersecurity & Communications Integration Cell [é. n.]: *ChatGPT and Its Impact on Cybersecurity.* Online: https://www.cyber.nj.gov/guidance-and-best-practices/artificial-intelligence/chatgpt-and-its-impact-on-cybersecurity

Introducing ChatGPT Enterprise. (2023). *OpenAI,* 2023. augusztus 28. Online: https://openai.com/index/introducing-chatgpt-enterprise/

Petkauskas, Vilius (2023): Lessons Learned from ChatGPT's Samsung Leak. *Cybernews,* 2023. május 8. Online: https://cybernews.com/security/chatgpt-samsung-leak-explained-lessons/

Proofpoint (2023): *2023 Security Awareness Study. How Effective Are Your Awareness Programs – and Do Your Employees Agree?* [H. n.]: Information Security Media Group. Online: https://www.proofpoint.com/us/resources/analyst-reports/ismg-security-awareness-training-perception-study

Shaw, R. S. et al. (2009): The Impact of Information Richness on Information Security Awareness Training Effectiveness. *Computers & Education,* 52(1), 92–100. Online: https://doi.org/10.1016/j.compedu.2008.06.011

SlashNext (2023): *State of Phishing.* Online: https://www.prnewswire.com/news-releases/slashnexts-2023-state-of-phishing-report-reveals-a-1-265-increase-in-phishing-emails-since-the-launch-of-chatgpt-in-november-2022--signaling-a-new-era-of-cybercrime-fueled-by-generative-ai-301971557.html

Solving the Security Challenges of Retrieval-Augmented Generation (RAG) (2025). *Polymer,* 2025. január 31. Online: https://www.polymerhq.io/blog/ai/solving-the-security-challenges-of-retrieval-augmented-generation-rag/

Verizon (2024): *2023 Data Breach Investigations Report: Frequency and Cost of Social Engineering Attacks Skyrocket.* Online: https://www.verizon.com/business/resources/reports/2023-data-breach-investigations-report-dbir.pdf

Yogarajah, Jesudhas – Hossain, Gahangir (2025): The Concept of Cognitive CyTutor Utilizing Federated Learning for Cybersecurity Education. In *2025 IEEE 15th Annual Computing and Communication Workshop and Conference (CCWC),* 681–690. Online: https://doi.org/10.1109/CCWC62904.2025.10903809

HADMÉRNÖK
VÉDELEMINFORMATIKA
20. évfolyam (2025) 2. szám 143–160.
DOI: 10.32567/hm.2025.2.9

András Tóth[1]

Enhancing Situational Awareness and Decision-Making: The Impact of Advanced ISR Solutions on Command and Control Systems[2]

Abstract

This document explores the transformative impact of advanced Intelligence, Surveillance and Reconnaissance (ISR) technologies on modern military Command and Control (C2) systems, particularly within NATO and EU contexts. It highlights how cutting-edge advancements like artificial intelligence (AI), machine learning (ML), edge computing and big data analytics enhance situational awareness, decision-making and operational efficiency. The transition from network-centric to data-centric warfare is examined, emphasising real-time data integration, autonomous systems and decentralised decision-making to address the complexities of modern combat. While these technologies offer unprecedented decision superiority and adaptability, challenges such as information overload and cybersecurity vulnerabilities are also discussed. The study underscores the need for continuous innovation and integration of emerging technologies to maintain a strategic advantage in dynamic military environments.

Keywords: situational awareness, Command and Control (C2) systems, Intelligence, Surveillance and Reconnaissance (ISR), data-centric warfare, edge computing, decision superiority

Introduction

Technological development has always played a key role in shaping the capabilities and efficiency of military organisations and alliances. This is no different for the

[1] Associate Professor, Ludovika University of Public Service, e-mail: toth.hir.andras@uni-nke.hu
[2] Project no. TKP2021-NVA-16 has been implemented with the support provided by the Ministry of Innovation and Technology of Hungary from the National Research, Development and Innovation Fund, financed under the TKP2021-NVA funding scheme.

North Atlantic Treaty Organization (NATO) and the European Union (EU), which heavily depend on robust Command and Control (C2) systems to maintain situational awareness and support decision-making. In recent years, rapid technological advancements have brought both new opportunities and challenges for these C2 systems. This document explores how these developments impact the current NATO and EU command and control systems, focusing on their potential to enhance situational awareness and decision-making.

Emerging intelligence, surveillance and reconnaissance (ISR) systems, open-source intelligence (OSINT), artificial intelligence (AI), machine learning, big data and data analytics have the potential to significantly transform military intelligence and analysis processes. As a result, they have a substantial influence on C2 processes, operational awareness, information superiority and decision-making. These advancements can also improve the speed and accuracy of information dissemination, enabling a quicker and more effective response to emerging threats.

Furthermore, integrating these technologies into C2 systems can enhance interoperability between NATO and EU forces, improving the overall coordination and efficiency of joint operations. Overall, the integration of advanced technologies into C2 systems can significantly boost military capabilities and contribute to mission success. By leveraging these developments, military forces can better adapt to evolving threats and achieve strategic objectives with greater efficiency.[3]

This article addresses the following research questions:

- How do advanced intelligence, surveillance and reconnaissance systems affect command and control systems?
- How do emerging and disruptive technologies, such as edge computing, artificial intelligence and machine learning, influence situational awareness and decision-making processes?

Materials and methods

In current military operations, there has been a significant shift from a network-centric approach to a data-centric approach to warfare. In data-centric warfare, the Army utilises advanced capabilities to enhance lethality, survivability and operational tempo. By providing timely access to critical information, leaders and soldiers can assess risks and optimise combat capabilities. Utilising analytical tools allows for effective understanding and response to dynamic situations, while integrated decision-driven capabilities promote informed decision-making and agile military operations.[4]

Achieving and maintaining informational and decision-making superiority has become critical to the effectiveness of modern military operations. This superiority enables the force to make decisions and manoeuvre ahead of its adversaries, increasing the likelihood of mission success while reducing the risks to personnel and assets. This evolution highlights the growing importance of data in ensuring the success of

[3] Tóth 2020.
[4] Rey–Saie 2023.

military operations. In a data-centric context, the efficiency of military operations increasingly depends on the comprehensive collection of relevant information, its effective processing and timely sharing across different levels of command. Advanced data analytics, artificial intelligence and secure communication networks play a crucial role in supporting these processes. These technologies enhance the ability to analyse complex datasets, allowing military leaders to make informed decisions quickly. Moreover, access to accurate and relevant real-time information is not only essential for executing operations but also for dynamically adapting operational procedures to changing battlefield conditions. In recent years, several studies[5] have identified that military operations have transitioned from network-centric warfare to data-centric warfare, rooted in data-driven decision-making processes.[6]

Data-centric warfare is an evolving military strategy that emphasises the critical role of data and information technologies in modern combat operations. This approach leverages advanced data analytics, artificial intelligence and machine learning to enhance decision-making, situational awareness and operational efficiency on the battlefield. As military forces increasingly integrate these technologies, the concept of data-centric warfare has become a significant factor in shaping contemporary military strategies, reflecting a shift from traditional resource-based models toward information dominance and agile responses to emerging threats. The significance of data-centric warfare lies in the rapid processing of massive amounts of data collected from various sources, including sensors and reconnaissance systems. This shift not only increases battlefield efficiency but also presents numerous challenges, such as data quality, human–machine collaboration, and technical issues related to the military applications of artificial intelligence. Integrating advanced technologies allows military personnel to make informed decisions quickly and navigate the complexities of modern warfare, characterised by hybrid threats and multi-domain operations.[7] One of the core principles of data-centric warfare is a proactive approach to information operations, which has become an integral part of contemporary military strategies. Data plays a central role not only in coordinating operations but also in influencing the C2 capabilities of adversaries. This approach emphasises the importance of anticipating military requirements and the capabilities of adversaries, enabling decisive actions during information operations. The principle of "attack" as an information activity embodies an aggressive mindset aimed at achieving information dominance over the adversary. This involves not only protecting one's own information systems but also actively disrupting the adversary's capabilities, including command and control systems and information dissemination networks.

Bobenrieth and Watts emphasise in their article that cyber operations, which are a critical component of data-centric warfare and information operations, encompass a broad spectrum from data theft and system mapping to denial-of-service attacks. These actions do not always constitute an "attack" in the legal sense under the laws of war. Defining the threshold of attack is crucial in data-centric warfare, as many

[5] Skoryk et al. 2021; Mayer 2023; Bronk – Cranny-Evans 2022.
[6] Milano 2023.
[7] Fazekas 2024.

operations focus on disrupting, manipulating, or rendering enemy data and systems unusable without causing physical damage. Fundamentally, this can be described as an "offensive orientation", requiring military forces to respond immediately to threats in the information domain while adapting quickly to emerging challenges. This means military forces must act swiftly against newly identified hostile information platforms and adapt to constantly changing circumstances, neutralising potential advantages held by adversaries. This approach integrates information operations into the broader operational framework, making them a vital component of overall military capability. These emerging operational procedures demand the decentralisation of C2 systems. Instead of traditionally centralised decision-making, smaller, local units are empowered to execute data-driven decisions quickly. The importance of decentralisation is particularly evident in environments where communication systems may be unreliable or vulnerable. By enabling independent data analysis at the local level, even in peripheral areas, military organisations can significantly improve their adaptability and responsiveness, enhancing the quality of operational execution.[8]

Data-centric warfare relies heavily on data analysis, a critical component in enhancing decision-making within the combat environment. A network of strategically placed sensors gathers comprehensive data about environmental conditions, troop movements and enemy positions, creating a detailed picture of the operational environment and supporting decision-making. This data is then processed and analysed to generate actionable insights, enabling data-driven decision-making processes.

The iterative decision-making process is supported by the OODA Loop (Observe, Orient, Decide, Act). This model is designed to improve decision-makers' ability to assess dynamic situations and respond faster and more effectively than the enemy. Rapid execution of the cycle allows for outpacing the enemy in decision-making by creating a "shorter time cycle" than the enemy requires. This forces reactions from the enemy, ensuring proactivity and supporting anticipation. The OODA Loop also provides flexibility, enabling leaders to adapt to changing environments and new information. Overall, effective use of the OODA Loop can disrupt the enemy's decision-making processes, ensuring decision superiority. The components of the OODA Loop in a military context are defined as shown in Table 1.

[8] Bobenrieth–Watts 2024.

Table 1: OODA Loop procedures and tools

Phases	Objectives and procedures	Tools
Observe	This initial phase focuses on a comprehensive assessment of the current situation to gather a broad range of relevant information. In a military context, various intelligence, surveillance and reconnaissance tools are utilised, including unmanned aerial vehicles (drones), satellites and reconnaissance teams, to collect and distribute critical data. Observing enemy movements, such as troop deployments and tactical manoeuvres, is essential for identifying strategies and intentions. Sensors are employed to analyse terrain, weather conditions and other environmental factors that could influence military operations or provide strategic advantages.	Using advanced sensor systems that play a crucial role in detecting potential threats and movements within the area, employing state-of-the-art technology to capture even the smallest changes in the environment. Deploying radar systems for real-time observation of hostile forces' movements, providing situational awareness and supporting strategic planning efforts. Conducting visual observations by personnel, who meticulously monitor and document enemy activities, helping to create detailed records that can serve as the basis for future actions and decisions. Robust Big Data intelligence integrates large amounts of data from different sources, supporting identifying patterns and insights that improve decision-making and increase operational efficiency.

Phases	Objectives and procedures	Tools
Orient	The primary goal is to thoroughly analyse and interpret the gathered information to create a comprehensive overview that serves as a foundation for decision-making. Evaluating the enemy's tactics and intentions: Gather information about the enemy's recent actions and activity patterns. Assess their strengths, weaknesses and possible future intentions or moves to understand their behaviour in the current situation. Assessing our own forces: Examine the current capabilities and limitations of our forces, including personnel, equipment and logistical support. Identify strengths that can be utilised and vulnerabilities that need to be addressed in light of the present circumstances. Comparing the current situation to strategic objectives: Analyse how the current scenario aligns with overarching strategic goals. Determine whether the current operational approach effectively supports achieving these goals or if adjustments are needed. Integrating observed information: Combine new intelligence with knowledge, skills and insights gained from previous military operations. Use this integrated information to gain a more detailed understanding of the battlefield and to inform tactical decision-making.	Using analytical software to review large amounts of data and identify patterns. Employing strategic modelling techniques to simulate different scenarios and predict outcomes based on various courses of action. Seeking expert opinions from military analysts and experienced personnel to gain diverse perspectives on the given situation. Comprehensive Big Data analytics to identify actionable information to support informed decision-making and significantly improve the operational efficiency of all operations.

Phases	Objectives and procedures	Tools
Decide	The primary goal is to develop a detailed and feasible plan to effectively manage military operations. Making quick, well-founded decisions: It is essential to analyse battlefield situations rapidly while ensuring that the assessment is based on reliable and relevant intelligence data. This allows commanders to respond effectively to dynamic situations without unnecessary delays. Choosing the most advantageous option: Commanders must evaluate multiple courses of action available during operations. This involves considering enemy movements, strengths, weaknesses, immediate tactical decisions and overarching strategic objectives that align with the mission requirements. Prioritising actions that effectively counter enemy manoeuvres is critical, while optimising the use of available resources. The element of time also plays a key role, as timely decisions can capitalise on opportunities before the enemy can react. Effective communication: After a decision is made, it is vital to immediately and clearly convey the chosen course of action to all involved teams and units. This ensures that everyone understands their role and responsibilities, aligning efforts towards the shared objective.	The use of battle management systems that integrate real-time data from various sources and provide commanders with a comprehensive overview of the battlefield to support decision-making. The application of decision-support systems, where analytical tools assist in evaluating different tactical options and predicting outcomes based on current and projected scenarios, thereby improving the decision-making process. The implementation of reliable command and control communication channels. These trusted communication networks enable the swift dissemination of orders and information among military units while maintaining confidentiality and integrity, facilitating coordination and the execution of planned strategies.

Phases	Objectives and procedures	Tools
Act	The primary goal is the efficient execution of decisions made. Carrying out offensive or defensive operations: Executing military activities planned according to objectives, aimed at either attacking the enemy (offensive) or protecting our forces and assets (defensive). Rapid mobilisation and coordination of troops: Quickly assembling and organising military units to ensure they are ready for deployment. This includes deploying forces to designated locations and establishing clear communication and command structures to enhance operational efficiency. Continuous monitoring of operational outcomes: Regularly evaluating the results of operations to determine their effectiveness. This ongoing assessment allows for timely adjustments and the initiation of a new OODA cycle, thereby refining tactics and procedures based on real-time feedback.	The use of weapon systems, including a wide range of arms from small firearms and artillery to advanced missile systems, which are designed to meet specific operational requirements. The implementation of reliable and secure communication networks, which are crucial for maintaining contact between units and for transmitting critical information and commands. These systems also play a key role in sending reports that are important for the further planning processes. The availability of effective logistical support, which is essential for providing the necessary supplies, equipment and maintenance support to ensure that the forces are properly equipped and sustained during their missions.

Source: Brehmer 2005

By integrating data-driven elements into the phases of the OODA Loop, military commanders can navigate complex scenarios more effectively and enhance their overall operational responsiveness. Incorporating data-driven solutions into the OODA Loop can significantly improve the process's efficiency and accuracy. The use of data-driven technologies in each step allows for more objective decision-making, faster analyses and real-time responses. Figure 1 illustrates the data-driven OODA Loop processes.

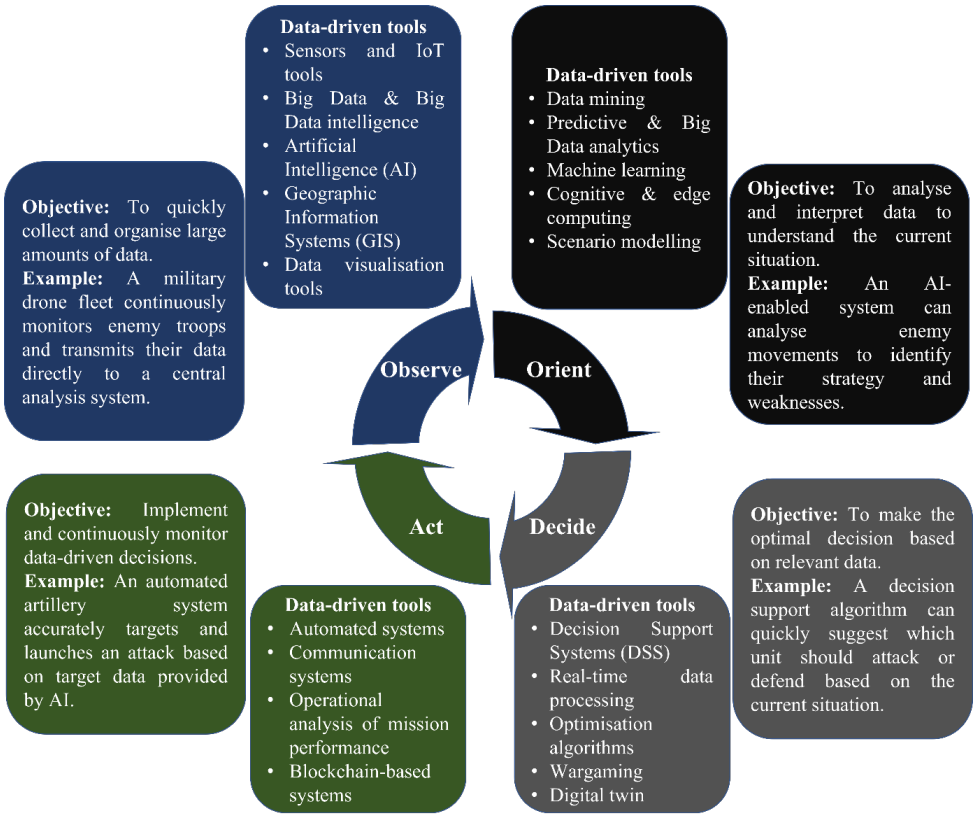


Figure 1: Data-driven OODA Loop processes
Source: compiled by the author

During the observe process, the sensors and IoT devices used include a variety of advanced technologies such as drones, satellites, radar systems, thermal cameras and other sensors, all designed for real-time data collection. These tools are crucial for accurate and timely information gathering across various fields, from environmental monitoring to tracking enemy activities. Big data technologies play an essential role in managing and organising the vast amounts of data generated by these sensors. Sophisticated intelligence systems are employed, using automated data collection and analysis methods that allow organisations to derive meaningful insights from large datasets. Artificial Intelligence enhances this process through automatic pattern recognition capabilities. By analysing data patterns, AI effectively identifies anomalies or deviations, such as unusual movements or behaviours, which can provide insights into enemy operational plans or potential next steps. For instance, computer vision technologies allow AI to interpret and understand visual data. At the same time, neural network-based object recognition algorithms are critical in the evaluation phase.

Together, these technologies enable the precise identification and tracking of objects in complex environments, bolstering situational awareness and decision-making processes in military operations. Geographic Information Systems (GIS) are indispensable for processing and analysing spatial data, enabling the creation of detailed maps and visualising connections based on the collected data in military contexts. This supports the development of a common operational picture. These efforts are complemented by data visualisation tools, which transform complex datasets into easily understandable formats. Using graphs, charts and interactive dashboards, these tools help stakeholders make sense of complicated information, facilitating informed decision-making and strategic planning.

In the orient phase, data mining refers to the process of extracting valuable and relevant information from vast databases. This technique allows military organisations to uncover patterns and trends that can provide the necessary information for decision-making. Predictive and Big Data analytics are essential for forecasting adversary intentions and actions. These techniques enable military leaders to identify patterns and make informed predictions by analysing extensive datasets. By analysing past experiences, available relevant data, statistical algorithms and machine learning techniques, analysts can develop models that predict potential threats and hostile military movements. Machine learning techniques analyse historical data to draw lessons and conclusions from previous combat situations. By recognising patterns and outcomes, military forces can adjust their procedures and tactics based on strategies and techniques that proved successful in the past, ultimately improving decision-making during operations. Cognitive computing and edge computing utilise advanced AI-based systems to analyse data at the perimeter of the network. This enables real-time detection and interpretation of complex situations, even in remote or challenging environments. Such capabilities are vital for understanding operational contexts that may not be immediately obvious. The concepts generated by these technologies can be analysed through scenario modelling, which involves simulating various potential situations to determine the most effective course of action. By evaluating situations with different outcomes based on various variables, military planners can prepare for multiple possibilities and make informed decisions.

Decision support systems (DSS) play a crucial role in modern military operations because they integrate advanced artificial intelligence and analytical tools to help identify optimal strategies. These systems are designed to process large amounts of data in real time, allowing military leaders to quickly assess critical information and make well-informed decisions in time-sensitive situations. By using optimisation algorithms, DSS enables a systematic evaluation of different courses of action, taking into account factors like resource allocation, logistical constraints and the timing of various operational manoeuvres. This analytical capability ensures that military planners can develop plans that maximise efficiency while making the best use of available resources. Wargaming also supports this process, serving as a strategic approach that involves simulating military scenarios to analyse and predict possible operational and tactical responses from adversaries. Through wargaming exercises, military organisations can better understand the dynamics of a conflict and refine their strategies based on anticipated enemy actions. The concept of the digital twin

is another innovative tool in military decision-making. A digital twin is a virtual replica of real-world situations, allowing decision-makers to simulate various scenarios and test different military options in a risk-free environment. This virtual simulation enables commanders to explore the consequences of different decisions, enhancing their ability to adapt to changing circumstances on the battlefield and improving overall operational effectiveness.

In the act phase, automated systems utilise advanced technologies such as robotics, autonomous vehicles and drones, which can process information and make decisions at speeds surpassing human capabilities. These systems are designed to operate efficiently in dynamic environments, providing significant tactical advantages. Communication systems play a crucial role in these military operations, as they enable real-time coordination and facilitate command and control interactions between command centres and frontline troops. This ensures a seamless flow of information, keeping teams accurately informed about changing conditions and instructions. The operational analysis of mission performance focuses on continuously monitoring the effectiveness of various measures implemented during the mission. This real-time assessment allows military leaders to evaluate which strategies are working and quickly adjust plans if necessary, enhancing the overall success of the operation. In addition, blockchain-based systems offer robust solutions to ensure the authenticity and security of operations and commands. By using decentralised technology and encryption, these systems protect data integrity and prevent unauthorised access, which is essential for maintaining operational secrecy and the trust of military personnel.

Results

Improving situational awareness (SA) and decision-making is crucial in various dynamic environments, particularly in military operations and the management of complex systems. SA refers to the perception, understanding and projection of elements within the environment, forming the foundation of effective decision-making processes. By integrating advanced ISR solutions, organisations are better equipped to obtain a comprehensive understanding of their operational environment. This is vital for C2 systems in high-stakes operations. The integration of technologies such as edge computing, artificial intelligence (machine learning), unmanned aerial vehicles (UAVs) and real-time data sharing through tactical data links significantly enhances the tactical-level situational awareness of military personnel on the battlefield. Tools like rugged mobile devices, tablets and augmented reality (AR) glasses help soldiers in the field process this information more effectively. Advanced helmet displays provide vehicle operators and pilots with critical tactical data, further improving their operational efficiency. Tactical data links, including radios and satellite communications (SATCOM), are essential for maintaining situational awareness. These systems distribute audio, video and sensor data, ensuring that teams have access to relevant information regardless of their circumstances.[9] As military operations evolve,

[9] Lombardo 2024.

the integration of advanced ISR solutions continues to enhance SA by delivering a comprehensive situational picture. This supports command and control decisions with reliable and verified information, often cross-validated from multiple sources, ensuring that decision-makers are equipped with all the critical data they need.[10]

These developments allow commanders to receive timely information and make well-informed decisions, which can significantly contribute to the successful execution of missions. With the continuous advancement of technology, the ongoing research and development of SA methods remain essential, especially as organisations strive to stay ahead of emerging challenges in both military and civilian contexts. The challenges related to data integration and the risk of information overload particularly highlight the complexity of enhancing situational awareness. Addressing these issues is crucial to ensuring that operators can effectively utilise advanced ISR technologies to make sound decisions in increasingly interconnected and dynamic environments.[11] The impact of advanced ISR systems on C2 operations in military activities is one of the central themes of this study, significantly influencing modern warfare. Advanced ISR technologies have revolutionised how military organisations collect and process information, enabling superior situational awareness and more informed decision-making in dynamic settings. This transformation is noteworthy as it enhances operational efficiency and decision-making superiority, providing commanders with comprehensive insights that greatly influence tactical outcomes on the battlefield.

A July 2024 analysis revealed that recent conflicts have underscored the need for C2 systems to adapt to the complex challenges of modern warfare, such as asymmetric threats and cyber operations. Russia's operations against Ukraine highlighted the importance of adaptability in hybrid warfare. Drones, satellite imagery and artificial intelligence play key roles in improving situational awareness and facilitating rapid decision-making. These technologies are fundamental for effectively adapting to various operational scenarios. Future C2 systems will rely on technological advancements such as data analytics, artificial intelligence and cloud computing. The rise of hybrid warfare demands abandoning traditional hierarchies and adopting more flexible, decentralised models and data-driven operations. The rapid data analysis capabilities of artificial intelligence, real-time multi-domain operations and coalition interoperability are becoming critical priorities.[12]

One of the deepest impacts of advanced ISR on C2 is achieving decision superiority. This concept refers to the military's ability to maintain better situational awareness and make faster, more informed decisions than their adversaries. By leveraging advanced ISR technologies, commanders can gain comprehensive insights into enemy movements, assess the efficiency of friendly forces and identify emerging threats in real time. This provides a critical advantage, allowing forces to manoeuvre better than the enemy on the battlefield. Further research has shown that autonomous systems are set to play a key role in military decision-making processes, fundamentally transforming these processes and enabling faster and more effective decision-making, thus

[10] Tóth–Farkas 2023.
[11] Green et al. 2023.
[12] Total Military Insight 2024.

ensuring the potential for achieving decision superiority. These systems integrate modular applications of artificial intelligence, data analysis and precision weapon technologies, reshaping the global balance of power and the functioning of C2 systems. By accelerating the OODA Loop, autonomous systems enable more efficient operations, particularly at the tactical level, where self-improvement and adaptation are also realised. The three levels of autonomous weapon systems – human-controlled, human-supervised and fully autonomous – require decreasing amounts of human intervention, creating information dominance. The authors point out that AI facilitates forecasting and provides unexpected suggestions, as it can process vast amounts of data. With these capabilities, autonomous systems enhance the speed, efficiency and complexity of warfare while demanding new approaches to cooperation between commanders and AI solutions.[13]

Regarding the impact of enhanced situational awareness and better decision-making processes on C2 systems, the conclusion can be summarised as follows: the integration of advanced ISR systems has transformed traditional C2 paradigms, enabling unprecedented levels of situational awareness and decision-making accuracy. Real-time data collection and analysis provide commanders with a comprehensive view of the operational environment, allowing them to anticipate enemy actions and make well-informed decisions with greater efficiency. This enhanced capability facilitates decision superiority, granting a strategic advantage on the battlefield. However, the massive influx of data also presents challenges, such as the risk of information overload and potential decision paralysis. To mitigate these issues, artificial intelligence and machine learning have become indispensable, streamlining data processing and enabling actionable insights at unparalleled speed. This evolution is also reshaping C2 systems by integrating data-driven operations that emphasise collaboration, interoperability and rapid adaptability.[14] Moreover, it has become evident that analysing the information collected by advanced ISR systems as early as possible is essential. Edge computing offers an excellent solution for this, enabling decentralised data processing at or near its source instead of relying solely on centralised systems. This technology is particularly critical in military operations, where rapid data processing and real-time decision-making are fundamental to success. Edge computing minimises latency, allowing military personnel to respond effectively, even in environments with weak or intermittent connectivity. As a result, frontline platforms can independently analyse and process data, significantly improving information flow and the speed of decision-making. Local data processing is especially advantageous in time-sensitive situations, eliminating delays caused by central command communication. Additionally, edge computing enhances operational resilience by reducing dependency on centralised data centres, which is vital in combat scenarios. By decentralising data processing, military units can manage sensitive information more securely, as it remains within the tactical environment. This approach not only strengthens security but also ensures that critical information for decision-making is always available in a timely manner. In conclusion, edge computing significantly contributes to the

[13] Simonetti–Tripodi 2020.
[14] Tóth 2021.

speed, efficiency and resilience of military operations. This technology plays a vital role in modern military contexts, where rapid reactions and real-time data provide a decisive advantage.

