NEMZETI KÖZSZOLGÁLATI EGYETEM

Hadtudományi Doktori Iskola

Doktori (PhD) értekezés

Horváth Dávid

Budapest, 2026

NEMZETI KÖZSZOLGÁLATI EGYETEM

Hadtudományi Doktori Iskola

Horváth Dávid:

Álhírek terjedése és működése az online politikai diskurzusban

-

Összehasonlító elemzés a 2014-es Krím-annektálás és a 2022-től tartó orosz–ukrán háború fegyvernek minősülő kommunikációs ökoszisztémájában

Doktori (PhD) értekezés

Témavezető: Jakusné dr. Harnos Éva

egyetemi docens

Tartalomjegyzék

Tartalom

1. BEVEZETÉS

1.1. A kutatás kontextusa és hadtudományi aktualitása

„A háború nem csupán a fegyverek harca, hanem az elmék harca is.” Clausewitz tétele – amely a fizikai megsemmisítés és a morális erők dialektikájára épül – sohasem volt időszerűbb, mint most. A 21. század első negyedének biztonsági környezetét alapvetően határozza meg az a tendencia, hogy a hadviselés súlypontja a fizikai (kinetikus) térből egyre láthatóbban a kognitív dimenzióba tolódik. A döntő pillanat sokszor már nem a terepen, hanem a percepcióban következik be. Abban, hogy a társadalmak, a politikai vezetés és a szövetségi rendszerek mikor és hogyan ismernek fel egy helyzetet, milyen gyorsan képesek értelmezni, és képesek-e egyáltalán időben reagálni. Ez nem metafora. Ez műveleti kockázat.

A döntéshozók és a társadalom attitűdjeinek célzott befolyásolása e folyamat kritikus eleme. Az információ ebben az értelemben nem csupán hadműveleti kísérőjelenség, hanem önálló műveleti dimenzió: olyan erőtér, ahol a döntési lánc rövidül, a bizonytalanság gyorsabban terjed, és ahol a késlekedés önmagában is hatás. A tételmondat egyszerű: a döntéshozatali bizonytalanság és a reakcióidő lassulása nem adminisztratív melléktermék, hanem tudatosan előállított műveleti kimenet, amelyet fegyvernek minősülő kommunikációval (FMK; weapon-grade communication) lehet előidézni.

Ezzel párhuzamosan a digitális platformok – ajánlórendszereikkel, moderációs gyakorlataikkal és disztribúciós mechanizmusaikkal – a kommunikáció terjedésének nem semleges csatornáivá, hanem aktív feltételrendszerévé váltak. A hadtudományi probléma így nem kizárólag az, hogy mi igaz, hanem az is, hogy mi válik hihetővé, láthatóvá vagy cselekvést kiváltóvá a platformlogika és a hálózati szervezettség keretei között. A disszertáció ezt a feltételrendszert platformökológiaként kezeli: a hatás nem csak az üzenetben, hanem az elosztási architektúrában (láthatóság, visszacsatolás, amplifikáció) is képződik. Ez nem csak kommunikációelmélet, hanem hadtudományi kockázat. A döntési környezetet olyan infrastruktúra alakítja, amelynek ösztönzői nem feltétlenül esnek egybe a biztonságpolitikai racionalitással – és amelynek célja, az Európai

Bizottság 2016-os hibrid-keretdefiníciójában is rögzített formulával, a döntéshozatali folyamatok akadályozása a kétértelműség előállításán keresztül.[1]

E kutatás aktualitását két, egymással szervesen összefonódó trend adja. Az egyik a technológiai ökoszisztéma robbanásszerű transzformációja. A generatív mesterséges intelligencia (GenAI), a szintetikus média és az automatizált terjesztési infrastruktúrák megjelenése ipari léptékűvé tette a megtévesztést, a hitelesség-eltérítést (credibility hijacking) és a figyelem túlterhelését. A változás lényege nem pusztán mennyiségi. Az előállítás, a sokszorosítás és a célba juttatás költségei radikálisan lecsökkennek, miközben a terjesztés sebessége és skálázhatósága ugrásszerűen nő. Ennek következtében a befolyásolási műveletek már nem egyedi üzenetekre, hanem komplett elosztási és visszacsatolási rendszerekre támaszkodhatnak.

A jelenség egyik legveszélyesebb kimenete az úgynevezett hazugok osztaléka (Liar's Dividend).[2] Ennek logikája szerint a szintetikus manipulációk puszta lehetőségének köztudatba kerülése önmagában stratégiai előnyhöz juttathatja azt az aktort, aki az elszámoltathatóság elől menekül. Elég a hitelességet támadni – és máris megkérdőjelezhetővé válnak a valódi bizonyítékok is. Vagyis a támadás akkor is elérhet műveleti célt, ha egyetlen konkrét hamisítványt sem lehet azonosítani. Elég, ha a közönség megtanulja, hogy minden hamisítható. A műveleti siker mércéje ily módon nem az, hogy a célközönség elhisz-e egy adott állítást, hanem az, mennyire válik tartóssá a gyanú, a cinizmus és a „nem lehet tudni” állapota – ami közvetlenül csökkenti a közintézmények, a média és az igazolási eljárások iránti együttműködési hajlandóságot.

A másik meghatározó trend a társadalmi reziliencia (societal resilience) átalakulása. A 2020-ban kirobbant COVID–19 világjárvány és az azt kísérő infodémia (infodemic) – amelyen a dezinformáció és a félretájékoztatás járványszerű, globális szintű terjedését értjük – olyan globális

---

[1] Európai Bizottság (2016), idézi: HEAP, Ben (szerk.) (2021): Strategic Communications Hybrid Threats Toolkit. Riga: NATO Strategic Communications Centre of Excellence, 11. o. [A kutatói munkában Monika Gill és Pia Hansen vett részt.] A hivatkozott idézet – „generating ambiguity to hinder decision-making processes” – az Európai Bizottság és az Unió külügyi és biztonságpolitikai főképviselőjének 2016. április 6-i Joint Framework on countering hybrid threats (JOIN(2016) 18 final) c. közös kerethatározatából származik.

[2] CHESNEY, Robert – CITRON, Danielle (2019): Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. California Law Review, 107. évf. 1753–1820. o., különösen 1785. o. A szerzők vezették be a „hazug osztaléka" (Liar's Dividend) fogalmat: a deepfake-technológia puszta léte elegendő ahhoz, hogy a valódi, kompromittáló felvételeket is hamisítványnak lehessen nyilvánítani. A fogalmat politológiai irányban fejlesztette tovább: SCHIFF, Kaylyn Jackson – SCHIFF, Daniel S. – BUENO, Natalia S. (2023): The Liar's Dividend: Can Politicians Claim Misinformation to Evade Accountability? Research Paper, 1–43. o.

kognitív hadgyakorlatként működött, amelyben társadalmak, intézmények és platformok egyszerre szereztek tapasztalatot ipari méretű félretájékoztatással, pánikkeltéssel és bizalomrombolással kapcsolatban. A kínai dezinformációs gépezet 2020-as működése, amely a vírus eredetét az amerikai hadseregnek tulajdonította, jól illusztrálja, hogyan használhatók fel válsághelyzetek a kognitív dimenzióban a felelősség áthárítására és a szövetségi rendszerek közötti feszültség szítására. A kockázat nem pusztán a téves információ, hanem a viselkedés-indukció: a félelem, a düh, a csoporthatárok megkeményedése, a döntési helyzetek bénítása. A szemantikai mezők időbeli torzulása dinamikus szóbeágyazási modellekkel is mérhető: a COVID-19-hez kapcsolódó kifejezések kontextuális „mérgezése" (például a „COVID" és az „5G" asszociációs összeolvadása) empirikus bizonyítéka a Generálás- Mosás- Terítés/Terjesztés-Validálás/Igazolás (G–M–T–V) lánc Mosás-fázisában végbemenő szisztematikus jelentéstorzulásnak[3]

A téma hadtudományi relevanciáját erősíti, hogy a hibrid fenyegetések, a stratégiai kommunikáció és a kognitív dimenzió kérdései a NATO és az Európai Unió intézményrendszerében is kiemelt figyelmet kapnak. A védekezés elsődleges felelőssége azonban a nemzeti szinteken marad, és ez a felelősség az állami szerveken túlra is kiterjed. Barbara J. Falk (2020) a Hybrid CoE keretében fejlesztette ki a „stratégiai polgár" (strategic citizen) koncepcióját,[4] amely pontosan ezt a kiterjedést ragadja meg: a közösségi média korában a katona és a civil közötti választóvonal elmosódott. Ahogy a poszt-9/11 katonai gondolkodásból ismert „stratégiai tizedes" (strategic corporal) fogalma[5] azt rögzítette, hogy a legkisebb egység döntése is stratégiai következményekkel jár, úgy a stratégiai polgár belátása azt mondja ki, hogy minden civil, aki információs tartalmat oszt meg, potenciálisan a hibrid hadszíntér részese – akár tudja ezt, akár nem. Ebből következik a védekezés alaplogikája is: a reziliencia nem deklaráció kérdése, hanem képességkészleté, és ez a képességkészlet nem szűkíthető le az állami szervekre. A felkészítés, az intézményrendszer, a

[3] Ld. a szemantikai mezők időbeli torzulásának mérésére: InfocomJournal (2025), amely dinamikus szóbeágyazási modellekkel (Word2Vec) mutatta ki a COVID-19-hez kapcsolódó kifejezések kontextuális „mérgezését" a közösségi médiában – empirikus bizonyítéka a G–M–T–V lánc Mosás-fázisában végbemenő jelentéstorzulásnak.

[4] FALK, Barbara J. (2020): Strategic citizens: Civil society as a battlespace in the era of hybrid threats. Hybrid CoE Strategic Analysis, 25. sz. European Centre of Excellence for Countering Hybrid Threats, Helsinki. A szerző a „stratégiai tizedes" (strategic corporal) post-9/11 katonai fogalmát kiterjesztve vezeti be a „stratégiai polgár" koncepcióját: a hibrid hadviselés korszakában minden információs teret megosztó civil potenciálisan a hadszíntér részese, ezért a védekezés felelőssége nem korlátozható az állami szervekre.

[5] KRULAK, Charles C. (1999): Marines Magazine: The Strategic Corporal: Leadership in the Three Block War

szabályozás, a kommunikációs rutinok és a technológiai beavatkozás mind szükségesek – és mindegyiknek a polgárig kell érnie.

A reziliencia és az elrettentés kapcsolatát Sean Monaghan (2022) a Communication–Capability–Credibility (3C) pillérrendszerben operacionalizálta.[6] A 3C-modell lényege, hogy a hiteles visszatartás nem elegendő egyetlen pillérre: szükséges, hogy a kommunikáció (a szándékok és az értékek következetes közvetítése), a képesség (a reagálási eszköztár tényleges megléte) és a hitelesség (a következetes végrehajtás bizonyítéka a múltban és a jelenben) egyidejűleg fennálljon. Ha bármelyik pillér hiányzik – ha a kommunikáció nem hiteles, ha a képesség nem látható, ha a végrehajtás ellentmond a deklarált szándéknak –, az elrettentés megbukik. A disszertáció abból a felismerésből indul ki, hogy a kognitív dimenzió mélyreható megértése nélkül nem építhető stabil, 3C-kritériumoknak megfelelő nemzeti ellenálló képesség: amit nem értünk, azt nem tudjuk kommunikálni, és amit nem tudunk kommunikálni, azt nem tudjuk hitelesen szavatolni.

1.2. A tudományos probléma megfogalmazása: a Krím-félsziget 2014-es hatékony annektálása és a 2022-es ukrajnai orosz információs műveletek hatékonytalansága: stratégiai paradoxon

Hol húzódik a határ az egyszeri siker és a reprodukálható képesség között? A kutatás kiindulópontja egy hadtudományi értelemben vett stratégiai paradoxon: hogyan lehetséges, hogy 2014-ben az orosz információs műveletek stratégiai meglepetést tudtak előidézni, míg 2022-ben – azonos támadó fél és hasonló doktrinális háttér mellett – ez a stratégiai meglepetés a nyugati információs térben elmaradt?

Az orosz hadtudomány erre a paradoxonra nem tétovázik magyarázatot adni: nyíltan leírja azt, amit a nyugati elemzők csak utólag azonosítanak. Nyikolaj Bordyuzsa, a Kollektív Biztonsági Szerződés Szervezetének (KBSZSZ) főtitkára 2014 májusában így fogalmazta meg az információs hadviselés logikáját: „In information warfare, the side that tells the truth loses."[7], vagyis az

---

[6] MONAGHAN, Sean (2022): Deterring hybrid threats: Towards a fifth wave of deterrence theory and practice. Hybrid CoE Paper 12. European Centre of Excellence for Countering Hybrid Threats, Helsinki. Monaghan az elrettentés ötödik hullámát tárgyalva azonosítja a Communication–Capability–Credibility (3C) pillérrendszert: a hiteles visszatartás feltétele, hogy a kommunikáció (szándékok és értékek közvetítése), a képesség (reagálási eszköztár megléte) és a hitelesség (következetes végrehajtás bizonyítéka) egyidejűleg álljon fenn. A reziliencia ebben a keretben az elrettentés alapja, de önmagában nem stratégia.

[7] GILES, Keir (2016): *Russia's „New" Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power*. London: Chatham House, Russia and Eurasia Programme. 27. o. A fejezet mottójaként Giles Nyikolaj Bordyuzsát idézi, a Kollektív Biztonsági Szerződés Szervezetének (KBSZ) főtitkárát (2014. május 23.): „In

információs hadviselésben az a fél veszít, amelyik kimondja az igazat. Ez nem provokatív álláspont – ez műveleti önleírás. A cél nem az igazság bizonyítása, hanem a döntési környezet torzítása: ha az igazság elmondása is veszteség, akkor a védekezés logikája is alapvetően más kell legyen, mint a klasszikus cáfolat-alapú stratégiai kommunikáció. Az igazság közlése csupán a szimmetria illúzióját adja, miközben az aszimmetria a módszerben rejlik: a dezinformátor számára az eredmény mindegy, a cáfoló számára viszont az igazság egyszerre eszköz és korlát.

2014-ben, a Krím-félsziget annektálásakor az orosz információs műveletek képesek voltak a döntési láncok valódi bénítására.[8] A narratív koherencia – az üzenetek egységessége az összes csatornán egyszerre – és a csatornaszinkron olyan konfigurációt alkotott, amely az eseményeket kész helyzetként tudta beállítani, mielőtt az igazolás és az értelmezés megkezdődhetett volna.[9] A bizonytalanság nem melléktermék volt, hanem eszköz: mire a helyzet definíciója stabilizálódhatott volna, a műveleti cél teljesült. Brad Allenby (2017) elemzése fontos árnyalattal egészíti ki ezt a képet: az orosz fegyverként alkalmazott narratíva nem hozta létre az ukrán társadalmi törésvonalakat, hanem a már meglévőket élesítette – az ország kulturális kettéosztottságát, amelyben a keleti területek oroszbarát orientációja előzetesen adott volt.[10] Ebből következik a 2022-es helyzet egyik magyarázata is: egy kulturálisan konszolidálódó, a 2014–2021-es időszakban összeforrott Ukrajna más ellenállóképességet mutat, mint a 2014-es, még megosztott célpont. A fegyverként használható törésvonal megléte tehát előfeltétele a kognitív bénításnak – és ahol ez az előfeltétel nem áll fenn, ott a mechanizmus hatásfoka radikálisan csökken.

2022-ben, az Ukrajna elleni teljes körű invázió megindításakor ez a mechanizmus lényegesen kisebb hatásfokkal működött. A nyugati és az ukrán reziliencia növekedése, az OSINT-kultúra (Open Source Intelligence – nyílt forrású hírszerzés, vagyis az online elérhető nyilvános adatok – műholdképek, geolokált felvételek, közösségi média posztok – szisztematikus elemzése)

information warfare, the side that tells the truth loses." A kijelentés az orosz információs hadviselés doktrinális leírása: a cél nem az igazság megvédése, hanem a döntési környezet torzítása.

8 DARCZEWSKA, Jolanta (2014): The Anatomy of Russian Information Warfare: The Crimean Operation, A Case Study. OSW (Centre for Eastern Studies), Warsaw. 5. o.

9 GILES, Keir (2016): *Russia's „New" Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power*. London: Chatham House, Russia and Eurasia Programme. 37–38. o.

10 ALLENBY, Brad (2017): White Paper on Weaponized Narrative. Center on the Future of War, Arizona State University, June 2017. 3. o.

elterjedése és a platformszintű beavatkozások valós időben törték meg az orosz narratív dominanciát.[11] Az adaptációs kényszerpálya megfordult: ahol 2014-ben a minőségi narratívaépítés dominált, ott 2022-re az ipari léptékű zajkeltés és a figyelem-túlterhelés kerültek előtérbe. A mennyiség a minőség helyébe lépett – de nem egyenértékű kimenetekkel.

A 2022-es keresztmetszeti adatok ugyanakkor arra figyelmeztetnek, hogy a narratív „áttörés" (cross-medium breakout) – vagyis az a jelenség, amikor egy dezinformációs üzenet eléri, hogy a mainstream média maga kezdje közvetíteni – nem maradt el teljesen. A YouGov Cambridge Globalism Project 2022-es felmérése szerint Magyarországon a megkérdezettek 34%-a tartotta valószínűnek vagy biztosan igaznak az orosz narratívát az invázió jogosságáról – ez az EU-n belüli legmagasabb értékek közé tartozott.[12] Ez az adat egyszerre illusztrálja, hogy a fentebb feltételezett „meglepetésvesztés" nem abszolút: a narratív behatolás 2022-ben is mérhető volt egyes nemzeti kontextusokban. A különbség azonban szisztematikus: ahol a törésvonal előzetesen adott volt – kulturálisan, politikailag, intézményi szinten –, ott a kognitív bénítás sikeresebb maradt. Ahol a reziliencia felépült, ott a hatás megjelenési formája a teljes bénítástól a részleges polarizáció irányába tolódott.

A kognitív hatásmechanizmusok megértéséhez a dezinformáció hagyományos, tartalomközpontú vizsgálatán túl kell lépni. Maxime Lebrun (2023) a Hybrid CoE keretében kidolgozott kognitív intrúzió (cognitive intrusion) fogalma pontosan ezt az irányváltást teszi meg.[13] A kognitív intrúzió nem egyszerűen dezinformációt jelent – annál mélyebb beavatkozás. Az egyéni és kollektív mentális folyamatok szándékos manipulálása, amelynek célja a politikai erőszak előmozdítása a liberális demokratikus társadalmakban – vagyis az, hogy a befogadó a manipuláció hatására önként

---

11 KOFMAN, Michael – ROJANSKY, Matthew (2015): *A Closer Look at Russia's „Hybrid War"*. Kennan Cable, No. 7. Washington D.C.: Wilson Center, Kennan Institute. 5. o.

12 YouGov Cambridge Globalism Project (2022): Annual Survey on Global Issues. University of Cambridge / YouGov. A 2022-es felmérés adatai szerint Magyarországon a megkérdezettek 34%-a tartotta valószínűnek vagy biztosan igaznak az orosz narratívát az invázió jogosságáról – ez az EU-n belüli legmagasabb érték volt Görögország (39%) után. Az adat a Kreml-narratívák „áttörési" (cross-medium breakout) képességét illusztrálja a populáris konszenzus szintjén, és közvetlen relevanciával bír a H2 hipotézis árnyalásához.

13LEBRUN, Maxime (2023): Anticipating cognitive intrusions: Framing the phenomenon. Hybrid CoE Strategic Analysis 33. European Centre of Excellence for Countering Hybrid Threats, Helsinki.

cselekszik olyan módon, amely a manipulátor érdekét szolgálja. Lebrun három szintet különböztet meg: az első a félretájékoztatás kultúrája, amely termékeny kontextust teremt; a második az érzelmek – különösen a harag és a felháborodás – erőszakba való átcsatornázása, amellyel a közvélemény dezorientálódik; a harmadik maga az erőszak, amely a demokratikus közvetítési rendszert számolja fel. 2014-ben ez a mechanizmus pontosan az első és második szinten működött maximálisan: a döntési bénulás nem azzal jött létre, hogy az emberek „nem hittek el valamit", hanem azzal, hogy a helyzet értelmezéséhez szükséges érzelmi és kognitív kapacitásuk kimerült, mielőtt a cselekvési ablak bezárult volna.

A tudományos probléma magja a következő: mi magyarázza ezt a kimeneti különbséget, ha a támadó fél alapvető szándéka és doktrinális önértelmezése 2014 és 2022 között nem változott radikálisan? A geopolitikai magyarázatok, mint a felkészültség, vezető kommunikáció, szövetségi egység releváns tényezők, de önmagukban nem adnak kielégítő választ arra, hogy a műveleti mechanizmus miért működött másként. A disszertáció két, 2014 és 2021 között felerősödő magyarázó változót azonosít: egyrészt a technológiai ökoszisztéma eltolódását (platformlogikák, algoritmikus terjesztés, automatizált hálózatok, szintetikus tartalom), másrészt a társadalmi és intézményi reziliencia változását (COVID–19 infodémia-tapasztalat, tényellenőrzési és előzetes cáfolat rutinok, OSINT-kultúra, platformszintű fellépések). A két változó metszéspontját a disszertáció a fegyvernek minősülő kommunikáció transzformációs időszakaként tárgyalja.

A klasszikus propaganda-definíciók, bár részben alkalmazhatók, már nem elégségesek e jelenség leírásához. Ennek oka nem az, hogy a propaganda eltűnt, hanem az, hogy a digitális–platformalapú terjedésben a műveleti hatás egyre kevésbé magából az üzenetből, és egyre inkább a szervezettségből, a terjesztési architektúrából és a kognitív kimenetből áll össze. Jelen értekezés ezért bevezeti és következetesen alkalmazza a fegyvernek minősülő kommunikáció (FMK) fogalmát – amelynek részletes definíciója és operacionalizálása a 2. fejezetben található.

A fegyverré tett narratívák kognitív rögzülését Gilles Fauconnier mentális terek elmélete[14] teszi diagnosztizálhatóvá. Fauconnier szerint a befogadó nem állításokat tárol izoláltan, hanem részlegesen felépített gondolati konstrukciókat – mentális tereket – rétegez egymásra, és ezek között megfeleltetéseket (mappings) hoz létre a megértés során. A döntéshozó tehát nem egy-egy

[14] FAUCONNIER, Gilles (1997): Mappings in Thought and Language. Cambridge University Press.

igaznak vagy hamisnak minősített állítás alapján cselekszik, hanem a számára alapértelmezetté vált mentális tér alapján. A műveleti hatás sokszor nem az üzenet igazságán múlik, hanem azon, hogy melyik mentális tér válik alapértelmezetté, és mely megfeleltetések rögzülnek. A kognitív dimenzióban a csapás sokszor nem egy állítás igaz/hamis voltán keresztül működik, hanem a következtetéseken és reakciókon keresztül. Azt éri el, hogy a célpont a bizonyítékot is gyanúként, a cáfolatot is manipulációként, az intézményi közlést is érdekként olvassa.[15] Ez a bizalmi infrastruktúra megbontása – és ennél nincs hatékonyabb kognitív fegyver.

A kutatási rés ennek megfelelően két szinten jelenik meg. Fogalmi és módszertani szinten: a fegyverminőség operacionalizálása a szakirodalomban gyakran hiányzik, vagy az elemzések a jelenséget túl tág kategóriákba sorolják (propaganda, dezinformáció, PSYOPS), ami nehezíti a két eset rögzített változók szerinti összevetését. Empirikus és időbeli szinten az irodalomban kevéssé kerül fókuszba a 2014–2021 közötti transzformációs időszak, amelyben egyszerre erősödött fel a platformkormányzás és a társadalmi igazolási fegyelem iránti igény, miközben a COVID–19 időszak infodémiája a kognitív túlterhelés és a bizalomválság globális tapasztalatát adta.

1.3. Terminológiai megjegyzés és fogalmi meghatározás: a mérhetőség előfeltétele

A fogalmi tisztánlátás nem nyelvjáték. Ez a mérhetőség és az operatív alkalmazhatóság előfeltétele – vagyis annak, hogy a disszertáció ne csupán jelenségeket írjon le, hanem diagnosztizálhasson, összehasonlíthasson és ajánlásokat fogalmazhasson meg. Ahol a fogalmak elmosódnak, ott az elemzés is elmosódik, nem lehet mérni azt, amit nem lehet megkülönböztetni.

A közbeszédben elterjedt „álhír” (fake news) fogalma tudományos elemzésre ma már alkalmatlan, mert egyszerre fed le véletlen tévedést, szatírát és tudatosan koordinált állami, vagy nem állami eredetű kognitív támadást. Ha mindhárom ugyanaz a szó, akkor a védekezés is egybemosódik: az oktatásalapú megközelítés helyes a véletlenre, de teljesen hatástalan a koordinált stratégiai beavatkozásra. A terminológiai rendszerezés ezért hadtudományi, és egyben tudományos igény.

[15] SCHIFF, Kaylyn Jackson – SCHIFF, Daniel S. – BUENO, Natália S. (2023): The Liar’s Dividend: Can Politicians Claim Misinformation to Evade Accountability? Research Paper. 2–3. o. és 8–10. o.

A disszertáció Claire Wardle és Hossein Derakhshan (2017) információs zavarok (information disorder) keretrendszerét alkalmazza alapkategóriaként.[16] A keretrendszer két független tengely – a szándék és a valóságtartalom – metszéspontján három élesen elkülöníthető kategóriát azonosít. A téves informálás (misinformation) olyan hamis vagy pontatlan tartalom, amelyet terjesztője nem szándékosan ártó céllal oszt meg. Ide tartoznak a jóhiszemű tévedések, a félreértett adatok, a szatírát valós hírként kezelő megosztások. A dezinformáció (disinformation) ezzel szemben szándékosan előállított, tudatosan kártékony tartalom, amelynek célja a megtévesztés és az ellenség döntési folyamatainak befolyásolása. A rosszindulatú információ (malinformation) az előző kettőtől eltérően valós tartalmakra épül – például kiszivárogtatott dokumentumokra, privát levelezésre, valódi felvételekre –, amelyeket kontextusból kiragadva, szándékosan ártó céllal terjesztenek: a lejáratás, a zsarolás és a polarizáció eszközeként.

E hármas megkülönböztetés kritikus az operacionalizálás szempontjából.[17] A téves informálásra (misinformation) az edukáció az elsősorban releváns válasz: ha az emberek felismerik a tévedést, megszüntetik. A dezinformáció (disinformation) esetén a szándékos, sokszor ipari méretű megtévesztéssel állunk szemben, itt a tényellenőrzés (fact-checking) és a platform-integritási intézkedések a releváns eszközök. A rosszindulatú torzítás (malinformation) az igazán nehéz eset, mert a terjesztett adat technikailag igaz, a pusztítást maga a kontextusból való kiragadás végzi el, és a hagyományos tényellenőrzési rutinok erre szinte hatástalanok. A disszertáció azért alkalmazza ezt a hármat egymás mellett, mert az orosz információs műveletek 2014-től 2022-ig mindhárom formát szimultán alkalmazták – és az egyes formákra adott védekezési válasz eltér egymástól.

A fegyvernek minősülő kommunikáció (FMK; weapon-grade communication) olyan kommunikációs műveleti termék, amely szándékos, szervezett és kognitív hatást céloz. Nem

---

16 WARDLE, Claire – DERAKHSHAN, Hossein (2017): Information Disorder: Toward an Interdisciplinary Framework for Research and Policymaking. Council of Europe Report DGI(2017)09. 20. o. A szerzők az információs zavarokat három kategóriára osztják a szándék és a valóságtartalom metszetében: misinformation (téves, de szándékolt ártalom nélkül), disinformation (hamis, szándékoltan kártékony) és malinformation (valós tartalom, szándékolt ártalom céljával, kontextusból kiragadva). E felosztás intézményi jogalkotási alapja lett az EU dezinformáció-ellenes keretrendszerének.

17 NOLAN, Susan A. – KIMBALL, Michael (2021): The Intent Behind a Lie: Mis-, Dis-, and Malinformation. Psychology Today, 2021. december 22. A szerzők a Wardle–Derakhshan taxonómiát közérthető formában operacionalizálják: a misinformation (szándékolatlan tévedés), a disinformation (szándékos megtévesztés) és a malinformation (valós, de ártó szándékú kontextusváltás) hármas felosztása az első lépés a megfelelő jogi, technológiai és oktatási válaszok allokálásához.

párbeszéd, hanem műveleti hatáskiváltás – torzítás, túlterhelés, bénítás, polarizáció. Ez a definíció három, egymást erősítő kritériumon nyugszik: (1) szándékoltság (proxyk alapján kikövetkeztethető ártó szándék), (2) szervezettség (koordinált infrastruktúra, nem organikus terjedés), (3) kognitív hatás (a döntési ciklus torzítása, nem szükségszerűen egyetlen állítás elfogadtatása). Az FMK tehát a Wardle–Derakhshan taxonómián belül a dezinformáció és a malinformation metszéspontján helyezkedik el – azzal a lényeges többlettel, hogy nem a tartalmat, hanem a művelet kimenetét és a szervezettséget emeli ki kritériumként. A teljes operacionalizálás a 2. fejezetben található.

Fontos elhatárolás, hogy az FMK nem azonos Brad Allenby és Joel Garreau (2017) „fegyveresített narratíva" (weaponized narrative) koncepciójával.[18][19] Allenby és Garreau az identitás, önkép és valóságértelmezés aláásását helyezi középpontba. Ez szélesebb, szociológiai kategória, amely magában foglalja a társadalom egészét érő narratív nyomás hosszú távú hatásait is. Az FMK ezzel szemben szűkebb és hadtudományi szempontból operacionalizálhatóbb. A döntéshozatali ciklus torzítására és a kognitív kimenet mérhetőségére fókuszál, miközben a terjesztési architektúrát és a koordináltságot is definíciós kritériumként emeli be. Az FMK tehát nem retorikai újranevezés, hanem a meglévő jelenség szűkítése és instrumentalizálása: azt vizsgálja, mikor válik egy kommunikációs aktus auditálhatóan műveleti termékké.

A hitelesség-eltérítés (credibility hijacking) a bizalmi horgonyok – személy, intézmény, arculat, hang, bizonyító erejű videó – eltérítése vagy kihasználása manipulációs céllal. A cél nem a szebb üzenet, hanem a hitelességi jelzők átírása. Az ingercsomag többcsatornás, multimodális üzenet-összeállítás, amely egyszerre több érzékszervre és értelmezési sémára hat: nem egyetlen üzenet, hanem összehangolt inger-konfiguráció.

A terminológiai rendhez kapcsolódik a jelölésrend szétválasztása is. A strukturált, fókuszált összehasonlítás (SFÖ; Structured, Focused Comparison – SFC) a kutatás módszertani gerince:

[18] ALLENBY, Brad – GARREAU, Joel (2017): Weaponized Narrative: The New Battlespace. Center on the Future of War, Arizona State University. 1–48. o.

[19] NISSEN, Thomas Elkjer (2016): *Social Media's Role in 'Hybrid Strategies'*. NATO Strategic Communications Centre of Excellence, Riga. Nissen hat komponenst különböztet meg a közösségi média weaponization-modelljében: célzás, felderítés, kiberműveletek, pszichológiai műveletek, védelmi műveletek, és irányítás-vezetés.

lehetővé teszi két eset összevetését rögzített kérdéssor mentén.[20] Ezzel szemben a Helyzet–Előrejelzés–Irányítás (H–E–I) logika a diagnosztikai és mérési bontás eszköze. A műveleti jelenséget a helyzetkép, a várható pályák és a beavatkozási opciók rögzítésével teszi összehasonlíthatóvá. Az SFÖ azt mondja meg, mit kérdezek mindkét esetben ugyanúgy; a H–E–I azt, mivel és milyen jelölésrendben mérem.

1.4. Szakirodalmi iránytű: hadtudomány – kommunikációelmélet – platformökológia

Terminológiai megjegyzésként jelzem, hogy ez az alfejezet nem teljes körű szakirodalmi szintézis – az a 3. fejezetben található. Ez egy iránytű: megnevezi a három domináns értelmezési tengelyt, amelyre a disszertáció épít, és kijelöli azt a kutatási rést, amelyre válaszolni kíván.

A hadtudományi tengelyen a kognitív dimenzió mint tartós műveleti környezet értelmezése a meghatározó. A 21. századi biztonsági környezetben a konfliktusok súlypontja egyre láthatóbban az információs és kognitív dimenzió felé tolódik. Az informális konfrontáció nem epizodikus kísérőjelenség, hanem tartós műveleti tér. Keir Giles[21] ezt a logikát nem kommunikációs mellékszálként, hanem az orosz hatalomgyakorlás következetes eszközcsoportjaként írja le. Resperger István[22] a hazai fogalmi rögzítést adja, a hibrid eszköztár kombinált alkalmazás, ahol a nem-kinetikus komponensek önállóan képesek kezdeményezést és tempót létrehozni. Haig Zsolt[23] a kiber- és kognitív dimenzió összekapcsolását végzi el, a kibertéri műveletek hálózatos infokommunikációs rendszereken keresztül közvetlen kognitív és közvetett technikai hatásokat válthatnak ki. E gondolatmenetet a hazai hadtudományi irodalomban Kovács is megerősíti, amikor az információs műveletek céljaként a célközönség szándékára, helyzetértelmezésére és képességeire gyakorolt kognitív hatást jelöli meg.[24]

---

[20] GEORGE, Alexander L. – BENNETT, Andrew (2005): Case Studies and Theory Development in the Social Sciences. MIT Press / BCSIA Studies in International Security. 83. o.

[21] GILES, Keir (2016): *Russia's „New" Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power*. London: Chatham House, Russia and Eurasia Programme. 38–39. o.

[22] RESPERGER István (2018): A válságkezelés és a hibrid hadviselés. Dialóg Campus Kiadó, Budapest. 22. o.

[23] HAIG Zsolt (2018): Információs műveletek a kibertérben. Dialóg Campus Kiadó, Budapest. 16. o.

[24] Kovács László (2023): *Hadviselés a 21. században: kiber műveletek.* Budapest: Ludovika. 102. o.

A kommunikációelméleti tengelyen a kognitív mechanizmusok, heurisztikák és túlterhelés vizsgálata kerül előtérbe. Daniel Kahneman kettős folyamat elmélete[25] az emberi gondolkodást két, egymással versengő rendszer modelljén írja le. Az 1-es rendszer gyors, automatikus, heurisztikus és érzelmi alapú. Ez az a folyamat, amellyel pillanatok alatt ítéletet alkotunk anélkül, hogy tudatosan mérlegelnénk. A 2-es rendszer lassú, deliberatív, analitikus és energiaigényes. Az FMK kognitív hadviselési logikájának szempontjából a kulcskérdés az, hogy milyen terhelés mellett omlik össze a kontrollált (2-es rendszerbeli) feldolgozás, és adja át a helyét az automatikusnak. Ha a bemeneti ingertömeg meghaladja a 2-es rendszer kapacitásküszöbét, a befogadó nem képes ellenőrizni, mérlegelni és cáfolni – az 1-es rendszer heurisztikái és érzelmi reflexei veszik át az irányítást. Ez nem emberi gyengeség, hanem biológiai erőforrás-gazdálkodás, amelyet a kognitív hadviselés pontosan mint sérülékenységet fegyveresít.

A platformökológiai tengelyen a láthatóság, skálázás, visszacsatolás és a hihetőség infrastruktúrájának megváltozása a meghatározó. W. Lance Bennett és Alexandra Segerberg[26] konnektív cselekvés (connective action) kerete azt írja le, hogyan szerveződik a politikai mobilizáció a digitális hálózatokban és miért válik ez műveleti kockázattá. A klasszikus kollektív cselekvéssel szemben, ahol egy szervezet közös üzenetet közvetít, a konnektív cselekvésben az egyén saját keretezésével oszt meg tartalmakat, amelyek hálózati szinten összegyűlve koordináció nélküli koordinációt hoznak létre. Nincs szükség központi irányítóra ahhoz, hogy egy narratíva egységesen terjedjen: elegendő, ha a platformlogika (algoritmikus rangsorolás, megosztási mechanizmusok, visszacsatolási hurkok) kedvez neki. Ebből következik a hadtudományi tét: a befolyásolási műveletek nem csupán tartalmakat injektálnak az információs térbe, hanem a hálózati önszerveződés logikáját fegyveresítik. Az üzenet maga lehet gyenge – de ha a platformarchitektúra felerősíti, a hatás aránytalanul nagy lesz.

A konnektív cselekvés elméletének hadtudományi kiterjesztése a memetikus hadviselés (memetic warfare) koncepciója, amelyet Jeff Giesea (2015/2021) a NATO StratCom COE keretében

[25] KAHNEMAN, Daniel (2013): Thinking, Fast and Slow. Farrar, Straus and Giroux. 16., 22. o.

[26] BENNETT, W. Lance – SEGERBERG, Alexandra (2012): The Logic of Connective Action: Digital Media and the Personalization of Contentious Politics. Information, Communication & Society, 15. évf. 5. sz. 739–768. o. DOI: 10.1080/1369118X.2012.670661

alapozott meg.[27] Giesea definíciója szerint a memetikus hadviselés „versengés a narratíváért, az eszmékért és a társadalmi kontrollért a közösségi média hadszínterén" – tehát nem puszta trollkodás, hanem az információs műveletek digitálisan natív változata. A mém – a kulturálisan rezonáns, könnyen terjeszthető, érzelmileg töltött egység – ebben az értelemben nem humoros kép, hanem kognitív lőszer: olyan formátum, amelynek terjesztése nem igényel tudatos döntést, mert a platform ajánlórendszere automatikusan amplifikálja. Ahogy Giesea fogalmazott: ha a propaganda és a nyilvános diplomácia a memetikus hadviselés konvencionális formái, akkor a trollkodás és a pszichológiai műveletek annak gerilla-változatai. A hadtudományi relevancia pontosan abban áll, hogy a memetikus logika a Bennett–Segerberg-féle konnektív struktúrát szándékolt célra irányítja: koordináció nélkül koordinált narratív erőt állít fel.

Christopher Paul és Miriam Matthews[28] hazugság tűzoltótömlő (firehose of falsehood) modellje rögzíti, hogy a nagy volumen és a többcsatornás, gyors, ismétlő terítés nem egyszerűen terjesztési technika, hanem kognitív terhelési mechanizmus. A metafora szándékosan vulgáris: a tűzoltótömlő nem céloz, hanem áraszt. Az orosz propaganda ebben a keretben szakít a klasszikus meggyőzés azon szabályával, hogy a hazugságnak konzisztensnek és hihetőnek kell lennie – ehelyett a mennyiségi fölényre és a folyamatos ismétlésre épít. Az ellentmondások nem gyengítik, hanem erősítik a hatást, mert a befogadó kognitív kapacitása kimerül a szétválogatásban, és feladja az ellenőrzést. A műveleti kimenet nem a meggyőzés, hanem a döntési környezet elszennyezése: ha elegendő egymásnak ellentmondó állítás kering egyszerre, a befogadó nem tud koherens helyzetképet alkotni, és a cselekvőképessége csökken.

Robert Chesney és Danielle Citron[29] deepfake-kerete azt mutatja meg, hogy a szintetikus média megjelenése nem csupán egy új hamisítási technikát jelent, hanem a bizalom infrastruktúráját rombolja szét rendszerszinten. A deepfake – mesterséges intelligenciával generált,

---

[27] GIESEA, Jeff (2015/2021): It's Time to Embrace Memetic Warfare. In: Memetic Warfare: Echoes from the Past, Visions of the Future. NATO Strategic Communications Centre of Excellence, Riga. Giesea a memetikus hadviselést a „versengés a narratíváért, az eszmékért és a társadalmi kontrollért a közösségi média hadszínterén" meghatározással vezette be. Elemzésében a propaganda és a nyilvános diplomácia a memetikus hadviselés konvencionális formái, a trollkodás és a pszichológiai műveletek pedig annak gerilla-változatai.

[28] PAUL, Christopher – MATTHEWS, Miriam (2016): The Russian „Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It. RAND Corporation. 1–5. o.

[29] CHESNEY, Robert – CITRON, Danielle (2019): Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. California Law Review, 107. évf. 1754., 1785. o.

hiperrealisztikus hang- vagy videófelvétel, amelyen egy valódi személy mondja vagy teszi azt, amit valójában sohasem mondott vagy tett – első ránézésre egyszerű tényhamisítási eszköz. A valódi hadtudományi veszélye azonban más irányból érkezik: ha a közönség tudja, hogy léteznek meggyőző deepfake-ek, akkor a valódi, kompromittáló felvételeket is hamisítványnak lehet titulálni. A hitelességi jelzők elveszítik rendszerszintű funkciójukat, mert a bizonyítás és a cáfolat rutinjai egyaránt megkérdőjelezhetővé válnak.

