HADMÉRNÖK

Kiemelt közlemények

19. évf. (2024)
1. 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, Resofszki Ágnes

Tartalom

Fórum

HADMÉRNÖK
KATONAI MŰSZAKI INFRASTRUKTÚRA

19. évfolyam (2024) 1. szám 5–20.
DOI: 10.32567/hm.2024.1.1

Hajós Bence[1]

A STANAG 2021 szerinti katonai járműteherosztályok a polgári hídszabályzatok tükrében

Military Vehicle Classes According to the STANAG 2021 in the Light of Civil Bridge Design Codes

Absztrakt

A katonai járművek és hidak teherbírási besorolási rendszerét a STANAG 2021 szabvány szerint kell végezni. Ehhez kapcsolódó feladat a meglévő polgári hidak katonai teherbírási besorolása. A besorolás gyors módszere lehet konverziós eljárások kidolgozása. A munkához szükséges a STANAG 2021 szerinti ideális járművek pontos ismerete, ezek paramétereinek részletes elemzése és a polgári szabályozástól eltérő részletek azonosítása.

Kulcsszavak: STANAG 2021, híd, hídszabályzat, teherbírás, méretezés

Abstract

The load classification of military vehicles and bridges shall be carried out according to the STANAG 2021. A related task is the military load classification of existing civil bridges. A quick method for classification could be the development of conversion procedures. This work requires a precise knowledge of the ideal vehicles according to STANAG 2021, a detailed analysis of their parameters and the identification of details that differ from the civil design codes.

Keywords: STANAG 2021, bridge, bridge code, load capacity, static calculation

[1] Hidászmérnök, 2012-ben Az év hidásza, az Első Lánchíd Bt. ügyvezetője, e-mail: elsolanchid@elsolanchid.hu

Bevezetés

Magyarország 1999. évi NATO[2]-csatlakozását követően a Honvéd Vezérkar főnökhelyettesének 17/2001. (HK 3/2002) intézkedésével vezették be a STANAG 2021-gyel[3] az AEP-3.12.1.5 NATO-szabványt,[4] amely hidak, kompok, tutajok és katonai járművek teherbírási osztályozásáról rendelkezik. Az egyezmény és a szabvány angolul készült, hivatalos magyar fordítása nincsen.

A szabvány eljárásrendet rögzít a katonai járművek terheinek és geometriájának függvényében való osztályba sorolására mind kerekes, mind lánctalpas járművekre vonatkozóan. A szabvány második része pedig hidak, kompok és tutajok teherbírásának osztályba sorolásáról rendelkezik. Az előírás célja, hogy amennyiben egy híd vagy komp, tutaj besorolási száma nagyobb, mint az adott katonai járműé, akkor nincs teherbírási akadálya az átkelésnek.

A korábbi katonai hídszabályzattól lényegesen eltérő, egységes NATO-szabályozás bevezetéséhez kapcsolódóan több részletes tanulmány,[5] vitaanyag,[6] vizsgálat készült, és 2003-ban országos konferencia[7] is foglalkozott a STANAG 2021-gyel kapcsolatos feladatokkal, kihívásokkal.[8] A témafelvetés érintőlegesen megjelent két PhD-disszertációban is.[9] A témához kapcsolódó utolsó publikáció 2018-ban jelent meg[10] a STANAG akkor hatályos 7. kiadását elemezve, egyúttal bemutatva azt a szakértői háttérmunkát, amelynek egy része beépült a szabvány jelenleg hatályos 8. kiadásába.

A szabványhoz kapcsolódó hazai publikációk pontosan kijelölték a szükséges teendőket, feladatokat, amelyek végrehajtását akadályozta, hogy ezzel egy időben történt a polgári hídszabályzat reformja és az Európai Unióhoz való csatlakozás okán az Eurocode bevezetése. A magyar közúti hídtervezésben használatos Útügyi Műszaki Előírás az Eurocode transzparens átvételét ekkor megkerülte, ami az egységes európai tervezési elvek átültetését bő két évtizeddel elhalasztotta. A napjainkban elkészülő új polgári hídtervezési előírások fogják ténylegesen átvenni az Eurocode előírásait.[11]

Jelen tanulmány célja a STANAG 2021 szerint megfelelőnek tartott katonai járműterhek bemutatása és elemzése, összehasonlítva ezeket a polgári hídtervezésben alkalmazott ideális hasznos terhekkel. E vizsgálat szükséges a meglévő polgári hidak katonai besorolásának elvégzéséhez, ami a STANAG 2021 mindennapi használatba vételének része kell hogy legyen.

A vizsgált szabványt számos NATO-tagállam évtizedek óta használja. A STANAG 2021 első kiadását az amerikai hadsereg készítette el, amit tükröz a teherosztályok

[2] North Atlantic Treaty Organisation – Észak-atlanti Szerződés Szervezete.
[3] STANAG 2021 (Standardization Agreement – Szabványosítási Egyezmény).
[4] A továbbiakban az egyezményre és a mögöttes szabványra együttesen STANAG 2021-ként hivatkozom. A szabvány szövege önmagára is STANAG 2021-ként utal.
[5] Deák–Havasi–Nagy 2001; Gulyás 2002.
[6] Gulyás–Havasi 2003.
[7] Lukács 2003.
[8] Gulyás 2003.
[9] Havasi 2007; Gulyás 2009.
[10] Polónyi 2018.
[11] Hajós 2024.

eredeti angolszász mértékegységrendszere, amit a jelenleg hatályos 8. kiadás már SI-mértékegységekre átváltva közöl.

A katonai teherbírási besorolási rendszert (Military Load Classification, MLC) sok ország alkalmazásba vette, így joggal merülhet fel a kérdés, miért szükséges ezzel nemzeti szinten foglalkozni egy már bevett eljárás helyett. Mivel az egységes európai méretezési rendszer, az Eurocode átvétele elmaradt, a meglévő magyar polgári hídállomány az elmúlt évtizedekben érvényes magyar hídtervezési előírások szerint épült.

A magyar hídállomány (körülbelül 16 000 hídszerkezet) katonai teherbírási besorolása óriási feladat. A besorolás végezhető hidanként, egyesével, részletes erőtani számítások készítésével, de praktikusan végezhető megfelelő teherbírási konverziós eljárással, a híd ismert polgári teherbírási osztályából és egyéb releváns paramétereiből kiindulva. E második módszerrel kellő pontossággal elvégezhető a katonai besorolás lényegesen kisebb idő- és költségráfordítással, mint egyedi számítások készítésével. Ennek előfeltétele a STANAG 2021 részletes elemzése, vizsgálata és az egyes korok polgári hídtervezési előírásaival való összehasonlítása.

Katonai járműteherbírási osztályok (MLC)

A kitűzött célhoz alaposan ismerni kell a STANAG 2021 ideális járműveit. A szabványban összesen 32-féle járműtípus van, 16 lánctalpas és 16 kerekes. Ezek jelölése MLC4-től MLC150-ig terjed. A 16-féle lánctalpas járműnél a szám azonos az ideális lánctalpas jármű angolszász mértékegységben kifejezett tömegével rövid tonnában *(short ton)*. Az ideális kerekes járműveknél az össztömeg nagyobb, mint a besorolási szám.

A rövid tonna (1 short ton = 2000 font) az SI-rendszerben 907,185 kg-nak felel meg. Így az MLC100 besorolású lánctalpas jármű össztömege 100 rövid tonna, ami az SI szerint 90,72 tonnának felel meg, ami súlymértékre átváltva (9,80665 m/s^2 nehézségi gyorsulással) 889,64 kN. A szabványban található besoroláshoz használatos nyomaték- és nyíróerő-adattáblák e fenti szabatos átváltásokkal készültek. Ez azért megjegyzendő, mert az SI-mértékegységek 1980. évi magyarországi bevezetésétől a polgári hidászatban nemes egyszerűséggel a hasznos teher tömegértékeinek súlyra való átszámítását 10 m/s^2 nehézségi gyorsulással végzik, ami közel +2% eltérést jelent a biztonság javára. Így lett a hatályos közúti előírásokban a korábbi 80 tonnás közúti járműteherből 800 kN és a 400 kg/m^2 közúti megoszló terhelésből 4 kN/m^2. A jelzett átváltási egyszerűsítés napjainkban a konkrét polgári járműszerelvények, jellemzően túlméretes, túlsúlyos különleges esetek ellenőrzésekor használatos.

A STANAG 2021 járműosztályait tekintve az első szembetűnő különbség a 16+16-féle osztály adta bő választék a közúti teherosztályokhoz képest. Ugyanazon MLC-osztályozás használatos a járművekre és a hidakra is. A hidakat tekintve túlságosan részletesnek tűnik a 16 fokozatú osztályzás, míg a katonai járművek esetében, tekintettel a járműbesorolásokból származtatható jármű-kombinációkra is, amit később részletesen is megvizsgálunk, indokolt a besorolás sokfélesége.

Hidak esetében 16-féle osztályt használhatunk (MLC4 – MLC150), a katonai járművek esetében viszont a 16-os skála valójában MLC4-től MLC150-ig terjedő, 147 fokozatú osztályzás iterációs besorolásához használatos. Ugyanis a megadott

ideális MLC-jármű-kategóriák között lineáris interpolációval kell képezni a tényleges jármű besorolását, a kapott eredményt egész értékre felfelé, a biztonság javára kerekítve. Érdekesség, hogy a járművek besorolásánál alkalmazandó módosító tényezőkkel vagy jármű-kombinációval akár MLC150-nél nagyobb besorolási számot is kaphatunk a járműre vagy jármű-kombinációra, amit az MLC150-ig terjedő hídosztályozás nem tud kezelni, így ezen esetek kívül esnek a szabvány alkalmazási körén.

A lánctalpas járművek nehéz és zömök paramétereikkel könnyen lehetnek mértékadók a hidak ellenőrzésekor. A nagyobb lánctalpas járműosztályok vonatkozásában talán kirívónak is tűnhetnek első olvasatban a minden korábbi hidászelőírásnál lényegesen nagyobb teherszintek. Hidászszemmel a lánctalpas katonai járművek esetében első kérdés, hogy mekkora a legnehezebb lánctalpas jármű, amelynek közlekedésére rövid, közép- vagy akár hosszú távon számítani kell.

Az eddigi hídtervezési osztályokat tekintve a II. világháború után hazákban, igazodva a KGST[12] előírásához, a legnagyobb ideális járműteher 80 tonna[13] volt. A legnehezebb hadrendbe állított harckocsikat tekintve kijelenthetjük, hogy a 80 tonna össztömeget a tényleges igények ma sem haladják meg.

A legnehezebb katonai járművek közé tartoznak a Honvédelmi és Haderőfejlesztési Program keretében beszerzett Leopard 2A7HU harckocsik, amelyek össztömege 73 tonna[14].

Ismeretes, hogy a hadtörténelemben voltak próbálkozások óriás szupertankok építésére, ezek közül a legnagyobb a Maus névre keresztelt náci német tank volt. A fejlesztés elején 100 tonnásra tervezett jármű végül 188 tonna lett, amelyből csak egy példány készült el 1944-ben, illetve egy második félkészen, fatoronnyal. Az 1942-ben tervezett, szintén német Landkreuzer P. 1000 grandiózus tank 14 m széles, 35 m hosszú és 11 m magas lett volna, 1000 tonna össztömeggel, de a terv a prototípusig sem jutott el.[15] A járművek tömegének emelése a kétségtelen előnyök mellett aránytalanul nehezíti a mozgásképességet, így nem véletlen, hogy a technológiai fejlődés nem ebbe az irányba folytatódott.

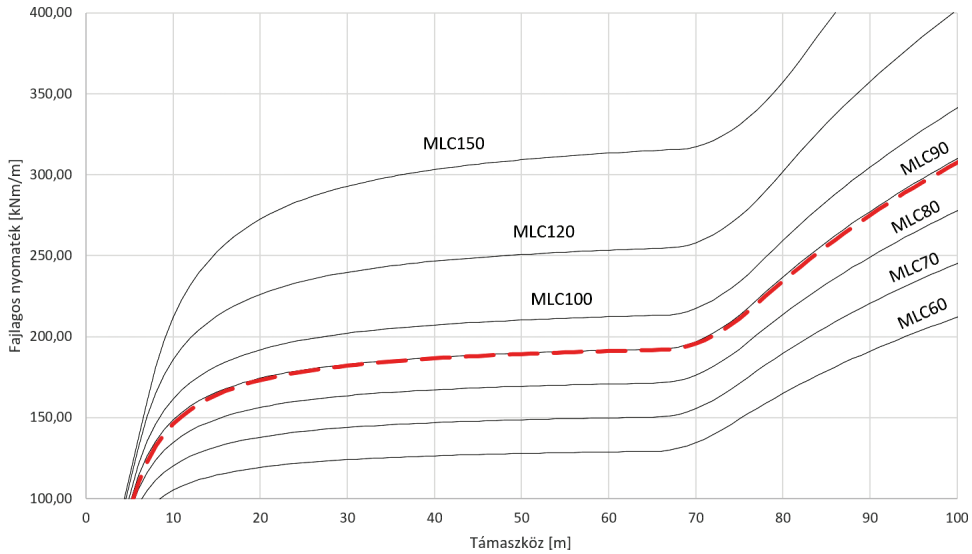
A lánctalpas járművek esetében a szabvány MLC90 feletti részének gyakorlati jelentősége elenyésző. MLC90 feletti terhelés a várható járművekkel csak kombinációval lehetséges, például két MLC75 besorolású harckocsi egymást vontatja, így az összegzés szabályai szerint MLC150 együttes járműbesorolást eredményezve.

A járművek MLC-besorolásának eredménye nem azonos a jármű össztömegével, hanem a szabványban szereplő ideális járműterhekhez kell arányosítani a vizsgált eszközt. Az arányosítást kéttámaszú tartón számított legnagyobb mezőközépi nyomatéki és támaszközeli nyíróerő-igénybevételek számításával kell elvégezni. Erre nézzünk egy gyors példát.

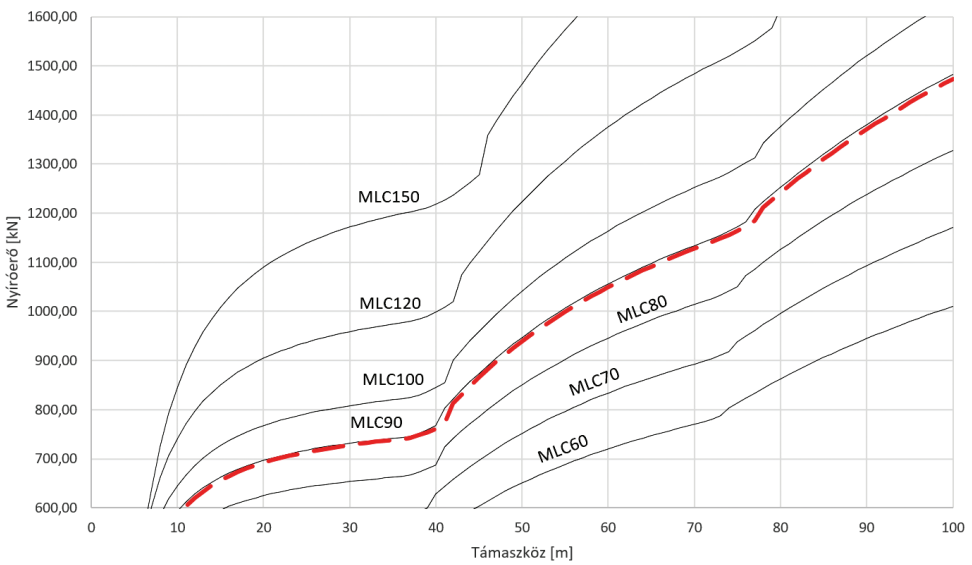
A járművek MLC-besorolásának menetét illusztrálva határozzuk meg egy harckocsi MLC-besorolását, össztömegét 800 kN-nak feltételezve, a lánctalpakat pedig 5,4 m hosszúnak, egyenként 55 cm szélesnek és 3,7 m keresztmetszeti szélességgel felvéve.

[12] Kölcsönös Gazdasági Segítség Tanácsa.
[13] Hajós 2024.
[14] Tóth 2022.
[15] Arndt [é. n.].

A szabvány szerint kéttámaszú gerendamodellen elvégeztük a vizsgált jármű okozta nyomatékok és nyíróerők számítását 1–100 m támaszköztartományban, méterenkénti léptékben. A vizsgált jármű és a STANAG 2021 szerinti ideális járművek igénybevételi grafikonját mutatja a támaszköz függvényében az 1. és a 2. ábra.



1. ábra: A 800 kN-os harckocsi nyomatéki vizsgálata
Forrás: a szerző szerkesztése



2. ábra: A 800 kN-os harckocsi nyíróerő-vizsgálata
Forrás: a szerző szerkesztése

Először a nyomatéki görbeseregeknél megállapíthatjuk, hogy sehol sem haladja meg az MLC90-hez tartozó értékeket. Az MLC90 görbéjét legjobban 63–66 m támaszköztartományban közelíti meg, így a vizsgált jármű MLC-alapértékének iterálását itt végeztük el. Az MLC80 és MLC90 közötti iterálással kapott nyers MLC-besorolási szám 89,76-ra adódott.

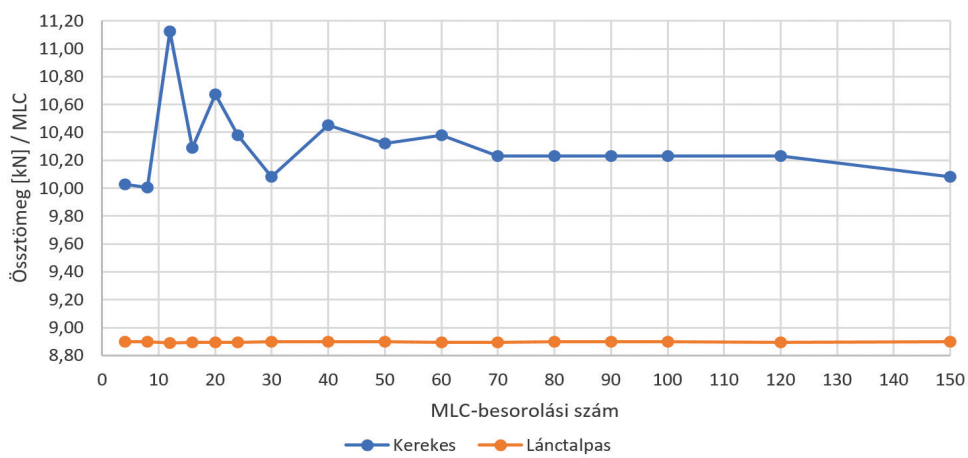
Második lépésben ugyanezt el kell végezni a nyíróerő-görbeseregekkel is. Itt szintén végig az MLC90 alatt marad a vizsgált jármű, az MLC90 görbéjét legjobban 35–36 m támaszköztartományban közelítve meg. Ezen támaszközön végzett iteráció eredménye 89,60, ez lesz a besorolási szám.

Végül a vizsgált jármű szélességének megfelelő korrekciót kell elvégezni. Az MLC90 ideális szélessége 3,81 m, a vizsgált jármű pedig 3,7 m, azaz 11 cm-rel keskenyebb – kedvezőtlenebb. A szabvány D melléklete szerint ezért az iterált nagyobbik besorolási alapszámot (6 / 25,4 × 11 =) 2,598%-kal növelni kell: 89,76 × 1,02598 = 92,1. A korrigált értéket egész számjegyre felfelé kerekítve kaphatjuk meg a vizsgált jármű MLC-besorolását, ami esetünkben tehát MLC93.

Az ideális járművek paraméterei

A szabványban megadott ideális járművek egyes paraméterei nem alkotnak tiszta matematikai sorozatokat, így érdemes megismerni ezeket részleteiben is.

Vizsgáljuk meg a STANAG 2021 ideális járműveinek paramétersorozatait. A lánctalpas járművek besorolási száma azonos az angolszász rövid tonnában kifejezett össztömeggel, így mind a 16 esetben az ideális lánctalpas jármű tömege kN-ban kifejezve egyenlő az MLC-besorolási számnak pontosan a 8,9-szeresével. A kerekes járművek össztömege az angolszász rövid tonnában mindig nagyobb, mint az MLC-besorolási szám, azonban itt a kettő között nincsen egyenes arányosság. Az ideális jármű tömege kN-ban kifejezve egyenlő az MLC-besorolási szám 10,0–11,12-szeresével (3. ábra).



3. ábra: A STANAG 2021 szerinti ideális járművek össztömegének [kN] aránya az MLC-besorolási számhoz
Forrás: a szerző szerkesztése

A 16-féle lánctalpas jármű további paramétereinek összehasonlítását tartalmazza az 1. táblázat és a 4. ábra. Az össztömeg kivételével az egyes paraméterek nem alkotnak lineáris sorozatot.

A jármű lánctalpainak keresztmetszeti szélessége közel egyenletesen növekszik a terhelési osztályokkal. A lánctalp felfekvési hossza ugyan monoton növekszik a besorolási számmal, de az MLC12, MLC16, MLC20 és MLC24 ideális járművek lánctalphossza egységesen 2,74 m. Hasonló helyzet látható a lánctalp szélességi értékében is, az MLC4, MLC8, MLC12 és MLC16 osztályok lánctalpszélessége egyformán 30 cm, de egyforma az MLC24 és MLC30 lánctalpszélessége is (46 cm).

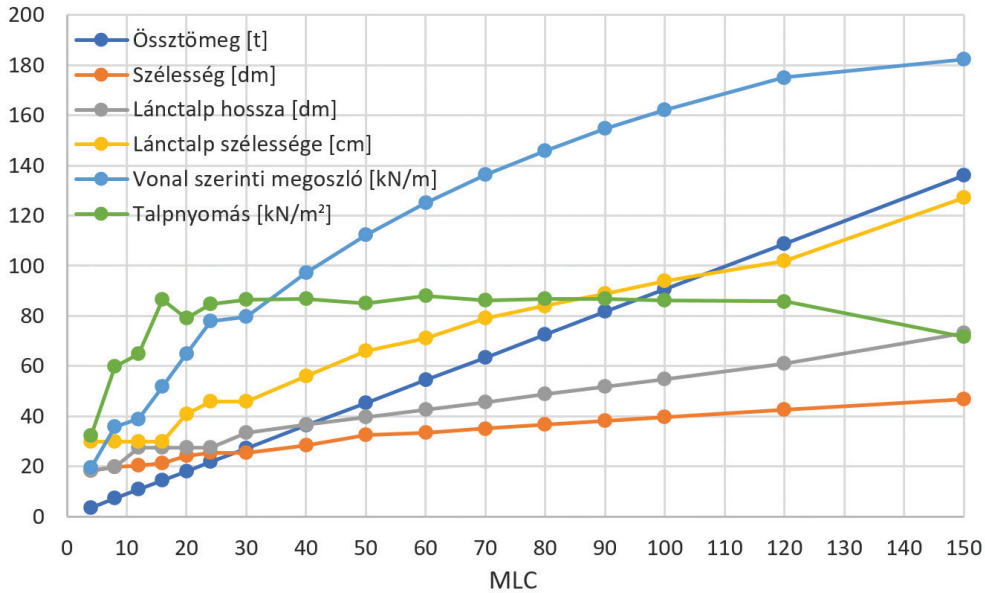
A lánctalpas járművek terhelésénél a lánctalp felfekvési hosszában egyenletesen megoszló vonal menti terhelést elemezve láthatjuk, hogy az egyes terhelési osztályok közötti változás szigorúan monoton nő. Ez kifejezetten fontos tulajdonság ahhoz, hogy egyszerűsített rúdmodellen lehessen számításokat végezni, és e tekintetben ne sérüljön az a kívánalom, hogy a nagyobb besorolási osztály okozta hatás ne legyen semmilyen esetben sem kisebb, mint a kisebb besorolású hatás.

A lánctalp alatti pecsétterhelést vizsgálva leginkább szembeötlő az egymást követő teherosztályok különbsége. A lokális fajlagos terhelés 32,42 kN/m^2 és 86,82 kN/m^2 között változik, a két legnagyobb teherosztályban pedig az értékek csökkennek. Ez a lokális vizsgálatok esetén akár problémát is eredményezne, de a szabvány előírja, hogy a lánctalpas járművek esetében a pecsétterhelésre figyelembe kell venni az azonos teherosztályú kerekes jármű mértékadó kerékterhelését fél értékkel, ami nagyobb terhet jelent (lásd 5. ábra), így a lánctalp alatti pecsétterhelés nem lehet egy esetben sem mértékadó. A legkisebb kerekes jármű pecsétnyomása 395,4 kN/m^2, ami fél értékkel számítva is több mint kétszerese a legnagyobb lánctalp alatti pecséttehernek.

1. táblázat: A STANAG 2021 szerinti ideális lánctalpas járművek paraméterei

MLC	Össztömeg		Szélesség	Lánctalp		Fajlagos teher	
	[t]	[kN]	[dm]	hossz [dm]	szélesség [cm]	[kN/m]	[kN/m^2]
4	3,63	35,60	18,3	18,3	30	19,45	32,42
8	7,26	71,20	19,8	19,8	30	35,96	59,93
12	10,88	106,70	20,3	27,4	30	38,94	64,90
16	14,51	142,29	21,3	27,4	30	51,93	86,55
20	18,14	177,89	24,4	27,4	41	64,92	79,18
24	21,77	213,49	25,4	27,4	46	77,92	84,69
30	27,22	266,94	25,4	33,5	46	79,68	86,61
40	36,29	355,88	28,4	36,6	56	97,24	86,82
50	45,36	444,83	32,5	39,6	66	112,33	85,10
60	54,43	533,78	33,5	42,7	71	125,01	88,03
70	63,5	622,72	35,1	45,7	79	136,26	86,24
80	72,58	711,77	36,6	48,8	84	145,85	86,82
90	81,65	800,71	38,1	51,8	89	154,58	86,84
100	90,72	889,66	39,6	54,9	94	162,05	86,20
120	108,86	1067,55	42,7	61,0	102	175,01	85,79
150	136,08	1334,49	46,7	73,2	127	182,31	71,77

Forrás: a szerző szerkesztése



4. ábra: A STANAG 2021 szerinti ideális lánctalpas járművek paraméterei az MLC-besorolási szám függvényében

Forrás: a szerző szerkesztése

A kerekes ideális járművek paramétereinek sorozata nagyobb belső egyenetlenséget mutat. Az adatokat a 2. táblázat és az 5. ábra tartalmazza. Ezek közül a teherbírás-ellenőrzés szempontjából fontosabb a mértékadó tengelyterhelés és az ebből származtatott gumiabroncs alatti pecsétnyomás. (A grafikonon a pecsétterhelést 0,1 kN/m^2 egységben ábrázoltuk, hogy a többi paraméterrel jól összehasonlítható görbesereget kapjunk.)

A kisebb teherosztályokban „ingadozó" intenzitású pecsétterhelés nem szerencsés egy szabványos ideális tehersorozatnál, de kétségtelen, hogy gyakorlati hatása elhanyagolható. A nagyobb járművek esetében viszont látható a pecsétteher szignifikáns visszaesése MLC50-től. Ennek oka, hogy innentől a mértékadó tengelyterheléshez négy abroncs tartozik, a kisebb teherosztályokban lévő két abroncs helyett.

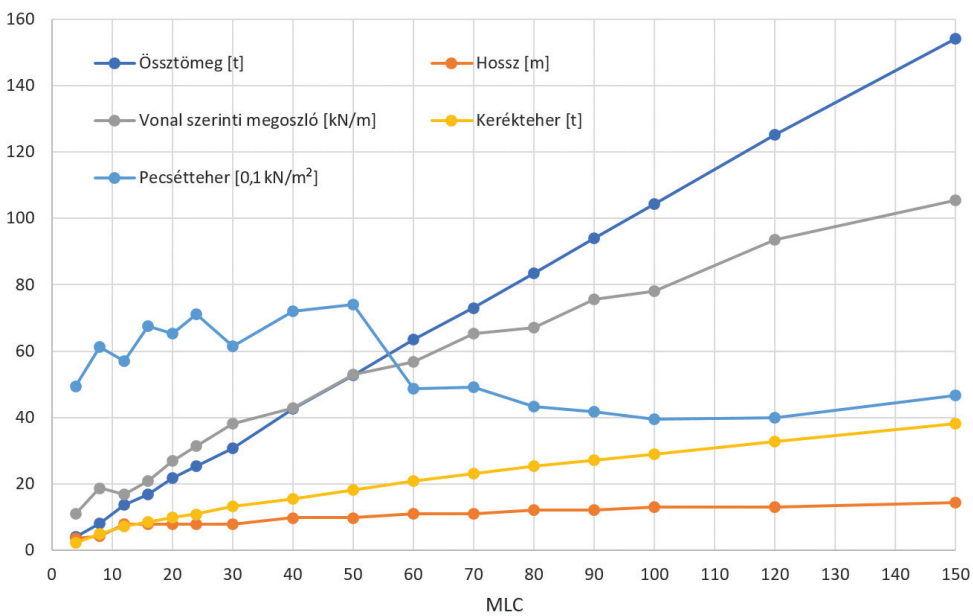
Ez azt eredményezi, hogy lokális vizsgálatra (például híd kocsipályaátszúródás-vizsgálata) a legnagyobb szélsőséget mutatva, az MLC100 osztályra ellenőrzött pecsétteher 187%-át okozza a kisebb osztályú MLC50 szerinti ideális jármű!

A kerekes ideális járművek mértékadó kerék-pecsétterhelésének bemutatott anomáliáját a hidak MLC-besorolásakor a lokális vizsgálatokban figyelembe kell venni. Ez történhet egyszerűen a legnagyobb pecsétteher (MLC50 szerinti 741,2 kN/m^2) egységes alkalmazásával valamennyi nagyobb teherosztályban.

2. táblázat: A STANAG 2021 szerinti ideális kerekes járművek paraméterei

MLC	Össztömeg		Hossz	Fajlagos teher	Mértékadó kerék					Pecsétteher
	[t]	[kN]	[m]	[kN/m]	hossz [cm]	kereszt [cm]	darab	kerék-teher [t]	tengely-teher [kN]	[0,1 kN/m²]
4	4,09	40,11	3,66	10,96	15	15	2	2,27	22,26	49,47
8	8,16	80,02	4,27	18,74	20	20	2	4,99	48,94	61,17
12	13,61	133,47	7,93	16,83	25	25	2	7,26	71,20	56,96
16	16,79	164,65	7,93	20,76	25	25	2	8,62	84,53	67,63
20	21,77	213,49	7,93	26,92	25	30	2	9,98	97,87	65,25
24	25,4	249,09	7,93	31,41	25	30	2	10,89	106,79	71,20
30	30,84	302,44	7,93	38,14	30	35	2	13,15	128,96	61,41
40	42,63	418,06	9,76	42,83	30	35	2	15,42	151,22	72,01
50	52,62	516,03	9,76	52,87	30	40	2	18,14	177,89	74,12
60	63,5	622,72	10,97	56,77	35	30	4	20,86	204,57	48,71
70	73,02	716,08	10,97	65,28	35	33	4	23,13	226,83	49,10
80	83,45	818,36	12,19	67,13	40	36	4	25,40	249,09	43,24
90	93,89	920,75	12,19	75,53	40	40	4	27,21	266,84	41,69
100	104,33	1023,13	13,11	78,04	40	45	4	29,03	284,69	39,54
120	125,19	1227,69	13,11	93,65	40	50	4	32,66	320,29	40,04
150	154,22	1512,38	14,33	105,54	40	50	4	38,10	373,63	46,70

Forrás: a szerző szerkesztése



5. ábra: A STANAG 2021 szerinti ideális kerekes járművek paraméterei az MLC-besorolási szám függvényében

Forrás: a szerző szerkesztése

Itt érdemes megemlíteni, hogy a STANAG 2021 szerinti legnagyobb tengelyterhelések lényegesen magasabbak, mint a járatos polgári közlekedésben engedélyezettek. A legnagyobb egységes európai polgári tengelyterhelés 11,5 t. Egyedi különleges szállítmányok esetében előfordulnak ennél nagyobb tengelyterhelések is, de 13 t feletti tengelyterhelés már egészen ritka speciális esetnek minősül, ennek közlekedéséhez a közútkezelő jellemzően részletes elemzéseket, vizsgálatokat is előír.

Az MLC150 osztályhoz tartozó legnagyobb tengelyterhelés 38,1 tonna, tehát a polgári közúti közlekedés tükrében rendkívülinek számít. A gyakorlatban ilyen tengelyterheléssel nem kell számolnunk, amire jó példák a Magyar Honvédség új beszerzésű nehézgépszállító eszközei.[16] Míg az ideális MLC150-es járműnek öt tengelye van, a ténylegesen várható 150 tonna körüli járműveknek várhatóan lesz legalább 9-10 tengelye. A polgári célú túlméretes szállítások esetén a 150 tonna össztömegű szerelvények tipikusan 13–15 tengelyesek.

Polgári hídszabályzatok szerinti pecsétterhelések

A STANAG 2021 ideális kerekes járműveinek pecsétterhelési kérdésköréhez kapcsolódóan vizsgáljuk meg a legfontosabb polgári hídszabályzatokban szereplő releváns értékeket.

A jelenleg hatályos Útügyi Műszaki Előírás[17] kétféle terhelési osztályt tartalmaz. Az A jelű teherhez 800 kN-os négytengelyes jármű tartozik, s ezt kell alkalmazni néhány marginális eset kivételével. A B jelű teherhez 400 kN-os háromtengelyű ideális jármű tartozik, ennek jelentősége napjainkra visszaszorult, de a meglévő hídállományban nagy számban előfordul, elsősorban mellékutakon.

Az A jelű jármű mértékadó pecsétterhelése 625,0 kN/m^2, a B jelű járműé 666,7 kN/m^2. Indokolatlan, hogy a fordított arány itt is előfordul, még ha kisebb arányban is, nevezetesen a nagyobb A jelűre méretezett pecsétteher 107%-át okozza a kisebb B jelű jármű.

A mindenkori magyar polgári hídszabályzatok közül az 1910. évi legelső előírás[18] tartalmazza a legnagyobb pecsétterhelést. Az ideális járműnek kijelölt acélkerekű gőzeke mértékadó tengelyterhelése 15 tonna, de az acélkerék miatt a felfekvési területe kicsi, így a fajlagos pecsétnyomása 1225,8 kN/m^2-re adódik.

Érdemes összehasonlításunkat kiegészíteni az Eurocode szerinti mértékadó tengelyterheléssel is. Napjainkban folyamatban van a közúti polgári hidak tervezésére vonatkozó Útügyi Műszaki Előírások megújítása, amelyben meg fog jelenni az Eurocode tehermodellje, habár a teherszintet módosító osztályba sorolási tényezők még véglegesen nem ismeretesek.[19] Tekintsük át az Eurocode alapértékét, amely hatályos az európai országok döntő többségében.[20]

[16] Farkas 2020.
[17] e-UT 07.01.12:2011.
[18] 33.034/1910 K.M. rendelet.
[19] Hajós 2023.
[20] Bartus–Kővári–Németh 2023.

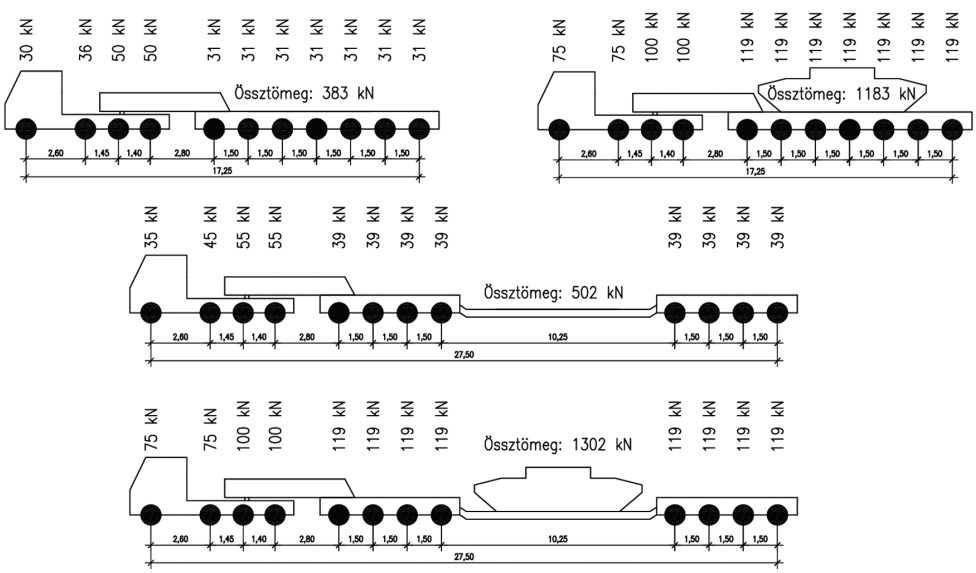
Az Eurocode 300 kN-os tengelyterheléséhez tartozó pecsétnyomás 937,5 kN/m^2, ami lényegesen nagyobb, mint a hatályos magyar A vagy B jelű jármű. Jelentős szabályozási különbség viszont, hogy az Eurocode szerinti járműterhek máshogyan kezelik a dinamikus hatást, alapesetben a tengelyterhek már tartalmazzák a dinamikus többletet, így részletes összehasonlító vizsgálat során erre is tekintettel kell lenni.

Jármű-kombinációk MLC-besorolása

Ha több jármű egymást vontatja vagy szállítja, akkor az egyes járművek besorolási számát összegezni kell. Ha az összeg MLC60-nál kisebb, akkor a kombináció besorolási értéke az összeg 90%-a, egyéb esetben az összeggel egyenlő (például MLC52 és MLC91 kombinációja MLC143-at eredményez).

Vizsgáljuk meg két egyszerű példán keresztül a legtipikusabb nehézgépszállítási konfigurációt az MLC-besorolások összegzésével és részletes elemzéssel is. A példában a mintául használt 800 kN-os harckocsit helyezzük nehézgépszállító trélerre. Megvizsgáljuk külön az „asztalon" szállítás és a mélybölcsőben szállítás esetét is. Ez utóbbi előnye, hogy alacsonyabb lesz a rakomány szállítási magassága. A trélerek szélessége legyen 3 m.

A vizsgálathoz a 6. ábra szerint vettük fel a járművek tengelyelrendezését és terhelését. A két tréler üresen 383 kN-os (11 tengelyes), illetve 502 kN-os (12 tengelyes, mélybölcsős).



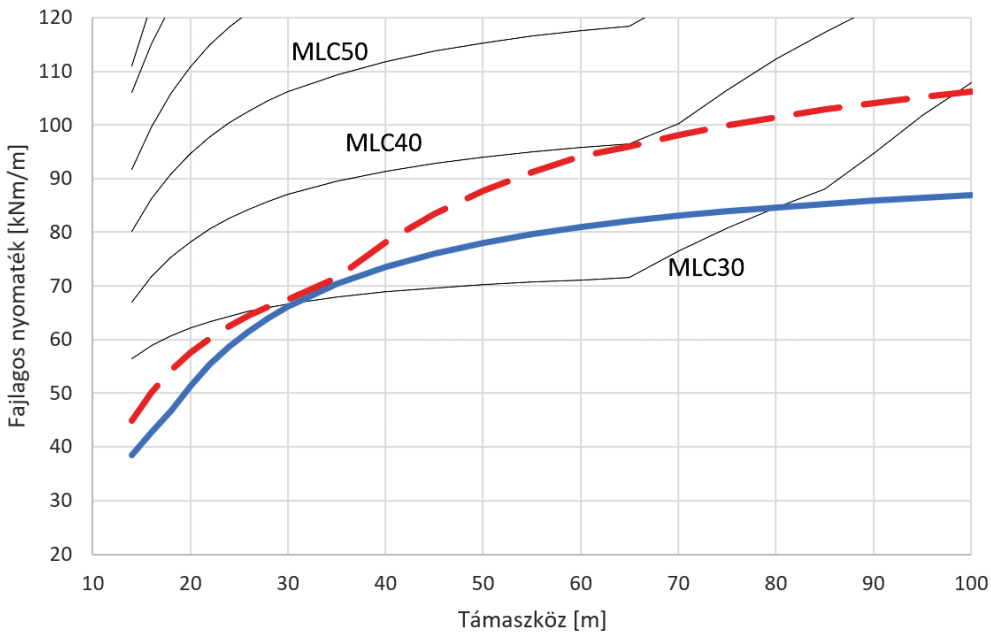
6. ábra: A mintaszámításhoz használt 11 tengelyes nehézgépszállító tréler üresen és rakottan, valamint a mélybölcsős, 12 tengelyes tréler üresen és rakottan

Forrás: a szerző szerkesztése

A példaszámításban a tréler tengelyei között tökéletesen egyenletes teherelosztást feltételeztünk, ami a hidraulikus felfüggesztésű járművekre jellemző, de konkrét esetben a tényleges terhelési értékeket mindenképpen javasolt mérlegeléssel ellenőrizni.

A STANAG 2021 kerekes járművekre vonatkozó szabályai szerint elvégeztük az üres trélerek MLC-besorolását. A könnyebbik tréler (11 tengelyes) iterációs besorolási alapértéke 34,2 – ami 65 m támaszközhöz tartozó nyomatéki számításnál volt mértékadó. Szélességkülönbségből fakadó korrekció nincsen (2 cm többlet), egészre kerekítve tehát a besorolás eredménye MLC35.

A mélybölcsős tréler esetében az iterációs besorolási érték 39,8, szélességi korrekció nincsen, egészekre kerekítve MLC40. A mértékadó fajlagos nyomatéki görbéket az ideális járművek görbeseregével a 7. ábra szemlélteti.



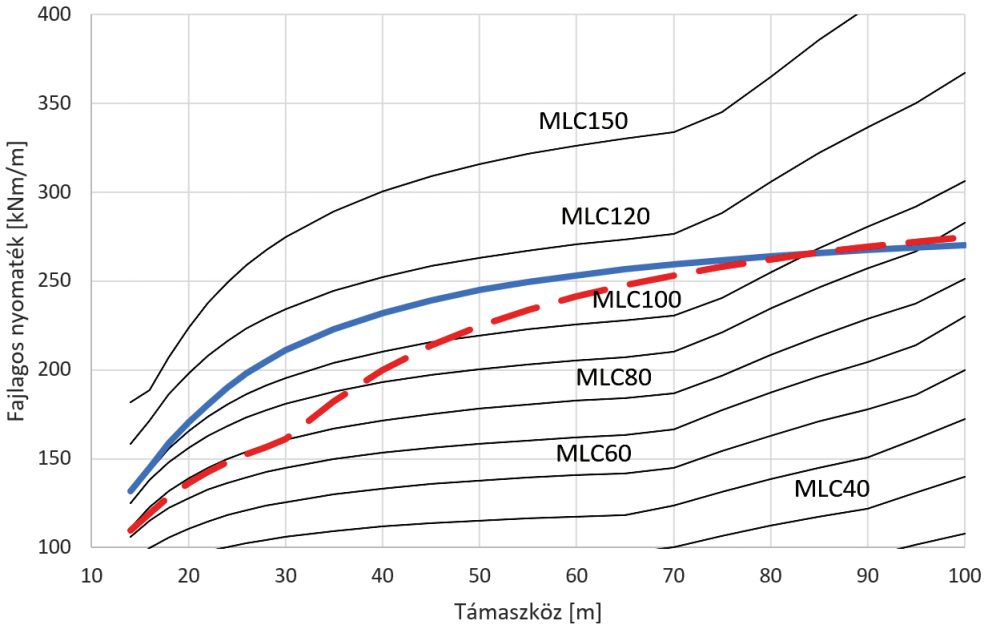
7. ábra: Az üres 11 tengelyes nehézgépszállító tréler (kék) és a mélybölcsős, 12 tengelyes tréler (szaggatott piros) fajlagos nyomatéki görbéje

Forrás: a szerző szerkesztése

A harckocsit az üres trélerekre helyezve, az összegzési szabályból származó besorolási szám a 11 tengelyes tréler esetében (35 + 93) MLC128, a mélybölcsős tréler esetében pedig (40 + 93) MLC133.

Elvégeztük a rakott trélerek MLC-besorolását a 6. ábra szerinti rakott terhelési értékekkel is. A 11 tengelyes rakott tréler iterációs besorolási alapértéke 106,3 – ami 65 m támaszközhöz tartozó nyomatéki számításnál volt mértékadó. A szélességkülönbségből fakadó korrekció után (48 cm hiány, azaz +11,3%) a korrigált érték 118,4, egészre kerekítve tehát MLC119.

A mélybölcsős tréler esetében az iterációs besorolási érték 104,9, ugyanazon szélességi korrekcióval 116,8, egészekre kerekítve MLC117. A mértékadó rakott fajlagos nyomatéki görbéket az ideális járművek görbeseregével a 8. ábra szemlélteti.



8. ábra: A rakott 11 tengelyes nehézgépszállító tréler (kék) és a mélybölcsős, 12 tengelyes tréler (szaggatott piros) fajlagos nyomatéki görbéje

Forrás: a szerző szerkesztése

Megállapíthatjuk, hogy a rakott trélerek MLC-besorolása összegzéses módszerrel 8 és 14%-kal nagyobb eredményre vezetett, mint a részletes besorolás elvégzése. A STANAG által engedett összegzés tehát a biztonságot növelte, miközben teljesen egyszerű és villámgyors megoldást adott az eseti jármű-kombináció együttes besorolására (3. táblázat). A példa rávilágít arra, hogy rendszeresített jármű-kombinációkra mindenképpen érdemes elvégezni a részletes iteráción alapuló besorolást is, mivel így kedvezőbb MLC-értéket kaphatunk, mint egyszerű összegzéssel. A rendszeresített jármű-kombinációkat tengelysúly-mérlegeléssel indokolt ellenőrizni besorolás előtt.

A STANAG 2021 az ideális járművek MLC-besorolásához járműoszlop vizsgálatát írja elő. Előírás, hogy az egymást követő járművek közötti távolság az elöl haladó jármű utolsó tengelyétől a követő jármű első tengelyéig 30,5 m legyen. Lánctalpas járművek esetében ez a távolság a lánctalpak felfekvési pontjai között értendő. Az előírás egyszerűsíti a számítást abból a szempontból, hogy nem kell figyelembe venni a jármű tényleges felépítményét, ami ezeken a pontokon adott esetben lényegesen túlnyúlik. Ugyanakkor a konvoj követési távolságának gyakorlatban való megtartásában ez jelentős nehézséget okoz.

3. táblázat: A példának vett trélerek MLC-besorolásának főbb adatai

	11 tengelyes tréler	**12 tengelyes mélybölcsős tréler**
üres tömeg	39,1 t	51,2 t
üres súly	383 kN	502 kN
üres MLC-besorolás	MLC35	MLC40
rakott tömeg	120,6 t	132,8 t
rakott súly	1183 kN	1302 kN
rakomány MLC	MLC93	MLC93
rakott MLC-összegzéssel	MLC128	MLC133
rakott MLC-számítással	MLC119	MLC117
összegzett/számított	108%	114%

Forrás: a szerző szerkesztése

Mivel a járművek MLC-besorolásához csak egyszerű kéttámaszú tartómodellt kell használni, a kéttámaszú erőjáték vonatkozásában elegendő e követési távolságot mint átlagértéket kezelnünk. (Az egyes hídszerkezet besorolásakor viszont a követési távolság bizonytalanságával részletesen foglalkozni kell.)

Az előző példa arra is rávilágít, hogy amennyiben a vizsgált jármű lényegesen hosszabb (esetünkben 17,25 m és 27,5 m), mint a besorolási iterációnál használt ideális jármű (MLC100 és MLC120 esetében is 13,11 m), akkor a vizsgált jármű konvojban való haladása bizonyosan nem lesz mértékadó sem nyomatéki, sem nyíróerő vonatkozásában. Éppen ezért a fenti számításban (7. és 8. ábra) egyszerűsítésül csak egyetlen trélerrel számoltunk. A hasonlító fajlagos nyomatéki görbeseregnél jól látható, hogy 65–70 m támaszköztartományban van egy iránytörés, ami az ideális jármű konvojhatásából származik. A vizsgált trélereink esetében ugyanezen töréspont 80–85 m-nél adódna.

Összegzés

A STANAG 2021 szerint egységes NATO-szabványt kell alkalmazni katonai járművek és hidak, kompok, tutajok teherbírási besorolásához. Cél a meglévő közúti hídjaink MLC-besorolása, különös tekintettel a NATO-szállítások szempontjából releváns útvonalak hídjai esetében.

Elemeztük a járművek osztályba sorolására vonatkozó szabályokat, amelyeknek pontos ismerete elengedhetetlen a kitűzött cél, a hidak teherbírási besorolásához. Bemutattuk, hogy az ideális járművek paramétersorozatai nem alkotnak letisztult sorozatokat, ellenben kedvezőtlen adatingadozások láthatók, elsősorban a kerekes járművek esetében.

Feltártuk, hogy az ideális járművek paramétereinek sorozatában a hidak teherbírási megítélésében külön vizsgálandó a pecsétterhelés esete. Ennek elemzése célszerűen az egyes polgári hídszabályzatok szerinti pecsétterhelések függvényében kezelendő.

Ugyanezen szabályozási belső aránytalanságot a polgári A és B jelű járműveknél is kimutattuk.

Vizsgáltuk két tipikus nehézgépszállítási elrendezésben a jármű-kombinációk MLC-besorolását szabvány szerinti összegzéssel és részletes besorolási iterációval. Megállapítottuk, hogy az egyszerű és gyors összegzés a biztonság javára 8–14%-kal nagyobb besorolást eredményez. Így javasolt a rendszeresített jármű-kombinációk részletes besorolását minden esetben elvégezni a kedvezőbb MLC-érték érdekében. A besorolás megbízhatóságához pedig javasolt előzetes tengelysúly-mérlegelést végezni.

Felhasznált irodalom

33.034/1910 K.M. rendelet: Szabályrendelet a közúti hidak tervezéséről, forgalomba helyezéséről, próbaterheléséről és időszakos megvizsgálásáról (Közúti hídszabályzat). Online: https://hidak.hu/konyvek/KHSZ1910.pdf

AEP-3.12.1.5 NATO Standard Military Load Classification of Bridges, Ferries, Rafts and Vehicles. Edition A Version 1, September 2017.

e-UT 07.01.12:2011 Erőtani számítás, Közúti hidak tervezése (KHT) 2. Útügyi Műszaki Előírás. Online: https://ume.kozut.hu/dokumentum/205

STANAG 2021 Standardization Agreement, Military Load Classification of Bridges, Ferries, Rafts and Vehicles. Edition 8, 14 September 2018 NSO/1074(2017) MILENG/2021.

Arndt, Rob [é. n.]: *Panzerkampfwagen VIII Maus (1943–1945)*. Online: https://web.archive.org/web/20130629194425/http://strangevehicles.greyfalcon.us/PANZERKAMPFWAGEN%20VIII%20MAUS.htm

Bartus Róbert – Kővári Ákos Róbert – Németh Gábor (2023): Észrevételek és javaslatok a készülő új e-UT 07.01.12 közúti hidak erőtani számítása – Útügyi Műszaki Előíráshoz. *Útügyi Lapok,* 11(18), 1–19. Online: https://doi.org/10.36246/UL.2023.2.01

Deák Ferenc – Havasi Zoltán – Nagy Zsolt (2001): A magyar katonai hídszabályzat kidolgozásának története és a vonatkozó NATO STANAG rövid bemutatása. *Közúti és Mélyépítési Szemle,* 51(5), 180–186.

Farkas Zoltán (2020): Új típusú nehézgépszállító szerelvények. *Haditechnika,* 54(5), 62–69. Online: https://doi.org/10.23713/HT.54.5.13

Gulyás András (2002): Az érvényben lévő hídtervezési előírások és a hidak terhelési osztályba sorolása a STANAG 2021 szerint. *Műszaki Katonai Közlöny,* 12(1–2), 53–68. Online: https://folyoirat.ludovika.hu/index.php/mkk/article/view/3181/2428

Gulyás András (2003): STANAG 2021 bevezetésének feladatai az országos konferencia tapasztalatai alapján. *Műszaki Katonai Közlöny,* 13(1–4), 125–133. Online: https://folyoirat.ludovika.hu/index.php/mkk/article/view/3086/2337

Gulyás András (2009): *Új építési technológiák alkalmazása a Magyar Honvédség béketámogató műveletei katonai építési gyakorlatában.* PhD-disszertáció. Zrínyi Miklós Nemzetvédelmi Egyetem, Katonai Műszaki Doktori Iskola. Online: https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/12155

Gulyás András – Havasi Zoltán (2003): Hidak terhelési osztályba sorolása. *Műszaki Katonai Közlöny,* 13(1–4), 105–124. Online: https://folyoirat.ludovika.hu/index.php/mkk/article/view/3085/2336

Hajós Bence (2023): Szempontok és javaslatok a közúti hídtervezés hasznos ideális jármű teherszintjének meghatározásához a készülő új Útügyi Műszaki Előírásban. *Útügyi Lapok,* 11(18), 30–43. Online: https://doi.org/10.36246/UL.2023.2.03

Hajós Bence (2024): Paradigmaváltás a közúti hídtervezésben a hasznos járműterhek vonatkozásában. Katonai alapterhek helyett polgári járműterhek bevezetéséről. *Műszaki Katonai Közlöny,* megjelenés alatt.

Havasi Zoltán (2007): *A Magyar Honvédség ideiglenes hídhelyreállítási képességeinek, lehetőségeinek vizsgálata.* PhD-disszertáció. Zrínyi Miklós Nemzetvédelmi Egyetem, Hadtudományi Doktori Iskola. Online: http://hdl.handle.net/20.500.12944/12072

Lukács László (2003): Hidak terhelési osztályba sorolása – országos konferencia. *Műszaki Katonai Közlöny,* 13(1–4), 103–104. Online: https://folyoirat.ludovika.hu/index.php/mkk/article/view/3084/2335

Polónyi Tibor (2018): A közúti és vasúti hidak teherbírásának számítása és osztályozása katonai módszerekkel, és az ilyen irányú fejlesztések jelenlegi helyzete. *Seregszemle,* 16(3–4), 46–56. Online: https://honvedelem.hu/files/files/116326/seregszemle_2018_34.pdf

Tóth András (2022): A Leopard harckocsi magyar típusváltozata: a Leopard 2A7HU. *Haditechnika,* 56(6), 27–32. Online: https://doi.org/10.23713/HT.56.6.05

HADMÉRNÖK
KATONAI MŰSZAKI INFRASTRUKTÚRA

19. évfolyam (2024) 1. szám 21–40.
DOI: 10.32567/hm.2024.1.2

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

Bepattanó kötések helye, szerepe, valamint 3D-nyomtatási technikával történő előállításának lehetősége a haditechnikában[6]

The Place, Role and Possibilities of 3D Printing of Snap-on Bindings in Military Technology

Absztrakt

A technika fejlődésével együtt jár az alkalmazott anyagok körének változása is. A gépjárműtechnikában egyre jobban elterjedtek a műanyag alkatrészek, amelyeket valamilyen módon egymáshoz vagy más anyagból készült elemekhez kell rögzíteni. A kötőelemek és kötési módok széleskörűsége biztosítja, hogy az elemeket oldhatóan vagy oldhatatlan módon kössük egymáshoz. A bepattanó kötések ismertek mindenki számára, mivel sok megvalósulási formája a háztartásokban is megtalálható, például a távirányító elemtartójának fedele, gyorskötöző vagy pedig táska- és övcsat. A gépjárműtechnikában a műanyag alkatrészek elterjedésével párhuzamosan a bepattanó kötések is terjednek

[1] Egyetemi docens, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Haditechnikai Tanszék, e-mail: vegh.robert@uni-nke.hu
[2] Építőmérnök, e-mail: denes.kalman.1975@gmail.com
[3] Robbanóanyag-ipari szakmérnök, e-mail: daruka.norbi@gmail.com
[4] Egyetemi docens, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Műveleti Támogató Tanszék, e-mail: kovacs.zoltan@uni-nke.hu
[5] Tanársegéd, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Műveleti Támogató Tanszék, e-mail: ember.istvan@uni-nke.hu
[6] A cikk a 2022-2.1.1-NL-2022-00012 számú „Kooperatív Technológiák Nemzeti Laboratórium” projekt a Kulturális és Innovációs Minisztérium Nemzeti Kutatási, Fejlesztési és Innovációs Alapból nyújtott támogatásával, a Nemzeti Laboratóriumok pályázati program finanszírozásában valósult meg.

és fejlődnek. A cikk ismerteti és bemutatja a különböző kötési módokat, főbb jellemzőiket és ezen kötésmódok között a bepattanó kötések helyét és szerepét. A 3D-nyomtatás mind nagyobb mértékben van jelen az alkatrész-előállításban a haditechnikai eszközök vonatkozásában is. A cikk megvizsgálja a 3D-nyomtatással készült bepattanó kötések előállítási lehetőségeit.

Kulcsszavak: 3D-nyomtatás, erőzáró kötés, alakzáró kötés, bepattanó kötés

Abstract

As technology evolves, so does the range of materials used. In automotive engineering, plastic parts are becoming more and more common, which then have to be fixed to each other or to other materials in some way. A wide range of fasteners and bonding methods ensure that elements can be fastened together in a releasable or non-releasable manner. Snap-fit fasteners are known to everyone, as many of their embodiments can be found in households, e.g. battery compartment cover for remote controls, quick fasteners or bag and belt buckles. As the use of plastic parts in the automotive industry spreads, snap-in joints are also spreading and developing. The article describes and explains the different fastening methods, their main characteristics and their placement and role of snap-fit among these fastening methods. 3D printing is increasingly taking its place in the production of parts for military equipment. This article examines the possibilities of producing snap-in joints using 3D printing.

Keywords: 3D printing, force-locking joint, form-locking joint, snap-on binding

Bevezetés

A műanyag elemek és alkatrészek egyre nagyobb mértékben terjednek a mai gépjárműtechnikában és ezen belül a haditechnikában is. Ezen műanyagból készült elemeket, alkatrészeket valamilyen módon össze kell kapcsolni, vagy pedig hozzá kell rögzíteni más elemekhez, akárcsak a fémből készülteket. A műanyag elemek kötéseire részben alkalmasak a különböző széles körben használt hagyományos kötőelemek és kötési módok, de megjelentek új kötések is, mint például a bepattanó kötések, amelyek kimondottan jól alkalmazhatók a műanyag elemeknél. A műanyag alkatrészek és vele együtt a bepattanó kötések általános előállítási módja a fröccsöntés, de egyre inkább terjedőben van a 3D-nyomtatás mint additív gyártástechnológia.

Ma már számos technológia és technikai megoldás létezik akár egyszerűbb, akár más módon nem megvalósítható, komplex formák 3D-nyomtatással történő hatékony előállítására, amelyeket egyre szélesebb körben és már nemcsak prototípusok készítésre használnak, hanem polgári vagy katonai területeken is. Alapanyagok tekintetében a műanyagok rendelkeznek a legszélesebb termékpalettával és így felhasználási körrel, és már bizonyították létjogosultságukat többek között az orvosi

protézisek, a robotika vagy éppen a fegyveralkatrészek, szerszámok, illetve speciális elektronikai megoldásuk területén is.[7]

Ezért érdemes lehet megvizsgálni a különböző kötésmódok ilyen formában történő előállításának és alkalmazásának lehetőségeit is, melyik milyen jellemzőkkel rendelkezik, és hogyan tehető alkalmassá a műanyag elemek kötésére. Vizsgálni kell például, hogy a 3D-nyomtatással előállított kötési mód, a bepattanó kötés, mennyire felel meg az elvárásoknak, és lehetséges-e ezzel a technológiával különböző kötési módokat előállítani úgy, hogy gazdaságos legyen, és alkalmazhatósági szempontból is maradéktalanul megfeleljen.

A gépek kisebb elemekből, úgynevezett géprészekből állnak, amelyeket állandó vagy ideiglenes módon kötnek össze. Az összekötésre többféle kötést és kötőelemet használnak, amelyek alkalmasak az erők és nyomatékok átadására. A kötéseket többféle szempont alapján csoportosíthatjuk, például a kötés kialakításának szempontjából, funkcionális vagy szerelhetőségi (oldhatósági) szempontból.

A kötés a kialakításának szempontjából lehet:

- erővel záró kötés (ékkötés, csavarkötés, szilárd illesztésű kötés, kúpos kötés, kúpos gyűrűs kötés, szorítókötés);
- anyaggal záró kötés (hegesztés, forrasztás, ragasztás, beágyazás és kiöntés);
- alakkal záró kötés (szegecskötés, peremezés, csapszegkötés, szegkötés, rögzítőgyűrűs kötés, reteszkötés, bordástengely-kötés, fogastengely-kötés, poligontengely-kötés, bepattanó kötés).

A kötés funkcionális szempontból lehet:

- teherviselő (amely erőt vagy nyomatékot ad át);
- rögzítő (az összekapcsolás mellett kisebb terhelés átadását is lehetővé teszi);
- fűző (csak összekapcsolásra alkalmas, terhelés átadását nem teszi lehetővé).

A kötés az oldhatóság alapján lehet:

- oldható kötés (az alkatrész jelentős sérülése nélkül szét lehet bontani, például az alakkal záró kötések a szegecskötés és a peremezés kivételével, valamint az erővel záró kötések);
- nem oldható kötés (az alkatrészt csak roncsolással lehet szétbontani, például az anyaggal záró kötések, a peremezés és a szegecskötés).

A zsugorkötést feltételesen oldhatónak nevezhetjük, mert oldás után az eredeti állapot az újbóli kötés után már tökéletesen nem állítható helyre.[8]

Erővel záró kötések

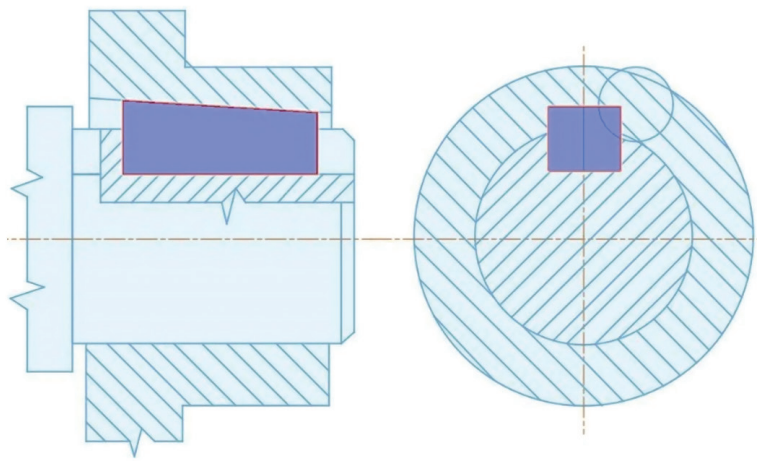
Az erővel záró kötés létrejöttéhez olyan működtető erő kell, amelynek hatására súrlódásos kapcsolat jön létre a két test között, és ez az erő akadályozza meg a testek

[7] Gál–Németh 2019.
[8] Zsáry 1984: 52.

egymáson történő elmozdulását. Mivel az érintkező felületek érdesek, a közöttük keletkező nyomásból származó súrlódóerő alkalmas az axiális és kerületi erők átadására. Az erővel záró kötések a túlterhelés hatására megcsúszhatnak, könnyen szerelhetők és újra felhasználhatók, viszont drágábbak, mint az alakkal záró kötések. 3D-nyomtatott alkatrészek esetében fontos lehet a felületek utólagos megmunkálása, mert a felület érdessége nagyban befolyásolja a kötés erősségét.[9]

Ékkötés

Az ékkötés alkalmas a tengelyek és a tengelyekhez kapcsolódó elemek (agyak) közötti oldható kapcsolat létrehozására. Az ékkötés létrehozásakor keletkező nagy súrlódási erő (a tengely és az agy közé befeszített önzáró ék) biztosítja az összekötött elemek szilárd kapcsolatát. Az ék lejtős kialakítású szabványos gépelem, amely pontos futást igénylő alkatrészekhez (például fogaskerekek) nem használható, mivel az ék feszítésének hatására excentricitás jön létre a tengely és az agy között (1. ábra). Az ékkötés előnye, hogy tengelyirányban is rögzít.



1. ábra: Ékkötés kialakítása
Forrás: a szerzők szerkesztése

Csavarkötés

A csavarkötések különböző anyagú elemek összekötésére alkalmasak, amelyek képesek teherviselő kapcsolat létrehozására. A csavarkötések alapvető elemei a külső menetes orsó (csavarorsó) és a belső menetes hüvely (csavaranya). A csavarkötés előnye, hogy nagy szilárdságú kötés létesíthető, amely dinamikus igénybevétel

[9] Zentay–Hegedűs–Végvári 2023.

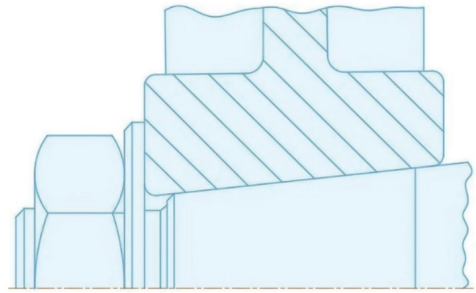
átadására is alkalmas. Rugalmas szorítóerő hozható létre vele, amely a terhelések fellépése után is megmarad. Bontható kötés, ami többszörös szét- és összeszerelést tesz lehetővé. A kötőelemek szabványosítottak, ennek köszönhetően a tömeggyártása olcsó. Hátránya, hogy a kötés létrehozása nagyobb időráfordítással jár és nagy a szerszámigénye. A csavarkötést lelazulás ellen biztosítani kell (például alátét, sasszeg, lemezbiztosítás). A kötés minősége függ a csavarfej és a csavaranya felfekvő felületeinek párhuzamosságától. Érzékeny a környezet korróziós hatásaira, ami az oldhatóságot nagymértékben befolyásolja. Műanyag elemek összekötése történhet önmetsző fémcsavarokkal vagy speciális betétek (insertek) használatával. Az insert alkalmazásának előnye az oldhatóság és a nagyobb kötésszilárdság. Az insertek a műanyag elembe beilleszthetők utólagos megmunkálással (például sajtolással, ultrahangos hegesztő berendezéssel), vagy pedig a fröccsöntő szerszámba helyezett insertre ráfröccsentik a műanyagot.