Conclusions

This document investigates the transformative impact of advanced ISR systems, alongside emerging technologies such as edge computing, artificial intelligence and machine learning, on modern military C2 systems. The analysis provides insights into two critical areas:

1. Effects of Advanced ISR on C2 Systems: Advanced ISR systems, including drones, satellites and real-time data analytics, significantly enhance situational awareness by offering comprehensive and timely insights into the operational environment. This capability empowers military leaders with decision superiority, enabling them to anticipate threats, make informed choices rapidly and maintain a strategic advantage. The integration of ISR with C2 systems has revolutionised traditional paradigms, fostering improved interoperability, operational efficiency and mission effectiveness. However, challenges such as information overload necessitate the adoption of AI and ML to streamline data processing and ensure actionable insights.
   For example, ISR drones and satellites can utilise advanced AI to identify enemy artillery positions by analysing heat signatures, muzzle flashes and gunfire acoustics. They predict firing patterns based on terrain and past actions, quickly transmitting coordinates to command posts for precise counter-battery strikes. This system directs munitions such as artillery, missiles and kamikaze drones while continuously monitoring enemy movements to ensure effective suppression and strategic advantage.
2. Influence of Emerging and Disruptive Technologies on Situational Awareness and Decision-Making: Technologies like AI, ML and edge computing are reshaping situational awareness and decision-making processes. AI and ML enable predictive and Big Data analytics, pattern recognition and rapid processing of vast datasets, enhancing decision-making speed and accuracy. Edge computing decentralises data analysis, allowing real-time decision-making at the tactical level, even in environments with limited connectivity. This decentralisation strengthens operational resilience and security while reducing latency, thereby ensuring that commanders and field units can act swiftly in dynamic combat scenarios.
   For example, the disputed area's forward operating base (FOB) requires strong surveillance to detect and neutralise threats before they reach the perimeter. Traditional surveillance methods, such as handheld surveillance cameras or UAV imagery, can cause serious problems with operator fatigue, delayed response times and centralised data processing that can be disrupted in contested environments. AI surveillance cameras and UAVs use ML models trained to identify enemy movements, unusual activities or potential threats. Pattern

recognition algorithms detect anomalous behaviour, such as when a person moves inappropriately near the perimeter or in a way that indicates a reconnaissance attempt. Instead of transmitting the raw video feed to a centralised command centre, edge computers (e.g. robust mini servers located at the FOB) process the data locally. Instant classification of potential threats provides real-time alerts, reduces latency and enables immediate response. AI-enabled automated response systems can trigger alerts and deploy countermeasures (e.g. automated turrets or drones).

Table 2 illustrates the effects found in the studies. The table shows the impact of each of the disruptive technologies on the areas under study.

Table 2: Impact of disruptive technologies on command and control systems, situational awareness and decision-making

Area of impact	**Impact on command and control systems**	**Influence on situational awareness and decision-making**
Advanced ISR Systems	Enhances common operational picture by providing real-time data and insights; improves interoperability and operational efficiency; challenges include information overload. Provides a unified operational picture through real-time data integration; enables enhanced coordination across multi-domain operations.	Improves decision superiority through real-time, comprehensive insights; supports proactive responses to threats. Supports the integration of augmented reality tools, improves real-time battlefield visualisation and enhances collaborative decision-making among units.

Area of impact	Impact on command and control systems	Influence on situational awareness and decision-making
Artificial Intelligence (AI) and Machine Learning (ML)	Enables predictive and Big Data analytics, rapid data processing, and pattern recognition; supports informed and real-time decision-making; mitigates risks of data overload and decision paralysis. Facilitates adaptive command structures by leveraging AI for scenario simulations and decision recommendations; supports enhanced human–machine collaboration in complex operations.	Accelerates decision-making processes by analysing complex datasets; supports forecasting and scenario modelling. Supports the integration of augmented reality tools, improves real-time battlefield visualisation and enhances collaborative decision-making among units. Facilitates autonomous decision-making systems, reducing the cognitive load on operators; enables real-time adaptation to emerging threats and enhanced multi-domain coordination. Enhances predictive situational analysis through machine learning models trained on historical data; supports the development of intelligent warning systems to prevent threats.
Edge Computing	Decentralises data analysis, allowing real-time decision-making even in low connectivity environments; enhances operational resilience and reduces latency. Strengthens tactical decision autonomy by decentralising critical data analysis; improves system resilience against cyber and connectivity disruptions.	Facilitates rapid and secure information flow; strengthens decision-making speed and efficiency in dynamic environments. Supports the integration of augmented reality tools, improves real-time battlefield visualisation and enhances collaborative decision-making among units. Allows for decentralised data sharing between units, enhancing local decision autonomy; provides redundancy and resilience in environments with disrupted central communication. Improves battlefield agility by processing environmental data in real-time; enables integration with wearable technologies for on-the-ground personnel, ensuring continuous situational updates.

Source: compiled by the author

Future research initiatives will concentrate on a thorough investigation of the limitations and challenges encountered in implementing advanced Intelligence, Surveillance and

Reconnaissance (ISR) systems alongside cutting-edge technologies such as Artificial Intelligence (AI), Machine Learning (ML) and edge computing. This comprehensive research will involve detailed quantitative analyses designed to assess measurable improvements in critical performance metrics, including response times, accuracy rates and overall operational efficacy, in real-world and simulated scenarios. Moreover, the research will aim to identify specific technological advancements, such as enhanced sensor capabilities, data processing speeds and decision-making algorithms, as well as operational enhancements related to teamwork and information sharing among various military units. By translating these technological and operational insights into actionable strategies, this work will provide valuable guidance on best practices, ultimately contributing to creating more resilient and effective command and control systems tailored for modern military operations.

References

Bobenrieth, Emily – Watts, Sean (2024): US Military Legal Doctrine and the Emerging Wartime Cyber Environment. *International Review of the Red Cross,* 107(928), 311–334. Online: https://doi.org/10.1017/S181638312400047X

Brehmer, Berndt (2005): *The Dynamic OODA Loop: Amalgamating Boyd's OODA Loop and the Cybernetic Approach to Command and Control. Assessment, Tools and Metrics.* Online: http://www.dodccrp.org/events/10th_ICCRTS/CD/papers/365.pdf

Bronk, Justin – Cranny-Evans, Samuel (2022): Building the Capacity to Conduct Joint All-Domain Operations (JADO). *RUSI,* 23 November 2022. Online: https://www.rusi.org/explore-our-research/publications/occasional-papers/building-capacity-conduct-joint-all-domain-operations-jado

Fazekas, Ferenc (2024): Military Command in Multi-Domain Environment. *Land Forces Academy Review,* 29(3), 312–321. Online: https://doi.org/10.2478/raft-2024-0034

Green, Elizabeth A. – Armstrong, Miriam E. – Mantua, Janna (2023): Scientific Measurement of Situation Awareness in Operational Testing. *The ITEA Journal of Test and Evaluation,* 44(3). Online: https://doi.org/10.61278/itea.44.3.1002

Lombardo, Ryan M. (2024): *Space Command and Control in a Contested Environment: Is USSPACECOM Getting It Right?* Online: https://www.spacecom.mil/Portals/57/Lombardo%20GCPME%202024%20Space%20C2%20in%20a%20Contested%20Environment.pdf

Mayer, Michael (2023): *Multi-Domain Operations, Emerging Military.* Online: https://publications.sto.nato.int/publications/STO%20Meeting%20Proceedings/STO-MP-SAS-OCS-ORA-2023/MP-SAS-OCS-ORA-2023-08.pdf

Milano, Russ (2023): DIL-Tailored Data Fabrics: Empowering Data-Driven Decision-Making and Achieving Network Resiliency in the Defense and Commercial Sectors. *Code Mettle,* 27 July 2023. Online: https://codemettle.com/wp-content/uploads/2023/08/CM_DataFabricWhitePaper_27JULY2023.pdf

Rey, Jeth – Saie, Cade (2023): Data Dominance: Meeting the Demands of the Digital Battlefield. *AUSA,* 23 February 2023. Online: https://www.ausa.org/articles/data-dominance-meeting-demands-digital-battlefield

Simonetti, Rosario M. – Tripodi, Paolo (2020): Automation and the Future of Command and Control: The End of Auftragstaktik? *Journal of Advanced Military Studies,* 11(1), 127–146. Online: https://doi.org/10.21140/mcuj.2020110106

Skoryk, Anatolii – Nizienko, Boris – Dudush, Anatolii – Shulezhko, Vasil – Romanchenko, Irina (2021): Evolution from the Network-Centric Warfare Concept to the Data-Centric Operation Theory. *Advances in Military Technology,* 16(2), 219–234. Online: https://doi.org/10.3849/aimt.01430

Total Military Insight (2024): *Understanding Command and Control Doctrine: Key Principles Explained.*

Tóth, András (2020): Information-Sharing Challenges and Issues in Multinational Operations, Part 1. *Land Forces Academy Review,* 25(4), 307–316. Online: https://doi.org/10.2478/raft-2020-0037

Tóth, András (2021): Information-Sharing Challenges and Issues in Multinational Operations, Part 2. *Land Forces Academy Review,* 26(1), 22–30. Online: https://doi.org/10.2478/raft-2021-0004

Tóth, András – Farkas, Tibor (2023): Opportunities and Directions for the Evolution of Command and Control Systems in the Context of Multi-domain Operations. *Vojenské Reflexie,* 18(3), 59–73. Online: https://doi.org/10.52651/vr.a.2023.3.59-73

HADMÉRNÖK
FÓRUM

20. évfolyam (2025) 2. szám 161–187.
DOI: 10.32567/hm.2025.2.10

Antal Tímea,[1] Számadó Róza[2]

A hazai és a nemzetközi szakirodalomban használatos *compliance* fogalmának vizsgálata bibliometriai elemzéssel

Kísérlet az újradefiniálására

Examination of the Concept of Compliance Used in Domestic and International Literature through Bibliometric Analysis

An Attempt at Redefinition

Absztrakt

Munkája során a kortárs biztonsági szakértő egyre gyakrabban találkozik a compliance és compliance management szakkifejezésekkel, viszont e fogalmak magyar nyelvű tisztázása olyannyira nem történt még meg egyértelműen, hogy számos definíció létezik a szakirodalomban. Jelen tanulmánynak kettős célja van, egyrészt az, hogy a használatban lévő angol nyelvű kifejezéseket vizsgálja a biztonság fogalmával együtt, majd bibliometriai eszközök (a Web of Science és a Magyar Tudományos Művek Tára nevű adatbázisok) alkalmazásával kísérletet tegyen a compliance újradefiniálására, végül az új fogalommagyarázatot összehasonlítsa a korábbi definíciókkal. Másrészt e kutatás rá kíván világítani arra, hogy az OpenAlex adatbázisban mely tudományterületek keretében született a legtöbb szakmai elemzés a compliance témájában. A végcél egy átfogó definíció létrehozása. Egy újfajta

[1] Doktori hallgató, Óbudai Egyetem Biztonságtudományi Doktori Iskola, e-mail: antal.timea@uni-obuda.hu
[2] Egyetemi adjunktus, Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, e-mail: szamado.roza@bgk.uni-obuda.hu

fogalommagyarázat alkalmazása lehetőséget adhat a compliance gyakorlati alkalmazásának továbbfejlesztésére is, illetve a segítségével kutatandó terület kiszélesítésére.

Kulcsszavak: compliance, compliance management, biztonság, definiálási kísérlet bibliometriai eszközökkel

Abstract

Nowadays, the technical terms compliance and compliance management are heard more and more, and there are many definitions in the literature. The aim of this study is twofold. On the one hand, it is dedicated to examining these terms together with the term security, and using bibliometric tools (Web of Science and the Magyar Tudományos Művek Tára databases) to try to redefine compliance and compare it with the theoretical definition. On the other hand, it also examines which scientific fields have published the most on the topic of compliance in the OpenAlex database. Based on the definition, it may be possible to further develop the practical application of compliance and to define the area to be further researched.

Keywords: compliance, compliance management, security, definition experiment by bibliometric tools

Elméleti definíció

A *compliance* rövid meghatározása: a megfelelőség biztosítása. Az 1. táblázat bemutatja a *compliance*-re vonatkozó szabályozási megközelítéseket, párhuzamba állítva a megfelelés típusát a megfelelőség tartalmi tényezőivel.

1. táblázat: Compliance definíciók

Szerző	**A compliance definíciója**	**Tartalmi tényezők**
Georg Gösswein	A joggal összhangban működés követelménye.[3]	Jogszabályi előírásoknak való megfelelés.
Balogh Mónika	„A vonatkozó összes (jogi és egyéb) szabálynak, elvárásnak való megfelelést, azok szerinti működést jelenti."[4]	Jogszabályoknak, egyéb szabályoknak, elvárásoknak való megfelelés.

[3] Gösswein 2018.
[4] Balogh 2015: 15.

Szerző	A compliance definíciója	Tartalmi tényezők
Dennis Bock	„A compliance legáltalánosabb értelemben – szervezeti megközelítésből – a jogkövető magatartás tanúsítását, a jogszabályi előírásoknak, belső szabályoknak, illetve egyéb követendő ajánlásoknak megfelelő magatartás elérését szolgáló intézkedések gyűjtőfogalma."[5]	Jogszabályoknak, belső szabályoknak, ajánlásoknak való megfelelés.
Thomas Rotsch	„A compliance [...] a vállalkozások hatályos jognak megfelelő működését jelenti, amely azokra a területekre jellemző, ahol a komplex és bonyolult szabályozás miatt a jogkövető magatartás tanúsításához szükséges a »szakértők« általi megelőző intézkedések alkalmazása."[6]	Jogszabályoknak való megfelelés.
Ambrus István, Mezei Kitti, Molnár Erzsébet	„[...] a compliance egyfajta szervezeten belüli normakonformitás, legyen szó akár jogi, akár szervezeti etikai szabályrendszerről."[7]	Jogszabályoknak, belső szabályoknak etikai normáknak, nemzetközi standardoknak, szabványoknak való megfelelés.

Forrás: a szerzők szerkesztése

Az 1. táblázat alapján megállapítható, hogy az elméleti definíciókban a *compliance* tartalmilag egyrészt megfelelést jelent a jogszabályoknak, másrészt megfelelést a jogszabálynak nem minősülő egyéb külső előírásoknak, belső szabályzatoknak, íratlan (etikai) szabályoknak, *soft law*-nak, piaci szokványoknak, nemzetközi standardoknak, szabványoknak. Étienne szerint bár a megfeleléskutatások terén kevés olyan összefoglaló tanulmány született, amely a meglévő empirikus eredményeket összegezné, a terület rendkívül aktív elméleti termékenységet mutat.[8]

A biztonság és a megfelelőség relációja

A vállalatok átlagosan az árbevételük 5%-át veszítik el különböző visszaélések miatt, ezzel összesen több mint 3,6 milliárd dollár a veszteség, átlagosan 8300 dollár kár keletkezik havonta, míg 1 év telik el átlagosan egy visszaélés felderítéséig.[9] A *compliance* kontrollok ezért jelentősen elterjedtek az elmúlt években. A jelentés szerint a következő

[5] Bock 2009: 293.
[6] Rotsch 2012: 47.
[7] Ambrus et al. 2021: 22.
[8] Étienne 2010.
[9] Association of Certified Fraud Examiners 2022.

öt csalás elleni kontroll alkalmazási aránya átlagosan körülbelül 13%-kal nőtt 2010–2022 közötti időszakban hotline 70%, munkavállalói visszaélés-megelőzési oktatások 61%, visszaélés-megelőzési szabályzat 60%, menedzser, vezetők visszaélés-megelőzési képzése 59%, kockázatértékelések 46%. A *compliance* mint biztonsági tényező jelenik meg a gyakorlatban. Mustapha hangsúlyozza, hogy az üzleti szervezetek számára rendkívül költséges, egyik kritikus szempont a különböző szabályozási forrásokból származó megfelelési követelményeknek való megfelelés, és a büntetések elkerülése érdekében különböző technikákat alkalmaznak ennek a feladatnak a megoldására.[10]

Módszertan és vizsgálat a gyakorlatban

Az elméleti *compliance* definíciók alapján a cél annak vizsgálata, hogy a *compliance* és a biztonság kifejezés hogyan jelenik meg a Web of Science és a Magyar Tudományos Művek Tára (a továbbiakban: MTMT) adatbázisokban. A módszertan meghatározásakor segítséget jelentett Nagy Andrea és szerzőtársai munkája, akik az Ipar 4.0 fogalmának bibliometriai áttekintéséhez hasonló módszertant használtak.[11]

A hipotézis az volt, hogy a mesterséges intelligencia elterjedésétől, legfőképpen a ChatGPT nevű nagy nyelvi modellel dolgozó keresőprogram megjelenésétől kezdve egyre több publikáció készült *compliance* és *compliance management* témában, ami megfigyelhető mind a magyar, mind a nemzetközi tudományos publikációk tárolásával foglalkozó weboldalakon.

Cél tehát, hogy releváns áttekintés készüljön a szakirodalomnak a *compliance*-re, a biztonságra és a *compliance management*re vonatkozó részeiről, továbbá ezek egymással való kapcsolatáról. A vizsgálandó publikációk esetében a fókusz arra helyeződött, hogy azokban mely szakkifejezések kerültek előtérbe a legutóbbi évek folyamán, és mely szakterületek publikálták a legtöbb fogalomtisztázással kapcsolatos kutatást. Fontos figyelemmel lenni továbbá arra, hogy milyen új irányú trendek érzékelhetők az egyes szakmai körökben.

A vizsgálat kvantitatív és kvalitatív elemeket egyaránt tartalmaz. A kvantitatív elemek használatát a kulcsszógyakoriságon alapuló módszer, míg a kvalitatív részeket az egyes elemzési pontokon az adatok megtisztításának manuális gyakorlata tette szükségessé, utóbbi esetében tehát a kvantitatív szelektálási metódusokat nem lehetett alkalmazni.

A jelen tanulmány definíciós kísérletéhez két mintát választottunk ki, a 2. táblázatban a legfontosabb ismérvek találhatók a kutatás ezen részével kapcsolatban.

2. táblázat: Az újradefiniálás módszertana

Forrásszöveg	A vizsgálat helye	A vizsgálat tárgya
Nemzetközi publikáció a Web of Science alapján	Címek és szöveg	A forrás kulcsszavainak halmaza
Hazai publikációk az MTMT alapján	Címek és szöveg	Compliance és security kulcsszavak

Forrás: a szerzők szerkesztése

[10] Mustapha 2020.
[11] Nagy–Tasner–Kovács 2021.

Az említetteken túl az OpenAlex adatbázisban arra kerestük a választ, hogy mely tudományterületek keretében született a legtöbb szakirodalmi elemzés *compliance* témában. Leginkább olyan tárgykörök vizsgálata történt meg, amelyek a *compliance*-szel foglalkoznak, és a modellezés célja annak bemutatása, hogy milyen jellegű összeköttetésben állnak az egyes tudományterületek egymással e témán belül.

Nemzetközi publikációk

A hipotézis az, hogy a tudományos publikációk száma folyamatosan emelkedik. Ennek bizonyítására különböző bibliometriai elemzések alkalmazása történt. Ahhoz, hogy bizonyítást nyerjen a feltételezés, éves bontásban kell vizsgálni a tudományos adatbázisok e témában megjelent adatait. A nemzetközi publikációk áttekintésére a Web of Science nevű weboldal (a továbbiakban: WoS) keresőmotorja segített.

A tudományterületek széles köréből származó tudományos cikkeket a WoS rendszerezi és őrzi; publikációk milliói, köztük könyvfejezetek, konferencia-előadások és folyóiratcikkek érhetők el a segítségével. A kutatók ezt az eszközt használhatják az idézések nyomon követésére, egyes konkrét dolgozatok keresésére és a kutatási trendek vizsgálatára is. A WoS az idézett publikációk összekapcsolásával egy információs hálózatot épít ki. A felhasználók a WoS által kínált keresőmotor segítségével számos paraméter – például a szerző neve, a cím, a kulcsszavak, a folyóirat neve és a megjelenés dátuma – segítségével kereshetnek cikkeket. Annak érdekében, hogy a felhasználók még jobban finomíthassák a keresési eredményeket, a keresőmotor olyan lehetőségeket is kínál, mint a mezőkeresés és az idézetkeresés. Ez a funkció segít szemléletes hálózati térképek alkotásában is egy-egy tudományterület publikációinak a kereszthivatkozásai, azonos kifejezései és szerzői tekintetében.

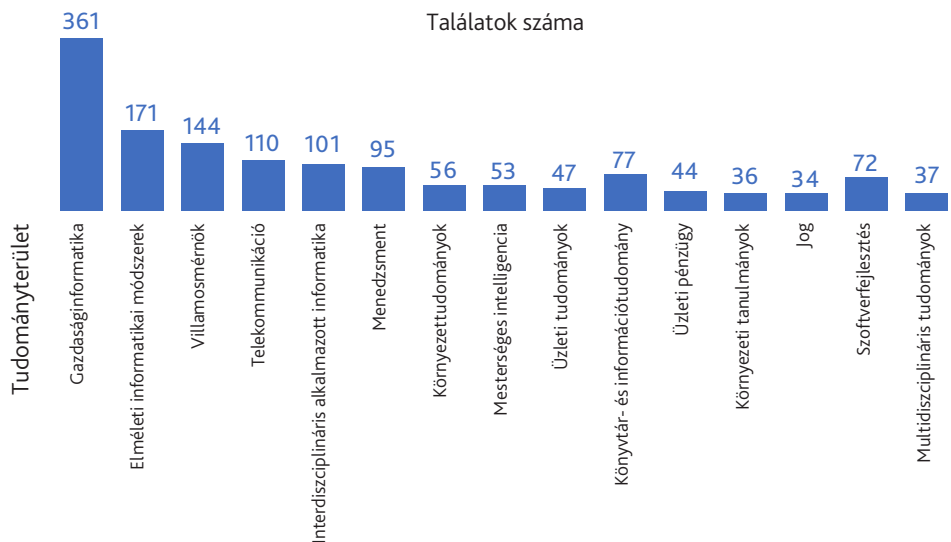
A Web of Science nem hoz létre közvetlenül grafikonokat, azonban biztosítja a nyers adatokat, amelyek felhasználhatók e vizualizációk létrehozásához. Amikor kulcsszavakat adunk meg a keresőmotorban, az lekérdezi a releváns publikációkat, beleértve azok címét, összefoglalóját, szerzőit, kulcsszavait és idézettségi adatait. Ezek az adatok ezután exportálhatók és feldolgozhatók speciális szoftverekkel, mint például a VOSviewer és a CiteSpace. Ezek az eszközök elemzik a kulcsszavak együttes előfordulását a különböző publikációkban. Ha két kulcsszó gyakran együtt jelenik meg ugyanabban a dokumentumban, akkor azokat szoros kapcsolatban állónak tekintik. A szoftver ezt követően ezeket a kapcsolatokat egy gráf formájában jeleníti meg, ahol a csomópontok a kulcsszavakat, az élek pedig a köztük lévő kapcsolat erősségét jelölik. A csomópontok mérete a kulcsszó gyakoriságát, az élek vastagsága pedig a kapcsolat erősségét jelzi.

Az adatok minőségének és konzisztenciájának biztosítása érdekében az exportált adatokat ezt követően tisztítási és előfeldolgozási lépéseken kell átvinni. Ez magában foglalhatja a hiányzó értékek kezelését, a formátumok szabványosítását és a duplikációk kiküszöbölését.

A WoS-adatbázisban a *compliance management* és a *security* szakkifejezések kerültek górcső alá első körben. Azért ez a két kifejezés, mert ezzel a kombinációval lehetett a legközelebb kerülni a *compliance*-nek a vállalatoknál alkalmazható definiálásához.

Mivel pusztán a *compliance* kifejezésre 251 767 találat érkezett, a *security*ra pedig még ennél is több, logikusnak tűnt a kettőt egybekapcsolni, és így kiszűrni az esetleges irreleváns forrásokat ahelyett, hogy a több százezer találat egyenkénti, manuális átnézése során keresnénk egy közös halmazt a két találati adatbázis között. Részben azért is létezik ennyi találat a *compliance*-re, mert számos tudományterületen, ahol eddig nem volt jellemző a szakkifejezés, újonnan a szerzők elkezdték használni ezt a szót. Fontos megjegyezni, hogy ez nem csak a társadalomtudományok területén van így, hiszen a *compliance* találatok között több mint 13 000 publikáció a farmakológiához, 8032 pedig a sebészethez tartozik, de van több mint 6000 találat az onkológia témakörében is.

A rengeteg adat miatt szükséges volt szűrni, ezért a két halmazt kombinálni kellett, és az így kapott forrásokat elemezni tovább. A két szakkifejezés keresésével nem kevesebb, mint 1236 publikációt dobott ki az adatbázis különböző tudományterületekről a 2017 és 2024 közötti időszakra vetítve. A találatok legnagyobb szelete a számítástechnika területén született 361 találattal, de jelentős számú publikáció jelent meg számítástechnika-elmélet (171), elektromos mérnöki (144), telekommunikációs (110), számítástechnikai interdiszciplináris alkalmazhatóság (101), menedzsment (95) és környezettudomány (56) területeken is. A keresési eredmények megoszlását a 1. ábra szemlélteti.



1. ábra: A compliance és a security kifejezések találati aránya a WoS adatbázisában
Forrás: a szerzők szerkesztése

Lényeges szempont volt a kutatás során, hogy az adatbázis tartalma tudományosan megalapozott legyen, ezért vizsgáltam, hogy a rendelkezésre álló publikációk közül

mekkora azoknak a száma, amelyekre további kutatók hivatkoztak. Ennek elvégzéséhez a *citation report* nevű funkciót használtam úgy, hogy az adatokat Excelbe töltöttem be. Az 1236 publikációból 890-et hivatkoztak legalább egyszer; ez az adatbázis tudományos szerzeményeinek 72%-át jelenti. Ugyanakkor a 890 hivatkozott publikációból mindösszesen 150-et hivatkoztak pusztán egyszer, a többi 740-et legalább kétszer, de leginkább annál többször. A legtöbbet hivatkozott cikkekről a 3. táblázat ad szemléltetést. A további információkat és az ugyanehhez az adatbázishoz vezető linket e tanulmány végén a *Felhasznált irodalom* tartalmazza.