Ez a mechanizmus 2022-ben empirikusan demonstrálódott. Március elején egy deepfake-videó terjesztésével Zelenszkij ukrán elnök látszólag arra szólítja fel a katonákat, hogy tegyék le a fegyvert – a videó az orosz közösségimédia-hálózatokon és egyes ukrán platformokon is megjelent, mire az ukrán StratCom-csapat perceken belül hitelesített cáfolatot adott ki, Zelenszkij saját videójával. Párhuzamosan a Doppelgänger-művelet keretében neves nyugati lapok – a Le Monde, a Der Spiegel, a The Guardian – vizuálisan szinte tökéletesen lemásolt klónoldalakon közölt orosz narratívákat tartalmazó „cikkek" terjesztésével próbálta a hitelesség-eltérítés mechanizmusát eszközre váltani. Mindkét esetben a formátum maga volt a fegyver: nem a tartalom meggyőző volta, hanem a hitelességi jelzők (az elnök arca és hangja, a lap fejléce és tipográfiája) eltérítése. A 6. fejezetben ezeket részletesen elemzem; az 1.4-ben csupán az elméleti keretet illusztrálják: a hazugok osztaléka lett az elnevezése a 2022-ben dokumentált és megismétlődő műveleti mintázatnak.

A három tengely közös metszete kijelöl egy kritikus kutatási rést: léteznek erős doktrinális és empirikus megközelítések a 2014-es krími fókuszhoz, és külön irodalmak a kognitív hatásmechanizmusokra és a platformökológiára – ritkább azonban az olyan empirikusan tesztelhető keret, amely a 2014–2021 közötti technológiai és platformkormányzási transzformációt magyarázó változóként beépíti a 2014-es és 2022-es összevetésbe. A disszertáció ezt a hiányt kívánja pótolni. A fenti tengelyek irodalmának részletes, kritikai szintézise – beleértve a genealógiai ívet, a megtévesztés evolúcióját és a szubliminális befolyásolás kérdéskörét – a 3. fejezetben (Szakirodalmi áttekintés) található.

1.5. Kutatási célkitűzések, kutatási kérdések és hipotézisek

A fenti probléma megválaszolása érdekében a disszertáció öt egymásra épülő célt tűz ki.

Az első cél a fogalmi elhatárolás: a fegyvernek minősülő kommunikáció (FMK; weapon-grade communication) egzakt hadtudományi definíciójának rögzítése és elhatárolása a hagyományos propagandától, a dezinformációtól (disinformation) és a nyilvános diplomáciától (public diplomacy), a műveleti hatáskiváltás logikájának középpontba állításával.

A második cél a komparatív elemzés: strukturált, fókuszált összehasonlítás (SFÖ) keretében a 2014-es krími és a 2022-es ukrajnai információs műveleti kimenetek különbségeinek elemzése, azonos kérdéskészlettel és rögzített indikátorokkal.

A harmadik cél a környezeti változók feltárása: a 2014–2021 közötti fegyvernek minősülő kommunikáció transzformációs időszakának (bridge period) értelmezése – különösen a COVID–19 infodémia reziliencia-növelő hatásainak, valamint a platformkormányzási és automatizációs tényezők erősödésének magyarázó változóként való beemelése.

A negyedik cél az elméleti modellalkotás: a védekezés (Irányítás/Control) dimenziójának tudományos megalapozása az emberi információfeldolgozás (Human Information Processing – HIP) pszichológiai korlátaiból levezetett OxIPO-modell keretrendszerének integrálásával.

Az ötödik cél a gyakorlati hasznosulás: egy multimodális reziliencia-mátrix (Multimodal Resilience Matrix – MRM) megalkotása, amely a hadsereg (StratCom), az állam (szabályozás) és az egyén (kognitív higiénia) szintjén is mérhetővé és alkalmazhatóvá teszi a védekezést.

A célokhoz igazodva a disszertáció négy kutatási kérdésre keresi a választ.

Az első kutatási kérdés (KK1): milyen objektív kritériumok mentén különíthető el a fegyvernek minősülő kommunikáció a szélesebb propaganda- és dezinformációs tértől a vizsgált esetekben?

A második kutatási kérdés (KK2): milyen strukturális különbségek azonosíthatók a 2014-es krími annektálás és a 2022-es ukrajnai orosz invázió kommunikációs műveleti környezetében a terjedési infrastruktúra, a platformkormányzás és a társadalmi reziliencia szempontjából?

A harmadik kutatási kérdés (KK3): milyen szerepet játszik a 2014–2021 közötti transzformációs időszak – különösen a COVID–19 időszak kognitív stresszteszt jellege – a 2022 utáni kommunikációs hatásmechanizmusok kialakításában?

A negyedik kutatási kérdés (KK4): milyen diagnosztikai és beavatkozási keret (H–E–I mátrix, OxIPO-modell, Multimodális Reziliencia Mátrix) képes a két eset összevetését mérhető–tanítható–alkalmazható módon a gyakorlat nyelvére fordítani?

A kutatási kérdések megválaszolására a disszertáció négy, egymást kiegészítő és cáfolható hipotézis mentén épül fel. A cáfolhatóság hangsúlyozása nem puszta módszertani formula: a disszertáció számol azzal, hogy egyes hipotézisek részleges cáfolatot is hozhatnak – ez tudományosan éppoly értékes, mint a teljes megerősítés.

Az első hipotézis (H1) – a doktrinális integráció és bénítás hipotézise: a 2014-es krími művelet során az orosz fél által alkalmazott magas narratív koherencia és csatornaszinkron sikeresen idézett elő döntésképtelenséget és kognitív bénultságot (cognitive paralysis) a krími területen, valamint az EU és a NATO szövetségesek között, amelyet a nyugati technológiai aszimmetria és a lassú reakcióidők tettek lehetővé.

A második hipotézis (H2) – a meglepetés elvesztésének hipotézise: 2022-ben a bénító hatás a megtámadott félben elmaradt, mert a nyugati és ukrán reziliencia növekedése, az OSINT-kultúra elterjedése és a platformszintű beavatkozások valós időben törték meg az orosz narratív dominanciát, adaptációs kényszerpályára állítva a támadót. A hipotézis nem abszolút érvényű: az 1.2-ben tárgyalt YouGov-adatok arra figyelmeztetnek, hogy a narratív hatás bizonyos nemzeti kontextusokban – köztük Magyarországon – kimutatható maradt, különösen ott, ahol az előzetesen meglévő törésvonalak megnövelték a fogékonyságot.

A harmadik hipotézis (H3) – a reziliencia-tanulás hipotézise: a COVID–19 infodémia globális kognitív hadgyakorlatként működött; a társadalom és az intézményrendszer ekkor sajátította el azokat a védekezési rutinokat (tényellenőrzés, pre-bunking, kommunikációs protokollok), amelyek 2022-ben részben immunizálták az információs teret bizonyos dezinformációs mintázatokkal szemben. A H3 ugyanakkor kétirányú tézis: a COVID-csatornák nem csupán védelmi tanulást hoztak, hanem a dezinformációs infrastruktúra fennmaradását is igazolják. Az EDMO (European Digital Media Observatory) dokumentálta,[30] hogy az összeesküvés-elméleti csoportok és az

[30] European Digital Media Observatory (EDMO) (2022): Coordinated Information Operations in the Context of the War in Ukraine. EDMO Task Force Report. Az EDMO dokumentálta, hogy a COVID-19 dezinformációs csatornák – összeesküvés-elméleti csoportok, oltásellenes mozgalmak – 2022 után zökkenőmentesen átálltak pro-Kreml Ukrajna-narratívákra. Ez bizonyítja, hogy a Híd-időszak alatt kiépített dezinformációs infrastruktúra nem

oltásellenes mozgalmak csatornái 2022 után zökkenőmentesen fordultak pro-Kreml Ukrajna-narratívák felé – ugyanazok a terjesztési hálózatok, perszóna-portfóliók és validálási rétegek képesek voltak egy új narratívát hordozni. Ez azt jelenti, hogy a COVID-időszak nem egyszerűen megerősítette a védekezést, hanem a támadói infrastruktúra számára is tesztkörnyezetként és bejáratott csatornarendszerként szolgált. A H3 helyes értelmezése tehát kettős: a védekezői oldal tanult, de a támadói oldal is megőrizte és transzferálta a képességeit.

A negyedik hipotézis (H4) – a kognitív nihilizmus és volumen-paradoxon hipotézise: a generatív mesterséges intelligencia (GenAI) és az automatizált terjesztés 2022 utáni alkalmazása nem elsősorban a stratégiai meggyőzés minőségét, hanem a műveleti zajszintet és a kognitív túlterhelést növelte meg, eltolva a támadó stratégiai céljait a tartós polarizáció és a valóságérzékelés felszámolása irányába. A H4 kulcsfogalma a kognitív nihilizmus: az az állapot, amelyben a célszemélyek esetében nem az a cél, hogy egy konkrét hazugságot higgyenek el, hanem hogy ne higgyenek többé az igazság megismerhető voltában. Ha semmit nem lehet biztosan tudni, nincs miért cselekedni. A 6. fejezet elemzése alapján ez a folyamat háromfázisú pszichológiai ívben írható le: a mobilizációs szakaszban (2022–2023) a kognitív műveletek cselekvésre ösztönöztek, a demobilizációs szakaszban (2024–2025) a passzivitás kiváltása lett a cél, a kognitív nihilizmus mint végállapot pedig az igazság fogalmának felszámolását célozza – a Liar's Dividend-mechanizmus (A hazug osztaléka-mechanizmus) maximalizálásával.[31] Módszertani megjegyzés: a H4 a négy hipotézis közül empirikusan a leginkább vitatható – a mennyiségi és a stratégiai hatékonyság közötti összefüggés nem-lineáris. A disszertáció e hipotézist alátámasztott, de nem teljes bizonyossággal lezárható következtetésként kezeli.

1.6. Kutatási módszerek és kutatási terv: SFÖ mint összehasonlítási módszer, H–E–I mint diagnosztika

A disszertáció módszertani gerincét a hadtudomány, a kommunikációelmélet és a kognitív pszichológia interdiszciplináris szintézise adja. A cél egy olyan integrált keretrendszer, amely az

témaspecifikus, hanem transzferálható: ugyanazok a terjesztési hálózatok, perszóna-portfóliók és validálási rétegek egy új narratívát is képesek hordozni.

[31] SCHIFF, K. J. – SCHIFF, D. S. – BUENO DE MESQUITA, B. (2023): The Liar’s Dividend. SocArXiv.

információs műveleteket nemcsak leírhatóvá, hanem mérhetővé és objektívan összehasonlíthatóvá teszi.

A kutatási terv alaplogikája a strukturált, fókuszált összehasonlítás (SFÖ; Structured, Focused Comparison – SFC) modellje.[32] A módszer strukturált, mert a 2014-es és a 2022-es esettanulmányok elemzése azonos, előre rögzített kérdéssor mentén történik – így az összevetés nem utólagos narratív párhuzamkeresés, hanem kontrollált összehasonlítás. Fókuszált, mert a vizsgálat kizárólag a kommunikációs hatásmechanizmusokra koncentrál, és nem vállalkozik a kinetikus hadműveletek teljes körű bemutatására. Ez a módszertan biztosítja, hogy a két eltérő időpontban és technológiai környezetben zajló konfliktushelyzet közötti kimeneti különbségeket magyarázható változók eredményeként lehessen bemutatni.

Az SFÖ-ben feltett kérdések operacionalizálását a H–E–I-mátrix adja. A Helyzet-dimenzió a műveleti tér bemeneti pillanatfelvétele: aktorok, csatornaszinkron, narratív koherencia, szervezettség foka. Az Előrejelzés-dimenzió a folyamatdinamika és a várható hatásmechanizmusok leírása: adaptációs idő, reakciósebesség, kognitív túlterhelés, bénulás vagy polarizáció valószínűsége. Az Irányítás-dimenzió a művelet stratégiai kimenete, valamint a beavatkozási és védekezési lehetőségek: intézményi ellenállóképesség, platformszintű szabályozás, visszacsatolási hurkok. A részletes indikátorkészlet a 2. fejezetben kerül kibontásra.

A forrásbázis több rétegből épül fel: tudományos szakirodalom; nyílt forrású elemzések (OSINT); intézményi és szakmai jelentések; valamint forráskritikai kezeléssel – nyilvánosságra került belső dokumentumok és szivárogtatások. Utóbbiakat nem kész tényként, hanem indikátorként kezelem: a szervezettség, a szándékoltság és az erőforrás-nyomok feltárásában lehetnek relevánsak, de minden állítás csak triangulációval – legalább két egymástól független forrástípus általi megerősítéssel – válik megtarthatóvá. A módszertani fegyelem egyik kulcsa ez: a bizonyítéklánc (chain of evidence) dokumentált és védhetőkell, hogy legyen.

A szándékoltság kérdése a kognitív dimenzióban különösen érzékeny: a kommunikációban a befogadó természeténél fogva szándékot tulajdonít, de tudományos vizsgálatban ez nem lehet puszta benyomás. A disszertáció ezért proxyk mentén közelít: célközönség jelölhetősége,

[32] GEORGE, Alexander L. – BENNETT, Andrew (2005): Case Studies and Theory Development in the Social Sciences. MIT Press / BCSIA Studies in International Security. 101. o.

ismétlődő mintázatok, csatornaszinkron és erőforrás-nyomok, forrás-eltakarás vagy hitelesség-horgonyok eltérítése, koordinációt valószínűsítő hálózati jelenségek. Ebből következik az is, hogy egy-egy állítás bizonyossági foka expliciten jelölve van – különbséget teszek az alátámasztott és a valószínűsített következtetések között.

1.7. A kutatás határai és korlátai

A vizsgált kognitív és információs tér komplexitása miatt a kutatás érvényességének biztosítása szigorú lehatárolásokat követel meg. Mindhárom tematikai, földrajzi és módszertani határt előre rögzítem.

Tematikai lehatárolás: a dolgozat nem hadtörténeti kronológia. A kinetikus események részletes leírása csak annyiban jelenik meg, amennyiben az a kommunikációs térben és a döntési helyzetekben közvetlenül releváns. A kutatás nem kód-szintű kiberanalízis: a kiberhadviselés technikai részletei nem képezik az értekezés tárgyát. A fókusz a kommunikációs és pszichológiai hatáskiváltáson van – azon a következményláncon, amelyben a műveleti termékek (narratívák, ingercsomagok, hitelességi jelzők) mérhető kimeneteket hoznak létre. A terminológiai és taxonómiai rend (Wardle–Derakhshan) azért szükséges előfeltétel, mert a mérhetőség csak akkor garantálható, ha a kutatás végig ugyanazt érti ugyanazon a szón.

Földrajzi és aktor-lehatárolás: a vizsgálat elsődlegesen az Oroszországi Föderáció információs műveleteire koncentrál az európai, ukrán és észak-amerikai információs térben. Más szereplők – például a Kínai Népköztársaság – csak a globális trendek szintjén jelennek meg. Az időbeli lehatárolás két csomópontra épül: a krími eseményekre (2014) és az Ukrajna elleni teljes körű invázió időszakára (2022–2025), a két pont közötti transzformációs időszakot (2014–2021) pedig magyarázó hídként kezeli.

Módszertani korlátok: a platformadatok hozzáférhetősége részben korlátozott, a moderáció és az ajánlórendszer logikájának teljes transzparenciája nem adott (black box jelenség), és a konfliktushelyzetekben megjelenő tartalmak egy része gyorsan eltűnik vagy nehezen archiválható (data void). Ezt az adatvesztési kockázatot a kutatás a forrásbázis diverzifikálásával, a triangulációs szabályokkal és a dokumentált bizonyítéklánccal kezeli. Rögzítem azt is, ami ebből nem következik: a disszertáció nem állítja, hogy az FMK az egyetlen vagy domináns tényező a 2014 és

2022 közötti kimeneti különbségben. Csupán azt állítja, hogy az FMK-mechanizmus – a két magyarázó változóval együtt – szükséges és auditálható részét képezi a magyarázatnak.

A normativitás kerülése külön rögzítendő: a disszertáció leíró–elemző és diagnosztikai célú. A mechanizmusok, kockázatok és beavatkozási lehetőségek objektív feltárása a cél, nem politikai értékítélet-alkotás. A vizsgálat logikája a „mi működik, milyen feltételek mellett, és milyen kimenettel" kérdésirányra épül. Az, hogy egy kommunikációs jelenség fegyvernek minősül, nem normatív ítélet, hanem műveleti diagnózis.

1.8. Várt eredmények, tudományos érték, hasznosulás és az értekezés felépítése

A disszertáció várható tudományos hozzájárulása négy, egymásra épülő kimenetben ragadható meg.

A fogalmi hozzájárulás az FMK olyan egzakt, hadtudományi definíciójának rögzítése, amely élesen elhatárolható a propagandától és az általános dezinformációtól, tartalmi elemzés helyett közvetlenül a műveleti hatásokhoz kapcsolható, és a meglévő „weaponized narrative" irodalomhoz képest operacionalizálható szűkítést és mérhető kritériumokat kínál. Ez a hozzájárulás a Wardle–Derakhshan taxonómia hadtudományi adaptálásán keresztül egyszerre illeszkedik a nemzetközi terminológiai rendhez és tölt be eredeti, az FMK-ra specifikusan alkalmazott definíciós funkciót.

A módszertani hozzájárulás az SFÖ kutatási terv és a H–E–I diagnosztikai logika összekapcsolása, amely két eltérő időpontban mutatkozó műveleti állapot objektív összevetését teszi megalapozottá, következetes szempontkészlettel. Ehhez kapcsolódik az OxIPO-modell kognitív mechanizmus-magyarázatként való alkalmazása, amely az emberi információfeldolgozás pszichológiai logikájának hadtudományi adaptálását jelenti. A keresztmetszeti összehasonlítás eredményeit a disszertáció a FMK Kognitív Olló modelljében (7. fejezet) szintetizálja. Ez az eredeti elméleti konstrukció a technológiai volumen és a stratégiai hatékonyság eltérő pályaívét írja le, és prediktív keretet kínál a kognitív hadviselés 2025 utáni fejlődési irányainak értékeléséhez.

Az empirikus hozzájárulás a 2014-es és 2022-es eset azonos kérdéskészletű elemzése, és a stratégiai kimeneti különbségek – a paradoxon – magyarázata a 2014–2021 közötti kommunikációs és környezeti átalakulással (híd-időszak). A COVID-csatornák transzferálhatóságának dokumentálása, a kognitív nihilizmus operacionalizálása és a 3C-pillérrendszer alkalmazása a reziliencia mérésére mind ezt az empirikus dimenziót gazdagítják.

Az operatív hozzájárulás a védekezési keret: az OxIPO-modell szemléletéből levezetett és egy multimodális reziliencia-beavatkozási csomag megalkotása mikro–mezo–makro bontásban – egyén, szervezet, állam –, amely a hadsereg (StratCom), az állam (szabályozás) és az egyén (kognitív higiénia) szintjén is alkalmazható. A stratégiai polgár koncepciójával összhangban ez az operatív keret nem csupán katonai vagy intézményi, hanem a civil–katonai interfészen átívelő beavatkozás-logikát kínál.

A gyakorlati hasznosulás szempontjából a dolgozat kifejezett célja, hogy a fegyvernek minősülő kommunikáció felismerése és kezelése ne ad hoc reakciók alapján, hanem mérhető indikátorok és szigorúan dokumentált bizonyítéklánc alapján történjen. A rögzített módszertan lehetővé teszi, hogy a disszertáció eredményei tréninganyagok, intézményi eljárásrendek vagy nemzeti reziliencia-keretek formájában is közvetlenül felhasználhatók legyenek a biztonságpolitikai döntéshozatalban.

Az értekezés a definíció → diagnózis → mérés → beavatkozás láncolatára épül, kilenc fejezetben. Az 1. fejezet (jelen fejezet) rögzíti a kutatási kontextust, a tudományos problémát, a célkitűzéseket, a hipotéziseket és a fogalmi és tartalmi lehatárolásokat. A 2. fejezet (Kutatási módszertan) operacionalizálja az FMK definíciót, az SFÖ kutatási módszertant és a H–E–I indikátorrendszert. A 3. fejezet (Szakirodalmi áttekintés és fogalmi keretrendszer) a vonatkozó nemzetközi és hazai elméletek kritikai szintézisét adja – genealógiától a szubliminális befolyásolás kérdéséig. A 4. fejezet a Krím-félsziget annektálásának műveleti hatékonyságát írja le. Az 5. fejezet a műveleti környezet iparosodását, a COVID–19 reziliencia-hatást és a platformszabályozás ébredését tárgyalja magyarázó változókként. A 6. fejezet (Ukrajna, 2022–2025) a hiperrealisztikus technológiák zajkeltő hatását és az adaptációs kényszerpályát elemzi. A 7. fejezet (Keresztmetszeti összehasonlítás) az azonos indikátorkosár alapján szintetizálja a két esetet. A 8. fejezet (Szintézis és védekezés) az Irányítás-dimenzió operatív keretét és az MRM gyakorlati alkalmazását mutatja be. A 9. fejezet (Összegzés és kitekintés) tételesen értékeli a hipotéziseket, rögzíti az új tudományos eredményeket és kijelöli a 2030-ig várható fenyegetettségi trendeket.

Az értekezés végső célja egyszerűen megfogalmazható: a kognitív dimenziót ne biztonságpolitikai metaforaként, hanem auditálható és mérhető műveleti térként kezeljük. Olyan térként, ahol a technológia gyorsít, a reziliencia fékez – és ahol a szigorú fogalmi fegyelem vezet el a gyors helyzetfelismeréshez, amely a 21. századi hibrid védekezés legfőbb előfeltétele.

2. KUTATÁSI MÓDSZERTAN

A disszertáció elméleti és szakirodalmi alapjait – a hadtudományi genealógiát, a kognitív sebezhetőség mechanizmusait, a technológiai környezet alakulását és a fegyvernek minősülő kommunikáció (FMK) fogalmi keretrendszerét – a 3. fejezet dolgozza fel. Jelen fejezet feladata ennélfogva nem az elméleti szintézis, hanem a kutatás módszertani architektúrájának levezetése: annak bemutatása, hogy a disszertáció milyen eszközökkel, milyen logikai rendben és milyen alátámasztási követelményekkel teszi összehasonlíthatóvá a 2014-es és 2022-es esettanulmányokat.

A fejezet felépítése deduktív láncolat: minden alfejezet az előző korlátjából vezeti le a következő eszköz szükségességét. Az összehasonlítási kutatási terv (SFÖ) adja a kutatás szerkezetét; a diagnosztikai rács (H–E–I) az operatív kérdéssort; az FMK-rács a helyzet-rögzítés sémáját; az OxIPO-modell a kognitív mechanizmus-magyarázatot; a Multimodális Reziliencia Mátrix (MRM) pedig a beavatkozás-tervezés keretét. A fejezet zárásában a forráshierarchia és a triangulációs szabályok rögzítik az evidencia elfogadásának feltételeit. Ami nem támasztható alá, visszaminősítésre kerül.

2.1. A módszertani architektúra levezetése: a „miért éppen ez?” kérdésre adott válasz

A disszertáció alapvető módszertani dilemmája a következő: miként tehető tudományosan összehasonlíthatóvá a 2014-es krími művelet – amely egy zárt, humán-intenzív, manuálisan koordinált információs offenzíva volt – a 2022-ben kezdődő háborúval, ahol az információs műveleteket már ipari léptékű automatizáció, generatív tartalomelőállítás és platformszintű koordináció jellemzi? A két eset eltérő ökoszisztémában zajlik: 2014-ben szűkösebb a valós idejű nyílt adat, gyengébb a platformtranszparencia és későn keményedik fel az intézményi diagnosztika; 2022-ben ezzel szemben erős OSINT-közösség, részletesebb platformjelentések és gyorsabb többcsatornás terjedés a jellemző. Ha ezt a két esetet kronologikus elbeszélésként mutatnám be, az összevetés szükségszerűen benyomás szintű maradna – és ez a tudományos igényű elemzés számára nem elfogadható.

Erre a problémára a választ egy ötszintű, egymásból következő módszertani architektúra adja. Minden szint az előző korlátjából fakad – vagyis nem tetszőlegesen összeválogatott eszközökről van szó, hanem deduktív láncolatról.

Az első szint a strukturált, fókuszált összehasonlítás (SFÖ; Structured, Focused Comparison – SFC). George és Bennett (2005) módszertana biztosítja, hogy a két fő esettanulmányt (Krím 2014, Ukrajna 2022–) és a közöttük húzódó transzformációs időszakot (2014–2021) ne ad hoc narratív párhuzamkeresésként, hanem kontrollált összehasonlításként vizsgáljam: azonos kérdéssort alkalmazok mindkét esetre, és a különbségeket azonos dimenziók mentén vezetem le. Az SFÖ tehát a kutatás koncepciója – de önmagában nem adja meg a mérés nyelvét.

A második szint a Helyzet–Előrejelzés–Irányítás (H–E–I) diagnosztikai rács. Az SFÖ kérdéssora három, egymásra épülő kérdés csoportra bontható: Mi történt a kognitív térben? (Helyzet), Milyen kognitív kimenetek voltak valószínűsíthetők? (Előrejelzés), és Hol és mivel lehetett volna beavatkozni? (Irányítás). A H–E–I tehát nem önálló módszer, hanem az SFÖ operatív kérdéssora – az a nyelv, amelyen a két eset összehasonlítható válaszokat ad. A saját korábbi kutatásaimban[33] rögzítettem: a H–E–I rács egyszerre diagnózis és döntési segédlet, mert nemcsak leír, hanem kijelöli a beavatkozási pontokat is.

A harmadik szint az FMK-rács (Fegyvernek Minősülő Kommunikáció rács). A H–E–I Helyzet-dimenziójának konkretizálására szolgál: minden esetben ugyanazon konfigurációs metszetben (aktor–csatorna/infrastruktúra–műveleti termék) rögzítem a vizsgált jelenséget. Vízszintes tengelyén az operatív kérdések állnak (Ki csinálja? Hol/hogyan jut el? Mi a műveleti termék?), függőleges tengelyén a hadtudományi hierarchia (ökoszisztéma → művelet → taktika → technika). Az FMK-rács nem új elmélet, hanem rögzítő eszköz: megakadályozza, hogy 2014-ben a technikai részletekbe, 2022-ben pedig az ökoszisztéma-szintű keretekbe csússzon át a leírás. A saját korábbi kutatásaimban[34] ezt a hierarchiát tizenkét esettanulmányon validáltam a szándék–csatorna–kognitív hatás metszetében. A rács jobb szélső oszlopa – „tipikus cél/kimenet” – a 2014-es esetnél elegendő a kognitív következmények jelzésére: a döntési bénulás és a bizalom rombolás a csatornaszinkron általános hatásaként áll elő, nem egyetlen modalitás célzott támadásaként. A

[33] HORVÁTH, Dávid (2025): Communication Classified as a Weapon and Generative Artificial Intelligence as Information Overload: Situation–Forecast–Control (S–F–C) Indicators and Multimodal Resilience Matrix in the OxIPO Model. *OxIPO – Interdiszciplináris tudományos folyóirat*, 7(4), 23–48. Online: https://doi.org/10.35405/OXIPO.2025.4.23

[34] HORVÁTH Dávid (2025): When Artificial Intelligence Generated Content Becomes Weapon-Grade Communication. *Mesterséges Intelligencia – interdiszciplináris folyóirat*, 7(2), 77–98. Online: https://doi.org/10.35406/MI.2025.2.77

2022-es esettanulmánynál azonban ez az oszlop korlátossá válik: amikor a generatív mesterséges intelligencia lehetővé teszi, hogy a támadó egyidejűleg és differenciáltan célozzon szöveges (értelmezési szűkület), vizuális (bizonyíték-illúzió), auditív (bizalmi rövidzár) és videóalapú (bénító sokk) feldolgozási utakat, a „tipikus cél/kimenet" oszlopot az FMK-mátrix szándék–csatorna-konfiguráció–kognitív hatás hármasával szükséges kibővíteni. Az FMK-mátrix tehát nem más eszköz – a rács evolúciója, amelyet a technológia kikényszerít.

A negyedik szint az OxIPO-modell (Organization × [Input + Process + Output]). A H–E–I Előrejelzés-dimenziója mechanizmus nélkül nem lenne több, mint utólagos kommentár. Mező Ferenc és Mező Katalin eredeti keretrendszerét[35] a kutatás a fegyvernek minősülő kommunikáció kognitív hatásmechanizmusára adaptálja: az FMK-rácsban rögzített konfigurációt (műveleti termék + csatorna + ritmus + hitelességi díszletek) a befogadói feldolgozás láncába helyezem. A kérdés így nem az, hogy egy állítás igaz vagy hamis, hanem az, hogy milyen bemeneti terhelés (Input) keletkezik, milyen feldolgozási rövid utak (Process) valószínűsödnek, és milyen kimenetek (Output) következhetnek – túlterhelés, torzítás, polarizáció, bénultság. A modern fegyvernek minősülő kommunikáció célja gyakran nem a meggyőzés, hanem a feldolgozási lánc megbontása, ahol a döntés minőségét az információfeldolgozás állapota és terhelhetősége határozza meg Giannopoulos szerint.[36]

Az ötödik szint a Multimodális Reziliencia Mátrix (MRM). A H–E–I Irányítás-dimenziója konkrét beavatkozási pontok nélkül közhelyes ajánlássá válna. Az MRM a beavatkozási lehetőségeket három dimenzió mentén rendezi: szint (mikro/egyéni – mezo/szervezeti – makro/állami), eszköztípus (technikai, jogi, kommunikációs) és modalitás (szöveg, kép, hang, videó). Ez utóbbi dimenzió azon a felismerésen alapul, hogy a generatív mesterséges intelligencia korszakában a védekezés nem lehet egy modalitású: más kontrollpont kell a szöveges manipulációhoz, a képi bizonyíték-illúzióhoz, a hangklónozáshoz és a videóalapú bénításhoz.

---

35 MEZŐ Ferenc – MEZŐ Katalin (2019): *Az OxIPO-modell – az interdiszciplináris kutatások egy lehetséges értelmezési kerete*. OxIPO – interdiszciplináris tudományos folyóirat, 2019/1. sz. 9–21. o.

36 GIANNOPOULOS, Georgios et al. (2021): *The Landscape of Hybrid Threats: A Conceptual Model*. JRC Technical Report, European Commission / Hybrid CoE.

A láncolat ok-okozati: SFÖ nélkül a dolgozat narratív szétcsúszásra hajlamos; H–E–I nélkül az SFÖ kérdéssora túl absztrakt; FMK-rács nélkül a Helyzet-dimenzió helyzetképe nem stabil; OxIPO nélkül az Előrejelzés értelmezése utólagos; MRM nélkül az Irányítás beavatkozási része közhelyes. A módszertani építkezés logikája tehát nem „öt eszköz felsorolása", hanem a probléma fokozatos operacionalizálása – ahol minden szint a megelőző szint korlátjából fakad, és a következő szintet szükségessé teszi.

A kutatás szerkezete ebből a módszertani logikából következik. A két fő esettanulmány (Krím 2014, Ukrajna 2022–) közötti időszakot – a 2014-es Krím-félsziget annektálását követő, 2021 végéig tartó periódust – a disszertáció transzformációs időszakként kezeli. Ez nem önálló esettanulmány, mert nem egyetlen trigger-esemény szervezi, hanem többféle technológiai, doktrinális és intézményi fejlemény halmozódása: a platformökológia átalakulása, az automatizáció terjedése, a szabályozási környezet keményedése és a COVID–19 időszak alatt világszinten tesztelt kognitív reziliencia rutinok[37]. A transzformációs időszak módszertani szerepe tehát magyarázó változó: megmutatja, milyen feltételek változtak meg 2014 és 2022 között, amelyek a kimeneti különbséget értelmezhetővé teszik.

2.2. Kutatási módszertan: Strukturált, Fókuszált Összehasonlítás (SFÖ)

A disszertáció kutatási tervének és elméleti-módszertani gerincének alapját a Strukturált, Fókuszált Összehasonlítás (Structured, Focused Comparison – SFÖ) módszertana képezi. Alexander L. George és Andrew Bennett amerikai politológusok és a nemzetközi kapcsolatok elismert szakértői által megalkotott esettanulmány-módszertan[38] bizonyítja, hogy ez az eljárásrend kivételesen alkalmas az olyan nemzetbiztonsági és hadtudományi anomáliák vizsgálatára, ahol a rendelkezésre álló esetszám determinisztikusan alacsony (kis N-számú kutatás), ugyanakkor az incidenseket befolyásoló technológiai és pszichológiai változók száma kiugróan magas, a műveleti kontextus pedig sokrétű.

---

[37] SZICHERLE Patrik – KREKÓ Péter (2020): *Burjánzanak az álhírek a koronavírus nyomában*. Political Capital, Budapest. 3–8. o. A COVID- dezinformáció magyarországi megjelenési mintáinak elemzése.

[38] GEORGE, Alexander L. – BENNETT, Andrew (2005): *Case Studies and Theory Development in the Social Sciences*. MIT Press, Cambridge, MA.

A választott módszertan strukturált jellegű, mert tudatosan elveti a hagyományos, ad-hoc jellegű történeti narrációt és a puszta kronológiai leírást. Ehelyett minden kiválasztott esettanulmányhoz (Krím 2014, illetve Ukrajna 2022–2025) pontosan ugyanazt a szigorúan rögzített, standardizált kérdéssort intézi, garantálva ezáltal a szisztematikus, reprodukálható és kutatói torzításoktól mentes adatgyűjtést. Továbbá a módszer fókuszált, mivel nem törekszik a fegyveres konfliktusok kinetikus hadműveleteinek vagy az átfogó diplomáciai történetnek a teljes körű rekonstrukciójára. Figyelmét célzottan kizárólag azokra a kognitív, információs és platform-architekturális dimenziókra szűkíti le, amelyek közvetlenül, ok-okozati szinten relevánsak a kutatás elején megfogalmazott (H1–H4) hipotézisek igazolása vagy cáfolhatósága szempontjából.

A vonatkozó 1. táblázat: A Strukturált, Fókuszált Összehasonlítás (SFÖ) rögzített kérdéskészlete címmel a mellékletek között található.

2.2.1. Az esettanulmányok kiválasztásának logikája

A kutatási kérdések tudományos megválaszolásához a disszertáció két fő esettanulmányra, valamint egy, a kettőt szervesen összekötő, magyarázó híd-időszakra – a 2014-es krími annektálást követő, 2021 végéig tartó transzformációs periódusra – építi fel az érvelését. A kutatás végpontjának (2025) kijelölése a disszertáció lezárásának évéhez igazodik, biztosítva a legfrissebb hozzáférhető forenzikus adatok integrálását:

- Krím (2014): A sikeres stratégiai meglepetés és a „kézműves” hibrid hadviselés modern őspéldája. Ebben a műveletben a kognitív támadás technológiai és automatizációs szintje (a mai, generatív modellekhez képest) alacsony volt, a stratégiai bénító hatásfok és a dezorientáció azonban maximális eredményt ért el.

- Híd-időszak (2014–2021) mint Környezeti Változó (a disszertáció szinonimaként a transzformációs periódus kifejezést is használja): Ez a szakasz metodológiailag nem önálló SFÖ-esettanulmányként szerepel, hanem a független változók (a technológiai platformok ökológiája és a társadalmi reziliencia) transzformációs folyamatának leírásaként funkcionál. Ebben a kritikus szakaszban jelenik meg a COVID–19 infodémia mint a globális társadalmak kognitív stressztesztje, valamint a kiszivárgott Vulkan-iratok által bizonyított orosz információs automatizáció (botnetek) állami szintű, ipari kiépülése.

A Híd-időszak elemzése két pilléren nyugszik. Az első az Anchor-mérföldkövek sora: azok a technológiai, módszertani és szervezeti ugráspontok, amelyek a G–M–T–V lánc egyes elemeit minőségileg változtatták meg (pl. az Internet Research Agency (IRA) ipari trollfarmja a Terítés skálázhatóságát, a Cambridge Analytica botrány a Mosás adatvezérelt formáját, a deepfake technológia a Generálás automatizáltságát). A második a Reziliencia-mérföldkövek sora: az EU-szabályozási lépcsők, a platform-integritási intézkedések (nem hiteles magatartás - Coordinated Inauthentic Behavior, CIB eltávolítása), az OSINT/tényellenőrzési hálózatok kiépülése, a NATO/Hybrid CoE diagnosztikai kapacitások és a szivárgás-alapú bizonyítékcsomagok (Surkov-levelek, Vulkan-iratok). E kétpilléres struktúra biztosítja, hogy az 5. fejezet a magyarázó változókat funkcionálisan – a támadás-védekezés aszimmetrikus spiráljaként –, ne pedig kronológiai narratívaként elemezze.

- Ukrajna (2022–2025): Az adaptációs kényszer és az ipari léptékű kognitív zajkeltés klasszikus esettanulmánya. A 2022-ben indult teljes körű orosz invázió kognitív kísérőműveleteiben a technológiai fegyveresítés szintje (generatív MI, kiterjedt és polimorf botnetek) történelmi csúcsot ért el, ugyanakkor a stratégiai meglepetés és a döntéshozói paralízis (a 2014-es Krímmel ellentétben) elmaradt. A kutatás fundamentális paradoxona pontosan ezen a kimeneti különbségen és technológiai aszimmetrián alapul.

2.2.2. Adatforrások és az összehasonlíthatóság validitása

A kutatás során kezelt adatforrások kapcsán egy kritikus módszertani korlátot, egyben sajátosságot kell rögzíteni: a vizsgált két végpont (2014 és 2022) között az elérhető adatok szerkezete erősen aszimmetrikus. Ennek elsődleges oka a digitális környezet és a technológiai elszámoltathatóság gyors evolúciója. Míg a 2022-es ukrajnai háború idején a kutatók számára már rendelkezésre állnak a globális technológiai vállalatok (Meta, Microsoft, Google) valós idejű kiberfenyegetettségi jelentései (Adversarial Threat Reports), valamint az Európai Unió által jogilag kikényszerített átláthatósági adatbázisok (DSA Transparency Database), addig a 2014-es krími műveletek idején ezek az iparági transzparencia-sztenderdek még egyáltalán nem léteztek. Ez utóbbi történelmi időszakot a strukturált platformadatok hiánya, azaz az „adatvákuum” (Data Void; ld. 3. fejezet) jellemzi.

Az objektív összehasonlíthatóság biztosítása és a tudományos érvényesség (validitás) megőrzése érdekében a kutatás a bizonyítéklánc felépítése során a metodológiai trianguláció, azaz a kettős verifikációs alapelvét alkalmazza:

- Állandó összehasonlítási alap (sarokpont): A két, időben távoli esettanulmány közötti analitikus folytonosságot a NATO Stratégiai Kommunikációs Kiválósági Központja (NATO StratCom COE), a helsinki székhelyű Európai Hibrid Fenyegetések Elleni Kiválósági Központ (Hybrid CoE), valamint a független, nyílt forrású hírszerzési (OSINT) szervezetek, mint a Bellingcat kiterjedt jelentései biztosítják. Utóbbi intézmény – ahogy azt Maxime Lebrun európai biztonságpolitikai elemző a kognitív beavatkozások (cognitive intrusions) értékelési keretrendszerében[39] rögzíti – mindkét korszakban azonos katonai-műveleti és pszichológiai fókusszal vizsgálta az orosz[40] információs beavatkozásokat . Mivel a vizsgáló entitás intézményi logikája és a kódolási módszertan megbízhatóan állandó, a kinyert adatok torzításmentesen összevethetők.

- Funkcionális megfeleltetés (Proxy adatok): A hiányzó 2014-es nyers platform-adatokat a disszertáció a korszakban készült, legmagasabb evidenciaszintű tudományos rekonstrukciókkal pótolja. E tekintetben a Prof. Philip N. Howard kanadai-amerikai szociológus által vezetett Oxford Internet Institute Computational Propaganda Project (Számítógépes Propaganda Projekt) retrospektív hálózatelemzései szolgálnak proxy (helyettesítő) adatként a 2014-es orosz bot-hálózatok működésének leírásához[41]. Bár ezek a kutatások nem a konfliktus pillanatában kiadott valós idejű iparági jelentések, tudományos funkciójukban pontosan ugyanazt a forenzikus hálózati és algoritmikus leírást adják meg, mint az évekkel későbbi Meta fenyegetettségi jelentések.

A gyakorlat nyelvére fordítva: a disszertáció a 2014-es utólagos, kvalitatív kutatási rekonstrukciókat és a 2022-es valós idejű, kvantitatív platform-naplóállományokat nem egymás

---

39 LEBRUN, Maxime (2023): *Anticipating cognitive intrusions: Framing the phenomenon*. Hybrid CoE Strategic Analysis 33. European Centre of Excellence for Countering Hybrid Threats, Helsinki. 3–7. o.

40 NATO STRATCOM COE (2015) / LANGE-IONATAMIŠVILI, Sanda és mtsai: *Analysis of Russia's Information Campaign against Ukraine*. NATO Strategic Communications Centre of Excellence, Riga. 3–10. o.

41 HOWARD, Philip N. – KOLLANYI, Bence (2016): *Bots, #StrongerIn, and #Brexit: Computational Propaganda during the UK-EU Referendum*. Oxford Internet Institute, Oxford University.

ellenében, és nem is egymást kizáró módon használja. Az általam kidolgozott H–E–I (Helyzet–Előrejelzés–Irányítás) indikátorrendszer megfelelő alkalmazásával ezt a két, forrásában és formátumában eltérő adathalmazt egy közös diagnosztikai nyelvre fordítom le. Ez az absztrakciós lépés teszi lehetővé az eltérő történelmi korszakok kognitív műveleti termékeinek egzakt, tudományos igényű összehasonlítását.