Szilárd illesztésű kötés

A szilárd illesztésű kötés esetén a tengely és az agy egymáson felfekvő felületei között túlfedés, vagyis negatív átmérőkülönbség van. A megfelelő nagyságú túlfedéssel összeillesztett alkatrészek felületein akkora tapadóerő jön létre, amekkora alkalmas az erőhatások és a csavarónyomatékok átadására. A szilárd illesztésű kötés a szerelés módjától függően lehet sajtolt vagy zsugorkötés. Sajtolt kötésnek hívjuk azt a kötést, ahol a tengelyt és az agyat nagy erővel egymásba sajtolják. Zsugorkötés létrehozásához az agyat felmelegítik vagy a tengelyt lehűtik (esetleg a kettőt együtt alkalmazzák), és szerelés, illetve lehűlés után jön létre a kötéshez szükséges nyomás. A szilárd illesztésű kötést többnyire nem oldható kötésként használják, mivel noha a kötés oldása és ismételt létrehozása lehetséges, az újabb összeszerelésnél általában kisebb túlfedés jön létre, így a teherbírás csökken.

Kúpos kötés

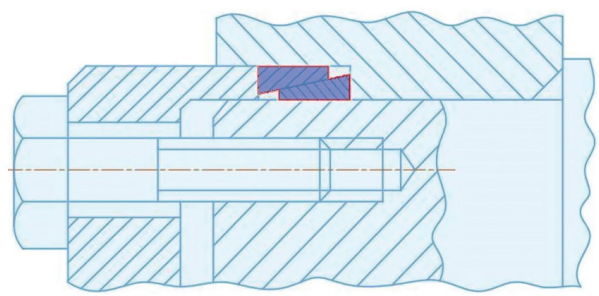
Kúpos kötésnél a rugalmas alakváltozást egy tengelyirányú feszítőerő hozza létre, amelyet elő lehet állítani csavarral vagy önzáró kötés létrehozásához beütéssel. A kúpos kötéssel összekötött alkatrészek a közös kúppalástон játékmentesen illeszkednek, amely kötés megfelelően központosít. A kúpos kötés a szilárd illesztésű kötéshez képest lényegesen drágább, mivel a megfelelő pontosságú kúpfelületek előállítása nagy gyártási pontosságot igényel. A kúpos kötés jellemző alkalmazási területe szerszámok befogása, tárcsák, tengelykapcsolók tengelyvégeken történő rögzítése (2. ábra).



2. ábra: Kúpos kötés kialakítása
Forrás: a szerzők szerkesztése

Kúpos gyűrűs kötés

Kúpos gyűrűs kötésnél a tengely és az agy közé helyezett, rugóacélból készült kúpos gyűrűpár viszi át a terhelést (3. ábra). A gyűrűkkel a sima tengelyre fel lehet erősíteni fogaskereket, tengelykapcsolót, amelyeket a kötés jól központosít. A nyomatékátvitel önzáró, a kúpos kötés alkalmas váltakozó és lökésszerű igénybevétel átvitelére is. A tengelyirányú feszítőerő hatására a feszítőgyűrűk egymásba tolódnak, és rugalmas alakváltozással kiegyenlítik a szerelés során létrejövő játékból adódó méretkülönbségeket. A gyűrűk befeszülnek a tengely és az agy közé, ezáltal kötőnyomást hoznak létre a felületeken. Több gyűrűpár alkalmazásával növelhető az átvihető nyomaték nagysága, de az első utáni gyűrűkre egyre kisebb feszítőerő jut. A kötés hátránya, hogy drágább, mint az ék-, a retesz- vagy a szilárd illesztésű kötés.

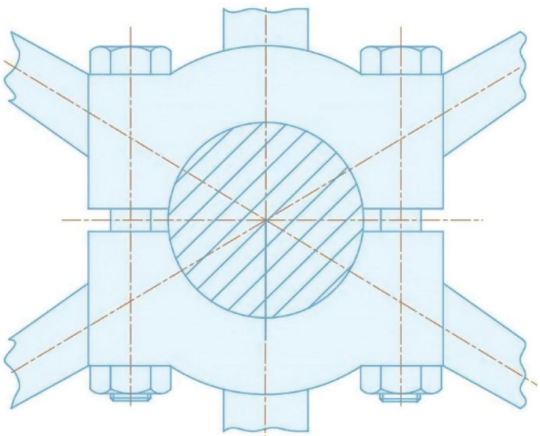


3. ábra: Kúpos gyűrűs kötés kialakítása
Forrás: a szerzők szerkesztése

Szorítókötés

A szorítókötést osztott vagy hasított aggyal lehet létrehozni, ahol a szorítást meg lehet valósítani csavarkötéssel. A felületek összeszorítása közvetlenül a tengely

mellett történik, az osztás vagy a felhasítás síkjára merőlegesen. A kötés kisebb, csekély mértékben változó nyomaték átvitelére a legalkalmasabb. A kötés előnye, hogy az agyat könnyen lehet állítani, mind hosszirányban, mind a kerülete mentén, és osztott kivitelnél a sugárirányú szerelés is megvalósítható (4. ábra).[10]



4. ábra: Szorítókötés létrehozása
Forrás: a szerzők szerkesztése

Anyaggal záró kötések

Az anyaggal záró kötések két alkatrész között olyan folyamatos anyagréteget hoznak létre, amely mindkét alkatrészhez olyan erősen kötődik, hogy alkalmas erők és elmozdulások átvitelére. Ez a kötő anyagréteg olvasztással, fizikai vagy kémiai kikeményítéssel hozható létre. A kötés szilárdságát a kohéziós (az anyagot felépítő atomok, illetve molekulák közötti összetartó erő) vagy az adhéziós erők (a különböző anyagok részecskéi, molekulái közötti tapadást okozó erő) határozzák meg.

Hegesztés

A hegesztés során munkadarabok egyesítése történik hővel, nyomással vagy mindkettővel, amely során kohéziós kapcsolat jön létre. A két egymással érintkező elemet felületük környezetében megolvasztják, esetleg külső anyagot (hegesztőhuzal) adnak hozzá. A hegesztés törött alkatrészek újraegyesítésére vagy kopott alkatrészek felületeinek javítására, kopásálló felületi réteg felrakására is alkalmas. A hegesztés lehet kötőhegesztés, amely két munkadarab egyesítésére alkalmas, vagy pedig felrakóhegesztés, amely során hozaganyagot hegesztenek a munkadarab felületére, a felületi

[10] Zsáry 1984: 169.

tulajdonság megváltoztatására vagy méretnövelésére. A nem fémes szerkezeti anyagok közül a hőre lágyuló műanyagok hő és nyomás együttes hatására hegeszthetők. A műanyagok hegesztésénél a cél a minél nagyobb szilárdságú kohéziós kapcsolat létrehozása. A hegedés létrejöttéhez szabad részecskemozgás, vagyis folyékony halmazállapot szükséges. A műanyag hegesztési technológiák lehetnek hővezetéses (például forrógázos), súrlódásos (például ultrahang) és sugárzásos (például lézersugaras) típusúak. A hegesztés feltételei, hogy közel azonos molekulaszerkezetű összeférhető anyagokat hegesszünk össze, optimális hőmérséklet álljon rendelkezésre, a felületeket összeszorító erő megfelelő időtartamon keresztül fennálljon, és a hegesztett kötés lehűljön.[11]

Forrasztás

Forrasztással fémes vagy nem fémes, de fémmel bevont elemek között lehet létrehozni kapcsolatot ömlesztett adalékfém segítségével. Az adalékfém olvadáspontja alacsonyabb a két összekötendő elem olvadáspontjánál. Az összekötendő elemeket felmelegítik, és a felületek közé juttatják a megolvasztott forraszanyagot, amely lehűlés után megdermed és összeköti az elemeket, így hozva létre adhéziós kötést. A forrasztás előnyei, hogy a forrasztási hőmérséklet alacsony, nem keletkeznek hő okozta deformációk, repedések, jó a villamos vezetőképessége és a tömítési tulajdonsága, és mivel a forraszanyagok rugalmassági modulusa kisebb az alapanyagénál, a kötés rugalmasabb. A forrasztás hátránya, hogy viszonylag kicsi a terhelhetősége, precíz előkészítést igényel a megfelelő minőségű kötés létrehozása, és a forraszanyagok (például ón, réz, ezüst) drágák. A forrasztás hőmérsékletétől függően a forrasztás lehet lágy (450 °C hőmérséklet alatt) vagy kemény. A lágy forrasztást kis szilárdságú kötések esetén alkalmazzák (például gépjármű hűtőtömbök, réz csővezetékek), ahol a tömítés az elsődleges szempont. A lágy forrasztás jól alkalmazható a villamos vezetékek kötéseinél, a kiemelkedő villamos vezetőképessége miatt.[12]

Ragasztás

A ragasztás az egyik legkorszerűbb kötési mód, amely roncsolás nélkül nem oldható, alapvetően anyagzáró, de a felületi érdesség miatt részben alakzáró kötés. Ragasztáskor az elemeket a közéjük juttatott ragasztóanyag rétege köti össze. A kötés szilárdságát a ragasztandó anyagok és a ragasztó belső szilárdsága, kohéziója, valamint a ragasztandó anyag és a ragasztó határfelületén fellépő erőhatás, az adhézió adja. A ragasztott kötés akkor megfelelő, ha az adhéziós erők legalább olyan nagyok, mint a kohéziós erők, vagyis a ragasztott kötés szétszakadása a ragasztott elemek anyagában vagy a ragasztóban következik be, nem pedig a ragasztó és az elem felületének elválása miatt. A ragasztott kötés előnye, hogy kevés helyet igényel, egyenletesebben oszlik

[11] Németh–Czigány 1999: 61–62.
[12] Jakab–Kodácsy 2011: 123–124.

el a kötésben a feszültség, kifáradási határa nagy, általában hidegen készíthető, jól tömít, korrózióálló, a vegyi hatásoknak ellenáll, és az összeragasztott elemek tulajdonságai nem változnak meg. A ragasztás varratmentes kötést biztosít, a felületek közül kifolyt ragasztó letörölhető. A ragasztás hátránya, hogy bizonyos ragasztóanyagok kötésének magas a nyomás- és a hőmérsékletigénye. Kicsi a fajlagos terhelhetősége, ezért viszonylag nagy felületek ragasztására van szükség, a hő hatására általában érzékeny, a magasabb hőmérséklet a kötésszilárdságot csökkentheti. A ragasztás kötésszilárdsága az idő függvényében fokozatosan csökkenhet. A ragasztási technológiák lehetnek ragasztószalagos és folyékony ragasztós (térhálósodó és nem térhálósodó ragasztók) típusok.

Beágyazás és kiöntés

Egyes alkatrészek nagyobb igénybevételnek kitett részeibe gyakran nagyobb szilárdságú elemeket építenek be öntéskor (például perselyek, betétanyák, egyéb erősítő elemek). Az erősítő elemek utólag is beépíthetők, ekkor az erősítő elemet egy megfelelően kialakított fészekbe kell helyezni, majd kiönteni. A kiöntéshez alacsony olvadáspontú fémet vagy hőre lágyuló műanyagot kell alkalmazni. A Nelson-féle Autothermik-dugattyú gyártásánál az öntőformába elhelyezett ötvözetlen acéllemez köré öntötték a dugattyú alumíniumanyagát, amely így egy bimetall fémkompozíciót alkotott.[13]

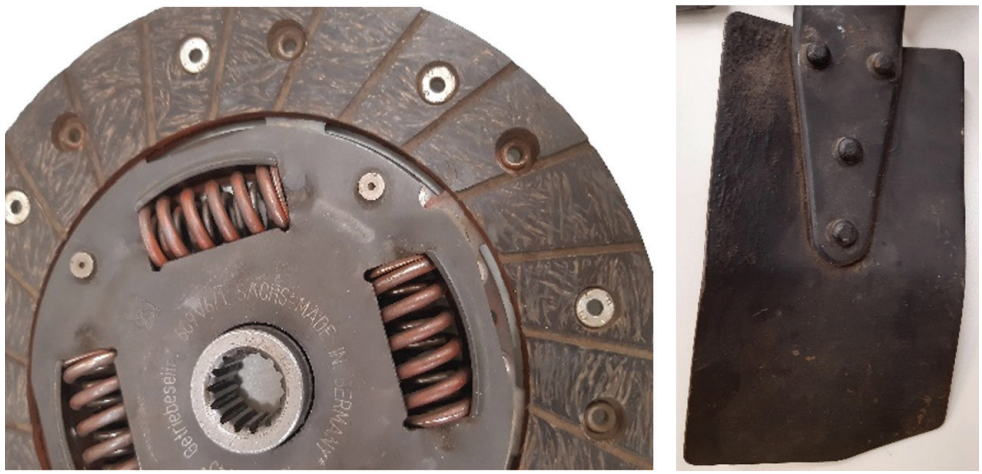
Alakkal záró kötések

A kötés szilárdságát a kötőelem kialakítása (amely meggátolja az elmozdulást) és anyaga határozza meg, sok változata ismert, amelyek többnyire oldható és ismételten helyreállítható kapcsolatot jelentenek. Különböző anyagok összekötésére is alkalmas.

Szegecskötés

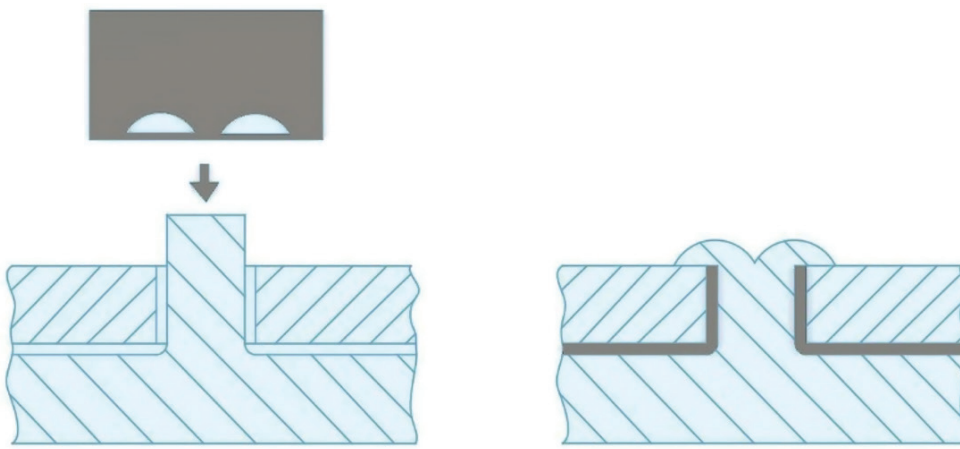
A szegecskötés nem oldható típusú kötés, csak roncsolással bontható szét. Alkalmazási területe széles körű például tengelykapcsoló súrlódótárcsájának súrlódóbetét-rögzítése vagy gépjárművek ventilátorlapát-rögzítése (5. ábra). Szegecskötések alkalmazásával különböző anyagú elemek is összekapcsolhatók. Előnye, hogy elkészítése gyors, olcsó és egyszerű, megbízhatóan és szilárdan kapcsolja össze az egyes elemeket. Hátránya, hogy a kötés szilárdsága kisebb más kötéstípusokénál, a kötés csak roncsolással oldható, és a kötés kialakítása nem esztétikus. A szegecskötések lehetnek teherviselő (például félgömbfejű szegecs) és nem teherviselő szegecskötések (például húzószegecs).

[13] Lukács 1998: 75–76.



5. ábra: Fém szegecskötés alkalmazása tengelykapcsoló súrlódótárcsánál és ventilátorlapátnál
Forrás: a szerzők szerkesztése

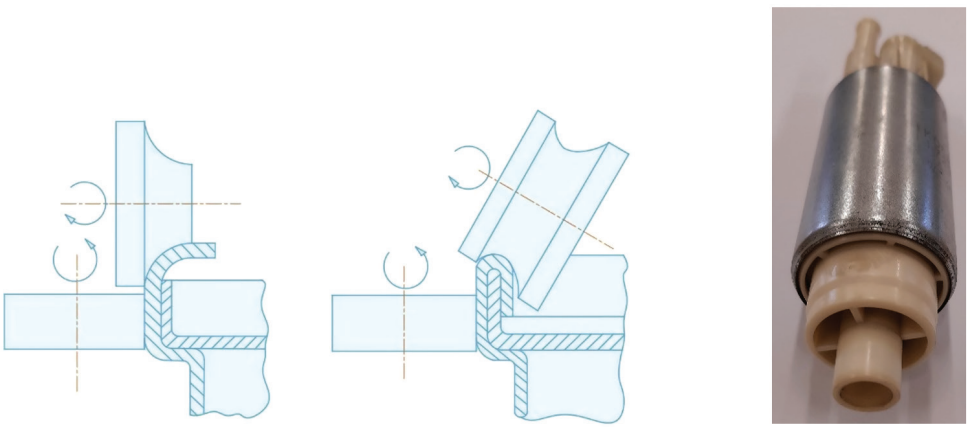
Műanyagok szegecskötését saját anyaggal is ki lehet alakítani, amikor az egyik elemen kialakított ellapítandó csapra illeszkedik a furattal ellátott ellendarab, majd a felmelegített szerszám által kifejtett nyomás hatására a megolvadt anyag felveszi a szerszám alakját, és létrejön a kötés (6. ábra).



6. ábra: Hőre lágyuló műanyagok szegecskötése
Forrás: a szerzők szerkesztése

Peremezés

Peremezésnek nevezik a lemezszélek tetszőleges görbületű behajlítását, valamint a cső alakú vagy az összekötés helyén csőszerűen kiképzett elemek és ezek záródarabjainak merev és oldhatatlan kötését. Peremezéssel az összekötött két alkatrész axiális és radiális irányban rögzített lesz, illetve az egymással szembeni elcsavarodásukat megakadályozza az erővel zárás. Peremezés során a peremezőszél kihajlításakor a külső övezet megnyúlik, befelé hajlításkor a belső övezet tömörödik. A peremezett alkatrésznek olyan anyagból kell készülnie, amely nem reped el az alakváltozás során. A peremezés hátránya, hogy nem tömít sem vízzel, sem gázzal szemben (7. ábra).[14]



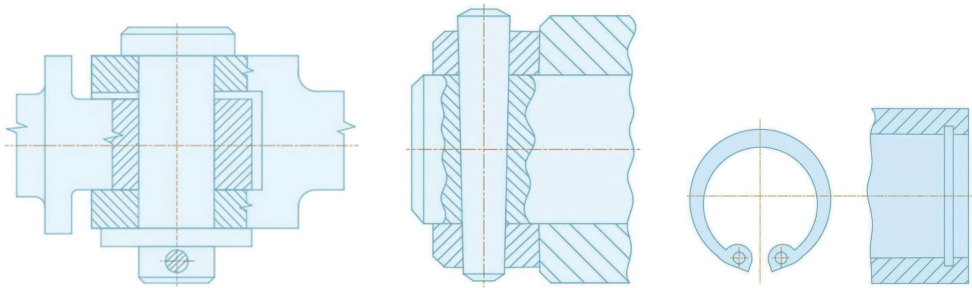
7. ábra: Peremezett kötés létrehozása és alkalmazása görgőcellás tápszivattyúnál
Forrás: a szerzők szerkesztése

Csapszegkötés, szegkötés, rögzítőgyűrűs kötés

A szegek és a csapszegek alkalmasak laza és szilárd kötések létrehozására. A csapszegeket általában csuklós kötésekben, valamint túlterhelés elleni biztosítóelemként alkalmazzák. A csapszeg furatból való kiesését sasszeggel, csavaralátéttel vagy csavaranyával akadályozzák meg. A különböző típusú szegeket általában központosításra és helyzetbiztosításra használják. A szegek három fő típusát különböztethetjük meg. Az illesztőszegeket levehető gép- és szerszámrészek helyzetének biztosítására, a rögzítőszegeket a gyakran oldható kötésekhez, a hasított feszítő csőszeget pedig a gyorsan készíthető és gyakran oldható kötésekhez használják.

A rögzítőgyűrűk egyszerű és olcsó kötőelemek, amelyek alkalmasak tengelyre fűzött alkatrészek (például gördülőcsapágy) vagy furatban levő elemek (például dugattyúcsapszeg) axiális irányú elmozdulásának biztosítására (8. ábra).

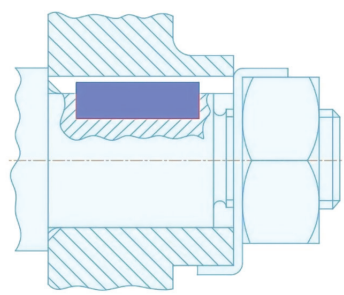
[14] Weltsch 2019.



8. ábra: Csapszeg-, szeg- és rögzítőgyűrűs kötések kialakítása
Forrás: a szerzők szerkesztése

Reteszkötés

Reteszkötésnél a tengelyben és az agyban kialakított horonyba helyezik el a reteszt, amely alkalmas erők és nyomatékok átadására. A reteszkötés a tengelykötések leggyakoribb módja. A reteszek lehetnek fészkes, sikló- vagy íves reteszek, amelyek nem lejtős kialakításúak, ezért kizárólag forgatónyomaték átadására alkalmasak, de tengelyirányú rögzítésre nem. A tengelyirányú erőt a retesz nem veszi fel, ezért az agyat a tengelyen axiális irányban rögzíteni kell. A retesz a horonyba szorosan van illesztve, de nem annyira, hogy a kötés kis erővel ne volna oldható (9. ábra).

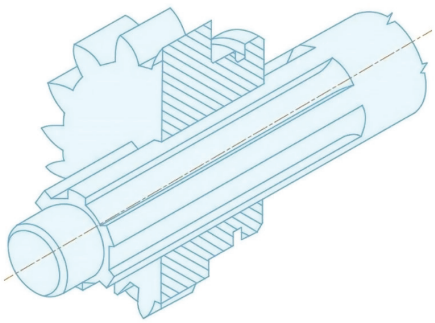


9. ábra: Reteszkötés kialakítása
Forrás: a szerzők szerkesztése

Bordástengely-kötés

A bordás tengelynél (agynál) a kerület mentén egyenletes osztásban helyezkednek el a bordák. A bordás kötéssel a nyomaték átadása egyenletes az egész tengely kerületén, ezért keskeny kötéssel is nagy nyomaték adható át. A bordástengely-kötés előállítása drágább, mint a reteszkötésé, mert nagyon pontos bordakialakítást kell készíteni mind a tengelyen, mind az agyban a megfelelő működés érdekében. A bordás kötéseket

többnyire gépjárművekben és szerszámgépekben használják párhuzamos, egyenes élekkel határolt, egyenes profilú bordázattal (10. ábra). A bordáskötés illeszkedő felületei gyakran el is csúsznak tengelyirányban egymáson (például sebességváltó kapcsolószerkezete,[15] fogaskereke). A bordás kapcsolat alkalmas dinamikus terhelések és váltakozó csavarónyomaték átvitelére.[16]

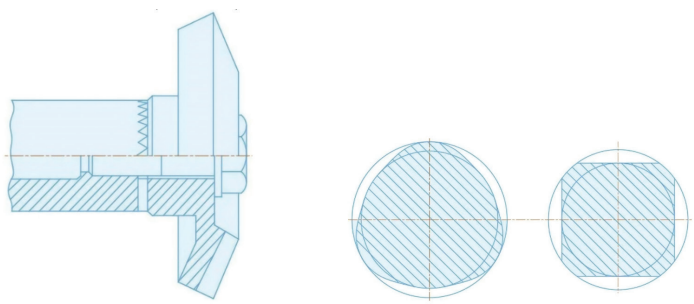


10. ábra: Bordástengely-kötés kialakítása
Forrás: a szerzők szerkesztése

Fogastengely-kötés, poligontengely-kötés

Fogastengely-kötésnél a fogakat lefejtő marással készítik, ami egyszerűbb és olcsóbb, mint a bordázat kötése, ezért az alkalmazása előnyösebb a bordástengely-kötésnél.

A poligontengely-kötés az erősen változó nyomatékok átadására jobban használható, mivel feszültséggyűjtő hatása kisebb. A poligon tengely profilja ívelt oldalú szabályos háromszög vagy négyszög. A profilt többnyire szoros illesztéssel készítik, laza illesztés esetén eltolható agyakhoz is alkalmazható (11. ábra).[17]



11. ábra: Fogastengely-kötés és poligontengely-kötések
Forrás: a szerzők szerkesztése

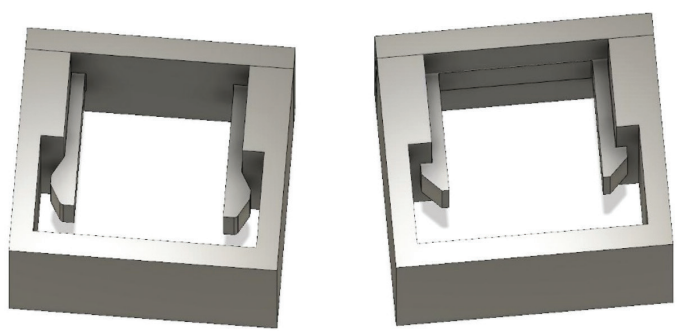
[15] Gyarmati 2023: 57.
[16] Fazekas 2013: 61–62.
[17] Jakab–Kodácsy 2011: 126–127.

Bepattanó kötés

A bepattanó kötés olyan alakzáró kapcsolat, ahol a két összeszerelendő elemet túlfedéssel illeszkedő szakaszon tolják át, amely során az egyik vagy mindkettő rugalmasan deformálódik. A kötés létrejöttekor a bepattanó elem terheletlen állapotba pattan vissza, majd addig marad ebben a helyzetben, amíg külső erőhatás a kötést bontani nem akarja. Az elektronikai eszközök miniatürizálásával és a műanyag alkatrészek egyre szélesebb körű használatával a kötéstípusok közül a bepattanó kötés mind nagyobb teret hódít. A kötés pontos illesztést tesz lehetővé alacsony költségekkel. A kötéssel létrehozott kapcsolat szereléséhez nincs szükség szerszámokra, és az elemek száma is nagymértékben lecsökkenhet. Jól megtervezett és kivitelezett kötés magas számú szerelési ciklust képes elviselni, miközben a kötés minősége és erőssége nem változik.

A bepattanó kötést többnyire műanyagok esetében alkalmazzák, de lehetséges fém-műanyag és fém-fém elemek kötése is. A bepattanó kötés műanyag elemek számára azért kedvező, mert a műanyagok a kis rugalmassági modulusuk[18] (Young-modulus) miatt nagy rugalmas alakváltozást tudnak elviselni, ezáltal a kötés rögzítésére szerelt állapotban nagyobb túlfedések állnak rendelkezésre. A bepattanó kötés további előnye, hogy nincs szükség külön kötőelemre, mivel a kapcsolatot az alapanyagból ki lehet alakítani, így a kisebb alkatrészek gyártása egyszerűbben megvalósítható.

A bepattanó kötéseket többféle szempont alapján lehet csoportosítani, például oldhatóság szerint lehetnek oldhatók és nem oldhatók (12. ábra). A geometria alapján csoportosítva lehet nyitott geometriás (karos és torziós típusú) vagy zárt geometriás (gyűrűs folytonos és gyűrűs felhasított típusú).



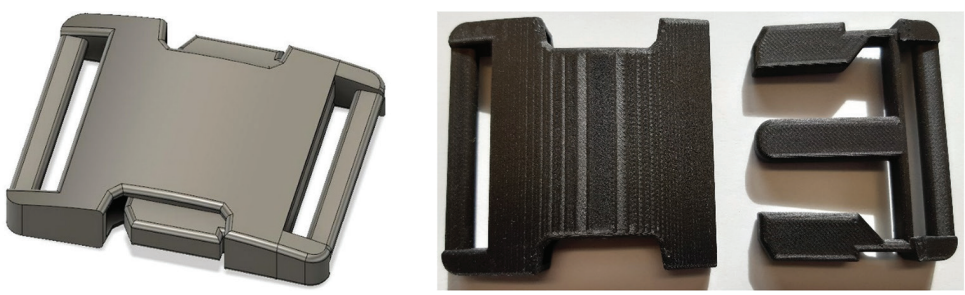
12. ábra: Oldható és nem oldható bepattanó kötések
Forrás: a szerzők szerkesztése

Az egyik legelterjedtebb bepattanókötés-típus a karos kötés, ahol a kötés egyik eleme a kar. A kar végének a kialakítása olyan, hogy be tudjon akadni a másik elem befogadó részébe, ezzel létrehozva a kötést. Többnyire csak az egyik elem, a kar deformálódik, a másik elem, a rögzítő pedig merev. Széles körű elterjedésének oka, hogy működése könnyen megérthető, egyszerűen gyártható, viszont nem minden területen alkalmazható

[18] A nyúlás változásának sebessége a feszültség függvényében.

egyedüliként. A kar keresztmetszete lehet téglalap, trapéz és félkör. A létrehozott bepattanó kötés csak szerelés irányú erőt tud felvenni, ekkor a kar feszített állapotba kerül. Amennyiben nem csak szerelési irányú erők érik a kötést, akkor biztosítani kell, hogy valamilyen szerkezeti elem ezeket az erőket felvegye.[19]

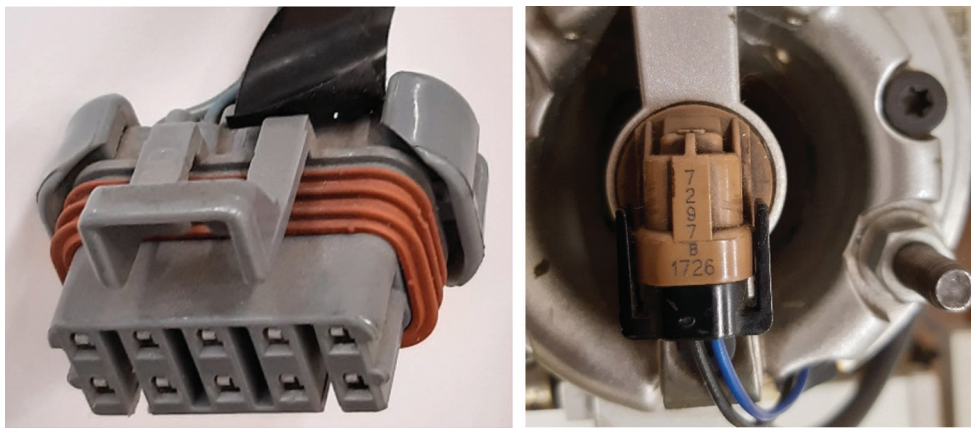
Túl nagy szerelési irányú erők esetén a kötés megszűnhet. A kar megengedett lehajlása a geometria mellett az anyagra megengedett nyúlástól is függ. A sokszor ismétlődő szerelések esetén a megengedett nyúlás az egyszeri szerelés értékéhez tartozó nyúlás 60%-a. A kötés létrehozásakor súrlódás lép fel az egymáson elcsúszó felületek között, amit a szerelési erővel kell leküzdeni. A kötés terhelhetőségét az oldáshoz szükséges erő határozza meg, megmutatja, hogy mekkora az az erő, amelynél az elemek még kapcsolatban maradnak egymással, vagy már szétválnak egymástól. Az oldáshoz szükséges erő a szerelési erővel ellentétes irányú. A karos oldható kötés rögzítő része úgy van kialakítva, hogy megfelelő nagyságú erő hatására az elemek el tudjanak mozdulni pozíciójukból, így a kapcsolat megszűnik. A nem oldható típusú kötések is szét tudnak válni egymástól kellően nagy erő hatására, de ekkor a rögzítőfülek deformálódnak, megcsavarodnak, és el is törhetnek. A kötés létrehozásához és oldásához szükséges erők a kötés létrehozásának sebességétől, a nyomástól és a felületek minőségétől is függnek. Nagyobb felületi érdességű anyagok kötéséhez nagyobb erő szükséges, mint a jobb felületi minőséggel rendelkezőknél.[20] A karos bepattanó kötés egy jellemző kialakítási módja az úgynevezett övcsat vagy táskacsat. A 13. ábrán látható övcsatot Fusion 360 tervezőprogramban rajzolták meg, majd nyomtatták ki a szerzők. A modell kinyomtatása Ultimaker S3 nyomtatóval történt PLA filamentből, valamint Markforged Onyx Pro nyomtatóval Onyx alapanyagból. Az elem nyomtatásához szükséges volt támasztékok alkalmazása, amelyek eltávolítása az övcsat belső részénél nem volt problémás, de a külső házrésznél ez komoly nehézséget jelentett a nehéz hozzáférhetőség miatt. Az Ultimaker S3 nyomtatóval történő nyomtatásnál lehetőség volt PVA (vízoldható filament) támaszanyag alkalmazására, amelynek eltávolítása sérülésmentesen történt. A 13. ábrán látható övcsat jelenleg is tesztelés alatt áll, többhetes használat során sem merült fel probléma vele kapcsolatban.



13. ábra: Övcsat 3D-modellje és a kinyomtatott elem Onyx alapanyagból
Forrás: a szerzők szerkesztése

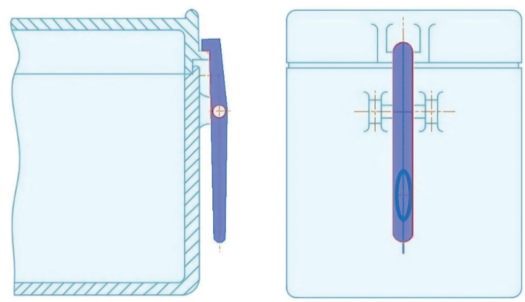
[19] Bonenberger 2016: 18–20.
[20] BASF Corporation 2007.

A karos bepattanó kötések a gépjármű-villamosság területén széleskörűen alkalmazottak a gépjárművek kábelkötegében, egyes elektronikus elemek összekapcsolására (14. ábra).



14. ábra: Gépjármű elektromos csatlakozói
Forrás: a szerzők szerkesztése

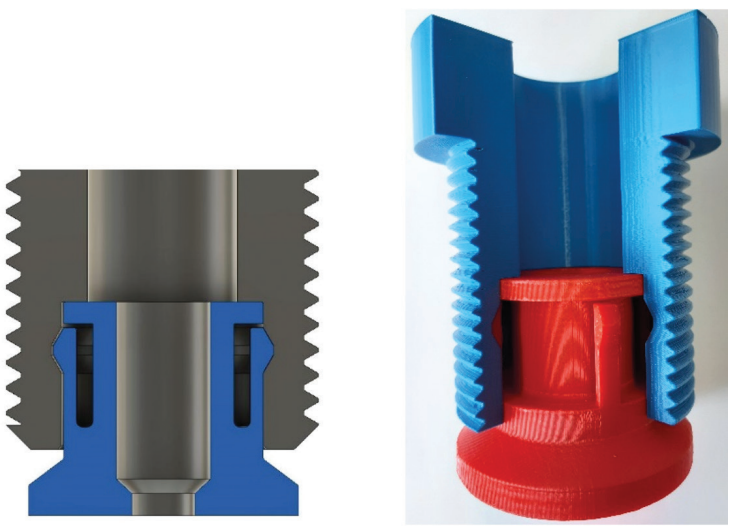
Torziós kötésnél a kötés létrehozására és oldására a csavarást használják ki. Az oldókar egyik végének megnyomásával a torziós rúd megcsavarodik, ezáltal a kar másik, rögzítő vége eltávolodik eredeti rögzített helyzetéből. Az erő megszűntével a kar zárófelülettel ellátott vége ismét zárási helyzetbe kerül (15. ábra). Olyan helyeken alkalmazható, ahol a karos kötés kialakítására nincs elegendő rendelkezésre álló hely. A torziós kötés előnye, hogy gyors és egyszerű.



15. ábra: Torziós bepattanó kötés kialakítása
Forrás: a szerzők szerkesztése

Gyűrűs kötésnél a bepattanó kötés a koncentrikus hornyok és bordák egymásba bepattanásával jön létre, ahol a külső és a belső hengeres felületek radiális irányú rugalmasságuk segítségével kapcsolódnak össze. A gyűrűs kötések szintén lehetnek oldhatók vagy oldhatatlanok, folytonos vagy felhasított típusúak. Összeszerelés után az alkatrészek feszültségmentes állapotban maradnak a szétszerelésig. A 16. ábrán látható

gyűrűs bepattanó kötés Fusion 360 programmal lett megtervezve, majd Ultimaker S3 nyomtatóval PLA alapanyagból kinyomtatva. A belső hengeres felület nyomtatása során, amely tartalmazza a pattanókötés-elemet, különös figyelmet kell fordítani a nyomtatás orientációjára. Célszerű nyomtatási helyzet első ránézésre a talpán álló pozíció, amit a nyomtató nagyon jó minőségben fel tud építeni, viszont szerkezetileg a végeredmény nagyon gyenge és gyakorlatilag használhatatlan. A belső kis kitöltési tényezővel történő nyomtatás, amely anyagtakarékosságot és nyomtatásiidő-csökkentést jelent, a kar számára nem megfelelő szilárdságú. Százszázalékos nyomtatási kitöltéssel túl sok anyagfelhasználás párosul, ugyanakkor a kar szilárdsága sem javul vele párhuzamosan kellő mértékben, a támaszték eltávolításakor a karok nagy része szintén letört. A fektetve történő nyomtatás jelentett megoldást, ekkor viszonylag csekély kitámasztással és nem teljes belső kitöltéssel nyomtatható volt az elem, amelynek a pattanó karja most már használható minőséget ért el, viszont ebben a pozícióban a hengeres felületek minősége elmaradt az állítva történő nyomtatástól.



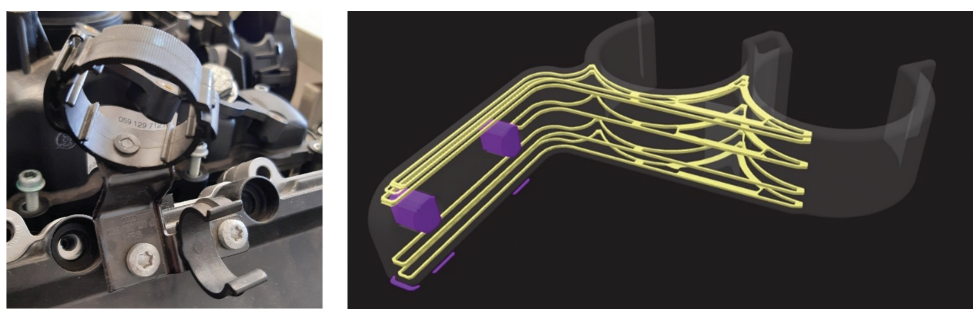
16. ábra: Gyűrűs felhasított típusú bepattanó kötés rajza és 3D-nyomtatással előállított makettje
Forrás: a szerzők szerkesztése

Gömbcsuklós kötésnél egy golyó vagy golyószegmens kapcsolódik össze a foglalattal. A gömbcsuklós bepattanó kötést többnyire térbeli mozgásátviteli elemeken alkalmazzák. A kötésben a gömbcsap merev, így a teljes alakváltozást a fészek veszi fel. A járműtechnikában alkalmazott burkolóelemek műanyag bepattanó gömbcsuklós rögzítésével csökken a rezgés és a zaj. A Böllhoff cég által gyártott SNAPLOC® gömbcsuklós kötés csak két darabból áll, amivel a tengelytávolság könnyen kiegyenlíthető, könnyen szerelhető, és olcsóbb a fémből készült változatnál (17. ábra).[21]

[21] Böllhoff Group [é. n.].

17. ábra: SNAPLOC® gömbcsuklós bepattanó kötés
Forrás: www.boellhoff.com/hu-hu/termekek/kueloenleges-koetoelemek/snaploc-rezges-es-zajmentesito-duga-szolhato-oesszekoettetes/

A bepattanó kötés használatára egy jellemző alkatrész a különböző csövek (például belső égésű motor hűtőrendszerének gumicsövei) vagy kábelkötegek rögzítésre szolgáló tartója. Ezek a tartók rögzített állapotban tartják a csöveket, kábeleket, amelyek ezáltal kevésbé rezegnek, és nem érnek hozzá mozgó vagy forró alkatrészekhez. A 18. ábra bal oldalán látható tartóelemek a belső égésű motorra vannak szerelve, és a motor működéséhez szükséges kábelek rögzítésére szolgálnak. A jobb oldalon látható tartó pedig az Unimog 1300 típusú terepjáró tehergépkocsi vízcsőtartójának 3D-modellje, amelyet üvegszál erősítéssel láttak el. A folyamatos üvegszál erősítés az – eleve mikroszénszál-erősítésű – Onyx alapanyag szilárdságát tovább növeli, ezáltal akadályozza meg az alkatrész meghibásodását, és biztosítja a hosszabb élettartamát.[22]



18. ábra: Kábelkötegtartó belső égésű motoron és vízcsőtartó 3D-modellje üvegszál erősítéssel
Forrás: a bal oldali ábra a szerzők szerkesztése, a jobb oldali ábra Gávay *2023: 230*

A bepattanó kötések számos egyéb alkalmazási megoldása ismert, például a gyors szerszámcsatlakozók, amelyek megkönnyítik és felgyorsítják egyes szerszámok gépbe történő befogását, vagy pedig adott csatlakozók gyors zárását és oldását. Mivel

[22] Hegedűs 2023: 62–66.

a bepattanó kötések lehetőséget adnak *ad hoc* kötések létrehozására, alkalmazásuk előnyös lehet katonai műveletek során, tábori körülmények között is.[23]

Összefoglalás

A cikk összefoglalta és csoportosította a különböző kötésmódokat, bemutatta főbb jellemzőit, előnyeit, hátrányait, a haditechnikában való alkalmazási lehetőségeit, valamint az egyes kötések műanyag alkatrészek rögzítésére vonatkozó megoldásait. Részletesen ismertette a különféle bepattanó kötéseket, azokat példákkal mutatta be a haditechnikában alkalmazott megoldásain keresztül. Ismertette egyes bepattanó kötések 3D-nyomtatással történő előállításának lehetőségeit és eddigi tapasztalatait. A bepattanó kötések helyének és szerepének megértésével lehetőség van további kutatások végrehajtására.

Felhasznált irodalom

BASF Corporation (2007): *Snap-Fit Design Manual.*

Bonenberger, Paul R. (2016): *The First Snap-Fit Handbook. Creating and Managing Attachments for Plastics Parts.* München: Carl Hanser Verlag. Online: https://doi.org/10.3139/9781569905968

Böllhoff Group [é. n.]: *SNAPLOC®.* Online: www.boellhoff.com/hu-hu/termekek/kueloenleges-koetoelemek/snaploc-rezges-es-zajmentesito-dugaszolhato-oesszekoettetes/

Fazekas Lajos (2013): *Válogatott fejezetek a gépészeti alapismeretekből.* Budapest: TERC Kft.

Gál Bence – Németh András (2019): Additív gyártástechnológiák katonai alkalmazásának vizsgálata, különös tekintettel a katonai elektronika területére. *Hadmérnök,* 14(1), 231–249. Online: https://doi.org/10.32567/hm.2019.1.19

Gávay György Viktor (2023): Logisztikai járművek alkatrészpótlása 3D nyomtatási technológia alkalmazásával. *Katonai Logisztika,* 31(3–4), 208–232. Online: https://doi.org/10.30583/2023-3-4-208

Gyarmati József (2023): Lánctalpas jármű kormányzása és ennek 3D modellezése. *Műszaki Katonai Közlöny,* 33(3), 51–61. Online: https://doi.org/10.32562/mkk.2023.3.5

Hegedűs Ernő (2023): Szálerősítéses anyagok 3D-s nyomtatásának hadiipari alkalmazási lehetőségei I. rész. UAV-k és könnyű járművek a haderőben és a katonai logisztikában. *Haditechnika,* 57(4), 62–66. Online: https://doi.org/10.23713/HT.57.4.12

Jakab Sándor – Kodácsy János (2011): *Szerelés és javítástechnika.* Budapest: Typotex.

Lukács Pál (1998): *Új anyagok és technológiák az autógyártásban I.* Budapest: Maróti-Godai.

[23] Végvári 2023.

Németh András – Czigány Tibor (1999): Hegesztett poliamid állapotvizsgálata és törési tulajdonságai. *Gép,* 51(5), 59–62.
Végvári Zsolt (2023): A 3D nyomtatás felhasználási lehetőségei a műveleti logisztikában. *Katonai Logisztika,* 33(1–2), 177–198. Online: https://doi.org/10.30583/2023-1-2-177
Weltsch Zoltán (2019): *Járműipari kötéstechnológiák.* Budapest: Akadémiai. Online: https://doi.org/10.1556/9789634543305
Zentay Péter – Hegedűs Ernő – Végvári Zsolt (2022): A 3D-s nyomtatás és katonai alkalmazásának lehetőségei 3. rész. *Haditechnika,* 57(2), 57–62. Online: https://doi.org/10.23713/HT.57.2.11
Zsáry Árpád (1984): *Gépelemek I. rész. Szilárdsági méretezés, kötések és kötőelemek, csővezetékek, tartályok, tengelyek, tengelykapcsolók.* Budapest: Tankönyvkiadó.

HADMÉRNÖK
KÖRNYEZETBIZTONSÁG

19. évfolyam (2024) 1. szám 41–54.
DOI: 10.32567/hm.2024.1.3

Árpád Győző-Molnár,[1] Lajos Kátai-Urbán,[2] János Bleszity[3]

Possibilities for Improving the Technical Equipment of Disaster Management Mobile Command Points

Abstract

The use of disaster management command centres is typically implemented in a static way, however, the experiences of the past period have shown that for their effective operation, it is necessary to use solutions that enable the monitoring of events, as well as rapid relocation and deployment. An obvious solution for creating the aforementioned capabilities is the use of mobile command centres to support driving groups. Currently, the professional disaster management organisation has several devices that can be used as mobile command points, but their capacity does not allow the work of larger teams. The purpose of this thesis is to examine capabilities, with the implementation of which both the capacity of the disaster management organisation and the effectiveness of the interventions can be increased, taking into account domestic and international development trends.

Keywords: disaster management, mobile command centeres, development, technical equipment, Hungary

[1] Civil Protection Supervisor, Disaster Management of Orosháza, e-mail: arpad.gyozo@katved.gov.hu
[2] Associate Professor, Head of Department Ludovika University of Public Service Institute of Disaster Management Department of Industrial Safety, e-mail: katai.lajos@uni-nke.hu
[3] Professor Emeritus, Ludovika University of Public Service Institute of Disaster Management, e-mail: bleszity.janos@uni-nke.hu

Introduction

The use of operational work units or command groups and mobile command points (MCPs) is common in the armed forces and various law enforcement and crisis response agencies. In the Hungarian professional disaster management organisation, the National Directorate General for Disaster Management, Ministry of the Interior (NDGDM), there are groups working in a complex, interdependent, hierarchical, but also independent and autonomous way for the operational control of emergencies. The operational work units follow the organisational structure of the NDGDM, which allows for the creation of operational groups at national, regional (county) and local levels.[4] However, the operating place of these groups is static and predefined.

Given the nature of the damage, there may be a need for equipment capable of dynamically tracking events, which can be deployed quickly and allow groups of at least limited numbers or tasks to work. In support of operational management, NDGDM and its subordinate bodies also have equipment that can be used as MCPs.[5]

The accelerated activity of elimination of damages and the increased information requirements, both in terms of reporting obligations as well as data provision and information, require that the persons responsible for the management of elimination of damages – the staff of the potentially established operational working bodies – start their activities with the help of modern MCP systems equipped with pre-configured computer workstations. This avoids delays in the core work related to the elimination of damages, in the establishment of the command centre and disruptions in the flow of information. These advanced systems, due to their mobility, can be of great help in starting the command activity as soon as possible.[6] In our view, the use of the above-mentioned state-of-the-art equipment can take disaster management operations to a new level and make them more efficient. Examining these MCP systems and suggesting improvements that also take into account cost effectiveness, and dislocation characteristics could further improve the effectiveness of the elimination of damages.

In view of the above, the research examined the experience of using MCP systems in disaster management and formulated recommendations for possible directions of development of operational work units and command points, taking into account domestic possibilities and conditions.

The objectives of the research included the following. To analyse and systematise the operational work units of national disaster management and the defence and security organisation system and their functioning, as well as the related legislative and internal regulatory environment, in order to formulate proposals for improving the organisation of the operational work units with the aim of increasing the efficiency of operational management and thus improving the effectiveness of elimination of damages.[7] To analyse and evaluate the existing MCP systems of the disaster management services, the domestic aspects of their deployment, the main requirements for

4 Muhoray 2019.
5 Győző-Molnár 2022.
6 Érces et al. 2023a.
7 Érces et al. 2023b.

their design and the experience of their use. Domestic and international experiences with MCP vehicles were systematised and, taking these into account, the development options for disaster management MCP systems were elaborated, considering the framework of the professional disaster management organisation.

The research topic is based on the study of the operational work units for the management of defence activities, the MCP vehicles and equipment that can be involved in operational management – already in use at the professional disaster management organisation – and other systems that support the mobility of the operational groups, in particular the possibility of operating the command groups in containers or tents.

Summary of the research results and conclusions

The professional disaster management organisation has undergone significant development in terms of its vehicle fleet and equipment over the past decade. As part of this development, the Disaster Management Radiation Reconnaissance Unit (Hungarian abbreviation: KSE) was established in seven counties in 2014.[8] In 2019, the Critical Infrastructure Protection Unit (Hungarian abbreviation: KIBE) was added to all county-level NDGDM disaster management directorates.[9] Both vehicles can be used as MCPs and, based on user experience, can be used effectively to support the activities of command groups during minor, containable damage events. However, the problem encountered with both equipment is that the limited capacity of the working space – designed to accommodate two people – prevents the work of larger groups or those scheduled for longer periods of use. Both vehicles are multi-purpose, and are therefore involved in the day-to-day activities of the disaster management services, primarily in relation to official procedures – inspections and surveys.[10]

The tents and tent systems currently used by the disaster management organisation:

- the 63M squad tent, which is commonly used by disaster management services
- so-called "party" tents without type designation, which can also be found in significant numbers in various organisational units
- pneumatic tents of various types (e.g. LGZ-5) or tents that can be quickly deployed, mainly for the HUNOR rescue services
- a limited number of advanced TAG 42 type pneumatic tents[11]

We believe that all tent systems are capable of meeting the MCP criteria. However, the disadvantages of tented systems are the heterogeneous nature of their types and the need to dismantle them before moving them to a new site, and then reassemble

[8] Győző-Molnár – Négyesi 2019.
[9] Győző-Molnár 2021.
[10] Cimer et al. 2021.
[11] Horváth 2013.

and reinstall them at the installation site. Another disadvantage is that a transport vehicle may be required to move not only the tent but also the equipment to the site.

The disaster management services have no MCP system installed in a container at present, but its development and implementation has started. Therefore, this article examines the specifications of the planned operational group container on the basis of the tender for its procurement.

Recommendations for development are based primarily on the current disposition of the disaster management organisation and the existing infrastructure and equipment. These would significantly simplify the acquisition and deployment of equipment and would be highly cost-effective and sustainable.

The three key requirements for the planned MCP equipment are as follows:

- the MCP equipment must be capable of accommodating at least two subordinates and a commander at one time, with the capacity to be expanded to allow larger teams to operate in suitable conditions
- the equipment can be quickly deployed on site and is operational within 4 hours
- it is capable of operating autonomously for at least 72 hours regardless of external conditions

An examination of the structure and functioning of the operational work units revealed the absence of a separate unit dedicated exclusively to reconnaissance tasks. In view of this, the creation of such a post in the operational groups is proposed in order to increase the efficiency of the groups' work.

Command point in a container

First of all, the potential applications of containerised operational work units should be explored, as container transport vehicles are currently available in the disaster management organisation. Based on their location, a nationwide network of stations can be established from which a group container can be dispatched to the site of the incident or group within 1 hour and be operational within 2 hours. The container transport vehicles and their personnel act as a stand-by unit for the professional disaster management organisation, which means that they are ready to start their journey to their designated destination as soon as possible after being loaded following an alarm, 24 hours a day.

At the time of writing, the professional disaster management organisation had 22 container transport vehicles of various designs, operated by the regional bodies shown in Figure 1.

The figure illustrates and confirms that the regional transport capacity to deliver the planned group container to the site of the incident is already available. The purchase of a transport vehicle is therefore not justified.

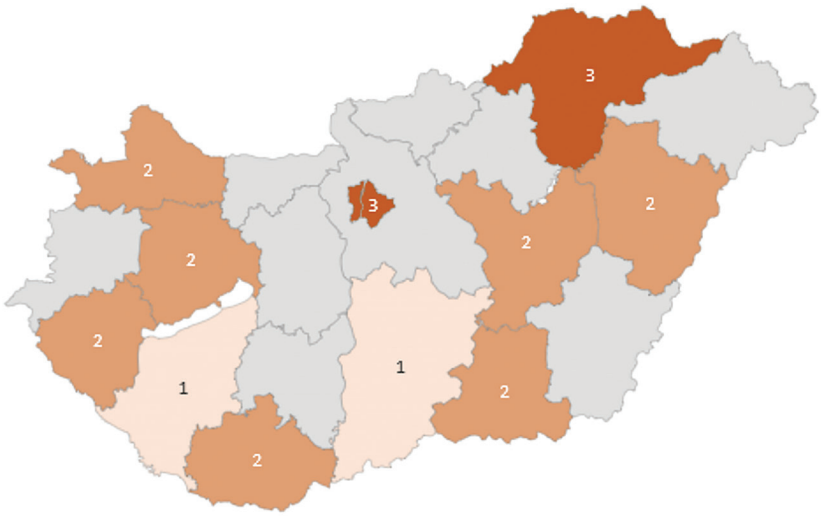


Figure 1: Number and disposition of container transport vehicles operated by the NDGDM and its regional bodies

Source: compiled by Árpád Győző-Molnár
Note: Measure No. 33/2020 of the NDGDM.

Moreover, it is not necessary to purchase new transport vehicles, as container transport vehicles have been continuously delivered in recent years, for example, two modern transport vehicles were delivered in 2021 within the project *KEHOP-1.6.0-15-2016-00021, EU Civil Protection Complex Modules.*[12] As a result, the vehicles that can be used for container transport generally meet the technical standards of their respective times.

In any case, the planned group container should have sufficient capacity to provide a reasonable number of workstations for the operation of the group, consisting of one main leader and two main subordinates, considered to be the basic staffing level, and, if necessary, for the liaison officers of the partner intervention agencies.

The common specifications for the main MCPs described earlier in this chapter should be compared with the requirements of the *KEHOP-1.6.0-15-2016-00021 Mobilizable Command and Control Point* tender, which is currently being implemented.[13]

The characteristics and the two main components of the planned command point container were formulated by the NDGDM in the above-mentioned public procurement tender as follows:

- one container transport system with sufficient load capacity to be placed on a semi-trailer, from a deployment control container system
- and associated IT system components

[12] BM OKF 2021.
[13] See: www.kozbeszerzes.hu/ertesito/2022/0/targy/portal_403/megtekint/portal_12424_2022/

When manufacturing and installing truck superstructures capable of autonomous operation, the units will incorporate the following:

- stand-alone power supply
- stand-alone air conditioning
- stand-alone camera system
- uninterruptible power supply
- remote access to IT and camera systems
- workstation for at least 6 people working simultaneously

where the work to be carried out includes installation tasks, meaning that the successful tenderer will also be responsible for the installation of the container and the associated IT system.

The MCP is a command-and-control support system for the NDGDM that is deployed at a safe distance from the incident site in a disaster situation. It serves as a communications node during prolonged operations such as major fires, floods and other natural and civil disasters that require the continuous and efficient work of the disaster management staff in the area.

"With a rapidly deployable command and control point, all the necessary IT and telecommunications functions and services can be brought together in a single area in a short period of time and moved to higher priority locations as required. The command-and-control point can be used effectively to hold meetings and coordinate tactical operations. All of these tasks are supported by state-of-the-art infocommunications equipment that provides direct network connectivity to the NDGDM's IT and telecommunications systems."[14]

The command centre includes several workstations, a videoconferencing system, presentation equipment and video surveillance functions to support analysis, operational control and decision making. The equipment provides the necessary conditions for the uninterrupted work and rest of the damage elimination leader and the personnel involved in the management.

There are many international examples of good practice in the use of container command points for disaster management. Among these, the German *Technisches Hilfswerk* (THW) should be considered and compared with the one planned for domestic implementation, as it operates a container MCP system with a high degree of operational autonomy. Power is self-supplied by a solar panel system with a capacity of six kVA. If the solar system does not produce enough electricity, a 10 kVA diesel generator is available to provide the necessary power supply.[15]

The system operated by THW is housed in two 20-foot containers with a command and meeting room and an operations control/communications room. The command and meeting room is primarily used for briefing and command work, but also offers the possibility of video conferencing. The operations control area is equipped with a range of analogue, digital and satellite communications equipment. Both emergency

[14] See: www.kozbeszerzes.hu/ertesito/2022/0/targy/portal_403/megtekint/portal_12424_2022/
[15] Bundesanstalt Technisches Hilfswerk 2018.

and long-range communications are provided by a retractable radio mast and a 2.4 m diameter ground satellite dish.

From a cost-effective point of view, a containerised command point is clearly advantageous. The group container, properly secured and loaded, can already contain all the equipment and fittings necessary to carry out the group's activities. This means that no extra time needs to be spent equipping the container, and it can be ready for use within a very short time of installation.

It is therefore worth continuing to study and develop in this direction, as the studies carried out show that there is no need for a set of units per county, but rather a regional approach covering several counties and taking into account the disposition of existing container transport vehicles. *Figure 1* clearly shows that the regional transport capacity required to deliver the planned group container to the site of the damage event is already available. In view of this and the procurement of recent years, there is no need to acquire a large number of transport vehicles.

Command point in a tent

The tents and tent systems used by professional disaster management services have already been described. A common feature and advantage of the tents systemised by NDGDM organisations is that their installation does not require significant prior training or preparation. It is essential to emphasise that the tents, which meet the technical specifications and operator requirements of the 21st century, are significantly lighter and consist of fewer elements than the previous generation of tents (e.g. the 63 M squad tent), thus simplifying logistical tasks, especially transport.

Modern, air-conditioned inflatable or pneumatic tents, such as the TAG 42 used by the disaster management body, have a net weight of only 180 kg and a floor area of ~42 m^2.[16] These specifications make it possible to transport the tent and its accessories to the site by 4 people and a truck with a sufficiently large loading area and, taking into account the experience gained during the installation, to have an equipped command point available within 4 hours to control the defensive operations. A significant advantage of this type of tent is that its interior space is highly variable and can be divided into several sections if necessary, allowing the different segments of the group to carry out their activities separately. An in-tent command point can be a good choice if the aim is to quickly establish national coverage, as all NDGDM county-level disaster management directorates have a set of this type of tent. A particularly positive aspect of the use of the tent is that, in conjunction with the KIBE, which is available on a countrywide basis, or the limited number of KSE vehicles, the MCP system, which is particularly suitable for independent operation and complies with modern principles, can be made available to disaster management.

A negative aspect of using a tent is its lower resistance to external weather conditions. A clear disadvantage compared to vehicle superstructures or container solutions is that the equipment and tools needed to assemble the tent have to be

[16] TAG 42 Inflatable Tent 2020.

transported separately to the site, so that once the tent is set up at its destination, it needs to be properly equipped. This solution also has a negative impact on the mobility of the command points designed in this way, as even the self-inflating tent can take at least 2 hours to dismantle, taking into account practical experience. The time required to evacuate the tent, which varies considerably depending on the number of items and equipment installed, must also be considered.

When examining international examples, it can be stated that self-inflating and inflatable systems, such as the TAG 42 system described above, are clearly gaining ground in disaster and crisis management operations.

Command point in a vehicle superstructure

The KIBE and KSE currently in operation belong to this family, as in all cases, the technology and equipment required to run the operational work units have been installed in the loading area.[17] There are several advantages to having the MCP in a vehicle superstructure, the most important of which is that it is easy to obtain commercially available base vehicles that can be later used as MCPs with only minor modifications.

The superstructure design allows for the availability of a ready-to-use MCP without any special preparation, with all the necessary equipment for command and control as well as communications installed, thus eliminating the need to install equipment prior to starting operations.

A very significant advantage of the MCP in a vehicle superstructure – similar to those already in service – is that it can be used continuously in peacetime to perform various tasks for disaster management services, such as the following:

- primarily, to support the conduct of official inspections
- secondly, passenger transport or
- freight transport after minor modifications

Consistent with Attila Zsitnyányi's findings, the disadvantage of the disaster management MCPs installed in the current vehicle superstructure is that the ability to expand the floor space is relatively limited by the superstructure's capacity and the vehicle's payload. The mass and space requirements of the IT and other communications equipment needed to manage the operation also severely limit the possibilities for expansion.[18] However, the dimensions of the current vehicles only allow for the deployment of the repeatedly mentioned smaller groups of personnel and thus the on-site management of defence tasks resulting from extreme weather events.

Consideration should be given to the procurement of vehicles with greater capacity and working space to complement the existing MCP vehicles, taking into account the space requirements to accommodate groups with larger numbers. There are a number of international examples of the use of MCPs in vehicle superstructures for disaster management purposes and the potential for their development, but there

[17] Győző-Molnár 2022.
[18] Zsitnyányi 2022.

is no typical size or capacity that clearly characterises this equipment. Depending on the dimensions of the base vehicle, the user's requirements and the intended application, the size range can vary from a passenger car to a semi-trailer.

Table 1: Comparison of KSE and KIBE vehicles

	Vehicle	
	KSE	**KIBE**
		
Year of entry into service	2014	2019
Number of systematised units	7 pcs	20 pcs
Type of vehicle	Fiat Ducato	Volkswagen Transporter
Core task	radiological reconnaissance, detection of illegal transport of radiological materials and prevention of release of dangerous substances	acting as a command-and-control point for incidents involving critical system elements
Operator staff	2 persons	2 persons
Permanent crew	none	none
Air-conditioned working space	yes	yes
Power supply from an external power source	yes	yes
Aggregator loaded	none	yes
Built-in EDR	yes	yes
Number of workstations in case of an MCP	2 pcs	2 pcs
Expandability of the number of workstations	no	yes
Off-road capability	exclusively built road network	limited

Source: compiled by Árpád Győző-Molnár

Reconnaissance post in operational work units

When examining the regulations of the disaster management organisation, it can be noted that there is no separate *reconnaissance* post in its operational work units.[19]

[19] Measure No. 12/2023 of the NDGDM.

In our view, it is essential to have an independent person or team to carry out specific (remote) reconnaissance activities (e.g. by using drones), to coordinate the reconnaissance tasks and to analyse and classify the data received from the reconnaissance activities in the event of incidents.

The studies show that although the groups are specialised in evaluation-analysis or operations control, and the tasks of these elements include the evaluation and management of reconnaissance data, the filtering of the data and information received by the group requires a separate division, given its heterogeneous nature, in order to receive information and data:

- from own organisation
- from partner professional intervention services
- and from other organisations involved

The person or organisational unit specialising in reconnaissance in the operational work unit is capable of filtering and organising this heterogeneous and diverse data from different sources in a consistent and systematic manner, based on principles defined in advance or by the leader, and then passing the synthesised data either directly to the leader or to the assessment analysis or operations control component for further action.

In addition to filtering, analysing and organising the data, it is important for the reconnaissance personnel to be able to manage the remote reconnaissance equipment that can be provided from the location where the groups are deployed or from the MCP. The most important of these, and increasingly used by operational forces, are drones, which have undergone significant development over the last decade. Along with this, the personnel handling the data obtained during reconnaissance can also carry out filtering, as already mentioned.

The main principles of the use of drones and aerial reconnaissance for disaster management, which are still relevant today, were formulated by *Rudolf Tóth* in an earlier work.[20] These include, but are not limited to, the following:

- fly or hover at low speed over the area of damage
- if necessary, take off and land within the damage area with little space, without technical personnel, technical equipment or external power source
- avoid, as far as possible, the need for runways or special control equipment, which can only be installed at high cost in or near the damage area
- the aircraft structures chosen and used in the damage area shall not require special operating conditions, it shall be simple and cost-effective to operate them
- they should be capable of continuous use, possibly on a rotating basis

The use of drones for aerial reconnaissance is well suited to both minor and major damage events. In such a case, if the drone is carrying out an activity that cannot be postponed in time, the drone pilot must consider the outcome of the operation. From a risk perspective, the performance of disaster management tasks is critical during and after a disaster. Prior to any aerial operation, it is always advisable to identify

[20] Tóth 2011.

the risk factors for the flight and, based on this, to communicate the risk factors of the operation to the operation commander or damage site commander in order to obtain a realistic picture. Following a risk assessment, if the drone can support the mission and contribute to the success of the operation, then it should be deployed. In addition to problems caused by the weather, other obstacles can affect the execution of operations, such as the release of hazardous substances into the air. For example, a toxic substance that adheres to the drone's frame structure and infects personnel upon return to the launch site, or even severe radiation contamination, which may result in irreversible malfunctions.[21]

This is particularly important when the technical equipment is at the disposal of the professional disaster management organisation in the form of drones, the acquisition of which is also included in the *KEHOP-1.1.0-15-2016-00003 operational programme*. The training of professional disaster management personnel in the use of drones was organised in 2022 with the support of the Ludovika University of Public Service, Faculty of Military Science and Officer Training, where the participants – including the author – were able to acquire the theoretical knowledge for the effective use of drones to be procured in the future.