3. táblázat: A legtöbbet hivatkozott szakirodalmak compliance és security tárgykörben

Szerző(k)	**Cím**	**Megjelenés éve**	**Hivatkozások száma**
Allam, Zaheer; Dhunny, Zaynah A.	On Big Data, Artificial Intelligence and Smart Cities	2019	445
Li, Jennifer; Greenwood, David; Kassem, Mohamad	Blockchain in the Built Environment and Construction Industry: A Systematic Review, Conceptual Models and Practical Use Cases	2019	322
Tandon, Anushree; Dhir, Amandeep; Islam, A. K. M. Najmul; Mantymaki, Matti	Blockchain in Healthcare: A Systematic Literature Review, Synthesizing Framework and Future Research Agenda	2020	189
Cram, W. Alec; D'Arcy, John; Proudfoot, Jeffrey G.	Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance	2019	176
Bernal Bernabe, Jorge; Luis Canovas, Jose; Hernandez-Ramos, Jose L. Torres Moreno, Rafael; Skarmeta, Antonio	Privacy-Preserving Solutions for Blockchain: Review and Challenges	2019	166

Szerző(k)	Cím	Megjelenés éve	Hivatkozások száma
Majumdar, Abhijit; Shaw, Mahesh; Sinha, Sanjib Kumar	COVID-19 Debunks the Myth of Socially Sustainable Supply Chain: A Case of the Clothing Industry in South Asian Countries	2020	161
Makhdoom, Imran; Zhou, Ian; Abolhasan, Mehran; Lipman, Justin; Ni, Wei	PrivySharing: A Blockchain-Based Framework for Privacy-Preserving and Secure Data Sharing in Smart Cities	2020	151
Mackey, Tim K.; Kuo, Tsung-Ting; Gummadi, Basker; Clauson, Kevin A.; Church, George; Grishin, Dennis; Obbad, Kamal; Barkovich, Robert; Palombini, Maria	Fit-for-Purpose? – Challenges and Opportunities for Applications of Blockchain Technology in the Future of Healthcare	2019	128
D'Arcy, John; Lowry, Paul Benjamin	Cognitive-Affective Drivers of Employees' Daily Compliance with Information Security Policies: A Multilevel, Longitudinal Study	2019	118
Attaran, Mohsen	Blockchain Technology in Healthcare: Challenges and Opportunities	2020	112
Angst, Corey M.; Block, Emily S.; D'Arcy, John; Kelley, Ken	When do IT Security Investments Matter? Accounting for the Influence of Institutional Factors in the Context of Healthcare Data Breaches	2017	103

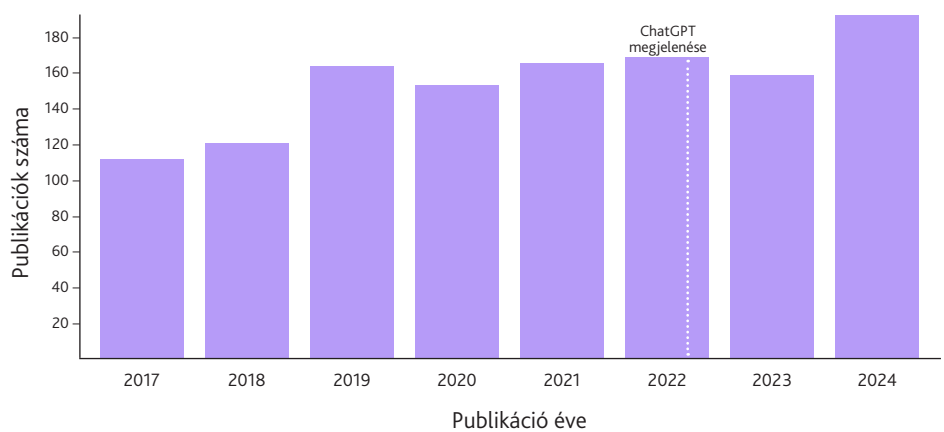
Forrás: a szerzők szerkesztése

Ebből a felsorolásból látszik tehát, hogy a legtöbbet hivatkozott cikkek *compliance* és *security* témában viszonylag frissek. A legtöbb cikk 2019 és 2020 között keletkezett; a leghivatkozottabbak közül szintén 2019 és 2020 között publikálták a legtöbbet,

a leghivatkozottabb cikk 2019-es, a legrégebbi pedig 2017-es. A keresési eredményekből több lényeges következtetés is levonható:

- Az egyik legnyilvánvalóbb tény, hogy egy dinamikusan fejlődő kutatási területről van szó, ahol a legtöbbet hivatkozott tanulmányok is csupán néhány évesek.
- A másik tény pedig az, hogy a tudományos világ a hét évnél régebbi tanulmányokat gyakorlatilag alig tekinti hivatkozható alapnak: elenyészően kevés szakértő támaszkodik ezekre az írásokra. Ez a tendencia az oka annak, hogy a 2025-ös évben időszerű a definíciós kísérlet elvégzése.

Annak érdekében, hogy minél kevesebb legyen a hiba, szúrópróbaszerűen körülbelül száz cikk ellenőrzése történt meg aszerint, hogy valóban a témával kapcsolatos irodalomról van-e szó. Ezt követően egyértelmű volt, hogy tényleg olyan publikációkat szelektált a WoS, amelyek relevánsak a kutatás számára, tehát folytatódhatott az adatok megtisztítása. A szemléletesség kedvéért a WoS-weboldal segítségével készült egy táblázat annak bemutatására, hogy egy adott évben 2017-től kezdődően mennyi publikáció jelent meg a *compliance management* és a *security* kulcsszavakkal összefüggésben (2. ábra). A függőleges, fehér pontokból álló vonal egy viszonylagos jelzése annak, hogy mikor vált elérhetővé a ChatGPT nevű mesterséges intelligencia a felhasználók számára is. Ezt a dátumot azért lényeges feltüntetni, mert a mesterséges intelligencia és a biztonság témakörét ettől a ponttól fokozott érdeklődés övezte, és az ezzel kapcsolatos szakirodalmak publikálása felgyorsult.



2. ábra: A compliance management és a security kulcsszavakkal összefüggésben megjelent tudományos szakirodalom megoszlása

Forrás: a szerzők szerkesztése

Noha a 2. ábra alapján arra lehet következtetni, hogy 2017-től kezdődően abszolút értelemben növekszik a *compliance menedzsment*tel foglalkozó publikációk száma, ez a tendencia nem érvényes éves bontásban, hiszen például meglepő módon 2023-ban

úgy csökkent a publikációk száma, hogy a ChatGPT nevű mesterségesintelligencia-alapú eszköz 2022 novemberében debütált. Logikusnak tűnhetne tehát, hogy a következő évben növekszik a *compliance*-szel kapcsolatos publikálások száma. Mégsem ez történt, tehát a hipotézis részben megdőlt.

Az idősoros elemzés alapján viszont a publikációk száma évente 16,01 publikációval nő. Ezt mutatja a 4. táblázat. A számítás az alábbi egyenletrendszerrel készült:

$$\sum y = b_0 \cdot n + b_1 \cdot \sum t$$
$$\sum ty = b_0 \cdot \sum t + b_1 \cdot \sum t^2$$

Ahol n = a vizsgált évek száma, y = a publikációk száma egy adott évben.

4. táblázat: A 2017–2024 között megjelent publikációk

Év	Publikációk száma (db)	t	t2	t*y
2017	112	1	1	112
2018	121	2	4	242
2019	165	3	9	495
2020	156	4	16	624
2021	167	5	25	835
2022	171	6	36	1026
2023	170	7	49	1190
2024	265	8	64	2120
Összesen	**1327**	**36**	**204**	**6644**

Megjegyzés: b1=16,01, b0=93,83
Forrás: a szerzők szerkesztése

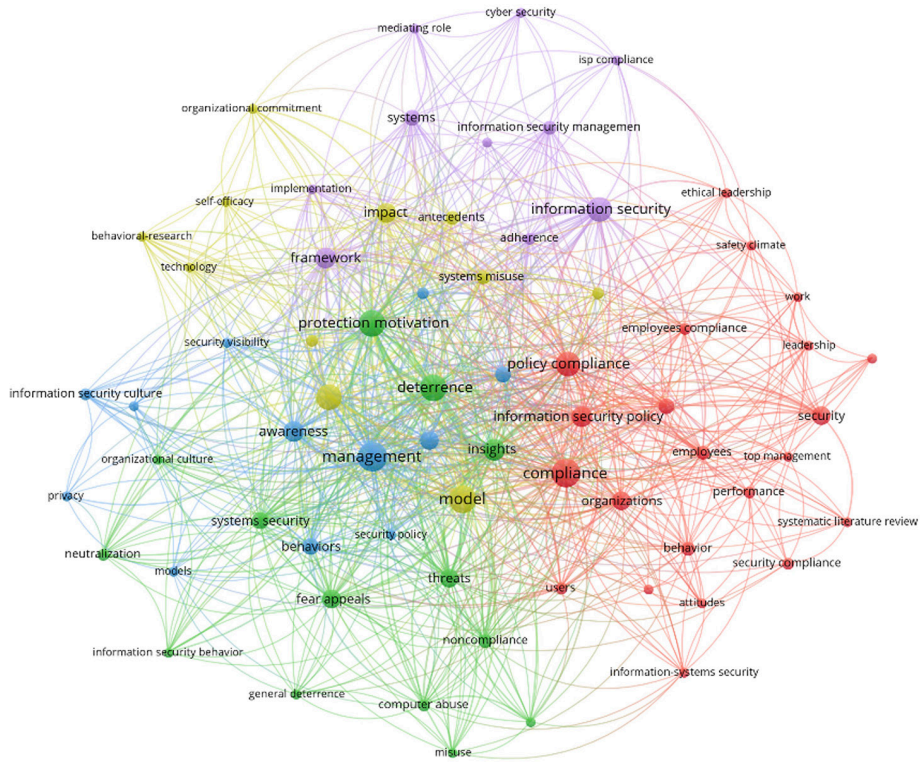
Megállapítható továbbá, hogy 2018 óta minden évben a 2017-es publikációk számát meghaladva születtek új tudományos írások a témában. A 4. táblázat annak szemléltetésére szolgál tehát, hogy az utóbbi években tényszerűen megnőtt a *compliance* és biztonság témájában írott cikkek száma a társadalomtudományok és a kiberbiztonság-számítástechnika területén. Ez annak köszönhető, hogy az utóbbi években kezdődött el azoknak a mesterségesintelligencia-alapú szoftvereknek a nyilvános használata, amelyek miatt számos szakértő fokozott érdeklődéssel fordult az adott tudományterület felé. Nemcsak a privát, individuális felhasználók kezdték el használni ezeket a szoftvereket, hanem a nagyvállalatok és a kisvállalkozások is. Az ő makroszintű tevékenységeik pedig újabb kutatások elindítását generálták – e kutatások pedig mélyebb *compliance* tudatosságot vontak maguk után.

Hogyan definiálható mégis a *compliance* az elkészült szakmai alapú anyagokból annak érdekében, hogy egy jól körülhatárolható kifejezés jöjjön létre? Ahhoz, hogy ez sikerüljön, a WoS által alkotott adatokat tovább kell finomítani, majd azokat importálni egy olyan adatvizualizációs programba, amely képes hálózatok rajzolására egy

adott kifejezés előfordulási gyakorisága alapján a felhasznált adathalmazban. Erre azért van szükség, hogy kiszűrhetők legyenek a ritka kifejezések. A ritka kifejezéseket azért kell szűrni egy definíció megalkotása során, mert egy szintetikus definíció elkészítéséhez a leggyakrabban ismétlődő kifejezéseket indokolt használni, nem pedig azokat, amelyek viszonylag ritkán fordulnak elő. Ennek érdekében a WoS weboldalán az adatokat *Plain Text File*-ként exportálva az *Abstract, Keywords and Addresses* opciónál az *abstract, keywords* és *research areas* kifejezéseket választottuk az adatok finomítása végett, a *Cited Reference and Use* oszlopban pedig minden opciót kiválasztottunk, ezek a *cited references, cited reference count, usage count, hot paper* és *highly cited* lehetőségek voltak.

Azért van szükség a kulcsfogalmak adatainak exportálására, nem pedig a szerzők nevére, mert a kutatás tárgya nem egy adott szerzőre vonatkozó hivatkozások száma, hanem az adott szerzők hasonló kifejezésekre utaló hivatkozásainak mennyisége. A hivatkozott szavakat ismerve egyszerűbben megalkotható egy definíció. Mindehhez olyan alkalmazás szükséges, amely segít az adathalmazt feldolgozni. Ilyenek a teljesség igénye nélkül a már említett VOSviewer és a CiteSpace. Ezek számos módszert tartalmaznak a bonyolult hálózatok megfejtésére és megjelenítésére. A VOSviewer alkalmazásra épült a kutatás: a program trendeket és kapcsolatokat keres a kifejezések, szerzők vagy intézmények együttes előfordulásának elemzésével, majd a kikalkulált kapcsolatok alapján létrehozza a hálózat vizuális ábrázolását, amelyben a csomópontok konkrét elemeket (például szerzőket vagy kulcsszavakat), az élek pedig a köztük lévő kapcsolatokat jelölik. A csomópontok méretén és színén, valamint az élek vastagságán és színén keresztül további információ, például az előfordulás gyakorisága vagy a kapcsolat erőssége is közölhető.

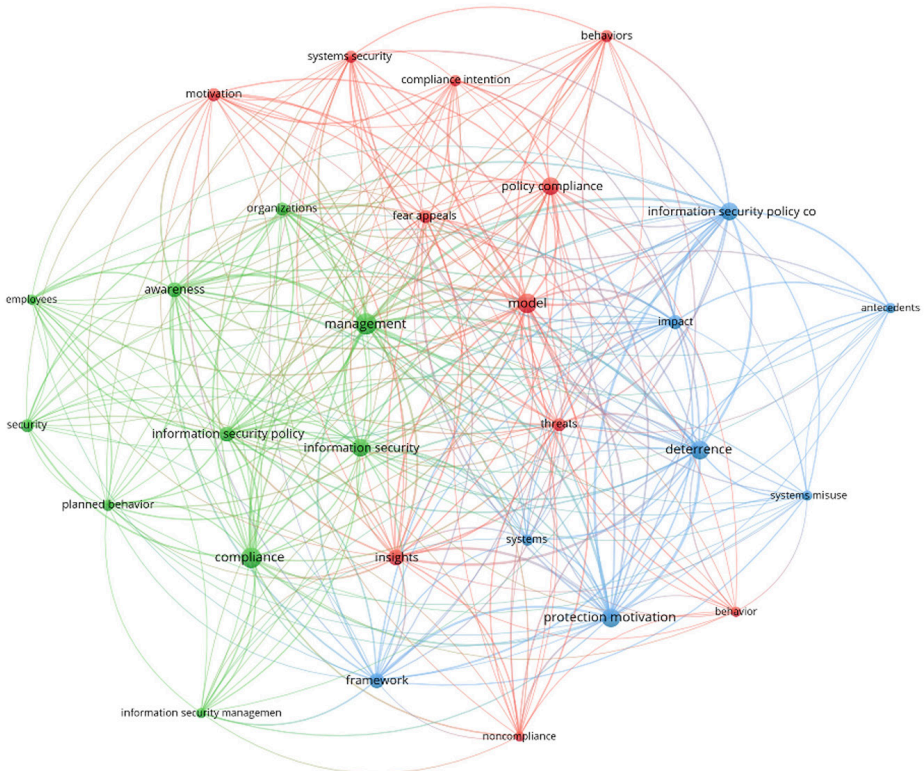
A VOSviewerbe betöltött találatok relevanciájuk szerint lettek rendszerezve. A VOSviewer saját keresőprogramja a szakkifejezések előfordulásának keresését végezte, aminek hatására az összes kulcsszót elemezte a feltöltött szövegekben. Ez összesen 293 kulcsszót jelentett a teljes tanulmánykorpuszon belül. Az első hálózati térkép megalkotása során (3. ábra) az volt a kitétel a kulcsszavak szelektálásakor, hogy egy adott szó legalább két szövegben jelenjen meg. Számszerűen ez 69 olyan kulcsszót jelentett, amelyek legalább két tanulmányban fordulnak elő az 1236 megfigyelt szakszövegben. A 69 szakkifejezés szerepel a 3. ábrán.



3. ábra: Legalább két tanulmányban leggyakrabban használt kulcsszavak és csomópontok
Forrás: a szerzők szerkesztése

A 3. ábrán az látható, hogy mely kulcsszavak rendelkeznek a legtöbb kapcsolattal, és melyek relatíve kevesebbel. Például az egyik legtöbb kapcsolattal rendelkező szakkifejezés ebben a verzióban a *management,* vagyis menedzsment. Minél nagyobb egy szó mögött az adott területű kör, annál többször fordult elő. A legtöbbször szereplő fő kifejezések máris jól értelmezhetők a tanulmányokban még akkor is, ha a térkép elég „zajos",[12] tehát túl sok részletet lenne szükséges egy olyan definícióba sűríteni, ami e szerint a hálózati térkép szerint készül. Ez az oka annak, hogyan módosítottuk az ábrát: a második hálózati térkép már aszerint készült, hogy legalább négy tanulmányban kell szerepelnie egy adott szakkifejezésnek annak érdekében, hogy csúcsot alkothasson a térképen. Az így megjeleníthető maximális találat 29 volt, ugyanis ennyi kifejezés fordul elő legalább négy tanulmányban. Az így kapott hálózat a 4. ábrán látható módon modellezhető.

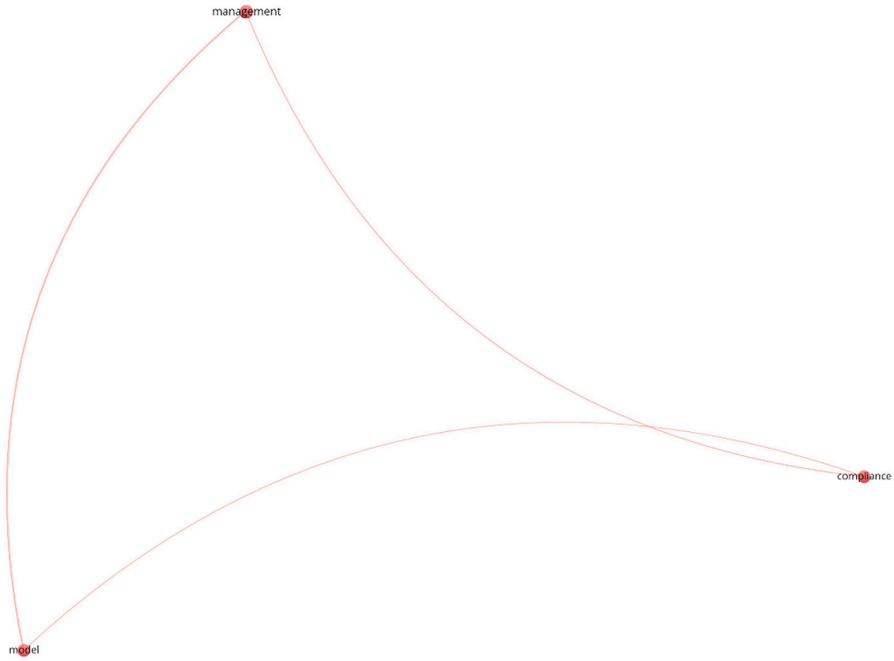
[12] Kahneman 2021.



4. ábra: Legalább négy tanulmányban leggyakrabban használt kulcsszavak és csomópontok
Forrás: a szerzők szerkesztése

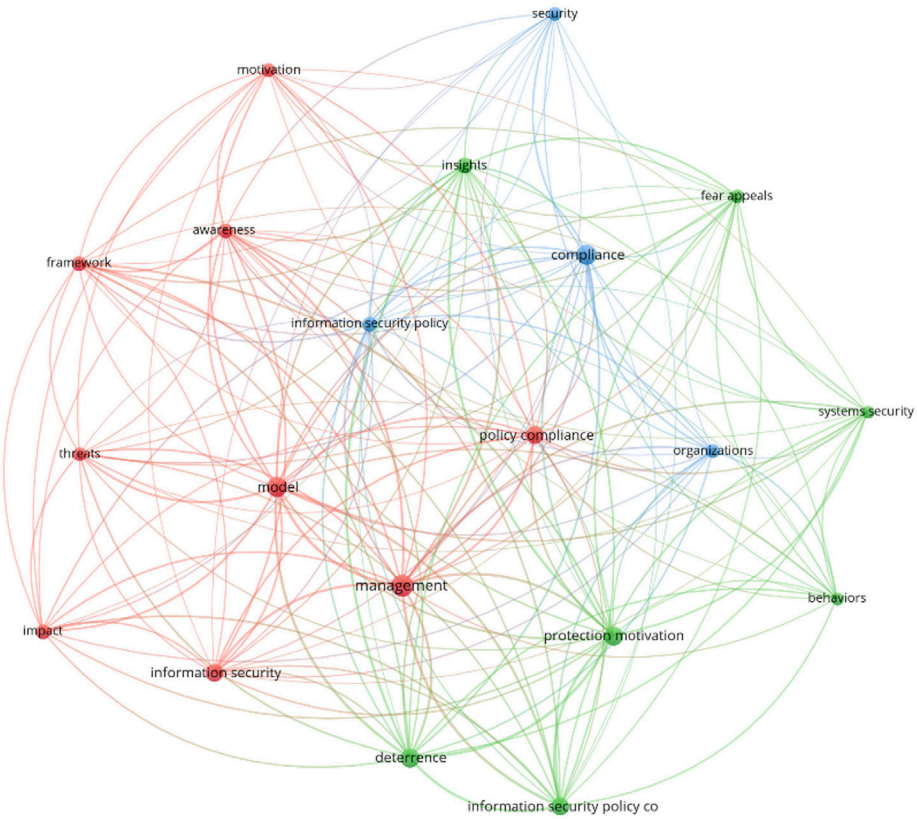
A 3. ábra viszonylag „zajos térképe" átláthatóbbá vált a 4. ábrán, és azok a szakkifejezések rajzolódnak ki benne, amelyek a 3. ábrában a legnagyobb számosságban fordultak elő a vizsgált publikációkban. Ez alapján megvizsgálható, hogy mi a maximális előfordulás, amit még ezzel a szoftverrel modellezni lehet.

Az 5. ábrán a maximális előfordulás szerint modelleztük a kulcsszavakat, ami 15 volt, vagyis 15 tanulmányban fordultak elő maximum a legtöbb tanulmányban szereplő fogalmak.



5. ábra: A leggyakrabban előforduló kulcsszavak és csomópontok
Forrás: a szerzők szerkesztése

Az 5. ábrán bemutatott térkép a kutatás szempontjából elvetendő, mert túl kevés kulcsszó éri el a beállított kritériumokat, tehát kevés él és csúcs található benne. A túl sok és a túl kevés kulcsszó kiküszöbölése érdekében végül hatra állítottuk be azt a minimum előfordulást, amennyiszer a tanulmányban egy adott szakkifejezésnek szerepelnie kell azért, hogy a térképen csúcsként megjelenjen, azonban ez a szám szabadon módosítható különböző szempontok szerint. Átláthatósági szempontból hat kulcsszó maradt. Hat kulcsszónál már relatíve kevésbé zajos térkép születik, ugyanakkor specifikus marad az adott ábra annyira, hogy a *compliance* és a *security* területek sokszínűségét és kiterjedt fogalmi kereteit jól szemléltesse egy ebből készülő definíció. Ekkor született a 6. ábrán látható térkép.



6. ábra: Compliance definiálási kísérlet csomópontjai
Forrás: a szerzők szerkesztése

A 6. ábrán bemutatott térkép már jóval kevésbé „zajos", könnyebb az adatok értelmezése. Látszik, hogy a legnagyobb csomópontok, csúcsok azok a kifejezések, amelyek relevánsak lehetnek a *compliance* körülírására. Ilyen például a *policy compliance, protection motivation, organization, information security, information security policy, management, model, deterrence, awareness*.

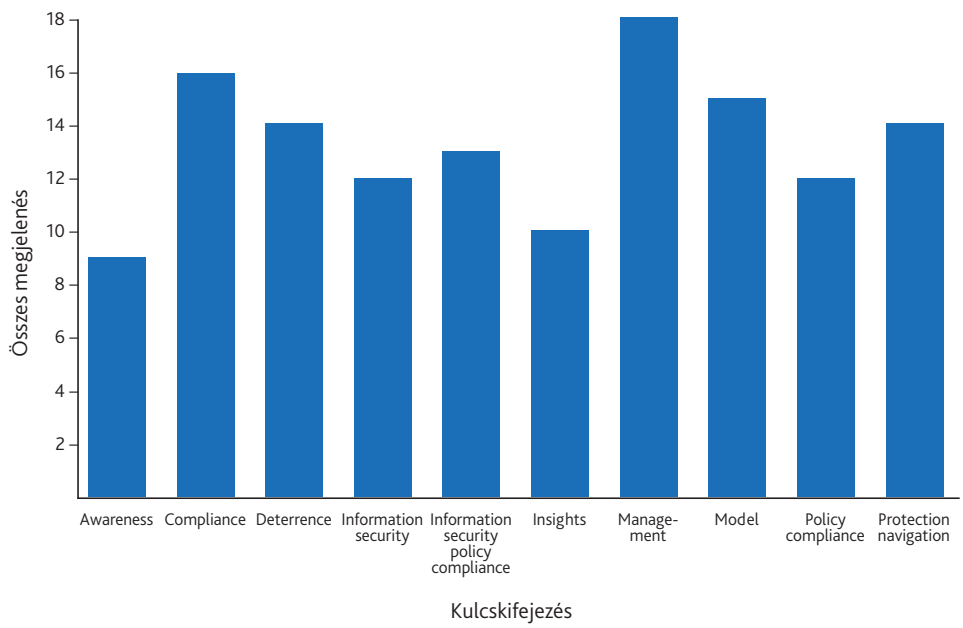
A leggyakrabban előforduló tíz kifejezés szemléltetésére készült az 5. táblázat. Ebben az Összes megjelenés című oszlop az adott szó összes előfordulási számát mutatja. Az Összes kapcsolat erőssége *(total link strength)* pedig egy adott kifejezés más kifejezésekkel való kapcsolatát tünteti fel. Minél nagyobb ez az érték, a kifejezésnek annál több kapcsolata van más szakszavakkal. Az utolsó oszlop pedig annak a mértékét jeleníti meg, hogy egy adott kulcsszó az összes tanulmány hány százalékában fordul elő.

5. táblázat: A leggyakrabban előforduló tíz kifejezés eloszlási adatai

Kulcskifejezés	Összes megjelenés	Összes kapcsolat erőssége	%
Managemenent	18	107	0,0145
Model	15	102	0,0121
Deterrence	14	93	0,0113
Protection navigation	14	91	0,0113
Information security policy compliance	13	80	0,0105
Insights	10	72	0,0080
Awareness	9	65	0,0072
Compliance	16	63	0,0129
Information security	12	61	0,0097
Policy compliance	12	61	0,0097

Forrás: a szerzők szerkesztése

A 5. táblázat adatai alapján készült a 7. ábra.



7. ábra: A leggyakrabban előforduló kifejezések darabszáma
Forrás: a szerzők szerkesztése

Az előbbiek alapján a *compliance* gyakorlati definíciós kísérletének eredménye így foglalható össze:

A *compliance* olyan szakterület, amely a szervezetek vonatkozó jogszabályi előírásoknak, belső irányelveknek és etikai normáknak való megfelelőségét biztosítja, továbbá védelmi eszköz. A *compliance* kulcsfontosságú működési terület a menedzsment számára, és alapvető szerepet játszik abban, hogy a szervezet tevékenysége törvényes, etikus és átlátható legyen, ami kiterjed többek között az információs biztonság, a céges menedzsment, a jog és az adózás területeire annak érdekében, hogy a különböző jogszabályi előírások maradéktalan betartásával legyen képes működni.