2.2.3. Forráshierarchia és triangulációs szabályok

A kutatás bizonyítási módszere háromszintű forráshierarchián nyugszik, amelynek belső logikája a következő bizonyítéklánc-követelményt követi. Az első szint az intézményi és stratégiai dokumentumoké: a NATO StratCom COE, az Európai Külügyi Szolgálat (EEAS), a RAND Corporation, az Europol és a nagy technológiai platformok fenyegetettségi jelentései adják a stabil definíciós és tipológiai keretet. A második szint a független kutatói esettanulmányoké: az Oxford Internet Institute, a Stanford Internet Observatory, a DFRLab és a Hybrid CoE elemzései adják a módszertan belső szerkezetét – az adatgyűjtés és kódolás menetét. A harmadik szint az OSINT/SOCMINT korpusz: mikroszintű nyomok, archív mentések, vizuális és hálózati elemek, amelyeket a Bellingcat típusú nyílt forráskódú hírszerzési közösségek dokumentálnak.

A következtetések érvényessége a három szint konvergenciáján áll vagy bukik. A trianguláció módszertani szabálya: ha a három szint konvergál, a megállapítás megtartható; ha nem konvergál, a minősítés visszalép. Ezt a logikát „nem tudom kapunak” nevezem: ha az attribúció, a csatorna-koordináció vagy a szervezettségi szint nem támasztható alá, nem erőltetem a kategorizálást, hanem a bizonytalanságot jelölöm. Ez biztosítja, hogy az elemzés ne ráhúzott narratíva, hanem transzparens és auditálható evidencialánc legyen.

2.3. A diagnosztikai eszköz: A H–E–I mátrix operacionalizálása

A strukturált, fókuszált összehasonlítás (SFÖ) előzőekben bemutatott módszertani kerete önmagában csak a kutatási irányt és a logikai felépítést jelöli ki, azonban nem adja meg a forenzikus mérés precíz eszközét. Ahhoz, hogy a 2014-es (Krím) és a 2022-es (Ukrajna) esettanulmányok összevetése ne ragadjon le az esszészerű, szubjektív történeti leírás szintjén, a kutatásnak szüksége van egy standardizált indikátorkészletre. Ez a mérőműszer hivatott arra, hogy mindkét történelmi időszakban azonos logikával tudja megragadni és kódolni a sokszor láthatatlan információs műveleti eseményeket.

A disszertáció a mérés és a kódolás elvégzésére a saját fejlesztésű Helyzet–Előrejelzés–Irányítás (H–E–I) diagnosztikai mátrixot alkalmazza. A mátrix koncepcionális újítása, hogy egyetlen, integrált „szupermodellként" funkcionál, amely a klasszikus hadtudományi műveletтervezés logikája mentén fogja össze a kutatás három másik, specifikus almodelljét. Ez a keretrendszer teszi lehetővé, hogy a kognitív hadműveleteket bemeneti (Input), folyamat (Process) és kimeneti (Output) szinten is mérhető változókra bontsuk.

A vonatkozó 2. táblázat: A Helyzet–Előrejelzés–Irányítás (H–E–I) diagnosztikai mátrix indikátorai címmel a mellékletben található.

2.3.1. A Helyzet-dimenzió (Situation): az információs zaj szűrése az FMK-ráccsal

A diagnosztikai mátrix első oszlopa a Bemenet (Input) feltérképezését végzi, arra a kérdésre válaszolva, hogy mit látunk a vizsgált információs térben. Ezen a szinten az elsődleges mérőszám a Narratív Koherencia és Szinkronizáció. A változó azt értékeli, hogy a támadó aktor által elindított dezinformációs narratíva milyen mértékben őrzi meg tematikus egységét a széttagolt platformökológiában. Peter Pomerantsev és Michael Weiss Oroszország-szakértők az információs műveletekről szóló tanulmányukban[42] rögzítik: egy koordinált fegyverként ható kommunikáció egyik legbiztosabb forenzikus bizonyítéka, ha a hierarchiailag és tulajdonosát tekintve látszólag teljesen független csatornák szinte ezredmásodperces szinkronban, azonos vizuális keretezéssel kezdik el sulykolni ugyanazt az esemény magyarázatot. A Helyzet-dimenzió második kulcsindikátora a Volumen és Amplifikáció (a mesterséges terjesztés aktivitási szintje).

A gyakorlat nyelvére fordítva: mielőtt ezeket az indikátorokat érdemben mérni lehetne, a kutatásnak ontológiailag is el kell döntenie, hogy a vizsgált jelenség valóban kognitív fegyver-e, vagy csupán organikus társadalmi zaj. Ennek a kritikus Helyzet-dimenziós szűrésnek a feladatát a saját fejlesztésű FMK-rács (Fegyvernek Minősülő Kommunikáció-rács) látja el, amely a szándékosság, a szervezettség és a hatás tengelyei mentén validálja a bemenetet. Az FMK-rács metodológiájának részletes kibontására a diagnosztikai modellt bemutató következő, önálló alfejezetben kerül sor.

[42] POMERANTSEV, Peter – WEISS, Michael (2014): *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*. The Institute of Modern Russia, New York.

2.3.2. Az Előrejelzés-dimenzió (Forecast): a kognitív támadás motorja és az OxIPO-modell

A mátrix második dimenziója a kognitív és műveleti Folyamat (Process) dinamikájára fókuszál, vagyis azt prognosztizálja, mi lesz ebből kognitív szinten. A szakasz legfontosabb technológiai indikátora az Adaptációs Idő, amely a konfliktusban részt vevő felek reflexeit méri.[43] Keir Giles , a londoni Chatham House biztonságpolitikai kutatója az orosz doktrína elemzésekor[44] rámutat, hogy a hibrid hadviselésben a stratégiai információs fölény (information superiority) sosem állandó, garantált állapot; a győzelem mindig a gyorsabb alkalmazkodási ciklus (OODA-hurok) függvénye.

A folyamat-dimenzió társadalomlélektani indikátora a Kognitív Túlterhelés. Ez a paraméter kizárólag a célcsoportban (emberi tényező) bekövetkező károkra fókuszál: a társadalmi polarizáció növekedésére, az intézményi bizalom zuhanására, valamint a kognitív apátia megjelenésére. Utóbbi során a befogadó – az információbőség súlya alatt összeroppanva – már nem keresi az igazságot, és hajlamos lesz a George Orwell által „duplagondolnak" (doublethink) nevezett állapot felvételére.

Ezek a pszichológiai és neurológiai torzulások nem esetlegesek, hanem egy jól strukturált mechanizmus eredményei. Ennek az Előrejelzés-dimenzióban zajló belső, kognitív folyamatnak (vagyis hogy pontosan miként vezet a bemeneti inger-túlterhelés a feldolgozási paralízisig, majd a torzult cselekvésig) a tudományos magyarázatát az OxIPO-modell biztosítja, amely a későbbiekben külön alfejezetben kerül részletes elemzésre.

2.3.3. Az Irányítás-dimenzió (Control): a védekezés operacionalizálása és az MRM

A mátrix lezáró szakasza a művelet realizálódott Kimenetét (Output) és az arra adott védekezési kontrollmechanizmusokat veszi górcső alá, azt a kérdést vizsgálva, hogy hova és mivel avatkozunk be. Itt az elsődleges indikátor a hálózati Visszacsatolási Hurkok (Feedback Loops) megléte. Egy

---

[43] SPILIOPOULOS, Leonidas (2025): *Robust Deterrence and Actor Rationality*. NATO Strategic Communications Centre of Excellence, Riga. 6., 9. o. A tanulmány az axiomatikus és ökológiai racionalitás közötti különbséget alkalmazza az elrettentés kontextusára: a „gyors és takarékos heurisztikák" (fast-and-frugal heuristics) az aszimmetrikus többszereplős környezetben hatékonyabban működhetnek, mint a klasszikus optimalizálási modellek.

[44] GILES, Keir (2016): *Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power*. London: Chatham House, Russia and Eurasia Programme.

fejlett információs művelet sosem egyirányú; a támadó folyamatosan méri a közönség elköteleződési (engagement) statisztikáit, és a begyűjtött adatok alapján valós időben finomhangolja a következő üzenethullámot. A mátrixot – és egyben a műveletet – a Stratégiai Hatásfok indikátora zárja. Ezt a legnehezebb objektíven kvantifikálni, ugyanakkor katonai és politikai szempontból ez a legdöntőbb elem, hiszen ez mutatja meg, sikerült-e elérni a stratégiai meglepetést vagy a döntéshozatal megbénítását.

Amikor az irányítás (védekezés) dimenziójába lépünk, a hagyományos, szoftver-alapú kibervédelmi megközelítések (mint a tűzfalak) elégtelennek bizonyulnak, hiszen a támadás a humán tényezőt célozza. Éppen ezért a H–E–I mátrix ezen kimeneti fázisához szorosan kapcsolódik a válaszcsapások és a reziliencia integrált rendszere, a Multimodális Reziliencia Mátrix (MRM). Az MRM hivatott arra, hogy a védekezést egyéni (mikro), szervezeti (mezo) és szabályozói (makro) szinteken operacionalizálja. Ezen védelmi architektúra struktúráját a módszertani blokk végén, önálló fejezetrészben fejtem ki részletesen.

2.4. Az FMK-rács a helyzet-dimenzió értelmezésében

Az előző alfejezet rögzítette, hogy a Helyzet-dimenzió elsődleges feladata az ontológiai szűrés: a vizsgált jelenség valóban fegyvernek minősülő kommunikáció-e, vagy csupán organikus társadalmi zaj? Az alábbiakban ezt a szűrést az FMK-rács kétlépcsős rendszerében – előbb zsilip, majd konfigurációs mátrix – bontom ki. A kétlépcsős logika célja a módszertani fegyelem: az első lépcső (zsilip) eldönti, hogy a jelenség egyáltalán a kutatás hatókörébe tartozik-e; a második lépcső (konfigurációs rács) a zsilipet átlépő jelenség strukturális leírását végzi el – ugyanazon séma szerint minden vizsgált időszakban, biztosítva az összehasonlíthatóságot.

2.4.1. Az FMK-ontológiai szűrő, a zsiliprendszer

A vizsgált kommunikációs eseménynek az FMK-rács ontológiai szűrőjén, azaz a módszertani zsiliprendszer mindhárom tengelyén magas értéket kell elérnie ahhoz, hogy kognitív fegyverként és így az esettanulmányok releváns tárgyaként legyen értelmezhető. A zsiliprendszer első dimenziója a szándékosság (intentionality), amely a károkozási szándékot vizsgálja. Míg a téves információ (misinformation) megosztása mögött a felhasználó részéről nincs ártó szándék, a fegyvernek minősülő kommunikáció kifejezetten a társadalmi kohézió megbontására, a bizalom erodálására vagy az ellenfél döntéshozatali ciklusának megzavarására irányul, még abban az

esetben is, ha valós tényeken alapul, mint a malinformation jelensége során. A kutatás folyamatában a szándékosságot elsősorban a kontextus manipulálása és a célzott időzítés, például egy választás vagy egy válsághelyzet kritikus pillanatában történő narratíva-indítás igazolja. A szűrő második, legkönnyebben kvantifikálható dimenziója a szervezettség és koordináltság (organization and coordination), amely a hálózati végrehajtásra fókuszál. A spontán pletykákkal ellentétben a fegyvernek minősülő kommunikáció mögött minden esetben tetten érhető egy parancsnoki és irányítási (command and control – C2) struktúra vagy egy összehangolt technológiai infrastruktúra. A diagnosztika során a koordináltság indikátorai közé tartozik a több, látszólag független csatornán, így az állami médiában, a proxy oldalakon és a bot-hálózatokon azonos időpontban megjelenő, megegyező narratíva, valamint a nem-valódi viselkedés (coordinated inauthentic behavior – CIB) magas aránya a terjesztési folyamatban. A zsiliprendszer harmadik pillére a hatás (impact), amely a kimeneti következményeket méri. Egy kommunikációs aktus akkor minősül módszertanilag fegyvernek, ha annak következményei túlmutatnak egy szűk véleménybuborék (echo chamber) keretein, és elérik a kognitív vagy fizikai tér stratégiai szintjét. Ez a hatás megnyilvánulhat a korábban bemutatott OxIPO-modell szerinti kognitív túlterhelésben, a célország társadalmi polarizációjának radikális és mérhető növekedésében, vagy a politikai-katonai döntéshozatal megbénításában, azaz a döntési paralízis (paralysis) állapotának előidézésében.

A gyakorlat nyelvére fordítva az FMK-rács ezen szakasza biztonsági zsilipként működik: ha a 2014-es ukrajnai események vagy a 2022-es invázió során vizsgált orosz narratívák átjutnak ezen a háromdimenziós szűrőn, akkor bebizonyosodik róluk, hogy nem a háborús káosz szülte spontán jelenségek, hanem mérnöki pontossággal tervezett kognitív csapásmérő eszközök.

2.4.2. Az FMK-rács operacionális szerkezete, a konfigurációs mátrix

Miután az FMK-zsilip azonosította a jelenséget, a kutatás elvégzi annak strukturális leírását. Az FMK-rács a fegyvernek minősülő kommunikáció négy szintjét (ökoszisztéma–művelet–taktika–technika) minden esetben ugyanazon konfigurációs metszetben rögzíti (aktor–csatorna–műveleti termék), kiegészítve a tipikus cél/kimenet mezővel. Ez a struktúra biztosítja a 2014-es és a 2022-es esetek tudományos összehasonlíthatóságát (strukturált, fókuszált összehasonlítás – SFÖ).

A vonatkozó 3. táblázat: FMK-rács – az FMK négy szintjének konfigurációs mátrixa címmel a mellékletben található.

Az FMK-rács „egyesített” jellege abban rejlik, hogy a vertikális fogalmi hierarchiát összekapcsolja a H (Helyzet) dimenzió kötelező leíró mezőivel. A táblázat jobb szélső oszlopa (tipikus cél/kimenet) pedig megteremti a logikai átvezetést az E (előrejelzés/OxIPO) és az I (irányítás/MRM) dimenziók felé: itt látható, hogy egy technikai szintű komment-spam miként járul hozzá az ökoszisztéma-szintű bizalom romboláshoz.

Az FMK-rács és az FMK-mátrix viszonya: evolúciós logika

Az FMK-rács a disszertáció állandó konfigurációs sémája: a négy hierarchiaszint (ökoszisztéma → művelet → taktika → technika) és a három operatív oszlop (aktor – csatorna/infrastruktúra – műveleti termék) minden vizsgált időszakban azonos szerkezettel töltődik ki. Ez biztosítja az összehasonlíthatóságot: amikor a 2014-es és a 2022-es eset „technika” sorát egymás mellé teszem, az eltérés nem a séma, hanem a kitöltés szintjén jelenik meg (kézi trollkomment versus generatív mesterséges intelligencia által előállított szintetikus tartalom).

A rács jobb szélső oszlopa – „tipikus cél/kimenet” – a 2014-es esetnél még elegendő ahhoz, hogy a művelet kognitív következményeit jelezze: a döntési bénulás, a bizalomrombolás vagy a legitimációs keret átrendezése a csatornaszinkron és a volumen általános hatásaként áll elő. A manuális eszközök nem tették lehetővé, hogy a támadó célzottan differenciáljon aszerint, melyik érzékszervi modalitáson milyen konkrét feldolgozási rövidutat kíván aktiválni.

A 2022-es háború és a generatív mesterséges intelligencia megjelenése azonban ezt a helyzetet szükségszerűen megváltoztatta. Amikor ugyanaz a műveleti hálózat egyidejűleg termel klónoldal-szöveget (értelmezési szűkületet célozva), szintetikus fotót (bizonyíték-illúziót generálva), klónozott hangüzenetet (bizalmi rövidzáratot kihasználva) és deepfake videót (bénító vizuális sokkot kiváltva), a „tipikus cél/kimenet” általános oszlopa már nem elegendő a hatásmechanizmus leírásához. Az FMK-mátrix – amelyet a jelen disszertáció a szándék–csatorna-konfiguráció–kognitív hatás hármasaként vezet be – nem új, versengő eszköz, hanem a rács szükségszerű

kibővítése[45]: a „tipikus cél/kimenet” oszlopot modalitásonként differenciált kognitív hatásmechanizmussá bontja ki, lehetővé téve, hogy a kód ne csupán azt jelölje, mi volt a termék, hanem azt is, milyen feldolgozási úton fejti ki a hatását. A gyakorlat nyelvére fordítva: az FMK-rács megmondja, mi van a táblázatban; az FMK-mátrix megmondja, miért ártalmas.

A disszertáció ennek megfelelően a Krím 2014-es esettanulmánynál az alap FMK-rácsot alkalmazza teljes konfigurációs kitöltéssel, a 2022-es esettanulmánynál pedig a rácsot kiegészíti a mátrix kognitív-hatás dimenziójával. A két eszköz közötti kapcsolat tehát nem választási lehetőség, hanem evolúciós szükségszerűség: a technológia kiterjesztette a támadási felületet, a diagnosztikának pedig követnie kell.

2.4.3. A modellek alkalmazása az összehasonlító elemzésben

A 2014-es és 2022-es események összevetésekor az FMK-rács a maga állandóságával teszi láthatóvá a minőségi transzformációt. A séma nem változik: mindkét esetben ugyanaz a négy hierarchiaszint és ugyanaz a három operatív oszlop töltődik ki. A kitöltés viszont gyökeresen eltér. 2014-ben a taktikai és technikai sorok dominánsan humán-intenzívek: manuális bérkommentelés, kézi vezérlésű álprofil-hálózatok, emberi műszakban szervezett amplifikáció. A technikai szint empirikus illusztrációját adja Jessikka Aro finn oknyomozó újságíró munkássága, aki a krími válság idején kimutatta, hogy az online zaklatás és a tömeges kommentelés nem egyéni túlkapás, hanem műveleti logika szerint szervezett, államilag támogatott eszközrendszer volt[46]. Ez a feltárás a 2014-es konfigurációban a technikai szint domináns kitöltési sűrűségét igazolja: manuális, humán erőforrás-igényes üzemmód, amely 2022-re automatizált amplifikációval és szintetikus identitásokkal cserélődött le. 2022-ben ugyanezek a sorok automatizált amplifikációval, szintetikus identitásokkal és a generatív mesterséges intelligencia (GenMI) által előállított műveleti termékekkel telnek meg – és ez a sűrűség váltás kényszeríti ki, hogy a rács „tipikus cél/kimenet” oszlopát az FMK-mátrix kognitív hatás dimenziójával bővítsem. A változás tehát nem az elemzési

[45] GIANNOPOULOS, Georgios et al. (2021): *The Landscape of Hybrid Threats: A Conceptual Model*. JRC Technical Report, European Commission / Hybrid CoE.

[46] ARO, Jessikka (2016): *The Cyberspace War: Propaganda and Trolling as Warfare Tools*. European View, 15. évf. 1. sz. 121–132. o.

keret cserélődése, hanem a technológia által kikényszerített diagnosztikai finomhangolás: 2014-re az alap FMK-rács teljes lefedést ad, 2022-re a rács + mátrix együtt biztosítja az operacionalizálást.

2.4.4. A G–M–T–V műveleti lánc: az FMK-rács fázisnézete

Az FMK-rács a szerkezetet rögzíti: milyen szinten, milyen aktorral, milyen csatornán, milyen termékkel zajlik a művelet. Ehhez szükséges egy kiegészítő nézet, amely a folyamatot ragadja meg: hogyan jut el a műveleti termék az előállítástól a célközönség kognitív terébe. Ezt a funkciót tölti be a G–M–T–V műveleti lánc, amely az FMK-rácsot négy egymásra épülő fázisra bontja. Somodi és Kiss (2019) rámutatnak, hogy a hibrid hadviselő hosszú távon nem csupán az egyes fázisokban operál, hanem magát az ingerküszöböt kísérli meg feljebb tolni – az oktatási, kulturális, szórakoztatóipari és közösségimédia-struktúrákon keresztül –, hogy a későbbi műveletek már ne ütközzenek az eredeti ellenállásba[47]

- G (Generálás / Generation): a tartalomvariánsok előállításának sebessége és költsége – szöveg, kép, hang, videó. A 2014-es konfigurációban ez kézi trollfarm-munka volt; a Híd-időszak alatt a generatív MI és a GAN-technológia a költséget és az átfutási időt nagyságrendekkel csökkentette.

- M (Mosás / Laundering): a forrás- és kontextus-átöltés hatékonysága – hogy a tartalom ne „orosz propagandaként", hanem helyi oknyomozásként, szakértői véleményként, kiszivárgott dokumentumként vagy klónoldalon megjelenő nyugati hírként érkezzen a célközönséghez. A mosás a hitelesség-eltérítés (credibility hijacking) műveleti megvalósítása.

- T (Terítés / Distribution): a terjesztés skálázhatósága és kontrollálhatósága – algoritmikus amplifikáció, bot-hálózat, nyílt→zárt csatorna-váltás (Telegram, WhatsApp), fizetett és organikus terítés kombinációja. A terítés az FMK-rács csatorna-oszlopának dinamikus olvasata.

- V (Validálás / Validation): kétirányú dimenzió: a támadó oldalán a hitelesítő réteg (civil tanú, tekintélyi proxy, „bizonyíték-érzet") hozzáadásának könnyedsége; a védekezői

[47] SOMODI – KISS (2019) i. m. 24. o.

oldalon az ellen-validálás (OSINT, tényellenőrzés, pre-bunking) sebessége. A V-dimenzió az, ahol a Helyzet-dimenzió közvetlenül összekapcsolódik az Irányítás-dimenzióval: a validálás és az ellen-validálás versenye határozza meg a művelet stratégiai kimenetét.

A G–M–T–V lánc és az FMK-rács viszonya nem alternatíva, hanem nézőpont-különbség: a rács a statikus pillanatfelvétel (milyen a konfiguráció egy adott időpontban), a lánc a dinamikus folyamat (hogyan halad a műveleti termék a fázisokon végig). Az 5. fejezet a Híd-időszak (2014–2021) elemzésére ezt a lánc-nézetet alkalmazza: minden Anchor-mérföldkőnél azt vizsgálja, melyik láncszem erősödött, gyorsult vagy olcsóbbá vált, és a Reziliencia-mérföldköveknél azt, melyik láncszemnél épültek ki védekezői ellenpontok. A két eset (Krím 2014 vs. Ukrajna 2022) közötti kimeneti különbség így nem narratív impresszióként, hanem láncszemenként mérhető eltolódásként lesz dokumentálható.

2.5. Az OxIPO-modell szerepe az előrejelzésben

A kognitív pszichológia Human Information Processing (HIP) modelljére építve az OxIPO-modell első eleme az Input (I), vagyis az inger-túlterhelés szakasza. A digitális térben a bemeneti ingerek volumene exponenciálisan nő, amit Paul és Matthews (2016) a Firehose of Falsehood (a hazugság tűzoltótömlője) modellel írnak le. Ebben a fázisban a támadó nem a minőségi meggyőzésre, hanem a nagy volumenű, többcsatornás és gyors üzenetáradatra épít, amelynek célja a figyelem teljes lefoglalása. Prier (2017) rámutat, hogy a közösségi média mint hadszíntér a trendek uralásáról (Commanding the Trend) szól: aki uralja a hírfolyamot, az uralja a valóságérzékelést. Külföldi példaként említhető az orosz trollgyárak szinkronizált tevékenysége az amerikai választási kampányok idején, míg hazai viszonylatban a COVID-19 infodémia során tapasztalt összehangolt, vírusszkeptikus posztolási hullámok szemléltetik ezt a „tűzoltótömlő” taktikát. Itt jelenik meg a zagyválás (bullshit) Harry Frankfurt (2005) által leírt jelensége is: a forrást nem érdekli a tények igazságtartalma, csupán a zajkeltés. Erre példa Donald Trump azon beismerése, miszerint tényeket kreált a Justin Trudeau-val való tárgyalásán a dominancia fenntartásáért (WASHINGTON POST 2018), magyar kontextusban pedig a kampányidőszakok azon szakértői jóslatai, amelyek adatok nélkül, pusztán érzelmi alapon vizionálnak azonnali államcsődöt vagy példátlan jólétet.

A modell második eleme a Process (P), vagyis a feldolgozási kapacitás kimerülése. Az emberi agy munkamemóriája biológiailag korlátozott (Miller-törvény), és ha az információ komplexitása

meghaladja ezt a küszöböt, a rendszer védekező üzemmódba vált. Az FMK célja, hogy Daniel Kahneman (2013) terminológiájával élve az analitikus „System 2" gondolkodást kikapcsolja, és az irányítást a gyors, érzelmi alapú „System 1" vegye át. Ebben a fázisban nyer teret a szándékos félreértelmezés (strategic misinterpretation), amelyet Paul Bernal (2021) a szabályozási kísérletek kudarcának egyik fő okaként nevez meg. A támadó szándékosan torzítja el a célpont üzeneteit, hogy agresszornak állítsa be őt. Külföldi példa a „Birds Aren't Real" mozgalom, amely bár paródia, bizonyította, hogy a szándékosan kiforgatott adatokból is építhető politikai identitás. Hazai példaként említhető a politikai viták azon gyakorlata, ahol az ellenfél szavait kiragadják eredeti környezetükből, és tudatosan olyan jelentéssel ruházzák fel, amely alkalmas a lejáratásra és a kognitív zavarkeltésre.

Végül az Output (Out) szakaszban a torzult cselekvés realizálódik. Ebben az állapotban a döntéshozó vagy a választópolgár már nem racionális mérlegelés, hanem heurisztikák és érzelmi reflexek alapján reagál: pánikból oszt meg egy hamis információt (hoaxot) vagy hoz megfontolatlan gazdasági döntést. Az FMK ezen a ponton válik fizikai hatássá, hiszen a torzult percepció torzult társadalmi cselekvést szül.[48]

2.6. A védekezés elméleti kerete: A Multimodális Reziliencia Mátrix (MRM) bevezetése

Bár a fejezet eddigi alfejezetei dominánsan a jelenségek diagnózisára és kódolására fókuszáltak, a kutatás végső célja a kognitív hadviselés (cognitive warfare) elleni elhárítási megoldások kidolgozása. Ennek elméleti alapját a Multimodális Reziliencia Mátrix (Multimodal Resilience Matrix – MRM) képezi. A modell alaptézise, hogy az információs műveletek elleni védekezést nem lehet egyetlen elszigetelt „csodafegyverre" alapozni; a védelemnek rétegezett kontrollokra (multi-layered defense strategy) kell épülnie .

A reziliencia ebben az olvasatban nem egy passzív állapot, hanem egy szintezett beavatkozási rend. A modell azért tekinthető multimodálisnak, mert felismeri, hogy a modern információs hadviselés nem egynemű: a támadó fél egyszerre és összehangoltan használja ki az egyes érzékszervi csatornák – szöveg (text), kép (image), hang (audio), videó (video) – specifikus kognitív sebezhetőségeit. A generatív mesterséges intelligencia (GenAI) korszakában a fenyegetés

[48] CULLEN, Patrick: *Hybrid threats as a new "wicked problem" for early warning*. Hybrid CoE (European Centre of Excellence for Countering Hybrid Threats), Strategic Analysis 8, 2018., 4-5. o.

súlypontja a hitelesség-eltérítés (credibility hijacking) felé tolódott el, ahol a technológia képes a valóságérzékelés alapvető heurisztikáit.[49]

A Multimodális Reziliencia Mátrix (MRM) logikája a mikro–mezo–makro reziliencia-szintekre épül, azonban az értekezésnek ezen pontján a védekezés kifejezetten az érzékszervi modalitásokra bontva jelenik meg.

Szöveges modalitás (text): A skálázott bizalomerózió terepe, ahol a generatív nyelvi modellek (LLM) legfőbb veszélyét a nyelvtanilag hibátlan, iparosított megtévesztés jelenti . A támadás itt az értelmezést és a logikai következtetést célozza, mivel a hibátlan stílus kikapcsolja a befogadó korábbi helyesírási gyanúszűrőit. A kontroll alapja a stilisztikai bizalmi zérus elv (stilisztikai Zero Trust): a nyelvhelyesség helyett a sürgetés és a szokatlan csatornaváltás válik a gyanújelzővé.

Képi modalitás (image): A bizonyíték-illúziót használja ki. A fotórealisztikus manipulációk (mint a Pentagon-robbanás vagy a Balenciaga-pápa képei) a másodperc töredéke alatt aktiválják az érzelmi választ és az első benyomáson alapuló valóság-heurisztikát, még a tudatos kogníció bekapcsolása előtt. A védekezés kulcsa a kontextus-validálás, amely rögzíti, hogy a kép önmagában nem bizonyíték, és hitelessége csak független források megerősítésével igazolható.

Hangi modalitás (audio): A legbizalmasabb kapuként funkcionál, ahol a hangklónozás (voice cloning) a legveszélyesebb közvetlen támadási forma. A hangtónus ismerőssége automatikus bizalmat generál (tekintély-torzítás / authority bias), kikerülve a vizuális szkepticizmust. A kontroll mechanizmusa a visszahívási protokoll, amely előírja, hogy a hitelesítést soha ne az érkező, hanem egy már ismert, megbízható csatornán végezzük el.

Videó (video): A vizuális sokk erejével a bénítás eszköze (paralysis-hatás), amely képes rövid időre megbénítani a döntéshozatalt a jelenlét-illúzió megteremtésével. A kontrollt itt a többforrásos megerősítés adja: a videót nem szemtanúként, hanem konstruált tartalomként kell kezelni, ahol a hitelességet a forráslánc és a metaadatok igazolják.

Az MRM két dimenzió mentén operacionalizálja a védelmet: egyrészt a beavatkozási szintek (mikro–mezo–makro), másrészt az egyes információs modalitások mentén. Ez utóbbi biztosítja,

[49] SZICHERLE Patrik – KREKÓ Péter (2020): *Burjánzanak az álhírek a koronavírus nyomában*. Political Capital, Budapest. 3–8. o. A COVID- dezinformáció magyarországi megjelenési mintáinak elemzése.

hogy a védekezés ne csak általános elv maradjon, hanem minden technikai csatornához hozzárendelje a megfelelő kognitív és technikai kontrollpontokat. A vonatkozó 4. táblázat: Multimodális Reziliencia Mátrix (MRM): kárpályák és kontrollpontok címmel a mellékletben található.

Ez a mátrix-szemlélet lehetővé teszi, hogy a védekezési stratégiákat ne statikus szoftveres megoldásokként, hanem az emberi információfeldolgozás (Human Information Processing – HIP) folyamatába épített aktív szűrőkként kezeljük. Az alábbiakban e védelmi szintek részletes kifejtése következik, az egyéni kognitív immunizációtól a globális platform-szabályozásig.

2.6.1. Mikroszint: Kognitív immunizáció és az ÁEI-protokoll

A kognitív hadviselés elleni védekezés legalsó, de egyben legkritikusabb rétege az egyéni szint (mikroszint), ahol a cél a káros információs behatás megállítása, még mielőtt az a döntéshozatali láncban mélyebb torzulást okozna. A hagyományos médiatudatossági képzésekkel szemben a disszertáció által javasolt megközelítés a kognitív immunizációra helyezi a hangsúlyt. Ez a stratégia nem csupán utólagos cáfolatokat (debunking) jelent, hanem a befogadó előzetes felkészítését a manipulációs technikák felismerésére (pre-bunking). A módszer lényege, hogy a legyengített „mentális kórokozóval" való találkozás képessé teszi az egyént a valódi támadás elhárítására, hasonlóan az orvosi értelemben vett védőoltásokhoz.[50]

A mikroszintű védekezés központi eleme a kognitív fék beiktatása. Daniel Kahneman (2013) kognitív modelljére építve a cél az, hogy az azonnali, érzelmi alapú és heurisztikus ösztönös válaszreakciókat egy tudatos, lassabb és analitikus reflexív gondolkodási folyamattal váltsuk fel. Mivel hibrid krízishelyzetben az egyén kognitív kapacitásai a stressz és az információs árasztás (infobesity) hatására beszűkülnek, a védekezést nem bonyolult elemzésekre, hanem egyszerű, feltételes reflexszé tehető rutinokra kell alapozni.

[50] ROOZENBEEK, Jon – VAN DER LINDEN, Sander (2021): *Inoculation Theory and Misinformation*. NATO Strategic Communications Centre of Excellence, Riga. 8–10. o. A szerzők McGuire (1961, 1964) eredeti inokulációs elméletét a dezinformáció elleni pszichológiai ellenálló-képesség kontextusába helyezik, és kimutatják, hogy a „technikaalapú" inokulációs megközelítés – amely nem konkrét állításokat, hanem manipulációs technikákat tanít felismerni – politikai hovatartozástól nagyrészt függetlenül hatékony.

Ennek elsődleges operacionális eszköze a kutatásomban használt Stop–Check–Confirm (SCC) protokoll[51], magyarul Állj–Ellenőrizz–Igazolj vissza (ÁEI-protokoll), amely magas kockázatú iparágak (pl. nukleáris energia, repülés, vegyipar) biztonsági kultúrájából fejlődött ki az elmúlt évtizedekben., de itt a multimodális fenyegetésekre (szöveg, kép, hang, videó) specifikus válaszokat kínál:

1. Állj meg! (STOP): A protokoll első és legfontosabb lépése a reakcióidő mesterséges lassítása. Amikor a felhasználó az online térben egy idői nyomást alkalmazó, sürgető, félelmet keltő vagy erős morális felháborodást kiváltó ingerrel találkozik – legyen az egy „rendkívüli" hír vagy egy gyanús privát üzenet –, a protokoll a kattintás vagy a megosztás azonnali felfüggesztését írja elő. Ez a „kognitív vészfék" akadályozza meg, hogy a fegyveresített tartalom elérje elsődleges célját: az automatikus érzelmi válasz által kiváltott reflexszerű továbbosztást.

2. Ellenőrizd (CHECK): Az ösztönös reakció megállítása után a befogadó tudatosítja a tartalom modalitását (lásd 2. táblázat).

   – Szöveg esetén: Észlelhető-e a mesterséges intelligencia által generált tartalmakra jellemző „túlzott sterilitás" vagy a szokatlan, sürgető hangvétel?

   – Kép/Videó esetén: Megfigyelhetők-e a deepfake-technológiák fizikai hibái (például a szemmozgás aszinkronitása, a haj és a háttér találkozásának elmosódottsága)?

   – Forrás szintjén: Megfelel-e a tartalom URL-je a valódi intézményének, vagy egy manipulatív, megtévesztő másolattal (doppelgänger) állunk szemben?

3. Igazold vissza (CONFIRM): A kognitív folyamat lezárása a többszörös megerősítés (trianguláció), amely már a lassú, racionális ellenőrző mechanizmusokat aktiválja. Az

[51] A módszertan gyökerei és legfontosabb forrásai: DuPont (STOP™ program): A biztonsági protokollok egyik úttörője a DuPont vállalat volt, amely az 1960-as évek végén vezette be a STOP (Safety Training Observation Program) rendszert. Bár ez nem azonos az SCC-vel, megalapozta a „megállás és megfigyelés" elvét az iparban. Nukleáris ipar (Self-Checking / STAR): A protokoll legközelebbi rokona a nukleáris iparban használt STAR (Stop, Think, Act, Review) módszer, amelyet az 1980-as években az amerikai Institute of Nuclear Power Operations (INPO) tett sztenderddé az emberi hibák csökkentésére. Vállalati adaptációk (pl. MOL, Shell, ExxonMobil): A konkrét „Stop–Check–Confirm" elnevezés főként olyan nagyvállalatok belső biztonsági kézikönyveiben (pl. a MOL Group EBK követelményei) kristályosodott ki, amelyek az SCC (Safety Certificate Contractors) tanúsítási rendszert alkalmazzák.

információt soha nem az érkező csatornán belül kell validálni. A módszertan az oldalirányú olvasást (lateral reading) javasolja: elhagyni az eredeti felületet, és legalább két független, hiteles és hivatalos forrásnál (pl. állami hírügynökség, ellenőrzött híroldal) keresni az állítás megerősítését.

Az ÁEI-protokoll következetes alkalmazása a hálózatba kapcsolt felhasználót a biztonsági lánc hagyományosan „leggyengébb láncszeme" pozíciójából aktív Emberi Tűzfallá (Human Firewall) minősíti át[52]. Ebben a paradigmában a felkészített állampolgár már nem csupán passzív áldozata a kognitív hadviselésnek, hanem proaktív védelmi réteg, aki képes a saját szintjén véglegesen elvágni a dezinformációs vírus terjedési láncát[53], megőrizve ezzel egyéni és társadalmi kognitív autonómiáját.

2.6.2. Mezoszint: Szervezeti reziliencia és a Narratíva-Vezérelt Kockázat (NVK) kezelése

A szervezeti szint – amely magában foglalja a kritikus infrastruktúrákat, az államigazgatási szerveket, a rendvédelmi alakulatokat és a multinacionális vállalatokat – kiemelt célpontja a kognitív műveleteknek, mivel itt a befolyásolás közvetlen működési anomáliákat válthat ki. Ezen a szinten a dezinformáció már nem csupán elvont véleményformáló eszköz, hanem a Narratíva-Vezérelt Kockázat (Narrative-Driven Risk – NVK) hordozója, amely fizikai és logisztikai reakciókat képes indukálni . Egy jól időzített, több csatornán összehangolt hamis állítás – például egy közműszolgáltatás leállásáról vagy egy pénzintézet fizetésképtelenségéről – percek alatt lakossági pánikot, a call-centerek túlterhelését és hibás vezetői döntéseket eredményezhet anélkül, hogy a szervezet informatikai rendszereit tényleges kibertámadás érné.

Ezen a kritikus mezoszinten a szervezeti túlélés alapköve a Központi Igazságforrás (Single Source of Truth – SSOT) elvének szigorú, doktrinális intézményesítése. A modell lényege, hogy a szervezetnek már békeidőben ki kell jelölnie azt az egyetlen, hitelesített kommunikációs gerincet, amely egy krízis során minden kifelé és befelé irányuló üzenet vonatkoztatási pontjaként szolgál.

---

[52] HUMAN FIREWALL COUNCIL (2003): *The Alarming State of Security Management Practices Among Organizations Worldwide*. Security Management Index.

[53] WHITMAN, Michael E. – MATTORD, Herbert J. (2011): *Principles of Information Security*. 4. kiadás. Cengage Learning, Boston.

Ez a megoldás garantálja, hogy a szervezet ne erősítse fel fragmentált, egymásnak ellentmondó üzenetekkel a támadó fél által keltett bizonytalanságot.

A szervezeti reziliencia operatív kereteit az alábbi pillérek határozzák meg:

- A hiteles csatorna rögzítése (SSOT): Olyan előre validált kommunikációs infrastruktúra (például dedikált incidensoldal vagy hivatalos parancsnoki üzenetrendszer), amely a válság során felülírja a párhuzamosan terjedő fegyveresített dezinformációt.
- Válságkommunikációs protokollok: Előre megírt forgatókönyvek rendszere, amely rögzíti a jóváhagyási folyamatokat, a kijelölt szóvivők körét és a minimális verifikációs lépéseket.
- Koordinált tájékoztatás: Az amerikai Nemzeti Incidenskezelési Rendszer (NIMS) keretében alkalmazott Közös Információs Központok (Joint Information Center) elvének adaptálása, amely az „egy hang, egy koordinációs központ” elvét érvényesíti.
- Gyorsaság és koherencia szimbiózisa: A Vészhelyzeti Kockázatkommunikáció (CERC) modellje alapján a közlésnek egyszerre kell időszerűnek és a lakosság számára transzparensen ellenőrizhetőnek lennie, megőrizve a narratív konzisztenciát a kognitív túlterhelés csúcsán is.

A disszertáció a későbbiekben (a 3. és 5. fejezetekben) ezen a kereten keresztül vizsgálja az ukrán állami kommunikáció professzionalizálódását: míg 2014-ben a bizonytalan tájékoztatás akaratlanul is kiszolgálta az orosz érdekeket, addig 2022-ben a centralizált SSOT-architektúra az ukrán kognitív védekezés stratégiai előnyévé vált.

A mezoszintű védekezés tehát a „human firewall” (emberi tűzfal) szervezeti kiterjesztése, ahol nemcsak az egyéni szűrők, hanem az intézményi eljárásrendek is a kognitív bénítás (paralysis) megakadályozását szolgálják .

A mezoszintű beavatkozás tervezés operatív gerincét az SCC-protokoll (Sebesség–Tartalom–Irányítás; angolul: Speed–Content–Control) adja. A protokoll három, egymásra épülő beavatkozási tengelyt rögzít. A Sebesség (Speed)-tengely a dezinformáció terjedési sebességét a szervezeti válaszreakció sebességével állítja szembe. Vosoughi, Roy és Aral 2018-ban 126 000 Twitter-pletykán igazolta, hogy a hamis hírek átlagosan hatszor gyorsabban jutnak el 1500 felhasználóhoz,

mint az igazak, és a leggyorsabb burjánzások perceken belül ezrekhez érnek el[54] – a hamis tartalom cáfolata eközben lassú és nehézkes marad, mivel az értelmezési fázisba belépő narratíva kognitív rögzülése megakadályozza a korrekciókat[55]. Wardle és Derakhshan 2017-es agent–message–interpreter fázismodellje alapján az intézményi válasznak a terjesztési szakaszba kell beavatkoznia, mielőtt az üzenet az értelmezési fázisba lép – a stratégiai kommunikációs szakirodalomban erre épülő operatív alapszabály az első 90 perc[56]. A Tartalom (Content)tengely azt rögzíti, hogy az ellen-narratívának nem a hazugságot kell megismételnie (inoculation trap), hanem alternatív kognitív keretet kell kínálnia. Az Irányítás (Control)tengely a csatorna- és amplifikációs döntéseket kezeli: mely platformon, milyen validálási réteggel és milyen célcsoportnak juttatják el a szervezeti választ. Az SCC-protokoll részletes operatív kifejtése a 8. fejezetben (Multimodális Reziliencia Mátrix) található; a 7. fejezet összehasonlító elemzése az SCC-protokollt mint a két eset közötti védekezési aszimmetria mérőeszközét alkalmazza.