The main tasks of the reconnaissance post with regard to the operational units are as follows:

- operating systemised reconnaissance equipment, such as drones, in order to conduct long-range reconnaissance and associated intelligence gathering
- analysing the reconnaissance data received from the intervention agencies involved in defence and from the professional intervention agencies
- gathering reconnaissance data from various sources and filtering it according to specified criteria for the analytical-assessment and operations management staff of the operational groups
- specialised management of the activities of the personnel carrying out reconnaissance at the damage site
- liaising with other members of the group/work units
- liaising with the reconnaissance personnel of partner agencies

In any case, the following minimum professional requirements are recommended for the staff to be assigned to the post of reconnaissance officer:

- at least an A1-B2 qualification to operate unmanned aerial vehicles, namely drones with a maximum take-off weight of 25 kg
- 3 years of professional experience in fire-fighting, technical rescue, civil protection or industrial safety
- at least a category B driving license
- access to disaster management databases and operational support applications

All this provides a good basis for groups with this capability to have access to continuous and accurate reconnaissance data. The volume of data and information coming in

[21] Hell 2022.

from the damage sites requires processing by specialised staff capable of interpreting and organising the information received.

Summary

We have focused primarily on domestic development opportunities that are feasible from a cost-effectiveness and organisational point of view, and on this basis, we make the following summary recommendations.

The disaster management MCPs currently installed in vehicle superstructures basically meet user requirements, but due to the limited capacity of their working space, it is necessary to purchase systems of larger dimensions.

For this reason, we believe that the use of group containers, which are already being systematised, is the right way forward. The container can be equipped with the operational tools and equipment ready for use, similar to the MCP installed in the vehicle superstructure. The only disadvantage of the planned systemisation of the group container is that the procurement of only one system is planned, which may delay the deployment due to the time needed to transport the MCP to the site of the incident and the time needed for installation.

On the other hand, the installation of technical, IT and communications equipment should be taken into account as a factor that increases the length of the installation period when using a tent. However, the use of a tent, together with the two MCPs already established, is a way forward and an option, which, using a hybrid system, can be used to temporarily extend the available working space to accommodate groups with larger numbers. Capacity for this is currently available in the system or planned for systemisation, but efforts should be made to acquire more advanced self-inflating systems when further tent systems are procured, as their installation time is significantly shorter than the previous types in the system.

Based on our investigations, the operational staff lacks an individual or organisational element solely responsible for reconnaissance tasks, for analysing complex reconnaissance data from multiple directions and channels, and for managing the reconnaissance assets at its disposal. In view of this, it is recommended that such a post be created in the operational groups in order to increase the efficiency of the groups' work.

References

BM OKF (2021): *Speciális tehergépjárművekkel bővült a katasztrófavédelem eszközparkja.* 5 May 2021. Online: https://katasztrofavedelem.hu/611/szechenyi-2020/19/251261/specialis-tehergepjarmuvekkel-bovult-a-katasztrofavedelem-eszkozparkja

Bundesanstalt Technisches Hilfswerk (2018): *Weltweite Kommunikation für die VN.* Online: www.thw.de/SharedDocs/Meldungen/DE/Veranstaltungen/internatio-

nal/2018/05/meldung_002_mcc_berlin.html?nn=922620&notFirst=true&idImage=10924654#sprungmarke

Cimer, Zsolt – Vass, Gyula – Zsitnyányi, Attila – Kátai-Urbán, Lajos (2021): Application of Chemical Monitoring and Public Alarm Systems to Reduce Public Vulnerability to Major Accidents Involving Dangerous Substances. *Symmetry,* 13(8), 1528. Online: https://doi.org/10.3390/sym13081528

Érces, Gergő – Rácz, Sándor – Vass, Gyula – Varga, Ferenc (2023a): Fire Safety in Smart Cities in Hungary With Regard to Urban Planning. *IDRiM Journal,* 13(2), 104–128. Online: https://doi.org/10.5595/001c.91474

Érces, Gergő – Vass, Gyula – Ambrusz, József (2023): Épületek károsító hatásokkal szembeni rezilienciájának jellemzői. *Polgári Védelmi Szemle,* 15(DAREnet Special), 117–130.

Győző-Molnár, Árpád (2021): Kritikus infrastruktúravédelmi bevetési egységek a katasztrófavédelem alkalmazásában. *Műszaki Katonai Közlöny,* 31(4), 79–90. Online: https://doi.org/10.32562/mkk.2021.4.6

Győző-Molnár, Árpád (2022): Mobil vezetési pontok a magyar katasztrófavédelemben In Földi, László (ed.): *Szemelvények a katonai műszaki tudományok eredményeiből III.* Budapest: Ludovika, 121–128.

Győző-Molnár, Árpád – Négyesi, Imre (2019): Katasztrófavédelmi sugárfelderítő egység mobil vezetési pontként történő alkalmazása. *Hadtudományi Szemle,* 12(2), 129–138. Online: https://doi.org/10.32563/hsz.2019.2.9

Hell, Péter Miksa (2022): *Drónok alkalmazhatóságának vizsgálata rendkívüli helyzetekben.* PhD dissertation. Budapest: Óbudai Egyetem.

Horváth, Zoltán (2013): A HUNOR hivatásos katasztrófavédelmi mentőszervezet tábori elhelyezésének sajátosságai. *Műszaki Katonai Közlöny,* 23(1), 138–153. Online: https://folyoirat.ludovika.hu/index.php/mkk/article/view/2538

Kátai-Urbán, Maxim – Bíró, Tibor – Kátai-Urbán, Lajos – Varga, Ferenc – Cimer, Zsolt (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

Muhoray, Árpád (2019): A katasztrófavédelmi műveletek tervezése és szervezése. In Hábermayer, Tamás (ed.): *II. Tolna Megyei Polgári Védelmi Munkaműhely.* Szekszárd: Tolna Megyei Katasztrófavédelmi Igazgatóság, 12–33.

Tóth, Rudolf (2011): A repülő eszközök alkalmazásának lehetséges területei és korlátai katasztrófák esetén. *Repüléstudományi Közlemények,* 23(2). Online: https://epa.oszk.hu/02600/02694/00055/pdf/EPA02694_rtk_2011_2_Toth_Rudolf.pdf

TAG 42 Inflatable Tent (2020). www.plastecomilano.com/en/special-products/self-erecting-tent-model-tag-29-tag-42-tag-56/

Zsitnyányi, Attila (2022): *A katasztrófavédelem iparbiztonsági műszaki technikai eszközrendszerének kutatása és fejlesztése.* PhD dissertation. Budapest: Nemzeti Közszolgálati Egyetem.

Legal sources

Measure No. 33/2020 of the NDGDM on the standby equipment of professional fire brigades and disaster management stations and the rules for the organisation of their services

Measure No. 12/2023 of the NDGDM on the establishment of disaster management operational working units, the conditions under which they operate, their organisational structure and their tasks

HADMÉRNÖK
VÉDELEMINFORMATIKA
19. évfolyam (2024) 1. szám 55–83.
DOI: 10.32567/hm.2024.1.4

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

Empirical Studies of Russian–Ukrainian War Related Fake News – Part 2[5]

Abstract

The Russian–Ukrainian war, which broke out on 24 February 2022, resulted in several paradigm shifts in cyberwarfare. One aspect of these changes is psychological operations. Russia and Ukraine have conducted extensive psychological operations campaigns to fulfil their war aims, 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 read 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] Senior Lecturer, Ludovika University of Public Service, Faculty of Public Governance and International Studies, e-mail: banyasz.peter@uni-nke.hu
[2] PhD student, Ludovika University of Public Service, Faculty of Public Governance and International Studies, e-mail: dub.mate@uni-nke.hu
[3] Student, Ludovika University of Public Service, Faculty of Public Governance and International Studies, e-mail: kugler.peti@protonmail.com
[4] PhD student, Ludovika University of Public Service, Doctoral School of Military Sciences, e-mail: inancsi.matyas@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 Programs of the Ministry of Innovation and Technology financed from the National Research, Development and Innovation Fund.

Introduction

The technological revolution of the 21st century, combined with the rapid development of info-communication tools (ICT) and the growing number of users on different online platforms, has identified new types of security risks in cyberspace. Consequently, the significantly increasing information and, more specifically, psychological operations, even as part of hybrid warfare, can be an excellent breeding ground for the prevalence of social media fears due to the lack of appropriate regulations on the part of service providers and the lack of a proper cybersecurity attitude on the part of individuals, among others. These platforms are also crucial as the various social media platforms are now the primary information and communication platforms, considered almost exclusive from Generation Y upwards.

Meanwhile, on 24 February 2022, Russia's attack on Ukraine broke out a war between two sovereign nations of an intensity not seen in Europe for decades, which, in the specificity of our modern information society, has thematised a significant part of online platforms from the very beginning to an unprecedented extent. In this context, it is in the primary interest of the opposing parties to convince their populations, from a domestic political point of view, the populations of the opposing country, and the world public opinion, from a foreign policy point of view, of their preferred interpretation of events.

Defending against such actions is a solemn task for a state, or in some cases a community within a state, because they exploit the basic human-based vulnerabilities, identifiable in the cognitive dimension, along which a community, or, more broadly, even the whole society, can be manipulated. The attackers, or more precisely the exploiters of these vulnerabilities, can be identified as individuals, cybercriminal groups, hacktivists, cyberterrorists, various intelligence services, or even state actors, or indirectly, for example, through the formation of opinion clusters, a wide range of service providers, commercial and economic groups, as well as non-state actors. As regards the analysis of the motives of the actors, it should be stressed that they are not limited to financial gain or to influencing decision-makers to deceive society, since the attackers may have as their objective the destruction of the fundamental values of democracy of which there have been several examples in recent years. Along these lines, it is essential to note that the various forms of influence are a challenge in countries that are not – fully – democratic and where attempts are made to make the democratic opposition impossible to influence, including through various information operations.

There are two main complementary objectives of our research:

- We aim to use sentiment analysis to measure the international public and Hungarian (more precisely, English and Hungarian) public opinion on the Russian–Ukrainian war, the posts and reaches of keywords and phrases related to Ukraine and refugees, and the emotional associations that society has with them, using so-called sentiment analysis. By examining the results of this empirical research, conclusions can be drawn regarding domestic and international perceptions, attitudes, and trends toward Ukraine and refugees.

- Our aim is also to analyse the perception of Russia and Ukraine in the context of the Russian–Ukrainian conflict from a network theoretical approach, as well as the support, the emergence of specific positions and patterns in the online space related to the countries and the Russian–Ukrainian war.

In the process of elaborating the research topic, we formulated the following hypotheses:

- H1: The number and reach of posts containing "Ukrainian" and "refugee" have followed the same trend in Hungarian and English.
- H2: Regarding the perception of refugees in Ukraine, both Hungarian users of online platforms and the global public tend to have a more positive emotional attitude towards online posts about Ukrainians and refugees.
- H3: From a network science perspective, isolated clusters are more likely to form on online social media platforms when promoting the Russian narrative versus the Ukrainian one concerning the Russian–Ukrainian war.
- H4: Network analysis can be effectively used to identify disinformation operations.

It should be noted that our initial study's extensive exploration of the scientific literature has yet to be replicated.

Methods

Following our research objectives, our research methodology can be structured along two complementary lines: sentiment analysis and network analysis.

Sentiment analysis

SentiOne is a platform for monitoring and analysing mentions and articles published on public Internet domains. In general, SentiOne's sources include websites and social media platforms. All monitored contents are indexed in one shared database, and results are available instantly after configuring a project. SentiOne's database includes over 20 billion mentions and expands second by second. Projects can be configured in over 70 languages. SentiOne uses its own unique language detection algorithms that combine linguistic features as well as additional metadata, which achieves 99.93% precision.

The system is deployed on over 200 dedicated servers and runs on an open-source stack. Each day, new domains are added to the system automatically and manually using web search APIs. Domains are searched using keywords in the topic configuration defined by SentiOne users.

SentiOne tries to gather as much data as possible for further analysis when crawling websites. It monitors domains with user-generated content like blogs, forums, news, and review sites. SentiOne uses a proprietary algorithm to extract data from unstructured HTML content. The data extraction process is streamlined by creating

manual XPath profiles for domains on which automatic algorithms fail or domains that use dynamic content.

Social media aspect within the sentiment analysis

SentiOne gathers data from various social media sites through their official APIs.

Regarding Facebook, public fan pages can be monitored, yet SentiOne cannot monitor private users even if their published content is marked as public. Most popular fan pages are discovered and added to the system automatically. New pages are searched using keywords defined in Topics. Twitter provides a public API for monitoring and indexing tweets. SentiOne searches for tweets using keywords from Projects and using streaming API that allows us, in the majority of cases, to gather new tweets instantly. From Instagram, SentiOne uses public API that allows to search for hashtags and users using keywords defined in Project configurations. Due to Instagram's new API rules (valid from 10 December 2018), there is a restriction that a single authorised account system can crawl at most 30 unique hashtags during a week timeframe. SentiOne is getting Instagram Stories from authorised accounts as well.

SentiOne uses public YouTube API to search for videos and comments. Due to API restrictions, mentions from YouTube can be stored for 30 days and cannot be visualised in the Analysis section.

SentiOne's sentiment analysis is based on research by John R. Crawford and Julie D. Henry. They analysed the Positive and Negative Affect Schedule (PANAS). Based on their study, SentiOne's developers created algorithms that help determine the author's emotional attitude to the discussed topic. SentiOne uses proprietary artificial intelligence algorithms to classify the overall sentiment of posts.

Since gender is relevant in this research, the software uses a knowledge-based approach in gender classification algorithms. The system automatically detects the author's gender based on the dictionary of over 35,000 names and analyses linguistic features that determine the author's gender.

Based on the above and the research objectives, we analysed the different emotional content and interactions on the Internet related to Ukraine and refugees according to the following criteria:

- The keywords are "Ukrainian/Ukrainian" and "refugee/refugee".

We intended to avoid pejorative terms and conceptual approaches when defining the keywords.

The analysis was conducted in English (as a world language) and Hungarian. (Even in Hungarian, the algorithm can determine the emotional attitudes towards content and access with ~87% accuracy.)[6]

The time interval defined and tested:

- 24 February – 20 December 2022. (Ten months after the outbreak of war to assess and study trends.)

[6] Bányász et al. 2022.

The amount of data collected:

- Content: 2,309,990 records
- Reach: 12,695,181,085 reactions

All of the analysed data are also available from open sources.

The other methodology of our research was the network analysis. This methodology allows us to investigate the spreading patterns of content on different platforms. For the network analysis, we used the software Netlytic. This text and social network analysis software can automatically summarise and visualise public online conversations on social networking sites, including Twitter.[7] The network analysis language was English (as the world language).

Results

As already mentioned above, the study aimed to analyse the sentiment related to the shared content and accesses, identify the contextual emotions that can be extracted from the context, and conclude the different language areas (more specifically, for the global/international context, English, and the Hungarian language in the domestic context). The languages studied were English (as a global language) and Hungarian.

The investigation focused on content and its accessions containing "Ukrainian" and "refugee" terms. Thus, we analysed these terms in both English and Hungarian about the following:

- the gender distribution of content sharers
- the chronological distribution of content
- the chronological distribution of reaches
- time distribution of positive and negative emotional content
- the aggregation of positive, negative, or neutral perceptions of the content
- most relevant platforms
- positive, negative, or neutral perception of content related to the most relevant platforms
- most relevant authors
- additional keywords appearing

Findings from the sentiment analysis

Figure 1 and Figure 3 illustrate the combination of the terms "Ukrainian" and "refugee" in English and Hungarian concerning the gender distribution:

[7] Bányász et al. 2023.

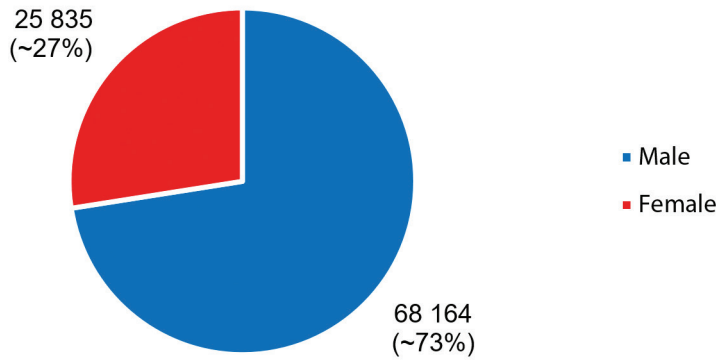


Figure 1: Gender distribution (per person) of Hungarian-language content (male indicated as blue, female indicated as red)
Source: compiled by the authors based on https://sentione.com

The pie chart presents the detailed distribution of gender references within the content related to "Ukrainian" and "refugee" in Hungarian. It reveals a pronounced disparity, with a significantly higher number of references to males, totalling 68,164, in contrast to the 25,835 mentions of females.

This discrepancy suggests that the conversation in this context tends to be more centred around or associated with male individuals.

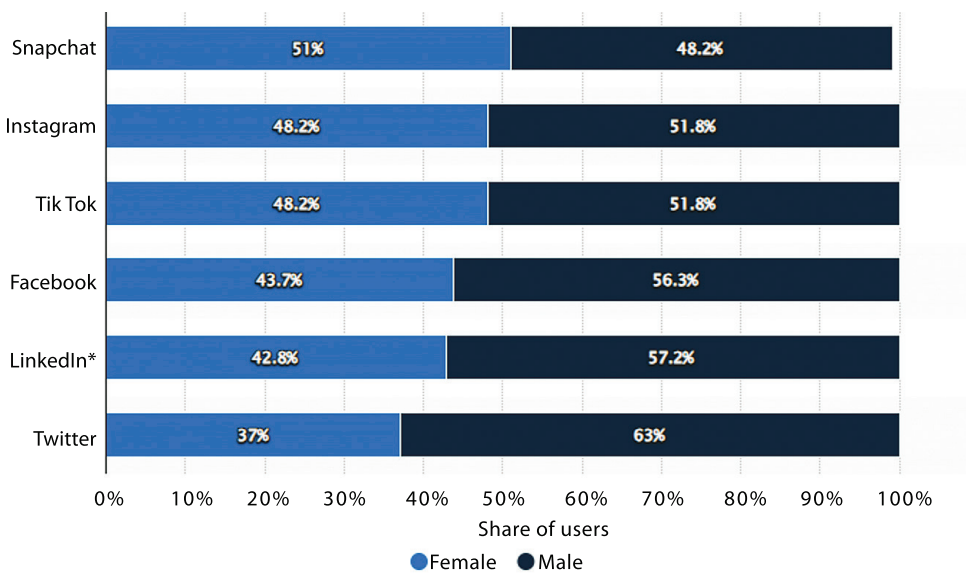


Figure 2: Gender distribution of social media platforms
Source: www.statista.com/statistics/274828/gender-distribution-of-active-social-media-users-world-wide-by-platform

Figure 2 shows the gender-oriented proclivities within social media platforms, demonstrating a preference towards a male-dominant share of users. This inclination parallels the observations made in Figure 1, where there is a notable male gender representation. Such a disparity is not merely indicative of the gender biases inherent within social media usage but also serves to contextualise the pronounced dominance observed in Figure 1.

The substantial male dominance, particularly in the context of the analysed keywords, suggests a broader trend of male-oriented engagement and representation. This trend reflects the underlying dynamics of social media interactions and possibly the societal narratives that drive the dissemination and engagement with content related to the specified keywords.

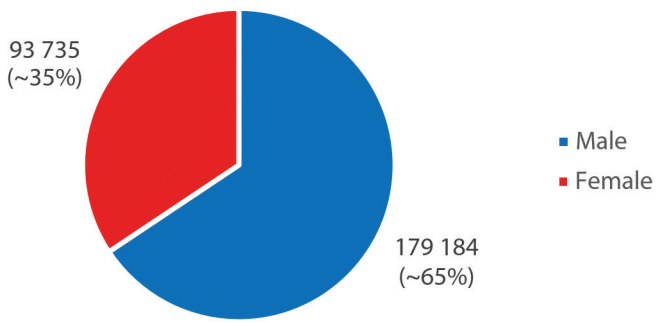


Figure 3: Gender distribution (per person) of English-language content
Source: compiled by the authors based on https://sentione.com

Shifting the focus to the Hungarian part, the analysis presented in Figure 3 reveals that the gender distribution within the Hungarian context for the specified keywords closely aligns with the international trend. This observation suggests a global consistency in gender representation across digital platforms, highlighting a pervasive male dominance. The cross-cultural similarity underlines the universal nature of gender biases in online content, suggesting that these trends reflect broader, global discourse patterns rather than isolated phenomena.

Figure 4 and Figure 5 represent the terms "Ukrainian" and "refugee" together in English and Hungarian concerning the chronological distribution of the content. Observing both data, we can clearly state that there was an initial conversation spike immediately after the war. We strongly believe that the quick drop in attention to the "refugee" keyword happened because the refugee crisis, while initially a hot topic, was resolved relatively quickly. Once the situation was addressed, public and media interest promptly waned, leading to a noticeable decrease in discussions about this topic. After the initial burst of attention, conversations about the refugee crisis occurred every day by June. This pattern shows that public focus can be intense but short-lived, especially when issues are resolved swiftly. It highlights how quickly topics

can move in and out of the spotlight on digital media platforms. After the average level, we observed that the keywords remain on topic. Additionally, the topic has shifted from the actual ongoing crisis to a broader discussion.

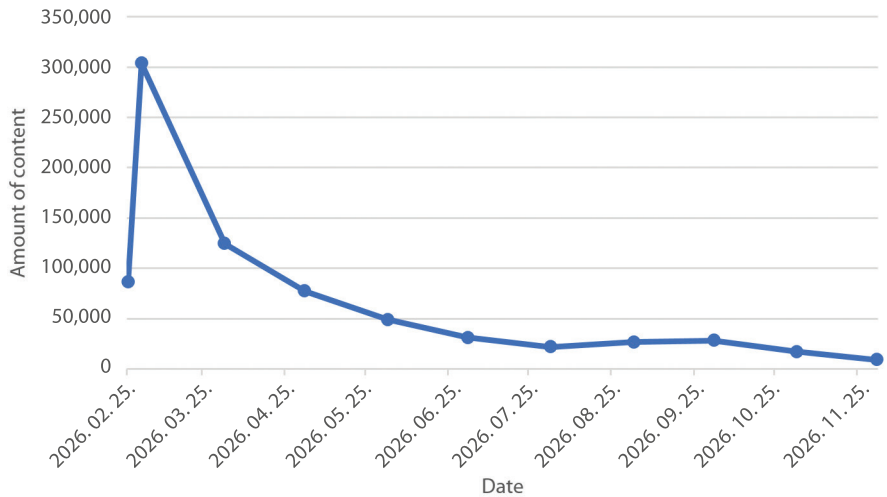


Figure 4: Chronological distribution of the number of Hungarian-language content (pieces)
Source: compiled by the authors based on https://sentione.com

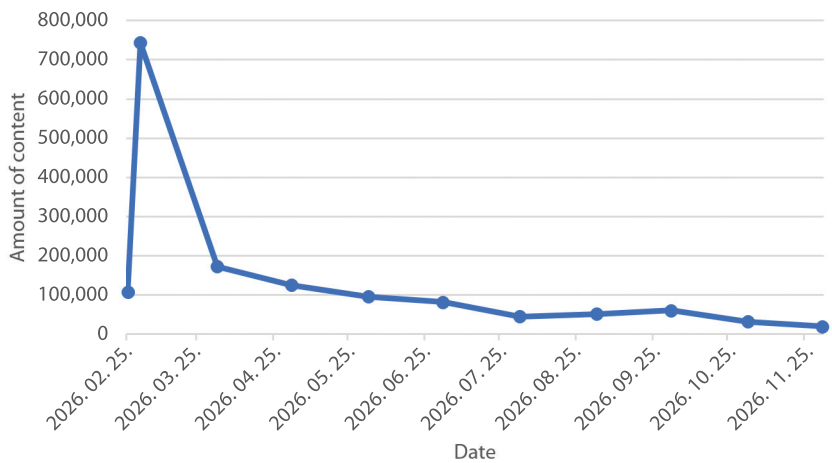


Figure 5: Chronological distribution of the number of English-language content (pieces)
Source: compiled by the authors based on https://sentione.com

In Figures 6 and 7, the terms "Ukrainian" and "refugee" are illustrated together in English and Hungarian concerning the distribution of accesses over time. We strongly emphasise that there's a significant difference between content distribution and

content reach. The content reach may overlap with users. One user might look at the same topic from multiple sources; this increases the reach but might not increase the reach of the content. The same spike and normalisation can be observed in the reaches as well. Comparing the two categories of datasets, we can highlight that the spike in reach was more significant than the spike in content. The conversation greatly exceeded the generated content. This indicates how users focused on discussion, not on content creation.

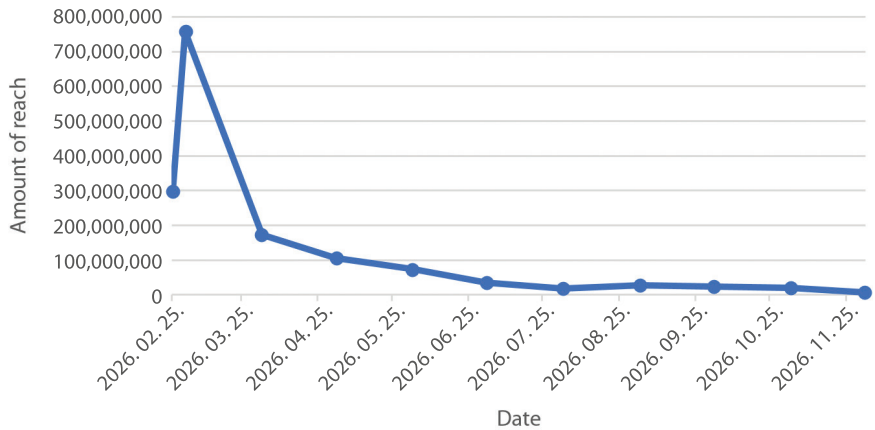


Figure 6: The chronological distribution of the number of reaches in Hungarian (pieces)
Source: compiled by the authors based on https://sentione.com

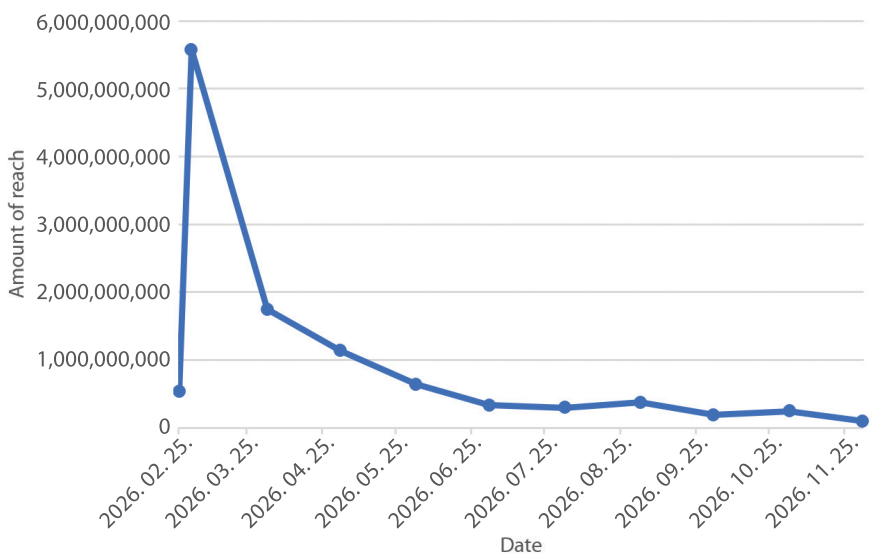


Figure 7: The chronological distribution of the number of reaches in English (pieces)
Source: compiled by the authors based on https://sentione.com

Revisiting our initial hypothesis, which posited that the frequency and dissemination of posts featuring the terms "Ukrainian" and "refugee" showcase parallel trends in both Hungarian and English languages, our observations confirm similar patterns across both linguistic contexts. The slight discrepancy observed is attributed to the fact that Hungarian speakers are comparatively less represented in the global Internet community than English speakers. Consequently, while the volume of such posts is lesser in the Hungarian context, the overarching trend aligns with that observed in English-language posts.

In Figures 8 and 9, the terms "Ukrainian" and "refugee" are presented together in English and Hungarian concerning the distribution of positive or negative perceptions of the content over time. Initially, there were many more negative mentions than positive ones. Over time, positive and negative mentions have decreased, but negative mentions have decreased faster, leading to a closer parity between the two. The rapid decrease of negative mentions displays how users had an initial negative feeling towards the Ukrainian refugees. We suspect as the situation unfolded, users gained a better understanding on the situation, therefore the negativity decreased.

In the English-language content graph, the positive and negative lines come closer together, suggesting a more balanced ratio of positive to negative mentions as time progresses. In contrast, the Hungarian-language content graph shows a consistent gap between the positive and negative mentions, with negative mentions consistently outnumbering positive ones.

Our analysis shows Hungary has a more negative view of the crisis than other places, ignoring neutral opinions found in Figures 10 and 11. This difference suggests that Hungarians are particularly concerned or critical about the situation. We left out neutral feelings to focus on the solid positive or adverse reactions. Reasons for Hungary's negative sentiment could include cultural factors or how the media shows the crisis. Understanding why Hungarians feel this way is essential for addressing their concerns.

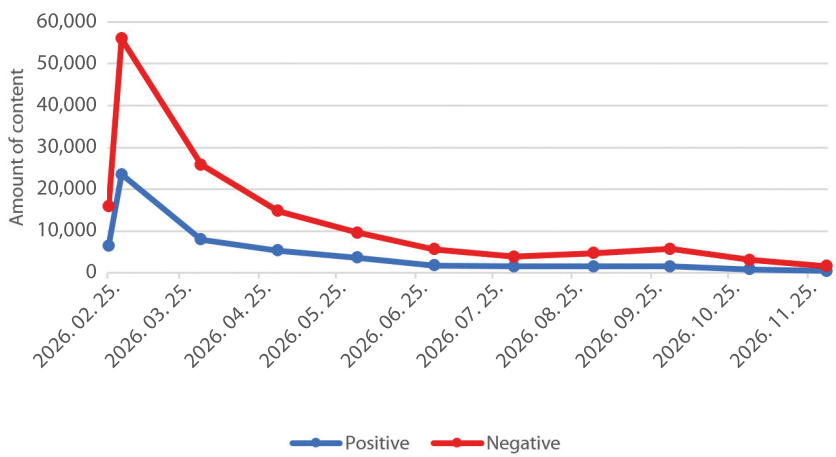


Figure 8: Distribution over time of positive and negative perceptions of Hungarian-language content (pieces)
Source: compiled by the authors based on https://sentione.com

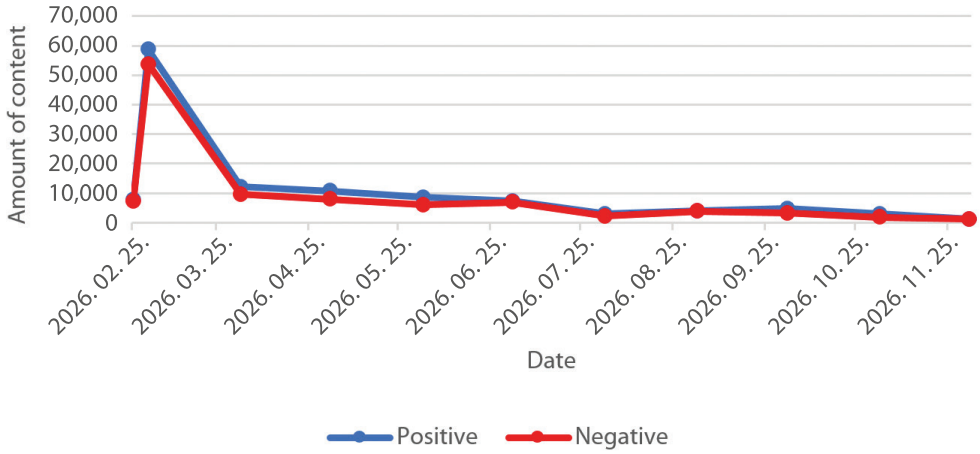


Figure 9: Distribution over time of positive and negative perceptions of English-language content (pieces)
Source: compiled by the authors based on https://sentione.com

In Figures 10 and 11, the terms "Ukrainian" and "refugee" are presented together in English and Hungarian concerning the aggregated positive, neutral, or negative perception of the content.

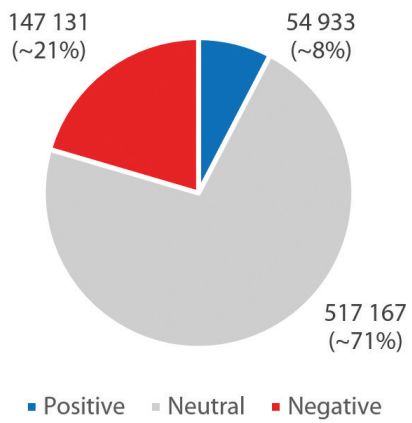


Figure 10: The distribution of positive, negative, and neutral (piece) sentiment in the Hungarian language entries
Source: compiled by the authors based on https://sentione.com

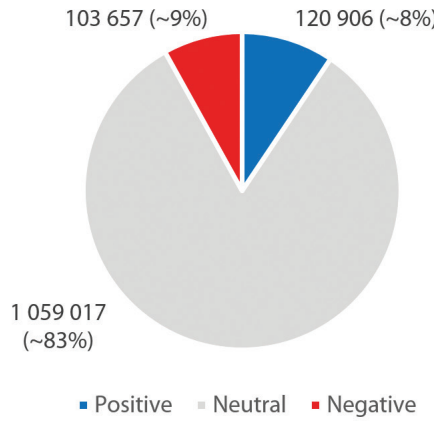


Figure 11: The distribution of positive, negative, and neutral (piece) sentiment in the English language entries

Source: compiled by the authors based on https://sentione.com

Hungarian and English texts show a larger share of neutral expressions in both, but with a noteworthy amount of negative sentiment, especially in English. The Hungarian data has fewer positive mentions than the English data, which has a relatively balanced spread between positive and negative sentiments. Both charts indicate a tilt towards neutral stances, with English texts displaying a more polarised sentiment distribution. Polarisation is a critical issue in our social media-driven world. The Capitol riot of 2021 is frequently characterised as a manifestation of political polarisation and the prevalence of echo chambers, which posed a significant threat to the security of the United States.[8]

Connecting to the second hypothesis – *Regarding the perception of refugees in Ukraine, both Hungarian users of online platforms and the global public tend to have a more positive emotional attitude towards online posts about Ukrainians and refugees* – we can observe a different result than the first hypothesis. We can say that the overall impression appears neutral, mainly involving straightforward reports.

When we delve into the actual emotions of the users, we find that the English language content supports our theory. The second hypothesis stands proven based on the English-language content. On the other hand, the theory does not hold for the content of the Hungarian language. This points to a notable contrast between the two languages, revealing subtle differences in how users react and feel across these linguistic contexts. Such distinctions may stem from cultural variances, the proximity of the conflict, different historical backgrounds (especially Hungary as a former USSR satellite state), or linguistic nuances that influence the expression and interpretation of sentiment online. Further investigation into these aspects could provide deeper insights into the dynamics of language and emotion in digital communication.

[8] Barrett et al. 2021.

To further understand the sentiments, we have compiled a dataset encompassing the 25 most prevalently utilised keywords within online content, analysed in both Hungarian and English languages. This dataset is systematically presented in Table 1. Notably, the keywords do not necessarily indicate a sentiment but a discussion. The keywords indicate what "topics" the conversations revolve around.

Table 1: Frequency of additional keywords in the content (number)

Frequency of additional keywords in the content			
Hungarian		English	
Keywords	Frequency of occurrence	Keywords	Frequency of occurrence
ukrajnai	43,803	ukrainian	48,126
ukrán	33,570	refuge	40,332
menekültek	32,011	russian	34,786
háború	28,775	country	31,803
ember	28,693	war	31,019
magyar	28,400	say	29,897
ország	27,101	report	28,931
orosz	25,618	nation	27,969
Magyarország	19,473	Russia	27,419
napping	16,882	help	26,365
év	14,881	Ukraine	24,834
európai	13,532	Putin	24,580
Oroszország	13,225	support	23,119
menekült	12,842	including	21,942
határon	12,109	state	21,669
ukránok	11,954	attack	21,477
részt	11,842	forces	21,215
kormány	11,280	continue	20,497
elnök	10,814	city	20,062
területen	10,172	officials	17,969
támogatást	9,342	border	17,646
kárpátaljai	7,396	civilian	16,279
Putyin	6,718	flee	15,370
Kijev	6,594	invas	14,807
Orbán	6,279	kyiv	13,107

Source: compiled by the authors based on https://sentione.com

Figure 12: Keyword cloud of content keywords
Source: compiled by the authors based on https://sentione.com and Table 1

From the dominant keywords, we have created a keyword cloud to visualise and understand this data better, as shown in both states, which primarily consists of the exact keywords regarding the two keyword sets. Hungarian and English spoken languages follow the same trend: they talk about Ukraine, Russia, Refugees, and political leaders, including their own. Both datasets show that war, country, and nation are universally significant. Figure 12 shows that support dominance is an important difference. The English dataset has a higher priority for support-related words, while in the Hungarian, that place is replaced with the keywords related to Hungary – as a nation. This also indicates a cultural difference between the Hungarian and English speakers. Based on the keyword analysis, Hungarians had an inner focus; they were concerned about how this war would affect Hungary and Hungarians, while English speakers were concerned how the war goes and how will it affect Ukraine and Russia.

Table 2 presents the top 6 online platforms with the highest number of posts in Hungarian and English.

Table 2: Frequency of appearance of entries (number of posts)

Frequency of appearance of posts			
Hungarian		**English**	
Platform	Posts	Platform	Posts
Facebook	510,435	Webpages	914,254
Webpages	259,860	Facebook	365,781
Blogs	1,805	Twitter	225,295
Twitter	1,586	Blogs	13,589
Forums	1,106	Forums	8,074
Instagram	53	Instagram	6,750

Source: compiled by the authors based on https://sentione.com

Upon initial examination, a significant disparity becomes evident in the popularity of various platforms across linguistic divides. Specifically, in the Hungarian context, Facebook and websites emerge as the predominant channels, overshadowing the relevance of alternative social media platforms. Conversely, within the English-speaking realm, Twitter and blogs secure a robust foothold regarding post frequency. This observation underscores the nuanced landscape of digital engagement, where linguistic and cultural factors play pivotal roles in shaping online platform dominance.

Table 3 shows the distribution of the positive, negative, or neutral emotional load of the Hungarian-language posts appearing on the most visited platforms.

Table 3: Distribution of sentiment in Hungarian on online platforms (pieces)

Sentiment distribution in Hungarian on online platforms (pcs)			
Platform	**Positive**	**Negative**	**Neutral**
facebook.com	41,849	103,964	364,622
Avg.hu	7,986	23,591	91,781
kuruc.info	2,075	7,923	26,533
vadhajtasok.hu	1,984	5,977	16,980
pestisracok.hu	227	2,025	5,721
444.hu	224	737	3,139
nemzeti.net	0	0	3,093
propeller.hu	101	852	2,138
mandiner. hu	72	402	2,194
ujszo.com	34	187	1,487

Source: compiled by the authors based on https://sentione.com

Table 4 shows the distribution of the positive, negative, or neutral emotional load of the English-language posts appearing on the most visited platforms.

Table 4: Distribution of sentiment in English on online platforms (pieces)

Sentiment distribution in English on online platforms			
Platform	**Positive**	**Negative**	**Neutral**
dailymail.co.uk	44,229	56,204	532,149
facebook.com	49,551	31,767	284,463
twitter.com	21,953	10,306	193,036
theguardian.com	708	1,293	11,211
yahoo.com	0	0	8,183
instagram.com	1,355	157	5,181
headtopics.com	0	0	5,669
heraldscotland.com	256	521	4,521
lawyersgunsmoneyblog.com	335	438	4,293
wonkette.com	327	391	3,601

Source: compiled by the authors based on https://sentione.com

As illustrated in Figures 10 and 11, the platforms exhibit a parallel sentiment distribution, yet a striking divergence is noted when comparing data across the English and Hungarian language spectrums. Specifically, within the English dataset, only Dailymail and Wonkette displayed a sentiment leaning more towards the negative than the positive. In stark contrast, the Hungarian dataset revealed a consistently more negative sentiment across every platform analysed. This discrepancy highlights significant linguistic and cultural variations in sentiment expression, suggesting a more pessimistic outlook amongst Hungarian language platforms than their English counterparts.

Table 5 shows the 30 authors with the highest number of hits for posts written in Hungarian and containing the famous words "Ukrainian" and "refugee".

Table 5: The most famous authors in Hungarian

The most famous authors in Hungarian						
Platform	**Name**	**Posts**	**Likes**	**Shares**	**Comments**	**Followers**
Facebook	Vujity Tvrtko	39	307,207	58,353	11,989	677,995
Facebook	Telex.hu	176	163,844	8,899	15,704	472,024
Facebook	24.hu	175	78,418	5,053	9,870	944,310
Facebook	HVG	174	71,105	4,094	8,884	627,575
Facebook	KárpátHír	383	67,706	5,879	6,404	53,629

The most famous authors in Hungarian						
Platform	**Name**	**Posts**	**Likes**	**Shares**	**Comments**	**Followers**
Facebook	Szijjártó Péter	9	65,810	3,517	3,838	367,715
Facebook	Migration Aid	82	54,515	17,254	1,370	54,026
Facebook	TV21 Ungvár	439	54,389	8,335	3,005	50,537
Facebook	nlc.hu	83	50,461	3,044	3,922	749,575
Facebook	Karácsony Gergely	13	48,927	3,888	1,470	307,449
Facebook	Elemi.hu	79	42,172	4,866	4,224	46,656
Facebook	Vadhajtások.hu	51	40,626	1,891	7,370	75,881
Facebook	Orosz Hírek	13	37,185	5,161	2,391	93,644
Facebook	Tibi atya	20	33,164	1,811	1,091	1 262,708
Facebook	Blikk	140	32,804	1,449	6,176	752,791
Facebook	Számok – a baloldali álhírek ellenszere	56	32,378	11,571	1,342	86,512
Facebook	Fidesz	7	28,366	3,998	3,606	358,081
Facebook	Márki-Zay Péter	15	27,436	2,033	2,624	171,217
Facebook	PestiSracok.hu	81	27,205	1,819	3,244	116,050
Facebook	Orbán Viktor	2	26,130	1,672	2,348	1 271,374
Facebook	444	52	24,956	1,995	2,958	394,142
Facebook	Egymillióan a magyar sajtószabadságért	31	24,933	2,443	1,587	184,711
Facebook	Tarjányi Péter – író és biztonságpolitikai szakértő	26	24,911	4,867	1,003	231,761
Facebook	hirado.hu	154	24,553	1237	3,006	358,092
Facebook	Juhász Zoli	177	23,244	14,020	1,302	74,104
Facebook	Jakab Péter	3	23,050	3,523	1,242	430,840
Facebook	Mága Zoltán	15	22,438	879	985	1 006,131
Facebook	ORIGO	102	21,395	877	2,378	515,078
Facebook	Hadházy Ákos	5	17,641	5,927	1,602	196,489
Facebook	atv.hu	33	16,953	1,401	3,384	389,841

Source: compiled by the authors based on https://sentione.com

Table 6 shows the 30 authors with the highest number of hits for posts written in English and containing both the keywords "Ukrainian" and "refugee".

Table 6: The most famous authors in English

The most famous authors in English					
Platform	**Name**	**Posts**	**Likes**	**Retweets**	**Followers**
Twitter	Jennifer Aniston (@jenniferaniston)	1	2,196,555	0	41,132,261
Twitter	The Kyiv Independent (@KyivIndependent)	47	366,873	61,657	2,215,066
Twitter	President Biden (@POTUS)	5	320,598	45950	28,489,051
Twitter	Reuters (@Reuters)	93	71,015	16,336	25,673,228
Twitter	The New York Times (@nytimes)	65	51,622	12,166	54,626,053
Twitter	Barack Obama (@BarackObama)	3	42,856	7,187	133,343,165
Twitter	MSNBC (@MSNBC)	13	37,603	6,406	4,711,945
Twitter	CNN (@CNN)	46	33,504	7,704	59,900,894
Twitter	Fox News (@FoxNews)	40	31,239	4,920	23,362,512
Twitter	ABC News (@ABC)	53	13,853	3,987	17,675,107
Twitter	AFP News Agency (@AFP)	54	12,879	4,998	2,426,336
Twitter	BBC News (World) (@BBCWorld)	8	10,698	1,710	37,522,394
Twitter	Sky News (@SkyNews)	68	10,245	2,057	8,274,837
Twitter	The Guardian (@guardian)	110	9,871	2,896	10,823,659
Twitter	The Associated Press (@AP)	10	7,934	2,617	16,081,511
Twitter	Greta Van Susteren (@greta)	48	7,539	697	1,163,273
Twitter	Binance (@binance)	8	4,318	865	10,026,131
Twitter	People (@people)	13	3,696	307	7,770,165
Twitter	ANI (@ANI)	11	2,542	250	7,403,258
Twitter	BBC News (U.K.) (@BBCNews)	7	2,429	625	14,792,028
Twitter	Bloomberg (@business)	36	2,333	729	8,850,280
Twitter	TIME	12	2,140	495	18,968,016
Twitter	Daily Mail Online (@MailOnline)	99	1,955	777	2,803,863
Twitter	Forbes (@Forbes)	25	1,764	477	18,405,854
Twitter	The Wall Street Journal (@WSJ)	13	1,605	427	20,389,886
Twitter	Newsweek (@Newsweek)	50	1,365	585	3,590,468
Twitter	UNICEF (@UNICEF)	12	1,327	431	9,323,334
Twitter	The Economist (@TheEconomist)	27	1,232	379	27,026,546
Twitter	The Washington Post (@washingtonpost)	4	834	242	19,965,825
most	TIME (@TIME)	13	390	117	19,426,733

Source: compiled by the authors based on https://sentione.com

Tables 5 and 6 again witness a discernible divergence in platform preferences between Hungarian and English speakers. Specifically, Facebook exhibits unequivocal dominance among Hungarian users, whereas Twitter holds a similar position of pre-eminence among English-speaking individuals. An interesting pattern emerges from the analysis: English-language content tends to have fewer posts, yet these posts achieve a broader reach or yield.

Conversely, data from Hungarian sources indicate a higher volume of posts. Moreover, the landscape of content authorship varies significantly between the two linguistic groups. In the Hungarian context, individuals, particularly influencers, play a prominent role in the dataset, suggesting a significant personal influence on social media.

On the other hand, the English-language data predominantly reflect the presence of traditional media entities, indicating a different dynamic in content creation and distribution. This contrast underscores the cultural and linguistic nuances of digital communication and highlights the differing strategies and impacts of content across languages.

Conclusions

Figure 5, 6, 7, and 8 show no differences in the fundamental trends (public discourse) between the Hungarian and English language areas, which are proportionally the same. The reason for this, in terms of the expressions studied, is partly the outbreak of the war and the fact that more than 8 million Ukrainians left their country after the outbreak of the armed conflict, and migration within the state was almost as high.[9]

Table 5 and 6 show that contrary to international trends in Hungary, Facebook is still the most basic social media platform with the most authors. At the same time, Twitter is dominant in English language use. In global terms, Facebook is not even indexed among the top 30 most accessed author source platforms in terms of reach. From a security point of view, in global terms, this is good news for Hungary and international trends, as psychological operations and disinformation campaigns aimed at thematising public discourse or promoting one's narrative on a global level are also more frequent on social media platforms that are also more frequent on an international level.

Of course, these campaigns can still reach Hungarian users or be promoted by various actors. This includes misleading and malicious disinformation, or even misinformation, which can be "perpetrated" even by a well-intentioned, ordinary user. Furthermore, from the point of view of Hungary's resilience to psychological operations, it should not be overlooked that attackers may also be aware, with the correct background information, of which sites are considered to be dominant and most visited in Hungary so that this statistic can be seen as a negative one.

[9] See: https://data2.unhcr.org/en/situations/ukraine

Figure 8, 9, 10, and 11, as well as Table 3 and 4, show that contrary to the international opinion in English, the proportion of positive content and hits is significantly lower in Hungary than in other countries. Overall, in the context of the high number of negative results, it can be said that Hungarian-speaking users are dismissive of Ukrainian refugees online. This could be a problem for Hungary in several respects.

- Firstly, Hungarian-speaking users are more exposed to possible – even hostile – influence by going against the general narrative and thus the interests and values represented by our allies (EU, NATO). The reason is that, as human beings, users instinctively seek out and agree with opinions contrary to the so-called "mainstream" perception. Such a situation in the public discourse can provide an excellent platform for a possible offensive psychological operation to achieve its objectives to be able to deliver its "message" in the most effective way to the target group(s) (be it economic, political, military, etc.), as the posts that are intended to be heard can easily hide additive elements aimed at influencing.
- Secondly, in the case of an established, specific Hungarian narrative, the negative perception of society abroad – even by our allies – can negatively impact the collective perception of our country. This perception can be expressed in bilateral economic, trade (professional), political, and even military issues, and changing it can be tricky, even with the effective intervention of a country's leadership.

All this applies to the results of the scientific analysis of user-generated content and hits on online sites. Our research does not include the political leadership of Hungary as a specific aspect of the study; the conclusions are drawn entirely at the social level, based on the information and professional theoretical background available to us.

Table 1 shows inconsistencies, or more accurately predict, between the other keywords that appear and the negative emotional charge described earlier. Among the most frequently appearing keywords, the terms "Transcarpathian" and "(cross-border)" appear as well, which leads us to conclude that Hungarian-speaking users are concerned about the situation, support, and assistance of Hungarians living beyond the border. However, despite this, Hungarian users have a negative attitude towards the issue of refugees concerning the trends detailed above.

This negative trend is further exacerbated by the English keyword "help", which is in 10th place, and "support", which is in 13th place. In contrast, in the case of Hungarian-language content, only support appears among the top 30 terms and only in 26th place.

Network analysis

Regarding the sentiment analysis results, we chose Twitter as the platform for the network analysis, as shown in Table 6, due to the international trend in the global use of this social media platform.

The continuous creation of data and tweets on Twitter means that the networks visualised in this chapter change regularly. At this stage of our study, it should be emphasised that the results refer to the period in consideration (usually one week before the research) so that the visualised networks may take a different form at other times. Moreover, these trends may be influenced by several factors, including external ones, which I will highlight at the points concerned.

The research covers two time intervals:

- from 3 to 10 October 2022
- the period from 16 to 23 April 2023

When visualising networks, the coloured elements represent clusters; each colour represents a different cluster. This is the programming notation, i.e. the set of points that define the network. The colouring better highlights the interconnectedness of a given centralised element.

In network research, graphs are visualised according to their type and number of degrees. From these data, you can see the group of users through whom the information reaches the most people and consequently forms the network's central elements. In addition, network points have been visualised as bridge elements. Here, you can see the users without whom the information would not spread to another network. With the central issues and bridge elements, the AA network would be complete and marginally complete.[10]

We collected data by looking at the occurrence of the following keywords in the periods mentioned above:

- standwithukraine
- standwithrussia
- russiainvadedukraine and #stoprussianagression
- standwithputin and #istandwithputin[11]

Findings

The user account observed on Twitter between 3 and 10 October 2022, spreading with astonishing speed and efficiency, was called "@partisangirl". The trend was brought to the attention of the Hungarian professional community by Ferenc Frész. The account name has since been changed and has been subject to several restrictions. About the extremely short time and the high reach of the network shown in Figure 13, it can be said that it is very likely that the user could have relied on the practical help of so-called "trolls" and "botnets" to promote the user, as such a large-scale spread of a network of this scale by an unknown author cannot be considered organic overall.

[10] Bányász et al. 2023.
[11] Bundtzen et al. 2022.

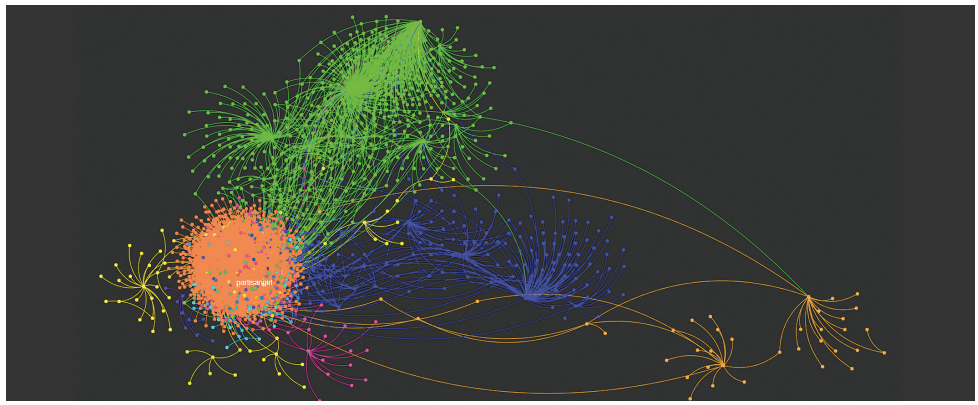


Figure 13: The spread pattern of the Twitter account@partisangirl between 3 and 10 October 2022
Source: compiled by the authors based on https://netlytic.org/

Looking into the visualisation, we can observe how key users are spreading the content further. Additionally, the spread is located very well; there are only a handful of hotspots, and there's no node connection between the spreading users. These observations alone do not indicate a "botnet" or "troll" activity; however, when multiple elements are present, we can state with a high degree of confidence that the spread of the content was assisted.

Figure 14 and 15 illustrate the networks formed by the term #standwithukraine.

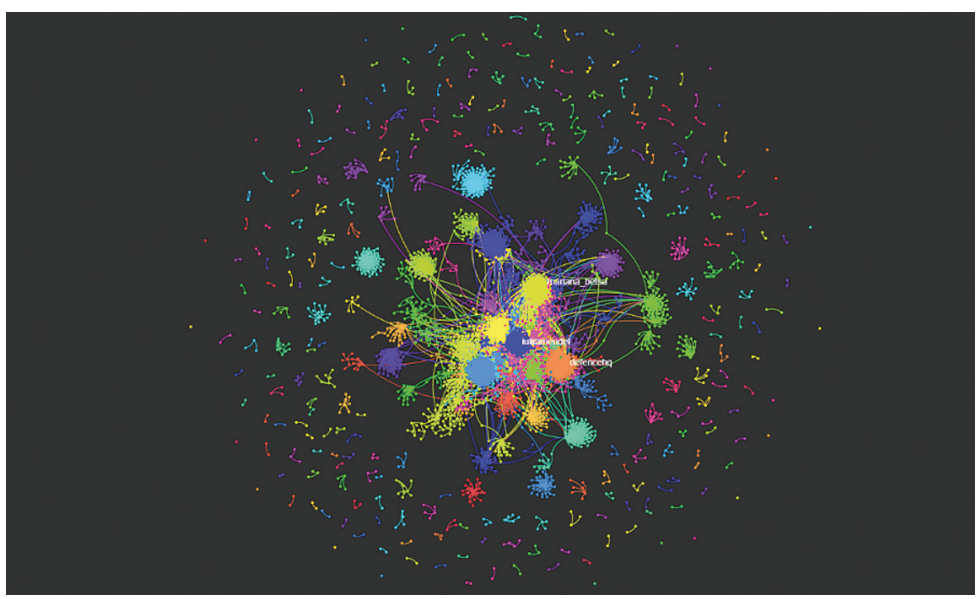


Figure 14: Patterns of networks around #standwithukraine I
Source: compiled by the authors based on https://netlytic.org/

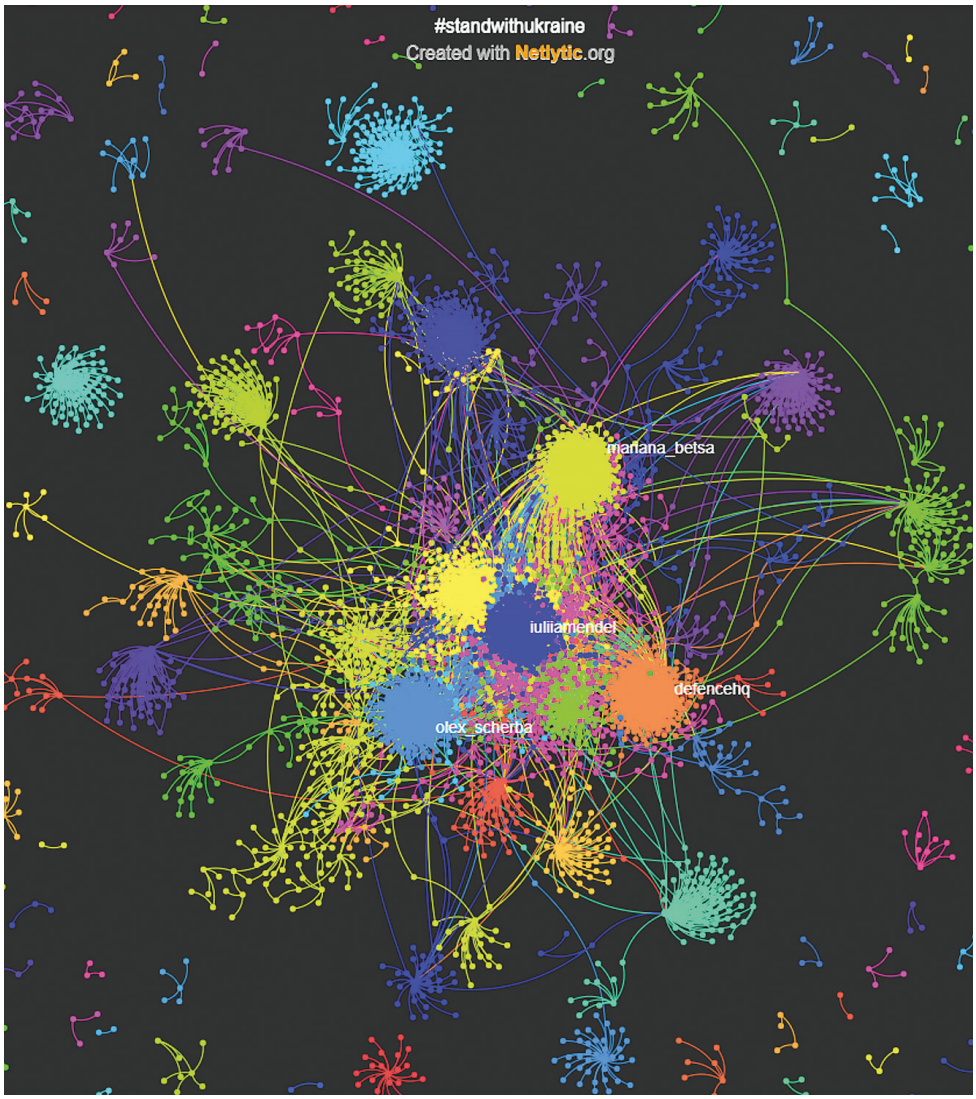


Figure 15: Patterns of networks around #standwithukraine II
Source: compiled by the authors based on https://netlytic.org/

Both these figures show a very different network compared to Figure 13. We can see hotspots similar to those in Figure 13. However, there are significant differences just at the hotspot level. The hotspots are smaller and more localised, and the hotspots are connected. This indicates an actual user activity in the data. This means that the users interact with each other and with each other's content. Meanwhile, the suspected "bot" assisted data showcases a spread from one key user, not a user interaction. More visibly, in Figure 14, however, also present in Figure 15, there are

"outsiders". This means some users formed conversations around the exact keywords but have not interacted with the hotspots. This is also possible when humans interact with each other, yet it is missing from Figure 13. Moreover, a difference between the datasets is the connection to the hotspots. The hotspots and the users within these interact with each other.

Figures 16 and 17 show the patterns of the networks formed for the term #standwithrussia.

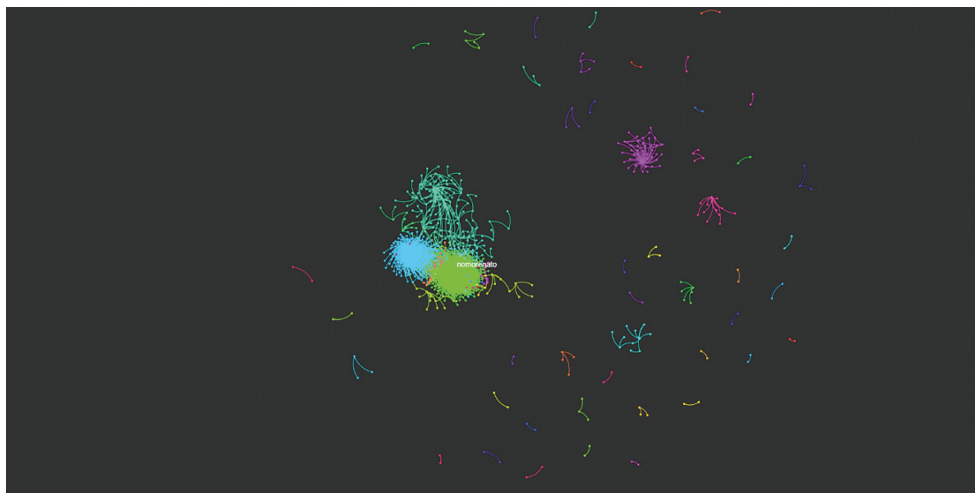


Figure 16: The term #standwithrussia patterns of networks around the phrase I
Source: compiled by the authors based on https://netlytic.org/

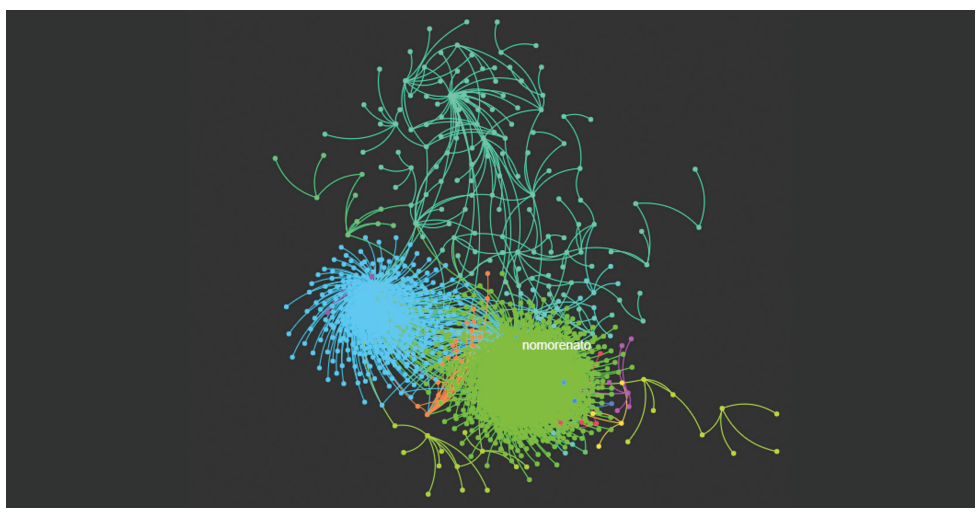


Figure 17: The term #standwithrussia patterns of networks around the phrase II
Source: compiled by the authors based on https://netlytic.org/

The issues we spotted in Figure 13 also appear in Figure 16 and 17. However, there's an exciting twist in Figure 16 with something we call "outsider nodes". These nodes look like they come from real people, but the solid and tight-knit hotspot we see in both images makes us wonder about "botnet" and "troll" involvement. When we get to the last image of this section, it's clear that mainly two users (highlighted in blue and green) are behind the spread of the hashtags. This adds a neat layer to our findings, showing how just a few individuals can significantly influence how things spread online. Connecting to our third hypothesis, *"From a network science perspective, isolated clusters are more likely to form on online social media platforms when promoting the Russian narrative versus the Ukrainian one concerning the Russian-Ukrainian war"* these results indicate a strong incentive towards a proven hypothesis. However, we still have more data to test the theory.

Figure 18 and 19 visualise the patterns of networks formed by the terms #russiainvadedukraine and #stoprussianagression.

Figure 18 and 19 show a natural user-like spread of the content with some hotspots but clear multiple connections between hotspots and nodes. However, this will change once again in the following two datasets. Figure 20 and 21 visualise the patterns of the networks formed by #standwithputin and #istandwithputin.