Magyarországi publikációk

A hazai publikációk szemléltetése nehezebb feladat, ugyanis jóval kevesebb a *compliance*-szel foglalkozó szakirodalom. Az eredeti terv szerint a WoS adatbázisából képzett térképhez hasonló módon alkottunk volna meg a hazai szakirodalomból is hálózati térképet. Ezt azonban nem sikerült megvalósítani, mert egy szemléletes térképhez a jelenleginél több adatra van szükség. A rendelkezésre álló cikkeket nem lehet a VOSviewerhez hasonló módon ábrázolni, mert a kevés *input* miatt az eredmény nem lenne látványos. A probléma megoldása, hogy a hazai publikációk alapján kell ellenőrizni a nemzetközi gyakorlat vizsgálata által létrehozott szintetizált definíciót.

A Magyar Tudományos Művek Tárának adatbázisa alapján összesen hét azoknak a tudományos publikációknak száma, amelyek említik a *compliance* és *security* kifejezéseket is. Ezek a következők:

- Tilli, Giuditta et al. (2024): Supporting Measures to Improve Biosecurity within Italian Poultry Production. *Animals,* 14(12), 1734, 1–15.
- Bálint, Ferenc (2023): Anti-Money Laundering with a Special Focus on the Cyber Security Threats and Vulnerabilities. *National Security Review,* (2), 144–157.
- Delpont, Mattias et al. (2023): Monitoring Biosecurity in Poultry Production: An Overview of Databases Reporting Biosecurity Compliance from Seven European Countries. *Frontiers in Veterinary Science,* 10.
- Dunay, Pál (2020): Arms Control Arrangements under the Aegis of the OSCE: Is There a Better Way to Handle Compliance? In Müller-Färber, Thomas – Weiß, Simon (szerk.): *In Times of Eroding Cooperative Security: How to Save Conventional Arms Control in Europe?* Loccum: Evangelische Akademie Loccum, 51–69.
- Bicaku, Ani et al. (2019): Security Safety and Organizational Standard Compliance in Cyber Physical Systems. *Infocommunications Journal,* 11(1), 2–9.
- Barta, Gergő (2018): Challenges in the Compliance With the General Data Protection Regulation: Anonymization of Personal Information and Related Information Security Concerns. In *Knowledge – Economy – Society. Business, Finance and Technology as Protection and Support for Society.* Cracow: Cracow University of Economics, 115–121.
- Dunay, Pál (2000): The CFE Compliance Record a Decade After Treaty Signature. *S + F Sicherheit und Frieden,* 18(4), 327–333.

A szükségesnél kevesebb publikáció miatt a keresési módszertan módosítása történt annyiban, hogy nem lett beállítva kezdő és záró év. Ettől függetlenül meglepő, hogy a hétből hat tudományos cikk 2018-nál nem régebbi, három pedig 2023 óta készült. Ezen a szűk mintán is látszik, hogy mennyivel izgalmasabb téma a kutatók számára az utóbbi években a *compliance,* mint korábban volt. A hét tudományos publikációban manuálisan ellenőriztük, hogy valóban szerepelnek-e benne a *compliance* és *security* kifejezések. A keresőmotor jónak bizonyult egy cikk kivételével, és valóban tartalmazták ezeket a kulcsfogalmakat. Ezeken a fogalmakon keresztül lett ellenőrizve a definíció relevanciája. Az az egy cikk, amelyikben nem szerepeltek a kulcsszavak, a „nem felelt meg" értékelést kapta, hiszen egy olyan teszten, ahol a *compliance* szó definíciója a vizsgálat tárgya, ez az adatsor nem megfelelő.

6. táblázat: A magyarországi szakirodalom megoszlása

Szerző(k)	**Megjelenés éve**
Tilli, Guiditta et al.	2024
Bálint Ferenc	2023
Delpont, Mattias et al.	2023
Dunay Pál	2020
Bicaku, Ani et al.	2019
Barta Gergő	2018
Dunay Pál	2000

Forrás: a szerzők szerkesztése

Látható, hogy a publikációk számának változása stagnál, az adatbázis szerint 2001–2017 között egyáltalán nem jelent meg tudományos igényű munka a témában. Emiatt is érdekes, hogy az utóbbi hét év adja a cikkek több mint 80%-át. Látható, hogy ez az adatbázis nem tud annyi adatot generálni, mint a WoS. A trendek azonban itt is látszanak, miután a keresett kifejezések az előző vizsgálatban használtakkal megegyezők: a keresőmotor algoritmusa a *compliance*security* volt, a WoS-en használt keresési algoritmussal megegyezően.

A definíció ellenőrzésének lényege, hogy mindegyik publikációban a vizsgált kifejezés előfordulásának gyakoriságát (7. táblázat) figyeltük. Ezt követően szúrópróbaszerűen kiválasztottunk három különböző cikkből három részletet, amelyben szerepel a *compliance* kifejezés.

7. táblázat: A vizsgált kifejezések előfordulásának gyakorisági adatai

A szakirodalom szerzője	A szakkifejezések száma a tanulmányban
Tilli, Guiditta et al.	11
Bálint Ferenc	0
Delpont, Mattias et al.	20
Dunay Pál (2020)	31
Bicaku, Ani et al.	174
Barta Gergő	17
Dunay Pál (2000)	33

Forrás: a szerzők szerkesztése

A három szakcikk ellenőrzésének szemléltetése

Dunay Pál *The CFE Compliance Record a Decade After Treaty Signature* című publikációjából: „Beyond certain non-compliance concerns, there were very few observations made on the general functioning of the Treaty."[13] Ez esetben helytálló a megalkotott definíció, hiszen kimondottan a nem megfelelőségre utal a szöveg valamilyen etikett vagy jogszabály alapján.

A második szövegből, Bicaku és munkatársainak *Security Safety and Organizational Standard Compliance in Cyber Physical Systems* című munkájából választott definíció: „In order to address the aforementioned concerns, in our previous work, we have proposed an initial approach to automatically verify standard compliance by using a monitoring and standard compliance verification framework, as shown in Figure."[14] A fogalom itt is helytálló, hiszen a szöveg alapján egy olyan verifikációs, megfelelőségi standardot kell felállítani, amely eleget tesz a belső előírásoknak. A szerző által használt jelentést lefedi a szintetizált definíció.

A harmadik idézet a Delpont és társai által jegyzett cikkből származik: „In practice, biosecurity compliance is assessed by various actors (e.g., academic, private and public institutions), and the results of such assessments may be recorded and gathered in databases which are seldom shared or thoroughly analyzed."[15] A szerzők ebben a cikkben is különböző megfelelési kritériumokról beszélnek, amelyeket különböző aktorok, például akadémiai és közintézmények alkotnak és ellenőriznek. Valamifajta

[13] Dunay 2020: 298.
[14] Bicaku 2019.
[15] Delpont 2023.

jogszabályi, etikai és belső szabályrendszeri megfelelőségről van szó, ennek esetében is elfogadható a szintetizált definíció.

Az adatok mennyisége a hazai adatbázisban limitált, a definíció megalkotásánál biztosabb alapot adtak a WoS-ből szerzett adatok és az ebből alkotott térképek. A források áttekintését illetően pedig megjegyzendő, hogy a szerzők által használt *compliance* kifejezés illik a szintetizált definícióra, egyáltalán nem módosítja azt. Nem volt olyan cikk a hatból, amelyben a *compliance* kifejezés használata módosította volna az eredeti definíciót, vagy hatására át kellett volna fogalmazni. Kijelenthető tehát, hogy a szintetizált definíció megállta a helyét az olyan független források esetében is, amelyek nem voltak benne az eredeti adatbázisban. Megjegyzendő továbbá, hogy a hazai publikációk mindegyike beilleszthető valamilyen társadalomtudományi kutatási területbe, ezen belül is a jog, a biztonságpolitika, illetve a kiberbiztonság tárgykörébe. Ezt azért fontos kiemelni, mert a WoS-adathalmaz kimondottan olyan cikkekből származik, amelyek javarészt ezekhez a területekhez kapcsolódnak. Nem véletlen tehát, hogy ilyen rugalmasan ráilleszthető a definíció ezekre a hazai cikkekre is. A többi tudományterület *compliance* vizsgálata pedig alkalmas tárgya lehet a jövőben további tanulmányoknak; kimondottan hiánypótló lenne a jelen tanulmány alapján azt megvizsgálni, hogy létezik-e olyan tudományterület, specializáció, ahol a szintetikus definíció esetleg nem használható.

A compliance megjelenése különböző tudományterületeken az OpenAlex adatbázis tükrében

Az OpenAlex egy átfogó katalógusa a tudományos munkáknak, szerzőknek és intézményeknek. Az adatbázis alapvetően egy hatalmas tudásgráfként működik, amely összekapcsolja a kutatási cikkek millióit, szerzőit és intézményeit. Számos adatforrást használ: a hagyományos akadémiai cikkektől a preprintekig, továbbá a konferencia-előadásokig terjedő széles spektrum indexelésével az OpenAlex átfogó képet nyújt a globális kutatási tájról. Egyik fő erőssége, hogy képes egyértelműsíteni a szerzőket és az intézményeket. Ez azt jelenti, hogy pontosan képes azonosítani ugyanazt a szerzőt vagy intézményt különböző publikációkban, még akkor is, ha a nevük kissé eltérő vagy következetlenül van írva. Ez az egyértelműsítési folyamat kulcsfontosságú a pontos idézetelemzés, az együttműködés nyomon követése és a hatásértékelés szempontjából.

A kutatásban fontos volt ez az adatbázis, mivel a rengeteg adatmennyiség lehetőséget adott annak vizsgálatára, mely tudományterületeken publikáltak a legtöbbet *compliance* témában. Olyan kifejezések kiszűrése történt, amelyek a *compliance*-szel foglalkoznak, és azt vizualizáltuk, hogy milyen összeköttetésben állnak ezek a tudományterületek egymással.

Az OpenAlex jóval nagyobb adatbázisból dolgozik, mint a WoS. A publikációk vizualizálása a korábban bemutatott VOSviewer alkalmazással készült, számos dolgot máshogyan kellett csinálni az adatok jóval nagyobb elérhetősége miatt. Az első szembetűnő különbség az volt, hogy a nagyobb adatbázis miatt jóval több találatot adott ugyanarra a keresési beállításra, mint a WoS-adatbázisnál. Ha csak a *compliance* és *security* szavakra keresünk rá, az OpenAlex 495 100 találatot ad, amiből 57% érhető el a nyílt hozzáférés miatt. Mivel sem az OpenAlexről nem lehet százezer találatnál nagyobb adathalmazokat

letölteni, sem a VOSviewerbe nem lehet pár ezer adatnál többet integrálni, finomítani kellett a keresési beállításokon.

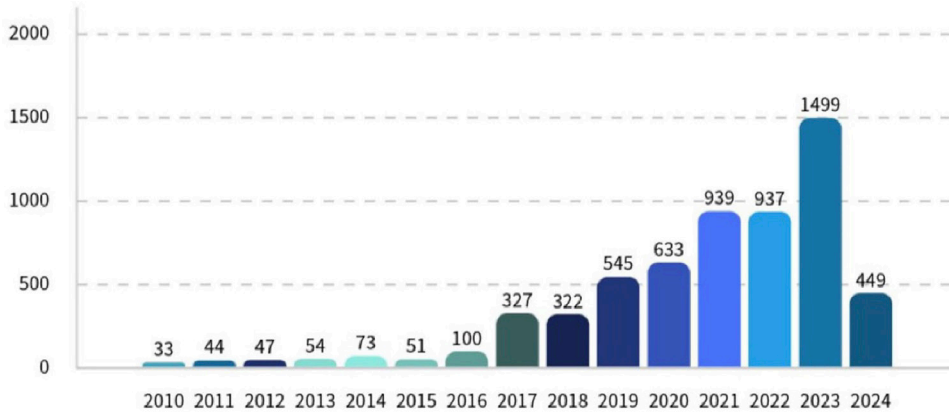
Idősávként a 2010 és 2024 közötti időszakot határoztuk meg, hiszen hasonló időkeretben mozogtak a Web of Science adatbázisából alkotott ábrák is. A fentieken túl fontos volt a rengeteg találat miatt szűkíteni és bonyolítani az adathalmazt, ezért a korábbi gyakorlattal ellentétben több kulcskifejezés szűrése valósult meg. A 8. táblázatban jól látszik, hogy különböző kulcskifejezés-kombinációkkal hány találat merült fel az OpenAlex adatbázisából.

8. táblázat: Kulcsszavak – OpenAlex

Kulcsszavak	**OpenAlex-találatok**
Compliance*security	357 800
Compliance*security*management	248 800
Compliance*security*management*business	160 600
Compliance*security*management*business*artificial intelligence	20 600
Compliance*security*management*business*artificial intelligence*law	13 240
Compliance*security*management*business*artificial intelligence*law*legal	10 970
Compliance*security*management*business*artificial intelligence*law*legal European Union	6054

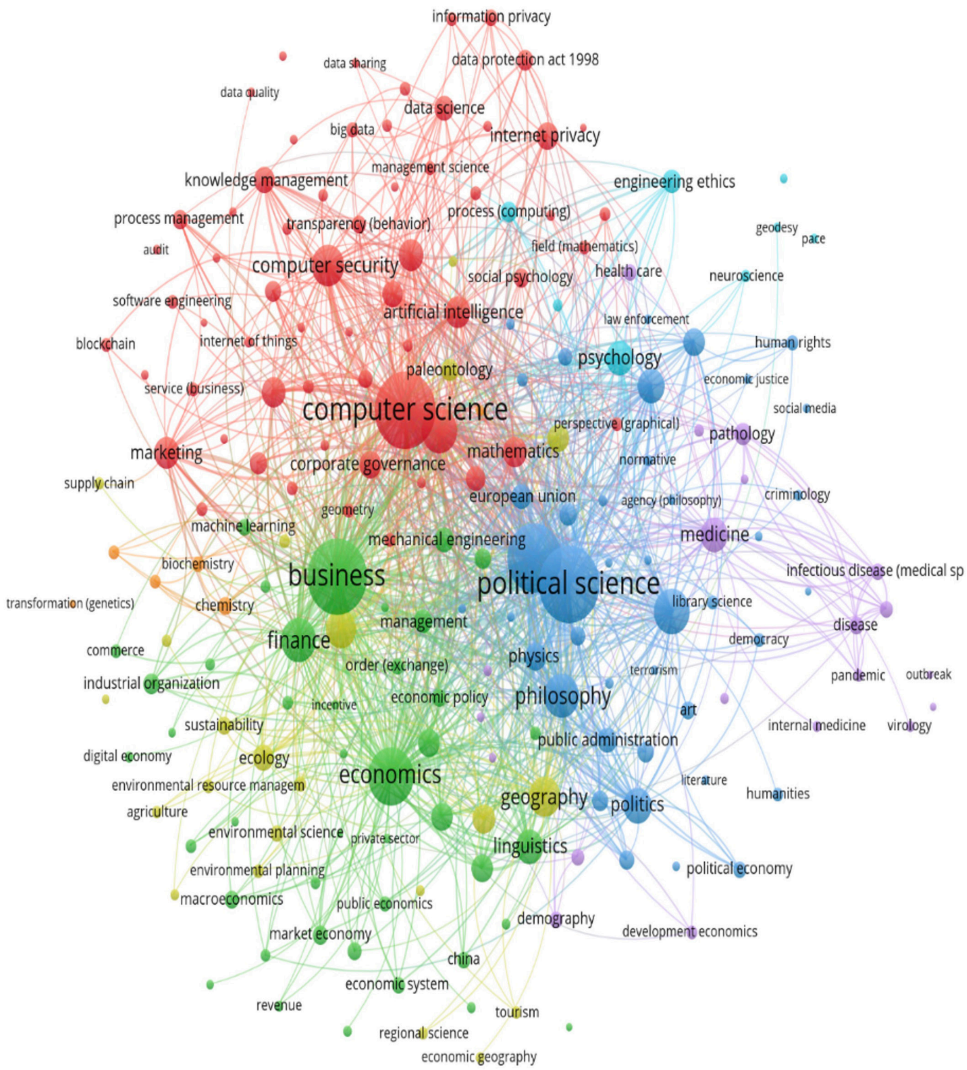
Forrás: a szerzők szerkesztése

Nyilvánvaló, hogy minél komplexebb egy szűrés, annál kevesebb találat van. A szemléletes adatvizualizáció érdekében csökkentettem a minta számosságát, hiszen ekkora adat mellett se nem szemléletes, se nem használható egy adatvizualizációs térkép, hiszen túl sok adat szerepelne rajta. 6054 találat lett betöltve a VOSviewerbe. Ebben az esetben is megfigyelhető, hogy az idő előrehaladtával tendenciózusan nő a témával foglalkozó tudományos cikkek száma, kivéve a 2024-es évet. Ez azzal magyarázható, hogy a keresés idején a legutolsó évből még nem volt minden szakcikk online elérhető, tehát még nem része az adatbázisnak. Az elkészült kutatások jellemzően először előfizetői formátumban jelennek meg, majd némi idő elteltével válnak korlátlanul nyilvánossá. Feltételezhető, hogy 2023-ra vonatkozóan ez a folyamat már lezajlott, mert más nem igazán magyarázhatja a 2024-ben írt cikkek számának ilyen mértékű visszaesését – már csak azért sem, mert a mesterséges intelligenciában íródott cikkek és publikációk száma nem csökkenhetett ekkora mértékben. A 8. ábra azt szemlélteti, hogy egy adott évre hány tudományos publikáció jut.



8. ábra: Az OpenAlex-kulcsszavak éves bontásban
Forrás: a szerzők szerkesztése

Miután az adathalmaz rendelkezésre állt, feltöltöttük a VOSviewerbe annak érdekében, hogy a szükséges gráfok kirajzolódjanak. Feltűnő volt, hogy ezekben a publikációkban sokkal több kulcsszó-előfordulás volt, mint azokban a publikációkban, amelyeket a Web of Science adatbázisából használtunk. Például sokkal több volt ugyanazoknak a kulcsszavaknak az előfordulási aránya, 5 előfordulásnál még 1094 publikáció esett ebbe a halmazba, vagyis ennyi olyan publikáció volt a több mint 6000 letöltött adatból, amelyikben egy kulcsszó legalább ötször szerepelt. A várakozásokkal ellentétben a *threshold* emelését követően csak viszonylag lassan csökkent a publikációk száma. Például 10 előfordulásnál még mindig 633 publikáció esett bele ebbe a halmazba, de 20-nál is, míg 37 247 előfordulásnál már csak pontosan 200 ilyen cikk volt. Ez utóbbi maradt, hiszen a VOSviewer ajánlása szerint körülbelül 200–250 kell hogy legyen a maximum csúcsok száma annak érdekében, hogy még átlátható legyen az adatvizualizációs térkép. 47 előfordulásra lett állítva a *co-occurrence* alapján a kulcsszókészlet. Az így kapott térkép a 9. ábrán látható.



9. ábra: OpenAlex-kulcsszavak tudományterületek szerinti csomópontjai
Forrás: a szerzők szerkesztése

Jól kivehetők azok a legfőbb tudományterületek, amelyek keretében a legtöbb publikáció készült. Nem meglepő módon ezek az informatika *(computer science)*, az üzleti tanulmányok *(business)*, a politikatudomány *(political science)* és a közgazdaságtan *(economics)* tudományterületbe estek. Tehát e kutatási területek gyakorlói publikáltak a legtöbbet a *compliance*, a *management*, a biztonság *(security)*, az üzleti élet *(business)*, a mesterséges intelligencia *(artificial intelligence)*, a jog *(legal)*, a törvény *(law)* és

az Európai Unió *(European Union)* kifejezések használatával. Szembetűnő a tény, hogy mennyire interdiszciplináris a kapcsolódó tudományterületek köre és ezek a nagyobb klaszterek; tulajdonképpen az összes akadémiai tudományterület felsorakozik valamilyen összeköttetésben ezen a térképen a virológiától kezdve a demokráciatudományokon és a geodézia kutatásán át az agysebészetig. Ez a szerteágazó eredmény megerősített abban, hogy a téma vizsgálata valóban szükséges, hiszen rendkívül sok területet érintenek a tudományos előrehaladással járó potenciális következmények. Ez a hálózati térkép (9. ábra) a bizonyítéka annak, hogy milyen sok kutatási területen van jelen a *compliance,* ami megerősített abban, hogy nem lehet figyelmen kívül hagyni a dinamikus fejlődése során módosuló fogalmával járó következményeket.

Összegzés

Összegezve a kutatást elmondható, hogy a *compliance* népszerű és egyre népszerűbbé váló témakör számos különböző tudományterület számára. A hazai és nemzetközi publikációk számából is kitűnik, hogy az utóbbi években megnőtt iránta a tudományos érdeklődés. A nemzetközi publikációk leggyakrabban előforduló kifejezéseivel alkotható hálózati térkép pedig hozzásegített szintetizálni egy, a kutatás eredményeire alapozó definíciót.

A *compliance* olyan szakterület, amely a szervezetek vonatkozó jogszabályi előírásoknak, belső irányelveknek és etikai normáknak való megfelelőségét biztosítja, továbbá védelmi eszköz. A *compliance* kulcsfontosságú működési terület a menedzsment számára, és alapvető szerepet játszik abban, hogy a szervezet tevékenysége törvényes, etikus és átlátható legyen, ami kiterjed többek között az információs biztonság, a céges menedzsment, a jog és az adózás területeire annak érdekében, hogy a különböző jogszabályi előírások maradéktalan betartásával legyen képes működni.

A definíció megállta a helyét akkor is, amikor manuális ellenőrzés történt a hazai szerzők által jegyzett cikkek alapján. Kijelenthető továbbá, hogy az első fejezetben bemutatott elméleti definícióval alapvetően összecseng a gyakorlati definíció. Tekintettel arra, hogy az elméleti definíciókban a *compliance* tartalmilag egyrészt megfelelés a jogszabályoknak, másrészt megfelelés a jogszabálynak nem minősülő egyéb külső előírásoknak, belső szabályzatoknak, íratlan (etikai) szabályoknak, *soft law*nak, piaci szokványoknak, nemzetközi standardoknak, szabványoknak. A gyakorlati definíció azonban tovább mélyíti a fogalmat, és kiemeli a biztonságot, a menedzsment szerepét és a tudatosságot is a *compliance*-szel kapcsolatban. A *compliance* definíciós kísérletének gyakorlati vetülete, hogy egyszerre jelennek meg a kontroll és a támogató feladatok is a *compliance* területén:

- kockázatok, érdekkonfliktusok azonosítása, kezelése;
- a szervezet szabályos működésének támogatása;
- hiányosságokat kezelő intézkedések, javaslatok megtétele;
- a megfelelőségért való belső, szervezeti szintű tudatosság terjesztése;
- riportolás a felső vezetésnek;
- a korrupció megakadályozása;
- összeférhetetlenség, érdekkonfliktusok kezelése;

- információáramlásra vonatkozó korlátozások betartása;
- piaci visszaélések (bennfentes kereskedelem, tisztességtelen árfolyam-befolyásolás) megelőzése;
- pénzmosás és a terrorizmus finanszírozása elleni küzdelem;
- külső és belső csalások megelőzése;
- titok- és adatvédelem (üzleti, bank-, értékpapír- és biztosítási titok, személyes adatok védelme);
- transzparens működés biztosítása;
- az ügyfelekkel való tisztességes bánásmód biztosítása, panaszkezelési tevékenyég;
- reputáció, jó hírnév megőrzése;
- ellenőrzések lefolytatása;
- hatóságokkal való kapcsolattartás.

Egyértelműen látható, hogy a *compliance* sokrétű és összetett, dinamikusan fejlődő, modern terület, amely számos kutatandó kérdést vet fel, mert olyan kritériumokkal foglalkozik, amelyek a szervezetek biztonságos létét igyekeznek megóvni.

Felhasznált irodalom

Allam, Zaheer – Dhunny, Zaynah A. (2019): On Big Data, Artificial Intelligence and Smart Cities. *Cities,* 89, 80–91. Online: https://doi.org/10.1016/j.cities.2019.01.032

Association of Certified Fraud Examiners (2022): *Occupational Fraud 2022: A Report to the Nations.* Online: https://acfepublic.s3.us-west-2.amazonaws.com/2022+-Report+to+the+Nations.pdf

Ambrus István – Mezei Kitti – Molnár Erzsébet (2021): *Magyarázat a compliance jogszabályairól I. Általános és büntetőjogi compliance.* Budapest: Wolters Kluwer.

Angst, Corey M. et al. (2017): When Do IT Security Investments Matter? Accounting for the Influence of Institutional Factors in the Context of Healthcare Data Breaches. *MIS Quarterly,* 41(3), 893–916. Online: https://doi.org/10.25300/MISQ/2017/41.3.10

Attaran, Mohsen (2022): Blockchain Technology in Healthcare: Challenges and Opportunities. *International Journal of Healthcare Management,* 15(1), 70–83. Online: https://doi.org/10.1080/20479700.2020.1843887

Bálint,Ferenc (2023): Anti-Money Laundering With a Special Focus on the Cyber Security Threats and Vulnerabilities. *National Security Review,* (2), 144–157. Online: https://s2prodstorage.blob.core.windows.net/s2cmsblob/Files/National%20Security%20Review/2023_2_NSR.pdf?sp=r&st=2025-03-25T09:37:58Z&se=2-035-03-25T16:37:58Z&spr=https&sv=2024-11-04&sr=c&sig=PAOb3jtCphbbzRgBEutrTUH2uSjRNnF3G8dVaL8Y3Z0=

Balogh Monika (2015): *A munkaügyi compliance audit.* Budapest: Wolters Kluwer.

Barta, Gergő (2018): Challenges in the Compliance with the General Data Protection Regulation: Anonymization of Personal Information and Related Information Security Concerns. In *Knowledge – Economy – Society. Business, Finance and*

Technology as Protection and Support for Society. Cracow: Cracow University of Economics, 115–121.

Bernabe, Jorge Bernal et al. (2019): Privacy-Preserving Solutions for Blockchain: Review and Challenges. *IEEE Access,* 7, 164908–164940. Online: https://doi.org/10.1109/ACCESS.2019.2950872

Bicaku, Ani et al. (2019): Security Safety and Organizational Standard Compliance in Cyber Physical Systems. *Infocommunications Journal,* 11(1), 2–9. Online: http://doi.org/10.36244/ICJ.2019.1.1

Bock, Dennis (2009): Strafrechtliche Aspekte der Compliance-Diskussion – § 130 OWiG als zentrale Norm der Criminal Compliance. *Zeitschrift für Internationale Strafrechtsdogmatik,* 2, 68–81.

Cram, W. Alec – D'Arcy, John – Proudfoot, Jeffrey (2018): Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance. *MIS Quarterly,* 43(2), 525–554. Online: https://doi.org/10.25300/MISQ/2019/15117

D'Arcy, John – Lowry, Paul Benjamin (2017): Cognitive-Affective Drivers of Employees' Daily Compliance with Information Security Policies: A Multilevel, Longitudinal Study. *Information Systems Journal,* 29(1), 43–69. Online: https://doi.org/10.1111/isj.12173

Delpont, Mattias et al. (2023): Monitoring Biosecurity in Poultry Production: An Overview of Databases Reporting Biosecurity Compliance From Seven European Countries. *Frontiers in Veterinary Science,* 10. Online: http://doi.org/10.3389/fvets.2023.1231377

Dunay, Pál (2000): Compliance Record a Decade After Treaty Signature. *S + F Sicherheit und Frieden,* 18(4), 327–333.