2.6.3. Makroszint: Platform-kormányzás és a szabályozás korlátai

Az MRM mátrix legmagasabb szintje (makroszint) az átfogó jogi, állami és globális technológiai szabályozás geopolitikai terepe. A kutatás által vizsgált időszak végére (2022–2025) a technológiai óriásvállalatok (Big Tech) puszta önszabályozásának kudarca teljes mértékben nyilvánvalóvá vált. A piaci szereplők profitérdekei (elköteleződés-maximalizálás) és a nemzetállamok biztonsági érdekei (kognitív stabilitás) közötti feloldhatatlan ellentét miatt a de facto kényszerítő erejű, nemzetek feletti jogszabályok vették át a főszerepet. Ennek az európai jogi architektúrának a

---

[54] VOSOUGHI, Soroush – ROY, Deb – ARAL, Sinan (2018): The Spread of True and False News Online. Science, 359. évf. 6380. sz. 1146–1151. o. DOI: 10.1126/science.aap9559. A vizsgálat 126 000 Twitter-pletykát elemzett 2006–2017 között; a hamis hírek átlagosan 6-szor gyorsabban jutottak el 1500 felhasználóhoz, mint az igazak, és a leggyorsabb burjánzások perceken belül ezrekhez értek el.

[55] ZUBIAGA, Arkaitz – LIAKATA, Maria – PROCTER, Rob – WONG SAK HOI, Geraldine – TOLMIE, Peter (2016): Analysing How People Orient to and Spread Rumours in Social Media by Looking at Conversational Threads. PLoS ONE, 11. évf. 3. sz. e0150989. DOI: 10.1371/journal.pone.0150989. A kutatás 330 Twitter-rémhír életciklusát elemezte 9 híresemény kapcsán; az igaznak bizonyuló pletykák gyorsabban oldódtak fel, míg a hamis tartalmak cáfolata lassú és nehézkes maradt – a téves narratíva rögzülési ablakának szűkítése ezért az első perceket igényli.

[56] WARDLE, Claire – DERAKHSHAN, Hossein (2017): Information Disorder: Toward an Interdisciplinary Framework for Research and Policymaking. Council of Europe, DGI(2017)09. Strasbourg. (2. kiad. 2018.) Az ágensek–üzenetek–értelmezők hármas fázismodellje megmutatja, hogy a dezinformáció a létrehozás–termelés–terjesztés szakaszain halad végig; az intézményi válasznak ezért a terjesztési szakaszba kell beavatkoznia, mielőtt az üzenet az értelmezési fázisba lép és kognitív rögzülés következik be. Elérhető: https://rm.coe.int/information-disorder-report-version-august-2018/16808c9c77

legfontosabb mérföldköve a Digitális Szolgáltatásokról szóló Rendelet (Digital Services Act – DSA).

A vonatkozó platform-kutatások és összehasonlító elemzések[57],[58] rámutatnak a jelenlegi, globális tartalom-szabályozási modellek fundamentális dilemmáira és műveleti korlátaira:

- A Centralizált moderáció (például a Meta/Facebook modellje): Ez a struktúra dominánsan a külső, professzionális tényellenőrző partnerek (mint az IFCN hálózat) ex-post, azaz utólagos elemzéseire épít. Előnye az objektív, újságírói szakmai alaposság és a jogi ellenőrizhetőség. Ugyanakkor műveleti hátránya a kritikus lassúság (az álhír napokkal megelőzi a cáfolatot), az átláthatatlan algoritmus-módosítások (shadow banning), valamint az állami vagy vállalati "cenzúra" politikai vádjának való állandó kitettség, amely tovább rombolja a platform hitelességét.

- A Decentralizált moderáció (például az X/Twitter „Community Notes” modellje): E megközelítés a tömegek bölcsességére épít: a vitatott tartalmak megjelölését és kontextualizálását maguk a minősített felhasználók (a közösség) végzik. Bár politikai szempontból demokratikusabbnak, organikusabbnak és a cenzúra-vádaktól mentesebbnek tűnik, a Center for Countering Digital Hate (CCDH)[59] független mérései drámai sebezhetőséget tártak fel. Egy hibrid támadás vagy egy feszült választási időszak során alkalmazott nagy volumenű, automatizált információs elárasztás (flooding) esetén a közösségi modell szinte teljesen hatástalan. A szükséges „konszenzus” kialakulása és a jegyzet láthatóvá válása ugyanis túl sok időt vesz igénybe, így a botok által felerősített szintetikus álhír pontosan abban a legkritikusabb, első 12-24 órában terjedhet akadálytalanul és érheti el a maximális kognitív hatásfokot, amikor a beavatkozásra a legnagyobb szükség lenne.

---

[57] GIANNOPOULOS, Georgios et al. (2021): *The Landscape of Hybrid Threats: A Conceptual Model*. JRC Technical Report, European Commission / Hybrid CoE.

[58] NATO StratCom COE (2017-2022): Robotrolling, majd Virtual Manipulation Brief (VMB)

[59] CCDH / CENTER FOR COUNTERING DIGITAL HATE (2024a): *Failure to Protect: How X's Community Notes fail to address antisemitism and disinformation*. CCDH Report, Washington D.C. / London.

2.7. Fejezetösszegzés és kitekintés

A fejezet a kutatás módszertani architektúráját vezette le. Az elméleti alapokat, a szakirodalmi szintézist és az FMK fogalmi keretrendszerét a 3. fejezet dolgozza fel; jelen fejezet feladata a mérőműszer összeállítása volt – annak rögzítése, hogy a disszertáció milyen eszközökkel, milyen logikai rendben és milyen bizonyítási követelményekkel teszi összehasonlíthatóvá a 2014-es és a 2022-es esettanulmányokat.

A fejezet három, egymásra épülő eredményt, illetve szempontrendszert rögzített.

Az első a módszertani architektúra levezetése. A fejezet nemcsak bemutatott öt módszertani eszközt (SFÖ, H–E–I, FMK-rács, OxIPO, MRM), hanem le is vezette, miért szükséges mindegyik: az SFÖ adja az összehasonlítási alapot, a H–E–I az operatív kérdéssort, az FMK-rács a helyzet-rögzítést, az OxIPO a kognitív mechanizmus-magyarázatot, az MRM pedig a beavatkozás-tervezést. Ez a láncolat deduktív építkezés, ahol minden szint az előző korlátjából következik. Az FMK-rács és az FMK-mátrix közötti evolúciós kapcsolat rögzítése biztosítja, hogy a 2014-es (alap FMK-rács) és a 2022-es (rács + mátrix kognitív-hatás dimenzió) konfigurációk összehasonlíthatósága módszertanilag átlátható legyen.

A második az bizonyítékgyűjtés szabályozása. A forráshierarchia és a triangulációs szabályok rögzítik, hogy a kutatás mikor fogad el egy megállapítást és mikor minősít vissza. A háromszintű rendszer (intézményi dokumentumok – független kutatói esettanulmányok – OSINT/SOCMINT korpusz) és a „nem tudom kapu” logikája biztosítja, hogy az elemzés ne ráhúzott narratíva, hanem transzparens és auditálható bizonyítéklánc legyen.

A harmadik a védekezési operacionalizálás. A Multimodális Reziliencia Mátrix (MRM) bevezetése megteremtette a keretet ahhoz, hogy a védekezést ne egyetlen „csodafegyverként”, hanem szintezett, modalitásonként differenciált kontrollrendszerként kezeljük – a kognitív immunizációtól (mikro) a szervezeti reziliencián át (mezo) a platform-szabályozásig (makro). Az MRM az OxIPO által feltárt kognitív mechanizmusokat (ld. 2.5; a mögöttes pszichológiai mechanizmusok: 3. fejezet) konkrét beavatkozási pontokká fordítja.

Az empirikus bázis tizenegy évet (2014–2025) ölel fel: a feldolgozott korpuszban több mint nyolcvan intézményi jelentés és fenyegetettségi adatbázis szerepel, a NATO StratCom COE és

OSCE helyszíni elemzéseitől a Meta negyedéves CIB-jelentésein át a Stanford Internet Observatory mélyelemzéseiig.

A vonatkozó 5. táblázat: A kutatás empirikus bázisát adó intézményi adatforrások és kiberfenyegetettségi jelentések (2014–2025) címmel a mellékletben található.

A 4. fejezetben ezt a módszertani eszköztárat a gyakorlatba ültetve alkalmazom. A 2014-es krími annektálás és a kelet-ukrajnai konfliktus hibrid műveleteinek elemzése során a H–E–I rács segítségével mutatom be, hogyan alakult ki a stratégiai meglepetés – és miben különbözött a 2022-es helyzettől, ahol a technológiai kapacitás nőtt, de a bénító hatás elmaradt. A paradoxon kulcsa nem a támadóban, hanem a két időpont közötti transzformációs feltételrendszerben rejlik.

3. SZAKIRODALMI ÁTTEKINTÉS ÉS FOGALMI KERETRENDSZER

A 2. fejezet a kutatás módszertani architektúráját vezette le – az összehasonlítás módszertanát (SFÖ), a diagnosztikát (H–E–I), a helyzet-rögzítést (FMK-rács), a mechanizmus-magyarázatot (OxIPO) és a beavatkozás-tervezést (MRM). A módszertani eszközök azonban légüres térben működnének, ha nem jelölnénk ki, milyen elméleti keretben értelmezzük a fegyvernek minősülő kommunikációt, milyen kognitív sebezhetőségekre épül, milyen technológiai környezetben működik – és mit írtak eddig a vizsgált esetekről.

Jelen fejezet ezt a feladatot végzi el. Felépítése három pillérre támaszkodik. Az első az elméleti szintézis (3.1–3.3): a hadtudományi perspektívától a kognitív sebezhetőség mechanizmusain át a technológiai környezet leírásáig. A második az empirikus irodalom feldolgozása (3.4–3.6): mit dokumentáltak eddig a Krím 2014-ről, a 2014–2021-es transzformációs időszakról és az Ukrajna 2022– esetről a fegyvernek minősülő kommunikáció szempontjából? A harmadik a kutatási rés azonosítása (3.7): hol hallgat a szakirodalom, és milyen kérdésekre kíván a disszertáció választ adni?

3.1. A kutatás elméleti alapjai: Információs műveletek a kognitív térben

A kutatás kiindulópontja, hogy az információs manipuláció a 21. században a hibrid hadviselés integráns, gyakran vezető komponense. A hazai hadtudományi alapvetésekkel összhangban a hibrid hadviselés lényege a hagyományos és nem hagyományos eszközök – a katonai erő, a

gazdasági nyomásgyakorlás, a kibertámadások és a propaganda – szinkronizált, összehangolt alkalmazása a politikai célok elérése érdekében. A hibrid hadviselés fogalmi vitáját Somodi és Kiss Álmos Péter 2019-ben négy fő csoportba rendszerezte: a teljesen újként, a részben újként, a semmilyen újdonságot nem nyújtóként, valamint az orosz értelmezés szerinti nyugati Oroszország-ellenes stratégiaként felfogó álláspontokat különböztették meg, rámutatva, hogy a hadviselést mindig is fenyegetések és erőszakos eszközök komplex, politikai célú rendszereként kell értelmezni[60]

Magyarország Nemzeti Biztonsági Stratégiája[61] a hibrid fenyegetések között nevesíti az összehangolt információs műveleteket, amelyek célja a kormányzati cselekvőképesség, a politikai stabilitás és a társadalmi kohézió gyengítése. E műveleti keretben az információs hadviselés célja nem pusztán a meggyőzés, hanem a döntési mechanizmusok megbénítása és az attribúció nehézségét kihasználva olyan helyzet előidézése, amelyet a megtámadott állam kénytelen elfogadni.[62]

A hazai stratégiai keret kibertéri dimenzióját Kovács László dandártábornok elemezte átfogóan a Hadtudományi Szemle hasábjain[63], összehasonlítva a 2012-es és a 2020-as Nemzeti Biztonsági Stratégia kibertéri vonatkozásait. Az elemzés egyik legfontosabb megállapítása, hogy míg a korábbi stratégiában a „kiber" kifejezés összesen hat alkalommal szerepelt, az új, 2020-as dokumentumban harmincháromszor jelenik meg különböző kontextusokban – és ez a statisztikai különbség nem puszta terminológiai bővülés, hanem a fenyegetéspercepció és a doktrinális gondolkodás mélyreható átalakulásának mutatója. A 2020-as NBS legmarkánsabb, paradigmaváltónak értékelhető kitétele, hogy Magyarország a fizikai biztonságot veszélyeztető

---

60 SOMODI Zoltán – KISS Álmos Péter (2019): *A hibrid hadviselés fogalmának értelmezése a nemzetközi szakirodalomban.* Honvédségi Szemle, 147. évf. 6. sz. 17–28. o. DOI: 10.35926/HSZ.2019.6.2. A szerzők négy csoportba sorolják a nemzetközi álláspontokat: (1) teljesen új hadviselési forma; (2) elemei nem újak, de az összehangoltság/kibertér igen; (3) a fogalom nem nyújt újdonságot; (4) az orosz nézet: a hibrid hadviselés a nyugati Oroszország-ellenes stratégia.

61 1163/2020. Korm. határozat, 124. pont c) alpont. Online: https://njt.hu/jogszabaly/2020-1163-30-22

62 Kiss Álmos Péter (2021): A NATO válasza a hibrid fenyegetésre. *Honvédségi Szemle*, 149. évf. 3. sz. 13–28. Online: https://real.mtak.hu/127225/1/KissAlmosPeter.pdf

63 Kovács László (2020): A kiberbiztonság és a kiberműveletek megjelenése Magyarország új Nemzeti Biztonsági Stratégiájában. *Hadtudományi Szemle,* 13(5), 3–18. Online: https://doi.org/10.35926/HSZ.2020.5.1

vagy jelentős anyagi károkat okozni képes kiberképességeket fegyvernek, alkalmazásukat fegyveres agressziónak tekinti, amelyre fizikai térben megvalósuló válaszadás is lehetséges – ezzel a kibertér és a kinetikus hadviselés közötti jogi és doktrinális választóvonal explicit módon átrajzolódik. Kovács ugyanakkor rámutat arra is, hogy a kiberműveletek az információs műveletek szerves részét képezik, és az offenzív kiberképességek fejlesztése már stratégiai célkitűzés a Magyar Honvédség fejlesztési irányaiban. Ez a doktrinális elmozdulás közvetlenül releváns a disszertáció FMK-fogalmának kontextualizálásához: a hazai stratégiai gondolkodás is felismeri azt a küszöbproblémát, amelyre az FMK-definíció épül – hogy a kommunikációs aktus mikor lép át a polgári információs tér kereteiből a fegyveres agresszió kategóriájába.

Ez a stratégiai megközelítés mélyen gyökerezik a hadtudomány klasszikus és modern elméleteiben egyaránt. A hálózatalapú hadviselés (network-centric warfare) fogalmát John Arquilla és David Ronfeldt, a RAND Corporation kutatói alapozták meg 1993-as tanulmányukban[64], amelyben rögzítették: az információs kor társadalmaiban a tudás és az adatok áramlása önmagában stratégiai erőforrás, és a kibercsata nem korlátozódik a technikai rendszerek elleni támadásra – az információ birtoklása és kontrollja a döntési ciklusok felgyorsítását és az ellenfél helyzetértékelésének lebénítását szolgálja. Ezt a gondolatmenetet emelték a narratív tér szintjére Brad Allenby és Joel Garreau 2017-ben, akik bevezették a fegyveresített narratíva (weaponized narrative) koncepcióját,[65] a konfliktusok már nem csupán a fizikai térben zajlanak, hanem a társadalmi értelmezési keretekben, ahol a történetmesélés stratégiai fegyverrendszerré válik, amelynek célja a célpopuláció identitásának és önképének aláásása.

Carl von Clausewitz például a háborút a politika más eszközökkel való folytatásaként definiálta, ahol a pszichológiai tényezők – amit ő a háború súrlódásának és a morális erőknek nevezett – döntőek lehetnek a kimenetel szempontjából.[66] A keleti hadtudományi hagyományban Szun-ce még tovább megy: nála a megtévesztés a hadviselés legmagasabb foka, ahol a cél az ellenség harc

64 ARQUILLA, John – RONFELDT, David (1993): *Cyberwar is Coming!* Comparative Strategy, 12. évf. 2. sz. 141–165. o.

65 ALLENBY, Brad – GARREAU, Joel (2017): *Weaponized Narrative: The New Battlespace*. Center on the Future of War, Arizona State University.

66 Clausewitz, Carl von (1961–1962) [1832]: *A háborúról* I–II. Ford. Dr. Réczey Ferenc. Budapest: Zrínyi Katonai Könyv- és Lapkiadó.

nélküli megtörése a szövetségi rendszereinek megbontásával és a vezetés elbizonytalanításával.[67] A modern NATO-doktrínák ezt a gondolatot adaptálták a digitális korra, amikor a hibrid fenyegetéseket olyan állami és nem állami szereplők koordinált fellépéseként definiálják, akik a sebezhetőségeket kihasználva a küszöbérték alatti zónában operálnak, elkerülve az 5. cikkely szerinti nyílt háborús választ.[68]

3.1.1. A kognitív hadviselés paradigmája

Ahhoz, hogy megértsük az információ fegyverként való alkalmazását, vissza kell nyúlnunk a tudatos befolyásolás intézményi gyökereihez. A propaganda fogalma történetileg nem hordozott negatív konnotációt: a XV. Gergely pápa által 1622-ben életre hívott Sacra Congregatio de propaganda Fide (Szent Kongregáció a Hitterjesztésért) intézménye a hit terjesztésének semleges, adminisztratív keretrendszereként szolgált. A fogalom pejoratívvá válása a 20. századi totális diktatúrák tömegmanipulációs gyakorlatához köthető. A 21. századi, hálózatba kapcsolt hibrid környezetben azonban a klasszikus, egyirányú propaganda-modell már nem elégséges a folyamatok leírására; helyét egy új, szofisztikáltabb keretrendszer, a Szervezett Meggyőző Kommunikáció (Organized Persuasive Communication – OPC) vette át.

Vian Bakir és szerzőtársai[69] 2019-es definíciója alapján a Szervezett Meggyőző Kommunikáció (SZMK) egy olyan átfogó ernyőfogalom, amely képes egyetlen analitikus keretbe integrálni a Public Relations (PR), a klasszikus propaganda, az információs műveletek (Information Operations) és a stratégiai kommunikáció elméleteit. Ez a megközelítés azért elengedhetetlen a hadtudományi vizsgálat számára, mert a modern információs térben e diszciplínák közötti határok végzetesen elmosódtak. A disszertáció szempontjából kritikus fontosságú az SZMK két alapvető típusának éles, működésmód-alapú elhatárolása: a konszenzuális és a nem konszenzuális meggyőzés szétválasztása.

---

[67] Szun-ce (1995): *A hadviselés törvényei.* Ford. Tőkei Ferenc. Budapest: Balassi Kiadó.

[68] NATO (2022): *NATO 2022 Strategic Concept*. 27. pont, 7. o. Online: https://www.nato.int/content/dam/nato/webready/documents/publications-and-reports/strategic-concepts/2022/290622-strategic-concept.pdf

[69] BAKIR, Vian – HERRING, Eric – MILLER, David – ROBINSON, Piers (2019): Organized Persuasive Communication: A new conceptual framework for research on public relations, propaganda and promotional culture. *Critical Sociology*, 45. évf. 3. sz. 311–328. o.

A konszenzuális SZMK olyan meggyőző folyamatot takar, amely a társadalmi nyilvánosság elismert, transzparens keretei között zajlik. Ebben a formában a befolyásolás szándéka, valamint a forrás kiléte a befogadó számára egyértelműen felismerhető – ilyenek például a nyílt politikai kampányok, a kereskedelmi reklámok vagy a klasszikus állami PR-tevékenységek. A kommunikáció hatékonysága itt az érvek ütköztetésén és a célközönséggel kialakított hosszú távú, ellenőrizhető bizalmi kapcsolat felépítésén alapul.

Ezzel szemben a nem konszenzuális SZMK képezi a Fegyvernek Minősülő Kommunikáció (FMK) elméleti és műveleti magját. Ebben a dimenzióban a meggyőzés rejtett, a forrás identitását tudatosan elfedik vagy meghamisítják, a célközönség pedig egyáltalán nincs tudatában annak, hogy kognitív autonómiáját külső, manipulatív beavatkozás éri. Bakir és kutatótársai rámutatnak, hogy a nem konszenzuális formák alkalmazása alapjaiban sérti a befogadó döntési szabadságát, mivel megfosztja őt a valós információkon alapuló mérlegelés lehetőségétől. Az FMK stratégiai zsenialitása pontosan abban rejlik, hogy a PR legitim eszköztárát (például a hitelesség imitálását, a függetlennek látszó szakértői hálózatok kiépítését, az álcivil kezdeményezéseket) használja fel a dezinformáció és a bénítás céljainak elérésére.

A szervezett meggyőző kommunikáció belső tipizálása azért különösen hasznos, mert a puszta „meggyőzés” szó könnyen elfedi a műveleti spektrum valódi mélységét: ugyanazon hálózati infrastruktúrával és szervezettséggel nemcsak állítások „elhitetetése” a cél, hanem konkrét viselkedésbeli döntések kikényszerítése, illetve a döntési horizont szándékos beszűkítése is kivitelezhető. Bakir és szerzőtársai a meggyőző kommunikációt négy, elvileg elválasztható – de a hibrid gyakorlatban gyakran konvergáló – működésmód mentén strukturálják:

2. Megtévesztés (Deception): A hazugság, az elhallgatás és a torzítás tudatos alkalmazása, amely a célpont információs környezetének manipulálásával éri el, hogy a befogadó hamis premisszák alapján hozzon meg számára káros döntéseket.

3. Ösztönzés (Inducement): Különböző (gyakran rejtett) jutalmak vagy előnyök kilátásba helyezése a kívánt viselkedés elérésére.

4. Kényszerítés (Coercion): Erőalkalmazással vagy fenyegetéssel történő nyomásgyakorlás, amely drasztikusan lecsökkenti a célpont választási alternatíváit.

5. Megtévesztő kényszerítés (Deceptive Coercion): A legagresszívabb kognitív műveleti forma, amely a megtévesztést és a fenyegetést ötvözi (például a hamis zászlós / false flag műveletek során), ahol a támadó egy mesterségesen kreált krízishelyzettel kényszeríti azonnali, irracionális reakcióra a célpontot.

Ez az elméleti bontás az FMK-értelmezéshez is közvetlen, operacionalizálható hidat ad. Bizonyítja, hogy a „taktika" nem pusztán az üzenet tartalmi vagy esztétikai formáját jelenti, hanem a befolyásolási mód megválasztását, amely a célcsoport kognitív autonómiáját eltérő mértékben korlátozza. Amikor az információs térben az ellenfél megtévesztő kényszerítést alkalmaz, a kiváltott kognitív kár – a bizalomvesztés, a pszichológiai túlterhelés és a társadalmi polarizáció – mérhető műveleti kimenetté (output) válik, amely közvetlenül ágyaz meg a kinetikus vagy politikai térnyerésnek.

A modern információs környezetben a köznyelvi álhír (fake news) fogalma tudományos elemzésre ma már elégtelen és félrevezető, mivel elmossa a határokat a véletlen tévedés, a szatíra és a szándékos, államilag támogatott kognitív támadás között. A fogalmi tisztánlátás és a műveleti elemezhetőség érdekében a disszertáció Claire Wardle és Hossein Derakhshan[70], valamint a Nolan és Kimball [71] által rögzített taxonómiát alkalmazza. Ez az elméleti keret az információs zavarokat (information disorder) két független változó – a károkozó szándék (intent to harm) és a valóságtartalom (veracity) – mentén három élesen elkülöníthető kategóriára osztja fel.

Terminológiai fegyelem nélkül az „álhír" fogalma könnyen mindent befedő ernyővé válik, ami a hadtudományi operacionalizálást és a védekezést gyengíti. A „hamis-e az állítás?" kérdés önmagában ritkán döntő, mert a műveleti termékdiagnózisban (és a fegyvernek minősülő kommunikáció azonosításában) az a meghatározó tényező, hogy egy adott információ miért, milyen szervezettséggel, milyen hálózati logikával és milyen várható kimenettel (output) jelenik meg. Az európai intézményi keretezés ezért nem pusztán a valótlan tartalmat emeli ki, hanem a mögöttes szándékot és a kárkeltési potenciált is. A dezinformáció eszerint olyan hamis vagy

[70] WARDLE, Claire – DERAKHSHAN, Hossein (2017): *Information Disorder: Toward an interdisciplinary framework for research and policymaking*. Council of Europe Report, Strasbourg.

[71] NOLAN, Susan A. – KIMBALL, Michael (2021): *The Intent Behind a Lie: Mis-, Dis-, and Malinformation*. Psychology Today, 2021. December 22.

félrevezető információ, amelyet tudatosan állítanak elő és terjesztenek közérdekű kár előidézése vagy gazdasági profitszerzés érdekében, miközben az egyszerű tévedés, a szatíra vagy a paródia – még ha félre is vezethet bizonyos befogadókat – teljesen eltérő motivációs logikába tartozik.

A vonatkozó 6. táblázat: Az információs zavarok típusainak elhatárolása a szándék és a valóságtartalom alapján a mellékletben található.

A mis-/dis-/malinformation hármas felosztás így nem pusztán akadémiai finomhangolás, hanem a védekezés, az elszámoltathatóság és a kárlogika alapvető különbségtétele. Nolan és Kimball (2021) rámutatnak, hogy e kategóriák precíz használata az első lépés ahhoz, hogy a társadalom és az állam megfelelően tudja allokálni a jogi, technológiai és oktatási erőforrásait az online fenyegetésekkel szemben. A téves informáláshoz (misinformation) rendszerint a „jóhiszeműség" narratívája társul, ahol az edukáció a megoldás. A dezinformáció (disinformation) már a tudatos, sokszor ipari méretű megtévesztést teszi láthatóvá. A malinformation pedig azt a hibrid helyzetet írja le, amikor a támadó valós, létező információkat válogat ki és kontextualizál újra úgy, hogy azzal reputációromboló vagy a társadalmi bizalmat megbontó hatást érjen el. E három kategória beemelése a disszertáció későbbi indikátorrendszerébe közvetlenül leképezhetővé teszi a „szándék–kár–elszámoltathatóság" tengelyeit, auditálhatóvá téve, hogy mikor beszélünk pusztán információs zajról, és mikor állunk szemben egy koordinált műveleti termékkel.

Az információs zavarok belső struktúrájának és a Fegyvernek Minősülő Kommunikáció (FMK) taktikai eszköztárának pontosabb feltérképezése érdekében elengedhetetlen a Wardle és Derakhshan által kidolgozott keretrendszer folyamatalapú (process-based) elemzése is. A szerzők rögzítik, hogy az információs zavarok vizsgálatakor három fázist kell elkülöníteni: a tartalom létrehozását (creation), a formátum előállítását (production) és a célközönséghez való eljuttatást, azaz a terjesztést (distribution). Ez a megközelítés bizonyítja, hogy az a szereplő, aki a hamis tartalmat megalkotja (ártó szándékkal), nem feltétlenül azonos azzal az aktorral, aki azt végül a platformokon terjeszti.

Ahogy arra korábbi kutatásaimban rámutattam,[72] pontosan ezen a ponton válik stratégiai jelentőségűvé a félretájékoztatás (misinformation). A kognitív hadviselés logikájában az egyszerű,

[72] Horváth Dávid (2022): Pandemic and Infodemic – Which One Is More Dangerous? *Acta Universitatis Sapientiae Communicatio,* 9(1), 125–139. Online: https://doi.org/10.2478/auscom-2022-0009

tévedésből fakadó megosztók adják a rendszer "hasznos idiótáit" és gyanútlan hordozóit. Ők azok, akik sokszor pszichológiai vagy szociális motivációból – például a saját politikai törzsükhöz való tartozásuk demonstrálása céljából – akarva-akaratlanul is felerősítik a narratívát a közösségi platformokon. Ahogy Lebrun 2023-ban a kognitív behatolás (cognitive intrusion) keretrendszerében megfogalmazza, a kognitív behatolás nem csupán az információ, hanem a mentális folyamatok és reprezentációk szándékos manipulálása – tehát az FMK túlmutat a misinformation, amennyiben a kognitív feldolgozás teljes láncolatát célozza[73].

Ezzel szemben a dezinformáció (disinformation) már a tudatosan létrehozott, hamisított tartalom (például a szintetikus média vagy az algoritmikus bot-hálózatok) bevetését jelenti, amely az FMK legaktívabb taktikai elemeként a társadalmi kohézió megbontását célozza. Végezetül a rosszindulatú torzítás (malinformation) alkalmazásakor a közölt adat önmagában valós, azonban annak célzott kiszivárogtatása (például hekkertámadások révén) kifejezetten a demokratikus intézmények ellen és az ellenfél lejáratása érdekében történik. A 2022-es orosz–ukrán konfliktus során e három forma tökéletes szimbiózisa figyelhető meg: míg a dezinformációs gépezet a stratégiai hazugságokat gyártotta (pl. ukrán biolaborok mítosza), a malinformation a célzott politikai karaktergyilkosságokért felelt, a misinformation-t terjesztő organikus hálózatok pedig biztosították a narratívák globális, ellenállhatatlannak tűnő áramlását. A Hybrid CoE konceptuális keretrendszere 13 doménen keresztül modellezi a hibrid fenyegetéseket, amelyek közül a stratégiai kommunikációs dimenzió pontosan ezt a szervezeti beágyazottságot ragadja meg: a dezinformáció nem véletlenszerű tartalom, hanem szervezetileg koordinált, több doménen átívelő műveleti lánc terméke[74].

Ez a hármas megkülönböztetés kritikus a disszertáció későbbi eset-összehasonlítása szempontjából, mivel rávilágít az orosz információs műveleti stratégia evolúciójára és kényszerű adaptációjára. Míg a 2014-es krími művelet még dominánsan a klasszikus dezinformációra (például a "zöld emberkék" jelenlétének nyílt tagadására és a valóság meghamisítására) épült, addig a 2014 és 2021 közötti transzformációs időszakban (például a 2016-os amerikai elnökválasztás

[73] LEBRUN, Maxime (2023): *Anticipating cognitive intrusions: Framing the phenomenon*. Hybrid CoE Strategic Analysis 33. European Centre of Excellence for Countering Hybrid Threats, Helsinki. 4. o.

[74] GIANNOPOULOS, Georgios et al. (2021): *The Landscape of Hybrid Threats: A Conceptual Model*. JRC Technical Report, European Commission / Hybrid CoE.

beavatkozásai vagy a Szurkov-leaks során) fokozatosan előtérbe került a malinformation fegyverként való alkalmazása. Utóbbi esetben a támadó már nem a valóságot akarja átírni, hanem magát a valóságot (például eltulajdonított szerveradatokat) használja fegyverként. Ez az eszköz azért rendkívül veszélyes a kognitív térben, mert a hagyományos védekezési rutinok – mint a tényellenőrzés (fact-checking) – szinte teljesen hatástalanok vele szemben, hiszen a közzétett dokumentumok technikailag igazak, a pusztítást maga a kontextusból való kiragadás végzi el.

A hazai hadtudományi kutatásban Tölgyesi Beatrix 2023-as doktori értekezésében az orosz információs hadviselés elméletét elemezve rögzítette: a modern konfliktusok súlypontja a társadalmi-pszichológiai dimenzió felé tolódik, ahol az információs befolyásolás nem csupán dezinformáció, hanem a reflexív kontroll (reflexive control) eszköztára – az ellenfél döntési mechanizmusainak szándékos torzítása úgy, hogy az a támadó érdekei szerint cselekedjen.[75] [76]Tölgyesi emellett részletesen elemzi a hibrid hadviselés fogalmának tükör-kép effektusát: a nyugati értelmezésben a gyengébb fél él hibrid eszközökkel, míg az orosz interpretációban a Nyugat alkalmazza azokat, és Oroszország csupán aszimmetrikus válaszra kényszerül; Galeotti óva int, hogy az orosz aktorok mögött átfogó, összehangolt „mestertervet" feltételezzünk[77]. Kiss Álmos Péter kritikai elemzéseiben[78] rávilágít a NATO és az EU hibrid-értelmezése, valamint az orosz „nem-lineáris" hadviselés közötti alapvető különbségekre: míg a nyugati doktrínák a hibriditást reaktív módon értelmezik, addig a keleti megközelítés a folyamatos befolyásolást tekinti a stratégiai érvényesülés alapjának.

---

[75] THOMAS, Timothy L. (2016): *Russia's 21st Century Information War: Working to Undermine and Destabilize Populations*. NATO Strategic Communications Centre of Excellence, Riga. 10., 14–15. o. Thomas a reflexív kontroll (RC) fogalmát Lefebvre definíciójából eredezteti, és a Minszki tűzszünet (2014/2015) „barátságos ölelés" (Makhnin 2013) RC-alkalmazását dokumentálja.

[76] Kiss Álmos Péter (2024): Az orosz–ukrán háború céljait támogató orosz stratégiai kommunikáció. *Honvédségi Szemle*, 152. évf. 2. sz. 19–34. Online: https://real.mtak.hu/213496/1/003_KissAlmosPeter_19-34.pdf

[77] TÖLGYESI (2023) i. m. 91–92. o. Tölgyesi részletesen elemzi a tükör-kép effektust: a nyugati értelmezésben a gyengébb fél él hibrid eszközökkel, míg az orosz interpretációban a Nyugat alkalmazza azokat – Oroszország aszimmetrikus válaszra kényszerül. Galeotti óva int attól, hogy az orosz aktorok mögött átfogó, összehangolt „mestertervet" feltételezzünk.

[78] KISS Álmos Péter (2024): *Az orosz–ukrán háború céljait támogató orosz stratégiai kommunikáció*. Hadtudományi Szemle, 17. évf. 2. sz. 19–34. o.

A kognitív hadviselés paradigmáját a Hybrid CoE Strategic Analysis 33 a kognitív behatolás (cognitive intrusion) fogalmával gazdagítja. A kognitív behatolás túlmutat a dezinformáción és a félretájékoztatáson: az egyéni és kollektív mentális folyamatok szándékos manipulálását jelenti a politikai erőszak előmozdítása érdekében a liberális demokratikus társadalmakban. Lebrun keretrendszere három szintet különböztet meg: (1) a félretájékoztatás kultúrája mint termékeny kontextus; (2) a közvélemény dezorientálása az érzelmek – különösen a harag és a felháborodás – erőszakba való átcsatornázásával; és (3) az erőszak szerepe a demokratikus közvetítési rendszer felszámolásában. Ez a keretrendszer közvetlen analitikai kapcsot teremt a disszertáció OxIPO-modelljéhez: a kognitív behatolás a feldolgozás (Process) (feldolgozás) szakaszban érvényesül leginkább, ahol a reflexív kontroll logikája az érzelmi és pszichológiai diszpozíciókat aktiválja[79].

A fogalmi rés mélységét jól mutatja az orosz védelmi minisztérium 2011-es Conceptual Views on the Activities of the Armed Forces of the Russian Federation in Information Space című dokumentuma, amely összehasonlító fogalomelemzésként az információs hadviselést úgy definiálja, mint „az ellenfél politikai, gazdasági és társadalmi rendszereinek aláásása; tömeges pszichológiai kampányok lefolyása az állam populációja ellen; az állam kényszerítése az ellenfél érdekében hozott döntésekre". Thomas (2016) rámutat, hogy az „aláásni, destabilizálni, kényszeríteni" igehármas éles kontrasztban áll a NATO stratégiai kommunikációs koncepciójának „koordinált és megfelelő használat" meghatározásával. Az asszimmetria nem puszta stilisztikai: míg a nyugati keret az információt a politikai cél elérésének támogató eszközének tekinti, az orosz doktrína az információt a politikai és katonai tevékenység elsődleges szintjére emeli. Ez a doktrinális különbség közvetlenül indokolja a disszertáció FMK-rácsának szükségességét: ha az egyik fél „koordinál" és a másik „aláás", akkor a két fogalmi rendszer közötti rés maga is sebezhetőség, amelyet a diagnosztikai eszköztárnak kezelnie kell.[80]

Az orosz modell sajátosságait kiemeli az összehasonlítás a kínai megközelítéssel. Camargo Lima összehasonlító nagystratégia-elemzése – amely dokumentumelemzésen és a George/Bennett-féle

[79] LEBRUN, Maxime (2023): Anticipating cognitive intrusions: Framing the phenomenon. Hybrid CoE Strategic Analysis 33. European Centre of Excellence for Countering Hybrid Threats, Helsinki. 3. o.

[80] Orosz Védelmi Minisztérium (2011): Conceptual Views on the Activities of the Armed Forces of the Russian Federation in Information Space. Moszkva. Ismertetése: THOMAS, Timothy L. (2016): Russia's 21st Century Information War: Working to Undermine and Destabilize Populations. In: Defence Strategic Communications, Vol. 1, No. 1, NATO Strategic Communications Centre of Excellence, Riga, 11–26. 11. o.

strukturált összehasonlító (SFÖ) módszeren alapul – kimutatta, hogy míg Kína „soft balancing”-et alkalmaz (gazdasági, diplomáciai és technológiai eszközökkel), addig Oroszország „hard balancing”-re épít, amely a katonai és nem-katonai megközelítések kombinációját jelenti, beleértve az információs és kiberintézkedéseket. A fordulópontot Camargo Lima a 2008-as orosz–grúz háborúra datálja: az információs műveletek kudarca után Oroszország átállt az „aszimmetrikus megközelítésre”, amelyet a nyugati elemzők hibrid hadviselésnek neveztek. A párhuzam azért fontos, mert mutatja: a FMK Kognitív Olló jelensége nem kizárólagosan orosz sajátosság, hanem eltérő mechanizmussal a kínai esetben is megfigyelhető.[81]

3.1.2. A Fegyvernek Minősülő Kommunikáció (FMK) definíciója

A fenti jelenségek rendszerezésére a disszertáció a Fegyvernek Minősülő Kommunikáció (FMK) fogalmát vezeti be. Ez a koncepció túllép a tartalomközpontú (az igaz/hamis bináris oppozícióra épülő) elemzésen, és a jelenséget komplex műveleti termékként kezeli. Az FMK elméleti hátterét Bakir és szerzőtársai a korábbiakban már említett Szervezett Meggyőző Kommunikációról (Organized Persuasive Communication – OPC) alkotott modellje adja. Az OPC ernyőfogalomként egyesíti a propagandát, a PR-t és a stratégiai kommunikációt, felölelve a befolyásolás valamennyi fajtáját, amennyiben azok rendszerszerűen, intézményesített háttérrel és erőforrás-allokációval törekednek a célközönség viselkedésváltozásának kiváltására.

A disszertáció definíciója értelmében FMK-nak tekinthető minden olyan kommunikációs aktus, amely együttesen megfelel az alábbi három műveleti kritériumnak:

- Szándékoltság: A cselekvés mögött egyértelműen azonosítható (vagy proxyk alapján kikövetkeztethető) aktor áll, akinek célja nem a tájékoztatás, a demokratikus vita elősegítése vagy a konszenzuskeresés, hanem a kényszerítő retorika alkalmazása és a kognitív befolyásolás. A szándékos ártalom (intent to harm) megléte az a választóvonal, amely élesen megkülönbözteti az FMK-t az organikus, spontán terjedő virális tartalmaktól vagy a jóhiszemű tévedésektől[82].

[81] CAMARGO LIMA, Raphael (2019): China’s and Russia’s Grand Strategies: Comparing the Role of Strategic Communications. In: Defence Strategic Communications, Vol. 6, 2019, 83–115. 108–109. o.

[82] ANDREWS, James R. (1969): *Confrontation at Columbia: A case study in coercive rhetoric*. Quarterly Journal of Speech, 55. évf. 1. sz. 9–16. o.

- Szervezettség: A tartalom terjesztése nem organikus úton, hanem egy mesterségesen koordinált infrastruktúrán keresztül történik. Ezen a ponton válik kritikussá a platformökológia megértése: a folyamat modellezéséhez a Bruno Latour által megalkotott cselekvő-hálózat elméletet (Actor-Network Theory – ANT)[83] kell alapul venni. Latour elmélete rögzíti, hogy a társadalmi hálózatokban a nem emberi entitások (non-human actants) – esetünkben az algoritmusok, a bot-hálózatok és az automatizált szoftverek – nem pusztán passzív közvetítők (intermediaries), hanem aktív mediátorok, amelyek önállóan is formálják, torzítják és felerősítik a cselekvést és az üzenet elérését[84],[85]. Az FMK esetében ez az ember–gép hálózati szervezettség (például a szinkronizált posztolás, az algoritmikus manipuláció) szolgál a legfontosabb forenzikus bizonyítékként a műveleti jelleg alátámasztására.