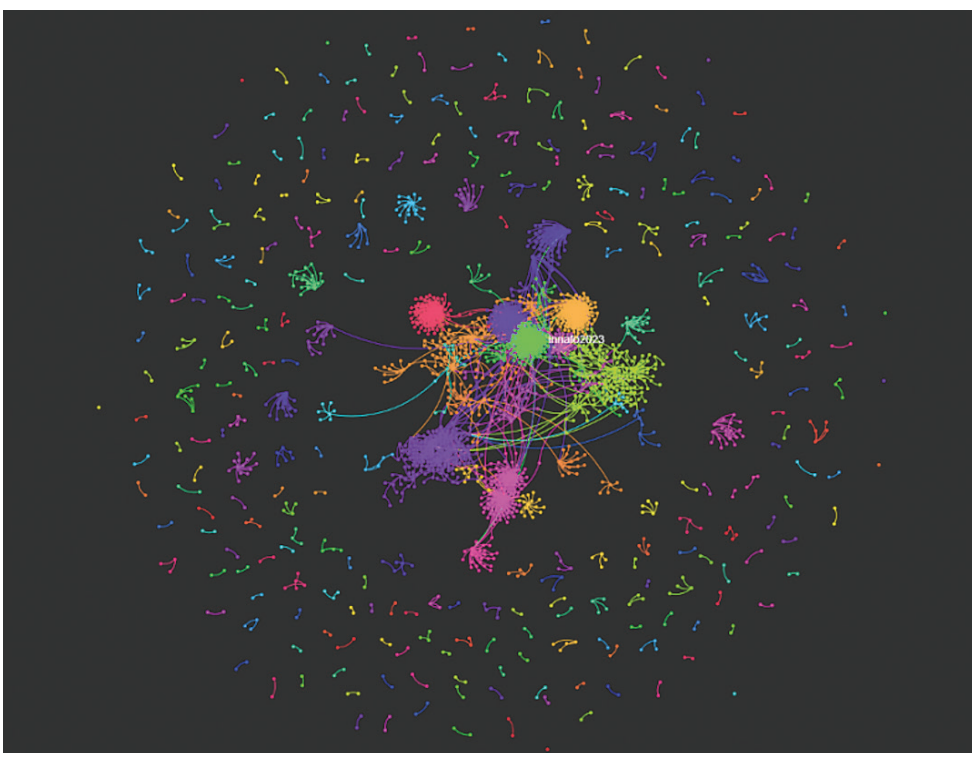


Figure 18: Patterns of networks around #russiainvadedukraine and #stoprussianagression I
Source: compiled by the authors based on https://netlytic.org/

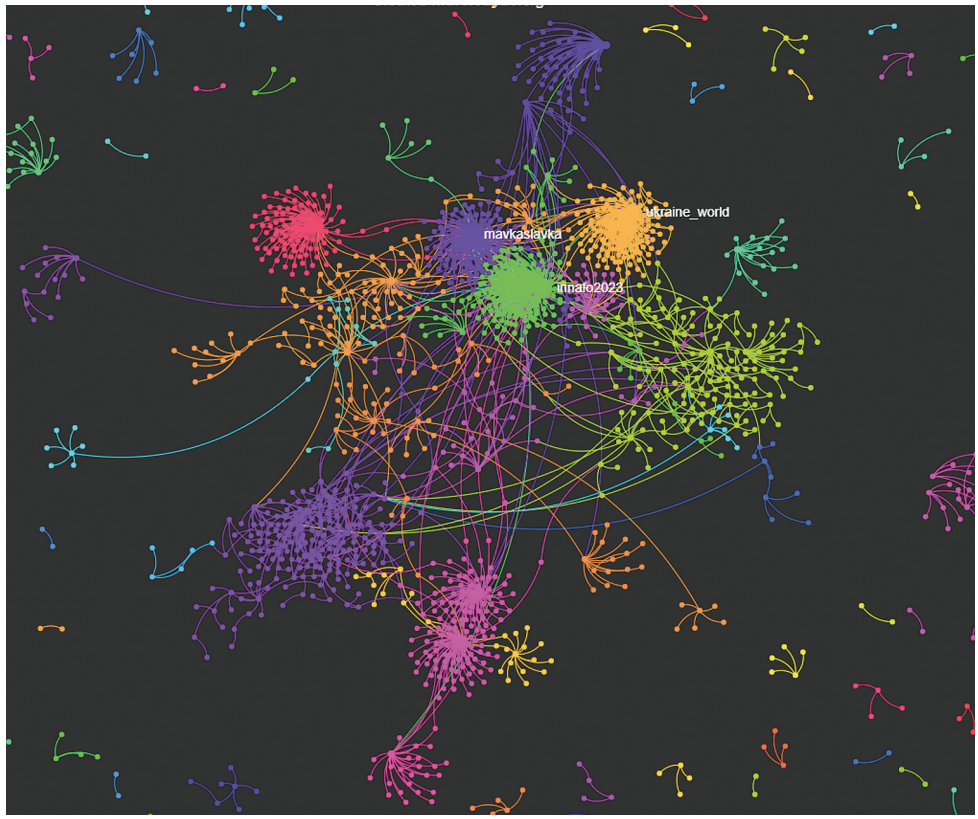


Figure 19: Patterns of networks around #russiainvadedukraine and #stoprussianagression II
Source: compiled by the authors based on https://netlytic.org/

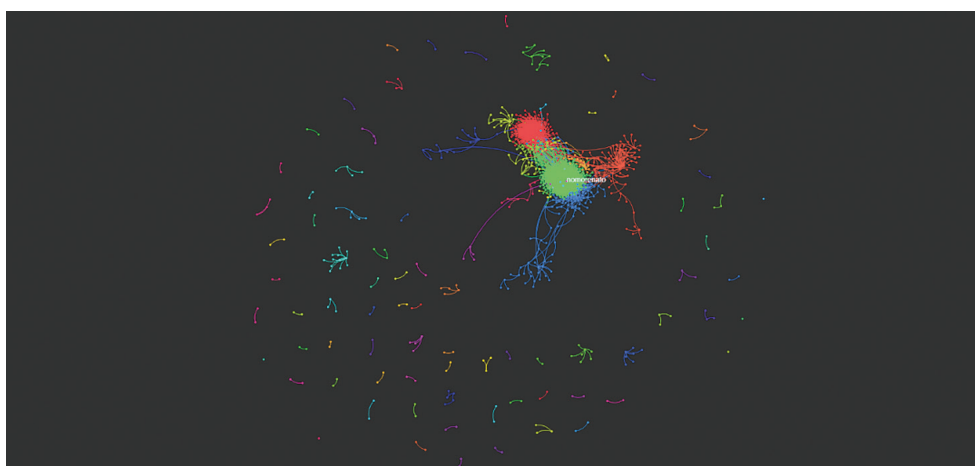


Figure 20: Patterns of networks around #standwithputin and #istandwithputin I
Source: compiled by the authors based on https://netlytic.org/

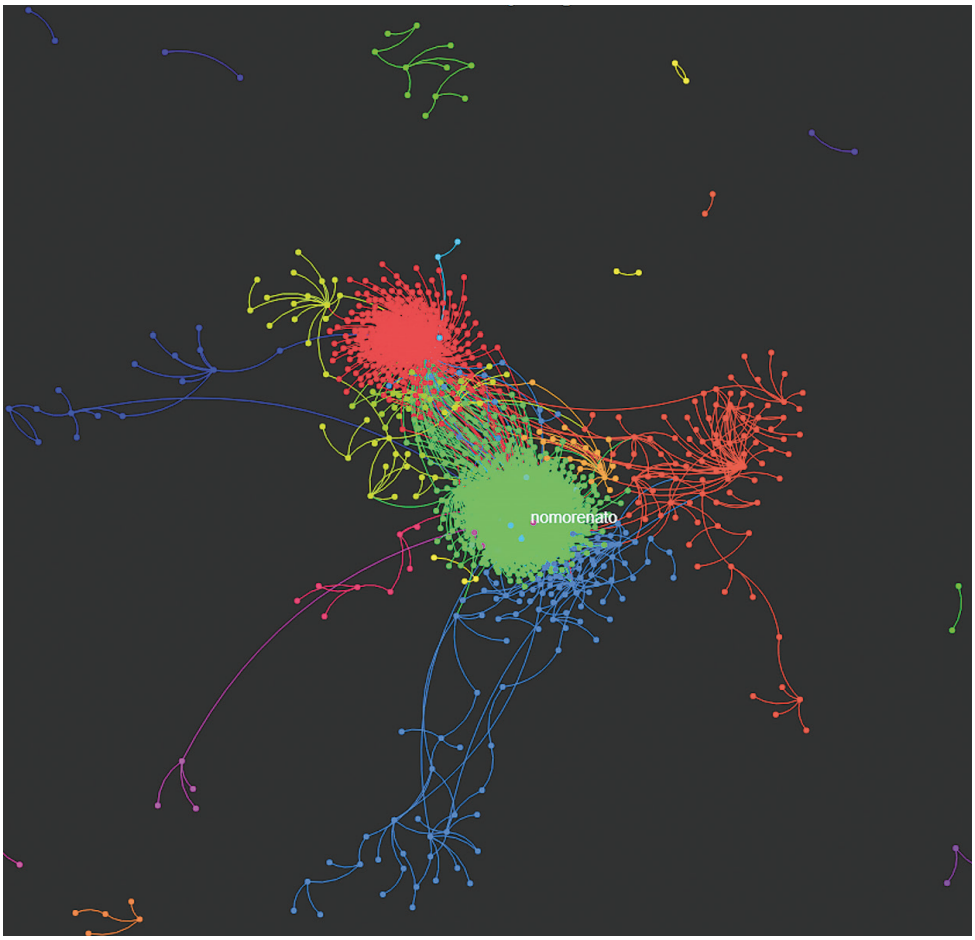


Figure 21: Patterns of networks around #standwithputin and #istandwithputin II
Source: compiled by the authors based on https://netlytic.org/

Drawing from the outcomes of the network analysis, it becomes evident that the third hypothesis has been substantiated. This is closely aligned with the fourth hypothesis, which posits that network analysis effectively identifies disinformation operations. The findings enable us to confidently assert that network analysis holds significant potential for detecting potential operations. This affirmation not only reinforces the utility of network analysis in digital communication research but also underscores its pivotal role in addressing the challenges of disinformation in the modern information landscape. Based on the insights gained from the network analysis, we can confidently affirm that our third hypothesis stands validated. This ties directly to the notion presented in our fourth hypothesis: network analysis is a powerful ally in spotting disinformation campaigns. The evidence gathered allows us to assert with a reasonable degree of certainty that network analysis is helpful and potentially

invaluable in uncovering and understanding disinformation efforts. This revelation highlights the significant role that network analysis can play in navigating the complexities of digital misinformation, offering a promising avenue for future research and application in this critical area.

Conclusions

The network research results show an overall decline in the pro-Russian narrative and a rise in support for the Ukrainian side on Twitter, the most dominant social media platform internationally.

The trend of posts containing pro-Ukrainian expressions forming a more interconnected network with more central and bridging elements can be said and seen in Figure 12–19, even though, regarding the spread patterns in Figure 11, the Russian side is investing many resources in promoting its narrative. Regarding expressions supporting the Russian side, there is a higher proportion of isolated clusters with few or no links to other focal points and users.

When examining the results, it can be seen that central nodes with high reach and multiple bridge elements also emerge for the Russian narrative. Still, they cannot connect to additional central elements to the same extent as the pro-Ukrainian entries.

Overall, the international trend on social media platforms is that Ukraine's global support is much higher than Russia's.

One of the benefits of network analysis is the ability to discover propagation bottlenecks that can be monitored, blocked, or triggered. Once identified, appropriate decisions can be made to neutralise the influencing factors, leading to the suspension of the profile or, in more severe cases, the arrest of individuals.[12] In this regard, it is essential to highlight that in the month before our research, at the beginning of March 2023, Twitter suspended around 100 accounts that shared the term #istandwithputin in high proportions.[13]

Discussion

The fight against psychological operations and disinformation campaigns can be identified as one of the outstanding security challenges of our time. The means and purposes of the disseminators of this information can be highly diverse. They may use online or physical means, and their activities may include demoralisation, misinformation, influencing economic, political, or military decisions, imposing or coercing their own will, or appealing to the undecided on a particular issue. In this context, comparing the results of the network research with the results of the sentiment analysis and the description of the operations detailed in the literature, it can

[12] Bányász et al. 2023.
[13] Collins–Korecki 2022.

be said that the position of Hungary concerning the Russian–Ukrainian war and the narrative around it can be considered a matter of concern.

Successful influence operations have unpredictable consequences. As a result, they can have negative implications for Hungary's relations with other countries and society, leading to a loss of trust in the government or the credible media, social tensions, a loss of faith in democratic values, and extremist reactions.

Regarding empirical research on Russia, it is also important to point out that there is a fundamental isolationism towards Ukraine in international public opinion regarding support. However, it is also important to stress that the resources to change this trend are available in the example presented, and it is up to Russian decision-makers to decide when to use them against an unstable community or one that is bucking international trends.

In conclusion, Hungary, with particular emphasis on the decision-making and decision-support segments, must prepare and raise public awareness of the relevance of the dangers and risks involved in psychological operations. With the right resources and international cooperation, good practices can be developed to detect these activities and operations in time and take appropriate countermeasures. Of course, a proper level of public awareness is also essential.

References

Bányász, Péter – Nagy, Gréta – Molnár, Ákos (2023): Empirical Studies of COVID-19 Related Fake News. *Hadtudomány,* 33(E), 20–36. Online: https://doi.org/10.17047/Hadtud.2023.33.E.20

Bányász, Péter – Tóth, András – László, Gábor (2022): A koronavírus oltással kapcsolatos állampolgári attitűd vizsgálata szentimentanalízis segítségével. *Információs Társadalom,* 22(1), 99–125. Online: https://doi.org/10.22503/inftars.XXII.2022.1.6

Barrett, Paul – Hendrix, Justin – Sims, Grant (2021): How Tech Platforms Fuel U.S. Political Polarization and What Government Can Do About It. *Brookings.edu,* 27 September 2021. Online: www.brookings.edu/articles/how-tech-platforms-fuel-u-s-political-polarization-and-what-government-can-do-about-it/

Bundtzen, Sara – Matlach, Paula – Mathelemuse, Nora (2022): Hashtag Pairing Is Being Used on Twitter to Facilitate Soviet Propaganda Tactic »Whataboutism«. *ISD – Institute for Strategic Dialogue* (blog), 15 March 2022. Online: www.isdglobal.org/digital_dispatches/hashtag-pairing-is-being-used-on-twitter-to-facilitate-soviet-propaganda-tactic-whataboutism/

Collins, Ben – Korecki, Natasha (2022): Twitter Bans over 100 Accounts That Pushed #IStandWithPutin. *NBC News,* 4 March 2022. Online: www.nbcnews.com/tech/internet/twitter-bans-100-accounts-pushed-istandwithputin-rcna18655

Nemeth, William J. (2002): *Future War and Chechnya: A Case for Hybrid Warfare.* Calhoun Naval Postgraduate School, Monterey. Online: https://core.ac.uk/download/pdf/36699567.pdf

HADMÉRNÖK
VÉDELEMINFORMATIKA

19. évfolyam (2024) 1. szám 85–99.
DOI: 10.32567/hm.2024.1.5

Gábor Horváth[1]

No Drone's Sky: Full Spectrum Drone Surveillance and Neutralisation Concept for Enhanced Counter-UAS Framework

(Part 1, Surveillance)

Abstract

Unmanned Aircraft Systems (UAS), commonly known as drones, have witnessed substantial global proliferation in the past decade. Their constructive applications hold the promise of being a useful, yet critical component in creating a more efficient society with the enhancement of safety, efficiency, and facilitating advancements in various domains, ultimately contributing to our modern daily lives. However, the escalating dependence on computer and communication technologies renders, especially small, UAS susceptible to various threats, posing risks to public safety, national security, and individual privacy. Addressing these concerns necessitates the development of innovative technologies designed to detect, track, identify, and eliminate UAS in a manner that upholds safety, security, and privacy. A Counter-Unmanned Aircraft System (C-UAS) is defined as a system or apparatus capable of legally and securely incapacitating, disrupting, or assuming control over an UAS. Recent years have witnessed significant research endeavours aimed at detecting and eliminate drone threats. Detection methodologies encompass acoustic, visual, passive radio frequency, radar, and data fusion techniques, while neutralisation strategies encompass physical capture and jamming approaches. This paper, delving into the realm of small drone surveillance, is the opening segment of a three-part series aims to envision a C-UAS framework; it provides an exhaustive review of existing literature in the domain of UAS surveillance, delineating the challenges associated with countering

[1] Senior ATM Officer, Ministry of Defence, State Aviation Department, e-mail: horvath.gabor@uni-nke.hu

unauthorised or unsafe drone operations, and evaluating the trajectory of detection to prepare against UAS-induced threats. Therefore, the fundamental objective of this paper is to offer a comprehensive surveillance baseline for a structured vision to a C-UAS framework, thus fostering a research community dedicated to the secure integration of drones into the airspace system.

Keywords: anti-drone, counter-UAS, drone sensing, drone neutralisation, drone surveillance

Introduction

The term "*no man's land*" is primarily known from history books and is closely associated with the tumultuous period of World War I. In this no man's land, an area which essentially sprawled between the opposing powers' trenches, soldiers only set foot when ordered to launch an attack, facing minimal chances of survival and constant exposure to the dangers of small arms and artillery fire.[2] Derived from the analogy of no man's land, envisioning a "no drone's sky" swaps the land for the sky, the soldier for the small drone, and the artillery fire for neutralisation techniques, ultimately creating a hostile space for adversarial and unlawful UAS activity.

The motivation behind formulating such a dire analogy lies in the recognition that small, unmanned aircraft systems (UAS), commonly referred to as drones, pose significant threats to both civilian and military entities,[3] as highlighted in recent episodes of the Russo–Ukrainian War[4] and the Israel–Palestine conflict.[5] Noting this challenge in Hungary, Government Decree 448/2023 (X. 3.) formally recognises small drones operating near critical infrastructure as genuine and emergent threats, emphasising the need for their surveillance and neutralisation. Within this context, advanced Counter-UAS (C-UAS) multi-spectral technologies are increasingly becoming the focus of interest, representing innovative approaches to the challenge, envisioning integrated solutions across multiple domains incorporating various sensors from active radars, through passive electromagnetic interceptors to acoustic sensors, all seamlessly connected to the neutralisation element via a dedicated command and control infrastructure. Additionally, the potential of cyber capabilities holds promise for countering mini-drone threats, although current solutions are still in their infancy, and these solutions demand advanced expertise, relatively rare skillsets, and expensive tools.[6]

Nonetheless, even though we have witnessed a significant progress in countering drones lately, the evolving threat landscape continues to present new challenges.[7] Rapid advancements in materials and the widespread availability of commercial off-the-shelf (COTS) technologies, including additive manufacturing, long-lasting batteries, and commercial navigational aids, have improved relatively cheap drone platforms with

2 Chen 2010.
3 Palik 2013.
4 Faragó 2022.
5 Freilich 2023.
6 Shukla 2023.
7 Krajnc 2018.

characteristics like high manoeuvrability and minimal signal-to-noise ratio (SNR).[8] Consequently, more advanced detection and tracking solutions are necessary to counter these evolving threats. In response to this rapidly evolving threat landscape, procurement rules for both military and law enforcement agencies have undergone significant changes. The traditional concept of time-to-market has started shifting to time-to-operation considerations.[9] Tender processes have expanded to include field trials and live competitions, highlighting the importance of availability over reliability in addressing these dynamic challenges. Therefore, the primary objective of this three-part study is to provide a comprehensive survey of the current body of literature pertaining to UAS surveillance, neutralisation and finally envisioning a C-UAS framework. It also aims to address the challenges associated with countering adversarial small UAS and evaluate emerging trends in detection and neutralisation methods, with the ultimate goal of cultivating a research community dedicated to the secure integration of UAS into the airspace system and supporting the adoption of Counter-UAS measures that align with legal obligations.

The etymology of drone surveillance

The catechism of comprehending the environment, accurately interpreting sensations, understanding the principles governing the material world, and delimiting the bounds of perception, consequently influencing surveillance capabilities, has perennially concerned mankind. Rooted in Western philosophy, this quest harks back to Plato's Theory of Forms, also known as the Theory of Ideas. According to Plato, every perceptible projection in the realm of (visual) sensory experiences emanates from the higher domain of ideas, a concept elucidated in the Allegory of the Cave.[10] These ideas epitomise the real, eternal, unalterable, and immaterial attributes of the thing-in-itself, accessible through the faculties of the human mind. The Platonic concept ιδέα (idea) traces its origins to ἰδέειν (seeing), symbolising the human capacity to deduce and abstract *a priori* existing categories and ideal archetypes from raw sensory input. Employing logic and mathematical formulations, one can encapsulate and approximate the realm of ideas, and this approach may propose a novel way of understanding the different forms of small drone surveillance techniques presented in this paper: radar, acoustic, optical, and data fusion.

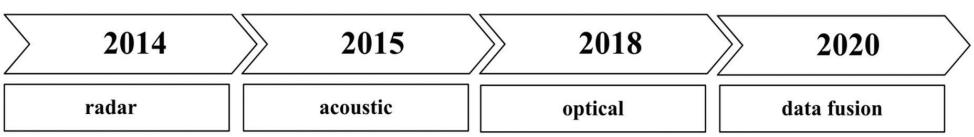


Figure 1: Advancement of UAS surveillance technologies
Source: compiled by the author

[8] Song et al. 2017.
[9] Jahangir–White 2021.
[10] Ross 1976.

The developmental trajectory of UAS detection technologies is illustrated in Figure 1. Subsequent sections delve into the specifics of each UAS detection technology, offering a comprehensive exploration of their respective advantages and disadvantages. The term "surveillance" in this context serves as an umbrella term, encompassing the integral components of detection, identification, and tracking.

Radar surveillance

Radar technology possesses distinctive advantages in detecting airborne objects, offering day and night operational capability, weather independence, and concurrent measurement of range and velocity. Nevertheless, traditional radar systems primarily target medium- and large-sized aerial objects with Radar Cross-Section (RCS) larger than 1 m^2, posing challenges in the detection of small-sized and low-speed UAS.[11] This challenge arises from the slow speed of UAS, necessitating efforts to develop new radar models or enhance the resolution of existing systems. To address this, two categories of radar-based UAS detection technologies are explored: active and passive radar surveillance.

Active radar surveillance

Enhancing the resolution of conventional radar systems for Unmanned Aircraft Systems (UAS) surveillance typically involves two strategies: utilising higher frequency carriers and employing multiple input multiple output (MIMO) beamforming radio front-ends. In pursuit of shorter wavelengths, X-band and W-band frequency modulated continuous wave (FMCW) radars designed for UAS detection are explored in its respective paper.[12] These solutions incorporate a bi-static antenna, ultimately converting received signals into a digital quadrature stream for subsequent processing, while leveraging ultra wide band (UWB) signals with a 24 GHz carrier has been demonstrated feasible.[13] The optimal carrier frequency for UAS detection radar, recommended to exceed 6 GHz (K-band), incorporates alternative approaches that employ multiple antennas to construct MIMO front-ends.[14] Notably, showcasing the detection of a small hexacopter using a 32 by 8 element L-Band receiver array, achieving notable sensitivity against micro-UAS.[15] Similarly, introducing a ubiquitous FMCW radar system operating at 8.75 GHz (X-band) with a PC-based signal processor, exhibiting the capability to detect a micro-UAS at a range of 2 km with an excellent range-speed association.[16] In another example, a K-band radar system with 16 transmitting and 16 receiving antennas forming 256 virtual antenna elements

[11] Károly–Sághi 2021.
[12] Park–Park 2017.
[13] Nakamura–Hadama 2017.
[14] Krátký–Fuxa 2015.
[15] Jahangir–Baker 2016.
[16] Duque De Quevedo et al. 2018.

demonstrates UAS detection even in a non-stationary clutter environment at a range of approximately 150 m.[17] The generation of a substantial volume of data for further processing is a noteworthy aspect of MIMO systems, prompting the author to employ the data cube and classifier concept to determine the presence and location of an incoming UAS.[18] In addition to employing a simplified multiple input single output (MISO) approach for UAS detection, other studies have shown the feasibility of utilising random sequence radar in the sub X-band, indicating potential cost-efficient solutions for UAS detection.[19]

Advancements in computation introduce the software-defined radio (SDR) based multi-mode radar, characterised by its small size and high configurability.[20] Nevertheless, the operational performance of software-defined radar (SDR) is closely tied to the capabilities of the backend processor; as demonstrated in an earlier research, the feasibility of UAS detection is tested through the presentation of two distinct implementations of FMCW radar and an implementation of continuous wave noise radar, revealing that the analogue implementation exhibits a superior updating rate and SNR.[21] The primary drawback associated with active radars is their reliance on specially designed transmitters, posing challenges in deployment and vulnerability to anti-radioactive attacks.

Passive radar surveillance

Passive radar technology represents a unique paradigm in radar systems, deviating from the conventional need for dedicated transmitters. Instead, it harnesses existing radiation sources, such as ubiquitous cellular signals, to effectively illuminate the surrounding space. Within the domain of Micro-Doppler effects, passive radars can be broadly categorised into two fundamental types: single station passive radar and distributed synthetic passive radar.[22]

The single-station variant operates by leveraging a singular illumination source, and the analysis of variations in received signals facilitates the discernment of the presence and characteristics of UAS. An illustrative example entails the utilisation of a Wi-Fi-based passive radar explicitly designed for the detection and two-dimensional localisation of small aircrafts, representing a direct emulation of active radar principles.[23]

Distributed synthetic passive radar, on the other hand, involves distributed stations leveraging existing telecommunication infrastructures as sources of illumination to enhance small UAS detection capabilities. Two primary approaches manifest within this category: cellular system-based solutions and digital video broadcasting (DVB) system-based solutions.

[17] Klare et al. 2017.
[18] Jian et al. 2018.
[19] Sacco et al. 2018.
[20] Kwag et al. 2016.
[21] Stasiak et al. 2018.
[22] Ghazalli et al. 2021.
[23] Martelli et al. 2017.

Within cellular system-based solutions, innovative approaches include utilising reflected Global System for Mobile Communications (GSM) signals for UAS location and tracking.[24] Another method involves the reception of 3G cellular signals reflected by the UAS for tracking, exploiting the Doppler features of the signal.[25] Furthermore, the investigation involves the deployment of 5G mm-wave radar infrastructure to detect small Unmanned Aircraft Systems (UAS), with captured signals being uploaded to the cloud for hazard analysis;[26] a comparable passive radar array system employs the orthogonal frequency division multiplexing (OFDM) echoes of UAS initially transmitted by nearby base stations.[27]

In the realm of digital video broadcasting system-based solutions, the utilisation of digital television signals as effective sources of illumination for passive drone detection radars has been explored. Significant research efforts have yielded the design and testing of passive drone detection radars, with a noteworthy emphasis on mirroring active radar methodologies;[28] micro-Doppler effects are employed for UAS classification, and experiments involving propeller-driven micro-Doppler signatures alongside machine learning underscored the distinguishability between plastic and carbon fibre propellers.[29]

Despite the promising potential of passive radar technology in leveraging ambient radiation, a notable challenge lies in the substantial passive surveillance efforts or the need for multiple receivers to achieve satisfactory detection accuracy. Nonetheless, if effectively addressed, challenges related to resource management, non-line of sight (NLOS) radar operation, noise mitigation, and big data management, passive radar technology holds the promise of significantly enhancing the safety and security of urban environments and critical infrastructure.

Acoustic surveillance

Utilising acoustic sensors for UAS detection involves capturing UAS sound, identifying and tracking these vehicles through audio analysis. Deployed around restricted areas, acoustic sensor arrays periodically record audio signals, which are then transmitted to ground stations for feature extraction and UAS detection. Traditionally, power spectra or frequency spectra are analysed to identify UAS sounds, with some studies employing advanced techniques.

Researchers have investigated linear predictive coding for the discrimination of UAS engine audio signal patterns from other ambient noises, despite sensitivity to weather conditions;[30] concurrently, in other papers have devised a real-time UAS sound detection and analysis system, showcasing its proficiency in acquiring real-time

[24] Zemmari et al. 2014.
[25] Chadwick 2017.
[26] Solomitckii et al. 2018.
[27] Xiaoqi et al. 2016.
[28] Liu et al. 2017b.
[29] Zhao–Su 2018.
[30] Vilímek–Buřita 2017.

sound data and recognising UAS sounds.[31] Noteworthy also that in another method, Euclidean distance and scale-invariant feature transform (SIFT) have been applied to differentiate UAV engine sound signatures from background noise, showcasing effectiveness despite processing efficiency challenges.[32]

Acoustic sensors, valued for their lightweight, cost-effectiveness, and ease of assembly, are instrumental in constructing arrays for UAS detection. An approach utilising a 24-microphone acoustic sensor array calibrated with time difference of arrival (TDoA) showed promise in tracking UAS flight paths but encountered limitations in scalability and calibration accuracy.[33] Another study enhanced UAS localisation by deploying two arrays of four microphone sensors, addressing multipath effects with a Gauss prior probability density function.[34] Advanced acoustic sensors, leveraging 2 to 4 cameras for sound strength distribution, demonstrated effectiveness in computing UAS locations both indoors and outdoors.[35] Additionally, an audio-assisted camera array captured video and audio signals simultaneously, employing histogram of oriented gradient (HOG) and Mel-frequency cepstral coefficients (MFCCs) features for object classification.[36]

Innovatively, machine learning has been introduced to classify UAS from audio data. Support vector machine (SVM) analysis of mid-term UAS engine sound signatures created a distinctive signal fingerprint, enabling precise UAS distinction in specific scenarios.[37] Another approach transformed UAS presence detection into a binary classification problem, employing Gaussian Mixture Model (GMM), Convolutional Neural Network (CNN), and Recurrent Neural Network (RNN) techniques, exhibiting effectiveness within short input signal durations.[38]

While current acoustic-based UAS detection technologies achieve precise recognition and localisation, the inherent limitations of acoustic approaches hinder large-scale deployment.[39] The integration of machine learning holds promise for enhancing small UAS detection performance in acoustic sensing, presenting a significant avenue for future research.

Optical surveillance

Vision-based Unmanned Aircraft System detection technologies primarily centre on image processing, utilising videos and cameras to capture images of intruding UAS. Computational methods at ground stations analyse videos and pictures to identify the presence of UAS. Conventional approaches heavily depend on image segmentation methods, using the differential between UAS and the environment in images

[31] Kim et al. 2017.
[32] Jang et al. 2018.
[33] Case et al. 2008.
[34] Chang et al. 2018.
[35] Busset et al. 2015.
[36] Liu et al. 2017a.
[37] Bernardini et al. 2017.
[38] Jeon et al. 2017.
[39] Gajdács 2022.

to discern UAS presence in restricted areas. Several studies tackle the challenges of separating UAS from the background and distinguishing UAS from flying birds.[40] In contrast, contemporary image segmentation methods employ neural networks to directly recognise UAS appearances. A novel approach employs a thermal camera for UAS detection, coupled with a neural network for identification.[41] Another research introduces a lightweight, fast algorithm capable of operating on embedded systems like Nvidia Jetson TX1, enabling small UAS identification in motion.[42]

A real-time vision-based UAS detection system combines FPGA-based and GPU-based platforms, emphasising power efficiency and processing speed.[43] Various convolutional neural networks were compared, demonstrating that the Visual Geometry Group (VGG 16) network with Faster R-CNN achieves superior performance.[44] Strategies, like combining images to create synthetic datasets, aim to enhance convolutional neural network training for improved UAS detection.[45] Convolutional neural networks also address the challenge of distinguishing UAS from birds, outperforming policy-based approaches in accuracy and efficiency.[46] Efforts employing infrared cameras aim to identify UAS by detecting heat variations, but challenges arise due to the significant impact of battery heat on detection results.[47] Dynamic vision sensors, capturing propeller rotation frequency, efficiently distinguish UAS from birds.[48] Vision-based approaches exhibit potential efficiency in specific scenarios, with the evolution of deep neural networks enhancing image processing capabilities. Real-time trials highlight their efficiency, yet challenges persist in implementing these algorithms across diverse environments. Robustness, adaptability, and precision are critical requirements. Robustness is essential for coping with rapid environmental changes, while mitigating image distortion caused by weather changes through multi-level image processors. Handling UAS mobility variations, distinguishing UAS from birds accurately, and improving overall detection and mitigation efficiency are ongoing challenges.

Data fused surveillance

The process of data fusion involves integrating diverse data sources to produce more consistent, accurate, and informative information than any individual source can provide. This approach has the potential to generate fused data that is not only more informative but also more synthetic than the original inputs. By leveraging the strengths of various methods, data fusion aims to yield a combined result that is robust, accurate, and efficient, overcoming the limitations of single approaches, particularly in specific scenarios related to Unmanned Aircraft Systems detection.

40 Dong–Zou 2017. Christnacher et al. 2016.
41 Sineglazov 2015.
42 Briese et al. 2018.
43 Perschke et al. 2018.
44 Saqib et al. 2017.
45 Aker–Kalkan 2017.
46 Coluccia et al. 2017.
47 Andraši et al. 2017.
48 Hoseini et al. 2017.

Upon reviewing the advantages and disadvantages of individual approaches, three categories of research in data fusion for UAS detection emerge: multiple-sensor data fusion, multiple-type sensor data fusion, and multiple sensing algorithm fusion.

Multiple-sensor data fusion

Different types of sensors possess distinct advantages and drawbacks in small UAS detection scenarios. To address the limited detection range of single approaches, specific sensor types are designed to overcome inherent limitations. For instance, an acoustic sensor array deploys distributed sensors to record audio, analysing the sound spectrum to locate UAS. In signal processing, adjusting the weight of each sensor enhances location accuracy. Another example involves RF-based detection with omni-directional antennas, enabling the tracking of UAS trajectories and the determination of malicious intent. Combining multiple sensors of the same type improves accuracy and functionality, extending detection range geographically.[49]

Multiple-type sensor data fusion

In scenarios where increasing the number of sensors does not mitigate the drawbacks of single sensors, researchers explore combinations of different sensor types. Fusion of acoustic and radar sensors, for example, has shown more precise UAS detection. Deploying sensors with varying detection ranges, such as passive RF receivers, cameras, and acoustic sensors, enhances accuracy in different field zones.[50] Despite the promising performance, the deployment and configuration of such systems require specific expertise and pose challenges.

Multiple sensing algorithm fusion

Efficiency and accuracy in small UAS detection remain challenging, prompting the exploration of combining multiple sensing algorithms. Activated sensors deliver information to ground stations, triggering relevant algorithms based on detection status. Unsupervised approaches, as demonstrated in one study, extract features of signals from various acoustic sensors, employing support vector machine and K-nearest neighbours (KNN) algorithms for UAS detection.[51] Balancing the weight of each sensing algorithm and establishing reasonable schedules for their activation present ongoing challenges.

In data fusion schemes, researchers may consider platform integration, wherein sensors are deployed on various platforms to enhance mobility; however, challenges

[49] Böniger et al. 2016.
[50] Müller et al. 2018.
[51] Klochko et al. 2019.

encompass maintaining consistency in detection results and balancing the weights of different approaches to achieve optimal outcomes.[52] The data fusion approaches demonstrated advantages over single methods, emphasising the need for further research to optimise their implementation in diverse scenarios.

Conclusion

The comprehensive introduction of small drone surveillance methodologies reveals a dynamic landscape marked by technological advancements and challenges. Radar surveillance, with active and passive variants, showcases potential, but further research is needed to optimise active radar technologies in order to detect small drones. Acoustic surveillance emerges as a cost-effective alternative, leveraging machine learning applications that exhibit potential for enhanced performance, while optical surveillance, dependent on image processing and neural networks, holds promise but necessitates ongoing refinement to ensure adaptability. Emerging as a unifying approach, data fusion demonstrates the potential of combining diverse data sources for a robust UAS detection method, with the versatility of multiple-sensor data fusion, multiple-type sensor data fusion, and multiple sensing algorithm fusion underscoring the imperative for comprehensive and resilient UAS detection solutions. In short, radar-based small UAS detection demonstrates superior performance, though challenges arise concerning deployment costs and technical expertise; the ongoing pursuit involves developing light, energy-saving, and affordable radar elements that facilitate easy deployment and maintenance.

Conclusively, this comprehensive study offers insights into existing small UAS surveillance methods, underscoring the importance of adopting a holistic approach to envision a Counter-Unmanned Aircraft System framework. As we advance to Part 2, concentrating on neutralisation methods, and Part 3, envisioning a comprehensive C-UAS system, the necessity of synergistic integration becomes evident.

Acknowledgement

This paper was prepared with the professional support of the Doctoral Student Scholarship Program of the Co-operative Doctoral Program of the Ministry of Culture and Innovation financed from the National Research, Development and Innovation Fund.

National Research, Development and Innovation Office

[52] Song et al. 2018.

References

Aker, Cemal – Kalkan, Sinan (2017): Using Deep Networks for Drone Detection. In *14th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS),* Lecce, Italy. Online: https://doi.org/10.1109/AVSS.2017.8078539

Andraši, Petar – Radišić, Tomislav – Muštra, Mario – Ivošević, Jurica (2017): Night-time Detection of UAVs using Thermal Infrared Camera. *Transportation Research Procedia,* 28, 183–190. Online: https://doi.org/10.1016/j.trpro.2017.12.184

Bernardini, Andrea – Mangiatordi, Federica – Pallotti, Emiliano – Capodiferro, Licia (2017): Drone Detection by Acoustic Signature Identification. In *Symposium on Electronic Imaging: Imaging and Multimedia Analytics in a Web and Mobile World,* 60–64. Online: https://doi.org/10.2352/ISSN.2470-1173.2017.10.IMAWM-168

Böniger, Urs – Otto, Beat – Wellig, Peter (2016): Detection of Mini-UAVs in the Presence of Strong Topographic Relief: A Multisensor Perspective. *In Proceedings of SPIE 9997, Target and Background Signatures II,* 999702. Online: https://doi.org/10.1117/12.2241757

Briese, Christoph – Seel, Andreas – Andert, Franz (2018): Vision-Based Detection of Non-Cooperative UAVs Using Frame Differencing and Temporal Filter. In *International Conference on Unmanned Aircraft Systems (ICUAS),* Dallas, TX, 606–613. Online: https://doi.org/10.1109/ICUAS.2018.8453372

Busset, Joël – Perrodin, Florian – Wellig, Peter – Ott, Beat – Heutschi, Kurt – Rühl, Torben – Nussbaumer, Thomas (2015): Detection and Tracking of Drones Using Advanced Acoustic Cameras. *SPIE Unmanned/Unattended Sensors and Sensor Networks XI; and Advanced Free-Space Optical Communication Techniques and Applications, 96470F,* Toulouse. Online: https://doi.org/10.1117/12.2194309

Case, Ellen – Zelnio, Anne – Rigling, Brian (2008): Low-Cost Acoustic Array for Small UAV Detection and Tracking. In *IEEE National Aerospace and Electronics Conference,* Dayton, OH, 110–113. Online: https://doi.org/10.1109/NAECON.2008.4806528

Chadwick, Andrew (2017): Micro-Drone Detection using Software-Defined 3G Passive Radar. In *International Conference on Radar Systems (Radar 2017),* Belfast, 1–6. Online: https://doi.org/10.1049/cp.2017.0419

Chang, Xianyu – Yang, Chaoqun – Wu, Junfeng – Shi, Xiufang – Shi, Zhiguo (2018): A Surveillance System for Drone Localization and Tracking Using Acoustic Arrays. In *IEEE 10th Sensor Array and Multichannel Signal Processing Workshop (SAM),* Sheffield, UK, 573–577. Online: https://doi.org/10.1109/SAM.2018.8448409

Chen, Hongwei (2010): No Man's Land: a Variation on Harold Pinter's Theme of Menace. *Journal of Language Teaching and Research,* 1(2), 169–174. Online: https://doi.org/10.4304/jltr.1.2.169-174

Christnacher, Frank – Hengy, Sébastien – Laurenzis, Martin – Matwyschuk, Alexis – Naz, Pierre – Schertzer, Stéphane – Schmitt, Gwenael (2016): Optical and Acoustical UAV Detection. In *Proceedings of SPIE Security and Defence,* 9988, Edinburgh, UK. Online: https://doi.org/10.1117/12.2240752

Coluccia, Angelo – Ghenescu, Marian – Piatrik, Tomas – De Cubber, Geert – Schumann, Arne – Sommer, Lars – Klatte, Johannes – Schuchert, Tobias – Beyerer, Juergen – Farhadi, Mohammad et al. (2017): Drone-vs-Bird Detection Challenge. In

14th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS), Lecce, Italy. Online: https://doi.org/10.1109/AVSS.2017.8078464

Dong, Qiang – Zou, Qinghua (2017): Visual UAV Detection Method with Online Feature Classification. *IEEE 2nd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC),* Chengdu, China, 429–432. Online: https://doi.org/10.1109/ITNEC.2017.8284767

Duque de Quevedo, Álvaro – Ibañez Urzaiz, Fernando – Gismero Menoyo, Javier – López Asensio, Alberto (2018): Drone Detection With X-Band Ubiquitous Radar. In *19th International Radar Symposium (IRS),* Bonn, Germany, 1–10. Online: https://doi.org/10.23919/IRS.2018.8447942

Faragó, Bence (2022): Drónok Harca – Az orosz–ukrán háborúban jelen lévő drónok felértékelődése, működésük taktikai és stratégiai vonatkozásai a megváltozó hadviselési környezetben [Game of Drones – The Increasing Importance of Drones in the Russian-Ukrainian War, Their Tactical and Strategic Implications in the Changing Warfare Environment]. *Nemzet és Biztonság,* 15(2), 36–54. Online: https://doi.org/10.32576/nb.2022.2.3

Freilich, Chuck (2023): Israel and the Palestinians: The Day After. *Survival: Global Politics and Strategy,* 65(6), 67–73. Online: https://doi.org/10.1080/00396338.2023.2285602

Gajdács, László (2022): Pilóta nélküli légi jármű érzékelésének lehetséges megoldásai [Possible Solutions for Unmanned Aircraft Vehicle Detection]. *Hadmérnök,* 17(4), 17–28. Online: https://doi.org/10.32567/hm.2022.4.2

Ghazalli, Nasyitah – Balleri, Alessio – Jahangir, Mohammed (2021): Passive Radar Detection of Drones with Staring Illuminators of Opportunity. In Clemente, Carmine – Fioranelli, Francesco – Colone, Fabiola – Li, Gang (eds.): *Radar Countermeasures for Unmanned Aerial Vehicles.* (eBook). Institution of Engineering and Technology. Online: https://doi.org/10.1049/SBRA543E_ch5

Liu, Hao – Wei, Zhiqiang – Chen, Yitong – Pan, J. – Lin, L. – Ren, Y. (2017a): Drone Detection Based on an Audio-Assisted Camera Array. In *IEEE Third International Conference on Multimedia Big Data (BigMM),* Laguna Hills, CA, 402–406. Online: https://doi.org/10.1109/BigMM.2017.57

Hoseini, Sahar – Orchard, Garrick – Yousefzadeh, A. – Deverakonda, B. – Serrano-Gotarredona, T. – Linares-Barranco, B. (2017): Passive Localization and Detection of Quadcopter UAVs by Using Dynamic Vision Sensor. In *5th Iranian Joint Congress on Fuzzy and Intelligent Systems (CFIS),* Qazvin, Iran, 81–85. Online: https://doi.org/10.1109/CFIS.2017.8003662

Jahangir, Mohammed – Baker, Chris (2016): Robust Detection of Micro-UAS Drones with L-Band 3-D Holographic Radar. In *Sensor Signal Processing for Defence (SSPD),* Edinburgh, UK, 1–5. Online: https://doi.org/10.1109/SSPD.2016.7590610

Jahangir, Mohammed – White, Daniel (2021): Good Practices and Approaches for Counter UAV System Developments – An Industrial Perspective. In Clemente, Carmine – Fioranelli, Francesco – Colone, Fabiola – Li, Gang (eds.): *Radar Countermeasures for Unmanned Aerial Vehicles.* (eBook). Institution of Engineering and Technology. Online: https://doi.org/10.1049/SBRA543E_ch12

Jang, Beomhui – Seo, Yoojeong – On, Baeksan – Im, Sungbin (2018): Euclidean Distance Based Algorithm for UAV Acoustic Detection. In *International Conference on Electronics, Information, and Communication (ICEIC),* Honolulu, HI, 1–2. Online: https://doi.org/10.23919/ELINFOCOM.2018.8330557

Jeon, Sungho – Shin, Jong-Woo – Lee, Young-Jun – Kim, Woong-Hee (2017): Empirical Study of Drone Sound Detection in Real-Life Environment with Deep Neural Networks. In *25th European Signal Processing Conference (EUSIPCO),* Kos, Greece, 1858–1862. Online: https://doi.org/10.23919/EUSIPCO.2017.8081531

Jian, Michael – Lu, Zhenzhong – Chen, Victor (2018): Drone Detection and Tracking Based on Phase-Interferometric Doppler Radar. In *IEEE Radar Conference (RadarConf18),* Oklahoma City, 1146–1149. Online: https://doi.org/10.1109/RADAR.2018.8378723

Károly, Bianka – Sághi, Balázs (2021): Assessing the Unmanned Aerial Vehicles' Surveillance Problems and Actual Solution Options from the Different Stakeholders' Viewpoint. *Periodica Polytechnica Transportation Engineering,* 49(1), 32–41. Online: https://doi.org/10.3311/PPtr.13749

Kim, Juhyun – Park, Cheonbok – Ahn, Jinwoo – Ko, Youlim – Park, Junghyun – Gallagher, John C. (2017): Real-time UAV Sound Detection and Analysis System. In *IEEE Sensors Applications Symposium (SAS),* Glassboro, NJ, 1–5. Online: https://doi.org/10.1109/SAS.2017.7894058

Klare, Jens – Biallawons, Oliver – Cerutti-Maori, Delphine (2017): UAV Detection with MIMO Radar. In *18th International Radar Symposium (IRS),* Prague, 1–8. Online: https://doi.org/10.23919/IRS.2017.8008140

Klochko, Vladimir – Strotov, Valery – Smirnov, Sergey (2019): Multiple Objects Detection and Tracking in Passive Scanning Millimeter-Wave Imaging Systems. In *Millimetre Wave and Terahertz Sensors and Technology XII,* Strasbourg, France. Online: https://doi.org/10.1117/12.2532546

Krajnc, Zoltán (2018): A drónok elleni stratégia és eljárások [Counter Drone Strategy and Procedures]. *Repüléstudományi Közlemények,* 30(3), 139–148.

Krátký, Miroslav – Fuxa, Luboš (2015): Mini UAVs Detection by Radar. *International Conference on Military Technologies (ICMT),* Brno, Czech Republic, 1–5. Online: https://doi.org/10.1109/MILTECHS.2015.7153647

Kwag, Young-Kil – Woo, In-Sang – Kwak, Ho-Young – Jung, Young-Ho (2016): Multi-mode SDR Radar Platform for Small Air-Vehicle Drone Detection. In *CIE International Conference on Radar (RADAR),* Guangzhou, China, 1–4. Online: https://doi.org/10.1109/RADAR.2016.8059254

Liu, Yuqi – Wan, Xianrong – Tang, Hui – Yi, Jianxin – Cheng, Yiyao – Zhang, Xun (2017b): Digital Television Based Passive Bistatic Radar System for Drone Detection. In *IEEE Radar Conference (RadarConf),* Seattle, 1493–1497. Online: https://doi.org/10.1109/RADAR.2017.7944443

Martelli, T. – Murgia, F. – Colone, F. – Bongioanni, C. – Lombardo, P. (2017): Detection and 3D Localization of Ultralight Aircrafts and Drones with a WiFi-based Passive Radar. In *International Conference on Radar Systems (Radar 2017),* Belfast, Institution of Engineering and Technology, 1–6. Online: https://doi.org/10.1049/cp.2017.0423

Müller, Wilmuth – Sander, Jennifer – Kuwertz, Achim – Mühlenberg, Dirk (2018): High-Level Data Fusion Component for Drone Classification and Decision Support in Counter UAV. In *Open Architecture/Open Business Model Net-Centric Systems and Defense Transformation,* Orlando, FL. Online: https://doi.org/10.1117/12.2306148

Nakamura, Ryohei – Hadama, Hisaya (2017): Characteristics of Ultra-Wideband Radar Echoes from a Drone. *IEICE Communications Express,* 6(9), 530–534. Online: https://doi.org/10.1587/comex.2017XBL0079

Palik, Mátyás (2013): A pilóta nélküli légijárművek katonai alkalmazása. In Palik, Mátyás (ed.): *Pilóta nélküli repülés profiknak és amatőröknek.* Budapest: Nemzeti Közszolgálati Egyetem, 281–298.

Park, Seungwoon – Park, Seong-Ook (2017): Configuration of an X-band FMCW Radar Targeted for Drone Detection. In *International Symposium on Antennas and Propagation (ISAP),* Phuket, Thailand, 1–2. Online: https://doi.org/10.1109/ISANP.2017.8228912

Perschke, Thomas – Moren, Konrad – Müller, Thomas (2018): Real-Time Detection of Drones at Large Distances with 25 Megapixel Cameras. In *Emerging Imaging and Sensing Technologies for Security and Defence III; and Unmanned Sensors, Systems, and Countermeasures,* Berlin. Online: https://doi.org/10.1117/12.2324678

Ross, William, David (1976): *Plato's Theory of Ideas.* Westport: Greenwood Press.

Sacco, Giulia – Pittella, Erika – Pisa, Stefano – Piuzzi, Emanuele (2018): A MISO Radar System for Drone Localization. In *5th IEEE International Workshop on Metrology for AeroSpace (MetroAeroSpace),* Rome, 549–553. Online: https://doi.org/10.1109/MetroAeroSpace.2018.8453572

Saqib, Muhammad – Khan, Sultan Daud – Sharma, Nabin – Blumenstein, Michael (2017): A Study on Detecting Drones Using Deep Convolutional Neural Networks. In *14th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS),* Lecce, Italy, 1–5. Online: https://doi.org/10.1109/AVSS.2017.8078541

Shukla, Sandeep (2016): Cyber Security of Cyber Physical Systems: Cyber Threats and Defense of Critical Infrastructures. In *29th International Conference on VLSI Design,* Kolkata, India, 30–31. Online: https://doi.org/10.1109/VLSID.2016.153

Sineglazov, Victor (2015): Multi-Functional Integrated Complex of Detection and Identification of UAVs. In *IEEE International Conference Actual Problems of Unmanned Aerial Vehicles Developments (APUAVD),* Kyiv, Ukraine, 320–323. Online: https://doi.org/10.1109/APUAVD.2015.7346631

Solomitckii, Dmitrii – Gapeyenko, Margarita – Semkin, Vasilii – Andreev, Sergey – Koucheryavy, Yevgeni (2018): Technologies for Efficient Amateur Drone Detection in 5G Millimeter-Wave Cellular Infrastructure. *IEEE Communications Magazine,* 56(1), 43–50. Online: https://doi.org/10.1109/MCOM.2017.1700450

Song, Houbing – Ravi, Srinivasan – Tamim, Sookoor – Jeschke, Sabina (2017): *Smart Cities: Foundations, Principles, and Applications.* Hoboken: Wiley. Online: https://doi.org/10.1002/9781119226444

Song, Houbing – Wang Jian, – Liu, Yongxin – Yue, Xuejun – Young, Thomas – Yuan, Jiawei – Seker, Remzi (2018): Integrating Ground Surveillance with Aerial Surveillance for Enhanced Amateur Drone Detection. In *Disruptive Technologies in Information Sciences,* Orlando, FL. Online: https://doi.org/10.1117/12.2304531

Stasiak, Krzysztof – Ciesielski, Marek – Kurowska, Anna – Przybysz, Wojciech (2018): A Study on Using Different Kinds of Continuous-wave Radars Operating in C-band for Drone Detection. In *22nd International Microwave and Radar Conference (MIKON),* Poznan, Poland, 521–526. Online: https://doi.org/10.23919/MIKON.2018.8405275

Vilímek, Jakub – Buřita, Ladislav (2017): Ways for Copter Drone Acoustic Detection. In *International Conference on Military Technologies (ICMT),* Brno, Czech Republic, 349–353. Online: https://doi.org/10.1109/MILTECHS.2017.7988783

Xiaoqi, Yang – Kai, Huo – Weidong, Jiang – Jingjing, Zhao – Zhaokun Qiu (2016): A Passive Radar System for Detecting UAV Based on the OFDM Communication Signal. *Progress in Electromagnetic Research Symposium (PIERS),* Shanghai, 2757–2762. Online: https://doi.org/10.1109/PIERS.2016.7735118

Zemmari, Reda – Broetje, Martina – Battistello, Giulia – Nickel, Ulrich (2014): GSM Passive Coherent Location System: Performance Prediction and Measurement Evaluation. *IET Radar Sonar Navigation,* 8(2), 94–105. Online: https://doi.org/10.1049/iet-rsn.2013.0206

Zhao, Yichao – Su, Yi (2018): Cyclostationary Phase Analysis on Micro-Doppler Parameters for Radar-Based Small UAVs Detection. *IEEE Transactions on Instrumentation and Measurement,* 67(9), 2048–2057. Online: https://doi.org/10.1109/TIM.2018.2811256

HADMÉRNÖK
VÉDELEMINFORMATIKA

19. évfolyam (2024) 1. szám 101–120.
DOI: 10.32567/hm.2024.1.6

Hunorfi Péter,[1] Paráda István,[2] Farkas Tibor[3]

Kiberbiztonsági kihívások a légi közlekedésben – Kronológiai folyamat a Boeing elleni kibertámadások tükrében

Cybersecurity Issues in Aviation – Timeline of Cyber Crimes against Boeing

Absztrakt

Jelen cikkben a szerzők bemutatják a légi közlekedés egyik információs alrendszerét, informatikai megoldását, valamint annak potenciális kibertéri veszélyeit és kockázatait. Ehhez a szerzők egy elemző-értékelő módszerrel meghatározzák a légi közlekedés bizonyos informatikai elemeit, elsősorban a kommunikációs, adatkapcsolati és fedélzeti repülési rendszereket, például az úgynevezett electronic flight bag-eket (EFB), amelyek kiberincidensek következtében kiemelt jelentőségűek. Ezt követően a szerzők ismertetik a Boeing vállalatnál a közelmúltban bekövetkezett kibertámadásokat, illetve azok kronológiai sorrendjét, majd mindezeket összegezve logikai következtetéseket vonnak le azok hatásairól, illetve a támadás elleni fellépések újabb formájáról.

Kulcsszavak: légi közlekedés, EFB, NOTAMS, Boeing, kibervédelem, ransomware

[1] Doktori hallgató, Óbudai Egyetem Biztonságtudományi Doktori Iskola, e-mail: hunorfi.peter@phd.uni-obuda.hu
[2] CIS Operations Officer, NATO Support and Procurement Agency, e-mail: paradaistvan@gmail.com
[3] Egyetemi docens, Óbudai Egyetem, e-mail: farkas.tibor@bgk.uni-obuda.hu

Abstract

In this article, the authors present an information subsystem of air transport, its IT solution, as well as its potential cyber threats and risks. To this end, the authors determine certain IT components of air transport with particular regard to communication, data link, and onboard flight systems, such as the so-called electronic flight bags (EFB), which have special significance due to cyber incidents. Following this, the authors describe the cyber attacks that occurred recently at Boeing, including their chronological order, and then, by summarising all these, they inductively draw logical conclusions about their impacts, as well as about new forms of response against the attacks.

Keywords: aviation, EFB, NOTAMS, Boeing, Cyber Defense, Ransomware

Bevezetés

Napjainkban a legtöbb kereskedelmi repülőgép innovatív technológiákat, rendszereket és példátlan infrastruktúrát használ a kibertechnológiákat is magában foglaló repüléselektronikai alkalmazásokhoz. A repülőgépek utasai ma már komplex informatikai rendszereket vesznek igénybe jegyvásárláskor, a repüléshez történő bejelentkezéskor, a repülőtéri biztonsági ellenőrzésen való áthaladáskor, valamint a nyílt, publikus internethez wifi és a beépített fedélzeti szórakoztató rendszerhez való csatlakozáskor. A kapcsolódó kibertechnológiák és a kapcsolódási lehetőségek a repülést a kiberfenyegetések veszélyes világának teszik ki, amelyek komoly kihívást jelentenek egy esetleges támadás során, és amelyek megnehezítik a kockázatok megértését vagy meghatározását. Emellett az új szolgáltatások és rendszerek fejlesztésével folyamatosan nőnek a támadások felületei és lehetőségei.

A repülési ipar jelentős átalakuláson ment keresztül az információs technológiai (IT) megoldások integrálásával, különösen az EFB-rendszerek formájában. Ezek a megoldások forradalmasították a repülési műveleteket, digitális hozzáférést biztosítva a pilótáknak a kritikus információkhoz és erőforrásokhoz. A digitális rendszerekre való fokozott támaszkodás azonban olyan kiberbiztonsági kihívásokat is jelentett, amelyeket kezelni kell. Ez a cikk a légi közlekedésben alkalmazott EFB-megoldásokhoz kapcsolódó kiberbiztonsági kihívásokat tárja fel, különösen a Boeing vállalatot ért kibertámadások szemszögéből. A repülőterek és a légi járművek elleni kibertámadások lehetősége valódi veszélyeket rejt magában, úgymint a földi és légi infrastruktúrák folyamatos és zökkenőmentes működtetésének akadályozása; az üzembiztonság sérülése; az adatok illetéktelen kezekbe kerülése vagy az informatikai és kommunikációs rendszerek összeomlása. A lehetséges kockázatok, az üzembiztonságra gyakorolt hatás és a szükséges mérséklő intézkedések vizsgálatával jobban megérthetjük a kiberbiztonság jelentőségét a légi közlekedés keretében.

A cikk legfontosabb kutatási kérdése, hogy a légi közlekedésben az Electronic Flight Bag (EFB) rendszerek és a kapcsolódó informatikai infrastruktúra kiberbiztonsági sebezhetőségeinek és fenyegetéseinek azonosítása, elemzése és kezelése milyen kihívásokat tartogat. A probléma magában foglalja a kiberfenyegetések változó

természetének megértését, a légi közlekedési ágazatra jellemző különleges biztonsági kockázatokat és a hatékony védelmi stratégiák kidolgozását a légi közlekedési ágazat egyedi igényeinek megfelelően. A Boeing vállalatnál bekövetkezett kibertámadások példáját felhasználva a kutatás célja az, hogy átfogó képet adjon az EFB-rendszerek potenciális kiberbiztonsági sebezhetőségeiről, azok lehetséges következményeiről a légi közlekedési műveletekre, valamint a megelőzés és a reagálás hatékony módszereiről.

A kutatás során alapvetően két hipotézis fogalmazható meg.

- (HT 1.) Az EFB-rendszerek integrációjának és a növekvő digitalizációnak köszönhetően a légi közlekedési ágazat egyre nagyobb kockázatnak van kitéve a kiberfenyegetésekkel szemben, ami jelentősen befolyásolhatja a repülésbiztonságot és az üzemeltetést. Ezen kiberfenyegetések kezelése érdekében a fejlett kiberbiztonsági protokollok és a személyzet folyamatos oktatása kulcsfontosságú lehet az EFB-rendszerek és a kapcsolódó informatikai infrastruktúra védelmében.
- (HT 2.) A Boeing vállalatot ért kibertámadások elemzése rávilágíthat arra, hogy a légitársaságok és a repülési szolgáltatások számára szükséges az EFB-rendszerek és a kapcsolódó informatikai infrastruktúra kiberbiztonsági kockázatainak proaktív kezelése, beleértve a rendszeres sebezhetőségi felülvizsgálatokat és a kiberbiztonsági incidensre való reagálási tervek kidolgozását. Az ilyen intézkedések jelentős mértékben csökkenthetik a kibertámadásokból eredő károkat, és biztosíthatják a légi közlekedés folyamatos és biztonságos működését.

A kutatás során alkalmazott módszertanként elsődlegesen a nemzetközi és a kevésbé jellemző hazai releváns szakirodalmak és információt biztosító oldalak feldolgozásával az EFB-rendszerek használatát, valamint működésének jellegét határozzuk meg. Ezt követően bemutatjuk a közelmúltban történt releváns kiberincidenseket kronológiai sorrendben, majd ajánlásokat teszünk a kockázatok lehetséges csökkentésére.

Informatikai és műveleti rendszerek a civil légi közlekedésben

Mára a kiberműveletek és a kibertámadások átszövik az élet minden területét. Nem képez kivételt ez alól a repülés, a légiirányítás, a repülőterek elleni támadások, illetve az ezen támadások elleni védelem sem.[4] A repülés teljes folyamata során alkalmazott rendszereket, szolgáltatásokat számos szempont szerint lehet csoportosítani:

- repülőgépek, repüléshez kapcsolódó eszközök, rendszerek (repülőgépek és elektronikai rendszerei, radarok, radarrendszerek, világítórendszerek stb.) tervezése, gyártása, üzemeltetése;
- repülőtéri utaskezelés (induló- és átszállójegy, valamint poggyász kezelése, beszállókártya és más forgalmi vonatkozások: repülőgép súly- és egyensúlyszámítása, rakodástervezés, konténeres rendezés, utashely foglalása, tarifálás, jegykiállítás);

[4] Szabó–Tóth 2013: 89–113.

- légiáru *(cargo)* helyfoglalása, tarifálás, okmányolás, raktári funkciók, járat-előkészítés, különleges árukategóriák, valamint a cargo kapcsolatrendszere a nemzetközi ügynökségi disztribúcióval, vámmal, repülőtéri funkciókkal stb.;
- légitársasági és repülőtéri automatizálás (nemzetközi poggyászkeresés és adminisztráció, utast és poggyászt összekötő és biztonsági megfeleltető megoldások, fizikai poggyászosztályozás és -irányítás, járatinformációs rendszerek);
- légitársasági operatív üzemirányítás: útvonal- és hálózattervezés, menetrend- és géprotáció-tervezés, menetrendszerkesztés és napi operatív menetrendi funkciók, repülőgépek műszaki karbantartásának tervezése és termelésirányítási rendszerek, hajózószemélyzet-tervezés és -vezénylés, navigációs rendszerek (útvonal- és üzemanyag-tervezés, repülési feltételek vizsgálata, például meteorológia), digitális föld-levegő kapcsolat.[5]

Ahogyan az az osztályozásból kikövetkeztethető, minden rendszerben megtalálható az informatika, az üzemeltetés nélkülözhetetlen alkotórésze az információs rendszer, amelynek számos eleme befolyásolható lehet, akár egy részegység működésének átprogramozásával, akár egy teljes rendszerbe történő behatolással, a rendszer irányításának átvételével. Fontos, hogy egy ilyen rendszer, a társaság vagy a szervezet méretétől függően, akár az egész világra is kiterjedhet. Mindenképpen mérlegelni kell azt is, hogy a fenti rendszerek különböző, más szervezetek által üzemeltetett elemekkel, hálózatokkal vannak kapcsolatban. Az ezekben lévő informatikai hiányosságok, illetve az ezek ellen indított támadások hatása befolyásolja a kapcsolódó egyéb rendszereket, szolgáltatásokat, ezáltal a repülést is.[6]

EFB

A pilótáknak rengeteg dokumentumot és információt kell ismerniük a repülés tartalmától függően. Ezen dokumentumok egy részének a repülés során fizikailag is elérhetőnek kell lennie. Ezek a fizikailag kötelező dokumentumok főként a repülőgép üzemeltetési kézikönyveit és a vészhelyzeti ellenőrző listákat, a teljesítményre és a súlyegyensúlyra vonatkozó irányelveket tartalmazzák. Ezenkívül vannak repülési dokumentumok is, amelyek a repülni kívánt útvonaltól és a leszálló gépeket fogadó repülőterektől függően változnak. Ezek a repülési dokumentumok tartalmazzák a légitársaság térképeit, a le- és felszállási területek süllyedési tervét, valamint a tartalék és vészleszállási területek süllyedési terveit is. Mindez rengeteg mappát eredményez, amelyeket a pilótáknak magukkal kell vinniük és használniuk.

A tablettechnológiák fejlesztése és a polgári légi közlekedési hatóságok általi használat eredményeként a repülési műveletekhez elérhetővé váltak az úgynevezett electronic flight bag-ek (EFB), amit magyar nyelvre leginkább „elektronikus repülőtáskának" lehetne fordítani. A légi úti térképeket és a leszállópályákat nyomtatott papírként előállító cégek most a „papírmentes pilótafülke" koncepcióra váltanak

[5] Gonda 2005: 14–15.
[6] Horváth 2020.

az általuk tervezett szoftverrel. Ahogy már fentebb szó volt róla, hagyományosan a pilóták papíron kapták meg a szükséges információkat. Manapság ezek az információk digitális formában vannak jelen. Az ilyen digitális adatok eléréséhez megkezdték a repülőgéprendszerekbe beágyazott vagy hordozható táblagépek alkalmazását. Az EFB név a pilóták által hordozott hagyományos repülőtáskákból ered, amelyek rengeteg papíralapú repülési ellenőrző listát tartalmaztak, repülési és időjárási térképeket, kézikönyvek köteteit.[7] A navigációs térképek, kézikönyvek és tanácsok létfontosságú források a repülési műveletekhez, főként a repülés kritikus szakaszaiban.[8] Ezeknek a dokumentumoknak a repülés közben gyorsan hozzáférhetőnek kell lenniük, mégpedig a repülésbiztonság veszélyeztetése nélkül. Az érintőképernyős eszközök megjelenése együttműködésre motiválta a repülőgépgyártókat és a repüléskezelő szoftverekre szakosodott szoftverfejlesztőket, mint például a Jeppesen, a ForeFlight és a Garmin cégeket. Együtt megoldásokat dolgoztak ki a papíralapú űrlapok elektronikus másolatokra való áttelepítésére.[9] A szoftverfejlesztők migrálták a repülőgép-dokumentumok papíralapú változatait, és integrálták a repülőgépteljesítmény-alkalmazásokat egy elektronikus platformba, amely táblagépeken lett elérhető.[10]

1. ábra: Boeing Jeppesen ForeFlight Mobile EFB mobil applikáció
Forrás: https://d32dgjuo8qzfhk.cloudfront.net/assets/foreflight_mobile_hero_www.png

7 Ateş 2017.
8 Babb 2017a.
9 Ohme 2014.
10 Babb 2017b.

Ezeknek a rendszereknek köszönhetően jelentősen csökkent a pilóták és a hajózószemélyzet fizikai terhelése. Az elektronikus repülőtáskák költséghatékonyak és felhasználóbarátak. Az új fejlesztéseknek és szabályoknak megfelelően felhasznált dokumentumok folyamatosan frissülnek. A pilótáknak a repülés megkezdése előtt meg kell győződniük arról, hogy az általuk használt dokumentumok minden módosítása frissült. Az összes dokumentum gyors elérése külön kihívást jelent.[11]

Az EFB közvetítő szerepet tölt be a pilóta és a légi közlekedésben részt vevő civil és katonai szervezetek, illetve társaságok között azáltal, hogy átláthatóvá teszi a légi járművek működési nyilvántartásait. Lehetőséget biztosít a pilótafeladat-folyamatok vagy validálások digitalizálására, valamint megakadályozhatja a dokumentumok elvesztését is. Továbbá a Global Position Systems (GPS) beépítésével az EFB-be a pilóták megtekinthetik a mozgó repülőtéri térképeket, ami csökkentheti a pilóták munkaterhét.[12]

Összességében az EFB a hagyományos papíralapú repülési anyagok digitális megfelelője. Hatékony hozzáférést biztosít az információk széles köréhez, ezáltal javítja a repülés előtti tervezést és a repülés közbeni műveleteket. Az EFB-k döntő szerepet játszanak a légi közlekedés modernizálásában, javítva a hatékonyságot, a biztonságot és a kényelmet a pilóták és a légitársaságok számára egyaránt. A komplex, hatékony előnyök mellett számos kockázatot is rejt a rendszer. Mint minden technikai eszköz, az EFB esetében is számolni kell hardver- és szoftverhibával. A műszaki jellegű hibák mellett a szabályozási kérdések és a technológiai függőség is jelentős lehet. A téma szempontjából a tárolt információk biztonságának szerepe kulcsfontosságú, ennek információ- és kiberbiztonsági megközelítése elengedhetetlen.