Dunay, Pál (2020): Arms Control Arrangements under the Aegis of the OSCE: Is There a Better Way to Handle Compliance? In Müller-Färber, Thomas – Weiss, Simon (szerk.): *In Times of Eroding Cooperative Security: How to Save Conventional Arms Control in Europe?* Loccum: Evangelische Akademie Loccum, 51–69.

Étienne, Julien (2010): La conformation des gouvernes. Une revue de la littérature théorique. *Revue française de science politique,* 60(3), 493–517. Online: https://doi.org/10.3917/rfsp.603.0493

Gösswein, Georg (2018): A vállalatok vezetői, mint az erőforrásokat kímélő compliance menedzsment rendszer meghatározó elemei. Ford.: Jacsó Judit. *AKV Európai Szemle,* 2(1), 85–87. Online: https://adreurope.uni-miskolc.hu/files/78/ADR-2018-1_G%C3%B6sswein.pdf

Kahneman, Daniel – Sibony, Olivier – Sunstein, Cass R. (2021): Noise. A Flaw in Human Judgment. *Statistical Review,* 69(1), 39–49. Online: https://doi.org/10.5604/01.3001.0015.8792

Li, Jennifer – Greenwood, David – Kassem, Mohamad (2019): Blockchain in the Built Environment and Construction Industry: A Systematic Review, Conceptual Models and Practical Use Cases. *Automation in Construction,* 102, 288–307. Online: https://doi.org/10.1016/j.autcon.2019.02.005

Mackey, Tim K. et al. (2019): 'Fit-for-Purpose?' – Challenges and Opportunities for Applications of Blockchain Technology in the Future of Healthcare. *BMC Medicine,* 17(68). Online: https://doi.org/10.1186/s12916-019-1296-7

Majumdar, Abhijit – Shaw, Mahesh – Sinha, Sanjib Kumar (2020): COVID-19 Debunks The Myth of Socially Sustainable Supply Chain: A Case of the Clothing Industry In South Asian Countries. *Sustainable Production and Consumption,* 24, 150–155. Online: https://doi.org/10.1016/j.spc.2020.07.001

Makhdoom, Imran et al. (2020): PrivySharing: A Blockchain-based Framework for Privacy-preserving and Secure Data Sharing in Smart Cities. *Computers & Security,* 88, 101653. Online: https://doi.org/10.1016/j.cose.2019.101653

Mustapha, A. M. et al. (2020): A Systematic Literature Review on Compliance Requirements Management of Business Processes. *International Journal of Systems Assurance Engineering and Management,* 11, 561–576. Online: https://doi.org/10.1007/s13198-020-00985-w

Nagy Andrea Magda – Tasner Dóra – Kovács Zoltán (2021): Ipar 4.0 a gazdaságtudományokban. A nemzetközi és hazai szakirodalom bibliometriai elemzése. *Vezetéstudomány,* 52(4), 63–79. Online: https://doi.org/10.14267/VEZTUD.2021.04.06

Rotsch, Thomas (2012): Compliance. In Achenbach, Hans – Ransiek, Andreas – Rönnau, Thomas: *Handbuch Wirtschaftsstrafrecht.* Heidelberg: C.F. Müller, 47.

Tandon, Anushree (2020): Blockchain in Healthcare: A Systematic Literature Review, Synthesizing Framework and Future Research Agenda. *Computers in Industry,* 122, 103290. Online: https://doi.org/10.1016/j.compind.2020.103290

Tilli, Giuditta et al. (2024): Supporting Measures to Improve Biosecurity within Italian Poultry Production. *Animals,* 14(12), 1734, 1–15. Online: https://doi.org/10.3390/ani14121734

HADMÉRNÖK
KIKÉPZÉS, FELKÉSZÍTÉS

20. évfolyam (2025) 2. szám 189–199.
DOI: 10.32567/hm.2025.2.11

Szabó Sándor[1]

Az átalakult NATO-kiképzési rendszer hatása a katonai gyakorlatok tervezésére

The Impact of the Transformed NATO Training System Regarding the Military Exercises Planning Process

Absztrakt

A NATO kiképzési rendszere az elmúlt években jelentősen átalakult, ami közvetlen hatást gyakorol a katonai gyakorlatok tervezésére és végrehajtására. Az innovatív kiképzési megközelítések a technológiai fejlődést, a hibrid hadviselés kihívásait és a többnemzeti együttműködés erősítését célozzák, így a gyakorlatok funkcionalitása fokozatosan igazodik a megváltozott biztonsági környezethez. A tanulmány elemzi a NATO kiképzési rendszerének főbb változásait, kiemelve az interoperabilitási képesség növelésének szükségességét, az adaptív kiképzési eljárások bevezetését. A kutatás rávilágít arra is, hogy ezek az újítások hogyan befolyásolják a NATO-tagállamok kollektív kiképzési eljárásrendjeinek harmonizációját, különös tekintettel a kollektív műveleti képességek kialakítására, a katonai gyakorlatok előkészítésére, valamint a törzsfelkészítések levezetésére.

Kulcsszavak: NATO, katonai kiképzés, gyakorlattervezés, törzsfelkészítés, művelettervezés, kollektív műveleti képesség

Abstract

NATO's training system has undergone a major transformation in the recent years, which has a direct impact on the planning and execution processes of military exercises. New,

[1] Adjunktus, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar, e-mail: szabo.sandor@uni-nke.hu

innovative training approaches are focusing on technological advances, the challenges of hybrid warfare and the strengthening of multinational cooperation, which is gradually adapting the functionality of exercises to the changed security environment. The study analyses the main changes in NATO's training system, highlighting the increase in interoperability and the introduction of adaptive training procedures. The research also highlights how these innovations affect the harmonisation of NATO member states' collective training procedures, in particular with regard to the development of collective operational capabilities, the preparation of military exercises and the conduct of training exercises.

Keywords: NATO, military training, exercise planning process, operational planning, collective operational capability

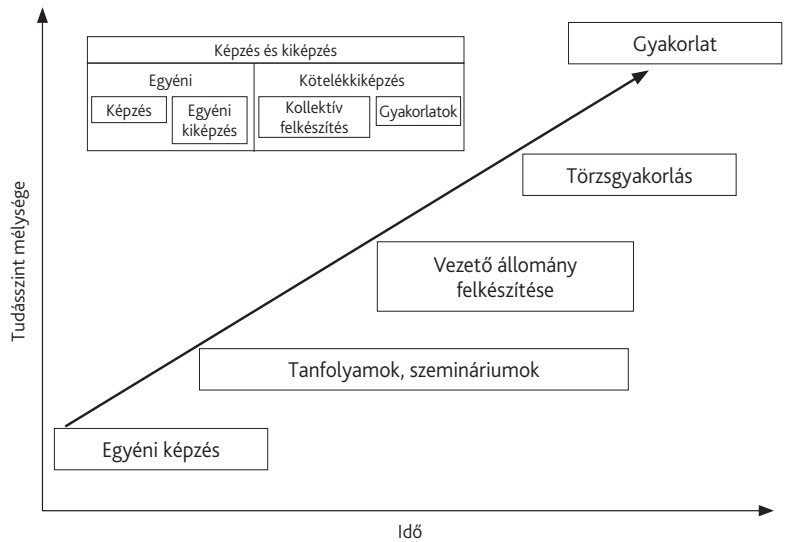
A NATO kiképzési rendszere

A NATO 1951-ben vezette le első katonai gyakorlatát, amelynek kiemelt célja volt a centralizált parancsnoki rendszer alatt álló, egységes NATO katonai haderő kialakítása. Ezt követően a NATO több ezer gyakorlatot hajtott végre, jellemzően a hidegháború idején. A kiemelt kiképzési rendezvények közé tartozott a REFORGER *(Return of Forces to Germany)* gyakorlatsorozat, amely az Egyesült Államok haderejének gyors európai telepítését tesztelte. A NATO gyorsreagálású műveleti képesség kialakítása érdekében a Szövetséges Parancsnokság Európai Mozgó Erők (*Allied Command Europe Mobile Force,* AMF) készenléti katonai köteléket állított fel, amely 1960-as évektől kezdve a hidegháború idején döntő szerepet játszott az elrettentés és a védelem terén. Az 1990-es években, reflektálva a változó európai biztonsági környezetre, a NATO kiterjesztette feladatrendszerét a válságreagálásra is. 2002-ben az AMF-et NATO Reagáló Erővé (*NATO Response Force,* NRF) alakították át, majd ezt a koncepciót felváltva 2024-től Egyesített Reagáló Erőként (*Allied Response Force,* ARF) működik a NATO készenléti hadereje, amely jelenleg is szerves részét képezi a NATO stratégiai koncepciónak, biztosítva a katonai gyakorlatok révén a NATO készenléti és adaptációs képességét.[2] A nemzetközi katonai gyakorlatok fontos szerepet töltenek be a fegyveres erők műveleti eljárásrendjének egységesítésére, az interoperabilitási képesség kialakítására, valamint a katonai műveletek végrehajtására irányuló felkészítésben. Elsődleges céljuk mellett a gyakorlatok célzott politikai jelzéseket is küldhetnek a nemzetközi közönségnek. Az adoptált szcenárió, a kiképzési tevékenység földrajzi elhelyezkedése és a részt vevő katonai kötelék mértéke az elrettentési stratégia eszközévé teszi a katonai gyakorlatot.[3]

Alapfilozófiájából adódóan a NATO elsődlegesen az országok közötti konfliktusok békés rendezése mellett érvel, amennyiben viszont a diplomáciai erőfeszítések nem vezetnek eredményre, rendelkezik olyan mértékű katonai erővel, amely alkalmassá teszi válságkezelési műveletek végrehajtására. Az ilyen jellegű fegyveres konfliktusokat a NATO alapszerződésének kollektív védelemről szóló pontja, a washingtoni szerződés 5. cikke szellemében egyedül vagy más országokkal és nemzetközi szervezetekkel

[2] Tarçın 2024.
[3] Kubai 2022: 155.

együttműködésben is felvállalhatja.[4] Ahhoz, hogy ilyen, akár globális léptékű fegyveres konfliktusok megvívására a NATO fel tudjon készülni, képesnek kell lennie robusztus kollektív műveleti képesség kialakítására, illetve fenntartására. Ebben a folyamatban játszik kiemelt szerepet a katonai kiképzés, mivel ezeket a kollektív katonai képességeket a személyi állomány oktatási, tanfolyami képzésen keresztül történő felkészülése, a katonai kötelékek törzsgyakorláson, gyakorlaton történő összekovácsolása révén tudja kialakítani, amelynek a folyamatát az 1. ábra illusztrálja.



1. ábra: A kiképzési rendszer főbb állomásai
Forrás: a szerző szerkesztése

A NATO-gyakorlatok kiemelt célja, hogy egy olyan komplex, szimulált műveleti környezetet biztosítson, ahol a katonai alegység, egység szintű szervezetek, akár terepen, akár virtuális térben mind az egyéni készségeket, mind a kollektív képességeket tudják fejleszteni, adott esetben NATO készenléti szolgálatra történő felkészülés jegyében mérni. Emellett a gyakorlatok elősegítik a nemzetek közötti interoperabilitás kialakítását, a közös reagálóképesség fenntartását, a stratégiai kommunikáció révén az erődemonstrációt, valamint a NATO-haderőn belüli eljárásrendek egységesítését.[5] A nemzetközi gyakorlatok fontosak a Magyar Honvédség és az alárendelt katonai szervezetek felkészítési és kiképzési rendezvényei kapcsán, mivel többek között a befogadó nemzeti támogatással kapcsolatos tevékenységek ellátása mellett lehetőséget biztosítanak a többnemzeti környezetben végrehajtott magas intenzitású műveletekkel

[4] NATO 2023.
[5] Szabó 2022: 82.

kapcsolatos katonai képességek fejlesztésére.[6] Az egységesítési törekvés a NATO kiképzési rendszere doktrinális hátterének kialakítására és fenntartására irányuló szándék kapcsán is megfigyelhető, mivel az egyéni felkészítések, a kollektív kiképzési események, gyakorlatok tervezését, előkészítését és végrehajtását a Katonai Tanács (*Military Committee,* MC) és a Stratégiai Parancsnokságok (*Strategic Commands,* SC) közös irányelvei szabályozzák. A haderők a harc megvívására történő felkészítés érdekében doktrinális kiadványok mentén elfogadott és egységesített szabványok szerinti előírások alapján működtetik a kiképzési rendszereiket. A szabályzatok egyszerre biztosítják az alapot egy adott műveleti képesség elérését szolgáló jártasság kialakítására, illetve tükrözik a műveleti környezet komplexitását, beleértve a konvencionális és a hibrid fenyegetéseket is.[7]

Az orosz–ukrán fegyveres konfliktus széles körű geopolitikai hatása katalizátorként befolyásolta a NATO-kiképzés szabályozási rendszerének átalakítását, amelynek eredményeként 2023-ban a NATO Katonai Tanács ratifikálta és kiadta az *MC 458/2 NATO Exercise & Training* irányelvet. Az MC 458/2 a NATO kiképzési rendszerének szakmai alapdoktrínája, amely stratégiai szintű szakpolitikai irányelveket határoz meg a NATO valamennyi egyéni és kollektív kiképzési eljárásrenddel összefüggő tevékenysége kapcsán. A szabályozási hierarchia alacsonyabb szintjét a *Bi-SC 75-2 2 Education and Training Directive* irányelv képviseli, amely leírja mindazokat a kiképzési programokat, illetve eljárásrendeket, amelyeket a két stratégiai parancsnokság a műveleti és transzformációs célok elérésének támogatása érdekében alkalmaz. Az irányelv meghatározza az alárendelt parancsnokok és katonai szervezetek számára azokat az alapvető oktatási és kiképzési stratégiai irányokat, amelyek a NATO egyéni és kollektív kiképzési rendszereinek működtetéséhez nélkülözhetetlenek. A *Bi-SC 75-7 Education and Individual Training Directive* a NATO-feladatrendszerhez kapcsolódó egyéni felkészülési területeket átfogó dokumentum, magában foglalja mindazon iránymutatást, amelyet a NATO struktúrájába tartozó szervezeteknek és tagországoknak implementálniuk kell annak érdekében, hogy kiképzési programjaik és felkészítési rendszereik szinkronizálva legyenek egymással. A *Bi-SC 80-6 Lessons Learned Directive* a tapasztalatfeldolgozás rendszerét meghatározó irányelv, amely a tapasztalatok gyűjtésére, feldolgozására irányul. A *Bi-SC 80-90 NATO Task List* olyan feladatspecifikus normagyűjtemény, amely összefoglalja a NATO-parancsnokságok és katonai szervezetek számára, hogy milyen kollektív képességcsomagokkal kell rendelkezniük, amelyek a műveleti alkalmazásuk szempontjából nélkülözhetetlenek. A feladatlista egységes terminológiát és referenciarendszert biztosít a kiképzés- és a gyakorlattervezők számára a kiképzési célkitűzések kialakítása érdekében. A *Bi-SC 75-4 Experimentation Directive* kísérletek lefolytatására irányuló direktíva, amely iránymutatást ad a gyakorlatok levezetése kapcsán különböző műveleti képességbeli összetevőkkel, technikai eszközökkel történő modellezés vagy kísérletezés végrehajtásához. Végezetül a törzsvezetési gyakorlatok előkészítése és levezetése szempontjából a legfontosabb szabályzó a *Bi-SC 75-03 Collective Training and Exercise Directive,* amely négy tervezési fázisban határozza meg a gyakorlatok előkészítésére, levezetésére és

[6] Hattyár 2022: 54.
[7] Department of the US Army 2021: 1–2.

értékelésére irányuló eljárásrendeket. Az aktuális hadműveleti igényekhez igazodva a NATO Szövetséges Erők európai főparancsnoka (*Supreme Allied Commander Europe,* SACEUR) évi rendszerességgel iránymutatását ad ki az oktatás, kiképzés, gyakorlatok és értékelés tekintetében *(SACEUR'S Annual Guidance for Education, Training, Exercises and Evaluation).* Ez a dokumentum tartalmazza a SACEUR által megfogalmazott stratégiai műveleti irányokat és prioritásokat, az oktatás, kiképzés, gyakorlatok és értékelések általános irányelveit, a kiképzési környezet, a feltételendszer megteremtése érdekében az erőforrások allokációjának szabályrendszerét és a kapcsolódó tervezési kereteket.[8]

A NATO gyakorlattervezési koncepciója

A NATO szervezeti elemek és a tagországok közötti gyakorlattervezési eljárásrend egy egységes módszertant követ, megteremtve ezáltal az interoperabilitást a NATO-műveletekre történő felkészülés jegyében. Az eljárásrend alapjául a *NATO BI-SC Collective Training and Exercise Directive (CT&ED) 075-003* gyakorlattervezési útmutató szolgál, amely a NATO-ban zajló kiképzési területet érintő reformtörekvések eredményeképpen, 2023 szeptemberében a NATO ACO (Allied Command Operations) gondozásában jelent meg.

Az átalakított NATO gyakorlattervezési eljárásrend szakaszai

A standardizált NATO gyakorlattervezési folyamat legfőbb célja, hogy harmonizált eljárásrendi keretet biztosítva szinkronizálja a gyakorlattervezés főbb állomásait, és pontosan determinálja a részfolyamatokhoz kötötten az elérendő koordinációs eredményeket és produktumokat. A gyakorlattervezési és levezetési folyamat az alábbi négy fő tervezési szakaszon keresztül valósul meg:

- 0. szakasz: a gyakorlat tervezésére és levezetésére irányuló kezdeményezés *(Initiation);*
- 1. szakasz: a gyakorlat alapkoncepciójának és a gyakorlattervezési alapadatoknak a kidolgozása *(Specification);*
- 2. szakasz: a gyakorlat tervezése *(Planning);*
- 3. szakasz: a gyakorlat levezetése *(Conduct).*[9]

Az átalakított jogkörök és hatáskörök a gyakorlatok tervezése és levezetése során

A gyakorlat tervezésének és levezetésének fontos kritériuma, hogy a tervezési eljárásrend felelősségi és jogkörökhöz kötötten valósuljon meg. A kapcsolódó koordinációs feladatok ellátása érdekében, az átalakult NATO kiképzési koncepció szellemében

[8] NATO 2013: 1–7.
[9] NATO 2023: 5.

megújult gyakorlattervezői funkcionális struktúrát hoznak létre, amelynek alapjául az alábbi kulcsbeosztások hatás- és jogkörei szolgálnak:

- A *gyakorlatot elrendelő parancsnok* (*the officer scheduling the exercise,* OSE) meghatározza a kiképzési követelményeket és jóváhagyja a gyakorlattervezési koncepciót, valamint a gyakorlattervezői események levezetésének rendjét. Irányítja a 0. és 1., felügyeli a 2. és 3. tervezési szakaszokat, és allokálja a gyakorlat végrehajtásához szükséges erőforrásokat. A számára felterjesztett értékelő jelentés alapján validálja a gyakorlaton elért eredményeket.
- A *gyakorlatot levezető parancsnok* (*the officer conducting the exercise,* OCE), támogatja a gyakorlatot elrendelő parancsnok munkáját a 0. és 1. tervezési szakaszokban. Közvetlenül felel a 2. és 3. tervezési szakaszok irányításáért, a kapcsolódó tervezési események és konferenciák levezetéséért. Koordinálja a kiképzési célok kidolgozásának menetét, a gyakorlat mindenoldalú biztosítása és előkészítése érdekében kiadja a gyakorlattervet (EXPLAN). Levezeti a gyakorlatot és a kapcsolódó felkészítő, kiképzési rendezvényeket, tevékenységét a gyakorlat végrehajtási fázisában a gyakorlatigazgató támogatja, valamint aktívan részt vesz a gyakorlat értékelési mechanizmusában.
- A *gyakorlatrendezésért felelős parancsnok* (*officer directing the exercise,* ODE) támogatja a gyakorlatot levezető parancsnokot a gyakorlat részletes megtervezésében és levezetésében, elsődlegesen felel a gyakorlat céljai és a kiképzési célkitűzések kapcsán lefektetett feltételrendszer kialakításáért.
- A *gyakorlatért közvetlenül felelős tiszt* (*officer with primary responsibility,* OPR) saját parancsnoksága, katonai szervezete által koordinálja a gyakorlattervezés és a végrehajtás teljes folyamatát, elsődlegesen felel a gyakorlat előkészítése, levezetése és értékelése koordinációs feladatainak ellátásáért. Felhatalmazás alapján képviseli a katonai szervezet parancsnokának döntését.
- A *gyakorlatigazgató* (*exercise director,* EXDIR) személyét a gyakorlatot levezető parancsnok javaslatára a gyakorlatot elrendelő parancsnok hagyja jóvá. A gyakorlat levezetési időszakában felel a gyakorlat céljainak és a kiképzési célkitűzéseknek a teljesüléséért, vezeti a *gyakorlatvezetőség* (*exercise control,* EXCON) feladatellátását.
- *Értékelő csoportparancsnok* (*director of evaluation,* DIREVAL) a gyakorlat végrehajtási időszakában a gyakorlatot elrendelő parancsnok közvetlen irányítása alatt vezeti az értékelő csoportot. A gyakorlat levezetése alatt teljesen független hatás- és jogkörökkel rendelkezik, de az értékelési követelmények teljesülése érdekében a gyakorlatigazgatóval koordinációs tevékenységet folytat.[10]

[10] NATO 2023: 10.

Az átalakított NATO gyakorlattervezési eljárásrend részletes bemutatása

0. szakasz: a gyakorlat tervezésére és levezetésére irányuló kezdeményezés (Initiation)

A 0. szakasz a gyakorlatfejlesztés előkészítő fázisa. Megerősíti a fő felelősségi köröket, és meghatározza a műveleti ambíció és a rendelkezésre álló erőforrások szintjét. A 0. szakaszt a gyakorlatot elrendelő parancsnok vezeti, aki az alárendeltségébe tartozó katonai szervezeten belül, az alapvető koordinációs feladatok ellátása érdekében Gyakorlatkoordinációs Csoportot *(Exercise Board),* a részletes tervezési feladatok ellátása érdekében Gyakorlattervező Csoportot *(Exercise Group),* valamint a katonai szervezet specifikus előkészítő feladatainak ellátásáért Gyakorlattámogató Csoportot *(Exercise Team)* állít fel. A 0. szakasz végén kiadják a gyakorlat kiinduló koncepcióját (*Exercise Initiation,* a továbbiakban: EXINT), amely tartalmazza az elöljárói szándékot, a gyakorlattal szemben támasztott követelményeket, a gyakorlat általános paramétereit és a főbb tervezési mérföldköveket, valamint a gyakorlat céljainak tervezetét.

A tervezési szakaszra jellemző főbb feladatok:

- a gyakorlat tervezését és levezetését kezdeményező konferencia *(Exercise Initiation Conference)* összehívása, a gyakorlat alapkoncepciójának kialakítása;
- parancsnoki validációs értekezlet előkészítése és levezetése. A gyakorlat tervezésében és levezetésében érdekelt parancsnoki állomány közötti egyetértés kialakítása a gyakorlat alapkoncepciója kapcsán, a prioritások felállítása, illetve a gyakorlatot elrendelő parancsnok iránymutatását tartalmazó dokumentumok kiadása.

1. szakasz: a gyakorlat alapkoncepciójának és a gyakorlattervezési alapadatoknak a kidolgozása (Specification)

Az 1. szakasz kiemelt célja véglegesíteni a gyakorlat célkitűzéseit (*Exercise Objectives,* EO), megteremteni egy megvalósítható gyakorlattervezési feladatrendszer alapjait. Az 1. szakasz kapcsán elvárt eredmény a gyakorlattervezési alapadatok (*Exercise Specification,* EXSPEC) kidolgozása és kiadása, amely dokumentum tartalmazza a gyakorlat időrendjére, helyszínére, a részt vevő állomány összetételére, finanszírozásra, a logisztikai, híradó-, informatikai támogatásra, jogi szabályozásra, az alkalmazandó szcenárióra irányuló útmutatást. Az 1. szakaszt a gyakorlatot elrendelő parancsnok vezeti a Gyakorlatkoordinációs Csoport, a Gyakorlattervező Csoport, valamint a Gyakorlattámogató Csoport támogatása mellett. A gyakorlattervet a gyakorlatot elrendelő parancsnoknak 12–18 hónappal a gyakorlat végrehajtási szakasza (3. szakasz) előtt jóvá kell hagynia annak érdekében, hogy az abban megfogalmazott gyakorlattervezési keretrendszer és az erőforrás-allokáció meg tudjon valósulni.

A tervezési szakaszra jellemző főbb feladatok:

- a tervező és a koordinációs munkacsoport üléseinek levezetése;

- kidolgozni a gyakorlattervezési alapadatait tartalmazó dokumentumot;
- a gyakorlat tervezett végrehajtási helyszínén szemrevételezés lefolytatása;
- levezetni a gyakorlattervezési alapadatokkal kapcsolatos koordinációs konferenciát (*Exercise Specification Conference);*
- parancsnoki validációs értekezlet előkészítése és levezetése, amelynek keretében a gyakorlat tervezési alapadatait tartalmazó dokumentumot elfogadják;
- a gyakorlat tervezési alapadatait tartalmazó dokumentum kiadása.

2. szakasz: a gyakorlat tervezése (Planning)

A 2. szakasz legfőbb feladata a gyakorlat részletes tervezésének és előkészítésének végrehajtása. A gyakorlattervezési alapadatok kiadása után a gyakorlatot levezető parancsnokhoz delegálnak minden hatás- és jogkört a gyakorlattervezés, a 2. szakasz irányítása és vezetése kapcsán. Ebben a tervezési szakaszban a gyakorlatot levezető parancsnok alárendeltségébe kerül a Gyakorlatkoordinációs Csoport és a Gyakorlattervező Csoport, ezeken keresztül történik a tervezési konferenciák, a koordinációs munkacsoport üléseinek, valamint a gyakorlattervnek (EXPLAN) az összeállítása, amely mint összefoglaló fő dokumentum a gyakorlat előkészítésének összes funkcionális területére kiterjedő központi információbázist jelent.