- Kognitív hatás: Az elsődleges műveleti kimenet (output) nem feltétlenül egy új politikai állítás maradéktalan elhitetése. A cél sokkal inkább a döntéshozatali ciklusok (OODA-hurok) lassítása, a társadalmi polarizáció mélyítése, vagy az ellenfél kognitív túlterhelésének (information overload) előidézése. A NATO StratCom COE Trend Report 4 (2020) ugyanezt a mechanizmust a digitális kommunikációs technológia „demokratizálódásával" kontextualizálja: a magas minőségű audiovizuális tartalom előállítása és azonnali terjesztése immár bárki számára elérhető, ami az információs túlterhelés korábban elképzelhetetlen volumenét teszi lehetővé[86].

A kognitív hadviselés logikája szerint a sikerhez gyakran elegendő a gyanú elültetése és a közös valóság felszámolása. Ezt a mechanizmust írja le az agnotológia (a tudatlanság és a kétely kulturális előállításának tudománya) alapvetése: a híres „A kétely a mi termékünk" („Doubt is our product")

---

83 LATOUR, Bruno (2005): *Reassembling the Social: An Introduction to Actor-Network-Theory*. Oxford University Press, Oxford.

84 CRESSWELL, Kathrin M. – WORTH, Allison – SHEIKH, Aziz (2010): *Actor-Network Theory and its role in understanding the implementation of information technology developments in healthcare*. BMC Medical Informatics and Decision Making, 10. évf. 67. sz.

85 ORBÁN Zsolt (2021): *E-learning projektek sikertényezői. Az e-learning megoldások Actor-Network Theory elemzése*. Doktori értekezés. Budapesti Corvinus Egyetem, Budapest.

86 Hybrid CoE (2020): *Trends in the Contemporary Information Environment. Hybrid CoE Trend Report 4*. European Centre of Excellence for Countering Hybrid Threats, Helsinki.

szlogen – amely eredetileg a dohányipar 1969-es, a tudományos konszenzus szisztematikus aláásását célzó belső feljegyzéséből származik – tökéletesen megvilágítja az FMK végcélját. A fegyveresített kommunikáció a kétely mesterséges gyártásával bénítja meg a társadalmi és politikai cselekvőképességet.

A meggyőzés és a kényszerítés klasszikus dichotómiáját érdemes egy finom, de műveletileg releváns megkülönböztetéssel kiegészíteni. Jowett és O'Donnell (2011) klasszikus definíciója[87] szerint a propaganda szándékos és szisztematikus kísérlet a percepciók formálására, a kogníció manipulálására és a viselkedés irányítására, a propagandista érdekeinek megfelelően. Jacques Ellul (1965) alapműve[88] ezt a mechanizmust azzal árnyalja, hogy a modern propaganda nem feltétlenül az egyén intellektuális meggyőzésére (ortodox hiedelmek kialakítására) törekszik, hanem a pszichológiai kondicionálásra, amely közvetlen cselekvéshez vagy éppen apátiához és bénultsághoz vezethet.

Ebből a nézőpontból az FMK nem pusztán egy "tartalom", hanem egy olyan szervezett hálózati folyamat, amely a célközönség megismerési lehetőségeit és értelmezési kereteit alakítja át – akár úgy is, hogy a tényszerűséget teljesen háttérbe tolja, a törzsi csoportazonosságot (polarizációt) pedig felerősíti. A kognitív térben a „dezorientáció” ezért sosem véletlen mellékhatás, hanem a leggyakoribb explicit cél: a bizalmi infrastruktúra szétzúzása és a racionális döntéshozatal premisszáinak végleges megingatása.

Az orosz katonai gondolkodásban a fegyvernek minősülő kommunikáció fogalmának legközelebbi megfelelője a „kognitív fegyver” (kognitivnoje oruzsie) koncepciója, amelyet Szulaksin 2014-ben definiált a Tudományos Akadémia katonai folyóiratában. A doktrinális fogalomelemzés keretében Szulaksin a fogalmat úgy határozza meg: hamis tudományos elméletek, paradigmák, koncepciók és stratégiák bevezetése az ellenfél szellemi környezetébe, amelyek az államigazgatást a jelentős védelmi potenciálok gyengítésének irányába befolyásolják. Thomas 2016-ban kiemeli, hogy az információ-pszichológiai hatás logikája két lépcsős: először a társadalom tömegtudataira hat, a hazafiságot kollaborációvá kódolva, majd az eliteket és azok döntéshozatalát veszi célba. A

---

87 JOWETT, Garth S. – O’DONNELL, Victoria (2011): *Propaganda and Persuasion*. 5. kiadás. SAGE Publications, London. 7. o.

88 ELLUL, Jacques (1965): *Propaganda: The Formation of Men’s Attitudes*. Vintage Books, New York.

párhuzam a disszertáció FMK-fogalmával szembetűnő: míg az FMK a kommunikáció fegyverként való besorolásának feltételeit operacionalizálja, a kognitív fegyver-fogalom ugyanezt a jelenséget az orosz doktrína belső terminológiájában ragadja meg. A két fogalom összevetése megerősíti, hogy a kommunikáció fegyverré alakítási potenciáljának felismerése nem kizárólag nyugati akadémiai konstrukció, hanem a támadó fél doktrinális önképének is része.[89]

3.2. Kognitív hadviselés és információfeldolgozás

A fegyvernek minősülő kommunikáció (FMK) hatásmechanizmusának megértéséhez nem elegendő pusztán a technológiai közvetítő közeget vagy magát a platformot vizsgálni; a célpontot, vagyis az emberi információfeldolgozó rendszert is modellezni kell. A disszertáció e célból a Mező-féle[90] OxIPO (Organization × [Input + Process + Output]) kognitív modellt alkalmazza. Ez az integratív keretrendszer olyan klasszikus kibernetikai és pszichológiai modelleket szintetizál a modern hadviselés környezetére, mint a Wiener-féle visszacsatolás és irányítás logikája, a Shannon–Weaver-féle kommunikációs átviteli modell, valamint a kognitív pszichológia kettős folyamatú információfeldolgozási megközelítése. E modellek részletes operacionalizálását és a köztük lévő megfeleltetéseket a következő alfejezetekben bontom ki, amikor az OxIPO Input–Process–Output elemeit rávetítem az FMK tipikus műveleti láncára.

Az OxIPO-modell kiinduló alapvetése, hogy az egyén a kommunikációs hálózatban nem egy passzív tartály, hanem aktív, ugyanakkor biológiailag korlátozott kapacitású feldolgozóegység, amelynek működését és értékelési rutinjait a fegyveresített kommunikáció szisztematikusan képes megzavarni.

A kognitív hadviselés védekezői oldalának elméleti megalapozásához a Hybrid CoE Strategic Analysis „stratégiai polgár” (strategic citizen) koncepciója szolgáltat fontos keretet. Az elemzés arra mutat rá, hogy a közösségi média korában a katona és a civil közötti választóvonal elmosódott: a civil társadalom maga vált hadszíntérré, amelyet az információáramlás tesz lehetővé. Ha a „stratégiai tizedes” (strategic corporal) koncepciója a 9/11utáni katonai gondolkodás terméke volt,

---

[89] SULAKSHIN, S. S. (2014): Cognitive Weapons — A New Generation of Information Weapon. In: Journal of the Academy of Military Science, No. 1, 57–65. Ismertetése: THOMAS (2016) i. m. 17. o.

[90] MEZŐ Ferenc – MEZŐ Katalin (2019): *Az OxIPO-modell – az interdiszciplináris kutatások egy lehetséges értelmezési kerete*. OxIPO – interdiszciplináris tudományos folyóirat, 2019/1. sz. 9–21. o.

a „stratégiai polgár” a hibrid hadviselés korszakának felismerése. Ez a belátás közvetlen következményekkel jár a demokratikus társadalmak civil-katonai kapcsolataira: a védekezés nem szűkíthető le az állami szervekre, hanem egész társadalmi megközelítést igényel[91].

A dezinformáció hatásmechanizmusainak elemzésekor nem kerülhető meg a társadalmi fenntarthatóság kérdésköre sem. Az infodémia (infodemic) jelensége – amely a COVID–19 világjárvány alatt vált globálisan is kritikussá – rávilágított, hogy a túlzott mennyiségű, gyakran pontatlan vagy egymásnak ellentmondó információ akadályozza a lakosságot a helyes döntéshozatalban és a hatékony állami védekezésben. A Hybrid CoE CORE Comprehensive Resilience Ecosystem elemzése a COVID-pandémia példáján mutatta ki, hogy az exogén sokk hatására az állampolgári, kormányzati és szolgáltatási terek közötti komplex interdependenciák kaszkádhatásokat generálnak, és a hibrid fenyegetési aktorok célzottan kihasználják a szolgáltatási tér megbízhatóságának hiányát[92]. Ez a fajta információs zavar közvetlenül veszélyezteti a társadalmi kohéziót, mivel a bizonytalanság és a félelem mesterséges felerősítésével erodálja az intézményrendszerekbe (egészségügy, kormányzat, tudomány) vetett bizalmat.

A kognitív pszichológia Human Information Processing (HIP) modelljére építve az OxIPO-modell első eleme az Input (I), vagyis az inger-túlterhelés és a bemeneti manipuláció szakasza. A digitális információs térben a bemeneti ingerek volumene exponenciálisan nő, amelyet a RAND Corporation kutatói, Christopher Paul és Miriam Matthews a Firehose of Falsehood (a hazugság tűzoltótömlője) modellel[93] írnak le. Ebben a fázisban a támadó (különösen az orosz doktrína alapján) nem a minőségi, logikus meggyőzésre épít, hanem a gátlástalan, nagy volumenű, többcsatornás és gyors üzenetáradatra. A stratégiai cél a célpont figyelmének teljes lefoglalása és a kognitív fárasztás: ha a befogadó sokszor, sokféle forrásból találkozik egy állítással, az agy az ismétlődést a hitelesség jeleként (familiarity effect) kódolja.

---

91 FALK, Barbara J. (2020): Strategic citizens: Civil society as a battlespace in the era of hybrid threats. Hybrid CoE Strategic Analysis 25. European Centre of Excellence for Countering Hybrid Threats, Helsinki.

92 JUNGWIRTH, Richard et al.: CORE – Comprehensive Resilience Ecosystem: A Practitioner’s View. Hybrid CoE, 2023.

93 PAUL, Christopher – MATTHEWS, Miriam (2016): *The Russian “Firehose of Falsehood” Propaganda Model*. RAND Corporation, Santa Monica. 1–2. o.

Ahogy arra Prier[94] is rámutat, a közösségi média mint modern hadszíntér immár a „trendek uralásáról" szól: aki uralja a platformok algoritmikus hírfolyamát, az uralja a valóságérzékelést. Külföldi példaként említhető az orosz trollgyárak szinkronizált tevékenysége a nyugati választási kampányok idején, míg hazai viszonylatban a COVID-19 infodémia során tapasztalt összehangolt, vírusszkeptikus posztolási hullámok szemléltetik tökéletesen ezt a „tűzoltótömlő" taktikát.

Szintén az Input szakaszban jelenik meg a zagyválás (bullshit) Harry Frankfurt által leírt jelensége[95] is. Frankfurt elmélete rögzíti, hogy míg a hazug ember tisztában van az igazsággal és azt próbálja elrejteni, addig a zagyváló aktort (bullshitter) egyáltalán nem érdekli a tények igazságtartalma, kizárólag a pillanatnyi narratív hatás és a figyelem uralása a célja. Erre a mechanizmusra kiváló példa Donald Trump egykori amerikai elnök azon nyílt beismerése, miszerint egy Justin Trudeau kanadai miniszterelnökkel folytatott kereskedelmi tárgyalásán ad-hoc módon kreált gazdasági adatokat, pusztán a tárgyalási dominancia fenntartása érdekében[96]. Magyar kontextusban e jelenség megfelelői a kampányidőszakok azon "szakértői" jóslatai, amelyek mindenféle adatalapú bizonyíték nélkül, pusztán érzelmi alapon vizionálnak azonnali államcsődöt vagy precedens nélküli jólétet a szavazók mozgósítása érdekében.

A modell második eleme a Process (P), vagyis a feldolgozási kapacitás kimerülése. Az emberi agy munkamemóriája biológiailag korlátozott – ahogy azt George A. Miller klasszikus „bűvös 7±2" törvénye[97] leírja –, így ha a beérkező információ komplexitása és sebessége meghaladja ezt a küszöböt, a kognitív rendszer védekező üzemmódba vált. Az FMK pontosan ezt a kapacitáskorlátot fegyveresíti. Daniel Kahneman terminológiájával élve a cél az, hogy a kognitív túlterheléssel energiát vonjanak el, és ezáltal „kikapcsolják" a lassú, analitikus és racionális (System 2) gondolkodást, átengedve az irányítást a gyors, heurisztikákra és érzelmi reflexekre épülő (System 1) hálózatnak.

---

94 PRIER, Jarred (2017): *Commanding the Trend: Social Media as Information Warfare*. Strategic Studies Quarterly, 11. évf. 4. sz. 50–85. o.

95 FRANKFURT, Harry G. (2005): *On Bullshit*. Princeton University Press, Princeton, NJ.

96 THE WASHINGTON POST (2018): *Trump admits he made up facts in trade meeting with Justin Trudeau*. 2018. március 15.

97 MILLER, George A. (1956): *The Magical Number Seven, Plus or Minus Two*. Psychological Review, 63. évf. 2. sz. 81–97. o.

Ebben a terhelt, asszociatív fázisban nyer teret a korábban említett szándékos félreértelmezés (strategic misinterpretation) [98], amelyet Paul Bernal (2021) a jogi szabályozási kísérletek kudarcának egyik fő okaként nevez meg. A támadó itt tudatosan torzítja el a célpont eredeti üzeneteit, hogy agresszorként, vagy épp nevetségesként állítsa be őt. Külföldi példa a „Birds Aren't Real" (A madarak nem igaziak) mozgalom, amely bár eredetileg szatírának indult, bebizonyította, hogy a szándékosan kiforgatott és áltudományosnak tűnő adatok köré is pillanatok alatt felépíthető egy valóság-tagadó, elkötelezett politikai identitás. Hazai példaként a politikai diskurzus azon mindennapos gyakorlata említhető, amikor az ellenfél egy-egy félmondatát kiragadják eredeti kontextusából, és az algoritmikus terjesztés során tudatosan olyan új jelentéssel ruházzák fel, amely alkalmas társadalmi felháborodás keltésére.

Végül, az Output (Out) szakaszban a torzult információfeldolgozás tényleges, fizikai vagy politikai cselekvésként realizálódik. Ebben a végső állapotban a döntéshozó vagy a választópolgár már nem a racionális mérlegelés, hanem a System 1 által aktivált heurisztikák és a félelemérzet alapján reagál: pánikból megoszt egy megtévesztő információt, irracionális egészségügyi vagy gazdasági döntést hoz, esetleg agresszíven fellép a vélt ellenséggel szemben. A Hybrid CoE Working Paper 29. száma dokumentálta, hogy az orosz dezinformáció több esetben is közvetlenül fizikai következményekhez vezetett: az Egyesült Királyságban 2020 áprilisában húsz 5G-mobiladót rongáltak meg az 5G-COVID összeesküvés-elmélet hatására; Ukrajnában a Kreml-dezinformáció a Novi Szanzsari településen az evakuáltak elleni erőszakos támadást provokált[99]. Az FMK kimenete ezen a ponton lép át a virtuális térből a fizikai valóságba, bizonyítva a hadtudományi tételt: a torzult percepció torzult társadalmi cselekvést szül.

3.2.1. A kognitív sebezhetőség anatómiája: Inger-túlterhelés és feldolgozási paralízis

A kognitív pszichológia Human Information Processing (HIP) megközelítése az emberi megismerést korlátozott kapacitású, szakaszolt feldolgozórendszerként írja le. Donald Broadbent

[98] BERNAL, Paul (2021): *Misunderstanding Misinformation: why most 'fake news' regulation is doomed to failure*. British Association of Comparative Law, 2021. január 29.

[99] HOYLE, Aiden – ŠLERKA, Josef (2024): Cause for concern: The continuing success and impact of Kremlin disinformation campaigns. Hybrid CoE Working Paper 29, Helsinki.

klasszikus szűrő-elmélete (filter theory)[100] bizonyította, hogy az emberi figyelem egy szűk keresztmetszeten keresztül szelektál a bejövő ingerek között, megakadályozva a kognitív rendszer azonnali túlterhelődését. Ezt egészíti ki Atkinson és Shiffrin több-táras memóriamodellje[101], amely rávilágít, hogy a szenzoros regiszterből a munkamemóriába, majd a hosszú távú memóriába (stabil értelmezésig és döntésig) jutó információ feldolgozása kognitív energiát és időt igényel. Az OxIPO-modellel a disszertáció ezt az információfeldolgozási logikát helyezi hadműveleti kontextusba. A modell láthatóvá teszi, hogy az extrém információs túlterhelés hogyan zúzza szét Broadbent szűrőjét, és hogyan tolja el a feldolgozást az ellenőrizhető, racionális mérlegeléstől a gyors, alapértelmezett (heurisztikus) mintázatfelismerés irányába. Vagyis a Fegyvernek Minősülő Kommunikáció (FMK) nem egyszerűen „üzeneteket" céloz a térben, hanem a döntéshozó figyelmi és munkamemória-kapacitását támadja. Ha ezt a kapacitást telíti, a kontrollált feldolgozás aránya drasztikusan csökken, a hibás ítéletek valószínűsége pedig megnő. A kríziskommunikációs irodalom összhangban van ezzel a megállapítással: a CDC CERC-kézikönyvének krízis-pszichológiai fejezete négy jellegzetes információfeldolgozási módot azonosít krízishelyzetben (egyszerűsítés, alagúteffektus, tagadás, regresszió), amelyek az OxIPO Process-dimenziójának empirikus alátámasztását nyújtják.[102]

A modell első kritikus fázisa az Input (I), amely a digitális ökoszisztémában az inger-túlterhelés jelenségében manifesztálódik. Ebben a térben a bemeneti ingerek – legyenek azok közösségi média posztok, azonnali értesítések vagy szubliminális vizuális jelek – volumene exponenciálisan növekszik, messze meghaladva az egyén biológiai szelekciós képességét. Christopher Paul és Miriam Matthews ezt a jelenséget, mint korábban említettem, a Firehose of Falsehood (a hazugság tűzoltótömlője) modellként azonosította[103]. Megállapításuk szerint a modern – elsősorban az orosz

---

[100] BROADBENT, Donald E. (1958): *Perception and Communication*. Pergamon Press, London.

[101] ATKINSON, Richard C. – SHIFFRIN, Richard M. (1968): *Human memory: A proposed system and its control processes*. In: SPENCE, K. W. – SPENCE, J. T. (szerk.): The Psychology of Learning and Motivation (Vol. 2). Academic Press, New York. 89–195. o.

[102] CDC (2019): Psychology of a Crisis. CERC Manual, 2019 Update. Centers for Disease Control and Prevention, CS 290397-E. A kézikönyv a krízis során történő információfeldolgozás négy módját (simplification, tunnelling, denial, regression) azonosítja, amelyek az OxIPO Process-dimenziójával összhangban a korlátozott kapacitású feldolgozás különböző állapotait írják le.

[103] PAUL, Christopher – MATTHEWS, Miriam (2016): *The Russian "Firehose of Falsehood" Propaganda Model*. RAND Corporation, Santa Monica. 2. o.

doktrínákban megfigyelhető – propaganda már nem a klasszikus, minőségi meggyőzésre és a logikai koherenciára épít. Ehelyett a nagy volumenű, többcsatornás, rendkívül gyors és gátlástalanul ismétlődő üzenetáradattal operál. Ebben a megközelítésben a műveleti cél a figyelem teljes elárasztása és a kognitív védekező mechanizmusok kimerítése, mivel a mai figyelemgazdaságban a fókuszált figyelem vált a legszűkebb, így katonai szempontból a leginkább sebezhető erőforrássá.

A kognitív hadviselés egyik legkevésbé vizsgált, mégis kritikus eszköze a tudatküszöb alatti (szubliminális) befolyásolás, amely a nyílt (szupraliminális) üzenetekkel összehangolva képes a döntéshozatali lánc észrevétlen eltolására. A Berni Egyetem kutatói (Simon Ruch, Katharina Henke és munkatársaik) által végzett neuropszichológiai kísérletsorozatok[104],[105] technikai részletei rávilágítanak e módszer rejtett hadműveleti hatékonyságára. A kutatás során alkalmazott „sandwich masking" (maszkolt felvillanás) protokoll lényege, hogy a célingert – például egy arcot és egy hozzá társított fogalmat – rendkívül rövid ideig, mindössze 17 ezredmásodpercig villantják fel zajmaszkok közé szorítva, ami fizikai gátat szab az inger tudatossá válásának. A vizsgálat során egy 6 másodperces „rejtett kódolási epizód" alatt, tizenkét ismételt felvillanás révén igazolták, hogy a hippocampus-alapú relációs kódolás tudatos észlelés nélkül is beindul. Ez a neurológiai folyamat lehetővé teszi a szavazó vagy döntéshozó agyában több elem tartós összekapcsolását (például egy politikai szereplő arca és egy negatív konnotáció). A kísérleti eredmények bizonyították, hogy egy rövid konszolidációs pihenő után a résztvevők tudatos döntései megbízhatóan – a véletlen szintje felett – a szubliminálisan betáplált irányba tolódtak el. Hadtudományi szempontból ezen „mikro-előkészítés" technikák jelentősége abban áll, hogy a kognitív túlterhelés és a szubliminális befolyásolás együttes alkalmazása megszünteti a befogadó képességét arra, hogy különbséget tegyen saját meggyőződése és a külsőleg indukált mesterséges ingerek között. A vonatkozó 7. táblázat: A szubliminális kísérletek paraméterei és műveleti relevanciája címmel a mellékletben található.

---

[104] RUCH, Simon – ZÜST, Mark A. – HENKE, Katharina (2016): *Subliminal messages exert long-term effects on decision-making*. Neuroscience of Consciousness, 2016. évf. 1. sz.

[105] RUCH, Simon – HERBERT, E. – HENKE, Katharina (2017): *Subliminally and supraliminally acquired long-term memories jointly bias delayed decisions*. Frontiers in Psychology, 8. évf. 1542. sz.

Az online platformok gazdasági modellje és a kognitív hadviselés mechanizmusai között ma már szoros szimbiózis figyelhető meg. Míg a közösségi média algoritmusai a felhasználói elköteleződés (engagement) maximalizálása érdekében az érzelmileg túlfűtött és megosztó tartalmakat részesítik előnyben, addig a kognitív műveletek aktorai pontosan ezeket a technológiai sajátosságokat (disparate impact) használják fel a dezinformáció virális terjesztésére. A NATO StratCom COE Robotrolling 2023–2024 elemzése empirikusan bizonyította ennek a mechanizmusnak az ipari léptékét: a NATO-hoz kapcsolódó automatizált kommentek aránya az angol nyelvű Twitter(X)-en mintegy 7%-ot, az orosz nyelvűn mintegy 15%-ot, a VKontaktén pedig mintegy 38%-ot ért el[106]. E folyamat során az álhír nem csupán téves tartalom, hanem egyfajta algoritmikus lőszer, amely a platformok profitérdekeire építve kerüli meg a hagyományos kapuőr-szerepeket. A NATO StratCom COE már 2018-ban dokumentálta a közösségi média manipuláció fejlődési ívét – az imperszonáció, a botnet-alapú keresőmotor-manipuláció és az kódolt üzenetrendszer (encrypted messaging) platformok felé való elmozdulást.[107] A támadások hatékonyságát tovább növeli az úgynevezett adatvákuum (data void) jelensége, amelyet Golebiewski és Boyd azonosított[108]. Ez a sebezhetőség akkor alakul ki, amikor egy váratlan, nagy érdeklődésre számot tartó krízisesemény kapcsán még nem áll rendelkezésre elegendő ellenőrzött információ. A hibrid aktorok ezt a keresési vákuumot használják fel arra, hogy saját, kulcsszavakra optimalizált narratíváikkal árasszák el a teret, mielőtt a hivatalos szervek reagálni tudnának. A Hybrid CoE Research Report 2 (Jean-Baptiste et al. 2021) négy ország dezinformáció-elleni gyakorlatait vizsgálva dokumentálta[109] ezt az aszimmetriát: Svédországban a Polgári Védelmi Hatóság (MSB) 2016 óta 16 000 köztisztviselőt képzett ki információs befolyásolás elleni programjában, míg az Egyesült Királyságban a GCHQ kapott kibervédelmi mandátumot az oltásdezinformáció ellen.

---

106 NATO STRATCOM COE: Robotrolling 2023–2024. Riga, 2024.

107 NATO STRATCOM COE (2018): *Social Media Manipulation: Trends and Developments*. NATO Strategic Communications Centre of Excellence, Riga. 5. o. A kiadvány az imperszonáció, a botnet-alapú keresőmotor-manipuláció (MH17 hamis narratívák PageRank-emelése), a deepfake-előrejelzés és az encrypted messaging platformok felé való elmozdulást dokumentálja.

108 GOLEBIEWSKI, Michael – BOYD, danah (2018): *Data Voids: Where Missing Data Can Easily Be Exploited*. Data & Society Research Institute.

109 Jeangène Vilmer, Jean-Baptiste (2021): *Effective State Practices Against Disinformation: Four Country Case Studies.* Helsinki: Hybrid CoE.

Ebben a környezetben az FMK egyik legfőbb műveleti erőssége sokszor nem maga az üzenet, hanem a formátum. A hírműfajhoz kapcsolt társadalmi rutinok (aktuálisnak tűnő, "forrásolt", egyszerű ok-okozati összefüggéseket kínáló dizájn) drasztikusan csökkentik a befogadó ellenőrzési késztetését, különösen a feljebb vázolt túlterheléses állapotban. Edward Bernays[110] , a modern PR megalapítója már évszázaddal ezelőtt rögzítette, hogy a tömegek befolyásolása nem logikai érveléssel történik, hanem a közönség meglévő sztereotípiáiba illeszkedő, mesterséges események (pseudo-events) és látszatvalóságok megteremtésével. A fegyveresített kommunikáció pontosan ezt a logikát emeli át a digitális térbe: a hírszerű álcázás révén végrehajtja a hitelesség-eltérítést (credibility hijacking), így a befogadó a legitim hírműfajba vetett előzetes bizalmát adja kölcsön a manipulált tartalomnak.

A folyamat következő szintje a Process (P), vagyis a feldolgozási kapacitás kimerülése. Ahogy arra George A. Miller 1956-ban megalkotott klasszikus kognitív törvénye[111] is rámutatott, az emberi munkamemória véges kapacitású, egyszerre csupán 7±2 információs egység aktív kezelésére képes. Amennyiben a bemeneti inger (az árasztás) komplexitása, sebessége vagy érzelmi töltete meghaladja ezt a küszöbértéket, az információfeldolgozó rendszer kényszerű védekező üzemmódba vált. Daniel Kahneman Nobel-díjas pszichológus rendszere kettős folyamat elméletébe[112] illesztve az FMK műveleti célja, hogy a folyamatos kognitív stresszel energiát vonjon el az agytól, ezáltal szisztematikusan kikapcsolva az analitikus, logikai alapú gondolkodást. Amikor a rendszer Miller-féle kapacitása túlterhelődik, az irányítást automatikusan az ösztönös, gyors és érzelmi alapú veszi át. Ebben a regresszív fázisban a döntéshozó már képtelen a racionális mérlegelésre; ítéleteit a leghangosabb heurisztikák és az elemi túlélési reflexek (félelem, harag) határozzák meg.

Végezetül az Output (Out) szakaszban a torzult cselekvés realizálódik: a bemeneti zavar és a feldolgozási hiba a fizikai és társadalmi térben konvertálódik akcióvá. Ebben a kognitív állapotban a kimenet már nem tekinthető szuverén, racionális döntésnek, csupán egy manipulált, reflexszerű

---

110 BERNAYS, Edward (1923/2019): *Crystallizing Public Opinion*. Dover Publications, New York.

111 MILLER, George A. (1956): *The Magical Number Seven, Plus or Minus Two*. Psychological Review, 63. évf. 2. sz. 81–97. o.

112 KAHNEMAN, Daniel (2013): *Gyors és lassú gondolkodás*. HVG Könyvek, Budapest.

válasznak. A nemzetbiztonsági veszélyeztetettség a társadalom minden szintjén megjelenik: az átlagfelhasználó kritikátlanul osztja meg a dezinformációt, a gazdasági szereplők a mesterséges zaj hatására pánikreakciókat (például tőzsdei eladási hullámokat) indítanak el, a kritikus infrastruktúrák vagy a katonai parancsnoki láncok operátorai pedig a kognitív túlterheltség állapotában végzetes döntéseket hozhatnak.

3.2.2. A tudatküszöb alatti fegyverek: A neurobiológiai kódolástól a mesterséges intelligencia árnyék-meggyőzéséig

A kognitív hadviselés (cognitive warfare) eszköztárának komplexitását vizsgálva a kutatás nem szorítkozhat kizárólag a nyílt, tudatosan észlelt narratívák elemzésére. A fegyvernek minősülő kommunikáció (FMK) egyik legkritikusabb, ugyanakkor legnehezebben detektálható dimenziója a tudatküszöb alatti, úgynevezett szubliminális ingerek műveleti alkalmazása. A modern neurobiológiai és kognitív pszichológiai kutatások egyértelműen rögzítik, hogy ez a jelenség már nem a tudományos-fantasztikus spekulációk, hanem a szigorúan mérhető és hadműveleti célokra konvertálható pszichológiai hatások tartományába tartozik.

A gyakorlat nyelvére fordítva: a technológiai fejlődés, különösen a mesterséges intelligencia (MI) térnyerése, ezt a pszichológiai sérülékenységet ipari mértékben alkalmazható fegyverré formálta. Míg a laboratóriumi kísérletek vizuális maszkolásra építettek, az algoritmikus térben a szubliminális befolyásolás szemantikai és strukturális szinten is megjelenik. Dr. Lance B. Eliot, a mesterséges intelligencia kutatásának elismert amerikai szakértője és technológiai tanácsadója az „árnyék-meggyőzés” (shadowy persuasion) elméletében[113] modellezi ezt a fenyegetést. Eliot elemzése rámutat, hogy a nagy nyelvi modellek (LLM) és a generatív MI rendszerek – akár emberi utasításra, akár a tanulási folyamat algoritmikus sajátosságaiból fakadóan – képesek olyan rejtett mintázatokat, manipulatív nyelvi affirmációkat vagy vizuális mikro-ingereket beépíteni a hétköznapi tartalmakba, amelyeket a felhasználó tudatosan nem vesz észre. Az árnyék-meggyőzés logikája az FMK keretrendszerében azért jelent extrém nemzetbiztonsági kockázatot, mert a generatív modellek skálázhatósága révén a pszichológiai kondicionálás – például a bizonytalan

[113] ELIOT, Lance B. (2024): *Generative AI Uses Subliminal Messaging For Shadowy Persuasion*. Forbes, 2024. október 20.

szavazói rétegek vagy a döntéshozók észrevétlen orientálása – immár nem egyedi laboratóriumi eset, hanem milliárdos felhasználói bázison, valós időben végrehajtható művelet.

3.2.3. A véleménybuborékok és a megerősítési torzítás

A dezinformáció műveleti hatékonysága végső soron a befogadó pszichológiai sebezhetőségének és a terjesztési környezet strukturális sajátosságainak szimbiózisában rejlik. A véleménybuborékok (filter bubbles) elméletében a közösségi média algoritmusai mesterségesen zárt információs tereket hoznak létre. Ezek a technológiai elzártságok folyamatosan, súrlódás nélkül visszaigazolják a felhasználó meglévő világképét, ezáltal elősegítik a hasonló gondolkodású csoportok radikális elkülönülését, azaz a törzsi táborokba rendeződést.

A Fegyvernek Minősülő Kommunikáció (FMK) ezt az organikus platform-elzárkózást használja fel elsődleges hadszíntérként. A hálózatba kapcsolt térben a narratívák láthatóságát nagy elérésű, automatizált botok és inautentikus álprofil-hálózatok képesek manipulatív módon felerősíteni. Ennek technológiai következménye, hogy a platform algoritmusa a mesterséges interakciókat „felkapott” (trending) témaként érzékeli, és további organikus elérést biztosít a tartalomnak. A befogadói térben így sikeresen előállítható a „mindenki erről beszél” hamis benyomása. A jelenség a hibrid hadviselés eszközrendszerében azért kritikus, mert maga a platformmechanika válik a kognitív művelet direkt multiplikátorává.

Katja Valaskivi a Hybrid CoE számára készített elemzésében ezt a jelenséget tartalmi zavarnak (content confusion) nevezi, rámutatva, hogy a probléma túlmutat az álhírek (fake news) leegyszerűsítő keretén: a digitális médiaökoszisztémában összeomlottak azok a hitelességi konvenciók, amelyek korábban lehetővé tették a befogadó számára a tartalom típusának, forrásának és szándékának azonnali beazonosítását. Az FMK műveleti hatékonysága éppen ebben a tartalmi zavarban gyökerezik.[114]

[114] VALASKIVI, Katja (2018): Beyond Fake News: Content confusion and understanding the dynamics of the contemporary media environment. Hybrid CoE Strategic Analysis 5. European Centre of Excellence for Countering Hybrid Threats, Helsinki. 2–4. o.

Ebben a mesterségesen szűkített és érzelmileg túlfűtött térben drasztikusan felerősödik a megerősítési torzítás (confirmation bias) kognitív jelensége. Csepeli György[115] és Síklaki István[116] szociálpszichológusok a meggyőzés és a csoportdinamika kutatása során bizonyították, hogy az egyén – kognitív energiát spórolva – reflexszerűen elfogadja azokat az információkat, amelyek illeszkednek a már rögzült előítéleteihez, miközben kritika nélkül, agresszíven elutasítja a tényalapú cáfolatokat . A véleménybuborék logikája miatt a belső kommunikáció a tényalapú mérlegelés helyett a puszta érzelmi azonosulást erősíti. Gunhild Hoogensen Gjørv és Outi Jalonen, a Hybrid CoE biztonságpolitikai kutatói stratégiai elemzésükben[117] rámutatnak, hogy a modern dezinformációs műveletek pontosan ezt az identitás-alapú azonosulást fegyveresítik. A kognitív manipuláció célja a modern társadalmakban eleve meglévő osztály-, nemi vagy politikai törésvonalak áthidalhatatlan kognitív szakadékká történő mélyítése, ahol a „mi" és az „ők" irracionális ellentéte végül teljesen felülírja az objektív valóságérzékelést.

Ez a pszichológiai zárvány-mechanizmus magyarázza a városi legendák és az összeesküvés-elméletek modern, virális terjedését is. Jan Harold Brunvand amerikai folklorista professzor az „urban legends" (városi legendák) elméletének[118] megalkotójaként a kortárs mítoszok elemzésekor rögzítette, hogy ezek a történetek sosem véletlenszerűek: mindig a mélyen gyökerező társadalmi szorongásokra, kollektív reményekre és fenyegetettség-érzetre építenek . Marinov Iván tényellenőrző újságíró és mítoszkutató hazai elemzései is igazolják, hogy a klasszikus vándormotívumok – mint például a mikrohullámú sütőben szárított macska közismert legendája – képesek folyamatosan újrakódolni az új technológiáktól vagy a társadalmi változásoktól való irracionális félelmeket[119].

---

115 CSEPELI György (1997): *Szociálpszichológia*. Osiris, Budapest.

116 SÍKLAKI István (1997): *A meggyőzés pszichológiája*. Scientia Humana, Budapest.

117 HOOGENSEN GJØRV, Gunhild – JALONEN, Outi (2023): *Identity as a tool for disinformation*. Hybrid CoE Strategic Analysis 34. European Centre of Excellence for Countering Hybrid Threats, Helsinki. 3–4. o.

118 BRUNVAND, Jan Harold (1981): *The Vanishing Hitchhiker: American Urban Legends and Their Meanings*. W. W. Norton & Company, New York. 3-4.o.

119 MARINOV Iván (2019): *Városi legendák: Mik azok, és miért hiszünk nekük?* Urbanlegends.hu, 2019. február 11.

A gyakorlat nyelvére fordítva ez azt jelenti, hogy a pszichológiai hadviselés és az FMK számára a véleménybuborék és az emberi megerősítési torzítás a leghatékonyabb fegyverarzenál. A támadó félnek nem kell a nulláról új hazugságokat kitalálnia és azokat nehézkesen elhitetnie a közönséggel; logisztikailag sokkal célravezetőbb a célcsoport már létező, a buborékban keringő félelmeit és kulturális hiedelmeit felerősíteni, majd azokat egy gondosan megkonstruált geopolitikai vagy belföldi ellenségképhez csatolni.

3.2.4. A kognitív befolyásolás nem klasszikus eszköztára: a narratív dominancia és a bizalomvesztés mechanizmusai

A kognitív hadviselés során alkalmazott „nem klasszikus" információs eszközök elsődleges célja a döntéshozatali környezet radikális átalakítása. A támadó fél arra törekszik, hogy a célpont számára – legyen az egy politikai vezető vagy a társadalom széles rétege – kizárólag a manipulátor által preferált értelmezési keretek maradjanak elérhetőek. Ennek az operációs logikának a legfontosabb módszertani alapját Robert M. Entman amerikai kommunikációkutató professzor keretezés (framing) elmélete[120] adja.

Entman klasszikus meghatározása szerint a keretezés egy tudatos szelekciós folyamat: a kommunikátor a valóság bizonyos aspektusait szándékosan kiemeli , miközben más, kontextualizáló elemeket elfed. Ennek célja egy konkrét problémaértelmezés, egy morális ítélet, vagy egy specifikus kezelési javaslat sulykolása a befogadóban. A hibrid hadviselésben ez nem csupán retorikai fogás, hanem a narratív dominancia megszerzésének legfőbb fegyvere. Külföldi példaként említhető a 2014-es ukrajnai események orosz katonai keretezése, amely a legitim, alulról szerveződő népmozgalmat következetesen „fasiszta puccsként" definiálta, ezzel a hazai közönség számára előre legitimálva az orosz beavatkozás „felszabadító" jellegét. Hazai viszonylatban a keretezés mechanizmusa kiválóan tetten érhető a komplex szakpolitikai kérdések (például az energiabiztonság vagy a migráció) tisztán érzelmi és biztonságpolitikai dimenzióba történő áthelyezésében. Ilyenkor a racionális, technikai részletek megvitatása helyett a „nemzeti fennmaradás" vagy a „külső fenyegetés" narratívája válik a közbeszéd egyetlen, kizárólagos értelmezési keretévé.

---

[120] ENTMAN, Robert M. (1993): *Framing: Toward Clarification of a Fractured Paradigm*. Journal of Communication, 43. évf. 4. sz. 51–58. o.

A keretezés mellett a kognitív műveletek másik pillére a befogadói tér szisztematikus megzavarása. Ettől a ponttól élesen el kell választani a tisztán gazdasági célú kattintásvadászatot (clickbait) a műveleti szintű kognitív támadásoktól. Az utóbbi kategóriába tartozik az a technika, amelyet Paul Bernal, a Kelet-Angliai Egyetem (UEA) informatikai jogi docense a szándékos félreértelmezés (strategic misinterpretation) koncepciójával ír le. Bernal elmélete[121] szerint a támadó fél ilyenkor tudatosan, célzottan torzítja el a célpont eredeti üzeneteit, kiforgatva a kontextust annak érdekében, hogy az áldozatot agresszorként, inkompetensként vagy fenyegetésként állítsa be. Ez a technika azért különösen veszélyes, mert a jogalkotók és a platformok moderátorai gyakran figyelmen kívül hagyják e félreértelmezések szándékos, hadműveleti (kárkozó) jellegét, és puszta véleménynyilvánításként kezelik azokat.

A kognitív fegyvertár következő, a társadalmi kohézió és az intézményi bizalom felszámolását célzó szintjét az összeesküvés-elméletek (conspiracy theories) és a modern városi legendák jelentik. Joseph E. Uscinski és Joseph M. Parent amerikai politológusok és összeesküvés-kutatók elméleti keretrendszere[122] rögzíti, hogy az összeesküvés-elméletek nem szimplán téves vagy hiányos információk. Ezek mélyen strukturált, hatalmi viszonyokról szóló narratívák, amelyek a társadalmi és gazdasági problémákat kivétel nélkül egy „gonosz, árnyékban működő elit" titkos, ártó tevékenységével magyarázzák . Műveleti szempontból ezek az elméletek a kognitív destabilizáció leghatékonyabb eszközei, mivel hermetikusan lezárják a befogadó elméjét, és eleve immunissá teszik őt a hivatalos, intézményi cáfolatokkal szemben – mondván, a cáfolatot is a „háttérhatalom" rendelte el. Külföldi példaként a QAnon mozgalom említhető[123], amely a demokratikus intézményrendszerbe vetett alapvető hitet számolta fel követői körében. Hazánkban a „háttérhatalmi" machinációkról vagy a COVID-19 vakcinákba rejtett mikrochipekről szóló teóriák illusztrálják szemléletesen, hogyan képes egy fegyveresített narratíva áthidalhatatlan kognitív árkokat ásni a társadalmi csoportok közé.