NOTAM

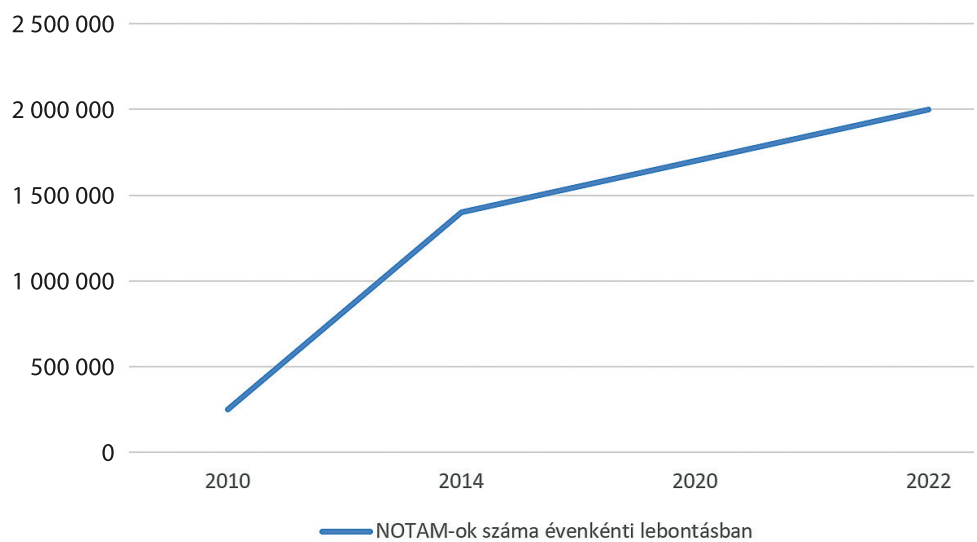
A NOTAM *(Notice to Airmen)* egy iparági kifejezés a légi közlekedési hatóságok által kiadott értesítésekre, amelyek célja a pilóták figyelmeztetése a repülési útvonalon felmerülő lehetséges veszélyekre. A légügyi hatóságok által kiadott közlemény rendeltetése a pilóták és más repülőszemélyzet tájékoztatása a légtér, a repülőterek vagy a navigációs eszközök, berendezések működésével kapcsolatos fontos információkról. A NOTAM-ok olyan lényeges információkat tartalmaznak, amelyek befolyásolhatják a repülés biztonságát, például a kifutópályák elérhetőségének változásáról, ideiglenes repülési korlátozásokról, navigációs segédeszközök kieséséről vagy a repülési útvonalon lévő veszélyekről. A veszélyekről szóló értesítések közzétételének elmulasztása kockázatot jelenthet a repülőgépekre és a repülésbiztonságra.[13] A Szövetségi Légi Közlekedési Hivatal (Federal Aviation Administration, FAA) szerint, amely az USA közlekedési minisztériumán belül működő ügynökség, a NOTAM olyan információkat tartalmaz, amelyek alapvető fontosságúak a repülést üzemeltető személyzet számára, és amelyek nem voltak ismertek eléggé előre ahhoz, hogy más módon terjeszthessék.

[11] Özkan–Aksoy–Şensoy 2021.
[12] Suppiah et al. 2020.
[13] Boeing Subsidiary Jeppesen Suffers Cyberattack 2023.

Értesíti a pilótákat különösen a Nemzeti Légtérrendszer (National Airspace System, NAS)[14] valamely összetevőjének rendellenes állapotáról. A NOTAM-okat az FAA számos különböző okból bocsátja ki, de elsősorban azért, hogy tájékoztassák a pilótákat a repülőtereket, a légi utakat és a helyi eljárásokat érintő változásokról, amelyek hatással lehetnek a személyzet vagy a földön tartózkodók biztonságára. Sokféle NOTAM létezik, beleértve a nemzetközi, a hazai, a katonai és a polgári NOTAM-okat. Lehetnek tanácsadó jellegűek vagy kötelező utasítások.[15]

Mindezek alapján látható, hogy a NOTAM-ok létfontosságúak a repüléstervezés és a biztonságos repülés lebonyolítása szempontjából, mivel valós idejű tájékoztatást nyújtanak a repülési műveleteket befolyásoló körülményekről. A pilótáknak minden repülés előtt át kell nézniük a NOTAM-okat, hogy tisztában legyenek a légtérben bekövetkező változásokkal vagy veszélyekkel. Ennek megfelelően az információk biztonsága kiemelt fontosságú, az esetleges incidensek beláthatatlan következményekkel járhatnak.

A NOTAM-ok száma évről évre folyamatosan növekszik. Míg 2010-ben 250 ezer NOTAM-ról beszélhettünk, ez a szám 2022-re meghaladta a kétmilliót.



2. ábra: A nemzetközi NOTAM-ok számának alakulása 2010–2022 között
Forrás: a szerzők szerkesztése PUFAHL *2022 alapján*[16]

[14] A NAS alatt az Egyesült Államok légterét, navigációs létesítményeit és repülőtereit, a hozzájuk kapcsolódó szolgáltatásokat és valamennyi szabályt, előírást, eljárást értjük, az ide tartozó személyzettel és felszerelésekkel együtt.
[15] *A repülésben használt NOTAM-ok különböző típusai* [é. n.].
[16] Global NOTAM Campaing 2022.

Az EFB-k kiberbiztonsági tényezői

Az EFB-megoldások számos előnnyel járnak, ugyanakkor érzékenyek a kiberbiztonsági sebezhetőségekkel és fenyegetésekkel szemben. E kihívások megértése alapvető fontosságú a légi közlekedési műveletek védelme szempontjából. Az EFB-rendszerekben lévő sebezhetőségek és veszélyek három fontosabb terület köré sorakoztathatók fel.

Az első a *külső kibertámadások.* Az EFB-rendszerek potenciális célpontjai a sebezhetőségeket kihasználni, jogosulatlan hozzáférést szerezni, adatokat manipulálni vagy a műveleteket megzavarni kívánó rosszindulatú szereplőknek.

A második terület a *belső fenyegetések és emberi tényezők.* A humán tényező olyan kockázatokat hordoz magában, mint például a nem szándékos hibák, hanyagság vagy szándékos, rosszindulatú tevékenységek, visszaélések az EFB-rendszerekhez magas hozzáféréssel rendelkező „bennfentesektől".

A harmadik terület az *adatszivárgás és jogosulatlan hozzáférés*. Az EFB-k érzékeny információkat tárolnak, beleértve az előzőekben már említett repülési terveket, az utasok jegyzékeit és a repülőgép teljesítményadatait, amelyek miatt vonzó célpontok a kiberbűnözők számára.

Az üzembiztonságra gyakorolt lehetséges hatásait szintén három alapvető területre lehet bontani: Az egyik a *repülési adatok és navigációs rendszerek manipulálása.* Az EFB-ket célzó kibertámadások manipulálhatják a repülési adatokat, a navigációs térképeket, vagy akár megváltoztathatják a kritikus repülési paramétereket, ami helytelen repülési pályákhoz, a helyzetfelismerés megsértéséhez és potenciális repülésbiztonsági veszélyekhez vezethet.

A második a *kommunikációs rendszerek kompromittálása*. Az EFB-k kommunikációs csatornákra támaszkodnak valós idejű időjárás-frissítések, légi forgalmi irányítási kommunikáció és egyéb kritikus információk érdekében. Az ilyen rendszerek megsértése megzavarhatja a kommunikációt és veszélyeztetheti az üzembiztonságot.

A harmadik pedig az *EFB működésének megzavarása*. A kiberbiztonsági incidensek, mint például a rosszindulatú programok fertőzései vagy a szolgáltatásmegtagadási támadások, megzavarhatják az EFB-rendszerek működését, akadályozva a repülési műveleteket, és befolyásolhatják a járatok, repülések általános biztonságát és hatékonyságát.

A kiberbiztonsági és információbiztonsági kockázatok mérséklése érdekében a légitársaságoknak és a légi közlekedési hatóságoknak szilárd biztonsági intézkedéseket kell bevezetniük, beleértve a titkosítást, a hitelesítést, a hozzáférés ellenőrzését, a behatolásjelző rendszereket és a rendszeres biztonsági ellenőrzéseket. Emellett a pilóták és a személyzet számára szervezett folyamatos kiberbiztonsági tudatossági képzés elengedhetetlen a biztonsági tudatosság előmozdításához a légi közlekedési ágazatban. A légi forgalmi társaságok ellen irányuló kibertámadások jelentős kockázatot jelentenek a repülésbiztonságra, az üzemeltetés integritására és az utasok bizalmára nézve. Az ágazatban az alábbi alapvető kockázatok, támadási formák okoznak, okozhatnak problémát.

Alapvető veszélyt jelentenek az *adatvédelmi incidensek.* Az EFB-k az előzőekben meghatározott, repüléssel kapcsolatos érzékeny információkat tárolnak, beleértve a navigációs térképeket, repülési terveket és üzemeltetési adatokat. Ha ezek az eszközök

nincsenek megfelelően biztosítva, akkor sérülhetnek az adatok, ami a bizalmas információkhoz való jogosulatlan hozzáférést vagy azok ellopását eredményezheti.

Az egyéb, általános célú információs rendszerekhez hasonlóan a *rosszindulatú programok és vírusok* hasonló veszélyt jelentenek. Az EFB-k, mint minden elektronikus eszköz, fogékonyak a rosszindulatú szoftverekre és vírusokra. Ha egy EFB megfertőződik, az veszélyeztetheti a repülési adatok integritását, megzavarhatja a működést, vagy lehetővé teheti a támadók számára, hogy jogosulatlanul hozzáférjenek a kritikus rendszerekhez.

Ehhez kapcsolódik a *jogosulatlan hozzáférés*. A gyenge hozzáférés-ellenőrzés vagy a nem megfelelő hitelesítési mechanizmusok lehetővé tehetik, hogy illetéktelen személyek hozzáférjenek az EFB-khez vagy a rajtuk tárolt érzékeny információkhoz. Ez a repülési tervek, navigációs adatok vagy más kritikus rendszerek jogosulatlan módosításához vezethet.

A *szolgáltatásmegtagadás-alapú támadások (DoS)* alapvetően korlátozhatják az információkhoz való hozzáférést. Az EFB-k a valós idejű adatokhoz, időjárás-frissítésekhez és egyéb szolgáltatásokhoz való hozzáféréshez hálózati kapcsolatra támaszkodnak. A szolgáltatásmegtagadásos támadás megszakíthatja a kapcsolatot, megakadályozva a pilótákat abban, hogy repülés közben hozzáférjenek az alapvető információkhoz, ezzel befolyásolva a helyzetfelismerést és a döntéshozatalt. A kibertérből érkező fenyegetések mellett fontos figyelembe venni a *fizikai biztonsági kockázatokat*. Az EFB-k olyan hordozható eszközök, amelyeket a pilóták a repülőgép fedélzetén hordoznak. Tehát ha egy EFB elveszik, ellopják vagy manipulálják, az potenciálisan veszélyeztetheti az érzékeny információkat, vagy biztonsági réseket hozhat létre a légi közlekedés ökoszisztémájában. Az utolsó kiemelt terület az *ellátási lánc kockázatai*. Az EFB-k különböző gyártóktól származó hardverkomponensekből és szoftveralkalmazásokból állnak. Az ellátási lánc kockázatai, például a hamisított alkatrészek, a rosszindulatú firmware vagy a nem biztonságos szoftverek olyan sebezhetőségeket hozhatnak létre az EFB-kben, amelyeket a támadók kihasználhatnak.

Az előzőekben leírtak jól alátámasztják, hogy a komplex védelmi tevékenységek elengedhetetlenek a fent említett, kiemelt támadások ellen. Az információbiztonság minden részterületére kiemelt hangsúlyt kell fektetni, amelyek mára már nemcsak a repülőgépekre mint eszközökre vonatkoznak, hanem a teljes kapcsolódó infrastruktúrára, rendszerekre és személyi állományra is.

A Boeing multinacionális vállalatot ért kibertámadások

Az előzőekben felsorolt veszélyforrások, támadási módszerek egyéb repülési rendszereket vagy a légi közlekedéshez köthető alrendszereket is fenyegetnek. Amennyiben a támadók hozzáférést szereznek a kritikus repülési rendszerekhez, manipulálhatják a navigációs vezérlőket, megváltoztathatják a repülési útvonalakat, megzavarhatják a fedélzeti rendszereket. Az ilyen támadások a repülőgép feletti irányítás elvesztését, a levegőben történő baleseteket vagy engedély nélküli leszállást eredményezhetnek.

A repülési társaságok hatalmas mennyiségű érzékeny információt tárolnak, beleértve az utasok adatait, a repülési menetrendeket és az üzemeltetési részleteket.

Az adatszivárgás személyes információk, pénzügyi adatok vagy védett üzleti adatok nyilvánosságra kerüléséhez vezethet, ami károsíthatja a vállalat hírnevét, és pénzügyi veszteségeket okozhat.

A légitársaságok foglalási rendszereit, járattervezési szoftvereit vagy kommunikációs hálózatait célzó kibertámadások megzavarhatják a járatok működését, ami járatkésésekhez, járattörlésekhez vagy logisztikai kihívásokhoz vezethet. Ezek a zavarok a teljes légi közlekedési ökoszisztémára hatással lehetnek, több érdekelt felet érintve és jelentős gazdasági hatást okozva. A 3. ábra a légi közlekedési iparhoz köthető, 2022-ben történt kibertámadásokat mutatja be.

3. ábra: Légiiparhoz köthető kiberincidensek 2022-ben
Forrás: a szerzők saját szerkesztése, online: https://konbriefing.com/en-files/cyber-attacks/2022-ind-aviation-tl-en.png [17]

A KonBriefing Research 2022-re vonatkozóan összesen 114 sikeres kibertámadást azonosított az alábbi iparágak vállalatai és szervezetei ellen: repülés (38); közlekedés (32);

[17] KonBriefing 2022.

repülőterek (21); légitársaságok (10); repülés és védelem (4); közszféra (2); katonaság (2); egyetemek (1); technológia (1); szolgáltatók (1); mentés (1); egészségügy (1).[18]

A leggyakoribb általános támadási formák a légi közlekedéshez kapcsolódóan is megjelennek. A zsarolóprogram-támadások kritikus rendszereket vagy adatokat titkosíthatnak, és a visszafejtésért a támadók pénzt követelnek. Ha a repülőcégek rendszereit zsarolóvírusos támadás éri, az működési leálláshoz, pénzügyi veszteségekhez és hírnévkárosodáshoz vezethet. Emellett fennáll a veszélye annak, hogy a váltságdíj kifizetése esetén is érzékeny információk kerülnek nyilvánosságra. Social engineering technikákat vagy adathalász e-maileket szintén használhatnak a támadók, hogy a repülőtársaságok alkalmazottait, pilótáit vagy az érzékeny rendszerekhez hozzáféréssel rendelkező személyzetet célba vegyék. Ha ezek a támadások sikeresek, akkor az rendszerekhez való jogosulatlan hozzáférést, adatlopást vagy rosszindulatú szoftverek telepítését eredményezheti.

Az elmúlt néhány évben a nemzetközi repülőterek földi és légi infrastruktúrájának működtetése egyre bonyolultabb technológiákat, automatizált rendszereket követelt, ami megnövelte a repülőterek és a légi közlekedési ágazat sérülékenységét a számítógépes bűnözőkkel és a terroristákkal, valamint azon bennfentes alkalmazottakkal szemben, akik az adatok ellopásával, a kritikus infrastruktúrák működési biztonságának akadályozásával zavart, bizonytalanságot, fennakadásokat kívánnak kelteni. Ezeket az állapotokat a járvány okozta helyzet még tovább súlyosbította. A légi közlekedési ágazat informatikai beruházásainak szintje 2014–2019 között 21,4 milliárd dollárról 35,2 milliárd dollárra növekedett. A teljes IKT- (információs és kommunikációs technológia) beruházásokon belül a kiberbiztonság növelését célzó fejlesztések aránya 2016-ban 4,6%; 2017-ben 7%; 2018-ban 9% és 2019-ben 14% volt.[19] A repülőterek kiberfenyegetettségekkel szembeni ellenállásának javítása azonban nem kizárólag a pénzügyi forrásokon múlik, ehhez az egyes repülőterek kiberbiztonsági érettségi szintjét is növelni szükséges. Ezen szemléletváltáshoz a járvány utóhatásai valószínűleg hozzá fognak járulni. Szükségeltetik egy tudatos kiberbiztonsági politika megfogalmazása a kockázatok rendszeres feltérképezésével és beazonosításával; információk, kiberbiztonsági incidensek, tapasztalatok, tanulságok, legjobb gyakorlatok kölcsönös megosztásával; valamint a hálózatos együttműködés kiépítése és megfelelő szabályozási környezet kialakítása a munkavállalók érzékenyítésével és a kiberbiztonsági tudatossági szint képzésekkel, tréningekkel történő emelésével.

Boeing-kiberincidens, 2018

A Boeing vállalatot 2018 márciusában érte WannaCry vírusos informatikai támadás. A Microsoft Windows XP szoftverének gyengeségeit kihasználva az úgynevezett WannaCry kibertámadás világszerte széles körű zavarokat okozott. Több százezer számítógépet fertőzött meg. Célja, hogy megakadályozza a felhasználók adatokhoz való hozzáférését, amíg váltságdíjat nem fizetnek, gyakran kriptovalutában.

[18] Cyber Attacks on the Aviation Industry in 2022. Statistics: Ransomware, Data Breaches, DDoS Attacks 2023.
[19] Florent 2020.

A vírus elsőként 2017. május 12-én jelent meg, és képes volt gyorsan terjedni a Windows operációs rendszereket futtató számítógépek között. A zsarolóvírus-támadás az évtized egyik legpusztítóbbja volt, több mint 150 országban érintett magánszemélyeket és szervezeteket. Megbénította az Egyesült Királyság kórházait, leállította a gyártósorokat, és felborította az emberek életét. A spanyol Telefónica távközlési vállalat az elsők között számolt be a támadásról, majd gyorsan terjedt Európa számos országában.

A Microsoft javításokat bocsátott ki a sebezhetőség orvoslására, habár egyes vállalatok, mint például Corey Nachreiner, a WatchGuard Technologies technológiai igazgatója szerint, óvakodnak a gyakori frissítésektől, attól tartva, hogy ez veszélyeztetheti egyedi rendszereiket. A Microsoft nem kívánta kommentálni a Boeing elleni kibertámadást.[20]

A támadás kezdetben aggodalmat keltett a Boeing vállalaton belül, különösen azért, mert attól féltek, hogy a vírus kárt tehet a kulcsfontosságú repülőgépgyártási eszközökben. Ennek ellenére a vállalat vezetése hamarosan közölte, hogy sikerült minimalizálniuk a támadás okozta károkat.

A helyzet napközben jelentős aggodalmat váltott ki mind a Boeing munkatársai, mind a légitársaságok között, de estére a vállalat megnyugtatást adott. Linda Mills, a Boeing Commercial Airplanes kommunikációs igazgatója kijelentette: „Elvégeztük a végső értékelést" – utalva arra, hogy a probléma csupán néhány gépet érintett, és hogy szoftverfrissítésekkel sikerült orvosolniuk a helyzetet. „Nem érintette a 777-es jet programját vagy bármely más programunkat." Mike VanderWel, a vállalat gyártásmérnöki részlegének vezetője az események kezdetén figyelmeztető üzenetet küldött, amely komoly aggodalmakat vetett fel, de ezek a félelmek alaptalannak bizonyultak.

A délutáni órákban a Boeing hivatalos közleményt adott ki, amelyben Mills elmagyarázta a helyzet kezeléséhez szükséges lépéseket, beleértve az IT-csapat teljes körű bevonását és a tények pontos azonosítását. Ebben a közleményben arra is rámutatott, hogy a kiberbiztonsági műveleti központ csak korlátozott számú rosszindulatú program behatolását észlelte, amit sikeresen kezeltek anélkül, hogy ez bármilyen termelési vagy szállítási problémát okozott volna.

Boeing-kiberincidens, 2022

A Jeppesen, amely vállalat a Boeing teljes tulajdonában áll, élen jár a légi navigációs szolgáltatások terén. Navigációs adatbázisokat, repüléstervezési alkalmazásokat kínál EFB-khez, valamint portfóliójába tartozik a NOTAM-kezelés is.

2022. november 2-án több Jeppesen-szolgáltatás is leállásra kényszerült, ami a következő figyelmeztetés megjelenését eredményezte a vállalat weboldalán (4. ábra):

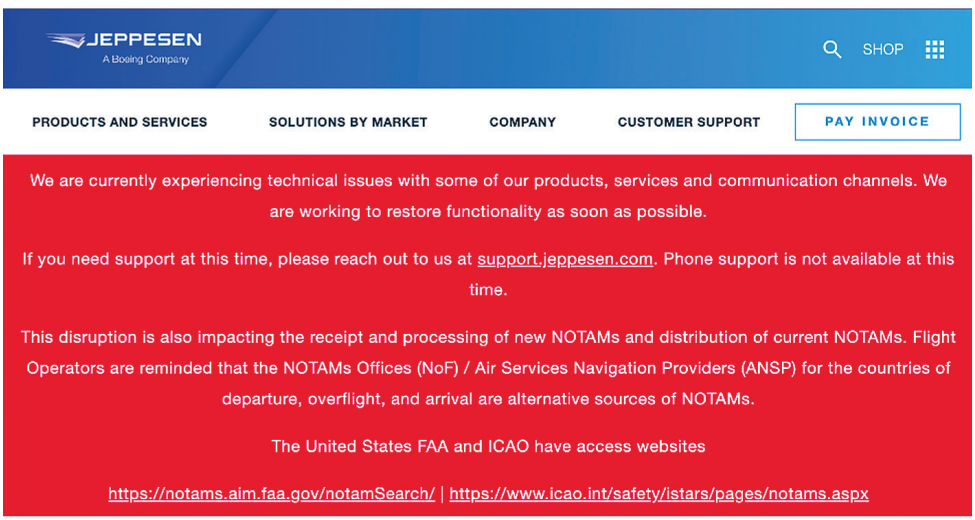
„Jelenleg technikai problémákat tapasztalunk egyes termékeinkkel, szolgáltatásainkkal és kommunikációs csatornáinkkal kapcsolatban. Dolgozunk a működőképesség mielőbbi

[20] Gates 2018.

helyreállításán. Ha jelenleg segítségre van szüksége, forduljon hozzánk a support.jeppesen.com címen. Telefonos támogatás jelenleg nem érhető el."[21]

A Boeing hivatalos közleményében a következőképpen nyilatkozott:

„Leányvállalatunk, a Jeppesen, kiberincidenst tapasztalt, amely bizonyos repüléstervezési termékeket és szolgáltatásokat érintett. A repüléstervezésben némi fennakadás történt, de jelenleg nincs okunk azt hinni, hogy ez az incidens veszélyt jelentene a repülőgépekre. Folyamatosan kommunikálunk az ügyfelekkel és a szabályozó hatóságokkal, és azon dolgozunk, hogy a lehető leghamarabb helyreállítsuk a teljes körű szolgáltatást."[22]



4. ábra: Jeppesen-közlemény a kibertámadás miatt nem működő elemekre, mint például a NOTAM
Forrás: Zee 2022

A támadás természetét, a károk kiterjedését, egyéb részleteket, valamint a helyreállítás várható időpontját a Boeing akkor nem kívánta ismertetni, és később sem mutattak be részletesebb információkat az ügyről.

A kibertámadás a légi közlekedés tekintetében jelentős kockázatokkal járhat, amelyekre fel kell készíteni és megfelelően támogatni a repülőgép-személyzetet és a légi közlekedéshez köthető valamennyi résztvevőt. Az FAA által kiadott, úgynevezett FAA Advisory Circular 90-100A az üzemeltetéshez kapcsolódó, útvonalakra, eljárásokra és egyéb üzemeltetéshez köthető szabványokra, szabályokra vonatkozó „tanácsadó körlevél", kiadvány. Ezek tájékoztató jellegűek, nem kötelező érvényű ajánlások. Az AC 90-100A szerint a fedélzeti navigációs adatoknak naprakésznek és a tervezett műveleti régióval összhangban kell lenniük, beleértve a navigációs segédeszközöket,

[21] Klint 2022.
[22] Thurber 2022.

útpontokat és a terminálra vonatkozó eljárásokat.[23] Mindehhez kapcsolódik Rich Pickett pilótának, a Personal Wings Inc. munkatársának a kiberincidenshez fűzött megjegyzése is:

„Ha a pilóta VFR[24]-es, noha előfordulhat biztonsági probléma a lejárt GPS-adatbázissal való repülés során, attól még VFR esetében ez nem előírás. Az IFR[25] esetében előírás. Az adatbázisnak aktuálisnak kell lennie, vagy más forrásból, például az FAA-grafikonokból leellenőrzöttnek kell lennie. Az IFR-terminálejárások esetében az FAA-diagramokkal való keresztellenőrzéssel ellenőrizniük kell, hogy az eljárások nem változtak-e az előző ciklushoz képest. Ha az útpont adatai megváltoztak, a pilóta nem használhatja az RNAV[26] megközelítést. A keresztezési magasságok és minimumok változásai azonban jelentős biztonsági problémákat okozhatnak, különösen a robotpilótával összekapcsolt megközelítéseknél. Más szavakkal: növeli a pilóták munkáját, és hatással van a biztonságra."[27]

A kiberbiztonság továbbra is jelentős aggodalom forrása a légi közlekedésben. A szolgáltatásmegtagadási támadásoktól – amelyek több repülőtéri weboldalt is érintettek – egészen a légitársaságokat célzó zsarolóvírus-támadásokig. Az Európai Légiközlekedés-biztonsági Szervezet 2021-es jelentése szerint a kibertámadások száma minden fenyegetési kategóriában nőtt, ami éves szinten 530%-os emelkedést jelent.[28]

Boeing-kiberincidens, 2023

2023. október 27-én a Boeing neve megjelent a LockBit weboldalán, ahol november 2-ig adtak időt a vállalatnak a kapcsolatfelvételre és a tárgyalások megkezdésére annak érdekében, hogy ne kerüljenek nyilvánosságra adatok komoly károkat okozva. A csoportnak nagy mennyiségű érzékenynek minősített adatot sikerült megszereznie.

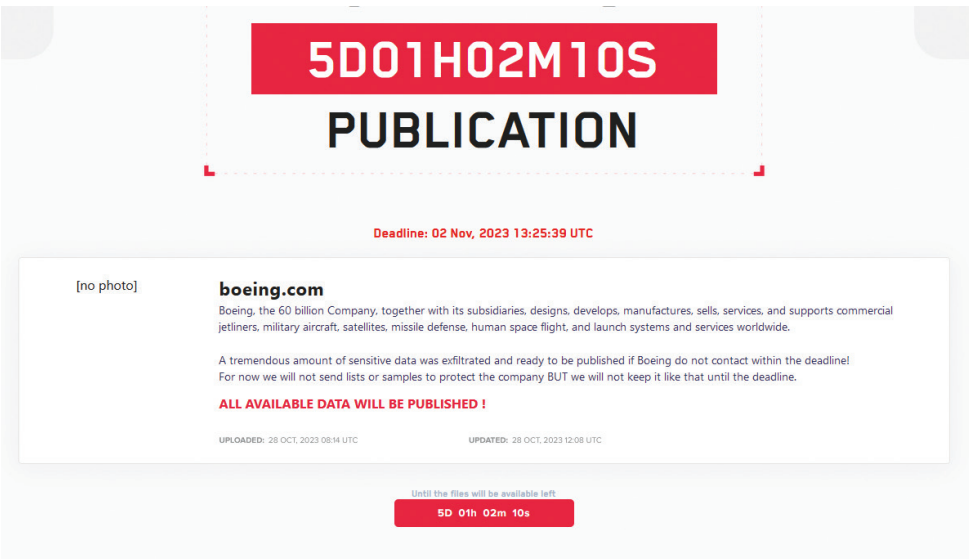
Egy rövid időre a Boeing eltűnt a LockBit áldozatainak listájáról, de november 7-én ismét felkerült, amikor a csoport kijelentette, hogy figyelmeztetéseiket figyelmen kívül hagyta a cég. November 10-én a LockBit közzétette a weboldalán a Boeingtől származó összes adatot, amelyek között IT-menedzsment-szoftverek biztonsági mentései, monitoring- és auditeszközök naplói találhatók. A hackercsoport közel 50 GB adatot szivárogtatott ki a Boeingtől, miután az nem volt hajlandó fizetni. A kiszivárogtatott információk nagy része biztonsági mentés volt, ezek között szerepeltek 2023. október 22-én készültek is.

A szivárgásban szereplő Citrix eszközök biztonsági mentései arra utalnak, hogy a LockBit kihasználhatta a Citrix Bleed sebezhetőségét (CVE-2023-4966), ennek igazolására október 24-én jelentek meg bizonyítékok.

[23] U.S. Department of Transportation 2015.
[24] VFR: Visual Flight Rules – „látvarepülési" szabályok, vizuális repülési szabályok.
[25] IFR: Instrument Flight Rules (műszeres repülési szabályok).
[26] RNAV: Area Navigation (területi navigáció).
[27] Personal Wings 2022.
[28] Britton 2022.

A Boeing megerősítette, hogy kibertámadás érte őket, de ebben az esetben sem árult el részleteket arról, hogyan történt a „betörés". A vállalat kiemelte, hogy a kiberbiztonsági incidens most sem veszélyezteti a repülésbiztonságot, és aktívan együttműködnek a bűnüldöző és szabályozó hatóságokkal az eset kivizsgálásában. A Boeing biztosította ügyfeleit, hogy a támadás nem érintette repülőgépeik működését, viszont továbbra is kérdéses maradt, hogy a hackerek pontosan mennyi adatot szereztek meg.[29]

A LockBit csoport ransomware-as-a-service (RaaS) szolgáltatást nyújt, több mint négy éve aktívan okoz károkat különböző szektorokban, az autóipartól kezdve a postai szolgáltatásokig. Az Egyesült Államok kormánya szerint a csoport 2020 és 2023 között több mint 1700 támadással közel 91 millió dollárt zsarolt ki, de tevékenységük globális szinten is jelentős. Például 2023 augusztusában a spanyol rendőrség figyelmeztetett egy LockBit által végrehajtott adathalászati kampányra, amely spanyol építőipari vállalatokat vett célba.[30]



5. ábra: Boeing-zsarolás a LockBit adatszivárgási oldalon
Forrás: Gatlan 2023

Kutatási eredmények

A Boeinget ért kiberbiztonsági incidensek rávilágítanak a nagyvállalatok előtt álló jelentős kihívásokra és kockázatokra, amelyekkel kényes információik és kritikus rendszereik kiberfenyegetésekkel szembeni védelme során szembesülnek. A kibertámadások kockázatának mérséklése érdekében a repülési vállalatoknak prioritásként

[29] Raj 2023.
[30] Ilascu 2023.

kell kezelniük a kiberbiztonsági intézkedéseket, például a robusztus hálózati biztonsági protokollok bevezetését, a szoftverek és rendszerek rendszeres frissítését, a munkavállalók kiberbiztonsági képzését, valamint az iparági partnerekkel való együttműködést a fenyegetésekkel kapcsolatos információk és a legjobb gyakorlatok megosztása érdekében. Emellett a szabályozó hatóságok döntő szerepet játszanak a kiberbiztonsági előírások betartatásában és a kiberbiztonsági kultúra előmozdításában a légi közlekedési ágazaton belül. Összességében tehát a kibertámadásokból levont következtetések kiemelik, hogy fontos a kibervédelem, a felkészültség minden részterületének folyamatos javítása a mai digitális környezetben működő szervezetek számára.

Lényeges továbbá kiemelni, hogy a Boeing az olyan vállalatok egyike, amelyek a polgári életben alkalmazott légi járművek gyártása mellett a védelmi iparban is jelentős szerepet játszanak repülőgépek, helikopterek, rakéták, műholdak és egyéb védelmi rendszerek tervezésével és gyártásával. Ezt figyelembe véve a kibertámadások elleni küzdelem hangsúlyosabbá válása vitathatatlan.

A Boeing által elszenvedett kibertámadások élesen emlékeztetnek arra, hogy a kritikus légi közlekedési infrastruktúra védelme, valamint a légi közlekedés biztonságának és védelmének biztosítása érdekében az egyre inkább digitalizálódó világban sürgősen átfogó kiberbiztonsági stratégiákra van szükség.

Az előzek alapján mit tehetünk, amikor egy partnercég kibertámadás áldozatává válik, és ez potenciálisan érinti a saját szervezet biztonságát vagy működését? Több kiberbiztonsági ellenlépést is meg kell fontolni annak érdekében, hogy minimalizáljuk a károkat, és megőrizzük a saját rendszereink integritását. Az alábbi néhány lépést érdemes végrehajtani, amelyek általános érvényűek szakterülettől függetlenül:

1. Azonnali értesítés és kommunikáció
   - Értesítse a saját kiberbiztonsági csapatát vagy szolgáltatóját a partnercég kibertámadásáról.
   - Létesítsen kommunikációs csatornát a partnercég és a saját szervezete között a támadással kapcsolatos információk és frissítések megosztására.
2. Hálózati elszigetelés
   - Izolálja azokat a hálózati szegmenseket, rendszereket vagy alkalmazásokat, amelyek közvetlenül kapcsolatban állnak a támadás által érintett partnerrel, hogy megakadályozza a potenciális kártékony tevékenységek terjedését.
3. Hozzáférés ellenőrzése és ideiglenes korlátozások
   - Ideiglenesen korlátozza vagy szüntesse meg a partnercég hozzáférését a saját hálózatához és rendszereihez, amíg a biztonsági kockázatokat fel nem mérjük és kezeljük.
   - Ellenőrizze és szigorítsa a hozzáférés-vezérlési szabályokat, beleértve a tűzfalakat, a VPN-eket és más határvédelmi eszközöket.
4. Biztonsági felülvizsgálat és sebezhetőségi ellenőrzés
   - Végezzen átfogó biztonsági felülvizsgálatot és sebezhetőségi szkennelést a saját rendszereken, hogy azonosítsa és orvosolja az esetleges gyengeségeket.
   - Győződjön meg arról, hogy a rendszerek naprakészek, és hogy az összes releváns biztonsági javítást alkalmazták.
5. Incidensreagálási terv aktiválása

- Aktiválja a saját incidensreagálási tervét, amely magában foglalja a lépéseket a potenciális fertőzések azonosítására, izolálására és megszüntetésére.
- Készítsen részletes naplózást és dokumentációt az eseményekről és a hozott intézkedésekről a későbbi vizsgálat és felülvizsgálat érdekében.

6. Biztonsági oktatás és tudatosság
- Informálja a dolgozókat a partnercég kibertámadásáról és annak potenciális hatásairól a saját szervezetre.
- Hangsúlyozza a biztonsági legjobb gyakorlatokat és az óvatosságot, különösen a gyanús e-mailekkel és kommunikációkkal kapcsolatban.

7. Jogi és szabályozási követelmények
- Konzultáljon jogi és szabályozási szakértőkkel a támadás jelentésével és a szükséges intézkedésekkel kapcsolatban.
- Ellenőrizze, hogy vannak-e kötelezettségek az adatvédelmi törvények és szabályozások alapján.

Összegzés, következtetések

A légi forgalmi infrastruktúrát célzó kibertámadások, köztük az olyan incidensek, mint a Boeing Jeppesen leányvállalata elleni támadás, aláhúzzák a légi közlekedési rendszerek kritikus sebezhetőségét a rosszindulatú szereplőkkel szemben. Az ilyen támadások jelentős kockázatot jelentenek a repülésbiztonságra, az üzemeltetés integritására és az utasok bizalmára. A Jeppesenhez hasonló, a légi navigációs szolgáltatásokat érintő támadások aggályokat vetnek fel a repüléstervezés, a navigációs térképek és a kritikus üzemeltetési adatok biztonságával kapcsolatban. Továbbá a repülési társaságokat célzó támadások megzavarhatják a működést, járatkésésekhez vagy járattörlésekhez vezethetnek, és gazdasági hatást gyakorolhatnak az egész légi közlekedési ökoszisztémára.

Mivel a légi közlekedési ágazat egyre inkább az EFB-megoldásokra támaszkodik, a kiberbiztonság fontosságát nem lehet túlbecsülni ezen a területen. A légi közlekedés és a Boeing mint ilyen tevékenységű vállalat sajátos kiberbiztonsági kihívásokkal néz szembe, amelyeket hatékonyan kell kezelni a repülések sikere, a műveleti biztonság és az érzékeny információk védelme érdekében. Hatékony biztonsági intézkedések bevezetésével, az együttműködés elősegítésével és a feltörekvő technológiák által nyújtott lehetőségek kihasználásával a légi közlekedési ipar hatékonyan mérsékelheti a kiberbiztonsági fenyegetéseket, és erősítheti az IT-s EFB-megoldások rugalmasságát.

A ransomware támadások hatásának minimalizálása érdekében a szervezeteknek javasolt rendszeresen biztonsági másolatot készíteni adataikról, és a biztonságos másolatokat offline állapotban tartani. Továbbá rendkívül fontos a rendszerek frissítésekkel és vírusirtó szoftverekkel való ellátása, azok frissítése. Ezeket a frissítéseket javasolt a szervezeten belül egy erre dedikált folyamatba ágyazni, vagy magát a folyamatot létrehozni és rendszeresen ellenőrizni azok végrehajtását, kontroll alatt tartását.[31]

[31] Tóth 2022: 192.

Ahogy a kiberfenyegetések folyamatosan fejlődnek,[32] az EFB kiberbiztonságának folyamatos fejlesztésére és javítására van szükség. A jövőbeni fejlesztések egyik területe a mesterséges intelligencia és a gépi tanulási algoritmusok integrációja a kiberfenyegetések észlelésének és a reagálásnak a javítása érdekében. Mindkettő segíthet javítani a légi közlekedési szervezetek azon képességét, hogy valós időben észleljék a kiberfenyegetéseket, és gyorsan reagáljanak rájuk. Például a hálózati forgalmi adatok elemzésével ezek az algoritmusok szokatlan tevékenységi mintákat észlelhetnek, amelyek egy folyamatban lévő kibertámadásra utalhatnak.

Ezenkívül a biztonságos kommunikációs protokollok és a fejlett hitelesítési mechanizmusok fejlesztése az EFB-k biztonságát is növelheti. Ezek a mechanizmusok segíthetnek megakadályozni az EFB-khez való jogosulatlan hozzáférést, és biztosítják, hogy csak az arra feljogosított személyzet férhessen hozzá az érzékeny adatokhoz.

Ahogy a légi közlekedési ipar folyamatosan fejlődik és felkarolja a digitális technológiát, az EFB kiberbiztonsági jelentősége csak nőni fog. A kiberbiztonságba való befektetéssel és a felmerülő fenyegetésekkel való szembenézéssel a légi közlekedési ágazat továbbra is biztonságos repülést biztosíthat az utasok számára szerte a világon.

Felhasznált irodalom

A repülésben használt NOTAM-ok különböző típusai [é. n.]. Online: https://hu.motonoticias.com/different-types-notams-used-aviation-82278

Ateş, Savaş Selahattin (2017): Electronic Flight Bag in the Operation of Airline Companies: Application in Turkey. *Computer Science and Information Technology,* 5(4), 128–134. Online: https://doi.org/10.13189/csit.2017.050402

Babb, Tyler A. (2017a): Professional Pilot Commercial Off-the-Shelf (COTS) EFB Usage, Policies and Reliability. *International Journal of Aviation, Aeronautics, and Aerospace,* 4(1), 1–29. Online: https://doi.org/10.15394/ijaaa.2017.1159

Babb, Tyler A. (2017b): Electronic Flight Bag Policies at Collegiate Aviation Programs. *International Journal of Aviation, Aeronautics, and Aerospace,* 4(4), 1–22. Online: https://doi.org/10.58940/2374-6793.1190

Boeing Subsidiary Jeppesen Suffers Cyberattack (2023). *Binary Defense,* 2023. április 18. Online: www.binarydefense.com/threat_watch/boeing-subsidiary-jeppesen-suffers-cyberattack/

Britton, Niki (2022): 'Cyber Incident' Affected Flight Planning. Boeing Subsidiary Jeppesen Apparently Targeted. *AOPA,* 2022. november 9. Online: www.aopa.org/news-and-media/all-news/2022/november/09/cyber-incident-affected-flight-planning

Cyber Attacks on the Aviation Industry in 2022. Statistics: Ransomware, Data Breaches, DDoS Attacks (2023). *KonBriefing,* 2023. február 28. Online: https://konbriefing.com/en-topics/cyber-attacks-2022-ind-aviation.html

Florent, R. (2020): Aerospace Cybersecurity: Building Resilience in the Hailstorm. *CyberInflight,* 2020. május 10. Online: www.cyberinflight.com/?p=1081

[32] Kovács 2023.

Gates, Dominic (2018): Boeing Hit by WannaCry Virus, But Says Sttack Caused Little Damage. *The Seattle Times,* 2018. március 28. Online: www.seattletimes.com/business/boeing-aerospace/boeing-hit-by-wannacry-virus-fears-it-could-cripple-some-jet-production/

Gatlan, Sergiu (2023): Boeing Confirms Cyberattack Amid LockBit Ransomware Claims. *Bleeping Computer,* 2023. november 2. Online: www.bleepingcomputer.com/news/security/boeing-confirms-cyberattack-amid-lockbit-ransomware-claims/

Gonda Zsuzsanna (2005): *Repülési informatika.* Bicske: SZAK. Online: https://real.mtak.hu/170257/1/Gonda-Zsuzsanna-Repulesi-Informatika-konyv-SZAK-Kiado-2005-NJSZT-publikacio.pdf

Horváth József (2020): A repülés elleni kibertámadás. *Hadmérnök,* 15(3), 179–196. Online: https://doi.org/10.32567/hm.2020.3.10

Ilascu, Ionut (2023): LockBit Ransomware Leaks Gigabytes of Boeing Data. *Bleeping Computer,* 2023. november 12. Online: www.bleepingcomputer.com/news/security/lockbit-ransomware-leaks-gigabytes-of-boeing-data/

Klint, Matthew (2022): Breaking: Boeing's Jeppesen Subsidiary Hit with Potential Ransomware Attack. *Live and Let's Fly,* 2022. november 3. Online: https://liveandletsfly.com/boeing-jeppesen-ransomware-attack/

Kovács László (2023): *Hadviselés a 21. században: kiberműveletek.* Budapest: Ludovika.

Ohme, Marty (2014): Use of Tablet Computer as Electronic Flight Bags in General Aviation. *Aviation / Aeronautics / Aerospace International Research Conference,* 37. Online: https://commons.erau.edu/aircon/2014_Challenges_Facing_our_Industry/january-17-2014/37

Özkan, N. Fırat – Aksoy, Emre – Şensoy, Gökberk (2021): Evaluation of Jeppesen and Garmin Electronic Flight Bags (EFBs) Applications in Terms of Cognitive Workload and Availability. *International Journal of Multidisciplinary Studies and Innovative Technologies,* 5(1), 36–45. Online: https://dergipark.org.tr/en/download/article-file/1787377

Peredy Zoltán – Venczel Márk (2020): Nemzetközi repülőterek kiberbiztonsági kihívásai. *Repüléstudományi Közlemények,* 32(2), 165–180. Online: https://doi.org/10.32560/rk.2020.2.12

Personal Wings [@PersonalWings] (2022): Aviation Cyber Security and Recent Boeing Jeppesen Ransomware Hack. *YouTube,* 2022. november 6. Online: www.youtube.com/watch?v=RhLeTHTKxoU

Pufahl, Alexander (2022): *Global NOTAM Campaign.* Online: www.icao.int/NACC/Documents/Meetings/2022/AIMTF5/AIMTF5-P04.pdf

Raj, Aaron (2023): Boeing Hack: Should the Airline Manufacturer Negotiate with Cybercriminals? *Tech Wire Asia,* 2023. november 6. https://techwireasia.com/2023/11/boeing-hack-should-the-airline-manufacturer-negotiate-with-cybercriminals/

Suppiah, Saravanan et al. (2020): Impact of Electronic Flight Bag (EFB) on Single Pilot Performance and Workload. *International Journal of Aviation, Aeronautics, and Aerospace,* 7(4), 1–14. Online: https://doi.org/10.15394/ijaaa.2020.1531

Szabó Sándor – Tóth Rudolf (2013): Repülőterek kialakítása, létesítményeinek kritikus elemei, védelmük lehetséges műszaki megoldásai. *Repüléstudományi Közlemények,*

25(2), 89–113. Online: www.repulestudomany.hu/kulonszamok/2013_cikkek/2013-2-07-Szabo_Sandor-Toth_Rudolf.pdf

THURBER, Matt (2022): Jeppesen Planning, Chart Products Suffer 'Technical Issues'. *AIN Online,* 2022. november 4. Online: www.ainonline.com/aviation-news/business-aviation/2022-11-04/jeppesen-planning-chart-products-suffer-technical-issues

TÓTH András (2022): *A digitális állam információbiztonsági kihívásai.* Budapest: Ludovika.

U.S. Department of Transportation (2015): *Federal Aviation Administration: Advisory Circular, 90-100A*. Online: www.faa.gov/documentLibrary/media/Advisory_Circular/AC_90-100A_CHG_2.pdf

ZEE, Mark (2022): Jetplanner, FD Pro, Charts – Down. *OPS Group,* 2022. november 3. Online: https://ops.group/blog/jetplanner-fd-pro-charts-down/

HADMÉRNÖK
VÉDELEMINFORMATIKA
19. évfolyam (2024) 1. szám 121–141.
DOI: 10.32567/hm.2024.1.7

Károly Kassai[1]

Emerging Challenges and New Responses, Building Capabilities to Counter Threats in Cyberspace

Questions and Answers on How to Improve Cybersecurity

Abstract

Cyberspace phenomena are changing rapidly at international and national levels. Growing threats, new vulnerabilities and protection against them require continuous action at the level of the EU, NATO and national competent authorities and organisations. Adequate protection of critical infrastructure and cyberspace is a vital strategic, operational and technical challenge for the EU, NATO and therefore nations. Cross-border impacts, threat actors and malicious actions require coordination of international and national procedures, mechanisms and cooperation. This article presents the most important phenomena and trends experienced today, as well as EU and NATO initiatives and requirements at the strategic level, illustrating what changes can be expected in cybersecurity.

Keywords: cybersecurity, critical infrastructure protection, cyber threat, vulnerability, security requirement

Introduction

The events, experiences, threats and new security requirements (and initiatives, regulations, recommendations) related to cyberspace constitute a constantly changing environment for states, governmental organisations, social and economic actors and citizens with varying impacts.

[1] E-mail: karoly.kassai@yahoo.com

Responsible organisations and actors are under pressure to continuously monitor threats and vulnerabilities in cyberspace, to identify impacts and malicious actors and to comply with international and national requirements.

Following international frameworks, trends and typical processes will support the development of national and military capabilities and the foundation of concepts and initiatives for more robust national cybersecurity and effective cyber operations.

The NATO and the EU has similar requirements and several common actions in the field of cybersecurity, as Kovács concludes,[2] and in line with this observation, it would be useful to examine the horizontally enhanced regulations and initiatives at a strategic level.

This study[3] aims to identify recent strategic changes in the international environment in the field of cybersecurity that may have implications on the national regulations to support the needed developments by competent authorities and organisations.

The study was carried out by analysing "first line requirements", initiatives, and related opinions as well as a high-level comparison of EU and NATO declarations and international/national-level opinions on cybersecurity.

Threats and responses at the strategic level

The NATO Strategic Concept (Concept) (2022) is a long-term strategic document for the Alliance, setting out its core missions and main lines of ambition in response to the current security environment and emerging threats. The main objective is the collective defence of the Allies "based on a 360-degree approach". NATO's core tasks are *deterrence and defence,*[4] *crisis prevention and management,* and *collective security*.

According to Szenes,[5] the change in core tasks from "defence and deterrence" to "deterrence and defence" is a clear response to the new security challenges.

The deterrence and defence functions are based on coordinated nuclear, conventional and missile defence capabilities, "complemented by space and cyber capabilities". The use of correct terminology should be a priority for the better understanding of the subject. It is not enough to categorise a force and identify it as a deterrent component. This answers the question of whether cyber operational capability alone is a deterrent or should be classified as a supporting force – today!

The Concept states that the security environment is becoming increasingly complex and unpredictable, which is clearly justifiable in cyberspace. One of the main challenges is the increasing frequency and sophistication of cyberattacks, which can have a significant impact on national security – and on other aspects as well (e.g. alliance, regional, international). The secure use of and free access to space

[2] Kovács 2018: 23.

[3] This article is an edited, extended version of a conference presentation held on 15 November 2023 (Budapest, Infocommunication 2023 Conference, "Strategic level changes in the cyberspace framework, major impacts/A kibertér keretrendszerének stratégiai szintű változásai, fontosabb hatások").

[4] This is an important change in focus because in the previous Concept, the formulation of tasks was "defence and deterrence".

[5] Szenes 2022: 7.

and cyberspace is a key factor in deterrence and defence. The Alliance will develop capabilities *using all possible tools to operate effectively in space and cyberspace*, addressing the full spectrum of threats.[6]

The EU Cybersecurity Strategy (2020) – as a strategic baseline – outlines a comprehensive approach to cybersecurity for the long term (ten years) to counter cyber threats. The strategy sets out three main pillars to strengthen cybersecurity across the EU:

- *Enhancing resilience.* Critical areas for development are resilient infrastructure and critical services, European Cyber Shield, secure communication infrastructure (e.g. satellite, quantum communication infrastructure), next generation networks, secure IoT,[7] supply chain security.[8]
- *Strengthening cyber operational capabilities for prevention, deterrence and response.* Key capability areas are the EU Joint Cyber Unit initiative, coordinated response to large-scale cybersecurity incidents and crises ('Blueprint'), cyber diplomacy toolbox, development of cyber defence capabilities (modernisation of the Cyber Defence Policy Framework, Military Vision and Strategy on Cyberspace as a Domain of Operations, Military CERT[9] Network and various EDA[10] cyber-related projects).[11]
- *Promoting a global and open cyberspace.* Key activities are international standardisation processes, efforts towards "responsible state behaviour in cyberspace", international cooperation (e.g. EU Cyber Diplomacy Network, EU–NATO cooperation), strengthening of the Budapest Convention on Cybercrime.[12]

Bihaly notes[13] that the key areas of the strategy are at different stages of development. The actors of the various processes (nations, EU institutions, organisations and agencies) still have a lot of work ahead to achieve coherence between organisations.

The next EU regulations and initiatives, which will be presented later, will demonstrate the different steps alongside the direction of the Cybersecurity Strategy.

The EU Strategic Compass for Security and Defence (Compass) (2022) document provides guidance and aims to strengthen security and defence policy in the EU with four pillars: *act, invest, partner* and *secure* by 2030.

The Compass highlights *strategic competition* and *complex security threats* in the security landscape. The frequency and impact of hybrid threats are increasing, and interdependencies (e.g. digitalisation) may cause more problems than before. Global commons (e. g. seas, space and cyberspace) are contested domains. The EU has an interest in *exploiting all operational domains* (land, sea, air, cyber and space). The EU will strengthen the elements of Cyber Defence Policy, improve cyber

6 NATO 2022b: 6, 7.
7 IoT: Internet of Things.
8 European Commission 2020: 5–12.
9 CERT: Computer Emergency Response Team.
10 EDA: European Defence Agency.
11 European Commission 2020: 13–18.
12 European Commission 2020: 19–22.
13 Bihaly 2021: 54.

intelligence capabilities for effective cyber resilience,[14] and enhance interoperability and information sharing capabilities among cyber organisations for more effective cooperation (e.g. cyber exercises).

The Compass notes that the new EU Space Strategy for Security and Defence will play an important role[15] in better understanding space-related risks and threats.

The Compass identified the need to strengthen command and control structures (e.g. military planning and conduct capability, strategic communication tools) to support EU-led missions and operations.[16]

Regarding conflicts and crises, Novák-Varró underlines[17] the spread of the concept of "integrated approach" in the EU's strategic thinking. Another important element is that the content of the former "national defence-oriented" resilience has changed and now includes the complex aspects of human security.

In line with the findings of the Compass, Kersánszky confirms[18] that cyberspace has become an area of geopolitical competition, requiring decisive and rapid responses to malicious cyber activities. The EU must place great emphasis on prevention, protection, early detection and countermeasures at military, civilian and political levels.

At the 2021 NATO Summit, the Alliance adopted the *Comprehensive Cyber Defence Policy,*[19] which *reinforces NATO's defence mandate* and commitment to actively deter, defend and counter cyber threats in support of NATO's three core tasks and its overall deterrence and defence posture.

Responses will be collective, using *political, diplomatic* and *military* tools. Significant malicious cyber activity may be considered an armed attack. NATO's comprehensive approach to cyberspace focuses on unity of effort at the political, military and technical levels.

The Alliance remains committed to compliance with international law, promoting a free, open and secure cyberspace, and supporting responsible state behaviour in cyberspace.[20]

The Hungarian approach is similar to the NATO and EU documents, mentioned in the Hungarian National Security Strategy (2020) (e.g. comprehensive approach to security, hybrid threat orientation, intelligence-led decisions). Szenes confirms[21] that the strategy addresses the hybrid threat with a two-level solution (national and alliance) supported by whole-of-government resources.

According to Kovács's interpretation,[22] the importance of information and communication systems, which ensure the functioning of society, has increased in

[14] The networks, digital services (including military, critical infrastructure and governmental services) will be more robust and secure by the requirements of the new Cyber Resilience Act (2022).
[15] Accessibility and operational capabilities of space objects have critical importance in the field of digital infrastructure and communications.
[16] European Union External Action 2022: 2, 3, 5, 14, 23.
[17] Novák-Varró 2021: 36–37.
[18] Kersánszky 2022: 74.
[19] This Policy is the NATO's highest-level strategic document on cyber defence in the support of NATO's Strategic Concept (similar in function to the EU's Cyber Security Strategy). The content is based on NATO's public extract.
[20] NATO 2021a.
[21] Szenes 2021: 45.
[22] Kovács 2020: 17.

the strategy. The protection of these systems is a national security interest (and a strategic object).

Bányász et al. conclude[23] that according to the strategy, national cyber defence cannot function without international cooperation. This cooperation is primarily within the Alliance system, which is based on trust to act quickly and effectively.

The new risks and threats in the security environment will have an impact on the Strategy, so its next revision *should consider the effects of the latest factors, threats and new technologies.* After main changes, the lower-level strategies and regulations should be updated (e.g. National Cyber Security, National Military Strategy and their supporting documents).

High-level risk identification

The EU Economic Security Strategy (2023) identifies the key considerations for the main risk types as follows:

- resilience of supply chains, including energy security
- physical and cybersecurity of critical infrastructure
- technology security and technology leakage and
- weaponisation of economic dependencies or economic coercion[24]

Based on strategic level considerations, the *EU Commission Recommendation on critical technology areas has prioritised and identified the highest level risks* (2023), which are *advanced semiconductor technologies, artificial intelligence technologies, quantum-* and *biotechnologies,* and they require urgent risk mitigation actions.[25]

The EU Space Strategy[26] (2023) underlines the *importance of the space segment,*[27] including *space objects, communication tools* and the fundamental importance of *open access* for the EU. The strategy states that critical infrastructure and communication requirements must apply to both space objects and ground facilities to ensure a safe and secure space. Member States should take *measures to regulate space activities, including security aspects.*[28]

The EU Council Conclusion on the Space Strategy (2023) emphasises the importance of timely action by Member States, considering hostile space behaviour (such as jamming, manipulation, destruction of space infrastructures and systems).[29]

The ENISA Threat Landscape 2023 identifies ransomware and denial of service threats as the highest threat level, after social engineering, data-related threats, information manipulation, supply chain attacks and malware. The most targeted

[23] Bányász et al. 2022: 9.
[24] European Commission 2023c: 4, 5.
[25] European Commission 2023a: 3
[26] European Union Space Strategy for Security and Defence.
[27] The later interpreted CER Directive and the NIS2 Directive identify the space sector as a critical domain (both as critical infrastructure and essential communication services).
[28] European Commission 2023b: 3.
[29] Council of the European Union 2023e: 6, 7.

sector in 2023 is the public sector (~19%). There is a significant increase in social engineering attacks supported by artificial intelligence in 2023.[30]

The ENISA's *Foresight 2030 Threats* (2023) has a more extended analysis horizon. The report ranks the supply chain attacks (software dependency compromise), disinformation campaigns and digital surveillance authoritarianism[31] in the top three.[32]

The report also identifies other threats that could be considered attractive, such as targeted attacks (e.g. ransomware) against smart devices; attacks on the vulnerability of space-based infrastructure (due to lack of understanding, analysis and control); threats to cross-border ICT providers (single point of failure effects in the case of critical infrastructure, e.g. transport, power grids and industry); and the abuse of artificial intelligence (manipulation of AI algorithms and training data).[33]

The EU Statement on Existing and Potential Threats in the UN Open-Ended Working Group on ICT of 19 December 2023 summarises the most critical cyber threats as:[34]

- attacks on software supply chains (the number of attacks on software supply chains tripled in 2022)
- ransomware attacks (the scale and severity of this attack are increasing, and the risk to essential services and critical national infrastructure may rise to the level of national and international security)
- malicious cyber activity driven by AI-powered software in the long term[35]

The strategy papers presented above demonstrate the need to analyse threats and their effects, and to provide the basis for the necessary response. At the national level, the Hungarian strategies (e.g. National Security Strategy, National Cybersecurity Strategy) – like the EU documents – contain threat statements and risk forecasts and, based on these, high-level security requirements and related tasks. However, due to the strategies' different life cycles and functions, the statements and requirements are not always consistent with each other and the security environment.

The space segment is critical not only for nations involved in spaceflight, therefore, Hungary must also consider the threat of loss of communication channels, communication or navigation equipment in space, which can cause severe disruptions in critical infrastructure or information environments with poor coverage (e.g. military missions and operations).

The new Hungarian approach is straightforward about the threats and risks at the national level. The Act XCIII of 2021 on the coordination of security and defence activities requires a specific risk summary as a decision of the Parliament ["the Principles of Security and Defence Policy" – §22 (1) a)] to create a common base for all strategic level documents.[36]

[30] ENISA 2023c: 4.
[31] The last two threats cannot be considered as pure cyber threats, but rather as complex threats with cyberspace elements.
[32] ENISA 2023b: 2–4.
[33] ENISA 2023b: 6, 7, 10–11.
[34] European External Action Service 2023f.
[35] Otherwise, the AI-powered cyber defences can detect and respond to cyber threats and bolstering security of military networks.
[36] Act XCIII of 2021.

Developments, new solutions to strengthen cybersecurity

The Network and Information Security Directive (NIS 2 Directive) (2022) aims to significantly enhance cybersecurity and establish a standard level of security measures[37] across the EU.

Expands the range of covered entities, creates categories of 'essential' and 'important' for entities in critical sectors, and includes – for the first time – medium-sized service providers.[38]

The Directive requires organisations to carry out regular risk assessments and to take the necessary security measures in line with EU CER[39] Directive and EU DORA[40] (specification for the secure financial sector).[41] Essential or important entities *must submit an incident notification in case of significant incidents within 72 hours,* applying a multi-stage approach.[42]

It requires Member States to establish national Computer Security Incident Response Team(s) (CSIRTs) for incident handling and information sharing, strengthens national competent authorities with additional powers and designates a single point of contact for communication and cooperation at the EU level.

The EU has established a cooperation network (CSIRTs Network), the European Cyber Crisis Liaison Organisation Network (EU-CyCLONe) and the EU NIS 2 Cooperation Group supported by national representatives to ensure effective cooperation. The EU-CyCLONe and the CSIRTs network should have procedural arrangements[43] to avoid overlap and duplication.[44]

Member States *should encourage the development of artificial intelligence and the use of open-source tools,* establish procedures to deal with ransomware and promote the use of encryption techniques.[45]

In parallel with the cybersecurity measures and procedures, Member States shall establish their national cybersecurity strategy within the general criteria of the framework provided by the Directive, including the adoption of policies to promote active cyber protection methods.[46]

The National Cybersecurity Strategies (NCSS) framework developed by ENISA (2020) helps Member States understand their maturity level and assist them in developing their cybersecurity capabilities. The framework has four focus areas: *cybersecurity governance and standards, capacity building and awareness, legislation and regulation* and *cooperation.*[47]

[37] Member States are obliged to implement the requirements into their national legal frameworks by 18 October 2024.
[38] Directive (EU) 2022/2555: 2–3.
[39] CER: Critical Entities Resilience.
[40] DORA: Digital Operational Resilience Act.
[41] Regulation (EU) 2022/2554.
[42] Directive (EU) 2022/2555: 16, 20.
[43] In principle, the EU CyCLON has a crisis management function, while the CSIRTs Network's main task is to support incident response at technical level.
[44] Directive (EU) 2022/2555: 14.
[45] Directive (EU) 2022/2555: 11.
[46] Directive (EU) 2022/2555: 7, 12.
[47] See: www.enisa.europa.eu/topics/national-cyber-security-strategies

The EU Directive on the resilience of critical entities (Critical Entities Resilience Directive – CER) focuses on improving the resilience of critical entities (organisations) as providers of essential services within the EU.[48]

To ensure a comprehensive approach, the Directive requires Member States to develop strategies[49] to support critical entities, integrating existing policies and regulations, considering hybrid threats.[50]

The Directive establishes standard rules for identifying critical entities in essential sectors.[51]

Member States should define significant disruptive impacts and their levels (taking into account negative consequences), designate a *competent authority* to supervise entities and procedures and identify a single point of contact for cross-border cooperation.[52]

Critical entities shall carry out risk analysis[53] concerning the provision of essential services and take *technical, security* and *organisational* measures proportionate to the risks. Critical entities should describe their measures in the *Resilience Plan* (or equivalent document). Each critical entity shall designate a *liaison officer* to the competent authority. Critical entities shall report significantly disruptive incidents to the competent authority within 24 hours. The initial notification shall provide only the strictly necessary information and the presumed reasons.

A Critical Entities Resilience Group composed of representatives of the Member States' competent authorities and of the Commission should be established, which should cooperate with the EU NIS 2 Cooperation Group.[54]

Roepke and Thankey explain[55] that more resilient countries have fewer vulnerabilities as a result of a whole-of-government approach and joint preparation by the public and private sectors. In addition, resilience is an important aspect of deterrence by denial: an attack will not achieve its intended objectives. Mógor and Angyal believe[56] it is important that, during complex exercises conducted in accordance with the requirements of Hungarian legislation, the operating organisations and the competent authorities jointly review the procedures set out in the security plan and the responses to threats.

The proposal for an EU Cyber Solidarity Act (2023) aims to strengthen the EU's cybersecurity capabilities *in the event of significant and large-scale cybersecurity threats and attacks.* The Act describes the detection, preparedness and response functions[57] and consists of three main pillars:

[48] The EU CER Directive has similar logic to the EU NIS 2 Directive.
[49] The Directive does not specify a name for the Strategy ("a strategy for enhancing the resilience of critical entities"), but defines its main aspects. (The Strategy may be a classified document, if necessary.)
[50] Directive (EU) 2022/2557: 2, 14–15.
[51] Energy, transport, banking, financial market infrastructures, health, drinking water, waste water, digital infrastructure, ICT service management (business-to-business), public administration and space.
[52] Directive (EU) 2022/2557: 5–7, 17–18.
[53] The risk assessment shall be reviewed every four years or in case of significant changes (risks, circumstances).
[54] Directive (EU) 2022/2557: 25–26.
[55] Roepke–Thankey 2019: 1.
[56] Mógor–Angyal 2022: 122.
[57] At this stage, these names and titles have only a 'working function' – given that the EU Act is still being developed at the time of writing.

- *European Cybersecurity Shield.* The Shield is not military equipment or a specific hardware-software platform, but a cooperative capability of national competent organisations participating in the EU-level capability voluntarily. The widely interconnected EU entities support the detection of incidents and threats, focus on crisis management and facilitate responses. The planned capability should not overlap with the EU CSIRT Network, the EU CyCLONe,[58] the EU NIS Cooperation Group or other competent national bodies as defined in the EU NIS 2 Directive.[59]
- *Cybersecurity Emergency Mechanism.* The proposal includes a comprehensive emergency mechanism to support critical entities and essential services in high critical sectors. The Mechanism consists of *preparation* (e.g. test of critical important entities in critical infrastructure sectors), reactions and restoration capabilities in case of severe cyberattacks, supported by trusted companies in the framework of Cybersecurity Reserve (e.g. trusted dedicated companies) and common solidarity support provided by national authorities and entities.[60]
- *Cybersecurity Incident Review Mechanism.* This mechanism provides support from ENISA in the event of significant and large-scale cyber-attacks, with *technical review* and *assessment* of incidents at the request of EU bodies or national competent authorities.[61]

The Cybersecurity Support Action (2023) provided by ENISA is a comprehensive set of services to Member States for prevention ('ex-ante') as incident management, response and coordination, and response ('ex-post') as cybersecurity exercises, training and capability assessments.[62]

The NATO Resilience Commitment has a similar methodology for the resilience capabilities of critical infrastructure and services important to NATO operations (including national supporting elements in NATO deployments).[63] In terms of resilience, Jacuch believes[64] that it is important that the baseline requirements are applied to the entire spectrum of crises.

The Alliance identified *Baseline Requirements for National Resilience* in 2016. The seven areas are where specific intent is needed: continuity of government, energy supply, uncontrolled movement of people, food and water resources, mass casualty and disruptive health crises, civil communications systems and transportation systems.[65] NATO created a framework for cooperation to support Allies' national resilience activities, including an annual updating process, consultations, courses and development of assessment criteria and methodologies.

[58] EU Cyber Crisis Liaison Organisation Network.
[59] European Commission 2023f: 23.
[60] European Commission 2023f: 26.
[61] European Commission 2023f: 32.
[62] ENISA 2023a.
[63] NATO 2016a.
[64] Jacuch 2020: 17.
[65] NATO 2016c.