A tervezési szakaszra jellemző főbb feladatok:

- A kiképzési célkitűzések kialakítása, amelyeket a gyakorlóállomány parancsnoka a törzsével, a katonai szervezet kollektív műveleti képességének kialakítása, fenntartása érdekében dolgoz ki és terjeszt fel jóváhagyásra a gyakorlatot levezető parancsnok részére. A kiképzési célkitűzések kialakítása elsődleges prioritást élvez a gyakorlat tervezési folyamatai között, amelyek pontos meghatározása érdekében egy precízen leírt eljárásrend követése valósul meg. A kiképzési célkitűzések kialakítása kapcsán a jövőben egyszerre kell vizsgálni a gyakorlóállomány *(Training Audience)* körét, az alapvető és támogató feladatrendszert (*Essential Task,* illetve *Supporting Tasks*), a fennálló körülményeket, feltételrendszert *(Conditions – Time, Space, Forces, Information)* és a szabályzói hátteret *(Standards).* A kiképzési célkitűzés pontos meghatározása érdekében egy koordinációs mátrixot alakítanak ki, amelyben az alapvető feladatot *(Essential Task)* a *NATO Task List* (BI-SC 80-90) alapján rögzítik mint elérendő kiképzési célt. A támogató feladatrendszer meghatározása során az alapvető feladat részletes bontása történik meg, valamint azonosítják a kapcsolódó műveleti alfeladatokat. A feltételrendszer kidolgozása során tisztázzák, milyen gyakorlattámogatói igények merülnek fel (például alájátszó állomány, szcenário, Main Events List / Main Incidents List, MEL/MIL vonatkozásában) a célkitűzés sikeres teljesítéséhez. A szabályzó háttér bemutatása révén egyértelművé válik a műveleti képesség doktrinális oldala, amely a célkitűzés megvalósításán keresztül értékelhető lesz. A kiképzési célkitűzést leíró mátrix alkalmazásával

egyszerűbbé és összehangoltabbá válik a szcenárió és a MEL/MIL kidolgozása, valamint az ellenőrzési és értékelési szempontok kialakítása.[11]

- Gyakorlatot levezető parancsnok gyakorlattervezési útmutatójának kiadása, amely tartalmazza a parancsnoki iránymutatást a részletes tervezési feladatok ellátása érdekében. A tervezési útmutató meghatározza a felelősségi és hatásköröket, az elérendő kiképzési célokat, a szcenárió kidolgozásának keretrendszerét, a pénzügyi erőforrás korlátait, a főbb tervezési időpontokat, a gyakorlatlevezetési terv kidolgozásának ütemtervét.
- Szcenáriómodulok kidolgozása, ami tartalmazza a geostratégiai és hadszíntéri ismereteket, a stratégiai bevezetést, a válságreagáló tervezési, az erők aktiválására és az áttelepülésre vonatkozó, valamint a végrehajtásra irányuló alapvető (STARTEX) információkat.
- Fő események, fő incidensek listájának (*Main Events List / Main Incidents List,* MEL/MIL) összeállítása.
- A Gyakorlattervező Csoport munkaértekezleteinek levezetése, amelyek fő célja a soron következő tervezői konferenciák előkészítése, valamint a gyakorlatterv kidolgozói folyamatainak koordinációja.
- A gyakorlat tervezett végrehajtási helyszínén szemrevételezés lefolytatása.
- Az indító, illetve fő tervezői, valamint záró koordinációs konferenciák levezetése.
- A technikai koordinációs konferencia levezetése.
- Gyakorlatterv kidolgozása, amely a részletes tervezést összefoglaló alapmű, tartalmazza a gyakorlat tervezésének és levezetésének részletes időrendjét, a szcenáriómodulokat, a szimulációs támogatást, a valós logisztikai támogatást, a vezetés rendjét, a kommunikációs eljárásrendet, a gyakorlatvezetés rendszerét, a gyakorlat elemzését, értékelését, a jelentések elkészítésének és felterjesztésének hátterét.
- Parancsnoki validációs értekezlet előkészítése és levezetése, amelynek keretében elfogadják a gyakorlattervet. A tervezési szakaszt a gyakorlatterv kiadása zárja.

3. szakasz: a gyakorlat levezetése (Conduct)

A 3. szakasz a gyakorlatnak a gyakorlattervben rögzített keretek közötti levezetésére irányul, a gyakorlat végrehajtása az egyéni és kollektív felkészítés biztosítása érdekében térben és időben elkülönülő kiképzési események útján valósul meg. A szakaszt a gyakorlatot levezető parancsnok vezeti, munkáját a gyakorlattámogató parancsnok segíti. A gyakorlat közvetlen irányítása a gyakorlatigazgatón keresztül valósul meg, parancsnoki elöljárói szerepkört tölt be a gyakorlatvezetőségen belül. A gyakorlatvezetőség kiemelt feladatai közé tartozik a gyakorlat valós biztosítási feladatainak koordinálása, a gyakorlóállománnyal történő interakciók lefolytatása alájátszói állomány (*response cells,* HICON, LOCON, GREY CELL) bevonása mellett, a MEL-/MIL-incidens bejátszásának koordinálása, a tapasztalatfeldolgozó rendszer működtetése. Az értékelő csoportparancsnok szervezi és vezeti az értékelési és elemzési feladatok ellátását.

[11] Szabó 2021: 90.

A tervezési szakaszra jellemző főbb feladatok:

- A blokk: alapozó felkészítés *(Academics),* amelynek keretében egyéni és kollektív felkészítések *(Internal Invidual and Collective Training),* keresztfunkcionális tréningek *(Cross-Functional Area Training)* történnek, valamint kulcsbeosztású vezetői állományt felkészítő foglalkozások zajlanak *(Key Leader Training);*
- B blokk: törzsfelkészítés *(Battle Staff Training);*
- C blokk: műveletтervezés (*Crisis Response Planning,* CRP);
- D blokk: átcsoportosítás *(Deployment);*
- E blokk: a gyakorlat végrehajtása *(Employment);*
- F blokk: a gyakorlatot követő értékelés *(Follow-on Training).*[12]

Összefoglalás

Az összhaderőnemi szintű kiképzés a NATO-n belül túlmutat az egyes tagállamok katonai képességbeli összetevőin. Ez magában foglalja azt a tágabb szövetségesi célt, hogy egy hatékony integráció és szinergia mentén, a különböző haderőnemek aktív együttműködésén keresztül a szövetség hatékonyan reagálhasson a biztonsági fenyegetések teljes spektrumára. A NATO a közös kiképzési doktrína megújításán keresztül, a parancsnoki struktúrák és a műveleti eljárások közös megértésének előmozdításával olyan egységes keret létrehozására törekszik, amely túllép a nemzeti határokon, megteremtve ezzel a szinkronizált és interoperabilitásra épülő katonai műveletek alapjait.[13]

A NATO gyakorlattervezésének és levezetésének folyamata egy többlépcsős, összetett eljárásrendet követ, amely a változó biztonsági környezet által indukált kihívásokra tekintettel elengedhetetlen a szövetség kohéziójának fenntartása érdekében. A tervezési eljárásrendet jellemző részletes koordináció, az innovatív kiképzési megoldások és a műveletikörnyezet-orientált szcenárióknak köszönhetően a tagállamok képesek hitelesen demonstrálni az elrettentés és a gyorsreagálási képesség iránti közös elkötelezettségüket. A 2023-ban megújult *BI-SC 075-003 Collective Training and Exercise Directive* gyakorlattervezési útmutató is annak a NATO-törekvésnek a szellemében született, amely elkötelezett a kollektív készenlétfokozási és alkalmazkodóképesség folyamatos fejlesztése, kialakítása irányába. Az együttműködés előmozdításával, a technológiai innovatív folyamatok támogatásával és a többnemzeti, nagy láthatóságú gyakorlatokon szerzett tapasztalatok beépítésével a szövetség biztosítja, hogy képes legyen hatékonyan megvédeni a tagállamok biztonsági érdekeit és elősegíteni a stabilitást egy kiszámíthatatlan geopolitikai környezetben. A jövőben a kiképzési rendszerek fejlesztésére, a gyakorlatok megrendezésére szánt magasabb pénzügyi erőforrások kulcsfontosságúvá válnak annak érdekében, hogy a NATO megőrizze stratégiai előnyét, és egységesen szálljon szembe a felmerülő globális biztonsági fenyegetésekkel.

[12] NATO 2023: F-1.
[13] Pînzariu–Neag–Pînzariu 2024: 112.

Felhasznált irodalom

Department of the US Army (2021): *FM 7-0 Training*. Washington, DC: Headquarters, Department of the US Army. Online: https://armypubs.army.mil/epubs/DR_pubs/DR_a/ARN35076-FM_7-0-000-WEB-1.pdf

Hattyár István (2022): A Defender-Europe 21 gyakorlat és a kapcsolt nemzeti kiképzési rendezvények tapasztalatai a koronavírussal terhelt időszakból. *Hadmérnök,* 17(2), 53–69. Online: https://doi.org/10.32567/hm.2022.2.4

Kubai, Danylo (2022): Military Exercises as a Part of NATO Deterrence Strategy. *Comparative Strategy,* 41(2), 155–161. Online: https://doi.org/10.1080/01495933.2022.2039009

NATO (2013): *NATO BI-SC 075-003 Collective Training and Exercise Directive, Supreme Allied Commander.* Online: https://www.coemed.org/files/Branches/DH/Files_01/bi-sc-75-3_final.pdf

NATO (2023): *Collective Defence and Article 5*. Online: https://www.nato.int/en/what-we-do/introduction-to-nato/collective-defence-and-article-5

Pînzariu, Sorin Gheorghe – Neag, Mihai Marcel – Pînzariu, Andra Ioana (2024): Enhancing Joint Training and Education in NATO (2024): A Comprehensive Framework for Interoperability and Operational Effectiveness. *Scientific Bulletin,* 29(1), 111–117. Online: https://doi.org/10.2478/bsaft-2024-0012

Szabó Sándor (2021): A kiképzési célok helye és szerepe a gyakorlatok tervezésekor és levezetésekor. *Honvédségi Szemle,* 149(2), 85–92. Online: https://doi.org/10.35926/HSZ.2021.2.7

Szabó Sándor (2022): A gyakorlattervezés szerepe a NATO-reagálóműveletekre való felkészülés tükrében. *Hadmérnök,* 17(2), 71–83. Online: https://doi.org/10.32567/hm.2022.2.5

Tarçın, Uğur (2024): NATO Exercises: The guarantee of Alliance Security and Test of Readiness. *Defense Journal by Atlantic Council in Turkey.* Online: https://www.atlanticcouncil.org/category/content-series/ac-turkey-defense-journal/

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG
20. évfolyam (2025) 2. szám 201–214.
DOI: 10.32567/hm.2025.2.12

Kátai-Urbán Maxim,[1] Cséplő Zoltán,[2] Cimer Zsolt[3]

A logisztikai raktárakban előforduló, veszélyes anyagokkal kapcsolatos baleseti eseménysorok és azok lehetséges következményeinek vizsgálata

Analysis of Accident Scenarios Involving Hazardous Materials in Logistics Warehouses and Their Potential Consequences

Absztrakt

Az elmúlt évek kihívásai rávilágítottak a „just in time" működési rend kockázataira, a raktározás növekvő jelentőségére. Ennek következtében a logisztikai központok iránti piaci kereslet dinamikusan bővül. A logisztikai központokban veszélyes anyagok raktározására is sor kerülhet, ezért számos esetben veszélyes üzemeknek minősülnek a létesítmények az iparbiztonsági szabályozás alapján. A logisztikai központok általi veszélyeztetés értékelése az egyedi jelleg miatt sajátos módszertant igényel. A szerzők jelen cikkben a nemzetközi és hazai szakirodalom mellett saját tapasztalataikra is támaszkodva tekintik át a legfontosabb összefüggéseket.

Kulcsszavak: *ipari balesetek, környezeti károk, veszélyes anyag, oltóvízszennyezés megelőzése, Magyarország*

[1] Osztályvezető, Semmelweis Egyetem Biztonságtechnikai Igazgatóság Biztonságszervezési Osztály, e-mail: katai.urban.maxim@semmelweis.hu
[2] Iparbiztonsági főfelügyelő, Fővárosi Katasztrófavédelmi Igazgatóság, e-mail: zoltan.cseplo@katved.gov.hu
[3] Dékán, Nemzeti Közszolgálati Egyetem Víztudományi Kar, e-mail: cimer.zsolt@uni-nke.hu

Abstract

The challenges of recent years have highlighted the risks of the 'just-in-time' operating model and the increasing importance of warehousing. As a result, market demand for logistics centers is expanding dynamically. In logistics centers, hazardous materials may also be stored, which is why, in many cases, these facilities are classified as hazardous establishments under industrial safety regulations. Due to their unique characteristics, the assessment of risks associated with logistics centers requires the application of a specialised methodology. In this article, the authors provide an overview of the key aspects based on both international and domestic literature, as well as their own experience.

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

Bevezetés

Az elmúlt években a logisztikai központok iránti kereslet tovább növekedett, amit a globális ellátási láncok változásai és a raktározás egyre nagyobb jelentősége is indokol. A logisztikai központok általános jellemzője, hogy különböző termékek nagy mennyiségben, koncentráltan vannak jelen. A készletszintek mellett sok esetben a raktározott termékek típusa is folyamatosan változik, ezért nehéz pontosan meghatározni, hogy a logisztikai központban tárolt vagy tárolható veszélyes anyagok mennyisége eléri-e a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről szóló 219/2011. (X. 20.) Korm. rendelet 1. mellékletében nevesített küszöbértékeket. Mindezek ellenére számos logisztikai központ veszélyes üzemként van nyilvántartva.

A veszélyes tevékenységek biztonságos működését ipari baleset-megelőzési oldalról nézve kockázat- és következményelemzési eljárások, módszerek, szoftverek segítik elő. Számos folyamatbiztonsági, veszteségmegelőzési és rendszerbiztonsági mérnöki tudományos munka foglalkozik e folyamatok mennyiségi kockázatalapú értékelési megközelítéseivel. Az 1990-es évek végén és a 2000-es évek elején jelentős előrelépés volt tapasztalható a kockázatelemzési technológiák ipari tevékenységekben történő felhasználásának szabványosítása és harmonizálása terén.[4] A kiváló elméleti biztonságirányítási eszközök alkalmazása széles körben elterjedt a biztonsági akadálydiagramok, mint például a csokornyakkendő-ábra[5] alkalmazásával, amely többek között a megelőző és következménycsökkentő intézkedések megfelelő alkalmazására szolgáltat műszaki alapot.

Általánosságban elmondható, hogy a helyi biztonsági rendszer működő- és ellenálló képessége megelőzési, felkészültségi és elhárítási intézkedések bevezetésével biztosítható. Ezen intézkedések alkalmazása a súlyos baleseti események – például

[4] Tixier et al. 2002.
[5] Duijm 2009.

robbanások, tűz, mérgező anyagok terjedése – főbb hatásainak és következményeinek csökkentését vagy megszüntetését célozza.[6]

A következmény- és kockázatelemzési eljárások alkalmazása szempontjából a veszélyes áru tárolása és raktározása számos sajátossággal bír. A veszélyes anyag gyártása és tárolása során bekövetkező események a környezetre és az egészségre káros anyagok kibocsátásával kezdődnek, ennek a következménye lehet a tűz vagy a robbanás.[7] A felszíni és felszín alatti vizek közvetlen szennyezésével járó környezeti károk megelőzése az ipari tevékenységek vonatkozásában elsősorban környezetbiztonsági kérdés.[8] További biztonságszervezési feladatot jelent a kémiai ártalmakkal kapcsolatos üzemeltetői munkavédelmi kötelezettségek előírása is.[9]

A környezeti katasztrófahelyzetek felszámolása a védekezés valamennyi időszakában a vezetés és az irányítás szoros összehangolását, az üzemeltetők hatóságokkal történő együttműködését, továbbá komplex infokommunikációs rendszer létrehozását és működtetését igényli.[10] Ugyanez vonatkozik természetesen a baleseti kockázatok kezelésének és elhárításának időszakára is, ahol a társhatóságok és a rendvédelmi szervek közötti együttműködés növeli az ipari biztonságot.[11]

A logisztikai központok általi veszélyeztetés értékelése a tevékenység sajátosságai miatt egyedi módszertant igényel. A módszertan – következmény- és kockázatelemzés – legfontosabb követelménye, hogy reális eseménysorokra épüljön, ellenkező esetben a veszélyeztetés mértéke alul- vagy túlbecsülhető, ami akár jelentős gazdasági károkat is okozhat. A következő fejezetekben tapasztalataink alapján bemutatjuk a logisztikai központok tevékenységéből adódó sajátosságot, amely a veszélyeztetés értékelésére hatással lehet. A hazai és a nemzetközi releváns szakirodalom alapján összefoglaljuk a veszélyeztetés értékelése során vizsgálandó baleseti eseménysorokat, a vizsgálati szempontokat pedig saját tapasztalatainkkal egészítjük ki.

A logisztikai központok működésének sajátos jellemzői

A logisztikai központok általános jellemzője, hogy a tárolt termékek típusa és mennyisége folyamatosan változik. A logisztikai központok esetében az üzemazonosítás rendkívül bonyolult és összetett folyamat.

Számos végfelhasználói fogyasztói termék – például kozmetikai termékek, gyógyszerek, élelmiszerek és élelmiszer-adalékanyagok, valamint háztartási tisztítószerek (ha a címkézés megfelel a vonatkozó szabályozásnak) – esetében a gyártónak nem szükséges biztonsági adatlapot kiállítania. Ennek következtében a logisztikai központokban ezen termékek veszélyeiről nem feltétlenül áll rendelkezésre releváns információ, ezért egzakt módon nem ítélhető meg, hogy a termék a 219/2011. (X. 20.) Korm. rendelet 1. melléklete szerint veszélyes anyagnak minősül-e.

6 Carter et al. 2003.
7 Kátai-Urbán et al. 2024.
8 Földi–Padányi 2021.
9 Nagy 2023.
10 Farkas 2016.
11 Bakai 2022.

A folyamat végrehajtását tovább nehezíti, hogy számos esetben vegyes termékek tárolására kerül sor, ami az jelenti, hogy az egységcsomagolás a veszélyes anyagon túl egyéb terméket is tartalmaz. Tipikus példa erre a kiskereskedelemben megjelenő „akciós" kínálat vagy a karácsony előtti kozmetikai vegyes csomagolások, amelyekben a veszélyes anyagnak minősülő dezodor mellett egyéb nem veszélyes termékek – krémek, testápolók – is találhatók.

Az üzemazonosítási folyamat további nehézsége, hogy a termékekben található veszélyes anyag nettó tömege általában nem ismert, mivel logisztikai szempontból ez az információ irreleváns. Ezért a termék bruttó tömegére vonatkozó adatok – például egy dezodor vagy egy arcszesz esetében – jelentős bizonytalanságot okoznak az üzemazonosítási folyamatban.

Az üzemazonosítás nehézségei nemcsak a logisztikai központ státuszának megítélésére vannak hatással, hanem a veszélyeztetés elemzésében is bizonytalanságot okoznak. A veszélyes anyagok tulajdonságainak és pontos mennyiségének ismerete nélkül a lehetséges baleseti eseménysorok sem azonosíthatók.

A logisztikai központok üzemeltetőinek célja a rendelkezésre álló tárhely maximális kihasználása, hiszen ezáltal optimalizálható a tárolás fajlagos költsége. A jelen lévő veszélyes anyagok típusa és mennyisége időben változhat, ezért az üzemeltetők csak ritkán tudják garantálni a veszélyes anyagok raktáron belüli állandó elhelyezését és lokációjának állandó kiosztását. A veszélyes anyagok raktáron belüli elhelyezkedése a következmény- és kockázatelemzés egyik input paramétere.

A logisztikai központok sajátossága, hogy a beérkező termékek jellemzően zárt térben mozognak. Egy jól tervezett, a rendeltetési célnak megfelelően kialakított raktárépület esetében kizárólag a tehergépjárműről történő le- és felrakodás során, a dokkoló környezetében fordulhat elő, hogy a veszélyes anyag kikerüljön a zárt raktári térből.

A logisztikai központok tevékenységének további sajátossága, hogy az egységcsomagolások mérete is változó, amit elsősorban a raktározási és szállítási szabályozások, valamint a rakodási kapacitások határoznak meg.

A logisztikai központokban előforduló legnagyobb egységcsomagolások:

- Raklapos egység: A leggyakoribb az EUR-raklap (1200 × 800 mm), de elterjedt az IPPC-raklap (1200 × 1000 mm) is. A maximális tömeg általában 1000–1500 kg. A raklapos egységen belül további küldeménydarabos egységek is elhelyezkedhetnek.
- IBC-tartályok *(Intermediate Bulk Container)*: Folyadékok és ömlesztett anyagok szállítására és tárolására használják. Az űrtartalom jellemzően 600–1000 l, a maximális tömeg a tárolt anyag sűrűségétől függően akár 1500 kg is lehet.
- Hordók, fém- és műanyag tartályok: A kis hordók jellemzően 50–100 l, a nagy hordók 200–250 l űrtartalmúak. A maximális tömeg a tárolt termék sűrűségétől függ, akár 250 kg is lehet.
- Big-bag zsákok: Ömlesztett áruk tárolására alkalmas csomagolás. Maximális térfogat: 500–2000 l. A terméktől függően a maximális tömeg 2000 kg is lehet.

A zárt térből kikerülő veszélyes anyag mennyiségét az egységcsomagolás mérete határozza meg, ezért a modellezés egyik inputadata.

A veszélyes áru szállítása, így a raktározása is kizárólag ADR-minősített csomagolási eszközben történhet. Az ADR-minősített csomagolási eszköz külső hatásokkal szembeni ellenállása jelentősen nagyobb, mint az általános csomagolási egységeké. Például az ADR-minősített IBC-k esetében az alábbi tesztek történnek:

- esésvizsgálat az ütésállóság és a szivárgásmentesség biztosítása érdekében;
- nyomáspróba a belső nyomás okozta deformációk vagy szivárgások elkerülése végett;
- halmazolhatósági teszt a raktározás és a halmozás stabilitásának igazolására.

A tesztkritériumoknak való megfelelés garantálja, hogy bizonyos eseménysorok esetén a veszélyes anyag ne kerüljön azonnal a környezetbe. Például az IBC-tartály ütésállósági tesztje során az üres vagy megfelelően feltöltött IBC-t 1,2 m magasságból ejtik le egy kemény felületre. Az esés különböző irányokban és szögekben történik (például sarkára, oldalára, aljára). A vizsgálat után nem lehet repedés vagy szivárgás az IBC-n. Ez a tesztelési eljárás biztosítja, hogy a logisztikai folyamatok során egy leborulás vagy leesés ne okozzon azonnali anyagkiszivárgást.

A logisztikai központokban a termékek be- és kiszállítása, tárolása, komissiózása, valamint egyéb logisztikai művelet – például címkézés, átcímkézés, egységrakomány-képzés vagy visszárukezelés – történhet. A tevékenységek közös jellemzője, hogy a termékek elsődleges csomagolását – veszélyes áru esetében az ADR-minősített csomagolást – a végzett tevékenység során nem bontják meg.

A logisztikai központok és raktárak tűzvédelmére az Országos Tűzvédelmi Szabályzatról szóló 54/2014. (XII. 5.) BM rendelet (OTSZ) szigorú előírásokat határoz meg. Az épület tűzállósági fokozatát a benne tárolt anyagok alapján kell meghatározni, szükséges továbbá a megfelelő tűzszakaszok kialakítása tűzgátló falakkal, ajtókkal és födémekkel. Az éghető és veszélyes anyagokat elkülönítve, a tárolási magasság és mennyiség korlátozásával kell raktározni, valamint biztosítani kell a megfelelő távolságokat a gyors beavatkozás érdekében. A raktárcsarnok méretétől és a tárolt árutól függően a jogszabály további tűzvédelmi berendezések – tűzjelző, automata tűzoltó berendezés, hő- és füstelvezető rendszer – létesítését írja elő. Ezek a megoldások hozzájárulnak a tűzesetek korai észleléséhez, az azonnali beavatkozás megkezdéséhez és a tűzterjedés megakadályozásához, ezáltal minimalizálva a károkat és a következményeket. Megítélésünk szerint az OTSZ és az egyéb jogszabályok hiányossága, hogy nem fogalmaznak meg követelményeket az esetlegesen keletkező szennyezett oltóvíz felfogására. Számos esetben a tervezők nem számolnak ezzel a tényezővel, így az üzemeltetés megkezdésekor, az építési fázis lezárását követően, utólag kell kialakítani a megfelelő megoldást. Tapasztalataink alapján ez a megközelítés bonyolultabb, mint ha már az építési fázisban gondoskodnának a megfelelő rendszer kiépítéséről.

Tapasztalataink szerint a veszélyes áru tárolása és a logisztikai központok üzemeltetése elsősorban az üzemeltetők belső előírásai alapján történik. Habár a munkavédelmi és tűzvédelmi jogszabályok tartalmaznak előírásokat a veszélyes áruk tárolására, ezek meglehetősen általánosak. Megítélésünk szerint a biztonságos üzemeltetés érdekében elengedhetetlen a veszélyes áruk tárolására vonatkozó alábbi területek szabályozása:

- veszélyes áru átvétele: a csomagolás és a jelölés ellenőrzése, sérült termék kezelése;
- raktározási rend kialakítása az együtt tárolási feltételek figyelembevételével;

- a betárolt veszélyes áru ellenőrzésére vonatkozó szabályok;
- a veszélyes áru kiadása: a csomagolás és a jelölés ellenőrzése, sérült termék kezelése.

A 219/2011. (X. 20.) Korm. rendelet hatálya alá tartozó logisztikai központok esetében az irányítási rendszer keretei között a szabályozás megvalósul.

A logisztikai központok által okozott veszélyeztetés megítélésében a fentiekben részletezett sajátosságok meghatározó szerepet játszanak. A veszélyes tevékenységből származó kockázat csökkentése érdekében már a tervezési fázisban kiemelten fontos figyelembe venni a veszélyes áruk tárolásának szempontjait, ideértve a megfelelő védelmi infrastruktúra – tűzvédelmi berendezések, szennyezett oltóvíz kezelése – megtervezését. Ebben az esetben a veszélyes anyagok tárolásából eredő veszélyeztetés valójában elhanyagolhatóvá válik, éppen a fent felsorolt egyedi jellemzőknek köszönhetően.

A logisztikai raktárakban előforduló veszélyes anyagokkal kapcsolatos baleseti eseménysorok azonosítása és következményeik elemzése

A baleseti eseménysorok azonosítása

Napjainkban számos logisztikai központ veszélyes üzemként működik, ami azt jelenti, hogy a tárolt veszélyes anyagok mennyisége elérheti vagy meghaladhatja a 219/2011. (X. 20.) Korm. rendelet 1. mellékletében meghatározott küszöbértéket. A veszélyes üzemként működő logisztikai központoknak a veszélyes tevékenység engedélyeztetése érdekében biztonsági jelentést vagy biztonsági elemzést kellett készíteniük. E két dokumentáció közös eleme a veszélyelemzés, amelynek során a logisztikai központoknak azonosítaniuk kellett a lehetséges baleseti eseménysorokat, meghatározniuk azok bekövetkezési valószínűségét, valamint modellezniük kellett a lehetséges következményeket. Az iparbiztonsági hatóság a kockázatelemzés eredményét a 219/2011. (X. 20.) Korm. rendeletben meghatározott kritériumokkal összevetve döntött a veszélyes tevékenység engedélyezéséről.

A logisztikai központoknál esetlegesen bekövetkező veszélyesanyag-kibocsátással járó súlyos baleseti eseménysorok azonosításához az úgynevezett RIVM[12] szakirodalom szolgáltat elemzési eljárást és módszertant. Az útmutató a logisztikai központokban az alábbi súlyos baleseti eseménysorok figyelembevételét javasolja:

- toxikus szilárd anyagok csomagolásának sérülése és diszperziója;
- toxikus folyadékok csomagolásának sérülése és a tócsa párolgása;
- tűzképződés a raktárban, toxikus égéstermékek keletkezése, terjedése;
- tűzképződés a raktárban, az el nem égett toxikus anyagok levegőbe jutása.

[12] National Institute of Public Health and the Environment 2009.