---

[121] BERNAL, Paul (2021): *Misunderstanding Misinformation*. British Association of Comparative Law, 2021. január 29.

[122] USCINSKI, Joseph E. – PARENT, Joseph M. (2014): *American Conspiracy Theories*. Oxford University Press, New York.

[123] EURONEWS (2020): QAnon in Europe: How the COVID pandemic helped promote a dangerous conspiracy theory. *Euronews*, 2020. október 23. Online: https://www.euronews.com/my-europe/2020/10/23/qanon-in-europe-the-meteoric-rise-of-a-dangerous-conspiracy-theory-boosted-by-the-pandemic

Ezt az intézményellenes folyamatot támogatják meg a Jan Harold Brunvand folklorista által 1981-ben definiált városi legendák, amelyek nem racionális érvekre, hanem mélyen gyökerező közösségi félelmekre és szorongásokra építik hatásukat. Míg Brunvand klasszikus civil példája, a „mikróban szárított macska" (MARINOV 2019) csupán a modern háztartási technológiáktól való kezdeti félelmet jelenítette meg, addig a Fegyvernek Minősülő Kommunikáció keretében ezek a legendák militarizálódnak. Hibrid konfliktusok idején a „mérgezett ivóvízkutakról", a „külföldi szabotőrökről" vagy a „titkos éjszakai mozgósításról" szóló rémhírek formájában térnek vissza, közvetlenül a hátország pszichológiai morálját támadva.

A fenti narratívák elleni védekezés, azaz a tényellenőrzés (fact-checking) és a korrekciók kudarca nem a véletlen műve, hanem kognitív szükségszerűség. Stephan Lewandowsky és Ullrich Ecker kognitív pszichológusok a memóriakutatásaik során írták le az úgynevezett „tartós hatás" (continued influence effect) kognitív torzítását. Elméletük empirikusan igazolja, hogy ha egy hamis állítás egyszer már beépült a befogadó egy adott eseményről alkotott koherens mentális modelljébe, a később érkező hivatalos cáfolat azt szinte soha nem képes nyomtalanul törölni. A cáfolat csupán egy versengő magyarázattá gyengül a memóriában az eredeti dezinformációval szemben[124]. A NATO StratCom COE szisztematikus áttekintése 2021-ben megerősítette, hogy a hagyományos tényellenőrzési módszerek hatékonyságát az „ismerősségi visszahatás" és a tartós befolyás hatása egyaránt korlátozzák, és önmagukban nem képesek a dezinformáció rendszerszintű visszaszorítására.[125] A gyakorlat nyelvére fordítva ez azt jelenti, hogy az FMK-műveletek tervezői tudják: akkor is masszív kárt okoznak, ha a bedobott hazugságuk másnapra „lebukik". A befogadó idegrendszerében ugyanis ott marad a gyanú, a narratív váz és a kiváltott érzelmi düh. Éppen ezért a modern kognitív védekezés (prebunking és debunking) alapszabálya, hogy nem elég csupán tagadni a hazugságot; a védekező félnek egy koherens, alternatív és logikus narratívát is kell kínálnia, amely képes az agyban strukturálisan is kiváltani a korábban beépült hamis modellt.

---

124 LEWANDOWSKY, Stephan – ECKER, Ullrich K. H. – SEIFERT, Colleen M. – SCHWARZ, Norbert – COOK, John (2012): *Misinformation and Its Correction*. Psychological Science in the Public Interest, 13. évf. 3. sz. 106–131. o.

125 NATO STRATCOM COE (2021): *Fact-Checking and Debunking*. NATO Strategic Communications Centre of Excellence, Riga. A kiadvány szisztematikusan elemzi a tényellenőrzési és cáfolati módszerek hatékonyságát és korlátait, különös tekintettel a tartós befolyás hatására (continued influence effect) és az ismerőségi visszahatásra (familiarity backfire effect).

A kognitív hadviselés eszköztára végül a szatíra és a paródia gátlástalan fegyveresítésével válik teljessé. Keir Giles, a Chatham House vezető tanácsadó kutatója 2023-as részletes esettanulmányában bizonyítja, hogy a humor a modern információs hadviselés egyik leghatékonyabb, kettős célú fegyvere. Míg támadóként (például az orosz műveletekben) a valóságérzékelés szétzúzásának, a cinizmus növelésének vagy az ellenfél dehumanizálásának eszköze, addig védekezésben a kognitív reziliencia és a közösségépítés páncéljaként funkcionál[126]. A humor védekezői hatékonyságának egyik kulcstényezője az ellenfél hiperszenzitivitása a nevetségessé tétellel szemben. Giles gyakorlati megfigyelésekre alapozva bizonyítja, hogy az orosz hivatalos szereplők és propagandisták kiemelten érzékenyek a gúnyra, mert önképük szerves része a komolyság és a „nagyság" mítosza – a humor pontosan ezt a központi identitás-elemet támadja. Az orosz parodista-fiókok üzemeltetőinek beszámolói szerint a trollfarmok működési költségét is növeli, ha a kimutatásaikban a felfelé ívelő interakciók nagy része gúnyos tartalom[127]. Bár ezek a műfajok történetileg a szabad, demokratikus diskurzus és a hatalomkritika eszközei, az FMK rendszerében a radikalizáció és a valóságérzékelés szétzúzásának eszközeivé degradálódnak. A „Birds Aren't Real" (2023) mozgalom külföldi példája rávilágított arra, hogy a végletekig vitt abszurd, parodisztikus narratívák – amelyek szerint a madarak valójában kormányzati megfigyelő drónok – képesek teljesen elmosni a valóság és a fikció közötti határvonalat, kognitív fáradtságot okozva és megágyazva a valódi dezinformációnak. Hazai környezetben a „Balaton-tagadók klubja" – bár eredetileg társadalomkritikus viccnek indult – kiválóan szemlélteti azt a szociálpszichológiai anomáliát, amelyben az egyén és a csoport képes a nyílt valóságtagadás köré is erős közösségi identitást építeni. Ezen „nem klasszikus" kognitív technikák – a keretezés, a szándékos félreértelmezés, a fegyveresített legendák és az abszurdba hajló paródia – szinergiája biztosítja, hogy a támadó fél ne csupán a pillanatnyi információáramlást, hanem a befogadó teljes valóságérzékelő és logikai szűrőrendszerét is az uralma alá vonja.

[126] GILES, Keir (2023): *Humour in online information warfare: Case study on Russia's war on Ukraine*. Hybrid CoE Working Paper 26. European Centre of Excellence for Countering Hybrid Threats, Helsinki. 11–15., 25–26., 29. o.

[127] GILES, Keir (2023): *Humour in online information warfare: Case study on Russia's war on Ukraine*. Hybrid CoE Working Paper 26. European Centre of Excellence for Countering Hybrid Threats, Helsinki. 16–17. o.

A kényszerített térképezés mechanizmusa: Fauconnier mentális terek elmélete a kognitív hadviselésben

A kognitív sebezhetőség megértéséhez a feldolgozási kapacitás túlterhelésén túl egy mélyebb mechanizmust is rögzíteni kell: a befogadó nem puszta állításokat tárol, hanem helyzetmodelleket – mentális tereket – épít és frissít a diskurzus során. Gilles Fauconnier mentális terek elmélete[128] azt írja le, hogyan működtetünk párhuzamosan több gondolati konstrukciót és hogyan hozunk létre köztük megfeleltetéseket (mappings): elemeket, szereplőket, ok-okozati viszonyokat viszünk át egyik térből a másikba .

A hadtudományi tét a következő: a fegyvernek minősülő kommunikáció kognitív veszélye nem csupán az, hogy hamis állításokat terjeszt, hanem az, hogy képes kényszerített térképezéseket létrehozni a befogadó mentális terei között. Amikor egy szintetikus médiatartalom – deepfake videó, fotórealisztikus generált kép, klónozott hangüzenet – bekerül a befogadó információs terébe, az agy kénytelen dönteni: melyik mentális tér lesz az „alapértelmezett”? A valóságot tükröző alap tér (base space), vagy az a lehetőség-tér (possibility space), amelyet a manipulált tartalom nyitott meg? Ha a hiperrealisztikus hamis kép vagy videó kellő érzelmi intenzitással érkezik és a korrekció késik, a kényszerített megfeleltetés rögzül: a befogadó mentális hivatkozási pontjai közé beköltözik a valótlanság, és később a cáfolat sem a hamis állítást, hanem a már rögzült helyzetmodellt kell felülírnia. Ez nagyságrendekkel nehezebb feladat.

Ez a mechanizmus közvetlenül összekapcsolódik az OxIPO-modell feldolgozási fázisával: a kényszerített térképezés az a pont, ahol a bemeneti túlterhelés (Input) a helyzetmodell szintjén okoz torzulást (Process), és ahol a kimenet (Output) már nem az eredeti állítás elfogadása vagy elutasítása, hanem a teljes értelmezési keret átrendeződése. A keretezés (framing) hatékonysága éppen abban rejlik, hogy a kognitív csapás sokszor nem az állítás igaz/hamis voltán keresztül működik, hanem a következtetések és reakciók előfeszítésén (priming). Azt éri el, hogy a célpont a bizonyítékot is gyanúként, a cáfolatot is manipulációként, az intézményi közlést is érdekként olvassa. Ez a bizalmi infrastruktúra megbontása – és a korábbi részben bevezetett hazugok osztaléka (Liar’s Dividend) mechanizmusának kognitív alapja.

[128] FAUCONNIER, Gilles (1997): *Mappings in Thought and Language*. Cambridge University Press, Cambridge.

A reflexív kontroll elméletének gyakorlati alkalmazására Thomas 2016 egy doktrínális-történelmi esettanulmányt mutat be, amelyet a Military Thought folyóiratban közzétett Makhnin-elemzésre épít. Makhnin 2013-as cikkében az RC azon dimenzióját vizsgálja, amelyben „az együttműködés látszatából a konfliktusba való átmenet" megtöri az ellenfél akaratát – ezt a műveletet a szakirodalom az ellenfél „baráti ölelésben való megfojtásának" (strangling the enemy in a 'friendly embrace') definiálja. Thomas kettős példával illusztrálja a mechanizmust. A 2014. szeptemberi Minszk-tűzszünet aláírását – amelyet a nemzetközi közösség a deeszkaláció jelének értelmezett – orosz csapatok egy további, körülbelül kétszáz négyzetmérföldnyi területszerzése követte. A mintázat megismétlődött: a 2015. februári Minszk-II megállapodás aláírása után mindössze órákkal a szeparatista erők elfoglalták Gyebálcevét. A két eset strukturálisan azonos: a diplomáciai gesztus (az „ölelés") az ellenfél éberségét csökkenti, míg a párhuzamosan végrehajtott katonai lépés a terepnyereséget maximalizálja. A disszertáció FMK-rácsának szempontjából a „baráti ölelés" a Manipuláció-dimenzió (M) tankönyvi esete: a kommunikáció formája diplomáciai, funkciója viszont fegyver.[129]

3.3. Technológiai környezet: Az algoritmikus hadviselés és a generatív MI

A kognitív hadviselés fogalmi keretrendszere nem értelmezhető a közvetítő közeg, azaz a modern technológiai infrastruktúra strukturális vizsgálata nélkül. A kutatás által vizsgált időszak (2014–2025) legkritikusabb paradigmaváltása, hogy a dezinformáció terjesztése egyedi, „kézműves" pszichológiai műveletből ipari léptékű, automatizált technológiai folyamattá transzformálódott. A disszertáció ezt a szinergiát – a generatív mesterséges intelligencia (GenMI) tartalomgyártó képessége és a platformok átláthatatlan ajánlórendszereinek (black box) felerősítő hatása közötti kölcsönhatást – Technológiai Környezeti Változóként definiálja. Ez a változó a műveleti térben nem csupán egy passzív kommunikációs csatorna; aktív katalizátorként viselkedik, amely önállóan is képes meghatározni az információ terjedési sebességét, topológiai elérését és a kiváltott társadalmi válaszreakciók intenzitását.

Az algoritmikus hadviselés (algorithmic warfare) korában egy adott információ vagy narratíva sorsa és túlélése már nem a tartalom minőségén vagy igazságtartalmán, hanem a globális

[129] THOMAS, Timothy L. (2016): Russia's 21st Century Information War: Working to Undermine and Destabilize Populations. In: Defence Strategic Communications, Vol. 1, No. 1, NATO Strategic Communications Centre of Excellence, Riga, 11–26. 14–15. o.

platformok átláthatatlan rangsorolási mechanizmusain múlik. Bene Márton elemzése[130] rámutat, hogy a közösségi média strukturális sajátossága a zárt információs terek, a véleménybuborékok (echo chambers) mesterséges kialakulása. Ezek az algoritmusok – a felhasználói figyelmi idő (engagement) maximalizálása érdekében – kizárólag olyan tartalmakat kínálnak fel, amelyek súrlódás nélkül visszaigazolják a befogadó meglévő világképét, ezáltal algoritmikusan kényszerítik ki a társadalom radikális táborokba rendeződését. Külföldi esettanulmányként említhető a Facebook ajánlórendszerének vitatott szerepe a mianmari események (rohingya krízis) során, ahol az elköteleződést prioritásként kezelő kód futótűzként erősítette fel a fegyveresített gyűlöletbeszédet, jóval azelőtt, hogy a humán moderációs mechanizmusok egyáltalán detektálták volna a problémát. Hazai viszonylatban ez a technológiai változó a mélyülő politikai polarizációban érhető tetten: az algoritmusok hermetikusan elzárják egymástól az eltérő nézeteket valló csoportokat. A gyakorlat nyelvére fordítva: ez a megosztottság biztosítja, hogy a korábban tárgyalt „nem klasszikus" manipulációs technikák (mint az AstroTurfing vagy a tömeges gázlángozás) kontroll és ellenérvek nélkül, telibe találják a sebezhető célközönséget.

A technológiai ökoszisztéma másik alapköve a generatív mesterséges intelligencia integrációja, amely a Fegyvernek Minősülő Kommunikáció (FMK) gyártási költségeit (barrier to entry) lényegében a nullához közelíti, miközben a hitelesség látszatát professzionális szintre emeli. Dr. Lance B. Eliot , a mesterséges intelligencia amerikai kutatója az „árnyék-meggyőzés" (shadowy persuasion) elméletében rögzíti, hogy a modern GenMI modellek képesek olyan rejtett nyelvi fordulatokat, mikro-affirmációkat és szubliminális mintázatokat beépíteni a mindennapi tartalomba, amelyek észrevétlenül kondicionálják a befogadót. E két pillér – az MI-alapú tömegtermelés és az algoritmikus terjesztés – fúziója alapjaiban változtatja meg a hibrid konfliktusok dinamikáját. A támadó félnek ma már nem kell feltétlenül meggyőznie a célközönséget egy konkrét hazugságról; elegendő, ha az algoritmusokat fegyverként használva információs túltelítettséget okoz, amiben a hiteles források elveszítik vonatkoztatási pontjukat.

[130] BENE Márton: Go Viral on the Facebook! *Information, Communication & Society*, 20(4), 2017, 513–529.

3.3.1. A generatív MI és a hitelesség-eltérítés (Credibility Hijacking)

A Nemzeti Kibervédelmi Intézet (NKI 2025)[131] jelentései és a vonatkozó A NATO StratCom COE AI in Support of StratCom Capabilities elemzése és a Robotrolling 2023–2024 kutatás egybehangzóan rámutatnak, hogy a generatív MI megjelenése nem csupán mennyiségi, hanem minőségi, exponenciális ugrást jelent a kognitív műveletekben.[132,133] A GenMI két kritikus ponton írja át a támadási felületeket:

- Polimorfizmus és skálázhatóság: A 2014-es krími konfliktus során alkalmazott hagyományos bot-hálózatok még a statikus üzenetek tömeges másolására (copy-paste) épültek. Ezeket a redundáns mintázatokat a platformok védelmi szűrői (hash-alapú detektálás) idővel viszonylag könnyen azonosították. Ezzel szemben a Nagy Nyelvi Modellekre (Large Language Models – LLM) épülő modern rendszerek képesek ugyanazt a stratégiai narratívát másodpercek alatt végtelen variációban előállítani. A gép tökéletes nyelvtannal, a célközönség lokális szlengjéhez, korosztályához és érzelmi profiljához igazítva generálja a posztokat. Ez a polimorfikus (alakváltó) tartalomgenerálás gyakorlatilag lehetetlenné teszi a klasszikus, kulcsszó-alapú algoritmikus védekezést.
- A jelenlét illúziója (Deepfake): A szintetikus szöveg, a hangklónozás (voice cloning) és a videómanipuláció konvergenciája lehetővé teszi az emberi evolúció legősibb bizalmi horgonyainak – a felismerhető arcnak és az ismerős hangnak – a teljes meghamisítását. Gilles Fauconnier kognitív nyelvész mentális terek (mental spaces) elmélete adja meg a jelenség kognitív magyarázatát. Fauconnier szerint a befogadó nem elszigetelt adatokat tárol, hanem a kommunikáció során a hosszú távú memóriából behívott sémákból épít

---

131 NBSZ NKI (2025): *Kiberbiztonsági fenyegetések és kihívások 2030-ig.* Budapest: Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézete. Online: https://nki.gov.hu/wp-content/uploads/2025/04/Kiberbiztonsagi-fenyegetesek-es-kihivasok-2030-ig.pdf

132 NATO STRATCOM COE (2023): *Trends in AI*. NATO Strategic Communications Centre of Excellence, Riga. 6., 8–9., 13. o. A tanulmány a szintetikus adatok kettős alkalmazását tárgyalja: az MI-rendszerek tanítóadataként és a dezinformáció eszközeként. A VKontakten azonosított pro-Kreml MI-generált tartalmak elemzése és a sentimentelemzés módszertani korlátai (fordítási torzítások, mikroagresszió-detektálás) releváns eredményeket közöl.

133 NATO STRATCOM COE: *The Role of AI in Digital Information*. NATO Strategic Communications Centre of Excellence, Riga. A kiadvány az MI szerepét vizsgálja a digitális információs környezetben, kiegészítve a The Double-Edged Sword of AI és a Trends in AI kiadványokat.

kontextusfüggő mentális konstrukciókat. A deepfake technológia egyfajta kognitív „gyorsút": a vizuális és auditív jegyek azonnal aktiválják a célszemély valós személyekhez kötődő mentális tereit. Így a hamis tartalom logikai ellenőrzés nélkül épül be egy már létező, ismerős referenciakeretbe.[134] [135] A deepfake tehát áttöri a „hiszem, ha látom" évezredes pszichológiai gátját, ahogy azt a 2024-es ARUP multinacionális vállalat elleni mélyhamisított pénzügyi csalás, vagy a 2023-as szlovákiai parlamenti választások hajrájában terjesztett hamisított politikai hangfelvételek is bizonyítják.

Ez a szintetikus képesség vezetett el a Kaylyn Jackson Schiff és Daniel S. Schiff politológusok által vizsgált Liar's Dividend (A hazug osztaléka) elméletéhez.[136] A jelenség lényege egy veszélyes paradoxon: a hiperrealisztikus szintetikus média puszta létezése és elterjedése önmagában is erodálja a társadalom objektív valóságba vetett hitét. Mivel a közönség megtanulja, hogy az online térben „bármi hamisítható", a dezinformátorok (vagy botrányba keveredett aktorok) a valódi, terhelő audio- és videóbizonyítékokat is könnyedén „MI-hamisítványnak" bélyegezhetik. A fegyvernek minősülő kommunikáció kimenete itt nem más, mint az objektív elszámoltathatóság (accountability) társadalmi mechanizmusának teljes összeomlása.

3.3.2. Platformökológia, algoritmikus torzítás és a láthatatlan korlátozás

A modern információs műveletek befogadói közegét a globális technológiai platformok (Meta, X, TikTok, Telegram) architektúrája határozza meg. A dokumentumelemzés igazolja, hogy e rendszerek társadalmi szempontból fekete dobozként (black box) funkcionálnak. Solon Barocas és Andrew D. Selbst technológiai jogászok a Big Data's Disparate Impact című elméletükben[137]

---

[134] Fauconnier, Gilles – Turner, Mark (2003): Conceptual Blending, Form and Meaning. *Recherches en communication*, 19. sz. 57–86. Online: https://tecfa.unige.ch/tecfa/maltt/cofor-1/textes/Fauconnier-Turner03.pdf

[135] Fauconnier, Gilles – Turner, Mark (2002): *The Way We Think: Conceptual Blending and the Mind's Hidden Complexities.* New York: Basic Books.

[136] Schiff, Kaylyn Jackson – Schiff, Daniel S. – Bueno, Natália S. (2024): The Liar's Dividend: Can Politicians Claim Misinformation to Evade Accountability? *American Political Science Review*, 118. évf. 4. sz. 2054–2073. DOI: 10.1017/s0003055423001454

[137] BAROCAS, Solon – SELBST, Andrew D. (2016): *Big Data's Disparate Impact*. California Law Review, 104. évf. 3. sz. 671–732. o.

levezetik, hogy bár a bemeneti adatok és a felhasználói kimenetek láthatóak, a gépi tanulás (machine learning) döntési logikája és az optimalizáció súlyozása szigorúan őrzött üzleti titok.

Ennek a strukturális átláthatatlanságnak az egyenes következménye az Algoritmikus torzítás (Algorithmic Bias). A jelenség informatikai gyökereit Batya Friedman és Helen Nissenbaum fektette le[138], bizonyítva, hogy a számítógépes rendszerek sosem értéksemlegesek; magukban hordozzák a tervezőik (vagy a betáplált adathalmazok) társadalmi és gazdasági preferenciáit. A közösségi média esetében ez a beépített preferenciális torzítás az elköteleződés (engagement) profitorientált maximalizálása. A gépi logika gyorsan felismerte, hogy a morális felháborodás, a félelem és az extrém polarizáció tartja a legtovább a felületen a felhasználót. A disszertáció érvelése szerint ez az algoritmikus amplifikáció az FMK legfőbb hatástöbbszörözője. A kognitív támadónak ma már nem kell felépítenie a saját fizikai terjesztési hálózatát; elegendő olyan pszichológiailag élesített tartalmat gyártania, amely maradéktalanul „kiszolgálja" a célplatform eleve meglévő torzításait. Giles 2016-ban, már a 2014-es krími konfliktus nyomán figyelmeztetett a réteges üzenetküldés (layered messaging) és a szűrőbuborék (filter bubble) kombinált hatására: a személyre szabott keresési találatok reklámmodellje hatékonyan izolálhatja a felhasználókat az alternatív nézőpontoktól, miközben az egyértelműen hamis tartalmak mögött futó árnyaltabb kampányok rejtve maradnak[139]

A platformökológia másik, defenzívnek szánt, ám könnyen fegyveresíthető sebezhetősége a Shadow Banning (láthatatlan tiltás) mechanizmusa. A fogalmat a platform-kutatásban Tarleton Gillespie formalizálta[140], rávilágítva a privát technológiai cégek tartalom-elfojtási gyakorlatára. A láthatatlan tiltás lényege, hogy az algoritmusok (vagy a moderátorok) anélkül csökkentik drasztikusan egy adott profil vagy narratíva elérését, hogy arról a felhasználót hivatalosan értesítenék, vagy a tartalmat fizikailag törölnék. Bár ezt eredetileg a spamek és a trollok ellen fejlesztették ki, a gyakorlatban súlyos „kettős mérce" viták alapjává vált. Ezt az átláthatatlansági krízist hivatott orvosolni az Európai Unió Digitális Szolgáltatásokról szóló Rendelete (Digital

138 FRIEDMAN, Batya – NISSENBAUM, Helen (1996): *Bias in computer systems*. ACM Transactions on Information Systems, 14. évf. 3. sz. 330–347. o.

139 GILES (2016) i. m. 31–32. o.

140 GILLESPIE, Tarleton (2018): *Custodians of the Internet*. Yale University Press, New Haven.

Services Act – DSA)[141] és az annak keretében létrehozott DSA Transparency Database (Átláthatósági Adatbázis). Az Európai Bizottság törekvése – amely a hibrid fenyegetések elleni küzdelem (Foreign Information Manipulation and Interference, FIMI) stratégiájába is illeszkedik –, hogy a platformokat rákényszerítse a moderációs döntéseik és algoritmikus paramétereik auditálható közzétételére. A technológiai környezet tehát kétélű fegyver: szabályozatlanul a dezinformáció terjedésének autópályája, míg az átláthatatlan korlátozások révén a legitim politikai véleménynyilvánítás szubjektív elfojtója is lehet.

3.3.3. Az automatizált amplifikáció: Bot-hálózatok és a narratívák felerősítése

A technológiai környezet (a feketedoboz-algoritmusok) sebezhetőségének műveleti kihasználását az automatizált szoftverágensek, azaz a bot-hálózatok teszik teljessé. A kutatás rögzíti, hogy egy modern dezinformációs kampány sikerét már nem pusztán a tartalom minősége, hanem a terjesztési hálózat matematikai sűrűsége és szervezettsége garantálja. Jarred Prier amerikai katonai elemző a „Commanding the Trend" (A trendek uralása) elméletében[142] vezeti le, hogyan válik a közösségi média hálózata taktikai hadszíntérré. A támadók nagy elérésű, mesterséges intelligenciával vezérelt álprofilok ezreit (botneteket) vetik be annak érdekében, hogy egy adott üzenet láthatóságát manipulálják .

A gyakorlat nyelvére fordítva: a bot-hálózatok feladata nem feltétlenül a bonyolult érvelés. Céljuk egy hirtelen, masszív interakciós hullám (összehangolt lájkok, megosztások, kommentek) generálása. A platform korábban tárgyalt algoritmusa ezt az anomáliát tévesen „hirtelen jött, organikus társadalmi érdeklődésként" érzékeli, beemeli a „felkapott" (trending) témák közé, és innentől kezdve a rendszer maga biztosítja az ingyenes, globális terjesztést. Ezzel a módszerrel az FMK áttöri az információs zajt, kijátssza az organikus szűrőket, és megteremti a társadalmi többség vagy az alulról szerveződő civil mozgalmak hamis látszatát (AstroTurfing). A bot-hálózatok és a generatív MI szinergiája alkotja a 21. századi kognitív hadviselés igazi „erőművét", amely a platformok kódolt pszichológiai sebezhetőségeit fizikai és politikai műveleti előnnyé konvertálja.

---

[141] DSA (2022): *Az Európai Parlament és a Tanács (EU) 2022/2065 rendelete a digitális szolgáltatások egységes piacáról*.

[142] PRIER, Jarred (2017): *Commanding the Trend: Social Media as Information Warfare*. Strategic Studies Quarterly, 11. évf. 4. sz. 50–85. o.

Ezt a platformdinamikát Bennett és Segerberg a konnektív cselekvés (connective action) logikájaként írta le:[143] a digitális médiában a tartalommegosztás és a szerveződés költsége olyan alacsonyra csökken, hogy koordinált viselkedés jöhet létre formális szervezeti háttér nélkül is – amit a támadó fél a saját céljaira fordíthat, mesterséges „alulról jövő" mozgalmak szimulálásával. A konnektív cselekvés és az AstroTurfing összefonódása a platformökológia egyik legveszélyesebb sebezhetősége.

A dezinformáció és az algoritmikus erősítés összefüggése nem 2022 után vált kutatási területté: a NATO StratCom COE Digital Hydra-projektje már dokumentálta, hogy a hamis tartalmak terjedési mintázata platformonként eltér, és a blogszféra, illetve a külső linkek az elsődleges közösségimédia-platformoknál hatékonyabb terjesztőcsatornát alkotnak.[144] A kutatás azt is kimutatta, hogy harmadik fél adatgyűjtők – tracking pixelek, analytics eszközök – ugyanolyan sűrűséggel vannak jelen dezinformációs oldalakon, mint normál híroldalkon, ami azt jelenti, hogy a célzott hirdetési infrastruktúra közvetlenül kiszolgálhatja az információs befolyásoló műveletek terítési fázisát. Ez a korai dokumentáció megerősíti, hogy a T(erítés)-dimenzió technológiai alapinfrastruktúrája nem esetleges fejlemény, hanem tudatosan kialakított és azóta is működtetett rendszer – amellyel szemben az SCC-protokoll Sebesség-tengelye önmagában nem elegendő válasz.

A bot-hálózatok és az automatizált amplifikáció ipari léptékét a NATO StratCom COE Robotrolling 2023–2024 elemzése friss empirikus adatokkal dokumentálta. A kutatás a 2023 novembere és 2024 májusa közötti időszakban a NATO-hoz kapcsolódó automatizált kommentek arányát mérte: az angol nyelvű Twitter(X)-en mintegy 7%-ot, az orosz nyelvű Twitter(X)-en mintegy 15%-ot, az orosz nyelvű VKontaktén pedig mintegy 38%-ot ért el az automatizált tartalom aránya[145]. A kutatók 17 koordinált csoportot azonosítottak 344 forrás bevonásával, amelyek közül 67% orosz, 17% angol, 11% francia és 5% finn nyelvű volt. A csoportok 53%-a a Telegramon volt

[143] BENNETT, W. Lance – SEGERBERG, Alexandra (2012): *The Logic of Connective Action*. Information, Communication & Society, 15. évf. 5. sz. 739–768. o.

[144] AGARWAL, N. – BANDELI, K. – BERTOLIN, G. – BITENIECE, N. – SEDOVA, K. (2017): Digital Hydra: Security Implications of False Information Online. NATO Strategic Communications Centre of Excellence, Riga. 28–35. o.

[145] NATO STRATCOM COE: Robotrolling 2023–2024. Riga, 2024 (ismételt hivatkozás, ld. 88. lj.).

aktív, egyetlen hálózat 130 Telegram-csatornát és 13 weboldalt üzemeltetett. Különösen figyelemre méltó, hogy a kutatók teljesen automatizált, nagy nyelvi modellekre (LLM) épülő hálózatokat is azonosítottak, amelyek weboldalakat szedtek szét és politikai híreket posztoltak újra, gyakran „MI-hallucinációkkal" – értelmetlen, kitalált tényeket tartalmazó szövegekkel. Ez az empirikus adat közvetlenül alátámasztja a 3.3.1 alfejezetben tárgyalt polimorfizmus-hipotézist. A tartalom-automatizáció nem csupán a közösségi médiában érhető tetten: a NATO StratCom COE fantom-újságíró esettanulmánya a Lenta.ru és más orosz hírportálok 27 szerzőjének elemzésével kimutatta, hogy a profilképek GAN-generált képek, a publikációs tempó (napi 15+ cikk percnyi szünetekkel) meghaladja az emberi kapacitást, és a szerzők többsége nem azonosítható valódi személyként.[146]

Végül a technológiai környezet sajátos veszélyét jelenti a hazug osztaléka (Liar's Dividend) – a Chesney és Citron által leírt jelenség[147], amely szerint minél elterjedtebbé válnak a deepfake-technológiák, annál könnyebben tagadhatja bármely szereplő a róla szóló hiteles felvételek valódiságát. A gyanú általánossá válása nem csupán a manipulált, hanem a valós tartalmak hitelességét is aláássa, paradox módon a dezinformáció-készítő és a leleplezett fél számára egyaránt előnyt biztosítva. A hazug osztaléka a bizonyítékalapú társadalmi diskurzus egyik legmélyebb eróziós tényezője, amelyet Bányász Péter és Szádeczky Tamás 2025-ös magyar felmérése is megerősít: a generatív MI-alapú vizuális manipulációval szembeni felhasználói reziliencia a Facebook-felhasználók körében alacsony[148].

---

146 KUBS, Jakub – MICHALOWSKA, Aleksandra – DAUKŠAS, Viktoras (2023): Phantom Pillars of Pro-Kremlin Disinformation: A Case Study of Russian Journalists Covering the Topic of War in Ukraine. In: BOLT, Neville et al.: *Kremlin Communication Strategy for Russian Audiences Before and After the Full-Scale Invasion of Ukraine*. NATO Strategic Communications Centre of Excellence, Riga. 125–137. o. 27 orosz „újságíró" profiljának elemzése: a Lenta.ru-nál GAN-generált profilképek, embertelen publikációs tempó (napi 15+ cikk, percnyi szünetek), a szerzők többsége nem azonosítható valódi személyként – sock puppet vagy automatizált tartalomlétrehozás.

147 CHESNEY, Robert – CITRON, Danielle K. (2019): *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*. California Law Review, 107. évf. 1753–1820. o.

148 BÁNYÁSZ Péter et al. (2025): *The resilience of social media users against Generative AI-based visual manipulation: A survey among Hungarian Facebook users*. In CEEeGov 2025: Proceedings of the Central and Eastern European eDem and eGov Days 2025. New York: ACM, 181–188. Online: https://doi.org/10.1145/3773002.3774813

3.4. A Krím 2014-re vonatkozó empirikus irodalom

A krími annektálás (2014.[149] február–március) az első olyan nagyhatalmi területszerzés volt Európában a hidegháború óta, amelyben az információs műveletek nem kísérő, hanem vezető szerepet töltöttek be. Az esettel foglalkozó irodalom három csomópont köré szerveződik: az orosz doktrinális háttér, a műveleti végrehajtás és a nyugati reakció kudarca.[150]

A doktrinális megközelítést Jolanta Darczewska 2014-es varsói OSW-elemzése tárta fel a legmélyebben[151]. Darczewska kimutatta, hogy a krími művelet nem improvizáció volt, hanem a szovjet „aktív intézkedések" (active measures) hagyományának digitális korra adaptált változata, amelyben a cél a célország társadalmi szövetének fellazítása a kinetikus erők megjelenése előtt. A reflexív kontroll (reflexive control) mechanizmusát alkalmazva az orosz műveletek nem csupán dezinformáltak, hanem olyan döntési környezetet teremtettek, amelyben az ukrán és a nyugati döntéshozók a támadó számára kedvező alternatívák között „választhattak".

Ivo Juurvee 2018-ban a Hybrid CoE számára készített elemzésében kimutatta, hogy a Darczewska által azonosított aktív intézkedések nem elszigetelt történeti örökség, hanem szervezetileg intézményesített képesség: az orosz Külföldi Hírszerzési Szolgálat (Szluzsba Vnyesnyej Razvegyiki, SVR), a Szövetségi Biztonsági Szolgálat (Fegyeralnaja Szluzsba Bezopásznosztyi, FSB) és a Katonai Felderítő Főigazgatóság (Glávnoje Razvegyivátyelnoje Upravlenyije, GRU) jelenlegi működési szabályzataiban az aktív intézkedések támogatási intézkedések (support measures) címen élnek tovább. A hatályos orosz Szövetségi Külhírszerzési Törvény (1996) 2. cikke

[149] NATO STRATCOM COE (2016): *Analysis of Russia's Information Campaign against Ukraine* (teljes jelentés). NATO Strategic Communications Centre of Excellence, Riga. 16., 26., 35. o. A teljes jelentés a stratégiai narratívák fejezete mellett részletes reflexív kontroll mellékletet tartalmaz (Annex 2), amely a Lefebvre-féle definícióból kiindulva a Georgia 2008 és Ukrajna 2014 közötti párhuzamokat elemzi.

[150] NATO STRATCOM COE (2016): *Social Media in the Service of Hybrid Warfare: The Ukraine Conflict Full Report*. NATO Strategic Communications Centre of Excellence, Riga. A jelentés Nissen weaponization-modelljének gyakorlati alkalmazásával elemzi a trollok működési és kommunikációs stratégiáit az ukrán konfliktusban.

[151] DARCZEWSKA, Jolanta (2014): *The Anatomy of Russian Information Warfare: The Crimean Operation, A Case Study* OSW (Centre for Eastern Studies), Warsaw.

a hírszerzést a politikai küzdelem titkos formájaként definiálja – olyan keretfogalom, amely a dezinformációs műveleteket normatív alapra helyezi.[152]

Kofman és Rojansky 2015-ben megjelent elemzésükben[153] fontos korrekciót végeztek a nyugati narratíván: a „hibrid hadviselés" címke félrevezető, mert koherens, előre megtervezett doktrínaként mutatja be azt, ami valójában gyorsan, helyzetfüggően alakult. A krími művelet sikerét nem egy új hadviselési forma, hanem az egyedi feltételek magyarázzák: Oroszország szevasztopoli bázisa, a Krím-félszigeti orosz médiafogyasztás dominanciája, Kijev politikai instabilitása és a nyugati döntéshozatali ciklus lassúsága. A szerzők figyelmeztetnek: a krími modell nem másolható tetszőleges helyszínre, mert sikerének kulcsfeltételei – az előre telepített katonai jelenlét, a médiakörnyezet előzetes formálása és a célpopuláció identitásbeli fogékonysága – helyspecifikusak. Beccaro (2024) a Hybrid Warfare Reference Curriculum keretében ugyanezt a clausewitzi logikát követi: az orosz műveletek nem új hadviselési formát, hanem a katonai erő mint végső eszköz – a diplomácia kudarca utáni – alkalmazását tükrözik, és a krími „modell" sem Szíriában, sem a Donbaszban nem volt megismételhető[154]

A NATO StratCom COE rigai elemzése[155] a műveleti végrehajtást dokumentálta: az orosz információs kampány négy rétegben működött párhuzamosan – állami média (RT, Sputnik), diplomáciai kommunikáció, közösségimédia-manipuláció (trollfarmok) és helyi proxyk. A szinkronizáció mértéke – azonos narratívák megjelenése több platformon perceken belül – forenzikus bizonyítékát adta a központi irányításnak. A NATO StratCom COE kiadványsorozatában Kelly és Paul a krími narratíva-dekonstrukciót végezte el, az orosz információs műveletek célzott keretezési technikáit azonosítva a területszerző művelet

152 JUURVEE, Ivo (2018): The resurrection of 'active measures': Intelligence services as a part of Russia's influencing toolbox. Hybrid CoE Strategic Analysis 7. European Centre of Excellence for Countering Hybrid Threats, Helsinki. 2–4. o.

153 KOFMAN, Michael – ROJANSKY, Matthew (2015): *A Closer Look at Russia's "Hybrid War"*. Kennan Cable, No. 7. Washington D.C.: Wilson Center, Kennan Institute.

154 BECCARO, Andrea (2024): The Evolution of Hybrid Warfare. In JOBBÁGY, Z. and ZSIGMOND, Edina. (eds.): *Hybrid Warfare Reference Curriculum, Volume III.* Budapest: Ludovika. 87–90. o.

155 NATO STRATCOM COE (2015) / LANGE-IONATAMIŠVILI, Sanda és mtsai: *Analysis of Russia's Information Campaign against Ukraine*. NATO Strategic Communications Centre of Excellence, Riga.

kommunikációs vonalán.[156] Jessikka Aro (2016) finn oknyomozó újságíró a trollfarmok működését dokumentálva feltárta[157], hogy az online zaklatás és a tömeges kommentelés nem egyéni túlkapás, hanem operatívan szervezett, államilag támogatott eszközkészlet volt, amely a 2014-es konfiguráció domináns jellemzőjét – a manuális, humánerőforrás-intenzív módot – jeleníti meg.

Keir Giles a Chatham House számára készített elemzésében[158] hangsúlyozta, hogy az orosz megközelítésben az igazság másodlagos a hatásossággal szemben; a „nem-lineáris hadviselés" célja a nyugati döntéshozatali mechanizmusok megbénítása a folyamatos, ellentmondásos narratívák áradatával. Giles dokumentálta az adaptációs fölény (adaptation superiority) jelenségét: az orosz információs műveletek az OODA-hurok logikáját alkalmazva gyorsabban módosították narratíváikat, mint ahogy a nyugati tényellenőrzés reagálni tudott volna.

A védekezési oldalon az OSCE Speciális Megfigyelő Missziója (SMM) helyszíni jelentései az egyetlen valós idejű, szervezetileg független dokumentációt jelentik a 2014-es krími és kelet-ukrajnai eseményekről. Ezek a jelentések a kreált diplomáciai narratívák és a fizikai valóság közötti rést (kinetikus rés) dokumentálták – azt a diszkrepanciát, amely a legkézzelfoghatóbb bizonyítéka volt az információs művelet szándékoltságának.

Az irodalom összképe egyértelmű: 2014-ben a stratégiai meglepetés sikere nem a technológiai fölényen, hanem a döntéshozatali aszimmetrián és a válaszadási idő drasztikus különbségén múlott. Ez a felismerés jelöli ki a 2022-es esettel való összehasonlítás egyik központi kérdését: megváltoztak-e ezek a feltételek?

Az orosz médiamanipuláció szerkezeti sajátosságait a NATO StratCom COE és a Lett Nemzetközi Tanulmányok Központja négy esettanulmányon (MH17, gazdasági szankciók, humanitárius konvoj, Minszk II) keresztül vizsgálva 19 alkalmazott technikát azonosított,[159] amelyek a

---

156 KELLY, Paul (2016): *Decoding Crimea*. NATO Strategic Communications Centre of Excellence, Riga. A krími annektálás narratíva-dekonstrukciója: az orosz információs műveletek célzott keretezési technikáinak azonosítása a területszerző kampány kommunikációs vonalán.

157 ARO, Jessikka (2016): *The Cyberspace War: Propaganda and Trolling as Warfare Tools*. European View, 15. évf. 1. sz. 121–132. o.