Kádár confirms[66] that the national regulations reflect the basic requirements for NATO resilience, complemented by aspects of preparedness and commitment.[67]

The EU proposal for a Regulation on Cybersecurity Requirements (the Cyber Resilience Act – CRA) aims to establish horizontal cybersecurity requirements for products with digital elements, including connected devices, software and cloud services.

The proposal defines products in the "critical product" category that contain digital elements according to their cybersecurity risk.[68]

Producers must establish *risk management processes* (risk identification and mitigation of cybersecurity risks throughout the product life cycle). Information on exploitable vulnerabilities *must be reported by manufacturers* to the notified authority (organisation) within 24 hours at the latest.[69]

Producers shall develop and maintain *accurate documentation of products* with digital elements to ensure compliance with the requirements for essential products.[70]

Member States must designate a notifying authority to certify quality assurance bodies to the EU and Member States and to *monitor* and *supervise* their activities following EU requirements.[71]

Similarly to EU certification efforts, the *NATO Information Assurance Product Catalogue* (NIAPC) provides up-to-date information on products (hardware, software) to meet NATO operational requirements following NATO strategic requirements for the protection of classified and unclassified information.[72]

The NATO Strengthened Resilience Commitment (2021) confirmed the need to strengthen the resilience of critical infrastructures (land, sea, space and cyberspace) and industry further. *The impact of emerging technologies must be addressed,* and next-generation communication systems must be secured. Investment is needed in robust, flexible and interoperable military capabilities, and supply chains must be secured and diversified. A *whole-of-government approach* is required in order to strengthen resilience capabilities.[73] In connection with cybersecurity, Stoltenberg clearly stated[74] that nations' security is impossible without the private sector, so it is needed "to talk, plan and exercise more together".

The EU Council Recommendation on Critical Infrastructure Resilience was adopted on December 2022. The aim of the Recommendation is to ensure an appropriate, high-level, coordinated and effective EU-wide response to current and future risks to essential services.[75] The Council invited the European Commission to develop

[66] Kádár 2022: 13.
[67] E.g. Act XCIII of 2021 on the coordination of security and defence activities.
[68] European Commission 2022: 36.
[69] European Commission 2022: 38, 40.
[70] European Commission 2022: 47.
[71] European Commission 2022: 49.
[72] See: www.ia.nato.int/NIAPC
[73] NATO 2021b.
[74] Stoltenberg 2023.
[75] The Council of the European Union 2022: 3.

a blueprint[76] to set out the principles for appropriate response to disruptions of critical infrastructure with a significant cross-border impact, in line with other legislation.[77]

The proposed EU Council Recommendation on a Blueprint to coordinate a Union-level response (2023) regulates the exchange of information between EU organisations (institutions, bodies, offices and agencies) and national competent organisations and authorities in case of significant cross-border threats. Nations and EU organisations must activate the appropriate tools if there is a significant disruption of services in six Member States, or a significant disruption of services to six countries, or there is a significant impact on two or more countries and the affected actors agree on the need for coordination at EU level.[78]

The planned Recommendation will regulate *operational, strategic and political cooperation.* States will have to designate a relevant national actor as the point of contact for the use of the Critical Infrastructure Blueprint.[79] The responsible actors recommended *testing the processes of the Critical Infrastructure Blueprint, including exercises at the* EU level with physical and cyber aspects. The results of the tests and the experience of the incidents should be evaluated by the Critical Entities Resilience Group, and nations must prepare a report with the lessons learned to the EU.[80]

In addition to technical responses to complex cyber threats, *the EU Cyber Diplomacy Toolbox* is a solution that enables complex economic and diplomatic responses.

Similarly, *the NATO North Atlantic Council consultation mechanism* can decide on Alliance-level actions and operations, including complex responses to cyber incidents, on *case-by-case basis.*

The proposal for a regulation amending the Cyber Security Act as regards managed security services (2023) creates new requirements in the field of cyber certification of ICT[81] products and services. The EU NIS 2 Directive introduced "managed security services" within the scope of ICT services. Managed security services are also important because service providers can provide (and receive) guarantees on the reliability of a cyber product and services within the framework of the Cybersecurity Emergency Mechanism (including Cybersecurity Reserve), as previously mentioned. Member States should address this regulatory change consistently and include this product in the scope of cyber product certification to avoid fragmentation inside the EU. Following the legislative change, Member States have to implement the change in their cyber product and service certification schemes and processes.[82]

The NATO Cyber Pledge (2016) is another tool to support the national cyber capability development in critical areas. The Pledge is a practical, strategic level

[76] The Council of the European Union 2022: 10.
[77] E.g. counter hybrid threats regulations, CER Directive, NIS2 Directive, 'Cyber Blueprint' (Commission Recommendation 2017/1584 on coordinated response to large scale cybersecurity incidents and crises).
[78] European Commission 2023d: 6, 11.
[79] The contact point should be same as the single point of contact (SPOC) in the CER Directive.
[80] European Commission 2023d: 14.
[81] ICT: Information and Communication Technology.
[82] European Commission 2023e: 5–6.

identification of the main capability development areas[83] for nations with annual self-assessment, national–NATO consultation and alliance-wide common evaluation.[84] Stoltenberg underlined that the Allies have increased their investments in cyber, and enhanced skills and capabilities to implement the national strategies in the NATO Cyber Pledge framework.

The NATO Vilnius Summit Communiqué (2023) states that the Allies restated the enhanced Cyber Defence Pledge with critical infrastructures.[85]

The NATO Madrid Summit Declaration (2022) announced that the Allies have decided to establish a virtual rapid response cyber capability, supported by nations on voluntary basis, to respond to significant malicious cyber activity.[86]

The Vilnius Summit Communiqué (2023) states that NATO has established the Virtual Cyber Incident Support Capability (VCISC) as a new solution to assist nations in responding to significant malicious cyber activity.[87]

Bányász et al. conclude[88] that the Allies are responsible for their cyber defences. The NATO provides a platform for consultation, exchange of information and best practice.

The International Counter Ransomware Initiative 2023 Joint Statement summarises the efforts of the international community in the last year:

- capability development (to disrupt attackers and the infrastructure used to carry out their attacks): mentoring and tactical training for new members; launching a project to use artificial intelligence in the fight against ransomware
- information sharing: developing a specific platform and CRI website to support member cooperation; encouraging reporting of ransomware incidents to relevant government authorities
- operations: drafting a policy statement that member governments will not pay ransoms; sharing data from illegal wallets; providing mutual assistance[89]

Members issued a joint statement against ransomware payments. Organisations controlled by member governments do not pay ransomware because payment:

- does not guarantee the end of the incident or the removal of malware from systems
- encourages criminals to continue and expand their activities
- provides funds for criminals to use for illegal activities
- does not guarantee the recovery of data[90]

[83] Capabilities to defend our national infrastructures and networks; adequate resources, interactions (cooperation, exchange of best practices); understanding of cyber threats (and information sharing), skills and awareness, cyber education, training and exercises and bolster security of national systems upon which NATO depends.
[84] NATO 2016b.
[85] NATO 2023.
[86] NATO 2022a.
[87] NATO 2023.
[88] Bányász et al. 2022: 18.
[89] ICRI 2023b.
[90] ICRI 2023a.

The EU proposal for a regulation on artificial intelligence (2021) addresses the risks associated with the use of this technology. The planned act identifies the prohibited AI practices[91] and establishes the classification rules of the high-risk AI systems,[92] as well as the requirement to establish and maintain a risk management system.[93] In addition, there are other requirements (e.g. data governance, documentation, event logs, cybersecurity) and obligations (e.g. providers, users, distributors).[94] Each Member State shall designate or establish a notifying authority to supervise and monitor conformity assessment bodies.[95]

The various aspects, functions and high-level risks of the use of artificial intelligence and finally, the possible, unpredictable effects, create a completely uncertain, foggy environment that slows down the pace of regulation. Recognising the difficulties, it is positive that – as a new step in regulation – the EU Parliament and the Council have reached a political consensus on the main issues of the proposal in late 2023, so that the planned Act can realistically be expected in 2024.[96]

The European Declaration on Quantum Technologies (Quantum Pact) (2023) recognises the strategic importance of quantum technologies based on the statements of the European Economic Security Strategy and the Commission Recommendation, as mentioned earlier in this paper. To protect the strategic assets, interests and security of the EU and to avoid strategic dependence on non-EU sources, it is necessary to build up its own research and development capabilities in the main areas of quantum technologies: *quantum computing and simulation, quantum communication, quantum sensing* and *metrology*.

Member States will coordinate their efforts in European national and regional research and development programmes and initiatives in quantum technologies. They will encourage companies to invest in quantum technologies to support the EU's economic security and technological autonomy.

Members will identify the necessary skills and training needs and undertake the activities required for a deeper understanding of the social and economic implications and challenges of quantum technologies.[97]

The European Cybersecurity Competence Centre has raised a specific quantum area in its Strategic Agenda (2023), the post-quantum cryptography. The EU still needs to *have a strategy-level document dedicated to these issues,* but the secure use of post-quantum cryptography requires close attention (e.g. development, implementation and assurance). The Agenda underlined the importance of risk analysis with prioritisation; on this basis, a strategy for using post-quantum cryptography should be developed.[98]

The Belgian Presidency has identified the main priorities in cybersecurity: "active cyber protection" (establish a common approach to prevent, detect, monitor and

[91] European Commission 2021: 43–45.
[92] European Commission 2021: 45–46.
[93] European Commission 2021: 46–48.
[94] European Commission 2021: 52–58.
[95] European Commission 2021: 58.
[96] European Parliament 2023b.
[97] European Union 2023c: 2–3.
[98] European Cybersecurity Competence Centre and Network 2023: 9, 10.

mitigate cyber incidents), trust in the digital domain and enhancing cyber resilience (including space infrastructure).

The Presidency plans to *finalise the Cyber Solidarity Act* and review *the EU's Cyber Defence Policy* and institutional landscape (gap identification).[99]

The report of the UN Open-ended Working Group on Security (2022) noted the importance of understanding national perspectives on the applicability of international law. States are invited on voluntary basis to share their national views and positions on international law in the use of ICTs.[100]

Generally, red lines are largely undefined and untested, and the threshold indicators – scale, effects, circumstances and motivations – are even more obscure in cyber domain as Pedersen states,[101] so publishing the national point of view is an effective tool for the next generation of international standards and norms.

According to Stoltenberg's speech,[102] the cyberspace should not be a "Wild West" free-for-all and "all Allies agree that fundamental rights and international law apply".

General considerations

Based on the observations of the study, it is possible to formulate general guidelines that can help to develop specific regulations at the national level. This is necessary because there is only one Hungarian cybersecurity framework (organisations, regulations, external interfaces, etc.), which must be capable of different (e.g. UN, EU, NATO) international cooperations.

Emerging threats. The increase in cyber threats (number, effectiveness and complexity), their focus on critical infrastructure and cyber infrastructure and the presence of hybrid operations are highlighted from both the EU and NATO perspectives.

Emerging and Disruptive Technologies (EDT). In addition to the increasing number of technical and regulatory question marks, the emergence of new threats and risks in the EDT and the expression of the need to address them is a growing international trend.

Complexity and interdependence. In support of the strategic objectives for the enhancement of the level of security in cyberspace, an increasing number of actions can be identified horizontally. Information systems, services and tools are an indispensable part of social and economic processes and critical infrastructures, so that their compromise can lead to further failures including cross-border impacts. Security issues must be enforced throughout the lifecycle of services and products (e.g. supply chain security, AI development and operation).

Risk based approach. The changing security environment requires ongoing risk-based, intelligence-driven security policies and governance.

Evolution and hierarchy. The sources presented justify the continuous evolution of cyber protection mechanisms and processes and the logic of sequential steps

[99] Centre for Cybersecurity Belgium 2023.
[100] United Nations 2022: 11.
[101] Pedersen 2023: 63.
[102] Stoltenberg 2022.

(including periodic review and reinforcement actions). The strategic, operational and technical structure is also clearly identifiable.[103] A multi-layered security structure and cooperation framework is necessary for the effective and fast international and national responses.

Solidarity and assistance. In addition to developing technical cyber protection mechanisms, various forms of solidarity and assistance (national, regional and EU-NATO) are strongly emerging. In addition to solidarity, operational and technical cooperation is needed to identify and respond effectively to cross-border impacts.

Sovereignty and self-defence. Effective resilience and self-defence – including countering the harmful effects of national and international dependencies – in the case of critical infrastructure protection and cybersecurity are essentially national responsibilities, complemented by EU and Alliance assistance.

International efforts. International cooperation frameworks (e.g. ransomware, artificial intelligence and quantum) are being developed to study important issues and find solutions (e.g. gap analysis, research, methods and procedures, education, information and best practices exchange, tests).

Taking into account the above guidelines, national frameworks and interfaces for participation in international and national processes should be continuously ensured.

National laws and regulations need to be managed in a complex manner along the above lines, as fragmentation of regulation can provide an unnecessary attack surface (lawfare effects) to achieve the objectives of the adversary.

National impacts

The EU NIS 2 and EU CER Directives directly impact Hungary. In the area of cybersecurity, the two existing Hungarian strategies[104] should be replaced by a modern national cybersecurity strategy. According to Bányász et al.,[105] the two cyberspace strategies are partly complementary and partly contradictory. In the area of critical infrastructure, a *national strategy should be adopted*, which has yet to be done in Hungary.

In both areas, laws and supporting directives need to be revised and updated to ensure EU compatibility. A recent example is the *revision of the national requirements for the security of electronic information systems*–with public consultation (security classification and security measures). [106]

The proposed Cyber Resilience Act will provide a broad EU basis for common risk-based requirements for cybersecurity certification of digital products (hardware, software) and support citizens' security awareness. The planned new EU requirement for mandatory certification of managed security services will *directly impact Hungarian*

[103] Ad-hoc decisions cannot establish and maintain strategic, stable states or processes even in cyberspace.
[104] 1139/2013 (III. 21.) Government Decision on Hungary National Cyber Security Strategy and 1838/2018 of 28 December 2018 Government Decision on Hungary Strategy for the Security of Network and Information Systems.
[105] Bányász et al. 2022: 4.
[106] Magyarország Kormánya 2023.

cyber product certification laws[107] and procedures in both commercial and military cases. *The NATO Resilience Commitment* and the *NATO Cyber Pledge* also aim to support the development of national capabilities analogous to the requirements of the EU. NATO and the EU share a common approach to critical infrastructure and cybersecurity, and there is close cooperation in a number of areas (exercises, joint working groups and forums, technical agreements).

The planned new EU Cyber Solidarity Capabilities will also provide technical support to Member States (e.g. incident management and recovery support, international cooperation) and provide an opportunity for industry to offer capabilities (e.g. Cyber Reserve System). The Hungarian Electronic Information Security Early Warning System complements the national incident management system by collecting one-way data flows from sensors of protected information systems, providing an enhanced protection solution.[108] *The planned EU Cyber Shield will offer possible cooperation,* depending on details in the future.

The upcoming EU Act on Artificial Intelligence (AI) will *directly apply in Hungary,* so preparing for its application and considering the potential threats is an urgent task.

The threat of ransomware has increased over the years. Following the international ICR initiative and studying the solutions provided by different entities and nations is useful. Of course, the best solution *would be for Hungary to join the initiative.*

The EU Quantum Pact is a cooperation for developing future capabilities of similar importance as artificial intelligence, of which Hungary is a member. This will provide access to joint research results and *the possibility of involving Hungarian companies and research institutions in projects.* The predictable new EU quantum requirements may lead to *direct changes in the existing Hungarian regulations* on the security of information systems.[109]

The recommendation of the UN Working Group on the applicability of international law in Cyberspace suggests that the expression of national positions is a useful process to support international cooperation. Hungary has yet to make such a declaration,[110] so it *would be useful to define the Hungarian position* within the framework of the new strategies (e.g. self-defence, the Hungarian concept of national sovereignty in cyberspace).

The promotion of the development of active cyber protection capabilities and the *revision of the EU's Cyber Defence Policy,* as indicated by the Belgian EU Presidency, also *represent new challenges for Hungary*.

Conclusion

Cybersecurity issues, once simplified to a primarily technical level, are now becoming more complex and sophisticated as the range of threats expands.

[107] Act XXIII of 2023.
[108] Government Decree 214/2020 (V. 18.).
[109] Act L of 2013, 22/F-H. §.
[110] There is no internationally agreed form of national positions, and the publication of the issues is usually straightforward (mainly in the form of a position paper).

The EU and NATO cybersecurity frameworks are constantly evolving, and processes and organisational relationships lead to increasingly complex defence mechanisms.

EU and NATO policies and programmes aim to support the development of national capabilities, improve coordination at the EU and NATO levels and stimulate cooperation and mutual support among nations.

The article describes several EU and NATO initiatives and requirements that will need developing or modifying national laws and procedures. These changes will impact Hungary's cybersecurity framework and capabilities and require revisions and national regulation updates.

The boundary between civil and military cyberspace (or physical and cyber dimensions) is sometimes foggy and mysterious. From another perspective, the military is part of national security, so the presented new requirements will affect military capabilities, cooperation and coordination issues at both national and international levels, but this may already be the subject of a future article.

Digitalisation is not a closed issue, so new needs and solutions will create new threats, needing new security requirements, processes and protection mechanisms to balance them. For this reason, the cybersecurity outlook and snapshot presented in this article will show significant differences and evolution in the coming years.

Finally, many thanks to friends and colleagues (both civilian and military) who contributed their opinions and suggestions to this article.

(The research for this publication was completed on 23 February 2024.)

References

BÁNYÁSZ, Péter – KRASZNAY, Csaba – TÓTH, András (2022): *A kibervédelem szakpolitikai szintjének helyzete és kihívásai Magyarországon, az EU-ban és a NATO-ban* [Situation and Challenges at the Policy Level of Cyber Defence in Hungary, the EU and NATO]. Military and Intelligence Cyber Security Research Paper 2022/8.

BIHALY, Barbara (2021): A kibervédelem szerepe az Európai Unió közös biztonsági és védelmi politikájában [The Role of Cyber Defence in the European Union's Common Security and Defence Policy]. *Hadtudományi Szemle,* 14(3), 45–55. Online: https://doi.org/10.32563/hsz.2021.3.4

Centre for Cybersecurity Belgium (2023): *Cybersecurity Priorities in the Upcoming Belgian Presidency Agenda.* Online: https://ccb.belgium.be/en/news/cybersecurity-priorities-upcoming-belgian-eu-presidency-agenda

The Council of the European Union (2022): *Council Recommendation of 8 December 2022 on a Union-wide coordinated approach to strengthen the resilience of critical infrastructure.* 2023/C 20/01. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023H0120(01)

The Council of the European Union (2023): Council Conclusions on the EU Space Strategy for Security and Defence. 14512/23. Online: https://data.consilium.europa.eu/doc/document/ST-14512-2023-INIT/en/pdf

ENISA (2023a): *Cybersecurity Support Action.* Online: www.enisa.europa.eu/publications/cybersecurity-support-action

ENISA (2023b): *Foresight 2030 Threats.* Online: www.enisa.europa.eu/publications/foresight-2030-threats

ENISA (2023c): *ENISA Threat Landscape 2023* (July 2022 to June 2023). Online: www.enisa.europa.eu/publications/enisa-threat-landscape-2023

European Commission (2020): *Joint Communication to the European Parliament and the Council. The EU's Cybersecurity Strategy for the Digital Decade.* JOIN(2020) 18 final. Online: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52020JC0018

European Commission (2021): *Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts.* COM(2021) 206 final. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206

European Commission (2022): *Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020.* COM/2022/454 final. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52022PC0454

European Commission (2023a): *Commission Recommendation of 03 October 2023 on critical technology areas for the EU's economic security for further risk assessment with Member States.* C(2023) 6689 final. Online: https://defence-industry-space.ec.europa.eu/commission-recommendation-03-october-2023-critical-technology-areas-eus-economic-security-further_en

European Commission (2023b): *Joint Communication to the European Parliament and the Council. European Union Space Strategy for Security and Defence.* JOIN(2023) 9 final. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023JC0009

European Commission (2023c): *Joint Communication to the European Parliament, the European Council and the Council on "European Economic Security Strategy".* JOIN(2023) 20 final. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023JC0020

European Commission (2023d): *Proposal for a Council Recommendation on a Blueprint to coordinate a Union-level response to disruptions of critical infrastructure with significant cross-border relevance.* Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023DC0526

European Commission (2023e): *Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2019/881 as regards managed security services.* COM(2023) 208 final. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2023%3A208%3AFIN

European Commission (2023f): *Proposal for a Regulation of the European Parliament and of the Council Laying Down Measures to Strengthen Solidarity and Capacities in the Union to Detect, Prepare for and Respond to Cybersecurity Threats and Incidents.* COM(2023) 209 final. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023PC0209

European Cybersecurity Competence Centre and Network (2023): *Strategic Agenda.* Online: https://cybersecurity-centre.europa.eu/strategic-agenda_en

European Parliament (2023b): *Artificial Intelligence Act: Deal on Comprehensive Rules for Trustworthy AI.* Online: www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai

European Union (2023c): *European Declaration on Quantum Technologies.* Online: https://ec.europa.eu/newsroom/dae/redirection/document/100585

European Union External Action (2022): *A Strategic Compass for Security and Defence. For a European Union that protects its citizens, values and interests and contributes to international peace and security.* Brussels, 21 March 2022. Online: www.eeas.europa.eu/sites/default/files/documents/strategic_compass_en3_web.pdf

European External Action Service (2023): *EU Statement – UN Open-Ended Working Group on ICT: Existing and Potential Threats.* Online: www.eeas.europa.eu/delegations/un-new-york/eu-statement-—-un-open-ended-working-group-ict-existing-and-potential-threats_en

ICRI (2023a): *CRI Joint Statement on Ransomware Payments* (2 November 2023). Online: www.gov.uk/government/publications/cri-joint-statement-on-ransomware-payments/cri-joint-statement-on-ransomware-payments

ICRI (2023b): *International Counter Ransomware Initiative 2023 Joint Statement* (1 November 2023). Online: www.whitehouse.gov/briefing-room/statements-releases/2023/11/01/international-counter-ransomware-initiative-2023-joint-statement/

Jacuch, Andrzej (2020): Countering Hybrid Threats: Resilience in the EU and NATO's Strategies. *The Copernicus Journal of Political Studies,* (1), 5–26. Online: https://doi.org/10.12775/CJPS.2020.001

Kádár, Pál (2022): *A kibertér és a kibertér műveleti képességek jelentősége a védelmi és biztonsági tevékenységek összehangolásában* [The Importance of Cyberspace and Cyberspace Operational Capabilities in Improving Coordination of Defence and Security Activities]. Military and Intelligence CyberSecurity Research Paper 2022/7.

Kersánszky, Tamás (2022): The Burden of Cyber Defense in the Common Security and Defence Policy of the EU. *Safety and Security Sciences Review,* 4(4), 69–79.

Kovács, László (2018): Cyber Security Policy and Strategy in the European Union and NATO. *Land Forces Academy Review,* 23(1), 16–24. Online: https://doi.org/10.2478/raft-2018-0002

Kovács, László (2020): A kiberbiztonság és a kiberműveletek megjelenése Magyarország új Nemzeti Biztonsági Stratégiájában [The Appearance of Cybersecurity and Cyber Operations in the New National Security Strategy of Hungary]. *Honvédségi Szemle,* 148(5), 3–18. Online: https://doi.org/10.35926/HSZ.2020.5.1

Magyarország Kormánya (2023): *Biztonsági osztályba sorolás és alkalmazandó védelmi intézkedések min. rendelet.* Online: https://kormany.hu/dokumentumtar/biztonsagi-osztalyba-sorolas-es-alkalmazando-vedelmi-intezkedesek-min-rendelet

Mógor, Judit – Angyal, István (2022): A létfontosságú rendszerek védelmére vonatkozó szabályozás fejlesztése [Development of the Regulations of the Critical Infrastructure Protection]. *Scientia et Securitas,* 3(2), 118–125. Online: https://doi.org/10.1556/112.2022.00102

NATO (2016a): *Commitment to Enhance Resilience.* Online: www.nato.int/cps/en/natohq/official_texts_133180.htm
NATO (2016b): *Cyber Defence Pledge.* Online: www.nato.int/cps/en/natohq/official_texts_133177.htm
NATO (2016c): *Resilience, Civil Preparedness and Article 3.* Online: www.nato.int/cps/en/natohq/topics_132722.htm
NATO (2021a): Cyber Defence. Retrieved 02 14, 2024, from www.nato.int/cps/en/natohq/topics_78170.htm
NATO (2021b): *Strengthened Resilience Commitment.* Online: www.nato.int/cps/en/natohq/official_texts_185340.htm
NATO (2022a): *Madrid Summit Declaration.* Online: www.nato.int/cps/en/natohq / official_texts_196951.htm
NATO (2022b): *NATO 2022 Strategic Concept.* Online: www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf
NATO (2023): *Vilnius Summit Communiqué.* Online: www.nato.int/cps/en/natohq/official_texts_217320.htm
Novák-Varró, Virág (2021): Az „ellenálló képesség", mint a békeépítés eszköze [Resilience as a Tool of Peacebuilding]. *Hadtudomány,* (3), 32–43. Online: https://doi.org/10.17047/HADTUD.2021.31.3.32
Pedersen, Torbjørn (2023): A Small State's Cyber Posture: Deterrence by Punishment and Beyond *Scandinavian Journal of Military Studies,* 6(1), 58–68. Online: https://doi.org/10.31374/sjms.191
Roepke, Wolf-Diether – Thankey, Hasit (2019): The First Line of Defence. *The Three Swords Magazine,* 34/2019. Online: www.jwc.nato.int/images/stories/_news_items_/2019/three-swords/ResilienceTotalDef.pdf
Stoltenberg, Jens (2022): *Keynote address by NATO Secretary General Jens Stoltenberg at the NATO Cyber Defence Pledge Conference in Italy.* Online: www.nato.int/cps/en/natohq/opinions_208925.htm
Stoltenberg, Jens (2023): *Speech by NATO Secretary General Jens Stoltenberg at the first annual NATO Cyber Defence Conference.* Online: www.nato.int/cps/en/natohq/opinions_219806.htm
Szenes, Zoltán (2021): A hibrid fenyegetések elleni szakpolitika Magyarországon [Governmental Policy against Hybrid Threats in Hungary]. *Hadtudomány,* 31(4), 39–56. Online: https://doi.org/10.17047/HADTUD.2021.31.4.39
Szenes, Zoltán (2022): Elrettentés és védelem: a NATO új haderőmodellje [Deterrence and Defence: The New NATO Force Model]. *Hadtudomány,* 32(2), 3–17. Online: https://doi.org/10.17047/HADTUD.2022.32.2.3
United Nations (2022): *Report of the Open-Ended Working Group on Security of and in the Use of Information and Communications Technologies 2021–2025.* A/77/275, 8 August 2022.

Legal sources

1139/2013 (III. 21.) Government Decision on the National Cyber Security Strategy of Hungary
1838/2018 (XII. 28.) Government Decision on the Strategy for the security of network and information systems in Hungary
Act L of 2013 on Electronic information security of state and municipal bodies
Act XCIII of 2021 on the coordination of security and defence activities
Act XXIII of 2023 on cyber certification and cybersecurity authority
Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance). Online: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555
Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2557
Government Decree 214/2020 (V. 18.) on the Electronic Information Security Early Warning System
Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Text with EEA relevance) Online: https://eur-lex.europa.eu/eli/reg/2022/2554/oj

HADMÉRNÖK
VÉDELEMINFORMATIKA

19. évfolyam (2024) 1. szám 143–176.
DOI: 10.32567/hm.2024.1.8

Lendvai Tünde[1]

Észak-Korea kiberképességei az északkelet-ázsiai régió műveleti környezetében

North Korean Cyber Capabilities in the Operational Environment of the Northeast Asian Region

Absztrakt

A tanulmány bemutatja a Koreai Népi Demokratikus Köztársaság (továbbiakban KNDK vagy Észak-Korea) kiberképességeinek szervezeti felépítését és feltételezhető kiberhadviselési stratégiáját. A kutatás célja, hogy átfogó képet adjon Észak-Korea offenzív kibertéri tevékenységének biztonságpolitikai összefüggéseiről az északkelet-ázsiai régió vonatkozásában, különös tekintettel a Kínai Népköztársasággal történő stratégiai együttműködés jelentette kockázatokra. A kutatás szekunder adatgyűjtésre épült a rendelkezésre álló szakirodalom, sajtóhírek és esetpéldák elemzésével.

Kulcsszavak: Észak-Korea, kiberműveletek, kiberstratégia, kiberhadviselés, KNDK

Abstract

The paper discusses the organisational structure of cyber capabilities and a hypothetical cyber warfare strategy of the Democratic People's Republic of Korea (hereinafter referred to as the DPRK or North Korea). It aims to provide a holistic view of North Korean offensive cyberspace activities in the context of security policy in the Northeast Asian region, with a particular focus on the risks posed by strategic cooperation with the People's

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola, e-mail: lendvai.tunde@uni-nke.hu

Republic of China. The research was based on secondary data collection through analysis of academic literature, press reports and publicly available case studies.

Keywords: North Korea, cyber operation, cyber strategy, cyberwarfare, DPRK

Bevezetés

Biztonság- és védelempolitikai megközelítésben a kiberműveleti képesség a nemzeti érdekérvényesítés eszköztárának egyik elemeként is értékelhető.[2] Napjainkig több kutatás is felvázolta a jelentős politikai hatást kiváltó incidensek alapján a Koreai Népi Demokratikus Köztársaság (a továbbiakban Észak-Korea vagy KNDK) kiberstratégiájának célrendszerét a phenjani rezsim biztonság- és külpolitikai érdekeinek kontextusában. A kutatások rávilágítottak arra, hogy Phenjan egyre fejlettebb kiberképességeivel képes pénzügyi erőforrásokhoz jutni, valamint a kiberműveletek általi provokációval politikai és stratégiai előnyöket kikényszeríteni a nemzetközi közösségből, amivel stratégiai célja, hogy elősegítse a Kim-rezsim fennmaradását. Észak-Korea nemzetközi helyzetében a kiberképességek oly módon is bevethetők a katonai értelemben vett szürkezónában, hogy még aszimmetrikus helyzetben[3] is (költség)hatékonyan alkalmazhatók politikai célú erődemonstrációra, hírszerzésre vagy a haderőfejlesztést finanszírozó anyagi javak megszerzésére, számottevő konfliktuseszkalációs kockázat nélkül.[4]

Noha a kiberképességek katonai alkalmazásáról Észak-Korea még nem publikált hivatalos, stratégiai szintű dokumentumot, a vezetők politikai nyilatkozatai alapján felvázolható az információs és kibertéri műveletek szerepe a hadászati gondolkodásban. Például a 2003-as iraki háború után Kim Dzsongil a következőket mondta katonai vezetőkhöz intézett beszédében:

„A hadviselés mindeddig a töltényekről és az olajról szólt, a 21. században azonban már az információ felhasználásáról. Az dönti el, hogy ki nyeri meg és ki veszíti el a háborút, hogy békeidőben melyik fél fért hozzá nagyobb mértékben az ellenség katonai technológiájával kapcsolatos információhoz, milyen hatékonyan képes megzavarni ellenfele vezetés-irányítási csatornájában az információáramlást, és milyen hatékonysággal használja fel saját információit."[5]

Kim Dzsongun 2012-ben úgy jellemezte a Koreai Néphadsereg Központi Felderítő Irodájának (Reconnaissance General Bureau, a továbbiakban: Központi Felderítő Iroda vagy RGB) számítógép-hálózati műveleti képességét, mint egy minden célra bevethető kardot, amely a nukleáris fegyverekkel és hordozórakétákkal együtt lehetővé teszi a rezsim számára a folyamatos csapásmérést.[6] Mindkét vezető összességében azt

[2] Berzsenyi 2023: 19; 99–104; 111–113; 123–125.

[3] Észak-Korea és az Egyesült Államok között aszimmetrikus helyzet áll fent több aspektusban is. Ezek például a térségben fennálló katonai és politikai szövetségesek (USA–Dél-Korea és USA–Japán) egyesített haderejében és ütőképességében mutatkozik meg az észak-koreai rezsim elszigeteltségével szemben, továbbá a haderőre fordítható erőforrások (pl.: költségvetés) és az eszközpark modernizáltságának (értsd: fejlettségének) relációjában.

[4] Ha 2022.

[5] Kong–Lim–Kim 2019: 2.

[6] „Cyberwarfare is an all-purpose sword that guarantees the North Korean People's Armed Forces ruthless striking capability, along with nuclear weapons and missiles." Fordítás: Berzsenyi 2023: 123–124.

az attitűdöt erősítette meg a kiberképességek önálló stratégiai funkciójával kapcsolatban, hogy a kibertéri katonai egységek offenzív és defenzív oldalon történő célzott és rugalmas alkalmazhatósága, valamint adaptív és fedett jellege miatt egyfajta elrettentésen alapuló védelmet is képesek nyújtani (a nukleáris csapásmérő képesség kialakításához hasonlóan) a modern háborúkat eldöntő elektronikai hadviselés korában.[7]

Észak-Korea nemzeti kiberműveleti képességeinek feltérképezését és stratégiai célrendszerének elemzését nehezíti, hogy az állami érdekeket megvalósító, jellemzően küldetésorientált műveletszervezési elvek nyomán összeállított egységek tevékenysége összefonódik a fejlett perzisztens fenyegetések (*Advanced Persistent Threat,* a továbbiakban APT vagy fejlett perzisztens fenyegetések)[8] működésével.[9] A kutatás elsődleges célja, hogy a KNDK jelentős[10] offenzív kibertéri műveleteiről és az ezeket végrehajtó katonai egységekről publikusan elérhető szakirodalom komparatív értékelése alapján jellemezze Észak-Korea kiberképességeit, és feltárja kiberhadviselési stratégiájának lehetséges elemeit.

Módszertan és hipotézis

A kutatási probléma felvetése rávilágított arra, hogy a létező elméleti keretrendszerek nem elegendő mélységben veszik figyelembe Észak-Korea (és ezáltal az északkelet-ázsiai szubrégió) kiberbiztonsági környezetének jellemzése során a kínai infrastruktúrával való összefonódás lehetőségében rejlő biztonságpolitikai kockázatokat. Ezért a kutatás új elemzési szempontként emeli be Észak-Korea feltételezhető kiberhadviselési stratégiájának értelmezésébe az ország Kínai Népköztársasághoz kötődő geopolitikai és biztonságpolitikai helyzetének értékelését és az együttműködés különböző aspektusait. A tanulmány második része ismerteti az észak-koreai állami hátterű fejlett perzisztens fenyegetések tevékenységének aktuális trendjeit. Ezután a szerző áttekintést nyújt Észak-Korea hálózati adottságairól, kiberképességeit keretező intézményi struktúrájáról, főbb stratégiai partnereiről. Végül pedig áttekinti az észak-koreai kibertéri műveletek stratégiai célrendszeréről publikált elméleteket, és bemutatja a lehetséges kiberhadviselési stratégiai irányokat. A biztonságpolitikai módszertani megközelítést alkalmazó elemzés az alábbi kutatási kérdés (KK1) és egy hipotézis (H1) felvetését vizsgálta meg:

KK1: A nyilvánosan észak-koreai aktorok tevékenységére attribútált kibertéri műveletek stratégiai célrendszere hogyan illeszkedik az ország védelempolitikájába, és miként támogatja a phenjani rezsim nemzetközi érdekérvényesítő képességét?

[7] Berzsenyi 2023: 123–125.

[8] Az APT *(Advanced Persistent Threat)* olyan kibertámadási modell, amelyben a támadó csoport vagy kiberbűnözők rendkívül komplex eljárásokat (TTP) és fejlett támadóeszközöket alkalmaznak, továbbá hosszú időn keresztül képesek észrevétlenek maradni a célzott hálózatokban, hogy érzékeny információkat szerezzenek meg. Ezen jellemzők és a célorientált feladatmegvalósítás okán feltételezhető, hogy az APT-csoportok tevékenységét állami támogatással hajtják végre. Az APT-csoportok műveletei tehát valamely hadsereg vagy nemzetbiztonsági szervezet egységének tevékenységét fedik le, vagy állami háttértámogatással működő kiberbűnözői célok megvalósítását foglalja magában.

[9] Kong–Lim–Kim 2019.

[10] Jelentős, vagyis nagy horderejű, stratégiai vagy politikai érdekek mentén bekövetkezett incidensek.

- H1: A békeidőszaki kiberműveletek kettős védelempolitikai célja, hogy egyrészt finanszírozza a haderőfejlesztést, másrészt a stratégiai céllal alkalmazott katonai provokációkat kiegészítve gazdasági és politikai engedményeket kényszerítsen ki a nemzetközi közösségből.

Észak-Korea geostratégiai helyzetéből adódóan alkalmas a Kínai Népköztársaság nemzetközi erőkivetítési törekvéseinek támogatására az északkelet-ázsiai régióban, mert a két állam között stratégiai érdekegyezés áll fenn az USA és a szubregionális politikai-katonai szövetség gyengítése tekintetében.[11] Ezért másodlagos kutatási célkitűzés a pekingi és a phenjani vezetés között feltételezhető stratégiai együttműködés kibertéri aspektusai által generált kockázatok feltérképezése és leírása. A beazonosított összefüggések hozzájárulnak a kínai és észak-koreai állami aktivitás feltárásához kapcsolódó, kiberfenyegetés-felderítő (*cyber threat intelligence,* CTI) tevékenység által nyert információk komplexebb értékeléséhez. A fenti célkitűzés mentén a szerző további egy kutatási kérdés (KK2) és hipotézis (H2) vizsgálatát végezte el:

KK2: Milyen stratégiai adottságok és érdekek teszik lehetővé a Kínai Népköztársaság és a Koreai Népi Demokratikus Köztársaság között feltételezhető együttműködést az offenzív kibertéri műveletek kivitelezésében?

- H2: A geopolitikai sajátosságok lehetővé teszik Kína számára, hogy infrastrukturális erőforrásokat bocsásson az észak-koreai katonai kiberegységek rendelkezésre, továbbá tudásmenedzsmenttel járuljon hozzá észak-koreai személyek képességeinek fejlesztéséhez.

Az Észak-Korea nemzeti kiberképességeinek vázát nyújtó szervezeti felépítés és a fejlett perzisztens fenyegetések stratégiai célrendszerének feltérképezéséhez szekunder forrásokból származó adatok álltak rendelkezésre. Ennélfogva a kutatás témaköre több módszertani limitációt is magában hordoz. Egyfelől Észak-Korea kiberképességeinek összetételét, valamint alkalmazásának stratégiai irányát ez irányú kormányzati kommunikáció hiányában csak induktív módszertani megközelítéssel lehet meghatározni, ám ez esetenként disszidensek és más hírszerzéssel kapcsolatban álló informátorok beszámolóira támaszkodik (így a forrás objektivitása csökken, emellett szekunder forrásból származó adatgyűjtésnek minősül). Ezt kiegészítve, az Észak-Koreához köthető APT-aktivitás deduktív vizsgálata betekintést adhat a képességek alkalmazásának célrendszerébe, ám ebben az esetben sem lehet élesen elkülöníteni a kiberbűnözői tevékenységet az állami hátterű, de anyagilag (is) motivált műveletektől. Mindamellett, hogy a technikai adatokra alapozott (például *digital forensics,* IoC- vagy TTP-adatok), kvalitatív és kvantitatív módszerekkel elkészített CTI-jelentések nagyobb objektivitást kínálnak, figyelembe kell venni a támadást elszenvedő fél érdekeit. A nyilvános attribúciót végző állam (egyedi nemzeti érdekei mentén) vagy a megtámadott szervezet (a kihasznált sérülékenység miatti felelősségrevonhatóságából adódóan, illetve a keletkezett kár megtérítési kötelezettsége vagy hatósági bírság miatt) ugyancsak torzíthatja az információk pontosságát és objektivitását.[12]

[11] Bartók–Wagner 2021.
[12] Berzsenyi 2023: 19.

Az északkelet-ázsiai régió biztonságpolitikai környezetének kiberbiztonsági összefüggései

Az északkelet-ázsiai régió (Kína és Tajvan, valamint Japán és a két Korea) biztonságpolitikai környezetét folyamatos haderőfejlesztési és haditechnikai modernizációs kényszer alakítja. Ennek több kiváltó oka is van, ám euroatlanti perspektívából nézve elsődleges indikátorként a kínai haderő modernizációját tartjuk számon. Ennek hátterében az áll, hogy a pekingi vezetés az Egyesült Államok (a továbbiakban USA) térségbeli jelenlétéből[13] fakadó fenyegetettségpercepcióját csökkentette a haderőfejlesztéssel és katonai reformokkal. A Koreai-félsziget elhelyezkedése egyfajta természetes védvonalat képez (és pufferzónát ad az amerikai és a dél-koreai erők között) Kína part menti régiója számára például egy amerikai blokád esetén, ami az ország védelempolitikájának egyik alapköve. Ezáltal Észak-Korea geostratégiai helyzetéből adódóan alkalmas a Kínai Népköztársaság nemzetközi erőkivetítési törekvéseinek támogatására. A kínai haderőreform mögött álló A2/AD stratégia[14] magyarázza a megnövekedett katonai – különösen haditengerészeti – aktivitást. A regionális erőkivetítés érdekében Kína a dél-kínai-tengeri zátonyokon létesített bázisokkal, haditengerészeti jelenlétével és az erődemonstrációs hadgyakorlatok révén juttatja *de facto* érvényre igényét a vitatott státuszú területek felett. Mindez az utóbbi években többek között Vietnámot, a Fülöp-szigeteket, Malajziát, Japánt és a Koreai Köztársaságot is haderejének transzformációjára késztette, ami általában partra szálló és területvédelmi képességfejlesztést takar. Ebből következik, hogy a térség dinamikus militarizációját kiváltó második indikátor a szigetcsoportok feletti kontroll megszerzését (a tengeri erőkivetítést) jelenti. A militarizációs trendeket befolyásoló harmadik indikátorként a Tajvani-szorosban és a Koreai-félsziget körül tapasztalható katonai provokációk azonosíthatók, különösképp az észak-koreai atom- és rakétaprogram fejlődése miatti fenyegetettség okán.[15]

Ebben a biztonságpolitikai környezetben az északkelet-ázsiai régió nemzeteinek haderőfejlesztési törekvései egyaránt irányulnak a területszerzésre vagy területvédelemre alkalmas katonai képességek kialakítására,[16] valamint az információszerzéstől a csapásmérésig terjedő változatos műveleti célokat kiszolgáló offenzív és kibertámadó képességek fejlesztésére. Az utóbbi öt évben számos állam – köztük Kína és Tajvan – alakította át olyan elvek mentén kibervédelmi struktúráját, amelynek eredményeképpen adaptív ellenálló képességük részévé tették a hiteles kibertéri elrettentés[17] koncepcióját kibertámadó képességek felépítésével.[18]A kibertámadó

[13] Ideértve az állandó amerikai katonai bázisok fenntartását Japánban és Dél-Koreában, a fegyverszállítást (például a Japán részére átadott Patriot és a Dél-Koreába telepített THAAD – Terminal High Altitude Area Defense légvédelmi rendszerek), a rendszeres hadgyakorlatokat, valamint a haditengerészeti erők jelenlétét.

[14] Angolul: Anti-Access/Area Denial (A2/AD) strategy: hozzáférést gátló és területmegtagadó stratégia.

[15] Bartók–Wagner 2021.

[16] Bartók 2020: 80–101.

[17] Egy ország védelmi koncepciójában a kibertéri elrettentés olyan kibertámadó képesség kialakítását foglalja magában, amely akkora mértékben csökkenti az ellenség képességeit, hogy nem tud hatékony támadást indítani. Azonban ezzel párhuzamosan elengedhetetlen egy olyan állami kibervédelmi rendszer fenntartása, amely csak aránytalanul nagy erőforrás-befektetéssel törhető át. (Lásd Kovács 2021).

[18] Yau 2020.

képességek felépítése világviszonylatban is jellemző kiberhadviselési stratégiai koncepcióváltás eredménye, amely a kibertéri szuverenitás biztosítását célozza, hiszen a 21. század műveleti környezetében, a civil információs rendszerek (például közösségi média, civil mobilkommunikációs technológiák: 4G és 5G) és katonai komponensek ugyanolyan fajsúlyosan járulnak hozzá egy ország kibervédelmi struktúrájához.[19] Az USA és térségbeli katonai szövetségesei hadgyakorlatok megszervezésével tartják fenn az általános készültséget és reagálóképességet, amelyek kiterjednek többek között haditengerészeti és kiberműveleti területre. Például az USA és Dél-Korea 2023 áprilisában jelentette be azon szándékát, hogy kibervédelmi gyakorlatokat is tartsanak *(table top excercise)* az integrált védelmi párbeszéd *(integrated defense dialogue)* kiberműveleti együttműködési munkacsoportja (Cyber Cooperation Working Group, CCWG) keretében.[20] Ugyanezen megfontolásból Tajvan kétévente rendezi meg nemzetközi résztvevőkkel a komplex (*full scale cyber range* típusú) úgynevezett Cyber Offensive and Defensive Exercise gyakorlatát.[21] Kiemelendő, hogy Tajvan esetében napjainkra a diplomáciai célú látogatások (például Nancy Pelosi amerikai demokrata házelnök tajvani útja) is eszkalációs tényezővé váltak és kínai erődemonstrációt indukáltak, amit korábban a hadgyakorlatok, haditechnikai vagy védelmi ipari együttműködések bejelentése váltott ki.[22]

Az északkelet-ázsiai régió biztonságpolitikájának relevanciája a hadiipari igények kiszolgálásának vonatkozásában is megmutatkozik: Japán, Dél-Korea és Tajvan IKT-ipara önmagában is jelentős hatást gyakorol a globális ellátási láncokra, különösen a háború sújtotta Európa számára. Emellett egyre jelentősebb az ázsiai fegyverexport volumene az EU-tagállamok irányába,[23] ezzel párhuzamosan Észak-Korea Oroszország részére szállít katonai felszerelést, többek között lőszereket. Az észak-koreai – orosz bilaterális kapcsolat kibővülése számos fenyegetést hordoz magában, amelyek a technológiai vagy haditechnikai szegmensben is megjelentek.[24]

Szakértői feltételezések szerint az orosz technológiai támogatásnak jelentős szerepe volt abban, hogy Észak-Korea 2023 novemberében sikeresen pályára állította első műholdját, ami hozzájárul az ország (katonai) felderítő képességének minőségi növekedéséhez. Az euroatlanti közösségnek fel kell készülnie az orosz – észak-koreai katonai és gazdasági együttműködés jelentette fenyegetésre – akár a kibertérből érkező fenyegetésekre is –, és ki kell dolgozni a kockázatcsökkentő szakpolitikai lépéseket.[25] Meglátásom szerint ezen szakpolitika kidolgozásában szerepe lehet a kínai érdekek felhasználásának (akár Oroszországgal szemben), mivel Észak-Korea korábban kizárólagosan a kínai kereskedelem és geopolitika védőernyőjének hatókörébe tartozott, ennek exkluzivitására (és Kína számára a profitabilitására) konkurenciát

[19] Kovács 2021: 119–137.
[20] US Department of Defense 2023.
[21] 2021-ben energiaipart érő támadást szimuláltak 33 ország, köztük az USA csapatának részvételével. Bővebben Taiwan National Computer Emergency Response Team 2022.
[22] Bartók 2022.
[23] Például Észtország, Törökország, Lengyelország, Finnország és Norvégia együtt 18 db K9-es önjáró lövegre adott megrendelést a dél-koreai Hanwha részére, míg az első 24 db K9-esből és 10 db K2-es harckocsiból álló szállítmány már 2022 decemberében megérkezett Lengyelországba. Bővebben McLeary–Hudson 2022.
[24] Geigenberger 2023.
[25] Cha–Lim 2024.

jelent az oroszországi fegyverexport és a potenciális technológiai együttműködés. Kulcsfontosságú tehát, hogy a NATO-tagországok és a velük partner ázsiai nemzetek a digitális államigazgatási rendszereiket felépítő adatvagyon és infrastruktúra integritását garantálni tudják az APT-vel és más kiberbűnözői aktorokkal szemben (amelyek akár lehetnek észak-koreai hátterűek),[26] továbbá az ezekre támaszkodó ipari irányítási rendszerek, gazdasági társaságok és folyamatok, valamint a csúcstechnológiákat érintő kutatóhálózatok rezilienciáját is szavatolják.[27]

Az észak-koreai kibertéri műveletek aktualitás trendjei

Észak-Korea nemzeti kiberműveleti képességei folyamatos fejlődésen mentek keresztül a hírhedt Sony Pictures Entertainment (2014) rendszereit ért erődemonstráció, a Banglades Bank kompromittációja (2016) és a WannaCry 2.0 zsarolóvírus (2017) terjesztése óta elmúlt években. Az észak-koreai kibertéri aktivitást vizsgáló elemzők jellemzően a pénzügyi és az egészségügyi szektor vertikumába tartozó célpontok elleni műveletek szofisztikáltságában (az alkalmazott technikák komplexitása, kifinomultsága) és volumennövekedésében azonosították be a képességfejlődés indikátorait. Erre példa a kriptovaluta-szolgáltatásokat kompromittáló AppleJeus kampányok (2018-tól)[28] és a kórházi rendszerek adatait titkosító MAUI zsarolóvírus, amelyet 2021 májusától kezdtek terjeszteni.[29]

Ezen incidensek kapcsán arra lehet következtetni, hogy az anyagi motiváció maradt a legmeghatározóbb faktor az állami hátterű, fejlett perzisztens fenyegetések és klasztereik tevékenységében.[30] Ezt a trendmegfigyelést támasztja alá a kriptovalutákkal való visszaélések, a fintech vállalkozások (pénzügyi technológia) és pénzügyi intézmények körébe tartozó célpontok incidensszámának éves változása alapján a Mandiant 2023-ban publikált, éves áttekintést adó kiberfenyegetettség-felderítési (CTI) jelentése az észak-koreai APT-tevékenységéről.[31] Az elemzők az anyagilag motivált incidensek domináns növekedését mutatták ki a 2020–2023 közötti időszakban, amire a Covid–19 okozta világjárvány is jelentős hatással lehetett. Azért, hogy megakadályozza a járvány kitörését az országon belül, a rezsim lezárta határait, és teljesen elvágta magát a külkereskedelemtől. A szöuli Korea Trade-Investment Promotion Agency szerint Észak-Korea Kínával folytatott kereskedelmi forgalma 2020-ban 80,7%-kal esett vissza.[32] Egyrészt, a Mandiant kutatóinak állaspontja szerint, a járvány miatti kínai határlezárás azért növelhette az anyagilag motivált célpontok

[26] Krasznay 2022: 29–46.
[27] Krasznay 2020: 83–97.
[28] US Cybersecurity and Infrastructure Security Agency 2021.
[29] US Cybersecurity and Infrastructure Security Agency 2022.
[30] Értsd: észak-koreai APT-csoportok és feladat-orientált tevékenységeik p APT38 – Cryptocore (Mandiant: UNC1069), AppleJeus-aktivitás (Mandiant: UNC1720), TraderTraitor (Mandiant: UNC4899) stb.
[31] Az elemzés a Mandiant CTI szolgáltatása révén összegyűjtött információk alapján készült. Forrásai közt említi a vállalat incidenskezelésből származó *(intrusion response)* saját adatgyűjtését, kormányzati közleményeket és tájékoztatókat, valamint az OSINT-eszközök felhasználásával kinyert és észak-koreai disszidensek által átadott hírforrásokat.
[32] Shim 2021.

volumenét, mert blokkolta az országba telepített külföldi műveleti egységek személyi állományát abban, hogy hozzáférjenek az észak-koreai erőforrásokhoz, finanszírozáshoz.[33] Megjegyzendő, hogy Észak-Korea korábban is határain kívülről hajtotta végre kibertéri műveleteit, számos esetben a Kínai Népköztársaság (a továbbiakban Kína) területéről. Ennek elsősorban infrastrukturális és geopolitikai okai vannak, amit a tanulmány egy későbbi fejezetében mutat be. Emellett esetenként a műveleteket végrehajtó személyek is külföldön tartózkodtak vendégmunkásként, amit jelentősen megkönnyít – például az anyanyelvhasználat miatt – a kínai–koreai etnikai kisebbség jelenléte Kína északi tartományaiban (Liaoning és Csilin).[34] Ezenfelül a távmunkavégzés térnyerésével párhuzamosan megjelent a globális piacon az „illegális" észak-koreai munkaerő, akiket tudatosan vagy tudtukon kívül alkalmaztak vállalatok az IT-szektorban. Az észak-koreai távmunka megjelenése az IT területén a kiberkémkedés, a számítógép-hálózatok felderítésének és a szankciós politika megkerülésének (illegális finanszírozás) kockázatát hordozza magában.[35]

A pénzügyi szektor leggyakoribb célponttá válásával párhuzamosan nőtt a kibertámadó képességek stratégiai beágyazottsága a Kim-rezsim biztonságpolitikai felfogásába. Ez egyrészt egybevág a világviszonylatban is jellemző célpontkiválasztási trendekkel, másrészt viszont praktikus okokra is visszavezethető Észak-Korea elszigeteltnek mondható nemzetközi helyzetében. A biztonságpolitikai megközelítést is alkalmazó szakirodalom az észak-koreai kibertéri műveletek egyik mérvadó stratégiai céljaként tekint az ország nukleáris és haderőfejlesztési programjának finanszírozására. Ez abban mutatkozik meg, hogy a kriptovaluták és az elektronikus pénzeszközök alkalmasak az ENSZ szankciós rezsimje által érintett termékek és nyersanyagok ellentételezésére is. A korábbi években több forrás is megerősítette, hogy a phenjani rezsim a katonai erő fenntartásához és fejlesztéséhez szükséges anyagi erőforrásokat többek között a kibertér által lehetővé tett illegális finanszírozással vagy kriptovaluták ellopásával fedezte. Például a Pentagon (az USA Védelmi Minisztériuma) az észak-koreai kibermőveletek tervezéséért és végrehajtásáért felelős Központi Felderítő Irodát (RGB) terror- és illegális műveleteket végrehajtó állami szervként tartja számon. Az USA bilaterális alapon több alkalommal is szankcionálta az RGB-t a szervezethez kötődő vállalkozásokon keresztül: 2010-ben fegyverkereskedelem, majd pénzmosás miatt, ezt követően 2015-ben a Sony Pictures-t ért incidens miatt.[36]

Ezt az összefüggést támasztja alá a Chainalysis (blokkláncelemző vállalat) felmérése is, amelynek számításai alapján a 2021-ben okozott kár mintegy 429 millió dollár értékű kriptovaluta volt, ami 2022-ben ennek négyszeresére, megközelítőleg 1,7 milliárd dollárnak megfelelő értékre emelkedett. Az elemzőcég a 2022-ben bekövetkezett globális kárérték (3,8 milliárd dollár) 44%-ának bekövetkezését köti észak-koreai hátterű kriptovalutákkal való visszaélésekhez.[37] Ezzel párhuzamosan Phenjan 2022-ben hajtotta végre eddigi legnagyobb volumenű rakétafegyverzet-kísérletét, amely a CSIS kutatóintézet adatbázisa alapján legalább 70 hordozóeszközteszt

[33] Barnhart et al. 2023.
[34] Kong–Lim–Kim 2019: 2–6.
[35] US. Department of Treasury 2022.
[36] Ha–Maxwell 2018: 4.
[37] Chainalysis Team 2023.

végrehajtását jelentette, ami a korábbi átlagos éves mennyiség négyszerese.[38] Phenjan számos indítóplatformot és eltérő hatótávolságú eszközt tesztelt, ennek kapcsán kiemelhető, hogy a hiperszonikus sebesség elérése és az önállóan célra vezethető (MIRV) visszatérő fejek (a rakéta harci része) alkalmazása egyaránt elképzelhető fejlesztési irány lehet a ballisztikusrakéta-eszközök tekintetében. Ezenkívül a nemzetközi megfigyelések szerint legalább 6 alkalommal teszteltek olyan robotrepülőgépeket *(cruise missile),* amelyek egyes típusai nukleáris robbanófejek[39] hordozására is alkalmassá tehetők.[40] A robotrepülőgépek ezen alternatív fejlesztési irányának kialakítását egyaránt kiválthatta a hegyi-karabahi fegyveres konfliktusban és az ukrajnai háborúban alkalmazott drónok és robotrepülőgépek taktikai hatásának eredményessége, ami komoly kihívást jelent a kiber-, az elektronikai és a légvédelem számára. Az észak-koreai fegyverzetkísérletek növekedésének és fenntarthatóbb finanszírozhatóságának további nemzetközi relevanciája, hogy az ukrán fronton (az iráni és török gyártmányú eszközök mellett) a későbbiekben észak-koreai irányított fegyvertípusok is feltűnhetnek, akárcsak a gázai övezeben, mivel az észak-koreai fél a múltban is adott el fegyvereket palesztin szélsőségeseknek.[41]

Mérvadó trend továbbá, hogy az észak-koreai hátterű aktorok (például: APT37, APT38, APT43 és egyéb kibertéri egységek)[42] célpontkiválasztásában, alkalmazott eljárásaiban és eszközeiben (például rosszindulatú kódjaiban) egyre nagyobb átfedések mutathatók ki. A Mandiant álláspontja szerint ez a jelenség az egyedi TTP-k (vagyis taktika, technikák és eljárások) egymás közti megosztására, továbbá műveletszervezési újításra utalhat. Ez alapján feltételezhető az APT-tevékenységhez kapcsolható észak-koreai hírszerző vagy katonai intézmények szervezeti és strukturális átalakítása (lásd *Kiberképességek adaptációja az észak-koreai hadviselési kultúrába* című fejezet). Egy ilyen típusú átalakítás alátámasztja, hogy miért bővülhetett az észak-koreai APT-csoportok támadói profilja a pénzügyi szektorbeli célpontokkal. Emiatt a Mandiant kutatói ugyanerre a jelenségre vezetik vissza a blokklánc *(blockchain)* és fintech vertikumot célzó támadások dinamikus növekedését.

Phenjan egy összehangolt célpontkiválasztáson és közösen felhasználható eszközrendszeren alapuló képességfejlesztéssel nemcsak racionalizálhatja az offenzív kibertéri tevékenységét és még nehezebben átláthatóvá teheti nemzeti kibertéri környezetét *(cyber threat landscape),* hanem a működésbeli átfedésekkel megnehezítheti az attribúciós kísérleteket is.[43] Mindemellett, amennyiben a 3CX Desktop App (kommunikációs szolgáltatásokat nyújtó szoftver) 2023. tavaszi kompromittálása kapcsán beigazolódik, hogy az UNC4736 azonosítóval ellátott tevékenység valóban észak-koreai hátterű művelet, úgy ez lesz az első úgynevezett kaszkádszerű hatással bíró hálózati behatolás, amely során észak-koreai aktorok kormányzati intézmények beszállítói láncát kompromittálták.[44] A Mandiant incidens kivizsgálására felkért szakértői a kezdeti behatolási

[38] Missile Defense Project 2023.
[39] Amennyiben sikeres lesz az észak-koreai miniatürizálási fejlesztés. Ez a képesség megléte még vitatott a szakemberek körében.
[40] Kertész 2023.
[41] Ramani 2023.
[42] Például az egyes esetekben gyűjtőfogalomként is használt csoportok, mint a Lazarus vagy az Andariel.
[43] Barnhart et al. 2023.
[44] Johnson et al. 2023.

vektort a Trading Technologies által biztosított X_Trader szoftvercsomag manipulált telepítőjére vezették vissza (amelyben Windows- és Mac-verziók egyaránt érintettek voltak). Az UNC4736 trójai típusú módszerrel érte el a legitim függőségnek álcázott *(legitimate dependency)* két rosszindulatú DLL-modul futtatását (SIGFLIP és DAVESHELL) és a Veiledsignal rosszindulatú program és moduljainak telepítését *(multi-stage modular backdoor),* amelyek egy többlépcsős folyamat során hátsó kaput nyitottak az érintett hálózatokba. A Veiledsignal backdoor két DLL-modulja a Chrome, a Firefox és az Edge webböngészők kommunikációjába történő folyamatbefecskendezést *(process injection module)* és a C2 kiszolgálóval való kommunikációt tette lehetővé (*command-and-control:* C&C modul).[45]

Észak-Korea kibervédelmi és digitális ökoszisztémája

Noha Észak-Korea relatív elmaradottságát és szegénységét a múltban gyakran szemléltették ritkás közvilágítást kiemelő éjszakai műholdfelvételekkel és az elektromos hálózat megbízhatatlanságáról szóló hírekkel, napjainkra a belföldi telefónia és egyéb hálózati szolgáltatások lefedettsége kielégítő mértékű. Az ország első (2G) mobilhálózatának telepítése 2002-ben indult el, de 2004-ben hirtelen leállították a projektet, egy hónappal azután, hogy Rjongcshonban robbanás történt egy vasútállomáson. A detonáció a város nagy részét lerombolta, és állítólag több ezer ember életét követelte. Az eset további nemzetbiztonsági relevanciája azonban az volt, hogy a vonat, amelyen Kim Dzsongil utazott, órákkal korábban haladt át a rjongcshoni állomáson. Emiatt az a híresztelés terjedt el, hogy a detonáció egy mobiltelefon használatával indított merényletkísérlet volt, és az észak-koreai hatóságok eszerint jártak el (egyebek mellett a mobiltelefonok használatát is betiltották).[46]

Észak-Korea napjainkban is működő két celluláris hálózatának egyikét, a Koryolink nevű belföldi mobilhálózatot az Orascom Telecom Media & Technology (OTMT) és a koreai Korea Posts and Telecommunications Co. (KPTC) kezdte el kiépíteni 2008 decemberében.[47] A Koryolink 2011-re stabil 3G-szolgáltatást nyújtott, amelynek lefedettsége kiterjedt Phenjanra, 15 nagyvárosra, több mint 100 kisvárosra, valamint néhány autópályára és vasútvonalra. Az ország egészéhez mérten ekkor 14%-os volt a területi lefedettség, amivel a lakossági részarány meghaladta a 90%-ot, 1,7 millióra becsülhető előfizetői bázissal.[48] A Kryolink profitmegosztása miatti 2015-ös viták következtében egy másik, „riválisˮ 3G adatátvitelt kínáló szolgáltatót hoztak létre, a Kangsongot, amely már kizárólagos kormányzati tulajdonban van, és teljes celluláris hálózati lefedést kínál Észak-Korea vidéki területein is.[49] Napjainkban is ez a két 3G-szolgáltatás működik a KNDK-ban, többek közt műholdfelvételek által igazoltan.

[45] Symantec Threat Hunter Team 2023.
[46] Williams 2019.
[47] A Koryolink szolgáltatást 75%-ban egy egyiptomi származású vállalkozó, Naguib Sawiris birtokolja az Orascomon keresztül, amely többségi tulajdonosa a kivitelező Cheo Technology vállalkozásnak. A tulajdoni hányad fennmaradó része a koreai Postaszolgáltatási és Távközlési Minisztérium birtokában maradt, a Koryolink márka mögött álló másik vállalaton (Korea Post and Telecommunications Co.) keresztül.
[48] Montlake 2012.
[49] Williams 2015.

A 4G- (és akár 5G-) adatátvitelt lehetővé tévő infrastruktúra-fejlesztést várhatóan a Huawei vállalat fogja kivitelezni, ám a celluláris technológiai generációváltás megkezdésének céldátuma még kétséges (habár ezzel kapcsolatos kutatási projektekről a Kim Irszen Egyetem már közzétett tudományos publikációkat). Feltételezhető, hogy a 2G- és 3G- infrastruktúra kiépítéséhez hasonlóan Észak-Korea ez esetben is a más szolgáltatók hálózatfejlesztése során piacra kerülő használt eszközöket építi be rendszerébe.[50]

A Koryolink máig a világ egyik legjobban kontrollált rendszerének tekinthető. Az észak-koreai előfizetők részére csak belföldi hívásokat és helyben hosztolt adatszolgáltatást tesz lehetővé (ami tulajdonképpen az erősen cenzúrázott és megfigyelt észak-koreai intranet kialakítását jelentette). A külföldi (előfizetők diplomaták és turisták) ellenben nem kezdeményezhetnek belföldi hívásokat, és kizárólag a globális internetes tartalmakhoz férhetnek hozzá, az észak-koreai intranethez nem. Ezeken felül a társadalom szűk, privilegizált rétege számára egy elkülönített hálózati szabály áll rendelkezésre, amely kivételként azonosítja az állam által kiadott, hazai titkosító algoritmussal ellátott mobiltelefonokat, így azokról lehetséges a külföldi hívások lebonyolítása (és elméletben mentesülnek a normának számító belföldi lehallgatás alól). Ezen kiadott mobileszközök száma a legutóbbi nyilvános forrás szerint körülbelül ezerfős kvótát jelentett (2008 körül), ami megegyezik a phenjani legfelső vezetés becsült létszámával.

A Koryolink felügyeleti és megfigyelési megoldásainak kialakításához, a celluláris környezet 2008-as kialakításától kezdve, kínai technológiai vállalatokat vontak be szakértőként. A Huaweit bízták meg a hálózati eszközök beszerzésével és annak kialakításával, hogy a titkosítási rendszer nem okoz-e instabilitást a hálózat működésében, míg a Panda International Information Technology Co. dolgozott a rendszer szoftveroldali kialakításán. A Koryolink belbiztonsági célú, törvényes lehallgatási kapacitásáról (*legal interception gateway,* LIG) ugyancsak 2008-as, a Huawei által készített tervdokumentumok adatai állnak rendelkezésre: így az infrastruktúra kezdetben legfeljebb 7 terabájtos tárolókapacitás mellett, 1200–2500 célpontot támogathatott, és egyidejűleg legfeljebb 240–300 telefonhívás és 250–300 adatmunkamenet megfigyelésére lehetett képes.