Véleményünk szerint a fent említett, RIVM szerinti baleseti eseménysorok csak részben fedik le a logisztikai központok üzemelésével kapcsolatos kockázatokat. Zárt épületen belül bekövetkező egységcsomagolás-sérülés várhatóan nem jelent komoly veszélyeztetést, azonban a kapcsolódó eseménysorok mennyiségi kockázatelemzés alóli kizárásához szakmai indoklás szükséges. A részletes vizsgálatnak ki kell terjednie az áruátvétel, az anyagmozgatás, a tárolás, az ideiglenes tárolás (beszállítást követő, illetve kiszállítás előtti átmeneti tárolás), valamint az áru kiadásának folyamataira is.

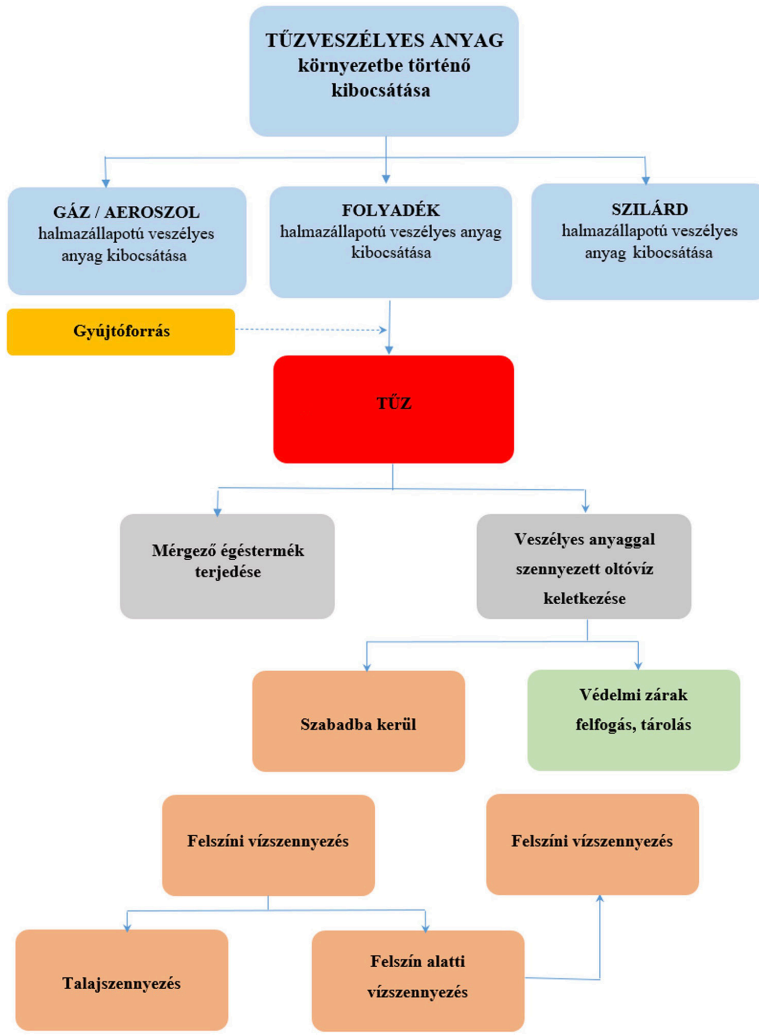
A logisztikai központok kockázatelemzésénél releváns eseménysor a raktártűz következtében szabadba kerülő toxikus anyagok és az égéstermékek keletkezésének hatása.[13] A fent említett baleseti eseménysorokon túlmenően megítélésünk szerint indokolt a környezeti veszélyeztetés vizsgálata is, különös tekintettel a raktártűz során keletkező szennyezett oltóvíz terjedésére.

Az alábbiakban a releváns baleseti eseménysor elemzésének módszertanát mutatjuk be.

Raktártűz, mérgező égéstermék keletkezése

A raktártűz kialakulásának feltétele a tűzveszélyes anyag, a megfelelő koncentrációjú oxigén és a gyújtáshoz szükséges energia térben és időben történő együttes jelenléte. A tűzveszélyes anyag szabadba kerülésének következményeit az 1. ábra foglalja össze.

[13] Cimer–Szakál 2015.



1. ábra: A tűzveszélyes anyag szabadba kerülésének következményei
Forrás: a szerzők szerkesztése

A kiemelt kockázatot jelentő létesítményekkel és a speciális veszélyforrásokkal, mint például a logisztikai raktárakkal kapcsolatos esetlegesen bekövetkező jelentős tűzesetekre külön fel kell készülni.[14] A tűzvédelmi tervezés egyik fontos eleme a helyi tűzoltó erők vonulási ideje, mivel ezen a ponton kapcsolódik a megelőző és mentő tűzvédelem a leginkább meghatározó módon.[15] A tűz bekövetkezésének kockázatát

[14] Varga 2018b.
[15] Varga 2018a.

növelő hatások közé tartoznak a gyújtóforrások, valamint az egyes vegyi anyagok egymással való veszélyes kölcsönhatásainak lehetősége.[16]

A logisztikai központokban előforduló tüzek megelőzésének egyik fontos eszköze a tűzjelző rendszerek kialakítása és üzemeltetése, amelyek a tűzoltó rendszerekkel együtt betöltik rendeltetésüket. A vagyonvédelmi rendszerek is a helyszíni fizikai védelmi rendszer részét képezik.[17]

Raktártűz esetén a hősugárzás hatása miatt elsősorban a műanyag tárolóedények sérülhetnek, aminek következményeként mérgező égéstermékek kerülhetnek a szabadba. Az égés során keletkező leginkább veszélyes gázok a foszgén, a hidrogén-cianid, a nitrogén-oxid, a kén-dioxid, a szén-dioxid és a szén-monoxid. Továbbá a magas hőmérsékleti körülmények között szabadba kerülő mérgező anyagok gyorsabban párolognak, így azok emberi egészséget károsító következményei súlyosabb mérgező hatást fejthetnek ki, mint a normál tárolási körülmények között történt veszélyesanyag-kibocsátás.

Nemzetközi szinten leginkább elterjedt módszertani útmutató a logisztikai raktárbázisokban végzendő mennyiségi kockázatelemzéshez használatos PGS 15[18] volt, amelynek hatálya alá tartoztak a – közúti veszélyesáru-szállítási ENSZ EGB-szabályozás (ADR) által meghatározott – csomagolt növényvédő szert és veszélyes anyagot raktározó logisztikai és kereskedelmi raktárak esetében alkalmazandó előírások. Az útmutató alkalmazásának szakmai alapjául a tűzmegelőzési létesítési és használati előírások szolgáltak. Az útmutató szerint amennyiben kiterjedt raktártűz alakul ki, az égés során keletkezett veszélyes anyagokban gyakran található arzén, kén, nitrogén, klór, fluor, továbbá brómatomokból mérgező égéstermékek, így arzén-oxid, kén-dioxid, nitrogén-dioxid, sósavgáz, hidrogén-fluorid vagy például hidrogén-bromid.

A raktártűz hatásainak elemzése során a mérgező égéstermékekből álló felhő kikerülését, terjedését és az általa okozott mérgezési hatást kell meghatározni. A felhőt különböző mérgező gázok keverékeként kell értelmezni a kiindulási anyagösszetétel függvényében. A raktárépületből kiáramló mérgező felhő hőmérsékletét a környezeti hőmérséklet és a raktár építményszerkezeteinek hűtő hatása befolyásolja. A veszélyes áruk logisztikai raktáraiban bekövetkező tüzek során keletkezett veszélyes szennyező anyagok többféle módon kerülhetnek ki és szennyezhetik a telephely környezetét.

Az Egyesült Királyságban alkalmazott és a Környezetvédelmi Ügynökség által kiadott útmutató[19] alapján a veszélyes anyag az alábbi utakon kerülhet a környezetbe:

- a telephely csapadék- és csurgalékvíz-elvezető rendszerén keresztül közvetlenül;
- a veszélyes anyag közvetlenül a létesítmény környezetében lévő felszíni vízbe folyása vagy a talajvizet közvetlenül veszélyeztető talajba szivárgása útján;
- a szennyvízrendszeren vagy a szennyvízkezelő üzemen keresztül;
- a levegőben terjedve, például párolgás útján.

[16] Érces–Vass 2018.
[17] Tóth–Tóth 2024.
[18] Ministry of Housing, Spatial Planning and the Environment 2016: 73.
[19] Environment Agency [é. n.]: 1.

A raktártűz eseménysorának és gyakoriságának meghatározásához a RIVM[20] szakirodalomban foglalt adat nyújt iránymutatást, ugyanakkor megítélésünk szerint az adat túl általános, adaptálni szükséges. A szakirodalomban egy 8,8 × 10-4/év gyakorisági érték szerepel, amely egy 1975 és 1987 között végzett holland felmérésen alapul. Ugyanakkor megítélésünk szerint ez az érték több szempontból is korlátozottan alkalmazható. Egyrészt a vizsgálat óta eltelt időszakban a raktárak építészeti kialakítása, az alkalmazott technológia, a tűzvédelmi rendszerek és a jogszabályi előírások jelentősen változtak, ami befolyásolhatja a tűzesetek gyakoriságát. Másrészt az eredeti felmérés földrajzilag Hollandiára korlátozódik, ezért nem feltétlenül tükrözi más országok – például Magyarország – sajátos ipari és logisztikai környezetét. Továbbá nem biztos, hogy a felmérés adatgyűjtési módszertana és az értékelési kritériumok megfelelnek a jelenlegi kockázatelemzési elveknek, különösen a modern veszélyesanyag-tárolási gyakorlatok tekintetében. Ezért indokolt az adat adaptálása az aktuális körülmények figyelembevételével.

Környezeti kockázat elemzése: szennyezett oltóvíz kezelése

Az Európai Környezetvédelmi Ügynökség 2010-es, *A természeti veszélyek és technológiai balesetek hatásainak feltérképezése Európában, az utolsó évtized értékelése* című jelentésében azt írja, hogy „az ökológiai rendszereket ért hatások közül a legsúlyosabb (mint azt a 2005-ben az Egyesült Királyságban bekövetkezett buncefieldi baleset is mutatja) volt a tűzoltási tevékenységből származó oltóvíz, amely hatékony felfogás nélkül a felszíni vagy a talajvizet szennyezi".[21]

Környezetkárosító hatásait a szennyezett oltóvíz közép- és hosszú távon fejti ki. A terület kármentesítése jelentős erőfeszítéseket követel az üzemeltetőtől és a hatóságoktól egyaránt, különösen akkor, ha az már a felszíni vizekbe vagy a talaj rétegeibe beszivárgott. A nemzetközi dokumentumok egyértelműen rögzítik az üzemeltetők által végrehajtandó kárelhárítási feladatokat és annak műszaki követelményeit, többek között a szennyezett oltóvíz összegyűjtését, tárolását, tisztítását és a környezet mentesítését.[22]

Az integrált szennyezés kialakulásának megelőzését szolgálják a 2014-ben készült és kiadott, *a Szennyvíz és szennyező gáz kezelése/a vegyipari irányítási rendszerek* című BAT referenciadokumentum irányelvei, amely ezen a téren az elérhető legjobb módszereket és technikákat ismerteti. Kimondja, hogy „a legtöbb esetben az elsődleges helyi (épületben elhelyezett) felfogórendszer elégséges a szennyezés megelőzésére. Ahol nincs helyi felfogórendszer, vagy a kockázatelemzés azt mutatja, hogy a több ezer köbméter szennyezett oltóvíz felfogása szükséges, ott vészhelyzeti tárolórendszert kell alkalmazni."[23]

[20] National Institute of Public Health and the Environment 2009.
[21] European Environment Agency 2010: 116.
[22] Meharg 1994.
[23] JRC 2014: 46.

A fentiekből következik az a megállapítás, hogy az oltóvízszennyezés elkerülésének legjobb módszere a különböző védelmi műtárgyak, technikai eszközök (műszaki zárak), valamint az ezek kötelező alkalmazását elrendelő jogszabályi előírások, követelmények.

A veszélyes tevékenységekkel kapcsolatos kockázatok és következmények értékelése hozzájárul a társadalmilag elfogadott szintű veszélyeztetettség meghatározásához, valamint a veszélyes tevékenység környezetében lévő lakosság magas fokú biztonságához. Ez utóbbi követelmény a társadalom biztonságérzetét és társadalmi ellenálló képességét erősíti.[24]

A szennyezett oltóvíz keletkezése lehetséges következményeinek elemzésére jógyakorlatként az eseményfa-elemzési módszert mutatjuk be. Az eseményfa-elemzés olyan – minőségi vagy mennyiségi – elemzési technika, amellyel azonosíthatók a kezdeti esemény bekövetkezésének lehetséges kimenetei, és amennyiben arra szükség van, bekövetkezési valószínűségei is. Az elemzési eljárás egy induktív módszer, amelynek alapkérdése: „mi történik, ha…?"[25]

Az elemzés alapvetően két fő lépésből áll:

- A vizsgált rendszer üzemelésének – beleértve a védelmi zárakat – részletes megismerése, valamint azok technológiai elemekre történő felbontása.
- A technológiai elemek lehetséges meghibásodásának feltárása, illetve a meghibásodás következményeinek elemzése.

Az eseményfa-elemzés kiválóan alkalmazható a veszélyes tevékenység tervezési fázisában, tekintettel arra, hogy a kezdeti esemény bekövetkezése utáni következmények azonosíthatók, így a védelmi zárak a tervezőasztalnál már meghatározhatók. Ahhoz, hogy a műszaki-biztonsági kialakítás teljes körű legyen, feltételezni kell – a valószínűségtől függetlenül – hogy minden azonosított eseménysor bekövetkezhet. A szennyezett oltóvíz szabadba kerülésének elemzésére nem szükséges részletes eseményfa-elemzés, ugyanis a valószínűségi értékek meghatározása jelen esetben indifferens. A lehetséges kimenetek három kategóriába sorolhatók:

- Lokális eseményként kezelendő kimenet során tényleges katasztrofális hatással vagy a környezet állapotában való tartós károsodással nem kell számolni.
- Jelentős hatással járó kimenet esetében katasztrofális hatás alakulhat ki, illetve a környezet állapotában tartós károsodás keletkezik, azonban országhatáron túli hatással nem kell számolni.
- Rendkívüli hatással járó kimenet során katasztrofális hatás alakulhat ki, illetve a környezet állapotában tartós károsodás is fennáll, amely országhatáron túli hatást is okozhat.[26]

A lehetséges következmények háromféle eseményfa alapján vizsgálhatók:

1. Épületen belül keletkező szennyezett oltóvíz eseményfája: Amennyiben az oltóvíz az épületen belül marad, az ipari padlón keresztül átszivároghat. Ha nincs megfelelő vízzáró réteg kialakítva, a szennyezett oltóvíz a talajba kerülhet.

[24] Bognár 2023.
[25] Kátai-Urbán 2013.
[26] Kátai-Urbán 2023.

A talaj típusától függően elérheti a talajvizet, majd annak útján akár felszíni vízfolyásokba is bejuthat.

2. Épületen kívülre kerülő szennyezett oltóvíz eseményfája: Ha az oltóvíz az épületen kívül keletkezik vagy oda kerül, a burkolt felületről a csapadékelvezető rendszeren keresztül távozhat. Védelmi zárak – beleértve a lokalizációs pontokat és a puffertárolót – hiányában a szennyezett oltóvíz az üzem területén kívüli befogadóba (jellemzően csapadékgyűjtő árokba) juthat, ahonnan bekerülhet a felszíni vízfolyásokba. A talaj típusától függően beszivároghat a talajvízbe, amelynek révén szintén felszíni vizekbe juthat.
3. Épületen kívül a talajra kerülő szennyezett oltóvíz eseményfája: Ha az oltóvíz közvetlenül a talajra kerül, a talaj típusától függően beszivároghat a talajvízbe, majd azon keresztül felszíni vízfolyásokba is eljuthat.[27]

A fenti általános eseményfa alkalmazása a tervezési fázisban lehetőséget biztosít arra, hogy a logisztikai központ olyan módon épüljön meg, hogy a kialakított védelmi záraknak köszönhetően az eseménysor kizárható legyen a további vizsgálatok alól.

Következtetések

A logisztikai központok által jelentett veszélyek értékelése az egyedi sajátosságok miatt speciális módszertant igényel. A szakirodalmi összefoglaló és a szerzők saját tapasztalatai alapján az alábbi következtetések vonhatók le:

1. Számos logisztikai központot veszélyes üzemi kategóriába sorolnak, ami azt jelenti, hogy jelentős mennyiségű veszélyes anyagnak minősülő termék tárolása történik ezekben a létesítményekben.
2. A kockázatelemzés során a nemzetközi szakirodalom által javasolt baleseti eseménysorok lokális adaptálása elengedhetetlen, különös tekintettel a szennyezett oltóvíz kezelésére.
3. A baleseti eseménysorok közül a raktártűz és annak következményei – különösen a mérgező égéstermékek és a szennyezett oltóvíz keletkezése – tekinthetők relevánsnak. A raktártüzek gyakoriságára vonatkozó nemzetközi szakirodalomban szereplő értékeket szükséges adaptálni a helyi sajátosságok figyelembevételével, mivel a különböző országok eltérő építési szabványokkal, tűzvédelmi rendszerekkel és üzemeltetési gyakorlatokkal rendelkeznek.
4. Az oltóvízszennyezés megelőzésének egyik legfontosabb eleme az oltóvízfelfogó és -tároló létesítmények megfelelő tervezése és telepítése. A műszaki követelményeknek az európai térségben célszerűen egységes szintet kellene képviselniük. Ebben kiemelt szerepük van a tűzmegelőzési előírásoknak, az üzemeltetői vízkárelhárítási intézkedéseknek. A jogszabályi előírások és az egységes műszaki normák segítenék a környezeti kockázatok minimalizálását.
5. A hazai iparbiztonsági felsőoktatásban, valamint az iparbiztonsági tevékenységi területeken a képzéseknek ki kell terjedniük az ipari környezetszennyezés

[27] Kátai-Urbán 2023.

megelőzésére is. Ennek célja, hogy a szakemberek megfelelő ismeretekkel rendelkezzenek a veszélyes anyagokkal kapcsolatos balesetek kezeléséről és a megelőző intézkedések kidolgozásáról.[28]

Felhasznált irodalom

Bakai Kristóf Péter (2022): Tudás a hatékony szervezet működéséért, avagy a Belügyi Szemle jelentősége a magyar vámhatóság hatékonyságának biztosításában. *Belügyi Szemle,* 70(11), 2165–2169. Online: https://doi.org/10.38146/BSZ.2022.11.1

Bognár, Balázs (2023): Social Resilience „Security Is What We Do!". *Védelem Tudomány,* 8(2), 49–64.

Carter, D. A. et al. (2003): Appropriate Risk Assessment Methods for Major Accident Establishments. *Process Safety and Environmental Protection,* 81(1), 12–18. Online: https://doi.org/10.1205/095758203762851949

Cimer, Zsolt – Szakál, Béla (2015): Control of Major-Accidents Involving Dangerous Substances Relating to Combined Terminals. *Science for Population Protection,* 7(1), 1–11.

Duijm, N. J. (2009): Safety-Barrier Diagrams as a Safety Management Tool. *Reliability Engineering & System Safety,* 94(2), 332–341. Online: https://doi.org/10.1016/j.ress.2008.03.031

Environment Agency [é. n.]: *Managing Fire Water and Major Spillages: PPG18.* Online: https://www.netregs.org.uk/media/1674/ppg-18.pdf

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

European Environment Agency (2010): *Mapping the Impacts of Natural Hazards and Technological Accidents in Europe. An Overview of the Last Decade.* Publications Office. Online: https://doi.org/10.2800/62638

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

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

JRC (2014): *Common Waste Water and Waste Gas Treatment/Management Systems in the Chemical Sector.* Online: https://eippcb.jrc.ec.europa.eu/sites/default/files/2020-03/superseded_cww_bref_0203.pdf

Kátai-Urbán Lajos szerk. (2013): *Iparbiztonságtan I. Kézikönyv az iparbiztonsági üzemeltetői és hatósági feladatok ellátásához.* Budapest: Nemzeti Közszolgálati és Tankönyv Kiadó Zrt.

[28] Vass 2017.

KÁTAI-URBÁN, Maxim et al. (2023): Identification Methodology for Chemical Warehouses Dealing with Flammable Substances Capable of Causing Firewater Pollution. *Fire,* 6(9), 345. Online: https://doi.org/10.3390/fire6090345

KÁTAI-URBÁN Maxim et al. (2024): Veszélyes áru raktározás oltóvízszennyezéssel kapcsolatos tűzvédelmi követelményeinek értékelése. *Polgári Védelmi Szemle,* 16(különszám), 312–323.

MEHARG, Andrew A. (1994): Industrial Accidents Involving Release of Chemicals Into the Environment: Ecotoxicology. *Environmental Technology,* 15(11), 1041–1050. Online: https://doi.org/10.1080/09593339409385512

Ministry of Housing, Spatial Planning and the Environment (2016): *PGS 15. Opslag van verpakte gevaarlijke stoffen.* Hague: VROM. Online: https://content.publicatiereeksgevaarlijkestoffen.nl/documents/PGS15/PGS_15_2016_versie_1_0_sept_2016_definitief.pdf

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

National Institute of Public Health and the Environment (2009): *Reference Manual Bevi Risk Assessments.* The Hague. Online: http://infonorma.gencat.cat/pdf/AG_AQR_2_Bevi_V3_2_01-07-2009.pdf

TIXIER, Jerome et al. (2002): Review of 62 Risk Analysis Methodologies of Industrial Plants. *Journal of Loss Prevention in the Process Industries,* 15(4), 291–303. Online: https://doi.org/10.1016/S0950-4230(02)00008-6

TÓTH Attila – TÓTH Levente (2024): Videóalapú tűzérzékelés. *Hadmérnök,* 19(2), 77–86. Onlne: https://doi.org/10.32567/hm.2024.2.6

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

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

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

Jogi források

ADR – Agreement Concerning the International Carriage of Dangerous Goods by Road

219/2011. (X. 20.) Korm. rendelet a veszélyes anyagokkal kapcsolatos súlyos balesetek elleni védekezésről

54/2014. (XII. 5.) BM rendelet az Országos Tűzvédelmi Szabályzatról

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG
20. évfolyam (2025) 2. szám 215–229.
DOI: 10.32567/hm.2025.2.13

István Mihály[1]

Estimating the Air Leakage Rate of Smoke Control Doors for Calculations Procedures, Part 1

Abstract

The extent of smoke spread during building fires is critical, as it can adversely affect both evacuation and firefighting intervention. Smoke migration can occur through structural gaps, therefore this possibility should be minimised. One way to exclude smoke is to pressurise the structure, and an important starting parameter for the design of this is to know the leakage areas. The need for knowledge of the size of structural gaps has been high since the inception of design methods. This article aims to identify the potential for improving the calculation procedures by using the results of measurements on existing smoke control doors in pressurised vestibules. In this section, the author presents the relevant literature on the leakage area of the openings and the air flow coefficient of the openings. It describes the measurement method for determining the air flow through doors and structures and the calculation procedure currently used.

Keywords: smoke control door, leakage area, air flow coefficient, stairwell pressurisation, fire safety design

Introduction

When a fire occurs in a building, it produces heat and toxic gases that can damage the people in the building, the objects in the building and the structure of the building.[2] The immediate release of large quantities of smoke that obstructs visibility and breathing must be given particular attention and combated from the start.[3] It can be seen that providing protection against heat and smoke is one of the main pillars of occupant's

[1] Certified Fire Protection Specialist, Judicial Expert, CEO, Brandplan Kft.; PhD student, Ludovika University of Public Service, Doctoral School of Military Engineering, e-mail: m.istvan@brandplan.hu
[2] Beda 2011: 94–98.
[3] Blume–Hegger 2021: 459–499.

safety. In order to achieve life safety objectives, the evolution of smoke must be limited or effective drainage of the resulting combustion products must be ensured.

Smoke may leak through open doors or windows, gaps around closed doors, cracks of structures, ventilation ducts or grills, shafts and other boundaries. The amount of the air leakage through the doors is influenced by several factors. Examples include the type of door and the pressure differential across the door, which causes air to leak through gaps and openings between the door and the frame.[4] Smoke can quickly spread to other areas of the building, which can impede evacuation from the building, among other things.[5]

The pressurisation created by mechanical fans can be used to control the movement of smoke through the barriers like doors. Air flow through the doors and the gaps of the structures keeps smoke from entering the higher pressure space. If the door is open and the air flow is sufficiently high, the backflow of smoke can be prevented.[6] In other words, the required overpressure and air volume are two important design parameters that have a decisive influence on the efficiency of the systems.

The creation of overpressure between two sides of a structure is typically provided by a mechanical fan.[7] To achieve overpressure, it is necessary to be able to determine the amount of air to be supplied. If the amount of air supplied is insufficient, the correct overpressure will not be created between the two sides of the structure. In this case, the smoke may infiltrate through the gaps into the lower pressure space. On the other hand, if the amount of air supplied is too large, an overpressure may develop that makes it difficult to open the doors or may even cause structural damage.

In the design process, it is crucial to know the amount of air that will flow through the structures at a given pressure and thus to determine the amount of air to be supplied with sufficient accuracy. Calculation methods provide a means of estimating this value by knowing the gap sizes of the structures. Since doors play a particularly important role in leakage losses, it is important to know the gap dimensions as accurately as possible.[8]

In many cases, smoke-protected spaces are separated from other spaces by so-called smoke control doors with a self-closing mechanism and restrict the entry of smoke at ambient or elevated temperatures.[9] Given the existence of test standards for these doors, it can be assumed that their air tightness is different from that of conventional doors and that their gap size can be estimated more uniformly if they passed the standard test.

In this paper, the author presents the literature on the air leakage of doors in the design process of positive pressure ventilation (called also pressurisation systems or pressure differential systems), and then describes two measurement methods for measuring the air tightness, and two calculation methods for estimating the amount of air leaking through door gaps.

4 Younes et al. 2011: 267–302.
5 Achakji 1987: 1.
6 Klote–Milke 1992: 39.
7 Klote–Milke 2002: 88.
8 Gross 1991: 171–177.
9 Gross 1981: 1–3.

Literature review

All countries have national regulations to minimise the risk of fire in buildings.[10] The use of positive pressure ventilation for smoke control as well as heat and smoke extraction started in the U.K. and Australia in the 1950s.[11] The idea of pressurising stairwells to provide a tenable environment within egress routes during building fires was first advanced in the late 1960s. ASHRAE (American Society of Heating, Refrigerating and Air-Conditioning Engineers) Smoke Control Manual was the first document on the subject specifically intended for use by designers.[12]

Early research has already highlighted that the leakage characteristics of walls and doors are particularly important, and more information is needed on the effective crack areas of installed leaf doors.[13] Even in a closed room, there is always some ventilation around doors, windows and through gaps in structures.[14]

Tamura's paper describes a computer study of smoke movement based on measured air leakage characteristics in office buildings. The equivalent leakage area for stairwell doors was 0.0185 m^2.[15] Soon afterwards, Hobson and Stewart carried out air leakage measurements on thirty doors with rebated frame. The results of the air leakage tests on the installed doors showed that the typical equivalent leakage area for single-leaf doors was 0.01–0.02 m^2.[16] This value was in good agreement with Tamura's previous result.