158 GILES, Keir (2016): *Russia's 'New' Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power*. London: Chatham House, Russia and Eurasia Programme.

159 NATO STRATCOM COE – Lett Nemzetközi Tanulmányok Központja (2016): *The Manipulative Techniques of Russia's Information Campaign: Executive Summary*. NATO Strategic Communications Centre of Excellence, Riga.

disszertáció M(osás)-dimenziójának részletes technikai rétegét képezik. Pulai (2023)[160] az RT lengyel–fehérorosz válság alatti működését vizsgálva hasonló mintázatot talált: az RT az ellenfél magatartásának bírálatát a saját oldal atrocitásainak elhallgatásával párosította, azonos közléseket akár tizenötszörös ismétléssel erősített, és Lengyelországot vádolta kegyetlenkedéssel, miközben kívülállónak pozicionálta magát – a G–M–T–V keretben ez a Terítés-fázis ismétlésalapú amplifikációja[161] A disszertáció modellje szempontjából különösen releváns a Pseudo-plurality (látszólagos sokszínűség egyirányú üzenet mögé rejtve), a Victimisation (az áldozatszerep instrumentalizálása – a Kreml-narratíva egyik legtartósabb eleme), a Moral Superiority (erkölcsi felsőbbrendűség igénye a nyugati kettős mércével szemben) és a Hypothetical Future (jövőbeli katasztrófa-narratíva). A kutatók rögzítik, hogy a módszerek kombinálhatók, és az alkalmazott technikák a jövőben kifinomultabbakká válnak – ezt az előrejelzést 2022–2024 valóban igazolta: az LLM-alapú tartalomgenerálás a korai taxonómiában leírt technikákat nem cseréli le, hanem skálázza és automatizálja.

3.5. A transzformációs időszak (2014–2021) irodalma

A 2014-es krími annektálás és a 2022-es teljes körű invázió közötti időszakot a disszertáció transzformációs perióduskénti kezeli (ld. 2. fejezet, 2.1. alfejezet). Ez nem önálló esettanulmány, hanem magyarázó változó: azoknak a technológiai, szabályozási, intézményi és kognitív reziliencia-változásoknak a dokumentálása, amelyek a két eset közötti kimeneti különbséget értelmezhetővé teszik. Az irodalom négy dimenzió mentén szerveződik.

A platformökológia átalakulása. A 2014-es művelet idején a közösségi média platformjai transzparencia-szempontból gyakorlatilag fekete dobozok voltak. A fordulópontot a 2016-os amerikai elnökválasztás körüli botrányok hozták el: a Cambridge Analytica-ügy és az orosz Internet Research Agency tevékenységének leleplezése nyomán a Meta (akkor Facebook) bevezette a negyedéves Adversarial Threat Report-ot, amelyben a koordinált inautentikus

A négy esettanulmány (MH17, gazdasági szankciók, humanitárius konvoj, Minszk II) alapján 19 alkalmazott manipulatív technikát azonosított, köztük: Pseudo-plurality, Victimisation, Moral Superiority, Hypothetical Future, dehumanizáció, social proof, „attacking with data”.

160 PULAI Bence (2023): *A befolyásolás mint a hibrid hadviselés eszköze a 2021-es lengyel–fehérorosz migrációs- és határválság során.* Honvédségi Szemle, 151. évf. 6. sz. 56–67. o.

161 PULAI (2023) i. m. 62., 64–65. o.

viselkedés (CIB) elleni fellépéseit dokumentálja.[162] Az Oxford Internet Institute Computational Propaganda Project retrospektív hálózatelemzései[163] szolgálnak proxy adatként a 2014-es bot-hálózatok működésének leírásához, míg a 2016 utáni időszakra már valós idejű platformadatok állnak rendelkezésre.

A szabályozási környezet keményedése. Az Európai Bizottság 2018-as Cselekvési Terve a félretájékoztatás ellen (Action Plan against Disinformation)[164] az első átfogó uniós válasz volt az orosz dezinformációs kampányokra. A dokumentum négy pillérre építette a védekezést: az EEAS stratégiai kommunikációs kapacitásainak megerősítése, a platformokra nehezedő átláthatósági nyomás növelése, a médiaműveltség javítása és a tagállamok rezilienciájának erősítése. A Cselekvési Tervet az EU Hetedik Előrehaladási Jelentése (2020) értékelte[165], amely rögzítette a magatartási kódex korlátait: a platformok önszabályozása inkább szimbolikus, mint operatív eredményeket produkált. A valódi szabályozási áttörést a Digitális Szolgáltatásokról szóló Rendelet (DSA, 2022) hozta, amely jogi kötelezettséggé tette a rendszerszintű kockázatértékelést és a koordinált inautentikus viselkedés elleni fellépést.

A COVID–19 infodémia mint kognitív stresszteszt. A 2020–2021-es pandémiás időszakot a WHO keretrendszerének[166] fényében lehet értelmezni: az egészségügyi válságkommunikáció modelljei (Reynolds–Seeger CERC-modell) a gyors, transzparens és következetes tájékoztatást jelölték meg a pánik megelőzésének kulcsaként. A COVID-infodémia azonban megmutatta, hogy az információs ökoszisztéma már képes a hivatalos válságkommunikációt is kioltani: a vírusszeptikus narratívák, az összeesküvés-elméletek és az intézményi bizalomvesztés összefonódása globális léptékű stressztesztet jelentett a társadalmak kognitív rezilienciája számára. A Hybrid CoE

---

162 Nimmo, Ben – Agranovich, David – Gleicher, Nathaniel (2022a): *Adversarial Threat Report*. Meta. 2022. április [Q1 2022 – az első negyedéves ATR-jelentés]. Online: https://about.fb.com/news/2022/04/metas-adversarial-threat-report-q1-2022/

163 HOWARD, Philip N. – KOLLANYI, Bence (2016): *Bots, #StrongerIn, and #Brexit: Computational Propaganda during the UK-EU Referendum*. Oxford Internet Institute, Oxford University.

164 EURÓPAI BIZOTTSÁG (2018): *Cselekvési terv a félretájékoztatással szemben*. JOIN(2018) 36 final, Brüsszel.

165 EURÓPAI BIZOTTSÁG (2020): *Seventh Progress Report on the implementation of the EU regulatory framework for electronic communications*. Brüsszel.

166 WHO (2017): *Communicating risk in public health emergencies: a WHO guideline for emergency risk communication (ERC) policy and practice*. World Health Organization, Geneva.

Working Paper 29 és a CORE Comprehensive Resilience Ecosystem elemzés egybehangzóan kimutatta:[167] a COVID-időszak nem csupán epizód volt, hanem a fegyvernek minősülő kommunikáció új dimenzióinak katalizátora, amely a társadalmi fragmentáció, a médiaellenség-képzés és az intézményi bizalomerózió mintázatait rögzítette a 2022-es háborút megelőzően. Az European Digital Media Observatory (EDMO) dokumentálta, hogy a COVID-dezinformációs csatornák 2022 után zökkenőmentesen átálltak pro-Kreml Ukrajna-narratívákra – bizonyítva a dezinformációs infrastruktúra transzferálhatóságát.

Az automatizáció terjedése. A Hybrid CoE 2023-as, identitás-alapú dezinformációról szóló elemzése[168] kimutatta, hogy a transzformációs időszakban a támadók egyre kifinomultabban alkalmazták a társadalmi törésvonalak célzott kihasználását: az identitáspolitika, az etnikai és vallási megosztottság, valamint a gender- és migrációs diskurzusok fegyveresítése a 2014-es kézi módszerektől az automatizált, mikrocélzott kampányokig fejlődött. A Hybrid CoE Trend Report 10 (2023) a gazdasági dimenzióban azonosított új sebezhetőségeket:[169] a technológiai függőség és az ellátási lánc-manipuláció a kognitív hadviselés kiegészítő eszköztárává vált.

A társadalmi identitások fegyveresítése. A Hybrid CoE Strategic Analysis 34 és a Hybrid CoE Paper 24 egyaránt rámutattak, hogy a transzformációs időszak egyik leghatékonyabb és legnehezebben kivédhető taktikája a társadalmi törésvonalak célzott kihasználása volt. A dezinformáció a leghatékonyabb, amikor meglévő társadalmi megosztottságokat feszít – a nem, az etnikai hovatartozás, az osztályhelyzet, a szexuális orientáció vagy a migráció mentén zajló vitákat. Az orosz, kínai és iráni hibrid fenyegetési aktorok ismert stratégiája az egyidejű, ellentétes pozíciók erősítése – például a Black Lives Matter mozgalom és a rendőrséget támogató narratívák párhuzamos amplifikálása –, amelynek célja nem a vélemény megváltoztatása, hanem a társadalmi

[167] HOYLE, Aiden – ŠLERKA, Josef (2024): Cause for concern: The continuing success and impact of Kremlin disinformation campaigns. Hybrid CoE Working Paper 29, Helsinki.; JUNGWIRTH, Richard et al. (2023): CORE – Comprehensive Resilience Ecosystem. Hybrid CoE.

[168] HOOGENSEN GJØRV, Gunhild – JALONEN, Outi (2023): *Identity as a tool for disinformation*. Hybrid CoE Strategic Analysis 34. European Centre of Excellence for Countering Hybrid Threats, Helsinki. 3., 5. o.

[169] HYBRID COE (2023): *Threat potential in the economy: from vulnerabilities to China's increased coercion*. Hybrid CoE Trend Report 10. Helsinki.

megosztottság elmélyítése és a demokratikus intézményekbe vetett bizalom erodálása[170]. A svédországi Korán-égetési események (2022–2023) és az azokhoz kapcsolódó külföldi befolyásolási kampány – amely átmenetileg megakasztotta Svédország NATO-csatlakozási folyamatát – szemléletes példa arra, hogyan képes egy identitásalapú sérülékenység kihasználása a legmagasabb szintű biztonsági döntéseket is befolyásolni .

A populizmus és a hibrid fenyegetések összefüggése. A Hybrid CoE Working Paper 22 (2023) a populizmus inherensen autoriter logikáját vizsgálva kimutatta, hogy a populista „nép vs. elit" dichotómia strukturálisan megkönnyíti a hibrid fenyegetési aktorok számára a demokratikus nyilvánosság fragmentálását[171]. A digitális közösségi média affordanciái – az érzelmi tartalom jutalmazása, az algoritmikus amplifikáció, a szűrőbuborékok – a populista logika természetes szövetségesei.

A memetikus hadviselés elméleti alapozása. A NATO StratCom COE 2021-es Memetic Warfare kötete a mémeket a stratégiai kommunikáció operatív eszköztárába helyezte. Giesea definíciója szerint a memetikus hadviselés „versengés a narratíváért, az eszmékért és a társadalmi kontrollért a közösségi média hadszínterén"[172]. A Hybrid CoE Working Paper 26 (2023) a humor dezinformáció-ellenes alkalmazását elemezve három funkciót azonosított: a szokásos közönségen túli rétegek elérése; a saját közönség moráljának és rezilienciájának erősítése; és a támadó hírnevének rontása.[173]

A nem-állami szereplők (NSA) szerepe az orosz hibrid fenyegetésben. A Hybrid CoE Paper 27 – a legfrissebb átfogó kézikönyv ezen a területen – öt NSA-típust különböztet meg: fegyveres (PMC-k, zsoldos hálózatok), kiber-, propaganda/dezinformációs, társadalmi-politikai és gazdasági-

---

170 HOOGENSEN GJØRV, Gunhild – JALONEN, Outi (2023): Identity as a tool for disinformation: Exploiting social divisions in modern societies. Hybrid CoE Strategic Analysis 34. European Centre of Excellence for Countering Hybrid Threats, Helsinki. 3., 5. o.; HEDLING, Elsa (2025): Social identities and democratic vulnerabilities: Learning from examples of targeted disinformation. Hybrid CoE Paper 24, Helsinki.

171 LEBRUN, Maxime (2023): Watching out for populism: Authoritarian logics as a vulnerability to hybrid threat activity. Hybrid CoE Working Paper 22, Helsinki.

172 GIESEA, Jeff: It's Time to Embrace Memetic Warfare. Defence Strategic Communications, Vol. 5, 2015/2021.

173 GILES, Keir (2023): *Humour in online information warfare: Case study on Russia's war on Ukraine*. Hybrid CoE Working Paper 26. European Centre of Excellence for Countering Hybrid Threats, Helsinki. 29. o.

pénzügyi nem-állami szereplőket[174]. A kézikönyv dokumentálja az Internet Research Agency (IRA), Glavnoje Razvegyivatyelnoje Upravlenyije (GRU) frontszervezetté, a Centre for Geopolitical Expertise-vé (CGE) történő átszervezését[175], a Wagner-csoport Expeditionary Corps-szá (Africa Corps + Volunteer Corps) való átnevezését, és a transznacionális bűnözői hálózatok fegyveresítését befolyásolási műveletek céljára.

A nem állami szereplők rendszerezését Janne Jokinen, Magnus Normark és Michael Fredholm korábbi Hybrid CoE-taxonómiája alapozta meg, amely a hibrid fenyegetésekben részt vevő nem állami szereplőket hat kategóriába sorolja: proxyk, zsoldoscsoportok, bűnözési hálózatok, ideológiai szervezetek, magánkatonai vállalatok és hacktivista közösségek. A 2022 utáni orosz szervezeti átalakulás – az IRA felszámolása, a CGE létrehozása, a Wagner-csoport fragmentálódása – e taxonómia dinamikus alkalmazását igényli.[176]

3.6. Az Ukrajna 2022– irodalom

A 2022. február 24-én indult teljes körű orosz invázió információs kísérőműveleteinek irodalma három szempontból tér el a 2014-es kutatásoktól: (1) a valós idejű adatok bősége, (2) a generatív MI megjelenése a műveleti eszköztárban és (3) a védekezési oldal horizontális önszerveződése.

A valós idejű forenzikus dokumentáció. A 2022-es háború az első olyan nagyszabású konfliktus, amelyben a digitális forenzikus közösség – a DFRLab, a Stanford Internet Observatory, a Bellingcat és a Mandiant/Google TAG – valós időben dokumentálta az információs műveleteket. A Mandiant „Fog of War" (2022) jelentései a kiber- és kognitív dimenziók konvergenciáját mutatták ki: a hack-and-leak műveletek, a wiperware-támadások és a narratívaindítások szinkronizált kampányokba rendeződtek, amelyek a kinetikus csapásokkal koordináltan működtek.

---

174 VOLĀNS, Eginhards et al. (2025): Handbook on the role of non-state actors in Russian hybrid threats. Hybrid CoE Paper 27, Helsinki.

175 Az IRA és a GRU az orosz befolyásolási gépezet két keze: az egyik a közvéleményt formálja dezinformációval (IRA), a másik pedig technikai támadásokat és hírszerzési műveleteket végez (GRU). Az amerikai pénzügyminisztérium 2024. decemberi jelentése szerint a GRU jelenleg olyan szervezeteken keresztül folytatja az IRA-hoz hasonló tevékenységet, mint a Center for Geopolitical Expertise (CGE).

176 JOKINEN, Janne – NORMARK, Magnus – FREDHOLM, Michael (2022): Hybrid threats from non-state actors: A taxonomy. Hybrid CoE Research Report 6. European Centre of Excellence for Countering Hybrid Threats, Helsinki. 14–22. o.

A Stanford Internet Observatory mélyelemzései az MI-generált profilok és a deepfake narratívák ipari alkalmazásának első adatvezérelt bizonyítékait szolgáltatták.

A generatív MI és a deepfake fenyegetés. Chesney és Citron jogelméleti elemzésükben[177] a deepfake-technológia három veszélydimenzióját azonosították: a magánszférát, a demokráciát és a nemzetbiztonságot fenyegető kockázatokat. A szerzők által leírt hazug osztaléka (Liar's Dividend) a 2022-es háborúban empirikusan is megjelent: a Zelenszkij-deepfake (2022. március) – amelyben az ukrán elnök állítólagos megadásra szólított fel – ugyan gyorsan leleplezésre került, de a jelenség bizonyította, hogy a technológia elérte a hadműveleti alkalmazhatóság küszöbét. A Doppelgänger-típusú műveletek – amelyekben a támadók nyugati hírportálok klónoldalait hozták létre – az EU DisinfoLab (2022) és az EEAS FIMI-jelentések (2023) által dokumentált új formát képviselték: a hitelesség-eltérítés (credibility hijacking) ipari léptékű alkalmazását.

A Kreml dezinformációjának mérhető hatásai. A Hybrid CoE Working Paper 29 (2024) az első szisztematikus kísérlet az orosz dezinformáció tényleges hatásának dokumentálására. Az elemzés kimutatta, hogy a Kreml-narratívákat nem csupán orosz médiumok, hanem befolyásos nyugati véleményformálók is reprodukálták – az Egyesült Államokban republikánus kongresszusi képviselők, Európában jobboldali populista pártok politikusai[178]. Az „információs áttörés" (cross-medium breakout) jelensége – amelyet Ben Nimmo írt le – akkor valósul meg, amikor a dezinformációs művelet olyan mértékű hatást ér el, hogy a mainstream média maga kezdi közvetíteni.

Ukrajna dezinformáció elleni válasza. A Hybrid CoE Research Report 11 az ukrán dezinformáció-elleni tapasztalatokat dokumentálta a 2022-es invázió kontextusában. A kutatás kiemelte az assessment bias jelenségét: egy 2023-as felmérés szerint az ukránok 46%-a nem számított háborúra, további 29%-a hitt benne, de nem akarta elhinni. Az ukrán válasz leghatékonyabb elemei közé tartozott a humor szisztematikus alkalmazása – ahogy Gosha Tykhyi, az MFA szóvivője fogalmazott: egy mém olyan célpontot is eltalálhat, amelyet egy minisztériumi sajtóközlemény

[177] CHESNEY, Robert – CITRON, Danielle K. (2019): *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*. California Law Review, 107. évf. 1753–1820. o.

[178] HOYLE, Aiden – ŠLERKA, Josef (2024): Cause for concern: The continuing success and impact of Kremlin disinformation campaigns. Hybrid CoE Working Paper 29, Helsinki. (cross-medium breakout).

nem –, a monitoring-rendszerek kiépítése és az Egyesült Államok pre-bunking stratégiája a 2022. februári inváziót megelőzően[179].

A védekezési oldal önszerveződése. A 2022-es háború irodalmának legmeglepőbb fejezete a horizontális védelmi hálózatok megjelenése. A NAFO (North Atlantic Fellas Organization) jelenségét Keir Giles (a Hybrid CoE számára készített elemzésében[180] dokumentálta: a humor és a mémek a dezinformáció elleni védekezés eszközévé váltak, az önszerveződő közösség a trollfarmok narratíváit nem cáfolattal, hanem szatírával semlegesítette, megzavarva a támadó OODA-hurkát. Ez a jelenség a konnektív cselekvés (Bennett–Segerberg 2012) védekezési alkalmazásaként értelmezhető.

Bányász Péter és Szádeczky Tamás magyar kutatása a felhasználói reziliencia állapotát mérte:[181] a generatív MI-alapú vizuális manipulációval szembeni ellenálló képesség a magyar Facebook-felhasználók körében alacsonynak bizonyult (318 fős mintán az átlagos felismerési pontosság mindössze 63,57%-ot ért el, a 70%-os küszöbérték alatt; a 18–25 éves korosztály 69,08%-os, a 26 év felettiek 58,53%-os eredményt mutattak, és a magasabb platformbizalom szignifikánsan rosszabb felismeréssel járt: 56,47% vs. 66,32%)[182], ami arra utal, hogy a 2022-es háború tanulságai a közép-európai társadalmakba még nem szívódtak fel kellő mértékben. A Lebrun (2023) által javasolt kognitív beavatkozás-előrejelzési keretrendszer[183] pontosan erre a résre reagál: nem a tartalom, hanem a kognitív feldolgozási folyamat szintjén próbálja anticipálni a támadást.

---

179 KALENSKÝ, Jakub – OSADCHUK, Roman (2024): How Ukraine fights Russian disinformation: Beehive vs mammoth. Hybrid CoE Research Report 11, Helsinki.

180 GILES, Keir (2023): *Humour in online information warfare: Case study on Russia's war on Ukraine*. Hybrid CoE Working Paper 26. European Centre of Excellence for Countering Hybrid Threats, Helsinki. 28. o.

181 BÁNYÁSZ Péter et al. (2025): *The resilience of social media users against Generative AI-based visual manipulation: A survey among Hungarian Facebook users*. In CEEeGov 2025: Proceedings of the Central and Eastern European eDem and eGov Days 2025. New York: ACM, 181–188. Online: https://doi.org/10.1145/3773002.3774813

182 A felmérés pontos paraméterei: 318 magyar Facebook-felhasználó; átlagos felismerési pontosság 63,57% (a 70%-os küszöbérték alatt); 18–25 éves korosztály: 69,08%, 26+ korosztály: 58,53%; magasabb platformbizalom rosszabb felismeréssel járt (56,47% vs. 66,32%). BÁNYÁSZ et al. (2025) i. m. 183–186. o.

183 LEBRUN, Maxime (2023): *Anticipating cognitive intrusions: Framing the phenomenon*. Hybrid CoE Strategic Analysis 33. European Centre of Excellence for Countering Hybrid Threats, Helsinki. 3., 7. o.

3.7. A kutatási rés azonosítása

Az előző alfejezetek áttekintése három szinten azonosít kutatási rést.

Az első a módszertani rés. A 2014-es és 2022-es esetet a meglévő irodalom külön-külön, részletesen dokumentálja, de a két időpontot strukturált, azonos kérdéssort alkalmazó összehasonlításban (SFÖ) eddig nem vizsgálták. A kronologikus vagy tematikus párhuzamkeresés nem elegendő: a paradoxon (2014-ben alacsony technológia + sikeres bénulás; 2022-ben magas technológia + kudarcot vallott bénulás) csak akkor válik tudományosan magyarázhatóvá, ha a két esetet azonos diagnosztikai nyelven – a disszertáció terminológiájával a H–E–I rácson – kódoljuk és vetjük össze.

A második a kognitív mechanizmus rése. A meglévő elemzések jellemzően a tartalomra (milyen narratívák keringtek?) vagy a csatornára (milyen platformokon terjedtek?) fókuszálnak. Hiányzik az a szisztematikus vizsgálat, amely a befogadói oldal feldolgozási mechanizmusait – a Kahneman-féle kettős rendszer, a szubliminális hatásmechanizmusok, a Fauconnier-féle mentális terek kényszerített átírása – a műveleti konfigurációkkal együtt modellezi. Az OxIPO-keretrendszer alkalmazása ezt a rést kívánja betölteni.

A harmadik a védekezési rés. A szabályozási irodalom (EU Action Plan, DSA) és a platformszintű válaszok (moderáció, Community Notes) között hiányzik az az integráló keret, amely a védekezést modalitásonként differenciáltan, mikro–mezo–makro szinteken operacionalizálja. A Multimodális Reziliencia Mátrix (MRM) ennek a résnek a betöltésére vállalkozik.

A negyedik – és a disszertáció szempontjából talán legfontosabb – rés a Híd-időszak magyarázó ereje. A meglévő irodalom a 2014-es és a 2022-es esetet részletesen dokumentálja, de a kettő közötti átmeneti periódust jellemzően kronológiai narratívaként kezeli, nem pedig strukturált magyarázó változócsomagként. A Hybrid CoE Paper 12 az elrettentés ötödik hullámát tárgyalva a reziliencia-alapú megközelítést jelöli meg a hibrid fenyegetések elleni védekezés alapjaként, és a Communication–Capability–Credibility (3C) pillérrendszert dolgozza ki[184], de ezt nem kapcsolja össze a konkrét esettanulmányok összehasonlításával. A disszertáció ezt a rést a Híd-időszak G–

[184] MONAGHAN, Sean (2022): Deterring hybrid threats: Towards a fifth wave of deterrence theory and practice. Hybrid CoE Paper 12, Helsinki.

M–T–V lánc szerinti elemzésével (5. fejezet) és a H–E–I diagnosztika alkalmazásával (4. és 6. fejezet) kívánja betölteni.

A disszertáció tehát nem újabb esettanulmányt ad a meglévő irodalomhoz, hanem a meglévő tudást egy összehasonlító, diagnosztikus és operacionalizálható keretbe rendezi. A 2. fejezetben levezetett módszertani architektúra (SFÖ → H–E–I → FMK-rács → OxIPO → MRM) a 4. fejezetben kerül első alkalmazásra: a 2014-es krími esettanulmány kódolásával.

4. A STRATÉGIAI MEGLEPETÉS PÉLDÁJA – KRÍM (2014) ESETTANULMÁNY

Az előző fejezetek (1–3.) után kimondható a 4. fejezet tételmondata: a Krím (2014) stratégiai meglepetése nem elsősorban katonai „trükk" volt, hanem egy olyan – időben előkészített – műveleti konfiguráció, amely a bizonytalanságot (ambiguity) fegyverként használta a döntési lánc megakasztására.[185]

Ebből két dolog következik. Egyrészt a fejezet nem a tartalmak propaganda jellemzőit vizsgálja, hanem a műveleti mintázatot: aktor–szándék–eszközmix, csatornák és időzítés, majd az ebből következő kognitív hatás.[186] Másrészt a fejezet nem úgy épül fel, hogy a „mi történt?" kérdésre válaszoljon, mert ezt a kronológia megadja, hanem arra ad választ, hogy miért működött – és miért bizonyult nehezen detektálhatónak és nehezen megválaszolhatónak a 2014-es konfiguráció.[187]

A 4. fejezet ezért a Strukturált, Fókuszált Összehasonlítás (SFC/SFÖ) rendjében ugyanazt a elemzési nyelvet fogja alkalmazni a Krím-félsziget annektálás esetére, amelyet a disszertáció módszertani része rögzített: H–E–I (Helyzet–Előrejelzés–Irányítás) mint diagnosztikai sorrend, majd ennek belső operacionalizálása az FMK-rács, az OxIPO-modell, és a multimodális reziliencia mátrix (MRM) felé. Ennek a sorrendnek logikai oka van: előbb rögzíteni kell, hogy mi volt a

185 MUMFORD, Andrew: *Ambiguity in hybrid warfare*. Hybrid CoE Strategic Analysis 24, Helsinki, 2020, 3–6. o.

186 DARCZEWSKA, Jolanta: *The Anatomy of Russian Information Warfare: The Crimean Operation, A Case Study*OSW (Centre for Eastern Studies), Warsaw, 2014, 5. o.

187 CULLEN, Patrick: *Hybrid threats as a new "wicked problem" for early warning*. Hybrid CoE (European Centre of Excellence for Countering Hybrid Threats), Strategic Analysis 8, 2018, 2018, 1-5. o.

helyzet (aktor, szándék, eszközmix), és csak utána érdemes megkérdezni, hogy miért nem jelzett időben a rendszer, illetve miért akadt el a legitim válasz (attribúció, reakció, kontrollok).

A fejezet elején ezért nem a 2014. február 27-i képekhez nyúlunk vissza azonnal, hanem röviden megmutatjuk: milyen előjelek tették 2012 és 2014 között a küszöb alatti működésmódot reálisan várhatóvá, és hogyan állt össze az a politikai–kommunikációs–műveleti háttér, amelyre a krími művelet ráépült.[188] Itt kulcs, hogy az időkeret nem utólagos, hanem több, egymástól független forrás által rögzített vizsgálati ablak: a NATO StratCom COE (NATO Strategic Communications Centre of Excellence), a Rigában, Lettországban található többnemzetiségű szervezet, amely a NATO stratégiai kommunikációs képességeinek fejlesztéséért felelős, elemzésében például kifejezetten a Vilniusban 2013. november 28–29-én tartott Keleti Partnerség csúcstól vezeti el a kampányívet a Krím orosz annektálásáig, és már ezen a szakaszon is nem-katonai, stratégiai kommunikációs szempontból értelmezi a válságot.

A 2012–2013-as előjelek között külön horgonyt érdemel az a doktrinális nyelv, amelyben a nem-katonai eszközök arányváltása (információs, politikai, gazdasági) a modern konfliktusok központi elemévé válik. Az orosz vezérkari főnök, Valerij Geraszimov 2013-ban publikált és később angolul is közölt írása, amely „A tudomány értéke az előrelátásban” (Cennoszty nauki v predvigyenyii) címmel jelent meg, a modern orosz katonai stratégia egyik legfontosabb elméleti alapvetése. Nyugati elemzők a cikket gyakran a „Geraszimov-doktrína” forrásaként említik, bár maga a szerző nem doktrínaként, hanem a hadviselés megváltozott jellegének elemzéseként tálalta. Írása nem a Krím „forgatókönyvét” adja meg, hanem azt a kognitív és operatív legitimációs keretet, amelyben a katonai és nem-katonai eszközök integrált alkalmazása racionálisnak és tervezhetőnek látszik.[189] A 4. fejezet bevezetőjében ennek azért van helye, mert ezzel előre rögzíthető: a Krím-félsziget annektálásának gondolata megalapozott volt egy olyan gondolkodási keretben, amely már eleve együtt kezeli a fegyveres jelenlétet, a megtévesztést, a kommunikációs nyomást és a legitimáció-építést.

---

[188] LANGE-IONATAMIŠVILI, Sanda et al.: *Analysis of Russia’s Information Campaign against Ukraine* (Executive Summary + teljes jelentés). NATO StratCom COE, Riga, 2015, Executive Summary: 2. o.; Teljes jelentés: 3., 7., 8. o.

[189] GERASIMOV, Valery: *The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations*. Military Review (Jan–Feb), 2016, 23–29. o.

A 2013 végi ukrajnai események (Euromajdan) nem azért fontosak, mert innen indul a háború, hanem mert innen indul a fogadófelület. Ugyanis a belpolitikai krízis és a geopolitikai töréspont olyan környezetet teremtett, amelyben a narratív keretezés (illegitim puccs / veszélyeztetett kisebbség / rend helyreállítása) műveleti értelmet nyerhetett. A NATO StratCom COE jelentése azért különösen hasznos ehhez, mert a nem-katonai aspektusokat már 2014-ben és 2015-ben stratégiai kommunikációs perspektívából rendszerezi, és a vizsgált időablakot egyértelműen meghatározza.

A krími művelet információs komponense elemeire bontható. A 2014-es átfordulásnál az OSW (Centre for Eastern Studies – magyarul: Keleti Tanulmányok Központja) Jolanta Darczewska elemző és Oroszország-szakértő által jegyzett esettanulmánya azért kulcsfontosságú előjel, mert a krími műveletet már a megjelenésekor úgy írja le, mint az információs hadviselési képességek demonstrációját. Vagyis nehezen detektálható módszerek, titkos és nyílt csatornák együttes használata (titkosszolgálatok, diplomácia, média), célként pedig az elitek és társadalmak alárendelése van megjelölve. Ezzel pedig kijelöli, hogy itt nem klasszikus médiaelemzés a cél, hanem a műveleti logika rekonstruálása a kognitív térben.

2014 februárjára tehető a többértelműség mint reakció-blokkoló eszköz (a stratégiai meglepetés mechanizmusa) megjelenése. A stratégiai meglepetés „magja" a krími esetben nem az volt, hogy megjelent a fegyveres erő, hanem az, hogy nem volt egyértelműen besorolható. Joggal merült fel a kérdés, hogy helyi milícia, különleges erők, önvédelmi egységek, vagy állami invázióhoz köthető aktorok? Dr. Andrew Mumford, a helsinki székhelyű Hybrid CoE (European Centre of Excellence for Countering Hybrid Threats) biztonsági szakértői csoportjának tagja és a Nottinghami Egyetem hadtudományi professzora ezt a krími mintát úgy írja le, mint kiszámított többértelműséget. A bizonytalanság nem a rejtőzködés melléktermé ke, hanem a legitim válasz megakasztására szolgáló műveleti eszköz.[190] Ez azért fontos, mert itt lehet először didaktikusan összekötni a stratégiai meglepetés fogalmát az OxIPO-logikával. Tehát a feldolgozási (Process) szakaszban keletkező döntési késés (mit látunk valójában?) időt ad a művelet fizikai konszolidációjához.

Így merül fel a kérdés, hogy miért nem jelzett a rendszer? És ennél a pontnál kell megemlíteni a „wicked problem", magyarul fondorlatos vagy makacs probléma fogalmát. A „wicked problem"

[190] MUMFORD, Andrew: *Ambiguity in hybrid warfare*. Hybrid CoE Strategic Analysis 24, Helsinki, 2020, 3–6. o.

(magyarul leginkább: „gonosz probléma” / „szelídíthetetlen probléma”) fogalmát két várostervező professzor, Horst Rittel és Melvin M. Webber vezette be: először egy 1967-es, a Berkeley Egyetemen tartott szemináriumon vált ismertté, majd a koncepció nemzetközi hivatkozási ponttá a Dilemmas in a General Theory of Planning című, 1973-ban a Policy Sciences folyóiratban megjelent tanulmányuk nyomán lett. Ebben az értelmezési keretben a fogalom lényege az, hogy a hibrid fenyegetések és az ezekhez kapcsolódó előrejelzés nem olyan feladat, ahol egyértelműen kijelölhető a „kész” állapot: ha végül nem következik be incidens, az ugyanúgy jelentheti azt, hogy a figyelmeztetés megelőzte a kárt, mint azt, hogy a riasztás eleve téves volt. Ráadásul az előrejelzés maga is belenyúl a rendszerbe: a jelzés hatására a támadó alkalmazkodik, taktikát vált, így az eredeti elemzés gyorsan részben érvényét veszítheti, vagy legalábbis újrakalibrálást igényel. A helyzetet tovább rontja, hogy a hibrid működés tudatosan a „szürke zónában” marad, ezért az események besorolása eleve vitatott: ami az egyik elemzőnek ellenséges befolyásolás, az a másiknak könnyen tűnhet puszta diplomáciai súrlódásnak vagy belpolitikai zajnak. Végül mindez nem redukálható technikai problémára, mert a jelenség több szintet egyszerre érint: politikai, pszichológiai és társadalmi tényezők szövedéke, ahol bármilyen „megoldás” (például szigorúbb ellenőrzés vagy szabályozás) szükségszerűen mellékhatásokkal járhat (például a nyilvánosság és a szólásszabadság terének szűkülésével), vagyis a beavatkozás mindig ellentételezéssel vagy kompromisszummal és normatív vitákkal terhelt. Vagyis a krími meglepetés nem pusztán figyelmetlenség volt. Patrick Cullen (Hybrid CoE) a Krím annektálása utáni korszakban a hibrid fenyegetéseket kifejezetten „wicked problem”-ként írja le a korai riasztás számára. A béke–háború határ elmosása és a küszöb alatti működés szándékos kialakítása a detektálást és a reakciót is megnehezíti. Ennek bevezető funkciója az, hogy a fejezet olvasója már az elején értse: a 4. fejezetben az „E” (Előrejelzés) nem kiegészítő, hanem a meglepetés logikai központja.[191]

Jeleznem kell, hogy a 2014-es esetben a támadó fél egyik fő erőforrása a letagadhatóság, ezért a bizonyítás nem mindig kész dokumentumból jön, hanem bizonyítékláncból, vagyis idővonal-rekonstrukcióból, nyílt forrású bizonyítékokból vagy akár kiszivárgásokból. A Bellingcat MH17-jelentése a nyílt forrású bizonyítékképítés mintáját adja[192], míg a RUSI (Royal United Services

[191] CULLEN, Patrick: *Hybrid threats as a new “wicked problem” for early warning*. Hybrid CoE (European Centre of Excellence for Countering Hybrid Threats), Strategic Analysis 8, 2018, 2018, 1-5. o.

[192] BELLINGCAT Investigation Team: MH17 – The Open Source Evidence. 2015, 1., 7., 10. o.;

Institute) Szurkov-leakek feldolgozása azt mutatja meg, hogyan lehet belső koordinációs és irányítási nyomokat rekonstruálni dokumentum-alapon.[193] A fejezet bevezetőjében ennek azért van helye, mert így előre rögzíthető a triangulációs alapelv: az intézményi elemzések + OSINT + idővonal együtt fogja kitölteni a Krím-esettanulmány bizonyítási terét.

4.1. A kézi vezérlésű hibrid hadviselés kora

A 2014 február–márciusi krími annektálás és a kelet-ukrajnai eszkaláció nem pusztán egy lokális, területszerző epizód volt, hanem olyan fordulópont, amely az európai biztonságpolitikai gondolkodásban cezúraként működik. Onnantól kezdve a katonai és nem-katonai eszközök integrált alkalmazása nem kivétel, hanem működési mód lett. A magyar hadtudományi diskurzusban például Resperger István, a hibrid hadviselés hazai értelmezésének szakértője, éppen ezt a kombinált, többrétegű, több színtéren egyszerre megjelenő fenyegetéslogikát emeli ki, amikor a hibrid hadviselést a modern konfliktusok egyik meghatározó mintázataként tárgyalja.[194] E fejezetben ezt a cezúrát nem retorikai fordulatként kezelem, hanem diagnosztikai problémaként. Vagyis mitől vált a Krím 2014-ben stratégiai meglepetéssé, és mitől volt a művelet nehezen detektálható, nehezen megnevezhető, végül nehezen megválaszolható konfiguráció?

A kiindulópontom – összhangban az 1–3. fejezetben rögzített módszertani kerettel – nem a „mi történt?“, hanem a „miért működött?” kérdésköre. A kronológia szükséges, de nem elég, mert a döntési láncban ukrán és nyugati oldalon egyaránt előálló késés és bizonytalanság nem magától értetődő, hanem előállított állapot. Ennek megértéséhez a fejezet a H–E–I-mátrix (Helyzet–Előrejelzés–Irányítás) sorrendet követi: előbb rögzítem a „Helyzetet” (aktor–szándék–eszközmix; csatornák; küszöb alatti működés), majd azt vizsgálom, hogy miért nem jelzett időben a rendszer (Előrejelzés), végül pedig azt, hogy miért akadt el a legitim válasz (Irányítás: attribúció, reakció, kontrollok).

A 2014-es eset sajátossága, hogy a hibrid konfiguráció nem technológiai csodafegyverrel érte el a kognitív fölényt, hanem egy olyan, kézi vezérlésű, mégis hálózatosan koordinált

---

[193] SHANDRA, Alya – SEELY, Robert: The Surkov Leaks: The Inner Workings of Russia’s Hybrid War in Ukraine. RUSI, 1–4. o.

[194] RESPERGER István: *A hibrid hadviselési mód jellemzői korunk konfliktusaiban*. Rendőrségi Tanulmányok, 2020/2, 104–118. o., különösen 106–107. o.

eszközrendszerrel, amely már a közösségi média (Facebook, Twitter, VKontakte) korszakában működött. Ugyanakkor a mai értelemben vett generatív mesterséges intelligencia multimodális tartalom tömegtermelés és a nagy léptékű, automatizált, algoritmikus célzás még nem állt rendelkezésre. A kérdés tehát nem az, hogy miért nem volt high-tech a Krím, hanem hogyan lehetett „low-tech" környezetben is kognitív dominanciát elérni. Ebben a logikában a Krím nem a 2022 utáni iparosított korszak kicsinyített mása, hanem az a kiindulópont, amelyhez képest később a technológiai ugrás értelmezhetővé válik.[195]

A kézi vezérlésű korszak lényege a források alapján nem az eszközök primitívsége, hanem a kombinált csatornahasználat és az ehhez illeszkedő műveleti időzítés. A Keleti Tanulmányok Központja (OSW – Centre for Eastern Studies) fentebb már említett elemzője és Oroszország-szakértője, Jolanta Darczewska már 2014-ben úgy írja le a „Crimean operation"-t, mint olyan információs hadviselési demonstrációt, ahol titkos és nyílt csatornák együtt, összehangoltan működnek (titkosszolgálati/operatív komponensek, diplomáciai csatornák, médiakomponens). A politikai cél pedig az döntéshozói elit és a társadalom „alárendelése" – vagyis kognitív és legitimációs térben történő kényszerítés.[196] Ez azért kritikus a 4.1 alfejezet szempontjából, mert rögzíti: a krími meglepetés nem a katonai jelenlét puszta ténye, hanem az a műveleti konfiguráció, amelyben a katonai és kommunikációs komponensek egymásra zárnak.

A 2013–2014-es kézi vezérlésű korszakban ekkorra stabilizálódik az a nyelv, amelyben a nem-katonai eszközök integrált alkalmazása racionális és tervezhető. Valerij Geraszimov, az orosz vezérkar főnöke a korábbiakban hivatkozott cikkében rögzíti, hogy a konfliktusokban a nem-katonai eszközök szerepe és aránya megnőtt, és a klasszikus formák/módszerek újragondolása szükséges. Fontos hangsúly, hogy ez nem Krím-forgatókönyv, hanem legitimációs és műveleti keret, amelyben a katonai–nem-katonai integráció normává váló stratégiai logika.

Ezzel párhuzamosan a Nyugat oldalán a detektálás és a válasz egy olyan térben kényszerül működni, amelyet a hibrid logika szándékosan küszöb alatti állapotban tart. A hibrid fenyegetések

---

[195] DARCZEWSKA, Jolanta: *The Anatomy of Russian Information Warfare: The Crimean Operation, A Case Study*OSW (Centre for Eastern Studies), Warsaw, 2014, 23–24. o. (a „Crimean operation" kombinált csatorna- és eszközhasználata).