A kivitelezési tervek második fejlesztési szakaszában, 10 terabájtos adattároló kapacitással 5000 célpontra és további 300 telefonos és adatátviteli munkamenetre növelték volna az egyidejűleg történő megfigyelés hatókörét. A megfigyelőközpont a kivitelezés első és második szakaszában akár 180–200 felhasználót is támogathatott, amelyből 60–80 operátor egyidejűleg kapcsolódhatott be a hálózati forgalomba. Az akkori technológiai standardoknak megfelelően az adatmegfigyelő rendszer a HTTP (weboldalak), FTP (fájlok fel- és letöltése), SMTP, POP3 és IMAP4 (e-mail) protokollokat támogatta.[51]

Az észak-koreai belföldi mobiltelefon-szolgáltatás kiépítésével és a kommunikációs csatornák megfigyelőrendszerének kialakításával párhuzamosan a phenjani vezetés megkezdte az illegálisan és legálisan behozott kínai mobiltelefonok (és a későbbiekben

[50] Williams 2023b.
[51] Williams 2019.

az okostelefonok) eszközfelügyeletének állami megvalósítását. Erre egyfelől azért volt szükség, mert az országba csempészett kínai mobiltelefonok lehetővé tették a határ menti területeken (ahol elérhető a kínai mobiltelefonos hálózat) élő emberek számára, hogy beszélhessenek a Kínában vagy Dél-Koreában élő rokonokkal, barátokkal. Ez a felügyelet nélküli kommunikációs csatorna olyan kockázatokat teremtett, amelyek megkönnyítik a nemzetbiztonsági szempontból értékes információk kiszivárgását vagy a csempészhálózatok észrevétlen, hatékony fenntartását. Számos Dél-Koreában élő disszidens úgy lép kapcsolatba a hozzátartozóival Észak-Koreában, hogy ezeket az illegális mobiltelefonokat eljuttatja az országba közvetítőkön vagy csempészeken keresztül.

Az illegális mobiltelefonok használata elleni kormányzati fellépés módszeréről nincs publikusan elérhető, hiteles információ,[52] azonban a legálisan birtokolt (regisztrált) kínai mobiltelefonokat kompenzáció nélkül elkobozták a kétezres évek elején, és saját eszközök fejlesztésébe (ezek számos beépített felügyeleti megoldást tartalmaznak) és államilag kontrollált elosztásába kezdtek, immár a társadalom szélesebb körében.[53] A 2020-as pandémiát megelőzően az állami híradások (KCNA News) rendszeresen számoltak be a hazai okostelefonok, SIM-kártyák kifejlesztésével és a phenjani publikus wifihálózat (a Mirae) területi lefedettségének kiterjesztésével kapcsolatos technológiai sikerekről.[54]

A globális internethez legálisan a társadalom szűkebb rétegei, például az ország főbb egyetemeinek informatikai karán tanuló hallgatók, egyes nagyvállalatok és kormányzati szervezetek munkatársai férhetnek hozzá kutatási vagy kereskedelmi céllal, a phenjani vezetés politikai és kulturális narratívájától eltérő információknak való kitettség miatt. A telekommunikációért felelős észak-koreai Postaszolgáltatási és Távközlési Minisztérium (Ministry of Post and Telecommunications, 체신성) felügyeli a hálózati kommunikációs csatornákat (így a globálisan is elérhető internetet) és hajtja végre a tartalomszűrést, vagyis a „nyílt" internet cenzúrázását.

A globális internetszolgáltatás elérhetősége területileg is korlátozott, hivatalosan (értsd: az állam által legálisan biztosítva) Phenjanból és a kereskedelmi és gazdasági érdekeltség miatt a különleges státuszú zónákból (például az ipari termelőközpont, Keszong vagy a kikötőváros, Raszon) hozzáférhető.[55] Észak-Korea világhálóhoz történő hozzáférését kezdetben kizárólag legnagyobb stratégiai partnere és szövetségese, a Kínai Népköztársaság garantálta a Star Joint Venture Co. nevű hálózat- és internetszolgáltatón keresztül. A vállalat mintegy 1024 IP-címet tartott fenn a 175.45.176.0 és 175.45.179.255 közötti tartományban az észak-koreai megrendelő részére, amelyeket többek közt az ország hivatalos hírportáljai (KCNA, Rodong Sinmun) is használnak.[56]

[52] A műholdas lehallgatást megakadályozó zavaró rendszer kiépítéséhez a KPTC egy 11,4 millió euró értékű elektronikai gyártó- és tesztberendezéseket tartalmazó listát adott át az Orascomnak, 6 db Rohde & Schwarz FSP40 spektrumanalizátor, valamint 3 db Rohde & Schwarz FSQ26 jelanalizátor beszerzését igényelhették. A következő években azonban több jelentés is említést tesz arról, hogy a német gyártmányú mobiltelefon-érzékelő berendezések segítségével az Állambiztonsági Minisztérium a határ menti területeken kínai mobiltelefonokat használó észak-koreaiakat fogott el. Bővebben Williams 2019.

[53] Kim 2014: 7–9.

[54] Williams 2023b.

[55] Williams 2014.

[56] Noland 2009: 62–74; Williams 2011.

Észak-Korea 2010-től a Korea Post and Telecommunications Co. (KPTC) vállalaton keresztül 256, szintén kínai IP-címet használhat a China Unicom (vagy United Network Communications Group) nemzetközi nagyvállalat szolgáltatása révén, amelyek a 210.52.109.0 és 210.52.109.255 hálózati azonosítók közé esnek.[57] A két szolgáltatótól való függés magas kitettséget eredményezett a hálózati hozzáférést megszakító, túlterhelő vagy ellehetetlenítő módszereknek, amire konkrét példát hozott 2014-ben a Sony Pictures-t ért észak-koreai támadásra reagáló amerikai válaszcsapás.[58] Az internetszolgáltatás diverzifikációját Észak-Korea 2017 októberére tudta megvalósítani, amikor Oroszországgal kötött megállapodást arról, hogy a TransTeleCom vállalat biztosít hozzáférést a világhálóhoz.[59] Az egyezség híre még jobban megterhelte a 2017-es interkontinentális ballisztikusrakéta-kísérletek (ICBM) miatt egyre súlyosbodó KNDK–USA viszonyt, ezért az amerikai fél kibertámadást indított a frissen felállított infrastruktúra ellen, ami ideiglenesen a hozzáférés teljes megszűnéséhez vezetett.[60]

Kiberképességek adaptációja az észak-koreai hadviselési kultúrába

Általánosságban elmondható, hogy az észak-koreai hadviselési kultúra ötvözi az irreguláris hadviselés sajátosságait és az aszimmetrikus képességeket, ez utóbbi egyik sarokköve a stratégiai elrettentést biztosító nukleáris triád kifejlesztésére való törekvés. Külföldre irányuló – főleg Japán és a Koreai Köztársaság (a továbbiakban Dél-Korea) elleni – műveleteit mélységi szinten hajtotta végre, amelyek jellemző formái a rajtaütések és a kommandós támadások voltak (például a dél-koreai elnöki palota, a Kék Ház elleni 1968-as rajtaütés), titkosszolgálati műveletek (köztük japán állampolgárok elrablása az 1970-es és 80-as évek fordulóján)[61] és orvtámadások, szabotőr akciók, valamint bombatámadások és merényletek.[62]

Az 1991-es Öbölháború, az 1999-es koszovói háború és a 2003-as iraki háború tapasztalatai rávilágítottak az információs fölény jelentőségére, és egyre sürgetőbbé tették a modernebb, hálózatba kapcsolt harceszközök által lehetővé váló, C4ISR-en alapuló vezetés-irányítás kialakítását, megváltoztatva a hadviselési feltételeket és kultúrát.[63]

A KNDK kibervédelmi stratégiájának megvalósítása szempontjából meghatározó, hogy Kim Dzsongil vezetése alatt 1996-ig végbementek a Koreai Néphadsereg (Korean People's Army, KPA) vezetés-irányítási struktúráját hálózatosító reformok, emellett (nagyjából 2002–2010 között) létrehoztak egy egyedül észak-koreai

[57] Jun–LaFoy–Sohn 2015: 53 és az APNIC adatbázisa alapján: https://wq.apnic.net/static/search.html
[58] Először fordult elő, hogy az USA nyilvánosan attribútálta egy államhoz az APT-tevékenységet, és nyíltan felvállalta a megtorló intézkedést. Az USA kiberművelete 2014. december 22–23. között 9 órán át tette elérhetetlenné Észak-Koreában a teljes internethálózatot, és szolgáltatáskiesést okozott az elektromos infrastruktúrában. Bővebben NATO CCDCOE [é. n.].
[59] Williams 2017.
[60] Wagstaff–Auchard–Kiselyova 2017; DeYoung–Nakashima–Rauhala 2017.
[61] Kato 2017.
[62] Csoma 2006: 25–31.
[63] Tóth 2022.

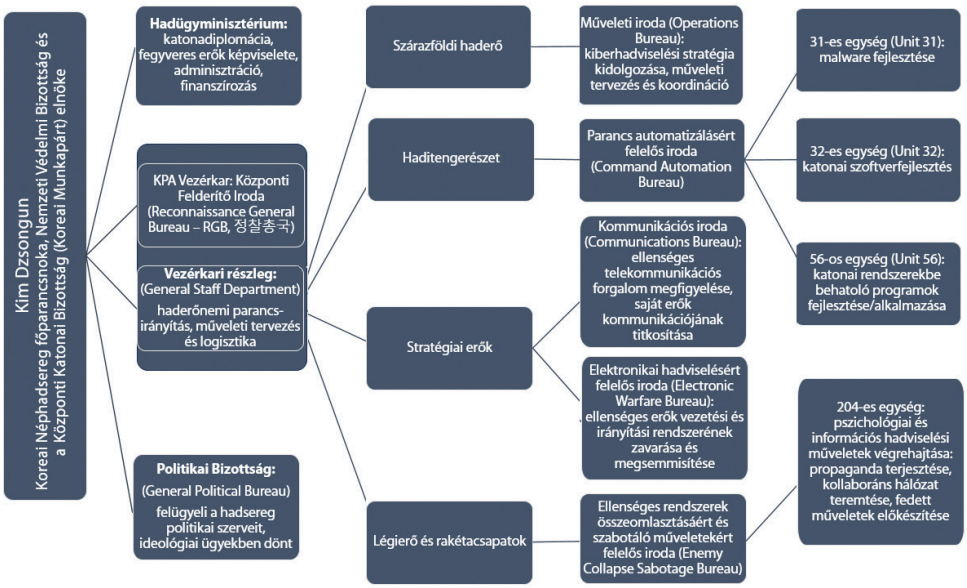
területről hozzáférhető internetstruktúrát, a Kvangmjongot (광명망, light network).[64] Az ország ezenkívül rendelkezik még három önálló kormányzati, katonai és nemzetbiztonsági intranethálózattal. A Bangpe (방패, „pajzsok", katonai célú), a Gumbjol (금별, „arany csillag") és a Bulgungom (붉은검, „vörös kardok") nevű hálózatok biztosíthatják a hadsereg irányítási láncának folytonosságát és más létfontosságú ellátórendszerek folyamatos üzemeltetését támadás esetén.[65] Ezzel párhuzamosan, Kim Dzsongil vezetése alatt, a phenjani védelempolitika felismerte, hogy az USA és szövetségesei hálózatosított haderejének aszimmetrikus erőfölénye mellett a folyamatosan fejlődő információs társadalmak sérülékenyek és kitettek a kibertérből érkező bomlasztó műveleteknek.

E gondolkodásmód kialakítására hatást gyakorolt a KNDK térségbeli szövetségese, a Kínai Népköztársaság. Kína a „korlátok nélküli hadviselés" elméleti keretrendszerének 1999-es publikálása nyomán emelte be saját hadviselési kultúrájába az információs társadalmak sérülékenységét.[66] Ezek alapján a phenjani rezsim logikus fejlődési utat járt be az információs műveletek alkalmazásával és vele együtt az elektronikai hadviselés és kibertámadó képességek beemelésével Észak-Korea érdekérvényesítő eszköztárába, amivel az ellenséges nemzetek belső politikai-társadalmi kohéziójának megbontására törekszik. Az észak-koreai katonai vezetési struktúrában a kiberműveleteket végrehajtó katonai egységek nagyrészt két csoportra oszlanak. Az egyik a Koreai Néphadsereg vezérkari részlege (Korean People's Army General Staff Department, KPA GSD), a másik a fentiekben is említett Központi Felderítő Iroda. A következőkben ezen szervezetek funkcióját mutatjuk be az észak-koreai haderőn belül.

Kim Dzsongil vezetése alatt, a 2000-es évek elején, a hadseregen belül kialakított elektronikai és informatikai képességek elsődleges funkciójaként a vezetés-tervezés-irányítás folyamatát biztosító rendszerek védelmét határozták meg (a KNDK-ban parancsautomatizáció biztosításának nevezték). Ezen védelmi fókuszú koncepció kibővítéséről a Koreai Néphadsereg publikálta 2005-ben Kim Dzsongil elektronikai hadviseléssel elérhető hatásokról tartott *(Electronic Warfare Referrence Guide)* közvetlen beszédét, amelyben a vezető kulcsfontosságú, művelettámogató és tartalék erőként jellemezte a kibertérben műveleteket végrehajtó egységeket. Kim ezáltal stratégiai szinten prioritásba helyezte a kiberképességek kiépítését. A haderőbe történő adaptáció strukturális alapjait a 2009–2010-es reformok teremtették meg, először haderőnemi kereteken belül.

Észak-Korea valószínűsíthető információs hadviselési stratégiai koncepcióját egy 2003-ban Dél-Koreába menekült disszidens – Kim Heungkvang, aki a Hamheung Egyetem informatikai karának professzora volt – segítségével tárták fel, a 2009–2010-es reformot követően megismert szervezeti struktúra alapján. A haderőnemekhez tartozó egységek információs és elektronikai műveletek tervezésére és végrehajtására voltak képesek, felépítésüket az 1. ábra szemlélteti.

[64] North Korean Internet: List of Internal Kwangmyong Websites. 2021. Bővebben: https://github.com/Alyzana/kwang-myong-addresses/blob/master/sites-en
[65] Jun–LaFoy–Sohn 2015.
[66] Bartók 2018.



1. ábra: Észak-Korea kiberhadviselési műveletekért felelős katonai struktúrájának ismert részlete

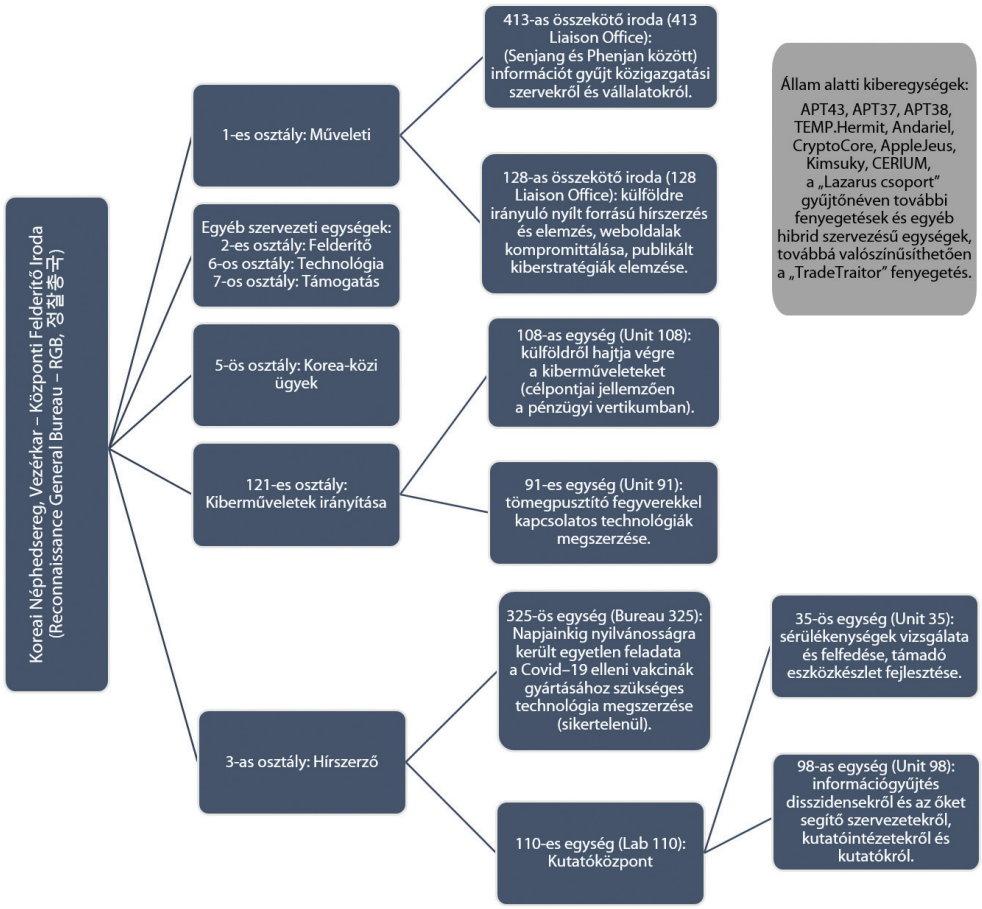
Forrás: a szerző szerkesztése a dél-koreai védelmi minisztérium 2018-ban kiadott védelmi fehér könyve[67] *és* Kong–Lim–Kim *2019 elemzése*[68] *alapján*

A haderőnemi szervezeten belüli kiber- és elektronikai műveleti egységek irányítását az összhaderőnemi erőkifejtés jegyében a vezérkar (General Staff Department, GSD) koordinálja. Tevékenységüket békeidőszakban (értsd: provokációs célú) a konvencionális műveletek támogatására korlátozták.

Ezt a feltételezést támasztja alá, hogy a Koreai Néphadsereg elektronikai műveleti egységei a 2010-es Jonphjong-szigetet érő bombázást megelőzően sikeresen zavarták egy dél-koreai AN/TPQ–37 radar működését.[69]

A Koreai Néphadsereg vezérkarának felderítő részlegén, az úgynevezett Központi Felderítő Irodán belül alakították ki a komplex(ebb) kiberműveleti képességet. Az RGB ismert szervezetrendszere, amelyet a 2. ábra mutat be, az önálló kiberműveletek megtervezését és végrehajtását támogatja, többek között belföldi és külföldi (összekötő irodák) telepítésű egységek révén, amelyeket az állam alatti kiberegységek tevékenysége egészít ki.

[67] ROK Ministry of National Defense 2018: 28.
[68] Kong–Lim–Kim 2019: 4.
[69] Jun–LaFoy–Sohn 2015: 37.



2. ábra: Az észak-koreai Központi Felderítő Iroda (RGB) szervezeti struktúrájának ismert részlete
Forrás: a szerző szerkesztése KONG–LIM–KIM *(2019)*[70] *és a CSIS tanulmányainak*[71] *információi alapján*

Az észak-koreai államigazgatási szervezetrendszeren belül az RGB jelentős autonómiát élvező szervként látja el feladatkörét, és közvetlen beszámolási kötelezettsége van Észak-Korea legmagasabb politikai döntéshozó szerve, a Koreai Munkapárt Politikai Bizottsága felé.[72] Szervezeti struktúráját tekintve a felderítő tevékenységi körök 6 főbb divízió (a 2. ábrán osztály) hatásköre alá vannak delegálva: műveleti, felderítő, hírszerző, Korea-közi ügyek, technológiai és támogató osztályok, amelyek tevékenysége főként

[70] KONG–LIM–KIM 2019: 4.
[71] JUN–LAFOY–SOHN 2015: 39–44.
[72] HA–MAXWELL 2018: 4.

japán, dél-koreai és amerikai műveletekre koncentrálódik.[73] Kim Heungkvang kiberbiztonsági területen dolgozó észak-koreai disszidens[74] beszámolója alapján ezen divíziókon kívül helyezkedik el a 121-es osztály műveleti területe. A megközelítőleg 500 fős egységet dél-koreai kutatásokban és védelmi dokumentumokban gyakran nevezik elektronikus felderítési vagy kiberhadviselés-irányító osztálynak (Bureau 121, Cyber Warfare Guidance Bureau vagy Electronic Reconaissance Bureau),[75] mert a kompetenciájába olyan műveletek tartoznak, mint a pénzügyi rendszerek elleni offenzív tevékenység; hírszerzési vagy technológiai (általában katonai fejlesztések) adatok kinyerése akár számítógépes rendszerekbe való behatolás által; sérülékenységek feltárása és támadóeszközök fejlesztése.[76]

Kim Dzsongun 2011-es hatalomra kerülése után közvetlenül a Koreai Munkapárt Belügyi Bizottsága (KKP State Affairs Commission) alá rendelték a kibertérben operáló egységeket (3. ábra). A testület Kim elnökletével működik, így az átszervezés jól mutatja az új vezető hatalom koncentrációját és bizalmasai körének törekvését a békeidőbeli információs műveletek feletti kizárólagos befolyás megszerzésére (a haderő legfelsőbb vezetői körével szemben).[77] Kim Dzsongun vezetése alatt 2012-re megduplázták az RGB és a GSD személyi állományát, így dél-koreai hírszerzési források szerint körülbelül 3000-ről megközelítőleg 6000 főre emelkedett a létszámuk, miközben a szervezetek feladatrendszerét és képességeit is bővítették, ezáltal nyilvánvalóvá vált, hogy az észak-koreai aszimmetrikus hadviselési keretrendszeren belül a kiberképességek önállóan is megjelentek műveleti szinten, nem csak harci támogató feladatkörben.[78] (Ezt igazolja az észak-koreai vezetőt lejárató film miatt 2014-ben politikai okokból indított, erődemonstrációs célú kibertámadás a Sony vállalat ellen.) A dél-koreai védelmi minisztérium kalkulációja alapján 2018-ra a kibertéri műveletek végrehajtására szakosodott állomány megközelítőleg 6800 fős lehetett.[79] Az állomány várható növekedésének kalkulációja kapcsán korlátozott információk állnak rendelkezésre. Az észak-koreai oktatásban már az alapszintű képzés alatt megkezdődik a matematika iránt fogékony hallgatók kiválasztása, akik középiskolai szakirányú tanulmányaikat már elkülönített, kiváltságosnak számító csoportokban folytatják, így későbbi tanulmányaik során informatikai képzést kaphatnak. A középiskolák legjobban teljesítő tanulói jelentkezhetnek a hazai felsőfokú informatikai képzésre: a Kim Irszen Egyetemre, a Mirim Egyetemre (katonai), a Kim Csaeng Egyetemre, a phenjani Pjongszung Tudományegyetemre és a Phenjani Informatikai Egyetemre. Ezen intézmények hallgatói kiválóságai az RGB vagy a GSD állományába kerülhetnek. Emellett a Kim Csaeng Egyetemen működik egy hallgatói képességeket fejlesztő

[73] Észak-Koreában az egyes közigazgatási szervek igazgatási egységeit számokkal jelölik, amelyek között megtalálhatók irodák vagy osztályok *(bureau)*, egységek *(unit)* és összekötő irodák *(liaison office)*, ezek általában külföldi kirendeltségű feladatellátó egységek és irányítóközpontok közötti kommunikációért felelnek.

[74] Kim Heungkvang az észak-koreai értelmiségek szolidaritási mozgalmának *(North Korean Intellectuals Solidarity)* alapítója, amely csoport kutatásaival és kampányaival Észak-Korea felszabadításáért és a disszidensek életkörülményeinek javításáért küzd. A csoport információit a dél-koreai Egyesítési Minisztérium és a védelmi szervek egyaránt használják a KNDK védelmi és offenzív képességeinek feltérképezésekor.

[75] Miller 2018.

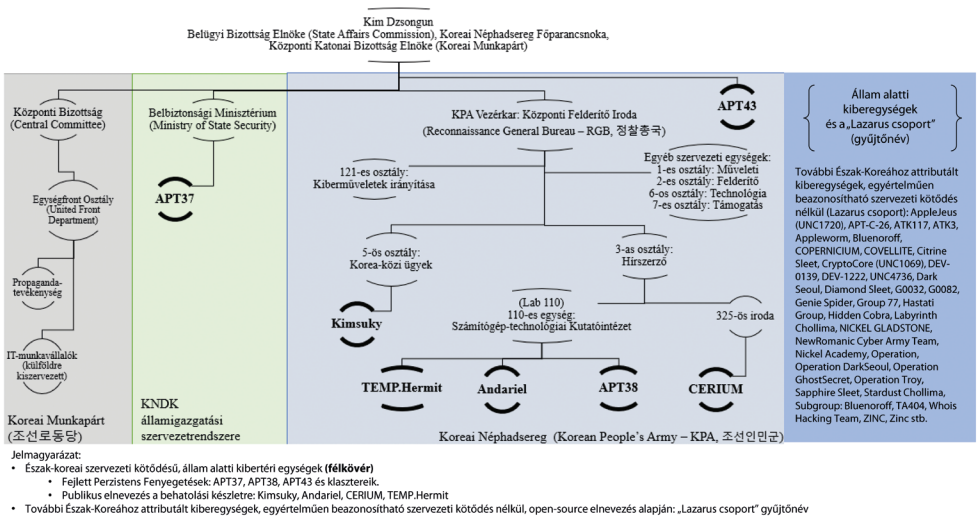
[76] Jun–LaFoy–Sohn 2015: 40–44.

[77] Kong–Lim–Kim 2019: 2–6.

[78] Gause 2015: 38.

[79] Kong–Lim–Kim 2019: 3.

központ, amelyet az észak-koreai programozói feladatokat, kutatásokat és képzéseket koordináló Koreai Számítástechnikai Központ (Korean Computer Center) tart fenn.[80] Az állomány képzése külföldön is zajlik, számottevő észak-koreai hallgatói közösség folytatja programozói és informatikai tanulmányait például India és Kína egyetemi képzésein, szoros nemzetbiztonsági felügyelet mellett.[81] Egy észak-koreai disszidens, aki korábban magas rangú tisztviselő volt, azt vallotta, hogy az ország évente 50–60 elit katonát küld külföldre, hogy informatikát tanuljanak, akik később akár offenzív területeken, kibertámadóként a Központi Felderítő Iroda vagy más irreguláris egységek személyi állományába kerülnek.[82]



3. ábra: A Koreai Népi Demokratikus Köztársaság állam alatti kiberegységeinek szervezeti kötődése

Forrás: a szerző szerkesztése a Mandiant 2023-as jelentése[83], Malpedia adatbázisa[84] és Kong–Lim–Kim 2019 elemzése[85] alapján

A phenjani rezsimhez köthető állam alatti kiberegységek (értsd: kiberbűnözői és egyéb hackercsoportok) ismert szervezeti beágyazottságát a 3. ábra mutatja be. Az Észak-Koreához köthető állam alatti fenyegető csoportok számontartása és elkülönítése nem egységes nemzetközi szinten. Az APT-k és klasztereik tevékenységét más-más kódnéven jegyzik az elemzőközpontok, továbbá a különféle fenyegető aktivitások elnevezése egy-egy kampányból ered (open-source módon például Kimsuky vagy DarkSeul), vagy csak összefoglaló jelleggel *Lazarus-csoport* néven vezeti a szakmai

[80] Jun–LaFoy–Sohn 2015: 52–53.
[81] Egy hallgatóhoz egy nemzetbiztonsági szervhez tartozó felügyelő van kirendelve.
[82] Han 2016.
[83] Barnhart et al. 2023.
[84] Malpedia 2024.
[85] Kong–Lim–Kim 2019: 4.

közösség a detektált eseteket nyilvántartásaiban.[86] Tovább nehezíti a tényleges észak-koreai „állami támogatású hackercsoportok" számának meghatározását, hogy az azonos eszközöket alkalmazó kampányokért más-más csoport vállal felelősséget nyilvánosan, így meglátásom szerint felmerül az a lehetőség, hogy azok létrehozása is eseti jellegű lehet, és a támadó személyek ugyanazok. Az egyes csoportok mögött a Központi Felderítő Iroda vagy a Koreai Néphadsereg egységeinek tagjai lehetnek, akiket *ad hoc* jelleggel válogatnak össze a különböző típusú, például kiberkémkedési kampányokra. A MITRE ATT&CK által önálló egységként jegyzett Lazarus (ID: G0032)[87] tevékenységéhez kötődnek az eddigi legjelentősebb károkat okozó támadások, feltehetőleg 2009 óta aktív az egység, azóta főleg a pénzügyi és magánszektort érintő célzott kibertámadások kötődtek hozzá. Ennélfogva tevékenységével az APT38 profilja is átfedésbe kerül, azonban jelentős, egyedül pusztító céllal indított, politikailag motivált kibertámadások is köthetők hozzá nyilvános attribúció alapján. Az APT38 és feltételezhetően a Lazarus csoport egyik ismert tagja Park Dzsinhjok, akit a Sony elleni támadásért és a WannaCry zsarolóvírus bevetéséért tett felelőssé az USA, ám nem fogták el, ezért igazságszolgáltatás elé egyelőre nem került, így az eset kiberdiplomáciai lépésként értékelhető. A Lazarus csoport további hírhedt kampánya a dél-koreai főváros villamosenergia-hálózatát érő DarkSeoul támadás és a 2011-es Ten Days of Rain nevű dél-koreai kormányzati weboldalakat és az Egyesült Államok Dél-Koreában állomásozó katonai egységének rendszerét érő túlterheléses támadássorozat (*distributed denial of service* – DDoS), amely kampány során a támadók által használt malware 10 napon keresztül elérhetetlenné tette a rendszert, majd törölve önmagát, használhatatlan állapotban hagyta a megfertőzött eszközt.[88] A Lazarusra (ID: G0032) jellemző programozási stílust, célpontkiválasztást és támadási módszereket (továbbiakban összefoglaló néven TTP, *tactics, technics and procedures*) több csoport is alkalmazta, ezért alcsoportjai, feladat-orientált műveletszervezési elvek mentén létrehozott *ad hoc* egységei vagy alternatív elnevezései is lehetnek (4. ábra).[89] A *Kimsuky csoport,*[90] amelyet először 2013-ban regisztráltak, elnevezését a célzott adathalász e-mailjeit küldő fiktív személyről, Kim Szukjangról kapta. A csoport dél-koreai kutatóintézetek és az Egyesítési Minisztérium ellen folytat kiberkémkedési tevékenységet trójai vírusok segítségével.[91] A Kimsuky által használt TTP szintén nagy hasonlóságot mutat a Korea Hydro & Nuclear Power vállalat elleni incidenssel, amely a dél-koreai atomenergia-szektort fenyegette.[92] Az APT37[93] és APT43 csoportok műveletei pedig

[86] Lásd a Malpedia adatbázisa: Malpedia 2024.
[87] MITRE ATT&CK 2023.
[88] McAffee 2011: 3.
[89] „A Lazarus Group további ismert azonosítói: Dark Seoul, Hidden Cobra, Hastati Group, Anderiel, Unit 121, Bureau 121, NewRomanic Cyber Army Team, Bluenoroff, Guardians of Peace. A csoport karakterisztikája összefüggést mutat további APT tevékenységekkel, mint pl. Group 77, Labyrinth Collima, Operation Troy, Operation GhostSecret, Operation AppleJeus, APT38, Stardust Chollima, Whois Hacking Team, Zinc, Appleworm, Nickel Academy, APTC-26, NICKEL GLADSTONE, COVELLITE." Berzsenyi 2023: 124.
[90] „A Kimsuky további ismert azonosítói: Velvet Chollima, Black Banshee, Thallium, Operation Stolen Pencil." Berzsenyi 2023: 124.
[91] Tarakanov 2013.
[92] Kong–Lim–Kim 2019: 8.
[93] Az APT37 további ismert azonosítói: Group 123, InkySquid, Operation Daybreak, Operation Erebus, Reaper Group, Reaper, Red Eyes, Ricochet Chollima, ScarCruft, Venus 121. (Berzsenyi 2023: 124).

feltehetően Észak-Korea ipari és katonai kémkedésre szakosodott offenzív tevékenységei.[94] Az Andariel (MITRE ID: G0138 és Mandiant: UNC614) elsősorban a dél-koreai kormányzati szervek, katonai szervezetek és amerikai vállalatok ellen intézett destruktív jellegű műveleteket. Az Andariel fenyegető csoport profiljába tartoznak még a pénzügyileg motivált műveletek, amelyeket kórházak (MAUI zsarolóvírus), ATM-ek, bankok és kriptovalutát forgalmazó vállalatok ellen is végrehajtott.[95]

Elméletek az észak-koreai kibertéri műveletek stratégiai koncepciójáról

Észak-Korea napjainkig nem publikált kiberképességei célrendszerére vonatkozó stratégiát. Ennek ellenére több olyan elméleti keretrendszert is megjelentettek, amelyeket a kutatók az észak-koreai kibertéri tevékenység önálló stratégiai célrendszerének leírására vagy éppen feltételezett kiberhadviselési doktrínájának feltárása érdekében alkottak meg biztonságpolitikai elemzési szempontok mentén. Az államhoz nyilvánosan attribútált kibertéri műveletek alapján három főbb stratégiai gondolkodási irány és műveleti szintű értelmezési keretrendszer különíthető el.

Az első elméleti keretrendszert Jun, LaFoy és Sohn (Center for Strategic & International Studies, CSIS kutatóközpont, 2015) dolgozta ki a KNDK hadviselési hagyományai és békeidőszakbeli provokációinak dinamikája mentén. Az elemzés kiindulópontja, hogy a Kim-rezsim évtizedek óta fegyverkísérletekkel, határkonfliktusokkal és terrorcselekményekkel igyekszik felhívni magára a nemzetközi közösség figyelmét és növelni a félsziget körüli katonai feszültséget. Ennek oka, hogy minél nagyobb a katonai eszkaláció kockázata, annál magasabb szintű diplomáciai fórumon próbálják meg rendezni a felek közti viszonyt. A rezsim által kikényszerített diplomáciai fórumon az észak-koreai fél általában gazdasági és politikai előnyöket követel az általa kiváltott feszültségek csökkentéséért cserébe.[96] Habár a kutatóintézet a későbbiekben sem mutatott ki általánosítható, közvetlen kapcsolatot a békeidőszaki provokációk politikai céljai és a kiberműveletek megindítása közt, megállapítható, hogy a phenjani vezetés érdekérvényesítő eszközként tekint a kiberképességekre, és alkalmazta azokat erődemonstrációs céllal.[97] A CSIS kutatói emiatt „háborús vagy magasabb intenzitású konfliktusos időszakra" és „békeidőbeli vagy alacsony intenzitású konfliktussal terhelt időszakra" osztották fel az Észak-Koreához köthető kibertérbeli műveleteket. A vizsgált időszakban a phenjani rezsim főként kiberhírszerzési (Kimsuky-kampányok) és bomlasztó hatást kiváltó kiberműveleteket hajtott végre az információs műveletek részeként, akár kritikusinfrastruktúra-szolgáltatók ellen is. Ez utóbbira példa a 2011-es Ten Days of Rain DDoS kampány, a 2013-as DarkSeoul művelet[98] és a 2014-es Operation KHNP (Korea Hydro and Nuclear Power), amely egy dél-koreai nukleáris erőmű műszaki leírásait

[94] Barnhart et al. 2023.
[95] MITRE ATT&CK 2022.
[96] Jun–LaFoy–Sohn 2015: 51.
[97] Cha–Lim 2024.
[98] 2013-ban a Dark Seoul elnevezésű észak-koreai csoport sikeresen kompromittálta és blokkolta három szöuli bank és három médiavállalat rendszereit. A támadók több napig zavart keltettek Dél-Korea pénzügyi szektorában, összesen több mint 800 millió dolláros kárt okozva. Bővebben Park–Park–James 2018.

és munkavállalóit érő adatszivárogtatás volt.[99] A tanulmány egyik konklúziója, hogy Észak-Korea (2009–2014 között) a békeidőszaki provokációk részeként eredményesen alkalmazta kiberképességeit, és ambícióként jelenik meg ezen számítógép-hálózati műveletek elektronikus és kiberhadviselésre alkalmas képességgé fejlesztése. Ám komoly kockázata van annak, hogy a szofisztikáltabb kiberműveletek hatásának téves felmérése miatt Phenjan átlépi a katonai *status quo*t. Emiatt a kutatók stratégiai szintű szakpolitikai lépéseket javasoltak az USA – Dél-Korea szövetség részére, amelyekkel korlátozhatják a KNDK haderejének irreguláris műveleti szabadságát a kibertérben, és növelhetik információs társadalmaik rezilienciáját.[100]

A második koncepciót megalkotó Ha és Maxwell (Foundation for Defense of Democracies, FDD, 2018) a gazdasági és politikai célokat egyaránt kiszolgáló incidenseket vizsgált meg és értékelte esetpéldaként a „*cyber enabled economic warfare*" (CEEW), vagyis „gazdasági hadviselés a kibertérben" elméleti koncepció keretrendszere mentén. Ez az elmélet a kibertéri műveletekkel elérhető illegális finanszírozás lehetőségének (például a megszerzett kriptovaluták hagyományos pénznemekké transzformálásával) és az információs társadalmak hosszú távú gazdasági kifárasztásának kombinálhatóságát emeli ki. Idesorolható a kriptovaluta- és számlapénzforgalomba beférkőző kiberbűnözői aktivitás, továbbá a FASTCash kampány, amely bankjegykiadó automatákat kompromittált Ázsia-szerte,[101] a bangladesi központi bank bankközi átutalásokat lebonyolító SWIFT rendszerének kompromittálása,[102] továbbá az APT38 tevékenységére visszavezetett WannaCry zsarolóvírusos kampány.[103] Biztonságpolitikai szempontból megközelítve a kiberműveletek célrendszerét, Észak-Koreának a rezsim fenntartásához és a katonai fejlesztések finanszírozásához szükséges támadások volumenét olyan mérték alatt kell tartania, hogy a szürkezónás tevékenysége ne hátráltassa a 2018-ban megindult politikai enyhülési folyamatot a további védelmi garanciák megadása és az ENSZ BT szankciós nyomásának enyhítése érdekében. Megjegyzendő, hogy az észak-koreai kibertéri tevékenység visszaszorítása érdekében már korábban is fellépett a nemzetközi közösség, habár csak korlátozott, diplomáciai eszközökkel. Az ENSZ BT 2006-tól tartja szankciós nyomás alatt a Központi Felderítő Irodát (RGB) és a vele együttműködő vállalkozásokat, mivel számos alkalommal kíséreltek meg tömegpusztító és csúcstechnológiás fegyverrendszerek technológiájára vonatkozó minősített adatot ellopni.[104] Ennek markáns esetpéldája a (Dél-Koreába is telepített THAAD rakétaelhárító rendszert fejlesztő) Lockheed Martin és alvállalkozóját érő

[99] 2014. december 15-től kezdődően a feltehetően észak-koreai patrióta hacktivisták „Who am I = No Nuclear Power" elnevezéssel kezdtek el a Korea Hydro & Nuclear Power (KHNP) alkalmazottairól információkat közzétenni az atomerőműre vonatkozó bizalmas műszaki dokumentumokkal együtt.

[100] Jun–LaFoy–Sohn 2015.

[101] A FASTCash kampány módszere, hogy távoli hozzáféréssel behatolnak a bankok pénzforgalmi Switch alkalmazásának szervereihez, és elősegítik a hamis tranzakciókat. Egy 2017-es incidens során a KNDK kiberegységei lehetővé tették, hogy több mint 30 különböző országban található ATM-ekből egyidejűleg készpénzt vegyenek fel. Egy másik, 2018-as incidens során 23 különböző országban lévő ATM-ből tudtak egyidejűleg készpénzt felvenni. Bővebben lásd US Cybersecurity and Infrastructure Security Agency 2020.

[102] A 2016. februári támadás során a támadók 951 millió dollárt akartak elrabolni, amelyből ténylegesen mintegy 81 millió dollárt sikerült átutalni az általuk megadott Fülöp-szigeteki számlaszámokra, ezzel hatalmas bevételhez juttatva a phenjani vezetést. Bővebben Hammer 2018; Rahman 2016.

[103] US Department of the Treasury 2020: 2.

[104] United Nations Security Council 2012.

sikertelen behatolási kísérlet, amelyet az USA Igazságügyi Minisztériuma a Lazarus észak-koreai APT-csoport tevékenységére attributált 2018-ban.[105] A másik konkrétabb példa, amely hathatott a kutatók elméletének kidolgozására, a 2018–2019-es évek bizalomépítő intézkedései. Kiinduló körülményként a Donald Trump elnöki ciklusa során felfokozott, ellenséges hangvételű kommunikáció tekinthető, amely mellett a 2017. szeptemberi intenzív interkontinentális rakétatesztek (ICBM) és a föld alatti nukleáris próbarobbantás olyan mértékűvé fokozták a katonai fenyegetést, hogy 2018-ra az észak-koreai fél ismételten tárgyalási pozícióba kerülhetett Dél-Koreával (2018. április, Mun–Kim-találkozó) és az amerikai legfelsőbb vezetéssel (2018. július, Szingapúr: Trump–Kim-találkozó). A 2018. áprilisi panmindzsoni nyilatkozatban a koreai felek többek között azt is vállalták, hogy a két állam kapcsolatának rendezéséig tartózkodnak a további provokatív akcióktól az összes műveleti térben, így a kibertéri műveletekben is.[106]Annak ellenére, hogy a két Korea viszonyrendszerének újbóli normalizálását célzó 2018. szeptemberi phenjani nyilatkozatban vállalt bizalomépítő kezdeményezések nem valósultak meg,[107] és az enyhülési folyamat 2019-re megrekedt, a diplomáciai párbeszéd és az addig nyert gazdasági előnyök (például a keszongi ipari park újranyitása) képesek voltak validálni a *de facto* állam[108] nemzetközi státuszát és megszilárdítani Kim belső hatalmát. Az amerikai és dél-koreai bilaterális csúcstalálkozók nyomán megvalósult a phenjani rezsim fennmaradását biztosító hosszú távú stratégiai célja: a békeidőszaki provokációkkal katonai patthelyzet kialakítása (a kínai geopolitikai érdekek védőernyője alatt) az USA és térségbeli szövetségeseinek erejével szemben, amit magas szintű diplomáciai kezdeményezések rendszere kezel.[109] Tanulmányában Ha és Maxwell megerősítette, hogy Észak-Korea az irreguláris kibertámadó képességeit a civil szféra és a pénzügyi kritikusinfrastruktúra-elemek ellen vetheti be, és amennyiben a rezsim politikai céljai nem valósulnak meg, az RGB tevékenységének növekedésére (anyagilag is motivált, de politikai és hírszerzési célú támadások) lehet számítani.[110]

2019–2020 fordulóján publikálták a harmadik koncepciót, amely a nemzetközi kutatási trendeket követve számításba vette a kibertér geopolitikai aspektusait. A NATO tallinni Kibervédelmi Kiválósági Központja (NATO CCDCOE) által közzétett elemzésben a kutatók (Kong Ji-Young, Jong In Lim, Kim Kyoung Gon) rávilágítottak arra, hogy Észak-Korea azért működik együtt más államokkal, mert ezzel nemcsak az attribúciót nehezíti, hanem egy összetett, további konfliktusokat generáló helyzet elé is állítja a megtámadott országot, amennyiben az megtorló válaszlépéseket kívánna tenni. A tanulmány a kibertér adta aszimmetriát felhasználó katonai stratégia végrehajtó szervezeteiként értelmezi a Központi Felderítő Iroda és a hadsereg vezérkara alatt elhelyezkedő kiberegységek (GSD) potenciális képességeit. Ebben a keretrendszerben a Központi Felderítő Iroda például kiberhírszerzési, befolyásoló vagy

[105] US Department of Justice 2018.
[106] Republic of Korea Ministry of Foreign Affairs 2018.
[107] Például a jongbjoni atomerőmű és a Tongchang-ri kísérleti rakétabázis bezárása. Bővebben Cheong 2018.
[108] A koreai háborút lezáró béke hiányában a nemzetközi jog alapján a KNDK-t számos ország nem ismeri el önálló államszervezetnek.
[109] Ha–Maxwell 2018: 1–2.
[110] Ha–Maxwell 2018.

zavarkeltő tevékenysége hozzájárul a katonai műveletek előkészítéséhez az információs és kibertérben. Az ismert szervezeti struktúra alapján az észak-koreai ambíciószint annak elérése lehet, hogy a GSD és az RGB kompetenciaterülete lehetővé tegye önálló offenzív kiberműveletek kivitelezését katonai vezetési rendszerek vagy kritikus információs infrastruktúra (*critical information infrastructure,* CII) elemei ellen. Ezzel párhuzamosan jelenik meg a haderőnemi kiberegységek meglepetésszerű vagy előzetes csapásmérő művelettámogató funkciója, amelyet a kutatók a *blitzkrieg* taktikához hasonlítottak.[111] A tanulmány az észak-koreai kiberhadviselési koncepció fő elemeként a minél nagyobb volumenű károkozási képesség megteremtését emelte ki – például sérülékenységek feltárása és malware-ek vagy kiberfegyverek fejlesztése által –, amit a nukleáris és rakétaprogramok mellett ugyancsak elrettentő képességként vagy megelőző csapásként alkalmazhatnak stratégiai kontextusban.[112]

Külföldről indított észak-koreai kibertámadások háttere

A bemutatott elméleteket egészíti ki a Recorded Future kiberbiztonsági vállalat 2020-ban publikált tanulmánya, amely az általuk elemzett esetpéldák technikai adatai alapján feltérképezte, hogy Észak-Korea mely államok területére visszavezethető lokációkról indított kibertámadást. Az Indiából és Kínából indított támadások esetében a támadók fizikailag is jelen voltak az országokban hivatalos tartózkodási engedéllyel rendelkező munkavállalóként és egyetemi képzésben részesülő hallgatóként vagy fedett személyként, míg a kutatócsoport által megnevezett további államok tekintetében távoli hozzáférésre utaló adatokat tártak fel. Az előbbi feltételezést erősítette meg egy disszidens is, aki korábban az észak-koreai hadseregben magas rendfokozatot töltött be, miszerint a KNDK éves szinten körülbelül 50–60 elit katonát vezényel külföldi egyetemekre informatikai képzésre, hogy tanulmányaik befejeztével a hírszerzéshez (RGB) vagy más kiberműveleteket végrehajtó egységekhez csatlakozzanak.[113] Ázsiában az érintett geolokációk Malajziára, Nepálra, Indonéziára, Thaiföldre és Banglades területére utaltak, míg Afrikában Kenya és Mozambik területe volt érintett. Új-Zéland esetében feltételezhető egy botnethálózat (magyarul zombigép- vagy zombihálózat) kialakítása, amely olyan végpontok (értsd: számítógépek és más okoseszközök) összessége, amelyek felett átvették az irányítást.[114] Napjainkra, a távmunkavégzés terjedésével párhuzamosan, ugyancsak megjelentek a magukat más nemzetiségűnek kiadó észak-koreai személyek az IT-ipar különböző szegmenseiben. Észak-Korea ezen személyeket Kínában és Oroszországban működő online munkaerő-közvetítő

[111] Kong–Lim–Kim 2019: 13.
[112] Kong–Lim–Kim 2019: 13–17.
[113] Kong–Lim–Kim 2019: 3.
[114] Recorded Future – Insikt Group 2020.

leányvállalatok segítségével juttatja munkához, bérezésük pedig hozzájárul a rezsim finanszírozásához.[115]

A Recorded Future és a korábban idézett, NATO CCDCOE által közzétett kutatói jelentések egyaránt mandzsúriai geolokációkat tártak fel az Észak-Koreához köthető APT-csoportok fő tevékenységi területeként, ahol a koreai–kínai etnikai kisebbség él. Ennek nemzetbiztonsági relevanciája, hogy megkönnyíti a koreai anyanyelvű, fedett műveletekben részt vevő személyek elhelyezését. Például a terület egyik központi városának számító Senjangból és környékéről már észleltek észak-koreai offenzív tevékenységet, emellett a geolokációs adatok alapján a Koreai-öböl mentén fekvő Dalian városának érintettsége is felmerült.[116] Dalianban található annak az észak-koreai cégnek a kirendeltsége (Chosun Expo Joint Venture), ahol a CIA által a Sony Pictures elleni és a WannaCry 2.0 zsarolóvírusos támadás egyik felelőseként megnevezett Park Dzsinhjok dolgozhatott szoftverfejlesztőként. Az amerikai hatóságok azzal vádolják Parkot, hogy az APT38 kódnevű csoport tagjaként kínai területről hajtott végre a phenjani rezsim céljait szolgáló kibertámadásokat, beleértve a 81 millió dolláros kárt okozó, bangladesi központi bankot kifosztó 2016-os incidenst.[117]

Az észak-koreai hírszerző és más nemzetbiztonsági műveletek kapcsán Japán territoriális érintettségét is feltárták. Ez valójában az ország területén élő, észak-koreai identitást valló koreai nemzetiség érdekvédelmi szervezetéhez (koreai nevén: Csongrjon) kötődik.[118] A szervezet radikális szárnya kapcsolatban áll a japán alvilági csoportokkal, továbbá támogatásához köthető a 80–90-es években elrabolt japán állampolgárok Észak-Koreába hurcolása.[119] A Csongrjon ezen radikális szárnya továbbra is hozzájárul Észak-Korea különböző illegális és titkosszolgálati aktivitásához. Például 2017-ben a japán Nemzeti Rendészeti Ügynökség arról számolt be, hogy a japán jakuzával és más nemzetközi bűnszervezetekkel kapcsolatban álló 260 személy segítette az észak-koreai támadókat abban, hogy 17 japán prefektúrában összesen 17 700 bankautomatát (ATM) kompromittálva, mintegy 16,6 millió dollárt lopjanak el.[120] Egy másik kirívó eset, amikor a japán rendőrség 2016-ban átkutatta a Csongrjon tokiói székházát (felbontva a szervezet *de facto* követségi immunitást élvező státuszát a sorozatos titkosszolgálati és pénzügyi botrányok következtében). A terhelő bizonyítékok alapján több észak-koreai személyt is letartóztattak, többek között a tokiói Korea Egyetem

[115] A Yanbian Silverstar Network Technology Co. Ltd. (ismertebb nevén China Silver Star vagy 延边银星网络科技有限公) egy csilini (Kína) székhelyű szoftverfejlesztő vállalat, amelyet az USA már 2018-ban szankcionált. A China Silver Star észak-koreai vezérigazgatója (Jong Szonghva (정성화) az oroszországi Vlagyivosztokban is létesített testvérvállalatot (Volasys Silver Star). Tehát mindkét vállalat észak-koreai irányítás alatt áll, és az amerikai kormányzat szerint IT-kiszervezési tevékenységet végeznek, amelyről jelentésében az FBI azt állítja, hogy „dollármilliókat" kerestek a phenjani rezsimnek. Bővebben lásd Williams 2023a.

[116] Kong–Lim–Kim 2019: 14.

[117] US Department of Justice 2018.

[118] Lee 2018.

[119] Kato 2017.

[120] Kyodo News 2020.

Gazdaságtudományi Karának volt dékánját, Pak Dzseiszót[121] (angol átírásban: Park Jae Isao) egy kiterjedt pénzügyi csalás ügyében. Azonban a Paknál tartott házkutatás után további terhelő bizonyítékok kerültek elő a lefoglalt számítógépéről, ez alapján feltárták, hogy Pak egy egész ügynöki és informátori hálózatot finanszírozott a Kínai Népköztársaságban és a Koreai Köztársaságban. Az ügynököket személyesen (Sanghajban) vagy elektronikus úton (titkosított vagy kódolt e-mailben és privát hálózaton keresztül) utasította, hogy manipulálják a 2007-es dél-koreai elnökválasztást, hatoljanak be a tömegmédiába. (Az elnökválasztást végül I Mjongbak nyerte meg [2008–2013], aki az észak-koreai kapcsolatok bővítését elutasító, konzervatív jobboldali Szabad Korea Párt tagja.) A számítógépen talált adatok alapján Pak arra is utasította ügynökeit, hogy a 2008-as dél-koreai általános parlamenti választásokon a Phenjan felé békülékeny politikát támogató erőket segítsék, és befolyásolják a közvéleményt az I Mjongbak elleni tüntetésen való részvételre, továbbá a „felbujtás" megszervezésében szintén közreműködhettek.[122]

Összegzés és konklúzió

A kutatás központi célkitűzése az volt, hogy az északkelet-ázsiai régió biztonságpolitikai környezetének kontextusában jellemezze az észak-koreai kibertéri műveletek stratégiai célrendszerét, és elősegítse további objektív következtetések levonását az államhoz köthető fejlett perzisztens fenyegetések tevékenységével kapcsolatban. Ennek érdekében a szerző két kutatási kérdés és két hipotézis vizsgálatát végezte el.

KK1: A nyilvánosan észak-koreai aktorok tevékenységére attribútált kibertéri műveletek stratégiai célrendszere hogyan illeszkedik az ország védelempolitikájába, és miként támogatja a phenjani rezsim nemzetközi érdekérvényesítő képességét?

Amennyiben abból indulunk ki, hogy a legtöbb államhoz hasonlóan Észak-Korea kibervédelmi stratégiai célja is alapvetően az, hogy csökkentse támadható felületét, az magyarázatot adhat sajátos, belföldi hálózati kialakítására és okoseszköz-felügyeleti törekvéseire, egyúttal megmagyarázza a külföldről indított műveleteinek szükségszerűségét. Összességében elmondható, hogy Észak-Korea internet- és hálózatfüggőségét stratégiai okokból szándékosan alacsonyan tartják, mert ez elméleti síkon csökkenti az ország és a társadalom technológiai függőségéből eredő kockázati szintjét és kitettségét a kibertámadások okozta károknak. Emellett a hálózati adatforgalom, a kommunikáció felügyelete és a cenzúrázás hozzájárul ahhoz, hogy az elérhető információ ne veszélyeztesse az elnyomó politikai rezsim stabilitását. Elméleti síkon ezt két alapvetés is megerősíti, amelyek hatottak a KNDK kiberképességekkel kapcsolatos hadviselési kultúrájára. Egyrészt a folyamatosan fejlődő információs társadalmak,

[121] Pak a tokiói rendőrség nyomozása, valamint a hivatkozott *Sankei* folyóirat tényfeltárása alapján nem csak a japánban élő, észak-koreai identitást valló koreaiak érdekvédelmi szervezetéhez, a Csongrjonhoz (japánul: Chosen Soren) kötődött. Az elérhető információk alapján a Csongrjonon keresztül kapcsolatban állhatott az észak-koreai hírszerző szolgálat egyik hírhedt szervével, amely harmadik országban ügynököket és illegális finanszírozási tevékenységet irányít, az úgynevezett 225-ös Irodával. Az Iroda műveleteinek felderítése során Pak tevőleges közreműködésére vonatkozó, terhelő bizonyítékok kerültek elő.

[122] *Sankei News* 2016.

a technológiai függőség mértékével megegyezően, sérülékenyek és kitettek a kibertérből érkező, például bomlasztó célú információs műveleteknek.[123] Ebből következik, hogy elrejthető és könnyen letagadható offenzív kiberműveletek révén csökkenthető az Egyesült Államok és térségbeli szövetségeseinek aszimmetrikus erőfölénye. Másrészt azon „szürkezónás", például (dez)információs, kiberhírszerzési vagy anyagilag motivált műveletek, amelyek a jelenleg publikus észak-koreai képességek révén elérhetők, ugyan alacsonyabb eszkalációs kockázattal járnak (ami jelenleg megfelel Észak-Korea érdekérvényesítési ambíciószintjének), ám nem használhatók fel hiteles kibertéri elrettentés eléréséhez. Az a műveleti képesség (amely például cselekvési vagy információs szempontok mentén megvalósuló stratégiai autonómia[124] elérését is jelenti a kibertérben) jelentős politikai és katonai eszkalációs kockázatot von maga után (például kiberfegyver bevetése).[125] Azonban egy hálózatosított, modern haderővel szemben hiteles elrettentést jelenthet, így Észak-Koreának érdekében áll ezen képességi szint elérése.

1. táblázat: A KNDK (állami és állam alatti) kiberegységei, amelyek kiberstratégiai funkciókat látnak el

Észak-Korea kiberstratégiai céljait végrehajtó egységek			
KPA Vezérkar (General Staff Department – GSD) • Haderőnemek • Elektronikai hadviselés	**Központi Felderítő Iroda (RGB)** • 121-es Iroda (Bureau 121) • Egységek és összekötő irodák (413, 128, 108, 110, 91, 35, 98)	**Fejlett Perzisztens Fenyegetések (APT)** • APT37, APT38, APT43 és klasztereik • További állam alatti kiberegységek	**IT-szakemberek** (távmunka) • Felderítő és anyagi haszonszerzési funkció

Forrás: a szerző szerkesztése

A védelempolitikájának gyakorlati átültetése során a phenjani vezetés megfordíthatta ezt a gondolatmenetet annak érdekében, hogy felkészíthesse digitális ökoszisztémáját az USA igazolt katonai (és állam alatti) kiberképességeivel szemben. A rezsim erőforrásainak szűkössége mellett védelempolitikai megfontolásból tudatosan alacsonyan tartja a saját területén elérhető hálózati megoldások lefedettségét, és társadalmi funkció szerint szegmentálja azokat: lakossági, katonai és belbiztonsági célok mentén. A belföldi és nemzetközi felhasználók közti információáramlás ellenőrzésére alkalmazott számos módszer egyike a Koryolink belföldi celluláris hálózatán kialakított tartalom- és forgalomszűrési megoldás. A hálózati kapacitások (fizikai infrastruktúra és adatforgalom) korlátozottsága az elavult (vagy alacsonyabb minőségű, saját fejlesztésű) belföldi technológiai megoldásokkal együttesen infrastrukturális szempontból

[123] Haig 2022.

[124] „A stratégiai autonómia […] alapvetően három fajtáját különböztethetjük meg […]: döntéshozatali autonómia, cselekvési autonómia és információs autonómia. Az első a politikai akaratra és a döntéshozatali folyamatra helyezi a hangsúlyt, a második a katonai és civil képességek és a műveleti készenlét fejlesztésére, a harmadik pedig a hírszerzésre, elemzésekre és adatgyűjtésekre." Bővebben lásd Szabolcs 2020: 28.

[125] Például nulladik napi *(zero-day)* sérülékenység felhasználásával vagy a teljes ún. *cyber-kill-chain* folyamaton (Lockheed Martin által kidolgozott koncepció) végbemenő számítógép-hálózati behatolással megvalósított kiberművelet.

korlátozzák Észak-Korea kibertéri egységeinek (1. táblázat) műveleti lehetőségeit, defenzív és offenzív oldalon egyaránt. Emiatt az offenzív kiberműveleteket végrehajtó egységek külföldre telepítésével a phenjani vezetés egy hatékonyabb erőforrás-allokációt valósít meg. Ennek további hasznos vetülete, hogy egyúttal ugyanezen célországban megvalósíthatja a személyi állomány képzését és/vagy munkaerőpiacra történő belépését (amivel ugyancsak további anyagi erőforrások előteremtése is lehetséges a rezsim számára). Mindezzel párhuzamosan védelempolitikai oldalon a korlátozott infrastruktúra fenntartására (és fejlesztésére) fordított erőforrás-felhasználás összességében csökkenti Észak-Korea technológiai függőségéből eredő kockázati szintjét a regionális szomszédjai társadalmához képest.

A kutatás első hipotézisét – miszerint (H1) „a békeidőszaki kiberműveletek kettős védelempolitikai célja, hogy egyrészt finanszírozza a haderőfejlesztést, másrészt a stratégiai céllal alkalmazott katonai provokációkat kiegészítve gazdasági és politikai engedményeket kényszerítsen ki a nemzetközi közösségből" – a szakirodalom összehasonlító elemzése igazolta. Összességében a KNDK aszimmetrikus nemzetközi viszonyrendszerében a kiberműveleti képességek kialakítása és fejlesztése költséghatékonyabb a konvencionális haderő eszközparkjának fenntartási és modernizációs költségeihez képest. Ezenfelül a kinetikus műveletekhez és fegyverkísérletekhez képest az offenzív kibertéri tevékenység kevésbé hordozza magában a válaszcsapás megindításának és a konfliktus eszkalációjának kockázatát, míg az általuk kiváltható hatás ugyanúgy kiterjedhet a fizikai térre. Az észak-koreai kiberegységek és az állam által támogatott irreguláris csoportok (APT) tevékenysége könnyebben elrejthető és letagadható a kinetikus műveletekhez képest, mindemellett adaptív alkalmazkodóképességük hosszú távú, célzott és fedett tevékenységet tesz lehetővé az ellenséges rendszerekben, ezáltal hatékonyan megvalósítva többek között a hírszerzési és felderítő vagy egyéb (például: anyagi) erőforrások kinyerésére irányuló célokat.[126] A Ha és Maxwell (2018) által leírt mechanizmus lényege, hogy a rezsim hosszabb távon igyekszik békeidőszaki provokatív akcióinak (például rakétakísérletek) eszközrendszerét kibővíteni olyan kibertéri műveletekkel, amelyekkel finanszírozni tudják a rezsim és hadereje fenntartását, és egyúttal növelhetik az információs társadalmak gazdasági alrendszereinek fenyegetettségét, gyengítve az államok gazdasági erejét adó kritikus pontokat. Ezzel arra kényszerítik ellenfeleiket, hogy a konfliktus eszkalációjának elkerülése érdekében gazdasági és politikai engedményeket tegyenek a rezsimnek, ami egy jellemző észak-koreai tárgyalási technika. Ha és Maxwell előrevetítette, hogy amennyiben Észak-Korea beleegyezik a nukleáris és fegyverprogramjainak korlátozásába, akkor a gazdaságilag motivált kibertámadások (elméletükben úgynevezett kibertér által lehetővé tett gazdasági hadviselés) valószínűleg még nagyobb részét fogják képezni a békeidőszaki provokációs stratégiának az esetek számától függetlenül. A 2024-es év a phenjani nemzetközi érdekérvényesítési gyakorlat eszkalációs (konfliktust fokozó) időszakába fog tartozni az áprilisban esedékes dél-koreai és a novemberi amerikai elnökválasztás miatt, mivel ezek új alkupozíció kialakítását teszik lehetővé. Ezzel összefüggésben Észak-Korea a korábbi évekhez képest több provokatív, köztük kiberműveleti akciót fog véghez vinni ezekben a hónapokban, vagy a dél-koreai – amerikai

[126] Jun–LaFoy–Sohn 2015: 19–25; Berzsenyi 2023.

bilaterális integrált védelmi párbeszéd tervezett kibervédelmi gyakorlatára reagáló válaszlépésként időzítve.

A második kutatási kérdés (KK2) arra kereste a választ, hogy milyen hatást gyakorol az északkelet-ázsiai régió biztonságpolitikai helyzetére a Kínai Népköztársaság és a Koreai Népi Demokratikus Köztársaság feltételezhető együttműködése az offenzív kibertéri műveletek kivitelezésében. Ennek kapcsán a kutatás alátámasztotta, hogy (H2) a pekingi vezetés észak-koreai felsőoktatást és munkavállalást támogató politikája, az infrastruktúra-szolgáltatás nyújtásával kiegészülve, olyan geopolitikai helyzetet teremt, amelyben az Észak-Korea által indított műveletek egyúttal alkalmasak Kína nemzetközi erőkivetítési stratégiájának és kibertérben megvalósítható céljainak kiszolgálására a kelet-ázsiai régióban az Egyesült Államok és szövetségesei ellen. Az ebből következő kockázati tényezők:

- Mobilitás. Kína különösen ideális környezetet nyújthat fedett kibertámadó tevékenység vagy hírszerző műveletek kivitelezéséhez az ott élő kínai–koreai közösség (például nyelvhasználat, munkalehetőség) jelenléte miatt.
- Kompetenciák átadása. A Kínában képzett új szakemberek létszáma és a külföldi munkavégzés révén szerzett tudástranszfer jelenti az észak-koreai kibertámadó képességek fejlődésének egyik indikátorát. A Koreai Néphadsereg vagy az RGB kibererőinek lehetséges növekedését előrejelző kalkulációk tovább árnyalhatók, amennyiben az észak-koreai felsőoktatási intézményekben képzett szakemberek mellett a külföldi hallgatók és munkavállalók létszámát és mobilitását megfigyeljük. E tekintetben a potenciális fogadó államokat (a felsorolást lásd a Recorded Future idézett kutatásában) kiberdiplomáciai csatornákon keresztül érdekeltté kell tenni úgy, hogy az adatszolgáltatást például védelmi célú felkészülésként vagy a kiberbűnözés csökkentésére tett erőfeszítésként tematizáljuk, elkerülve a NATO és globális partneri közösségének érdekeivel való további szembehelyezkedést.
- A nemzetközi jog korlátai. Harmadik ország infrastruktúrája ellen nem lehet retorzió kockázata nélkül támadást indítani.

Ezek mentén megállapítható, hogy a Központi Felderítő Iroda (RGB) kiberegységeihez köthető fejlett perzisztens fenyegetések a szürkezónában operálva, saját céljaik megvalósítása mellett, alkalmasak Kína térségbeli kiberhatalmi céljait kiszolgáló erőfeszítéseinek támogatására, mert a kínai területről megindított műveletek nyilvános attribúciója magas politikai kockázattal jár.[127] Ezzel alátámasztható az Egyesült Államok (kiberhatalmi státuszával összefüggő) érdekérvényesítő képessége térségbeli szövetségesei előtt, és egyúttal csökkentheti a szövetségesi kohéziót.

[127] F. Yang 2022.