BS5588-4, published in 1978, made a distinction according to the opening direction of the doors.[17] The typical leakage area values given by the standard for single-leaf doors in rebated frame opening into a pressurised space were 0.01 m^2. For single-leaf doors in rebated frame opening from a pressurised space, this value was 0.02 m^2. Both values were given for a crack length of 5.6 m for doors 2.0 m high and 0.8 m wide.[18] The 1998 (2004) edition of the standard contained an informative annex with air leakage data for doors, but still recommended a value of 0.01 m^2 for single-leaf doors opening into a pressurised space and 0.02 m^2 for single-leaf doors opening from a pressurised space.[19]

Klote et al. gave flow areas of gaps values for single-leaf doors in tabular form, which can be used in the orifice equation with a flow coefficient of 0.65. For doors 2.13 m high, 0.914 m wide and 44.5 mm thick, the typical value is 0.0073–0.0428 m^2 depending on the thickness of the gaps above and below the door.[20]

In Annex A of the 2005 edition of EN 12101-6, the recommended air leakage data for doors opening into or out of the pressurised space were also 0.01–0.02 m^2.[21]

[10] Majorosné Lublóy et al. 2023: 4.
[11] Usemann 2003: 416.
[12] Klote 1987.
[13] Barrett–Locklin 1969: 299–310.
[14] Bedford–Chrenko 1974: 233.
[15] Tamura 1970.
[16] Hobson–Stewart 1972: 47.
[17] British Standards Institution 1978: 13–15.
[18] Butcher–Parnell 1979: 145–146.
[19] British Standards Institution 1998: 66–67.
[20] Klote et al. 2012: 116–122.
[21] CEN 2005: 88–91.

In the modernisation of the standard, the methods for designing pressure differential systems have been transferred to EN 12101-13, which also recommends values of 0.01–0.02 m^2 depending on the opening direction of single-leaf doors to be taken into account when estimating the air leakage through closed doors.[22]

There is another approach. The air leakage coefficient and gap length can be used to characterise the air flow through the gaps in the openings. The problem is that there is little literature data available on the values of air leakage coefficients.[23]

This is also the basis of the Fire Protection Technical Guideline in the field of Protection against Heat and Smoke Spread (TvMI), which proposes a method for determining the amount of air leakage through S_a/S_{200} smoke control doors.[24] The calculation procedure according to the TvMI is derived from the national fire protection regulations issued by Decree 9/2008 (II. 22.) ÖTM.[25]

In Hungary, the National Fire Safety Code defines the cases in which it is necessary to install a smoke-free staircase.[26] The safety level defined in the National Fire Safety Code can be achieved by applying the technical solutions and calculation methods developed in the Fire Protection Technical Guidelines.[27] A major part of designers and experts use the technical solutions proposed in the fire protection technical guidelines in their work.[28] It is important to give preference to systems that do not require physical intervention.[29]

The air leakage coefficient was also a traditional parameter for air leakage through windows and doors in Poland, defined as the amount of air entering a window 1 m in length at a pressure difference of 1 daPa in 1 hour.[30]

In Table 1, the author summarises air leakage coefficient values from various literature sources. The table clearly shows the variation in the air volume values theoretically required to maintain a given pressure differential depending on the literature sources.

The fire prevention solutions presented in this publication provide an opportunity to prevent or reduce the harmful effects of a possible fire on health.[31] The examination of the harmful effects shows similarities with the consequences of toxic combustion products produced in an industrial environment like chemical warehouses.[32] Additional technical solutions can be fire protection signalling systems, the development of which provides many new solutions in the field of property protection and fire protection.[33] Finally, we can learn important practical lessons for the development

[22] CEN 2022: 66–72.
[23] Baumann 2011.
[24] National Directorate General for Disaster Management 2025: 51–52.
[25] Decree 9/2008 (II. 22.) of the Minister for Local Government and Regional Development.
[26] Decree 54/2014 (XII. 5.) of the Ministry of the Interior.
[27] Act XXXI of 1996.
[28] Bérczi–Badonszki 2021: 66–96.
[29] Bérczi 2025: 19–23.
[30] Lis–Lis 2021.
[31] Almási et al. 2023.
[32] Berger et al. 2024.
[33] Tóth 2005.

of fire protection authority activity when dealing with the policing issues of event order security.[34]

Table 1: Air leakage coefficient of doors from various sources

Reference	Air leakage coefficient of doors [m3/hmPa2/3]		Air flow through door gaps at 25 Pa and 6.0 m gap length [m3/h]	
	With threshold	Without threshold	With threshold	Without threshold
Recknagel et al.35	9	3	467	156
Várfalvi36	8	1	415	52
Barna37	6	2	311	104
Gábor–Zöld38	4	1.5	207	78
Hobson–Stewart39	7.4	3.9	380	200
Liddament40	5.22 (weather-stripped)	5.67 (unsealed)	268	291
TvMI 3.641	1.11 (for Sa and Sm/S200 rated doors)		58	
ME-04–132–8442			184	

Source: compiled by the author

Estimating the amount of air flowing through door openings is an important factor in the design of positive pressure ventilation.

A review of the literature suggests that estimates of the effective leakage area for single-leaf closed doors have been in the order of 0.01–0.02 m^2 since early research. Recent studies on single-leaf smoke control doors have shown that the effective leakage area of single-leaf smoke control doors is independent of the opening direction and smaller than previous values reported in the literature.[43]

[34] Kanyó–Vásárhelyi 2019.
[35] Recknagel et al. 2000: 882–891.
[36] Várfalvi s. a.
[37] Barna 2015.
[38] Gábor–Zöld 1981: 130–131.
[39] Hobson–Stewart 1972: 47.
[40] Liddament 1986: 6.25.
[41] National Directorate General for Disaster Management 2025: 51.
[42] ÉSZK 1984: 6–7.
[43] Mihály et al. 2025.

Another method used to calculate the amount of air flow through closed doors is the air flow coefficient, which can be used to calculate the amount of air flowing through the closed door as a function of the length of the door slots.

Materials and methods

Description and characteristics of the subject of the study

In a previous study by Mihály et al., air leakage was measured from the smoke control doors of a mid-rise residential building, from which the effective leakage area of the doors could be calculated. The horizontal structures bounding the vestibule are reinforced concrete slabs, while the vertical structures are reinforced concrete and masonry. The lobby is 1.32 m × 2.18 m, with a ceiling height of 2.57 m, and the interior walls are plastered and painted white.

There are two doors per level to the vestibules, one to the vestibule and one from the vestibule. The doors with self-closing mechanism were made in 2013 and according to the available documents have Sm smoke control characteristics. The width of the door gaps to the lobby was 0.98 m and the height was 2.073 m. The width of the door gaps from the lobby was 0.92 m and the height was 2.05 m.

Due to door use, the actual air leakage through doors can vary greatly over the years.[44] This finding also suggests that tests should be carried out on structures already installed.

The pressurisation of the vestibules was ensured by an axial fan on the roof with a separate air duct. The design air flow rate of the fan was approximately 2,300 m^3/h according to the manufacturer's data sheet. The air was supplied to the vestibule from below the ceiling via a manually adjustable valve plate mounted on the side wall. The amount of air supplied could be varied by manually adjusting the valve plate.

Measuring air permeability with a Blower Door instrument

The pressure method is a pressure measurement method developed by the Department of Building Engineering at the Lund Institute of Technology and others to measure the compactness of a whole building.[45] The Blower Door instrument is used to measure air tightness. The principle of operation is to install an adjustable fan in a door or window frame and record the volume of air required to maintain a given pressure differential.[46] Figure 1 shows a Blower Door instrument installed in a door frame during the measurement process. If the flow characteristics, flow coefficient and exponent

[44] Cho et al. 2010: 3.
[45] Kronvall 1980a: 62.
[46] Sherman 1995.

of a building element, e.g. doors and windows, are known, the infiltration caused by the element can be calculated as a function of the pressure difference.[47]

According to the standard for determining the air permeability of buildings, there are several ways to create negative or positive pressure in the building envelope to perform measurements. One possible way is the blower door assembly, but for some buildings, the use of a building ventilation system fan is also possible to determine the air permeability.[48]

Figure 1: Blower Door instrument installed in a door frame
Source: compiled by the author

[47] Ridley et al. 2003.
[48] CEN 2016: 17–18.

Mihály et al. used a Duct Blaster B fan and a DG-1000 micromanometer with a maximum flow rate of 2,500 m^3/h at 50 Pa. The accuracy of the DG-1000 digital pressure and flow meter is 0.9% of the pressure value or 0.12 Pa (whichever is greater) under typical conditions of use, with a resolution of 0.1 Pa up to 1,000 Pa.[49]

In preliminary tests, the instrument was installed in a vestibule door and the differential pressure and air flow rate values were recorded.

Many infiltration models are based on an empirical (power law) relationship between flow and pressure differential through a crack or opening in the building envelope.[50] The flow of air through openings or ducts and the associated relationship is a well-studied phenomenon.[51] Physically, it is assumed that the exponent should have an expected value between 0.5 (for orifice flow) and 1.0 (for fully developed, long-tube laminar flow).[52]

Measuring air permeability with funnel and vane probe

EN ISO 9972 describes in an information annex the equipment used for pressurising buildings. The air permeability can also be tested using fans that are part of the heating or ventilation and air conditioning system of the building.[53]

If the supply system in the vestibule can provide the air volume required to perform the test at the specified pressure differentials, it may be suitable for determining the air permeability.

This requires an adjustable valve plate to control the amount of air supplied. In addition, a suitable and sufficiently accurate instrumentation to measure the amount of air discharged through the disc valve. An instrument for this purpose may be, for example, a funnel with a vane probe (Figure 2). By manually adjusting the disc valve during measurements, it is possible to establish the pressure levels and, with a sufficient seal between the funnel and the wall, to measure the amount of air flowing out with high accuracy.

The result of the series of measurements is a pressure and flow volume value pair that can be used to characterise the air tightness of the structures.

[49] Mihály et al. 2025.
[50] Ridley et al. 2003.
[51] Klems 1983.
[52] Zheng–Wood 2020.
[53] CEN 2016: 18.

Figure 2: Measurement with funnel vane probe
Source: compiled by the author

Use of the recommendation for estimating air leakage through doors according to EN 12101-13

The informative annex to EN 12101-13 proposes calculation methods for estimating the air flow through different structures, e.g. windows, doors, walls, floors.
The standard recommends that when air flows through an opening, the flow can be expressed as a function of the area of constriction and the differential pressure across the opening according to equation (1).[54]

$$Q_{OPENING} = C_v \times A_{OPENING} \times \sqrt{\frac{2}{\rho}} \times (\Delta P)^{\frac{1}{R}} \qquad (1)$$

where

$Q_{OPENING}$ – is the airflow through the relevant opening (m^3/s)
C_v – is the coefficient of discharge (0.6–0.9); in the absence of additional data, 0.65 should be used for the calculations of the Pressure Differential System
$A_{OPENING}$ – is the opening area (m^2)

[54] CEN 2022: 64.

ΔP – is the pressure difference across the opening (Pa)
ρ – is the density of air (kg/m³); use 1.2 kg/m³ as typical
R – is the coefficient of flow (for wide cracks may be taken to be 2.0, narrow leakage paths R is 1.6)

Using equation (1), if the leakage area and pressure difference are known, the amount of air flowing through the gap can be estimated. In another approach, knowing the amount of air flowing through the gap and the pressure differential forcing the air, the gap area can be estimated. The standard suggests tabular values for estimating the leakage area of different doors, walls and floors. For walls and floors, it is proposed to take the value of R as 1.6, and for doors as 2.

By combining the constants in equation (1), equation (2) is used to estimate the flow through gaps in closed doors, while equation (3) is used to estimate the flow through walls and floors.

$$Q_{DOOR\ CLOSED} = 0.839 \times A_{DOOR\ CLOSED} \times \Delta P^{\frac{1}{2}} \quad (2)$$

$$Q_{FL/W} = 0.839 \times A_{FL/W} \times \Delta P^{\frac{1}{1.6}} \quad (3)$$

where
$Q_{DOOR\ CLOSED}$ – is the airflow through the gap of the closed door (m3/s)
$A_{DOOR\ CLOSED}$ – is the leakage area of closed door (m2)
ΔP – is the pressure difference (Pa)
$Q_{FL/W}$ – is the airflow through the gap of floors or walls (m3/s)
$A_{FL/W}$ – is the leakage area of floors or doors (m2)

From equations (2) and (3), the estimated leakage areas can be expressed in terms of the differential pressure and the volumetric flow rate according to equations (4–6).

$$A_{FLOOR} = \frac{Q_{FLOOR}}{0.839 \times \Delta P^{\frac{1}{1.6}}} \quad (4)$$

$$A_{WALL} = \frac{Q_{WALL}}{0.839 \times \Delta P^{\frac{1}{1.6}}} \quad (5)$$

$$A_{DOOR\ CLOSED} = \frac{Q_{DOOR\ CLOSED}}{0.839 \times \Delta P^{\frac{1}{2}}} \quad (6)$$

where
A_{FLOOR} – is the leakage area of floors (m2)
Q_{FLOOR} – is the airflow through the gap of floors (m3/s)
ΔP – is the pressure difference (Pa)

A_{WALL} – is the leakage area of walls (m2)
Q_{WALL} – is the airflow through the gap of walls (m3/s)
$A_{DOOR\ CLOSED}$ – is the leakage area of closed door (m2)
$Q_{DOOR\ CLOSED}$ – is the airflow through the gap of the closed door (m3/s)

In the above calculation, if the air volume flow rate can be measured for a given pressure difference across walls and floors (for example, by taping door gaps), then the total gap area of walls and floors can be estimated. If a further measurement is made by removing the adhesive tape from the door under test, the volumetric flow rate measured in this situation can be corrected by the air flow rate determined on the walls and floors. The leakage area of the door can then be estimated. This is possible because these components form a branch with flow resistances parallel to their flow characteristics, and both resistances are affected by the same pressure differential.[55]

Use of the recommendation for estimating air leakage through doors according to TvMI

When designing a smoke-free stairwell according to TvMI, the gap loss of closed opening structures must be taken into account when calculating the air volume to be introduced into the stairwell using formula (7).[56]

$$\dot{V} = c \cdot \Delta p^n \cdot l \qquad (7)$$

where

$\dot{V}$– air leakage from the closed opening structure (m^3/h)
c – 1.11 (for S_a and S_{200} rated openings)
Δp – the pressure difference between the two sides of the opening (Pa)
n – 0.67 (for S_a and S_{200} rated openings)
l – the perimeter of the opening, in relation to the nominal size (m)

This relationship is similar to the formulas used in previous research to determine the amount of air flowing through window openings.[57]

By expressing equation (7) in terms of "c", we can obtain the air leakage coefficient for the door, given the pressure difference between the two sides of the opening, the length of the opening gap and the amount of air flowing through the gap (8).

[55] Kronvall 1980b: 91–96.
[56] National Directorate General for Disaster Management 2025: 51.
[57] Baumann 2011; Baumann 2005: 28–30; Mainka–Winkler 2010.

$$c = \frac{\dot{V}}{\Delta p^{n} \cdot l} \tag{8}$$

where

$\dot{V}$ – is the airflow through the gap of the closed door (m^3/h)
c – is the air leakage coefficient ($m^3h^{-1}m^{-1}Pa^{\wedge -0.67}$)
Δp – is the pressure difference between the two sides of the opening (Pa)
n – 0.67 (for S_a and S_{200} rated openings)
l – the perimeter of the opening, in relation to the nominal size (m)

Summary

In this article, the author has shown that the spread of smoke during fires poses a risk when evacuating building occupants. Smoke propagation through gaps in structures, including flows through door gaps, plays a significant role.

A recent experiment has shown that the effective leakage area of single-leaf smoke control doors is smaller than the values reported in the literature.58 In this context, the author investigated the calculation procedure used in Hungary for the design.

In the next part of the paper, the author describes the measured determination of the leakage area and the air flow coefficient. The conclusions are drawn and suggestions are made for improving the values used in the design procedures. (8)

References

Achakji, George Y. (1987): *NRCC Experimental Fire Tower for Studies on Smoke Movement and Smoke Control in Tall Buildings.* Internal Report No. 512. Ottawa: National Research Council Canada Institute for Research in Construction. Online: https://doi.org/10.4224/20338144

Almási, Csaba – Kátai-Urbán, Lajos – Cimer, Zsolt (2023): ABV-felderítő eszközök bemutatása és fejlesztési lehetőségei. *Védelem Tudomány,* 8(Különszám), 195–205.

Barna Lajos (2015): Tüzelőberendezések égési levegő ellátása. Előadás. „A szén-monoxid mérgezések hatékony megelőzése" Országos szakmai konferencia, Budapest, 5 March 2015. Online: http://www.vedelem.hu/files/UserFiles/File/aktualis/20150403/04.pdf

Barrett, Richard E. – Locklin, David W. (1969): A Computer Technique for Predicting Smoke Movement in Tall Buildings. *Fire Technology,* 5(4), 299–310. Online: https://doi.org/10.1007/BF02600417

Baumann, Mihály (2005): Tüzelőberendezések légellátása. *Magyar Installateur,* 15(10–11), 28–30.

[58] Mihály et al. 2025.

Baumann, Mihály (2011): *Épületek légforgalma.* 17th "Building Services, Mechanical and Building Industry Days" International Conference, Debrecen, 13–14 October 2011. Online: https://www.e-gepesz.hu/files/cikk9422_EUG_Baumann.pdf
Beda, László (2011): Gondolatok az épületek tűzbiztonságáról. *Magyar Építőipar*, 56(3), 94–98.
Bedford, Thomas – Chrenko, Frank Ambrose eds. (1974): *Bedford's Basic Principles of Ventilation and Heating.* London: H. K. Lewis.
Bérczi, László – Badonszki, Csaba (2021): A tűzvédelmi tervezés fő tartópillérei a tűzvédelmi műszaki irányelvek. *Védelem Tudomány,* 6(2), 66–96. Online: https://ojs.mtak.hu/index.php/vedelemtudomany/article/view/13473
Bérczi, László (2025): Új kihívások és alternatív megoldások a tűzoltásban. *Tűzvédelem,* 32(2), 19–23.
Berger, Ádám – Kátai-Urbán, Lajos – Németh, Zsolt – Zsitnyányi, Attila – Kátai-Urbán, Maxim – Cimer, Zsolt (2024): Applicability of Design Methodology for the Remediation Bund of Flammable Dangerous Liquid Storage Tanks. *Fire,* 7(7). Online: https://doi.org/10.3390/fire7070246
Blume, Gary – Hegger, Thomas Fr. (2021): Rauch- und Wärmeabzug. In Fouad, Nabil A. (ed.): *Bauphysik Kalender 2021.* Brandschutz, 21. Jahrgang. Berlin: Ernst & Sohn GmbH & Co. KG, 459–499. Online: https://doi.org/10.1002/9783433610572.ch19
British Standards Institution (1978): BS 5588-4:1978 Fire Precautions in the Design and Construction of Buildings. Part 4. *Code of Practice for Smoke Control in Protected Escape Routes Using Pressurisation.* London: British Standards Institution.
British Standards Institution (1998): BS 5588-4:1998 + A2:2004 Fire Precautions in the Design, Construction and Use of Buildings. Part 4. *Code of Practice for Smoke Control Using Pressure Differentials.* London: British Standards Institution.
Butcher, Edward G. – Parnell, Alan C. (1979): *Smoke Control in Fire Safety Design.* London: E. & F. N. Spon Ltd.
CEN (2005): EN 12101-6:2005 Smoke and Heat Control Systems. Part 6. *Specification for Pressure Differential Systems.* Kits. Brussels: Technical Committee of the European Committee for Standardisation.
CEN (2016): *EN ISO 9972:2016 Thermal Performance of Buildings. Determination of Air Permeability of Buildings.* Fan Pressurisation Method (ISO 9972:2015). Brussels: Technical Committee of the European Committee for Standardisation.
CEN (2022): *EN 12101-13:2022 Smoke and Heat Control Systems.* Part 13. Pressure Differential Systems (PDS). Design and Calculation Methods, Installation, Acceptance Testing, Routine Testing and Maintenance. Brussels: Technical Committee of the European Committee for Standardisation.
Cho, Heejin – Liu, Bing – Gowri, Krishnan (2010): E*nergy Saving Impact of ASHRAE 90.1 Vestibule Requirements: Modeling of Air Infiltration through Door Openings.* Technical Report, PNNL-20026. Online: https://doi.org/10.2172/1017117
ÉSZK (1984): *ME-04–132–84 Füstmentes lépcsőházak követelményei.* Budapest: Építésügyi Szabványosítási Központ.
Gábor, László – Zöld, András (1981): *Energiagazdálkodás az építészetben.* Budapest: Akadémiai Kiadó.

Gross, Daniel (1981): *A Review of Measurements, Calculations and Specifications of Air Leakage Through Interior Door Assemblies.* Gaithersburg, MD: National Institute of Standards and Technology. Online: https://doi.org/10.6028/NBS.IR.81-2214

Gross, Daniel (1991): Estimating Air Leakage Through Doors for Smoke Control. *Fire Safety Journal,* 17(2), 171–177. Online: https://doi.org/10.1016/0379-7112(91)90040-6

Hobson, P. J. – Stewart, L. J. (1972): *Pressurisation of Escape Routes in Buildings. Fire Research Note No. 958.* Bracknell: Heating and Ventilating Research Association. Online https://publications.iafss.org/publications/frn/958/-1/view/frn_958.pdf

Kanyó, Ferenc – Vásárhelyi-Nagy, Ildikó (2019): Research for New Physical Ability Testing Method for Firefighters in the V4 Countries. *Műszaki Katonai Közlöny,* 29(1) 161–166. Online: https://doi.org/10.32562/mkk.2019.1.13

Klems, Joseph H. (1983): Methods of Estimating Air Infiltration Through Windows. *Energy and Buildings,* 5(4), 243–252. Online: https://doi.org/10.1016/0378-7788(83)90012-9

Klote, John H. (1987): *An Overview of Smoke Control Technology.* Gaithersburg, MD: National Institute of Standards and Technology. Online: https://doi.org/10.6028/NBS.IR.87-3626

Klote, John H. – Milke, James A. (1992): *Design of Smoke Management Systems.* Atlanta, GA: American Society of Heating, Refrigerating and Air-Conditioning Engineers – Boston, MA: Society of Fire Protection Engineers.

Klote, John H. – Milke, James A. (2002): *Principles of Smoke Management.* Atlanta, GA: American Society of Heating, Refrigerating and Air-Conditioning Engineers.

Klote, John H. – Milke, James A. – Turnbull, Paul G. – Kashef, Ahmed – Ferreira, Michael J. (2012): *Handbook of Smoke Control Engineering.* Atlanta, GA: American Society of Heating, Refrigerating and Air-Conditioning Engineers.

Kronvall, Johnny (1980a): *Airtightness. Measurements and Measurement Methods.* Stockholm: Swedish Council for Building Research.

Kronvall, Johnny (1980b): *Air Flows in Building Components.* PhD Thesis. Lund University.

Liddament, Martin W. (1986): *Air Infiltration Calculation Techniques.* An Applications Guide. Coventry: The Air Infiltration and Ventilation Centre. Online: https://www.aivc.org/resource/air-infiltration-calculation-techniques-applications-guide

Lis, Piotr – Lis, Anna (2021): The Required Amount of Ventilation Air for the Classroom and the Possibility of Air Infiltration through the Windows. *Energies,* 14(22). Online: https://doi.org/10.3390/en14227537

Mainka, Georg-Wilhelm – Winkler, Heiko (2010): *Influence of New External Protective Glazing on Historic Painted Windowpanes in Medieval Churches.* Online: http://eprints.sparaochbevara.se/610/1/31_Mainka%5B1%5D.pdf

Majorosné Lublóy, Éva Eszter – Major, Zoltán – Szép, János – Hlavička, Viktor – Biró, András (2023): *Méretezés tűzteherre az Eurocode szerint. Vasbeton, acél-, fa-, falazott és öszvérszerkezetek tervezése.* Budapest: TERC Kereskedelmi és Szolgáltató Kft.

Mihály, István – Bérczi, László – Bognár, Balázs – Kátai-Urbán, Maxim – Tóth, Levente – Kátai-Urbán, Lajos – Vass, Gyula – Varga, Ferenc (2025): Experimental Study to Determine the Leakage Area of Single-Leaf Smoke Control

Doors in the Design of Pressure Differential Systems. *Fire,* 8(1). Online: https://doi.org/10.3390/fire8010005

National Directorate General for Disaster Management (2025): *Tűzvédelmi Műszaki Irányelv [Fire Protection Technical Guideline]. Hő és füst elleni védelem [Protection against Heat and Smoke Spread].* TvMI 3.6:2025.02.01. Belügyminisztérium, Országos Katasztrófavédelmi Főigazgatóság. Online: https://www.katasztrofavedelem.hu/application/uploads/documents/2024-12/84963.pdf

Recknagel, Hermann – Sprenger, Eberhard – Schramek, Ernst-Rudolf (2000): *Fűtés- és klímatechnika 2000. I. kötet.* Budapest–Pécs: Dialóg Campus.

Ridley, Ian – Fox, J. – Oreszczyn, Tadj – Hong, Sung-Hugh (2003): The Impact of Replacement Windows on Air Infiltration and Indoor Air Quality in Dwellings. *International Journal of Ventilation,* 1(3), 209–218. Online: https://doi.org/10.1080/14733315.2003.11683636

Sherman, Max Howard (1995): The Use of Blower-Door Data. *Indoor Air,* 5(3), 215–224. Online: https://doi.org/10.1111/j.1600-0668.1995.t01-1-00008.x

Tamura, George T. (1970): *Computer Analysis of Smoke Movement in Tall Buildings.* Research Paper No. 452. Ottawa: National Research Council of Canada, Division of Building Research. Online: https://doi.org/10.4224/40000451

Tóth, Levente (2005): *CCTV magyarul.* Budapest: BM Nyomda Kft.

Usemann, Klaus W. (2003): *Brandschutzanlagen. In Brandschutz in der Gebäudetechnik. VDI-Buch.* Berlin–Heidelberg: Springer, 333–437. Online: https://doi.org/10.1007/978-3-642-19001-8_3

Várfalvi, János [s. a.]: *Ablakszerkezetek légáteresztése.* Online: http://152.66.45.150/EPFIZ/Ablakszerkezetek_legatreresztese.pdf

Younes, Chadi – Shdid, Caesar Abi – Bitsuamlak, Girma (2011): Air Infiltration through Building Envelopes: A Review. *Journal of Building Physics,* 35(3), 267–302. Online: https://doi.org/10.1177/1744259111423085

Zheng, Xiaofeng – Wood, Christopher J. (2020): On the Power Law and Quadratic Forms for Representing the Leakage-Pressure Relationship – Case Studies of Sheltered Chambers. *Energy and Buildings,* 226. Online: https://doi.org/10.1016/j.enbuild.2020.110380

Legal sources

1996. évi XXXI. törvény a tűz elleni védekezésről, a műszaki mentésről és a tűzoltóságról [Act XXXI of 1996 on Fire Prevention, Technical Rescue and Fire Brigades]. Online: https://njt.hu/jogszabaly/1996-31-00-00

9/2008. (II. 22.) ÖTM rendelet az Országos Tűzvédelmi Szabályzat kiadásáról [Decree 9/2008 (II. 22.) of the Minister for Local Government and Regional Development on the Issuance of the National Fire Protection Regulation]. Online: https://njt.hu/jogszabaly/2008-9-20-1V.2#CI

54/2014. (XII. 5.) BM rendelet az Országos Tűzvédelmi Szabályzatról [Decree 54/2014 (XII. 5.) of the Ministry of the Interior on the Issuance of the National Fire Protection Regulation]. Online: https://njt.hu/jogszabaly/2014-54-20-0A

Tartalom