Felhasznált irodalom

Barnhart, Michael et al. (2023): Assessed Cyber Structure and Alignments of North Korea in 2023. *Mandiant,* 2023. október 10. Online: www.mandiant.com/resources/blog/north-korea-cyber-structure-alignment-2023

Bartók András (2018): „Korlátok nélküli hadviselés" (超限战) – Egy kínai nézőpont a 21. század hatalmi versengéséről. *Hadtudományi Szemle,* 11(3), 338–346. Online: https://folyoirat.ludovika.hu/index.php/hsz/article/view/3995/3261

Bartók András (2020): Sárkányok és kistigrisek: Kelet-Ázsia regionális fegyverkezési versenyének általános és országspecifikus jellemzői a Kínával kapcsolatos fenyegetettségpercepciójú országok esetében 1. *Nemzet és Biztonság,* 13(4), 80–101. Online: https://doi.org/10.32576/nb.2020.4.6

Bartók András (2022): Sokan tartanak Kína tajvani inváziójától, megnéztük a forgatókönyveket. *Telex,* 2022. augusztus 25. Online: https://telex.hu/velemeny/2022/08/25/tajvan-kina-aggodalmak-szembenallo-erok-invazio-forgatokonyvek-usa-japan-tamogatas

Bartók András – Wagner Péter (2021): A kínai A2/AD és a válaszreakciók Kelet-Ázsiában (2.). *KKI Elemzések,* 2021/7, 3–18. Online: https://doi.org/10.47683/KKIElemzesek.E-2021.07

Berzsenyi Dániel (2023): *Különleges kiberműveletek. A kiber különleges műveleti képesség és kialakításának vizsgálata.* PhD-disszertáció. Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola. Online: https://doi.org/10.17625/NKE.2023.012

Cha, Victor – Lim, Andy (2024): Slow Boil: What to Expect from the DPRK in 2024. *CSIS,* 2024. január 16. Online: www.csis.org/analysis/slow-boil-what-expect-dprk-2024

Chainalysis Team (2023): 2022 Biggest Year Ever For Crypto Hacking with $3.8 Billion Stolen, Primarily from DeFi Protocols and by North Korea-linked Attackers. *Chainalysis,* 2023. február 1. Online: www.chainalysis.com/blog/2022-biggest-year-ever-for-crypto-hacking/

Cheong, Wa Dae (2018): *Pyongyang Joint Declaration of September 2018.* Online: www.mofa.go.kr/eng/brd/m_5476/view.do?seq=319608&srchFr=&srchTo=&srchWord

Csoma Mózes (2006): *A koreai félsziget politikai viszonyai és azok biztonságpolitikai aspektusai.* PhD-disszertáció. Zrínyi Miklós Nemzetvédelmi Egyetem Hadtudományi Doktori Iskola. Online: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/12047/ertekezes.pdf;jsessionid=D2CBB0501C9C3852B9F788A081906D14?sequence=1

DeYoung, Karen – Nakashima, Ellen – Rauhala, Emily (2017): Trump Signed Presidential Directive Ordering Actions to Pressure North Korea. *The Washington Post,* 2017. szeptember 30. Online: www.washingtonpost.com/world/national-security/trump-signed-presidential-directive

F. Yang, Fan (2022): The Problem with Ill-Substantiated Public Cyber Attribution: A Legal Perspective. In Levite, Ariel E. et al. (2023): *Managing U.S.-China Tensions Over Public Cyber Attribution*. Washington, D.C.: Carnegie Endowment for Inter-

national Peace. Online: https://carnegieendowment.org/files/Perkovich_et_al_Cyber_Attribution_web.pdf
Gause, Ken E. (2015): *North Korea's Provocation and Escalation Calculus: Dealing with the Kim Jong-un Regime.* Washington: CNA Analysis & Solutions. Online: https://apps.dtic.mil/sti/tr/pdf/ADA621100.pdf
Geigenberger, Laura (2023): Russian Ambassador to Pyongyang Provides Insights into Current Trade with North Korea and the Status of its Weapons Development. *Daily NK,* 2023. május 30. Online: www.dailynk.com/english/russian-ambassador-to-pyongyang-provides-insights-into-current-trade-with-north-korea-and-the-status-of-its-weapons-development/
Ha, Matthew (2022): The Evolution of Kim Jong Un's 'All-Purpose Sword'. *FDD,* 2022. október 28. Online: www.fdd.org/analysis/2022/10/28/the-evolution-of-kim-jong-uns-all-purpose-sword/
Ha, Mathew – Maxwell, David (2018): *Kim Jong Un's 'All-Purpose Sword'. North Korean Cyber-Enabled Economic Warfare.* Washington, DC: FDD Press.
Haig Zsolt (2022): Kibertéri kognitív befolyásolás az információs műveletekben. *Hadtudományi Szemle,* 15(2), 115–130. Online: https://doi.org/10.32563/hsz.2022.2.7
Hammer, Joshua (2018): The Billion-Dollar Bank Job. *The New York Times,* 2018. május 3. Online: www.nytimes.com/interactive/2018/05/03/magazine/money-issue-bangladesh-billion-dollar-bank-heist.html
Han, Sangmi (2016): North Korea sends 50 to 60 Talented Students to Study Abroad to Train as Cyber Agents. *Voice of America,* 2016. június 14. Online: www.voakorea.com/a/3375411.html
Johnson, Jeff et al. (2023): 3CX Software Supply Chain Compromise Initiated by a Prior Software Supply Chain Compromise; Suspected North Korean Actor Responsible. *Mandiant,* 2023. április 20. Online: www.mandiant.com/resources/blog/3cx-software-supply-chain-compromise
Jun, Jenny – LaFoy, Scott – Sohn, Ethan (2015): *North Korea's Cyber Operations. Strategy and Responses.* Lanham: Rowman & Littlefield. Online: https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/151216_Cha_NorthKoreasCyberOperations_Web.pdf
Kato, Katsunobu (2017): *Abductions of Japanese Citizens by North Korea.* Tokyo: Secretariat of the Headquarters for the Abduction Issue. Online: www.mofa.go.jp/files/000433596.pdf
Kertész Bence (2023): A lopakodó tigris: Észak-Korea rakétafejlesztésének titkos rekordéve. *Biztonságpolitika.hu,* 2023. február 11. Online: https://biztonsagpolitika.hu/kiemelt/a-lopakodo-tigris-eszak-korea-raketafejlesztesenek-titkos-rekordeve
Kong, Ji-Young – Lim, Jong In – Kim, Kyoung Gon (2019): The All-Purpose Sword: North Korea's Cyber Operations and Strategies. *11th International Conference on Cyber Conflict (CyCon),* 1–20. Online: https://doi.org/10.23919/CYCON.2019.8756954
Kovács László (2021): Offenzív kiberműveletek II.: Kibererők és képességeik. *Hadmérnök,* 16(3), 119–137. Online: https://doi.org/10.32567/hm.2021.3.7
Kim, Yonho (2014): *Cell Phones in North Korea. Has North Korea Entered the Telecommunications Revolution?* Washington: US–Korea Institute at SAIS – Voice

of America. Online: https://38north.org/wp-content/uploads/2014/03/Kim-Yonho-Cell-Phones-in-North-Korea.pdf
Krasznay Csaba (2020): Kiberbiztonsági K+F+I Európában. In Török Bernát (szerk.): *Információ- és kiberbiztonság.* Budapest: Ludovika, 83–97. Online: https://tudasportal.uni-nke.hu/xmlui/static/pdfjs/web/viewer.html?file=https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/16195/TKP_Kiberbiztonsag_01_25.pdf?sequence=1&isAllowed=y#page=84
Krasznay Csaba (2022): Adatok és automatizáció a kiberbiztonság szemszögéből. *Századvég,* 2022/1, 29–46. Online: https://szazadvegfolyoirat.hu/wp-content/uploads/2023/09/Szazadveg_2022_01_teljes.pdf
Kyodo News (2020): Suspected Ringleader of Huge, Coordinated ATM Scam Entered N. Korea. *Kyodo News (South Korea),* 2020. április 5. Online: https://english.kyodonews.net/news/2020/04/2b45db5e313b-suspected-ringleader-of-huge-coordinated-atm-scam-entered-n-korea.html
Lee, Yaecan (2018): Japan's North Korean Diaspora. *The Diplomat,* 2018. január 5. Online: https://thediplomat.com/2018/01/japans-north-korean-diaspora/
Malpedia (2024): *Lazarus Group.* Online: https://malpedia.caad.fkie.fraunhofer.de/actor/lazarus_group
McAffee (2011): *Ten Days of Rain. Expert Analysis of Distributed Denial-of-Service Attacks Targeting South Korea.* Online: www.mcafee.com/blogs/wp-content/uploads/2011/07/McAfee-Labs-10-Days-of-Rain-July-2011.pdf
McLeary, Paul – Hudson, Lee (2022): Better Call Seoul: U.S. Watches Nervously as Europe Turns to South Korea for Weapons. *Politico,* 2022. november 1. Online: www.politico.com/news/2022/11/01/europe-south-korea-weapons-00064427
Miller, Steve (2018): Where Did North Korea's Cyber Army Come From? *VOA News,* 2018. november 20. Online: www.voanews.com/a/north-korea-cyber-army/4666459.html
Missile Defense Project (2023): North Korean Missile Launches & Nuclear Tests: 1984–Present. *Missile Threat,* 2023. április 25. Online: https://missilethreat.csis.org/north-korea-missile-launches-1984-present/
MITRE ATT&CK (2022): *Andariel.* Online: https://attack.mitre.org/groups/G0138/
MITRE ATT&CK (2023): *Lazarus Group.* Online: https://attack.mitre.org/versions/v7/groups/G0032/
Montlake, Simon (2012). Pyongyang Calling For Egyptian Telecoms Tycoon Naguib Sawiris. *Forbes,* 2012. november 19. Online: www.forbes.com/sites/simonmontlake/2012/11/18/pyongyang-calling-for-egyptian-telecoms-tycoon-naguib-sawiris/
NATO CCDCOE [é. n.]: *Sony Pictures Entertainment attack (2014).* Online: https://cyberlaw.ccdcoe.org/wiki/Sony_Pictures_Entertainment_attack_(2014) Letöltés ideje: 2020. 07. 07.
Noland, Marcus (2009) Telecommunications in North Korea: Has Orascom Made the Connection? *North Korean Review,* 5(1), 62–74. Online: www.jstor.org/stable/43910262.
Park, Kyoung Jae – Park, Sung Mi – James, Joshua I. (2017): A Case Study of the 2016 Korean Cyber Command Compromise. *European Conference on Information Warfare and Security,* 315–321. Online: https://arxiv.org/pdf/1711.04500

RAHMAN, Mizanur (2016): *A Forensic View of Bangladesh Bank Reserve Heist.* University of Dhaka. Online: https://doi.org/10.13140/RG.2.2.35280.51200

RAMANI, Samuel (2023): North Korea's Covert Alliance With Iran Aligned Militias in the Middle East. *38north,* 2023. október 23. Online: www.38north.org/2023/10/north-koreas-covert-alliance-with-iran-aligned-militias-in-the-middle-east/

Recorded Future – Insikt Group (2020): *How North Korea Revolutionized the Internet as a Tool for Rogue Regimes.* Online: www.recordedfuture.com/blog/north-korea-internet-tool

Republic of Korea Ministry of Foreign Affairs (2018): *Panmunjom Declaration for Peace, Prosperity and Unification of the Korean Peninsula.* 2018. április 27. Online: www.mofa.go.kr/eng/brd/m_5478/view.do?seq=319130&srchFr=&srchTo=&srchWord=&srchTp=&multi_itm_seq=0&itm_seq_1=0&itm_seq_2=0&company_cd=&company_nm=&page=1&titleNm=

ROK Ministry of National Defense (2018): *Defence White Paper: Changes and Challenges in the Security Environment – North Korea's Military Command Structure.* 28. 2018. december 31. Online: www.mnd.go.kr/user/mndEN/upload/pblictn/PBLICTNEBOOK_201908070153390840.pdf

Sankei News (2016): 朝鮮大学校元幹部逮捕「スパイ天国・日本」狙い撃ち 北朝鮮の指示役、韓国大統領選でも暗躍 (A Korea Egyetem előző intézményvezetőjének letartóztatása, „Kémek Paradicsoma, Japán" – Az észak-koreai ügynökök a dél-koreai elnökválasztással kapcsolatban is tevékenykedtek). *Sankei News.* 2016. Online: www.sankei.com/affairs/news/160202/afr1602020050-n1.html

SHIM, Elizabeth (2021): Report: North Korea's Trade with China Declined 80% in 2020. *UPI,* 2021. február 22. Online: www.upi.com/Top_News/World-News/2021/02/22/Report-North-Koreas-trade-with-China-declined-80-in-2020/2431614020515/

Symantec Threat Hunter Team (2023). X_Trader Supply Chain Attack Affects. Critical Infrastructure Organizations in U.S. and Europe. *Symantech Enterprise Blogs,* 2023. április 21. Online: https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/xtrader-3cx-supply-chain

SZABOLCS Laura (2020): Európai stratégiai autonómia – A közös védelem alapjai és korlátjai. *Nemzet és Biztonság,* 13(3), 15–35. Online: https://doi.org/10.32576/nb.2020.3.3

Taiwan National Computer Emergency Response Team (2022): *Annual Report 2021.* Online: www.twncert.org.tw/Download/TWNCERT%20Annual%20Report%202021.pdf

TARAKANOV, Dmitry (2013): The „Kimsuky" Operation: A North Korean APT? *Securelist,* 2013. szeptember 11. Online: https://securelist.com/the-kimsuky-operation-a-north-korean-apt/57915/

TÓTH András (2022): A Katonai Egységes Felhőalapú Eszközrendszer fogalmi rendszerének meghatározása. *Hadtudomány,* 32(4), 112–125. Online: https://doi.org/10.17047/Hadtud.2022.32.4.112

United Nations Security Council (2012): *Security Council Committee Determines Entities, Goods Subject to Measures Imposed on Democratic People's Republic of Korea by Resolution 1718 (2006).* New York, 2012. május 2. Online: www.un.org/press/en/2012/sc10633.doc.html

US Cybersecurity and Infrastructure Security Agency (2020): *Guidance on the North Korean Cyber Threat*. Online: www.cisa.gov/news-events/cybersecurity-advisories/aa20-106a
US Cybersecurity and Infrastructure Security Agency (2021): *AppleJeus: Analysis of North Korea's Cryptocurrency Malware.* Online: www.cisa.gov/news-events/cybersecurity-advisories/aa21-048a
US Cybersecurity and Infrastructure Security Agency. (2022): *North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector.* 2022. július 7. Online: www.cisa.gov/news-events/cybersecurity-advisories/aa22-187a
US Department of Defense (2023): *Joint Press Statement for the 22nd Korea-U.S. Integrated Defense Dialogue.* 2023. április 12. Online: www.defense.gov/News/Releases/Release/Article/3360919/joint-press-statement-for-the-22nd-korea-us-integrated-defense-dialogue/ Hozzáférés: 2023. 05. 31.
US Department of Justice (2018): *North Korean Regime-Backed Programmer Charged With Conspiracy to Conduct Multiple Cyber Attacks and Intrusions.* 2018. szeptember 6. Online: www.justice.gov/opa/pr/north-korean-regime-backed-programmer-charged-conspiracy-conduct-multiple-cyber-attacks-and
US Department of the Treasury (2020): *Guidance on the North Korean Cyber Threat.* Online: https://ofac.treasury.gov/sanctions-programs-and-country-information/north-korea-sanctions
US Department of Treasury (2022): *Guidance on the Democratic People's Republic of Korea information technology workers.* 2022. május 16. Online: https://ofac.treasury.gov/media/923131/download?inline
Wagstaff, Jeremy – Auchard, Eric – Kiselyova, Maria (2017): Russian Firm Provides New Internet Connection to North Korea. *Reuters,* 2017. október 2. Online: www.reuters.com/article/us-nkorea-internet-idINKCN1C70D2
Williams, Martyn (2011): North Korea's Chinese IP addresses. *38 North,* 2011. június 26. Online: www.northkoreatech.org/2011/06/26/north-koreas-chinese-ip-addresses/
Williams, Martyn (2014): Internet Coming to Kaesong Industrial Zone. *38North,* 2014. február 10. Online: www.northkoreatech.org/2014/02/10/internet-coming-to-kaesong-industrial-zone/
Williams, Martyn (2015): Koryolink Faces Big Problems with Cash, Competition. *38North,* 2015. június 25. Online: www.northkoreatech.org/2015/06/25/koryolink-faces-big-problems-with-cash-competition/
Williams, Martyn (2017): Russia Provides New Internet Connection to North Korea. *38North,* 2017. október 1. Online: www.38north.org/2017/10/mwilliams100117/
Williams, Martyn (2019): North Korea's Koryolink: Built for Surveillance and Control. *38North,* 2019. július 26. Online: www.northkoreatech.org/2019/07/26/north-koreas-koryolink-built-for-surveillance-and-control/
Williams, Martyn (2023a): North Korean Programmers Used a Hosted Laptop to Freelance Online, Says FBI. *38North,* 2023. október 24. Online: www.northkoreatech.org/2023/10/24/north-korean-programmers-used-a-hosted-laptop-to-freelance-online-says-fbi/

Williams, Martyn (2023b): Is 4G on the Horizon for North Korea? *38North,* 2023. november 4. Online: www.northkoreatech.org/2023/11/04/is-4g-on-the-horizon-for-north-korea/

Yau, Hon-min (2020): Evolving Toward a Balanced Cyber Strategy in East Asia: Cyber Deterrence or Cooperation? *Issues & Studies,* 56(3). Online: https://doi.org/10.1142/S1013251120400111

HADMÉRNÖK
FÓRUM
19. évfolyam (2024) 1. szám 177–195.
DOI: 10.32567/hm.2024.1.9

Frederick Omoyoma Odorige[1]

Coups, Regional Security Complexes and the Impact of Nigeria's Peacekeeping in West Africa, 1960–2022

Abstract

Over the years, Africa has continued to experience conflicts caused by civil wars and the tussle for power through military coups. Despite having the Mediation & Security Council within ECOWAS, it has been unable to create sustainable peace within the region. The many porous borders between the countries further exacerbate the complexities of its regional security. The consequences of these problems usually affect neighbouring countries, thereby resulting in regional security complexes and the consequent challenges of peacekeeping operations. This paper uses historical, descriptive and comparative analysis by focusing on coups as precursors to security challenges in the region of West Africa and the resulting peacekeeping operations by countries such as Nigeria. Based on the premise of ECOWAS, it introduces some conflicts caused by coups; the challenges of Regional Security Complex in West Africa and the examination of Nigerian Peacekeeping efforts. Furthermore, it offers some recommendations towards sustainable regional peace. Results show that there is a need for the African Union (AU) to do more to secure the continent. Reliance on non-African countries to support its internal security problems has become counterproductive. It recommends that Nigeria should temporarily suspend its peacekeeping operations and channel its resources towards addressing its internal security challenges; that the AU must establish a standing army as a quick response force to address the various continental crises before they become exponential threats and that ECOWAS should implement its common currency plan. Finally, the African Union must develop best practices that can alleviate poverty and guarantee security in line with the 17 UN Sustainable Development Goals.

Keywords: Nigeria, ECOWAS, peacekeeping, region, security complex

[1] PhD candidate, Ludovika University of Public Service, Faculty of Military Science and Officers Training, e-mail: fodorige@hotmail.com

"Just weeks after gaining independence in 1960, Nigeria deployed its first contingent of peacekeepers to the Congo. Since then, hundreds of thousands of Nigerian military, police, and civilian personnel have served under the UN flag across 41 operations worldwide […] You have shown exceptional bravery, dedication, and professionalism, and we are grateful for your service and your sacrifice."

Matthias Schmale, United Nations Resident and Humanitarian Coordinator in Nigeria[2]

Introduction

The Economic Community of West African States (ECOWAS) was established on 28 May 1975 under the signed *Treaty of Lagos*. It is the regional bloc upon which fifteen West African countries (Benin, Côte d'Ivoire, Gambia, Ghana, Guinea, Guinea-Bissau, Liberia, Mali, Niger, Nigeria, Senegal, Sierra Leone, Togo, Burkina Faso and Cape Verde) collectively pursue a common political, economic and peace agenda towards self-sufficiency and development within an area of 5,114,162 km^2 (1,974,589 sq mi) and an estimated population of 424.34 million.[3]

ECOWAS relies on the fundamental principles of cooperation, solidarity, equity, non-aggression, interdependence, promotion of human rights and social justice. These principles are also projected towards achieving regional security.

During the1950s and 1960s, a coup or attempted coup occurred every 4 months in Latin America, every 7 months in Asia, every 3 months in the Middle East, and every 55 days in Africa.[4] These coups resulted in conflicts and threatened the political, social and economic security of neighbouring countries.

Regional security complex theory (RSCT) on international relations, as developed by Buzan and Wæver, states that: "Simple physical adjacency tends to generate more security interaction among neighbours than among states located in different areas, a point also emphasized by Walt […] Adjacency is potent for security because many threats travel more easily over short distances than over long ones."[5]

When related to the security challenges in the West African region, this theory is further justified, because there are some similarities of security problems in this region. Such problems usually start in one country and gradually permeate into the socio-economic and political fabrics of neighbouring countries through security interactions as a result of proximity. Records show that the region has been beclouded by military coups, terrorist activities, power struggles and citizen discontentment with the government. I believe that interest in corporate matters is a luring pull for soldiers to seize power with barrels of guns in order to be involved in politics.

When coups and other conflicts occur, it rapidly affects other countries within the region, resulting in loss of lives, economic hardship, instability and the exodus of refugees. Apart from the proximity of the countries, the situation has become

[2] UN Nigeria 2023.
[3] See: www.worlddata.info/trade-agreements/ecowas-west-africa.php
[4] Bertsch et al. 1978.
[5] Buzan–Wæver 2003: 6–20, 41–47, 77–82.

more precarious because of the agreed freedom of movement, the 1998 regulations on Transhumance[6] between ECOWAS member states and their many porous and undelineated borders.

Figure 1: Map of the Economic Community of West African States (ECOWAS)
Source: www.euractiv.com/wp-content/uploads/sites/2/2014/03/ecowas_map.jpeg

West Africa, Central Africa and the Sahel region have experienced nine coups since 2020. In all of these coups, the people thronged the streets to celebrate the fall of governments which had either been in office for too long and/or been a source of artificial poverty to the people. The 16 West African countries, Benin, Burkina Faso, Cape Verde, Côte D'Ivoire, Gambia, Ghana, Guinea, Guinea-Bissau, Liberia, Mali, Mauritania, Niger, Nigeria, Senegal, Sierra Leone and Togo, have all been involved in various conflicts which affected the entire region. Some of the consequences of these conflicts led to international interventions, which applied the machineries of diplomacy, sanctions, military interventions or peacekeeping. In most cases, the Economic Community of West African States (ECOWAS) and its erstwhile military formation known as ECOWAS Military Operation Group (ECOMOG) have also carried out the military interventions in the West African region.[7] However, these interventions continue to affect the economic resources and political stability of the region.

[6] ECOWAS Official Journal 1998.
[7] About ECOMOG as a viable solution see Molnár 2008.

As of 2024, seven countries in Africa are under military rule. Apart from Sudan, six of such countries are in West Africa and they came into power through coups – Gabon, Guinea, Burkina-Faso, Niger, Mali and Chad. The history of these countries shows the interconnectedness, the consequences of conflicts and how these conflicts affect the others.

The uranium-rich Nigerhas faced international threats after a coup by the presidential guard on 26 July 2023, which overthrew democratically elected President Mohamed Bazoum. Thereafter, on 16 September 2023, "Mali, Niger and Burkina Faso, three West African Sahel nations ruled by military juntas, signed a security pact […] promising to come to the aid of each other in case of any rebellion or external aggression".[8] Such an inter-state cooperation is also the proof of a functioning regional security complex. For overthrowing democratically elected governments, these countries were sanctioned by ECOWAS. As a consequence of the sanctions, food smuggling through porous borders has increased.

In the aftermath of coups and other conflicts, the deployment of peacekeepers was necessary to restore normality. Since 1960, Nigeria has participated in at least 41 peacekeeping operations within and outside the African continent. The missions are usually done in conjunction with the United Nations, ECOWAS or the African Union. Examples of such operations include the United Nations Operation in Congo (ONUC) 1960–1964, the United Nations Security Force in West New Guinea (UNSF) 1962–1983, the United Nations India–Pakistan Observer Mission (UNIPOM) 1965–1966, the United Nations Interim Force in Lebanon (UNIFIL) 1978–1983, Chad Operation (Operation Harmony I) Bilateral 1979, the Organization of African Unity (OAU) Mission Intervention Force in Chad (Operation Harmony II) 1981–1982, the United Nations Mission in Sierra Leone 1999, the ECOMOG Operation Harmony in Liberia 1990, the UN Observer Mission in Liberia (UNOMIL) 1990–1997, the United Nations Iraq–Kuwait Observer Mission (UNIKOM) 1991, the OAU Monitoring Group in Rwanda 1992–1993, the African Union – United Nations Hybrid Operation in Darfur (UNAMID) 2007, the United Nations Multi-Dimensional Integrated Stabilization Mission in Mali (MINUSMA) 2013, the UN Assistance Mission in Rwanda (UNAMIR) 1993–1995, Nigeria Peacekeeping in Somalia, 2021, the ECOWAS mission in Guinea Bissau (ECOMIB), 2020, 2022, et cetera. These operations were necessary for Nigeria due to its interest for international peace and security. These interests are based on the legal backing and the concepts of Nigeria's peacekeeping operations.

Regional security complex in West Africa: coups and conflicts

When there are crises in a country, it affects the region due to demographic proximity or *physical adjacency*. Barry Buzan, through the Copenhagen School of security studies, developed an academic thought, which placed emphasis on the non-military

[8] Reuters 2023.

aspects of security.[9] Patterns of regional security show that the interconnectedness of countries with close borders shows underlying links (Figure 2).[10]

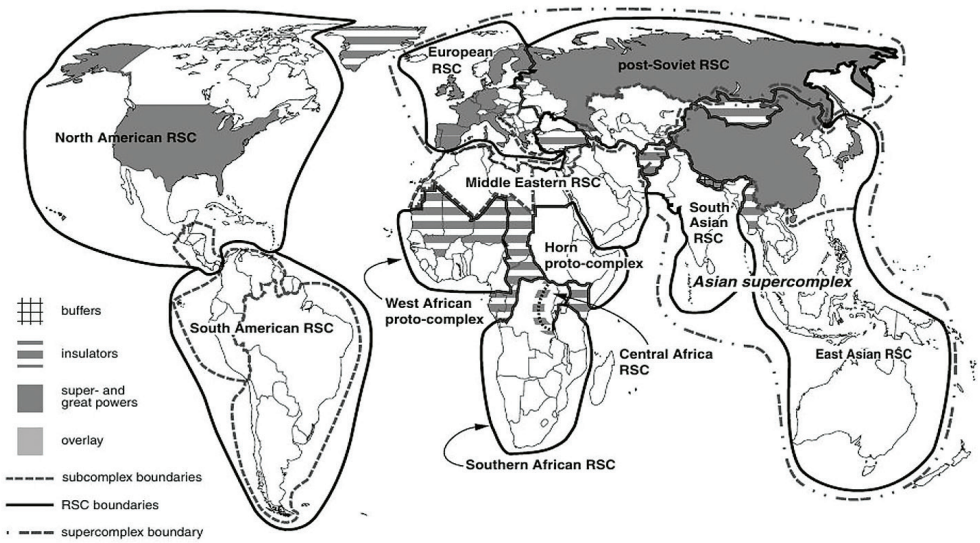


Figure 2: Patterns of regional security
Source: Buzan–Wæver 2003

If related to the exodus of refugees in times of conflicts, this notion becomes relevant. As non-military actors, undocumented refugees could pose security risks and socio-economic challenges to host communities.

In their book, Barry Buzan, Ole Wæver and Jaap de Wilde consider military/state, political, social, economic and environmental issues as new sectors of security.[11] While Buzan examined the sectoral, Wæver conceptualised securitisation where state actors should transfigure national political discourse into affairs of security as existential problems that need to be addressed. Therefore, when this transfiguration is lacking, it gives way to insecurity. They further defined Regional Security Challenge (RSC) as "a group of states whose primary security concerns link together sufficiently closely that their national security cannot realistically be considered apart from one another".[12] African leaders conduct foreign policies and "securitise" a range of external and domestic challenges as part of efforts to guarantee regime and state survival.[13] In the light of this, the statement by the African Union Peace and Security Council becomes very relevant. It states that coups often originate from "deficiencies

[9] Collins 2016.
[10] Buzan–Wæver 2003.
[11] Buzan – Wæver – de Wilde 1998.
[12] Buzan – Wæver – de Wilde 1998.
[13] Clapham 1996: 267–274.

in governance" along with "greed, selfishness, mismanagement of diversity, mismanagement of opportunity, marginalization abuse of human rights, refusal to accept electoral defeat, manipulation of constitution[s], as well as unconstitutional review of constitution[s] to serve narrow interests and corruption".[14]

Since the first African coup d'état, which took place on 13 January 1963 in Togo with the alleged support of the French government, subsequent conflicts that led to peacekeeping had elements of military coups.

For every coup that took place in West Africa, it threatened the stability of neighbouring countries in two ways. First, when a coup succeeds and the people pour out to celebrate, the presidents of neighbouring countries become nervous that their soldiers will do the same. For example, immediately after the 2023 coups in Niger and Gabon, President Paul Biya of Cameroon[15] and President Paul Kegame of Rwanda[16] were so gripped by the security complex that they quickly reshuffled their cabinets and retired some of their top military personnel. Both presidents have been in office for 41 and 23 years, respectively. They knew that their long time in office was a cause for concern for their people.

Second, every conflict or coup poses the danger of the influx of refugees to neighbouring countries. On the other hand, the influx consequently poses security challenges to the host countries because the biometric details and backgrounds of the refugees are usually not checked. Security complex is further worsened by the many porous borders in many African countries. For example, though Nigeria has 17 land borders, five maritime borders and 84 approved border controls, *there are over 1,400 illegal routes into Nigeria – 1,316 more than the approved number of border control posts.*[17] These porous borders give rooms for irregular migration and the smuggling of lethal weapons across countries.

Every conflict leads to exodus of refugees. For example, the 1989 Liberian war resulted in at least 750,000 civilians fleeing Liberia as internally displaced persons and refugees to the neighbouring countries of Cote d'Ivoire, Sierra Leone, Guinea, Nigeria, Mali, Ghana and Gambia. Some of them left the African continent.[18] Such exodus put social and economic pressure on the receiving countries. The mass exodus also made it difficult to determine the movement of terrorists and dangerous weapons, because the backgrounds and biometrics of the refugees were mostly unchecked. The war in Sierra Leone also became interconnected with the war in Liberia, because some Liberians were masters of the Sierra Leone conflict. In February 2012, Charles Taylor, the former president of Liberia (1997 to 2003) was jailed by the International Criminal Court in the Hague for the role he played in the war in Sierra Leone.[19] According to the court, Taylor *gave orders to Revolutionary United Front (RUF) rebels in the 11-year civil war in neighbouring Sierra Leone that killed about 50,000 people.*[20]

[14] African Union 2014.
[15] TRT Afrika 2023.
[16] Rwanda's Kagame fires slew of military officials in big shake-up 2023.
[17] Business Times 2014.
[18] Palmisano–Momodu 2013.
[19] For more details see Molnár 2009.
[20] Al Jazeera 2012.

It was also difficult to ascertain how many of such refugees returned home because many of them lost everything and had to start all over again. In sharp contrast with the number of Liberian refugees that left the country, the United Nations High Commissioner for

Refugees (UNHCR) was only able to repatriate 155,000 Liberians 23 years after the civil war.[21]

The Boko Haram and the Islamic State West Africa Province (ISWAP) insurgencies introduced a new wave of terrorism across West Africa with links from Libya, Niger and Syria. The fight against terrorist groups created new alliances of cooperation between Nigeria, Cameroon, Chad and Niger, even as refugees fled from the same countries to safe regions within these countries. Some of them were suspected to have joined in the farmers-herders clashes, which occurred in Benue and Plateau states of Nigeria.

Former president Buhari of Nigeria claimed that the weapons used by these terrorist groups mostly came from Libya. "These gunmen were trained and armed by Muammar Gaddafi of Libya. When he was killed, the gunmen escaped with their arms. We encountered some of them fighting with Boko Haram."[22]

Every coup has impact on regional security complexes as it sends jitters to neighbouring countries. Examples of how conflicts and coups in some West African countries resulted in regional security complexes, will suffice.

Nigeria experienced various coups in 1966, 1975, 1976, 1983, 1985, 1990 and 1993. She also fought a civil war between 1967 and 1970, which destabilised the region and attracted foreign interventions. *During the two and a half years of the war, there were about 100,000 overall military casualties, while between 500,000 and 2 million Biafran civilians died of starvation.*[23] Over 3 million persons were displaced, and refugees moved to neighbouring countries of Cameroon, Chad, Niger, Benin and beyond.

The northern region of the Republic of Benin has endured an increasing number of attacks by Islamic militias since 2018. This is because a stretch of land connects Benin, Niger and Burkina Faso, which are countries in conflicts. This situation continues to aid uncontrolled transit of weapons, people and goods across the porous borders.

Between 1960 and 2023, there has been 8 successful coups (1966, 1974, 1980, 1982, 1983, 1987, January 2022 and September 2022) and 5 attempted coups (1982, 1989, 2003, 2015, 2016) in Burkina Faso. In 2014, there was an uprising in response to the attempt by the government to change the constitution to make way for President Blaise Compaore to continue in office after 27 years in power. This led to several killings and the destruction of infrastructure. One of the consequences is the uncontrolled movement of suspicious persons across the region. For example, Fulani herdsmen reportedly crossed national borders with their cows and dangerous weapons, and later terrorised the countries they migrated to. Former President Buhari of Nigeria claimed that terrorism worsened in Nigeria because some persons got weapons from Libya after the demise of Gaddafi. Instead of taking proactive measures to arrest the situation, in December 2019, Buhari declared *issuance of visa*

[21] Al Jazeera 2012.
[22] Ogundipe 2018.
[23] American University 2017.

at the point of entry into Nigeria to all persons holding passports of African countries with effect from January, 2020.[24]

In the case of Cape Verde, though it has enjoyed political stability, the 1980 coup in neighbouring Guinea-Bissau affected the political alliances between both countries.

The First Ivorian Civil War occurred in 2002, 2004 and 2007. The military coup of December 24 1999 was followed by the removal of the coup leader, Robert Guei and the election of Laurent Gbagbo. The conflicts continued into a civil war in September 2002. Foreign countries such as Belarus, Russia, Bulgaria and Burkina Faso, got involved in the crises through their supports for various interests. Further conflicts in 2008 led to the internal displacement of 45,000 persons. By 2011, the number rose to 30,000 who fled to neighbouring countries of Liberia, Togo and Ghana. *Overall, it is estimated that at least 160,000 Ivorians fled to nearby West-African countries.*[25]

Gambia experienced two successful coups in 1981 and another in 1994. Due to the proximity in the region, people also suffered from the conflict in Senegal known as the Casamance conflict which began in 1982. It resulted in the death of at least one thousand persons.

The Konkomba–Nanumba conflict in Ghana, also known as the Guinea fowl war, which began as a tribal war in 1994 over land dispute, resulted in an estimated 2,000 deaths, a displacement of 150,000 people, some of whom fled to Togo. The coups in 1966, 1972, 1975 and 1979 also unsettled Ghana. Jerry Rawlings seized power in 1979 and ordered the execution by firing squad of eight military officers, including General Kotei, Joy Amedume, Roger Felli and Utuka, as well as the three former Ghanaian heads of state; Acheampong, Akuffo and Akwasi Afrifa.[26] This action sent shock waves throughout the western region of Africa and beyond. The allies of the victims also fled to exile.

Guinea experienced coups in 1984, 2008 and 2021, and the ensuing security complex affected neighbouring countries. The coup led to an emergency summit of the Economic Community of West African States (ECOWAS) in Accra in which it decided to freeze the financial assets and impose travel bans on the members of Guinea's junta and their relatives.

In Mauritania, coups were experienced in 1978, 1979, 1980, 1984, 2005 and 2008. Two other coup attempts were made in 1981 and 2003. Whenever there is a coup, regional blocks and the international community usually interfere. The interference is, in itself, an evidence of security complex.

Coups in Niger began in 1974 through 1996, 1999, 2010, 2021 and 2023. In the coup of 26 July 2023, soldiers from the country's presidential guard deposed President Mohamed Bazoum, and it drew the wrath and condemnation of ECOWAS, AU, UN, US and the European Union.

Togo experienced coup in 1963, 1967 and a failed attempt in 1986. Conflicts revolved around marginalisation and the desire for elongated tenures in office.

[24] Nuhu 2019.
[25] Aning 2021.
[26] Nugent 2009.

The non-military intervention in democratic matters have helped in stabilising Senegal over the years. However, regional crises have led Senegal to participate in various peacebuilding and peacekeeping operations as a way of preventing escalation in their territory and to maintain international peace. For example, in October 1980 and August 1981, a coup attempt was stopped in Gambia. In August 1989, in conjunction with the Gambian military, the Senegambian Confederation was dissolved. In 1992, they participated with ECOMOG peacekeeping group in Liberia. They also participated in peacekeeping in Rwanda, 1994, in Guinea-Bissau, 1998, in Central African Republic, 1997 and in Gambia, 2017.

On 16 July 2003, there was a coup d'état in São Tomé and Príncipe. The intervention of Nigeria in the coup was very timely. The coup was successfully launched as led by Major Fernando Pereira against the government of President Fradique de Menezes who was on a visit to President Olusegun Obasanjo in Nigeria. President Obasanjo called and negotiated with the coup plotters to return power to Menezes and the negotiation succeeded with a promise to grant amnesty to the plotters. The military held on to power for 7 days in São Tomé and Príncipe.

In Niger, ensuing conflicts were also connected to coup d'états. There were coups in 1974, 1996, 1999 and 2010, and an attempted coup in 2021. On 18 February 2010, there was a coup in Niger led by squadron leader Salou Djibo against President Mamadou Tandja who was kidnapped and replaced with the leader of the opposition.

Guinea-Bissau experienced coup d'états in 1980, 1999, 2003, 2010 and 2012. On 1 April 2022, there was an attempted coup led by Admiral Bubo Na Tchuto and the Deputy Chief of Staff of the Army, Antonio Ndjai. The head of the military was arrested after the failed coup which witnessed the brief arrest of the prime minister.

In the Democratic Republic of Congo, there has been various coup d'états and conflicts which led to several peacekeeping operations. Five failed coup attempts were made at various times in 1966, 1968, 1972, 1987 and 2011. Three others succeeded. On 14 September 1960, Mobutu Sese Seko overthrew Patrice Lumumber. On 25 November 1965, Mobutu Sese Seko overthrew Joseph Kasa-Vubu and on 16 May 1997, Laurent-Désiré Kabila overthrew Mobutu Sese Seko which led to the First Congo War.[27]

In Mali, they have also experienced five coup d'états in 1968, 1991, 2012 (attempted), 2020 and 2021. The aftermath of the 2020 coup, which overthrew President Ibrahim Boubacar Keita, received global condemnation especially from the African Union, the United Nations and the European Union. The United States of America took a step further by cutting off military aid to Mali.[28]

Though there has been no peacekeeping mission in the West African country of Burkina Faso (formerly Upper Volta), the country witnessed 14 coup d'états between 1966 and 2022. Ten of them succeeded.[29] Such coups pose security challenges, disrupts developmental agenda of predecessors and derail the socio-political and economic stability of the country. These disruptions account for why Burkina Faso is considered

[27] Britannica 2024.
[28] Diallo–Ross 2020.
[29] January 3, 1966; February 8, 1974; November 25, 1980; November 7, 1982; October 15, 1987; September 18, 1989; September 17, 2015; October 30, 2014, January 23, 2022 and 30 October 2022.

as one of the poorest countries in the world, as it ranks 144th among 157 countries in the World Bank's Human Capital Index. Since 2015, the situation of the country has been worsened by terrorist attacks, leading to population displacement. There were 50,000 internally displaced persons in the country in January 2019. By January 2022, more than 3,000 schools (13% of educational institutions) were closed because of the insecure environment.[30]

The crises that rocked Liberia were mostly precipitated by coup d'états. Though there was a historic occurrence when the Liberian people deposed President Edward James Roye on 26 October 1971, the two coups of 1980 and 1990 destabilised the country. On 12 April 1980, Master Sergeant Samuel Kanyon Doe overthrew President William R. Tolbert, Jr and on 9 September 1990, Prince Johnson overthrew Samuel Kanyon Doe. Charles Taylor's militia overthrew the regime of Samuel Doe in 1989. The upheaval plunged the country into a 14-year bloody civil war. By the end, 200,000 were killed in the fighting and more than half of the population became refugees.[31] On April 26 2012, the United Nations-backed Special Court for Sierra Leone (SCSL), sitting in The Hague, found former Liberian president, Charles Taylor guilty of abetting horrific war crimes, rape and mutilation in Sierra Leone.

Five coup d'états took place in Sierra Leone on 21 March 1967, 19 April 1968, 29 April 1992, 16 January 1996 and 25 May 1997. From the coup of 1992, Sierra Leone was already in chaos. However, the Jonny Paul Koroma coup of May 25 1997, launched on the platform of the Sierra Leone Army (SLA), overthrew President Ahmed Tejan Kabba and set the tone for the bloody war, which lasted 11 years and reportedly left over 50,000 persons dead.

In Chad, three successful coups took place: on 13 April 1975, 7 June 1982 and 1 December 1990. Three failed coup d'états occurred on 16 May 2004, 14 March 2006 and 1 May 2013. Several rebel factions waged the 1965–1979 Civil War in Chad against two governments. There were outcries against high level corruption, authoritarianism and nepotism. The renewed war that began on 18 December 2005 was also a result of the same agitations, especially by Muslim northerners and Christian southerners who attacked each other whenever the other was in power.

A wider overview of coups in the African continent shows that of 492 attempted or successful coups carried out around the world since 1950, Africa has seen 220, the most of any region, with 109 of them successful.[32]

[30] UNICEF 2022.
[31] History 2018.
[32] Duzor–Williamson 2023.

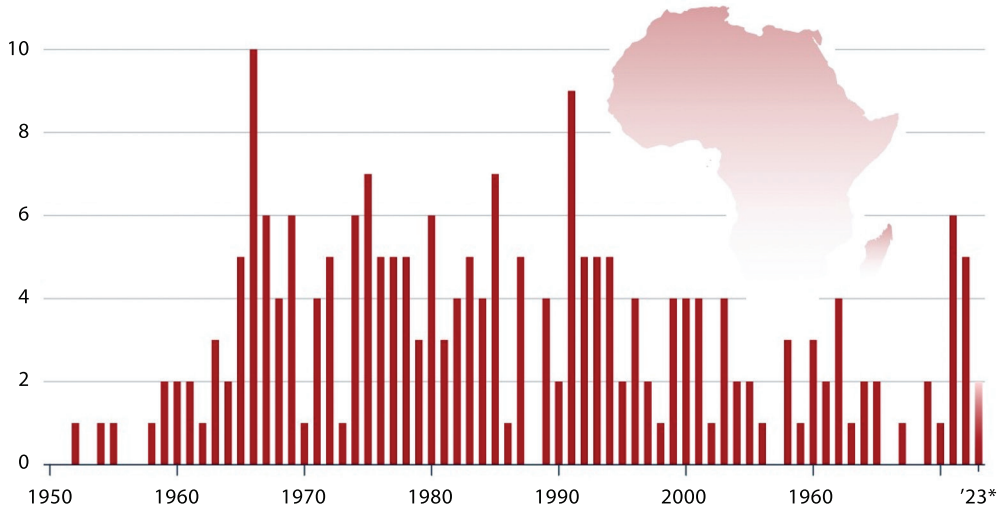


Figure 3: Number of coups d'état (successful and unsuccessful) per year in Africa between 1950 and July 2023

Source: Powell–Thyne 2011; Statista research; Duzor–Williamson 2023

Examining Nigerian peacekeeping

The concept of Nigeria's participation in peacekeeping lies on its commitment to promote and protect its foreign relations. This is in line with Section 19 of the 1999 Constitution, which states the objectives of Nigeria's foreign relation and lays the foundation for the country's peacekeeping concept, theory and practice. Two aspects of related foreign policies are the *promotion of international cooperation for the consolidation of universal peace and mutual respect among nations and elimination of discrimination in all its manifestation*. The other part is *respect for international law and treaty as seeking settlement of the internal dispute by negotiation, mediation, conciliations, arbitration, and adjudication*.[33] In both situations, Nigeria uses negotiation and force to implement its policies as enumerated in this research.

As a member of the United Nations since 1960, Nigeria is, to a larger extent, obligated to respect the Charter of the United Nations. Chapter VII mandates the body to take *action with respect to the peace, breaches of the peace and acts of aggression.* This chapter is usually invoked as a legally binding force when approving the deployment of UN peace operations. One of the structures built by the Nigerian government to enhance the framework for participation in peacekeeping is the Nigerian Police Peacekeeping Office. The office was established in 2005 with the aim of engaging in meaningful research and for the training of officers for global deployment in support of operations. The office also equips personnel with the skills and capacities needed

[33] See: https://foreignaffairs.gov.ng/about-us/foreign-policy/

for complex peace support operations in all environments, towards professional and international best practices.

"In 1960, the Nigerian police deployed the first ever contingent of Individual police officers (IPOs) to UN mission in the Congo led by ACP Louis Edet while the pioneer Formed Police Unit (FPU) of 120 officers and men were deployed to Liberia in 2004 under […] over twelve thousand personnel to various UN/AU and ECOWAS peace support operation."[34] The Department of Peacekeeping Operations (DPKO) was formally established as *a department of the UN Secretariat in 1992, has nearly 122,000 personnel, with 118 countries contributing military and police to 16 different DPKO-led missions around the world.*[35]

Despite the huge domestic security challenges, Nigeria has participated in at least 41 peacekeeping missions, out of which six have been commanded by Nigerian senior military officers (in Congo, Angola, Lebanon, Liberia, Sierra Leone and Chad). The financial cost of peacekeeping in Chad (1979–1982) was borne by Nigeria under the auspices of the OAU. On the other hand, Nigeria has occupied the chair position of the UN Special Committee on Peacekeeping Operations since 1972. In 2020, Nigeria was re-elected, for the 48th time, to chair the United Nations Special Committee on Peacekeeping Operations – regarded as the UN's most strategic committee, which is also known as C-34. This special committee, which consists of 147 member states and focuses on peacekeeping operations, was established in 1965 by the General Assembly, and it reviews and provides crucial recommendations on United Nations peacekeeping operations.[36]

Though Nigeria has participated in several peacekeeping operations, its role in peacekeeping in West Africa has its loudest expression in terms of the financial commitment and the high deployment of human capacity. Nigeria has also intervened in various ways in the coups and conflicts that took place in West Africa.

In August 1990, Nigeria led ECOMOG to contain the civil war in Liberia until peace was restored in 2003. Apart from the fact that the war was a regional threat, Nigeria was also keen on rescuing its citizens in Liberia where at least 3,000 Nigerians reportedly lived and were entrapped by the war. After the restoration of peace and the conduct of elections, the Nigerian troop continued to be stationed in Liberia for 15 years until the last batch departed Liberia in February 2018. During that period, with the support of the UN, they were able to restore peace, train the soldiers and supervise the electoral process. Throughout its presence in Liberia, Nigerian military claimed that it spent $8bn to restore peace in Liberia.[37] Human Rights Watch cited, that in September 1997, when the new Zimbabwean high commissioner to Nigeria was presenting his credentials, he paid tribute to Nigeria's leadership in ECOWAS and described the end of the Liberian war as *a classic in the history of peacekeeping in the world.*[38] Nigeria's role in the war in Sierra Leone, which started in March 1991, was also very substantial. Effective mechanisms were put in place for sustainable

[34] See: www.npf.gov.ng/info/peace_keeping.php
[35] See: https://peacekeeping.un.org/en
[36] Business Day 2020.
[37] Punch 2023.
[38] Human Rights Watch 1997.

peace. Nigerian government started by giving the coup plotters an ultimatum to relinquish power.

Thereafter, it started to shell the base of the coup plotters by using the tactics of "containment", which was all about using force. Some other countries did not support the use of force. However, diplomatic resolutions by multinational groups and the UN were later reached, and it led to the signing of the Abidjan Peace Accord in Abidjan, Côte d'Ivoire on 30 November 1996. Since peacekeepers left Sierra Leone, it did not return to war. "A critical factor in Sierra Leone's stability is the complex interaction of domestic, subregional and external actors, which is crucial to the success of conflict management and conflict prevention processes."[39]

Between 2016 and 2017, there were constitutional crises in which the sitting president, Yahya Jammeh refused to relinquish power to Adama Barrow, the winner of the election. When negotiations failed, a military force by West African states superintended by Nigeria, Ghana Togo, Mali and Senegal entered into Gambia. Jammeh escaped, went into exile, and power was handed over to Barrow.

The Nigerian president was holding the position of the chairman of ECOWAS when the coups in Niger and Gabon occurred in 2023. They understood that if action was not taken, it could lead to regional crisis. Therefore, in conjunction with other West African leaders, the chairman spearheaded the imposition of sanctions against the juntas that forcefully took over power from democratically elected presidents. The economic, political and social sanctions were geared towards isolating the countries and muzzling their economic strength as a way of coercing them into agreeing to mutual diplomatic resolutions that could restore democratic rule. The sanctions imposed on Niger included the freezing of all its enterprises and parastatals in commercial and Central banks in all ECOWAS member states; closure of land and air borders; declaration of ECOWAS no flight zone to all commercial flights to and from Niger; suspension of all commercial and financial transactions; freezing of all service transactions including energy transactions, state enterprises and parastatals in commercial banks; suspension from all financial assistance and transactions with all financial institutions, and the imposition of travel bans on the military officials and the families of the coup plotters.[40]

In the case of the 2023 coup in Gabon, the African Union's Peace and Security Council immediately suspended the participation of Gabon in all activities of the AU.[41]

Nigeria's role in peacekeeping has been consistent and exemplary due to its commitment to burden sharing, its ability to navigate the difficult path from conflict to peace, and the ability to swiftly deploy troops and police officers from among the 14 other countries involved in the operation anywhere in the world. Data from the UN Peacekeeping Department classified Nigeria as among the world's 15th largest troop contributor to UN Peacekeeping operations and the eighth in Africa. For example, in 2016, Nigeria contributed 2,170 peacekeeping personnel composed of 403 policemen and 46 military experts.[42] In the course of these operations, there were

[39] Adebajo 2021: 345.
[40] Sahara Reporters 2023.
[41] Al Jazeera 2023.
[42] Al Jazeera 2023.

ongoing internal conflicts in Nigeria, which the world did not seem to be concerned about. Between 2015 and 2023, when retired army general Buhari was president, 63,111 Nigerians were killed by non-state actors.[43] No tangible support was received from the international communities.

Due to international cooperation and the instrumentality of the United Nations within the past two decades, more civil wars have ended through negotiations and diplomacy, than it did in the previous 200 years.

However, some of the conflicts in Africa – especially coups – had backings from foreign countries. Their aim is to have their stooges in offices where they could exploit the resources of such countries. Having at least 13 countries having military presence in Africa, with about 11 foreign military bases in the Horn of Africa,[44] does not help matters. Africa must decide her future through an AU standing force, while Nigeria must focus more on solving its internal crises before participating in peacekeeping operations in foreign countries. Trade and prosperity could be achieved through the interdependence of countries without setting up military bases in foreign countries. However, there must be individual liberty, which forms a strong ingredient of peace and security.[45]

When charity starts from abroad

Though it is said that charity starts at home, it seems to come from abroad when Nigeria addresses the problem of conflicts. While serious security challenges were mostly left unaddressed by the Nigerian government, it spent so much in securing and stabilising other countries.

For example, in 2021, when Nigeria was busy participating in peacekeeping in Somalia, various conflicts and other serious security challenges were going on in the country.

A recorded number of 6,895 Nigerians were reportedly killed in 2021.[46] Out of this number, 844 of persons killed were state security officers and 6,051 were civilians. While at least 2,002 persons were abducted in 2020, at least 5,663 were in 2021. Analysis of the demographic spread of terrorism in Nigeria shows that in 2021, when a Nigerian troop was sent to Somalia, five states in the northern part of the country was experiencing over 57.3 per cent of abductions. 4 of the 5 occurrences were in the North-West and the last was in the North-Central. Of the 5,663 abductions, at least 3,246 were recorded in the North West in 2021. 1,225 of these had occurred in Kaduna state, just barely more than the at least 1,169 abductions that took place in Zamfara State. Around 1,522 abductions occurred in the North Central. Within this number, Niger state had the highest number of 1,127 abductions.

[43] Vanguard 2023.
[44] Isilow 2023.
[45] Dunne–Schmidt 2001.
[46] Eromosele 2022.

Students were not spared either. Over 1,000 Nigerian students were kidnapped between December 2020 and September 2021 in northern Nigeria,[47] particularly in the mass kidnaps that took place in Kaduna, Kebbi, Niger, Zamfara and Katsina state – which is the home state of Muhammadu Buhari, the then President who, as a retired army general, was expected to have the professional experience to secure the country. His failure became ridiculous because during his campaign for election in 2015, he promised to end terrorism within six months of resuming office.

It can be stated that Nigeria has technically been at war due to the internal armed conflicts since 2022. Not all wars are between states. When an armed conflict passes the threshold of 1,000 battle-related deaths during one calendar year, it is considered a war.[48]

Boko haram has caused huge security challenges within the region. Between 2011 and 2023, it was responsible for thousands of deaths in Nigeria, Cameroon, Chad, and Niger. Nigeria is the country most affected by terrorist group attacks. States in the North-East register the highest number of deaths. Borno is by far the most threatened state, in that, Boko Haram has caused over 38,000 deaths in this area.[49] Figure 4 shows details of death per 1000 people to the ratio of annual percentage change from 2015 to 2023.

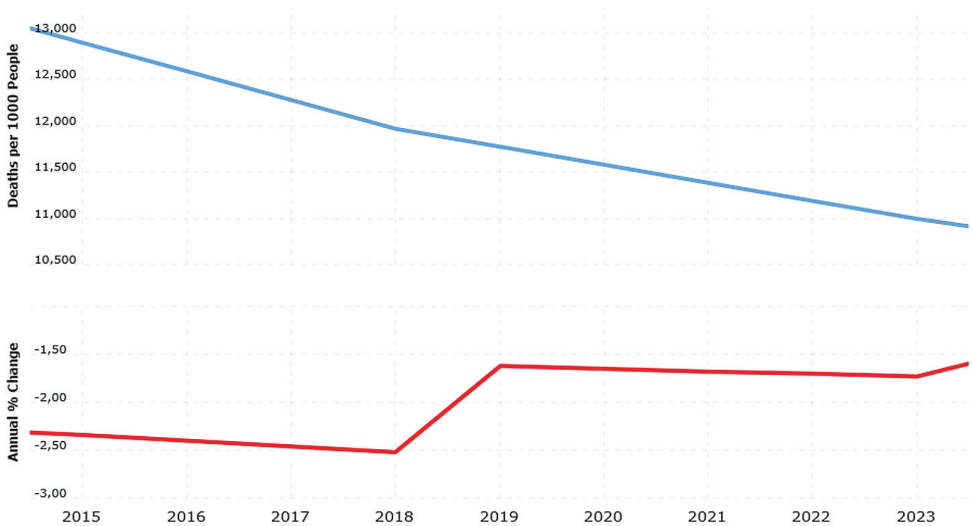


Figure 4: Nigeria death rate 2015–2023

Source: www.macrotrends.net/global-metrics/countries/ranking/death-rate

However, death by ritual killings, kidnapping, secessionist, political and mob attacks worsened. With such deaths that ought to have been prevented, it was ironic that

[47] Asadu 2021.
[48] Arolsen Archives 2022.
[49] See: www.statista.com/statistics/1197570/deaths-caused-by-boko-haram-in-nigeria

a country that should have been strengthening security on its own territory was sending troops to ensure the security of other countries.

Conclusion and recommendations

All the conflicts, which have negatively affected the West African region are results of coups and other conflicts. Regional security complexes are reflected by the interconnectedness of countries within the region these times. The relationships between these countries are in terms of proximity, porous borders and other political and economic ties. These conflicts are mostly caused by coups, struggle for power or marginalisation, which are consequences of the dissatisfaction, which arises from the distribution of public wealth. Some of the coups are allegedly sponsored by foreign powers who mostly have military bases within some of the African countries. Their goals are allegedly geared towards exploiting mineral resources and to interfere in the internal political affairs of such countries.

Based on the findings of the study, my recommendations are as follows:

1. The African Union should explore the possibility of establishing a standing army as a quick response force to address the various conflicts threatening the continent. This could also be actualised when the AU creates deeper working relations with the UN for multilateral and more collaborative peacekeeping operations. Such collaborations should include the incorporation of African countries as permanent members of the United Nations Security Council.

2. Nigeria should temporarily withdraw its peacekeeping troops from other countries and use its manpower to end internal conflicts and terrorism before returning to peacekeeping operations.

3. ECOWAS should actualise the common currency goal, as it will help to foster more economic, social, political and security cohesion.

4. Finally, the AU needs to set up measurable strategies that could prevent the overthrow of democratically elected governments through military coups. Such models should align with international standards – such as the practical actualisation of the 17 UN Sustainable Development Goals – geared towards improving the security of the people and the drastic reduction of poverty.

References

Adebajo, Adekeye (2021): The Dog That Did Not Bark: Why Has Sierra Leone Not Returned to War After Peacekeepers Left? In McNamee, Terence – Muyangwa, Monde (eds.): *The State of Peacebuilding in Africa.* Cham: Palgrave Macmillan, 343–361. Online: https://doi.org/10.1007/978-3-030-46636-7_19

African Union (2014): *Press Statement of the 432nd Meeting of the PSC on 'Unconstitutional changes of Governments and popular uprisings in Africa'.* 29 April 2014. Online: www.peaceau.org/en/article/press-statement-of-the-432nd-meeting-on-unconstitutional-changes-of-governments-and-popular-uprisings-in-africa

African Union Suspends Gabon's Membership after Military Coup. *Al Jazeera,* 31 August 2023. Online: www.aljazeera.com/news/2023/8/31/african-union-meets-on-gabon-situation-after-military-coup

American University (2017): *ICE Case Studies*. *The Biafran War.* 14 February 2017. Online: https://web.archive.org/web/20170214103207/http://www1.american.edu/ted/ice/biafra.htm

Aning, Kwesi (2021): Cote d'Ivoire. *Journal of International Peacekeeping,* 24(3–4), 336–366. Online: https://doi.org/10.1163/18754112-24030004

Asadu, Chinedu (2021): Gunmen Kidnap 73 Students in Latest Attack on Nigeria School. *AP News,* 1 September 2021. Online: https://apnews.com/article/africa-education-nigeria-9408a6c2d1895d1a465cc3045c004cbd

Bertsch, Gary K. – Clark, Robert P. – Wood, David M. (1978): *Comparing Political Systems. Power and Policy in Three Worlds.* New York: Wiley.

Britannica, T. Editors of Encyclopaedia (2024): *Laurent Kabila*. *Encyclopedia Britannica,* 25 April, 2024. Online: www.britannica.com/biography/Laurent-Kabila

Business Day (2014): *Nigeria's Porous Borders,* 28 April 2014. Online: https://businessday.ng/editorial/article/nigerias-porous-borders/

Business Day (2020): *Nigeria Re-elected UN Peacekeeping Committee Chair.* 7 March 2020. Online: https://businessday.ng/uncategorized/article/nigeria-re-elected-un-peacekeeping-committee-chair/

Buzan, Barry – Wæver, Ole (2003): Patterns of Regional Security post-Cold War. In *Regions and Powers: The Structure of International Security.* Cambridge: Cambridge University Press, xxvi–xxvi. Online: https://doi.org/10.1017/CBO9780511491252.003

Buzan, Barry – Wæver, Ole (2003): *Regions and Powers: The Structure of International Society.* Cambridge: The Press Syndicate of the University of Cambridge. Online: https://doi.org/10.1017/CBO9780511491252

Buzan, Barry – Wæver, Ole – de Wilde, Jaap (1998): *Security: A New Framework for Analysis.* Boulder, Colo.: Lynne Rienner. Online: https://doi.org/10.1515/9781685853808

Clapham, Christopher (1996): *Africa and the International System: The Politics of State Survival.* Cambridge: Cambridge University Press.

Cameroon's President Biya reshuffles top military brass. *TRT Afrika,* 31 August 2023. Online: www.trtafrika.com/africa/cameroons-president-biya-reshuffles-top-military-brass-14757982

Collins, Alan ed. (2016): *Contemporary Security Studies* (4th ed.). Oxford: Oxford University Press.

Diallo, Tiemoko – Ross, Aaron (2020): U.S. Halts Military Cooperation with Mali as Coup Supporters Celebrate. *Reuters,* 21 August, 2020. Online: www.reuters.com/article/mali-security-idINKBN25H1A9/

Dunne, Tim – Schmidt, Brian (2001): Realism. In Baylis, John – Smith, Steve (eds.): *The Globalization of World Politics: An Introduction to International Relations.* New York: Oxford University Press.

Duzor, Megan – Williamson, Brian (2023): Coups in Africa. *Voice of America News,* 3 October 2023. Online: https://projects.voanews.com/african-coups/

Eromosele, Fortune (2022): Insecurity: 6,895 persons killed in 2021 – Report. *Vanguard,* 27 May 2022. Online: www.vanguardngr.com/2022/05/insecurity-6895-persons-killed-in-2021-report/

History (2018): *Former Liberian president Charles Taylor found guilty of war crimes.* 18 May 2018. Online: www.history.com/this-day-in-history/former-liberian-president-charles-taylor-found-guilty-of-war-crimes

Human Rights Watch (1997): *Nigeria's Intervention in Sierra Leone.* Online: www.hrw.org/reports/1997/nigeria/Nigeria-09.htm#P602_157494

Insecurity: 63,111 Persons Killed in Buhari's Eight Years (2023). *Vanguard,* 20 May 2023. Online: www.vanguardngr.com/2023/05/insecurity-63111-persons-killed-in-buharis-eight-years/#:~:text=A%20new%

Isilow, Hassan (2023): Chains of Colonialism. Western Powers in Africa vying for Control, Geopolitical Edge. *Anadolu Agency,* 27 July 2023. Online: www.aa.com.tr/en/africa/-chains-of-colonialism-western-powers-in-africa-vying-for-control-geopolitical-edge/2956190

Jowett, Philip (2016). *Modern African Wars. The Nigerian-Biafran War 1967–70.* Oxford: Osprey.

Molnár, D. (2008): ECOMOG: The Example of a Viable Solution for African Conflicts. *AARMS – Academic and Applied Research in Military and Public Management Science,* 7(1), 55–61.

Molnár, D. (2009): Charles Taylor's Trial: It has Started. *AARMS – Academic and Applied Research in Military and Public Management Science,* 8(1), 83–89.

Nugent, Paul (2009): Nkrumah and Rawlings: Political Lives in Parallel? *Transactions of the Historical Society of Ghana,* (12), 35–56.

Nuhu, Salome (2019): All Africans Travelling to Nigeria Can Get Visa on Arrival from 2019 – Official. *Premium Times,* 11 December 2019. www.premiumtimesng.com/news/headlines/367865-all-africans-travelling-to-nigeria-can-get-visa-on-arrival-from-2019-official.html

Ogundipe, Samuel (2018): Buhari blames Gaddafi for killings across Nigeria. *Premium Times,* 12 April 2018. Online: www.premiumtimesng.com/news/top-news/264764-buhari-blames-gaddafi-for-killings-across-nigeria.html

Omotuyi, Sunday (2021): Reassessing the Power of a Sub-Regional Security Provider: The Case of Nigeria in the Gambian Crisis. *The African Review*, 48(2), 359–380. Online: https://doi.org/10.1163/1821889X-12340056

Palmisano, Laura – Momodu, Sulaiman (2013): UNHCR Completes Repatriation of 155,000 Liberians. *UNCHR,* 4 January 2013. Online: www.unhcr.org/news/stories/unhcr-completes-repatriation-155000-liberians

Powell, Jonathan M. – Thyne, Clayton L. (2011): Global Instances of Coups from 1950 to 2010: A new Dataset. *Journal of Peace Research,* 48(2), 249–259. Online: https://doi.org/10.1177/0022343310397436

Punch (2023): *Nigeria spent $8bn to restore peace in Liberia, says Irabor.* 24 May 2023. Online: https://punchng.com/nigeria-spent-8bn-to-restore-peace-in-liberia-says-irabor/

Reuters (2023): *Mali, Niger and Burkina Faso Sign Sahel Security Pact.* 16 September 2023. Online: www.reuters.com/world/africa/mali-niger-burkina-faso-sign-sahel-security-pact-2023-09-16

Rwanda's Kagame Fires Slew of Military Officials in Big Shake-Up. *Al Jazeera,* 7 June 2023. Online: www.aljazeera.com/news/2023/6/7/rwandas-kagame-fires-slew-of-military-officials-in-major-shakeup

Sahara Reporters (2023): *ECOWAS Imposes 'Stiff' Sanctions Against Niger Republic, Coup Leaders And Families.* 30 July 2023. Online: https://saharareporters.com/2023/07/30/ecowas-imposes-stiff-sanctions-against-niger-republic-coup-leaders-and-families

Twenty-first conference of heads of states, Decision A/DEC.5/10/98 Relating to the regulations on Transhumance between ECOWAS Member States (1998). *ECOWAS Official Journal,* 35, 1–14. Online: www.ecpf.ecowas.int/wp-content/uploads/2016/01/Decision-1998-English.pdf

Uche, Chibuike (2008): Oil, British Interests and the Nigerian Civil War. *The Journal of African History*, 49(1), 111–135. Online: https://doi.org/10.1017/S0021853708003393

UNICEF (2022): *Global Annual Results Report 2022.* Online: www.unicef.org/media/142921/file/Global%20annual%20results%20report%202022:%20Goal%20area%202.pdf

UN Nigeria (2023): *We salute Nigerian UN Peacekeepers, past and present – Schmale.* 30 May 2023. Online: https://nigeria.un.org/en/234801-we-salute-nigerian-un-peacekeepers-past-and-present

War in Ukraine: What Does the Death Toll Mean? *Arolsen Archives,* 6 October, 2022. Online: https://arolsen-archives.org/en/news/war-in-ukraine-what-does-the-death-toll-mean/

War Crimes Court Finds Charles Taylor Guilty *Al Jazeera*, 27 April 2012. Online: www.aljazeera.com/news/2012/4/27/war-crimes-court-finds-charles-taylor-guilty#:~:text=According

Tartalom