[196] DARCZEWSKA, Jolanta: *The Anatomy of Russian Information Warfare: The Crimean Operation, A Case Study*OSW (Centre for Eastern Studies), Warsaw, 2014, 23–24. o.

elleni fellépésre létrehozott Európai Kiválósági Központ (Hybrid CoE – European Centre of Excellence for Countering Hybrid Threats, helsinki székhelyű, többnemzeti szakpolitikai és elemző központ) szakértője, Andrew Mumford hadtudományi kutató a krími mintát úgynevezett kiszámított többértelműségként írja le. Amikor a bizonytalanság nem a rejtőzködés mellékterméke, hanem reakció-blokkoló eszköz, amely a legitim válasz megakasztását célozza.[197] Ez adja a kézi vezérlésű korszak egyik kulcskövetkeztetését: a kognitív dominancia nem feltétlenül a legfejlettebb technológiából, hanem a döntési késleltetés megteremtéséből fakad, amit később az OxIPO-feldolgozási szakaszban fogok operacionalizálni.

A kézi vezérlésű korszak további sajátossága, hogy bár a hálózati manipuláció iparosodása - különösen 2016 után - lesz majd igazán látványos, a 2013–2014 körüli időszakban már megjelenik az a mintázat, amely később számítógépesített propagandaként írható le. Ez a platformtérben végzett szervezett aktivitás korai, alacsony intenzitású, majd felfutó szakaszaiból áll. Az Oxfordi Egyetemhez kötődő Computational Propaganda Project tudományos kutatócsoport például empirikus idősoros megfigyelésekre támaszkodva rögzíti, hogy bizonyos, később az Internet Research Agency-hez (IRA) kapcsolt aktivitások már 2013 körül megjelennek, és később fokozódnak.[198] Tehát a krími annektáláskor használt online jelenlét nem a semmiből jött, hanem egy épülő, hálózatos befolyásolási gyakorlat korai, még kézi irányítású fázisába illeszkedett.

Végül rögzítenem kell a bizonyítási módszereket is: a 2014-es esetben a támadó fél egyik fő erőforrása a letagadhatóság, ezért a bizonyítás nem mindig kész dokumentumból áll, hanem bizonyítékláncokból (idővonal-rekonstrukció, nyílt forrású bizonyítékok, kiszivárgások, intézményi elemzések összeolvasása). A Bellingcat (független, nyílt forrású vizsgálatokra szakosodott oknyomozó kollektíva) MH17-ügyben alkalmazott OSINT-evidencialánca módszertani mintát ad arra, hogyan lehet letagadhatóság mellett is rekonstruálni felelősségi mintázatokat.[199] A Royal United Services Institute (RUSI), a londoni védelem- és biztonságpolitikai think tank pedig a Szurkov-leakek feldolgozásával azt mutatja meg, hogyan

[197] MUMFORD, Andrew: *Ambiguity in hybrid warfare*. Hybrid CoE Strategic Analysis 24, Helsinki, 2020, 1–2. o.

[198] Oxford University / Computational Propaganda Project: *The IRA, Social Media and Political Polarization in the United States* (feltöltött PDF), 9. o., 25. o. (2013-tól megjelenő, majd felfutó aktivitásminták).

[199] BELLINGCAT Investigation Team: *MH17 – The Open Source Evidence*. 2015, 1., 7., 10. o.

lehet belső koordinációs és irányítási nyomokat dokumentum-alapon visszafejteni.[200] Így a Krím-esettanulmány kézi vezérlésű korszakát triangulált bizonyításból igyekszem felépíteni.

A 4.1 összegző tézise ezért a következő: 2014-ben még nem a technológiai automatizáció, hanem a kézi irányítású, de hálózatcentrikusan koordinált információs és műveleti konfiguráció termelte ki a stratégiai meglepetést. A fejezet következő alrészei ezt a konfigurációt bontják vissza a H–E–I diagnosztikai sorrendben, majd az FMK-rács, az OxIPO és az MRM nyelvére fordítva a műveleti mintázatot kísérlem meg feltárni.

4.1.1. A vizsgálati ablak és a kódolási logika rögzítése (SFC/SFÖ és trianguláció)

A 4. fejezetben a célom nem az, hogy a krími eseménysort „újra elmeséljem", hanem hogy egy alátámasztható vizsgálati keretet rögzítsek: mi az, ami 2012–2013–2014 között már előkészítette a krími konfigurációt, és mi az, ami 2014 február–márciusban stratégiai meglepetéssé állt össze. Ezt a vizsgálati ablakot nem utólagos dramaturgia alapján rajzolom meg, hanem úgy, hogy több, egymástól független forrás egybehangzóan jelöli ki a krími műveletet megelőző és közvetlenül kísérő információs–műveleti folyamatokat.[201]

A Strukturált, Fókuszált Összehasonlítás (SFC/SFÖ) rendje itt egy fegyelmi eszköz a narratív technika elkerülése érdekében: ugyanazt a kérdésrácsot alkalmazom a krími esetre, amit a módszertani fejezetben rögzítettem. A 4. fejezet első lépése ezért a H–E–I (Helyzet–Előrejelzés–Irányítás) diagnosztikai sorrend, mert a krími meglepetés logikáját csak akkor lehet tisztán megmutatni, ha előbb tisztázódik: milyen helyzetet építettek fel (aktor–szándék–eszközmix, csatornák, időzítés), és csak utána érdemes megvizsgálni, miért nem jelzett időben a rendszer, illetve miért akadt el a legitim válasz (attribúció, reakció, kontrollok).[202]

---

[200] SHANDRA, Alya – SEELY, Robert: *The Surkov Leaks: The Inner Workings of Russia's Hybrid War in Ukraine*. RUSI, 1–4. o.

[201] NATO STRATCOM COE (NATO Strategic Communications Centre of Excellence – Riga): *Analysis of Russia's Information Campaign against Ukraine* (vizsgálati időablak és narratív ív), 2015, több helyen (pl. 3., 7–8., 12–15. o.).

[202] DARCZEWSKA, Jolanta: *The Anatomy of Russian Information Warfare: The Crimean Operation, A Case Study*. OSW (Centre for Eastern Studies), Warsaw, 2014, pl. 4–7., 23–24. o.

A H–E–I rögzítése után következik az operacionalizálás: ugyanazt a krími jelenséget több elemzési keret nyelvére fordítom le, mert a krími konfiguráció egyszerre volt kommunikációs és műveleti probléma. Az FMK-rács (fegyvernek minősülő kommunikáció) az „aktortermék" (szándékosság–szervezettség–hatás) felől teszi kódolhatóvá a kampányt; az OxIPO-modell a feldolgozási szűkületet mutatja meg (Input–Process–Output), vagyis azt, hogy a bizonytalanság miért bénította meg a döntési láncot; a multimodális reziliencia mátrix (MRM) pedig a válaszoldali leltárt készíti elő (milyen kontrollok léteztek/hiányoztak, és melyik szinten: intézményi, társadalmi, technológiai).[203]

A trianguláció ebben a fejezetben bizonyítási kényszer: a krími eset egyik fő erőforrása a letagadhatóság volt, ezért az igazolásom nem mindig „egy dokumentum = egy bizonyíték" logikával áll elő, hanem bizonyítéklánc-jelleggel (idővonal, OSINT, kiszivárgott anyagok, intézményi jelentések). A nyílt forrású bizonyítás (OSINT) szerepe ezért két okból fontos. Egyrészt a letagadhatóság áttörésére képes módszertani sablont ad, másrészt megmutatja, hogy mi az, ami egyáltalán állítható nagy bizonyossággal a krími művelet belső logikájáról.[204],[205]

Következésképpen célom, hogy ugyanazt a krími konfigurációt először H–E–I szerint rögzítem (diagnózis), majd FMK-rács/OxIPO/MRM szerint „lefordítom" (operacionalizálás). Ettől lesz az esettanulmány alkalmas arra, hogy később a 2022-es invázióval összevethető legyen – nem történetként, hanem mintázatként.[206]

4.1.2. 2012–2013–2014-es előjelek, a krími konfiguráció előzményei

A 2012–2013–2014 közötti időszakot azért teszem a fejezet elejére, mert ezzel elkerülhető az a visszatérő interpretációs hiba, hogy a Krím villámcsapásként jelenik meg. A krími művelet stratégiai meglepetése nem azt jelenti, hogy nem volt előzménye, hanem azt, hogy az előzmények

[203] MUMFORD, Andrew: *Ambiguity in hybrid warfare*. Hybrid CoE Strategic Analysis 24, Helsinki, 2020, pl. 3–6. o.

[204] BELLINGCAT Investigation Team: *MH17 – The Open Source Evidence*, 2015, pl. 1–3., 12., 21–23. o.

[205] SHANDRA, Alya – SEELY, Robert: *The Surkov Leaks: The Inner Workings of Russia's Hybrid War in Ukraine.* RUSI Occasional Paper, July 2019, pl. 1–3., 8–9., 16., 23. o.

[206] CULLEN, Patrick: *Hybrid threats as a new "wicked problem" for early warning*. Hybrid CoE (European Centre of Excellence for Countering Hybrid Threats), Strategic Analysis 8, 2018, 2018, pl. 1–5., 7. o.

nem kaptak időben megfelelő besorolást (küszöb alatti működés, többértelmű aktor-azonosítás, szürkezóna-jog). Ez a különbség a H–E–I logikájában azonnal látszik: a H (helyzet) elemei sokszor már jelen voltak, csak az E (előrejelzés) nem tudta őket időben fenyegetéssé összeállítani, az I (irányítás) pedig nem tudott legitim és gyors választ adni.[207]

Már megjelent a doktrinális előjel, vagyis a nem-katonai eszközök integrált logikája. A krími konfigurációt egy olyan gondolkodási keret teszi tervezhetővé, amelyben a katonai és nem-katonai eszközök nem külön világok. Ennek egyik, sokat idézett – és a nyugati szakirodalomban gyakran félreértett – horgonya Valerij Geraszimov orosz vezérkari főnök írása („The Value of Science Is in the Foresight"), amely a modern konfliktusok megváltozott jellegét tárgyalja, és a műveleti formák és módszerek újragondolását sürgeti.[208] Nem „Krím-forgatókönyvként" használom, hanem a legitimációs nyelv bizonyítékaként: abban a keretben, ahol a nem-katonai eszközök integrált alkalmazása racionális, a krími művelet nem improvizáció, hanem konfiguráció.

A műveleti előjel az információs hadviselés mint demonstráció és alárendelés. A Keleti Tanulmányok Központja (OSW – Centre for Eastern Studies, Varsó) által publikált, Jolanta Darczewska Oroszország-szakértő elemző esettanulmánya már 2014-ben úgy írja le a krími műveletet, mint információs hadviselési képességek demonstrációját: nyílt és rejtett csatornák együtt, valamint olyan cél, amely nem pusztán narratív győzelem, hanem elitek és társadalmak alárendelése.[209] Ezt én nem „médiaelemzésnek" olvasom, hanem H (helyzet) alapállításnak: a krími esetben a kommunikáció a művelet része, nem kísérő jelenség.

Politikaikommunikációs előjelek is voltak. A NATO Stratégiai Kommunikációs Kiválósági Központ (NATO StratCom COE, Riga) 2014–2015-ös időablakot használó elemzései azért fontosak, mert a krízist már korán nem-katonai (stratégiai kommunikációs) perspektívából rendszerezik, és egyértelmű vizsgálati ablakot jelölnek ki, például a 2013. november 28–29-i vilniusi Keleti Partnerség csúcstól induló ívben. Ez a fejezet szempontjából azt jelenti: a

---

[207] KOFMAN, Michael – ROJANSKY, Matthew (2015): *A Closer Look at Russia's "Hybrid War".* Kennan Cable, No. 7. Washington D.C.: Wilson Center, Kennan Institute. 1–5., 7–8. o.

[208] GERASIMOV, Valery: *The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying Out Combat Operations.* Military Review (January–February 2016), 23–29. o.

[209] DARCZEWSKA, Jolanta (2014): The Anatomy of Russian Information Warfare: The Crimean Operation, A Case Study. OSW (Centre for Eastern Studies), Warsaw. 5–7. o.

„fogadófelület” (legitimációs vákuum, narratív polarizáció) nem utólagos találmány, hanem dokumentáltan része a válságmechanizmusnak.[210]

Technológiai–szervezeti előjel volt a kézi vezérlésű, de már hálózati működés. A krími korszakot nem generatív MI és nem deepfake dominálta, de a hálózati és platformlogikai dimenzió már jelen volt – emberi irányítással, kezdetleges automatizációval, szervezeti koordinációval. A 2013-tól működő Internet Research Agency (IRA) köré szerveződő, platformokon átívelő befolyásolási aktivitásról a későbbi, empirikus elemzések olyan bizonyítékokat adnak, amelyek segítenek megérteni: a 2014-es kognitív nyomás nem a technológiai csoda miatt működött, hanem a szervezett, emberi hálózatok és a platformdinamika kihasználása miatt.[211] Ennek a fejezetben azért van helye, mert ez adja a kézi vezérlésű, de skálázásra kész állapot fogalmilag tiszta leírását.

Attribúciós előjelnek tekinthető a letagadhatóság és evidencialánc. A krími művelet egyik központi trükkje nem a puszta erő alkalmazása volt, hanem az aktor-besorolás elbizonytalanítása („kik ők?“). Ezt a mechanizmust Andrew Mumford – a Helsinki székhelyű Európai Hibrid Fenyegetések Elleni Kiválósági Központ (Hybrid CoE) szakértői közösségéhez kapcsolódó hadtudományi elemző – a „calculated ambiguity” (kiszámított többértelműség) fogalmával írja le. A bizonytalanság a legitim válasz megakasztására szolgáló műveleti eszköz volt. Attias (2024) a maszkirovka stratégiai szintű alkalmazását dokumentálja a 2014-es műveletre vonatkozóan: az orosz katonai jelenlét szisztematikus tagadása, a veszteségjelentések elnyomása és a „hihető letagadhatóság” (plausible deniability) fenntartása nem mellékes taktika, hanem a művelet gerincét képező megtévesztési rendszer volt[212] Itt kapcsolható össze didaktikusan a stratégiai meglepetés az OxIPO „Process” szűkületével: a feldolgozásban keletkező késés (mit látunk valójában?) időt ad a fizikai konszolidációra.

---

[210] LANGE-IONATAMIŠVILI, Sanda et al. (2015): Analysis of Russia’s Information Campaign against Ukraine. NATO Strategic Communications Centre of Excellence, Riga. 3., 7–8. o.

[211] Oxford University / OII: *The IRA, Social Media and Political Polarization…* (Internet Research Agency és polarizációs hatás), 2010-es évek empirikus visszaépítése, pl. 3–5., 9., 20. o.

[212] ATTIAS, Shay (2024): Hybrid Warfare and Informational Strategies: Russia’s Campaign in Ukraine (2014). In JOBBÁGY, Z. és ZSIGMOND, E.. (eds.): *Hybrid Warfare Reference Curriculum, Volume II.* Budapest: Ludovika. 238–239. o.

Hanna Smith (2022) a Hybrid CoE kutatási igazgatójaként a Mumford-féle kiszámított többértelműség (calculated ambiguity) mögött mélyebb döntéshozatali logikát azonosít. A kilátáselmélet (prospect theory) – Daniel Kahneman és Amos Tversky (1979) viselkedési közgazdaságtani modellje – szerint az emberek a veszteségek elkerülése érdekében aránytalanul nagyobb kockázatot vállalnak, mint amennyit a nyereségek megszerzéséért tennének. Smith ezt az egyenlőtlenséget alkalmazza az orosz katonai döntéshozatalra: az orosz vezetés a nagyhatalmi státusz vélt elvesztését olyan fenyegetésnek érzékeli, amely indokolja a Nyugat számára irracionálisnak tűnő katonai lépéseket. A Krím sikere és Ukrajna lerohanásának 2022-es viszonylagos kudarca így nem ellentmondás, hanem ugyanannak a veszteségkerülő kockázati logikának két kimenetele.[213]

A krími eset nem csak nem lett időben észlelve, hanem rosszul volt típusosítva. Horst W. J. Rittel és Melvin M. Webber 1973-as klasszikus tanulmánya („Dilemmas in a General Theory of Planning") a „wicked problem" fogalmával pontosan azt a helyzetet írja le, amikor a probléma nem rendelkezik egyértelmű lezárási ponttal, a beavatkozás maga visszahat a rendszerre, és a besorolás normatív vitákkal terhelt.[214] Patrick Cullen – a Hybrid CoE keretéhez kapcsolódó elemző – a hibrid fenyegetéseket kifejezetten ilyen „wicked problem"-ként tárgyalja a korai riasztás szempontjából, és a Krím utáni korszakot fordulópontként kezeli: a béke–háború határ elmosása és a küszöb alatti működés szándékos kialakítása a detektálást és a reakciót is megnehezíti.[215] Ennek a fejezetben azért kell szerepelnie, mert előre jelzi: a 4. fejezet „E" (Előrejelzés) dimenziója a meglepetés logikai központja.

A letagadhatóság miatt a krími esettanulmány nem építhet kizárólag „szép, kész" intézményi dokumentumokra. A Bellingcat MH17-aktája módszertani mintát ad arra, hogyan épül fel egy nyílt forrású evidencialánc (idővonal, geolokáció, vizuális bizonyítékok, platformnyomok), míg a Royal United Services Institute for Defence and Security Studies (RUSI) „Surkov Leaks" feldolgozása

[213] SMITH, Hanna (2022): How to read Russia: Internal structural disunity, risk-taking, and Russia's restless soul. Hybrid CoE Working Paper 17. European Centre of Excellence for Countering Hybrid Threats, Helsinki. 6–9. o.

[214] RITTEL, Horst W. J. – WEBBER, Melvin M.: *Dilemmas in a General Theory of Planning.* Policy Sciences, 4(2), 1973, 155–169. o.

[215] CULLEN, Patrick: *Hybrid threats as a new "wicked problem" for early warning*. Hybrid CoE (European Centre of Excellence for Countering Hybrid Threats), Strategic Analysis 8, 2018. 1–5. o.

azt mutatja meg, hogyan rekonstruálható a belső koordináció dokumentum alapon.[216],[217] A 4. fejezetben ezt azért rögzítem előre, mert így tiszta: a bizonyítási tér vegyes (szervezeti és OSINT és idővonal), és ezt következetesen végigviszem.

A NATO StratCom COE 2016-os jelentése – amely nyílt forrású stratégiai dokumentumokra és a fő orosz TV-csatornák doktrinális-narratológiai tartalomelemzésére épül – dokumentálja, hogy az annexációt megalapozó narratívákat („Krím Oroszországé", „Ukrajna egyesül Oroszországgal", a „neonáci fenyegetés elleni harc") nem az akció pillanatában alakították ki, hanem évekkel korábban szándékosan építették és tartották fenn. A jelentés Narrative Control melléklete doktrinális szövegként elemzi a narratív kontroll fogalmát: eszerint a narratív kontroll erősebb eszköz, mint a médianapirend meghatározása, mert a befogadók elutasítják azokat a történeteket, amelyek ellentmondanak az „alapnarratívájuknak". Ha egy autoritárius állam elég hosszan gyakorolja a narratív kontrollt, a kritikusan nem gondolkodó társadalmi szegmens változatlan formában fogadja be az információt. Ez a mechanizmus közvetlenül releváns az FMK-rács Narratív Koherencia paraméteréhez: a 2014-es narratív koherencia nem a kampány során jött létre, hanem évek előkészítő munkájának eredménye volt.[218]

4.2. Helyzet-dimenzió (Situation): A bemeneti oldali mintázatok rögzítése

A H–E–I diagnosztikai mátrix első oszlopa, a Helyzet (Situation) azt rögzíti, miből állt össze a krími konfiguráció 2014 elején: milyen aktor–szándék–eszközmix jelent meg, milyen csatornákon futott a műveleti termék, és milyen terjesztési architektúra tette lehetővé, hogy a kinetikus műveletek még „névtelenül" (jelzés nélkül) fussanak, miközben az információs térben összehangolt offenzíva zajlott.

A „helyzet" dimenziót ebben a fejezetben három, egymással összefüggő indikátorcsoporttal kódolom. (1) Narratív koherencia: a mesternarratíva és a hozzá illesztett rész-narratívák összhangja (milyen üzenetek, milyen érzelmi horgonyok, milyen keretezés). (2) Csatorna-szinkronizáció: a

---

[216] BELLINGCAT Investigation Team (2015): MH17 – The Open Source Evidence. 1–3., 21–23. o.

[217] SHANDRA, Alya – SEELY, Robert (2019): The Surkov Leaks: The Inner Workings of Russia's Hybrid War in Ukraine. RUSI Occasional Paper. 8–9., 16., 23. o.

[218] NATO STRATCOM COE (2016): Analysis of Russia's Information Campaign against Ukraine. NATO Strategic Communications Centre of Excellence, Riga. 16., 39. o. (Narrative Control melléklet)

hagyományos média, a hivatalos nyilatkozati tér és az online tér összehangolt működése (hibrid médiarendszerként). (3) Volumen és amplifikáció: a terjesztés tömegessége és „hangosítása", amely 2014-ben még döntően kézi vezérlésű, de már hálózatosan koordinált (kommentelők, álprofilok, korai troll-kapacitások).[219]

A 2014-es krími konfigurációt nem „média tartalmi" jelenségként olvasom, hanem műveleti konfigurációként. Ezt a szemléletet a Keleti Tanulmányok Központja (OSW – Centre for Eastern Studies, Varsó; regionális biztonságpolitikai kutatóintézet) Jolanta Darczewska által jegyzett esettanulmánya különösen tisztán támasztja alá: a krími műveletet az információs hadviselési képességek demonstrációjaként írja le, ahol nyílt és rejtett csatornák kombinációja (titkosszolgálati/operatív komponensek, diplomáciai tér, média) együttesen szolgálja a társadalmi-politikai alárendelést és a legitimációs tér átrendezését.[220] Ez a fejezetben azt jelenti: a „Helyzet" dimenzió nem háttér, hanem a művelet egyik fő hadszíntere.

4.2.1. Narratív koherencia: fenyegetés-keretezés és legitimációs átfordítás

A narratív koherencia a Krím 2014 esetén nem abban állt, hogy minden állítás „igaz" volt, hanem abban, hogy a kommunikációs termékek következetesen ugyanabba a magyarázó keretbe illeszkedtek. A keretezés-elméleti alap (frame-fogalom) szerint a keretezés lényege, hogy bizonyos aspektusokat kiemel, másokat háttérbe tol, és ezzel megadja, mit kell problémának, oknak és következménynek látni.[221] A krími művelet „H" dimenziója ebből a szempontból úgy működött, hogy a helyzetet nem katonai agresszióként, hanem (váltakozó hangsúlyokkal) „rendhelyreállításként", „védelemként", „humanitárius szükségszerűségként" láttatta – ezzel a legitim válasz küszöbét már a bemeneti oldalon megemelte.[222]

---

[219] LANGE-IONATAMIŠVILI, Sanda és mtsai: *Analysis of Russia's Information Campaign against Ukraine*. NATO StratCom COE (NATO Strategic Communications Centre of Excellence), Riga, 2015, 3., 7–8., 12–15. o.

[220] Uo. 5–7. o.

[221] ENTMAN, Robert M.: *Framing: Toward Clarification of a Fractured Paradigm*. Journal of Communication, 43(4), 1993, 51–58. o.

[222] CULLEN, Patrick: *Hybrid threats as a new "wicked problem" for early warning*. Hybrid CoE (European Centre of Excellence for Countering Hybrid Threats), Strategic Analysis 8, 2018, 1–5., 7. o.

A NATO Stratégiai Kommunikációs Kiválósági Központ (NATO StratCom COE) 2015-ös ukrajnai kampány-elemzése azért fontos, mert a válságot kifejezetten nem-katonai (stratégiai kommunikációs) perspektívából elemzi, és kimondja: az információs jellegű aktivitásoknak primátust tulajdonít a vizsgált időszakban. A narratív koherenciát itt nem stílusjegyekben keresem, hanem a műveleti hasznosságban: hogyan épült fel egy olyan mesternarratíva, amely a célcsoportban fenyegetettséget és jogosultság-érzetet egyszerre tudott termelni (fenyegetés-keretezés + legitimációs átfordítás).

A 2014-es időszak egyik didaktikusan is megfogható tanulsága, hogy a koherencia nem az ellentmondások hiánya, hanem a keret egysége. A többértelmű működésmódban is lehet koherens a keret: miközben a „kik ők?" kérdés szándékosan nyitva marad, a „miért vannak ott?" kérdésre a kommunikáció folyamatosan ugyanazt a legitimáló választ kínálja. Ez az a pont, ahol a „Helyzet" dimenzió átvezet az OxIPO-logikára: a keret egységessége olyan kognitív előbeállítást hoz létre, amely a feldolgozási szakaszban késlelteti a veszély korrekt besorolását.[223]

4.2.2. Csatorna-szinkronizáció: hibrid médiarendszer és visszhangképzés

A csatorna-szinkronizáció a Krím 2014 esetén nem egyszerűen „sok platform használatát" jelenti, hanem azt, hogy a hagyományos (lineáris) média, a hivatalos nyilatkozati tér és az online tér egyetlen, egymást erősítő visszhangstruktúrává zárt össze. A hibrid médiarendszer logikája szerint a politikai hatás ma nem egyetlen csatornán, hanem az egymásba fonódó csatornák dinamikáján keresztül jön létre: a hagyományos média és a digitális platformok egymást idézik, egymást legitimálják, és ezzel gyorsítják a keretezés rögzülését.[224] Az orosz médiarendszer infrastrukturális alapját a VGTRK állami médiaholding (Rosszija 1, Rosszija 24, RTR-Planeta), a Gazprom-Media NTV-csatornája és az RT/Sputnik külföldi terjesztési hálózata képezi, amelyek együttesen mintegy 250 millió nézőt érnek el – ez a koncentrált struktúra biztosítja a csatorna-szinkronizáció fizikai hátterét.[225]

---

[223] MUMFORD, Andrew: *Ambiguity in hybrid warfare*. Hybrid CoE Strategic Analysis 24, Helsinki, 2020, 3–6. o.

[224] CHADWICK, Andrew: *The Hybrid Media System: Politics and Power*. Oxford University Press, 2013, 1–18. o.

[225] HANLEY, Monika – KUZICHKIN, Andrey (2021): *Russian Media Landscape: Structures, Mechanisms, and Technologies of Information Operations*. NATO Strategic Communications Centre of Excellence, Riga. 18. o. A VGTRK állami médiaholding (Rosszija 1, Rosszija Kultura, Rosszija 24, RTR-Planeta) 250 milliós nézettségét, a

A NATO StratCom COE 2015-ös időkerete (Vilnius 2013 → Krím 2014) azért használható itt, mert már a vizsgálati ablak kijelölésével is azt jelzi: a kommunikációs és nem-katonai komponensek nem „utólag" érkeznek, hanem a válságfolyamat részeként futnak. A csatorna-szinkronizációt ezért úgy kódolom, hogy a televíziós-hírügynökségi állítások az online térben megerősítést kapnak (civil hang, helyi hang, „szemtanú" hang), miközben az online térből visszacsatolás történik a hagyományos médiába („a közösségi média is ezt mondja"). Ennek a mechanizmusnak a leíró, korai „labor" változatát a NATO StratCom COE 2016-os, a trollolást hibrid eszközként vizsgáló lettországi esettanulmánya is megfoghatóvá teszi: a közösségi média felületei a valóságérzékelés és a bizalom elterelésének terévé válnak, és a komment-/profil-műveletek nem elszigetelt jelenségek, hanem műveleti funkciót töltenek be.[226]

A csatorna-szinkronizációs szempontból ugyanakkor fontos megállapítani: Krím 2014-ben a platform-szabályozási és transzparencia eszközök még kifejezetten kezdetlegesek voltak, ezért a csatornák közti „bizonyítás" (validáció) sokszor a látszat-hitelességre épülhetett. Ez a későbbi MRM-elemzésben (kontroll-leltár) lesz döntő, de a helyzetdimenzióban már most rögzítendő háttérfeltétel.[227]

A kibertér és az információs hadviselés szinkronizációját a NATO StratCom COE 2016-os jelentése esemény-rekonstrukciós módszerrel, nyílt forrású incidens-elemzések alapján dokumentálja. A Victoria Nuland és az amerikai nagykövet közötti, valamint a Catherine Ashton EU-külügyi főképviselő és az észt külügyminiszter közötti telefonbeszélgetés kiszivárogtatása kettős célt szolgált: egyfelől a nyugati kommunikációs vonalak sebezhetőségét demonstrálta, másfelől –a reflexív kontroll logikájával – a nyugati vezetők megosztását célozta. Párhuzamosan az Ukrtelekom infrastruktúrájába behatoló fegyveresek a teljes krími kommunikáció összeomlását okozták, majd a Cyber Berkut nevű csoportosulás az ukrán kormányzati weboldalakat, a NATO CCDCOE-t és magát a NATO-t is támadta. A fizikai infrastruktúra-bénítás, az információs

Gazprom-Media NTV-csatornáján keresztüli befolyását és az orosz médiarendszer centralizált struktúráját dokumentálja.

226 SVETOKA, Sanda (szerk.) et al. (2016): *Internet Trolling as a Tool of Hybrid Warfare: The Case of Latvia*. NATO Strategic Communications Centre of Excellence, Riga. 5–12., 18–22. o.

227 LANGE-IONATAMIŠVILI, Sanda és mtsai: *Analysis of Russia's Information Campaign against Ukraine*. NATO StratCom COE (NATO Strategic Communications Centre of Excellence), Riga, 2015, 3., 7–8., 12–15. o.

kiszivárogtatás és a kibertámadás egyidejűsége pontosan a disszertáció G–M–T–V láncának Terjesztés (T) dimenzióját operacionalizálja: a több csatornán egyidejűleg végrehajtott műveletek a védekező fél információs terét szimultán szűkítik.[228]

4.2.3. Volumen és amplifikáció: „kézi vezérlésű” hálózati hangosítás és korai troll-kapacitás

A 2014-es időszakban a volument nem algoritmikus szintetikus tartalomgyártás, hanem elsősorban emberi erőforrás-alapú amplifikáció adta. A lényeg itt nem az, hogy mennyire fejlett volt a technológia, hanem hogy a hálózati logika már működött: az üzenetek ismétlése, sokszorosítása, a viták eltérítése, az ellenhangok elnyomása, és a „közvélemény-látszat” előállítása olyan módon, hogy az a platformok akkori detektálási korlátai mellett is képes legyen teret nyerni.[229] Petykó Márton az öncélú trollkodás kommunikációs identitásgyakorlatait elemezte magyar politikai blogok diskurzusaiban; a stratégiai, fizetett trollkodás ettől elkülönülő jelenség.[230]

Az IRA-előzmények ebben a fejezetben nem Krím-helyettesítő bizonyítékok, hanem képesség-teszt: azt jelzik, hogy a 2013 körüli időszakban már jelen van egy olyan szervezett végrehajtói infrastruktúra, amely később mérhetően skálázódik. Az Oxfordi Egyetemhez kötődő (computational propaganda jellegű) feldolgozás a platformok közti idősoros mintázatokkal támasztja alá, hogy az IRA-hoz köthető aktivitások korai szakaszai már 2013 körül megjelennek, és később felfutnak.[231] Ezt a krími esettanulmányban úgy használom, hogy egyértelműen rögzítem: a „kézi vezérlésű” korszak nem azt jelenti, hogy „nem volt hálózat”, hanem azt, hogy a hálózat emberi munkával volt fenntartva és működtetve.

A volument tovább erősíti az a működésmód, amit a „Firehose of Falsehood” modell fogalmaz meg: nagy volumen, gyors ismétlés, többcsatornás szórás és az objektív valóság iránti elkötelezettség hiánya. Ez a logika a „Helyzet” dimenzióban azért fontos, mert a bemeneti oldalon

---

[228] NATO STRATCOM COE (2016): Analysis of Russia’s Information Campaign against Ukraine. NATO Strategic Communications Centre of Excellence, Riga. 29. o.

[229] SVETOKA, Sanda (szerk.) et al. (2016): *Internet Trolling as a Tool of Hybrid Warfare: The Case of Latvia*. NATO Strategic Communications Centre of Excellence, Riga. 5–12., 18–22. o.

[230] PETYKÓ Márton (2013): Az internetes troll mint identitás kialakítása politikai blogok diskurzusaiban. *Magyar Nyelvőr*, 137(3). 274–313. o. Online: https://real.mtak.hu/9008/1/137303.pdf

[231] Oxford University / Computational Propaganda Project: *The IRA, Social Media and Political Polarization in…* (feltöltött PDF), 3–5., 9., 20–21. o.

nem egy állítást kell cáfolni, hanem a rendszer működésmódját kell felismerni: a cél nem meggyőzés, hanem túlterhelés és keretezési dominancia.[232]

A krími annektálás Helyzet-dimenziója azért működött hatékonyan, mert a narratív keretet fegyelmezetten, összehangoltan terjesztették volt, a csatornák egymást erősítették, és a volumen kézi vezérléssel is elegendő volt ahhoz, hogy a célpont döntési környezetében bizonytalanságot termeljen. A következő alfejezet (4.3 – Előrejelzés) azt fogja megmutatni, hogy ez a helyzetkép miért nem állt össze időben riasztássá, és miért vált a krími eset akorai riasztás szempontjából „wicked problem"-má, azaz "megoldhatatlan problémává".[233],[234]

A trollgyár működésének első kézből származó leírását Ludmila Savcsuk, a szentpétervári Internet Research Agency volt alkalmazottja adta. Chen 2015-ban a New York Times Magazine számára készített riportot, amelyet Thomas 2016-ban belső informátori beszámolóként dolgoz fel. Savcsuk leírása szerint a trollok feladatai közé tartozott Porosenko ukrán elnök lejáratása, optimista kommentárok írása az orosz pénzügyi válságról, és Borisz Nyemcov meggyilkolásának ellenzéki összeesküvésként való bekeretezése. A tartalom párhuzamosan ment a VKontaktera, LiveJournalra, Twitterre, Instagramra és az orosz hírportálok kommentszekcióiba – a párhuzamos platform-használat a centralizált narratíva-vezérlés korai bizonyítéka. Savcsuk bírósághoz fordult és nyert; emberi jogi aktivisták értékelése szerint a fő eredmény „egy hivatalosan megszerezett céges dosszié, a tevékenység nyilvánosságra kerülése" volt. Ez a kvalitatív primérforrás azért releváns, mert a trollgyár működését nem külső megfigyelésből, hanem a szervezet belső logikájának rekonstrukciójából érthetjük meg.[235] A vonatkozó 8. táblázat: Helyzet-dimenzió összegző táblázat – Krím 2014 címmel a mellékletben található. A vonatkozó 9. táblázat: FMK-

[232] PAUL, Christopher – MATTHEWS, Miriam: *The Russian "Firehose of Falsehood" Propaganda Model*. RAND Corporation, 2016, 1–7. o.

[233] CULLEN, Patrick: *Hybrid threats as a new "wicked problem" for early warning*. Hybrid CoE (European Centre of Excellence for Countering Hybrid Threats), Strategic Analysis 8, 2018, 1–5., 7. o.

[234] RITTEL, Horst W. J. – WEBBER, Melvin M.: *Dilemmas in a General Theory of Planning*. Policy Sciences, 4(2), 1973, 155–169. o.

[235] CHEN, Adrian (2015): The Agency. In: New York Times Magazine, 2015. június 7. Ismertetése: THOMAS, Timothy L. (2016) i. m. 13. o.

rács / FMK-mátrix – a Helyzet-dimenzió operacionalizálása, Krím 2014 címmel a mellékletben található.

4.3. Előrejelzés-dimenzió (Forecast): Folyamatdinamika és az adaptációs aszimmetria

A 4.2-ben rögzített Helyzet-dimenzió nem önmagáért volt fontos, hanem azért, mert ebből kellene időben előállnia annak, amit a gyakorlat riasztásnak, a kutatás pedig előrejelzésnek (forecast/early warning) nevez. Egy olyan, kellő bizonyosságú besorolásnak, amelyre a döntéshozó lánc legitim és arányos válaszlépést tud építeni. A krími esetben a stratégiai meglepetés lényege épp az, hogy ez a besorolás nem állt össze időben. Nem a jelek hiányoztak, hanem a jelek értelmezése és a besorolás jogi–politikai küszöbe vált bizonytalanná.[236]

Az E-dimenziót ezért nem eseménysorként, hanem riasztáslogikaként írom meg. A riasztáslogika három kérdésre vezethető vissza: (1) Mit látunk? – vagyis mi a kategória (belső válság, helyi rendészeti epizód, proxy-művelet, állami agresszió). (2) Mekkora a tévedés kockázata? – vagyis mi a politikai/jogi ára annak, ha tévesen riasztunk. (3) Milyen bizonyossági szinten tudunk állítani? – vagyis mi az, ami valószínűsíthető és mi az, ami csak utólag bizonyítható. A krími konfiguráció egyik fő erőforrása az volt, hogy ezt a három kérdést szándékosan összekeverte: több legitim olvasatot kínált, közben pedig időt nyert a művelet fizikai konszolidációjához.[237]

A fejezet végén az E-dimenziót két kimenetben rögzítem: egy E-táblában (kódolható, rövid összefoglaló) és egy OxIPO-fordításban, ahol az előrejelzési kudarcot a feldolgozási (Process) szűkületekhez kötöm. Fontos hangsúly: az OxIPO itt nem „külön fejezet”, hanem az E-dimenzió kötelező operacionalizálása: ha a rendszer nem jelzett időben, akkor meg kell tudni nevezni, hol tört meg a feldolgozás folyamata a bemenettől a kimenetig (ld. 2.5 alfejezet).

4.3.1. Besorolási csapda: amikor a fenyegetés szándékosan „félreolvasható”

A krími esetben a legelső előrejelzési probléma a kategória volt. Egy klasszikus katonai mozgásnál a jelrendszer viszonylag stabil: csapatösszevonás, jelzett egységek, formális nyilatkozatok,

---

[236] CULLEN, Patrick: *Hybrid threats as a new “wicked problem” for early warning*. Hybrid CoE (European Centre of Excellence for Countering Hybrid Threats), Strategic Analysis 8, 2018, 2018, 1., 2., 4., 5., 7. o.

[237] MUMFORD, Andrew: *Ambiguity in hybrid warfare*. Hybrid CoE Strategic Analysis 24, Helsinki, 2020, 3., 4., 5., 6. o.

hadműveleti mintázatok. A krími konfiguráció ezzel szemben olyan jelenségeket termelt, amelyek mind külön-külön magyarázhatók voltak „alacsonyabb szintű” eseményként: belpolitikai válság, rendészeti krízis, helyi milícia-mozgás, „önvédelem”, zavargás. Az E-dimenzió csődje itt nem információhiány, hanem típusosítási kudarc: a rendszer nem tudta egyértelműen megmondani, hogy amit lát, az melyik kategóriába tartozik, és ez a döntési láncban természetes módon óvatosságot és késleltetést szül.

Ennek a csapdának a lényegi oka, hogy a hibrid fenyegetés – különösen a krími prototípus – nem egyetlen dimenzión fut. A NATO StratCom COE elemzéseinek egyik erőssége, hogy már a vizsgált időablak kijelölésével (Vilnius 2013 → Krím 2014) azt üzeni: a válságot nem lehet tisztán katonai eseményként kezelni, mert a nem-katonai (hibrid műveleti, illetve stratégiai kommunikációs) komponensek a folyamat részei, nem utólagos „zajok”. Ez az előrejelzés nyelvén azt jelenti, hogy a klasszikus riasztási rutinok (amelyek a katonai dimenzióhoz vannak kalibrálva) később kapcsolnak, és több időt töltenek a besorolással.

A besorolási csapda harmadik eleme a reakciókockázat. A riasztás nem semleges aktus: ha valamit idő előtt „állami agressziónak” minősítek, akkor politikai és jogi válaszlépéseket indítok el, amelyeknek költsége van; ha pedig későn minősítek, akkor kész tényekkel találkozom. A „wicked problem” logika pontosan ezt írja le: nincs egyértelmű „kész állapot”, a riasztás sikeressége utólag sem mérhető könnyen, és az értelmezés normatív vitákkal terhelt.[238]

4.3.2. A kiszámított többértelműség: előrejelzés-rombolás mint műveleti technika

A besorolási csapda nem puszta elemzői hiba, hanem a krími konfigurációban műveleti eszköz. A kiszámított többértelműség (calculated ambiguity) logikája szerint a bizonytalanság felhője nem azért jön létre, mert a támadó „nem tudja pontosan”, mit csinál, hanem azért, mert a bizonytalanság maga termeli ki a legnagyobb időelőnyt: amíg a célpont és a külső szereplők azon vitatkoznak, hogy mit látnak, addig a művelet fizikai konszolidációja megtörténik. Mumford ezt a krími mintánál kifejezetten reakció-blokkoló mechanizmusként írja le: a cél nem feltétlen a rejtés, hanem a legitim válasz megakasztása.

[238] RITTEL, Horst W. J. – WEBBER, Melvin M.: *Dilemmas in a General Theory of Planning*. Policy Sciences, 4(2), 1973, 155., 156., 160–162., 167–169. o.

Az E-dimenzióban ennek a következménye úgy fogalmazható meg: a riasztás küszöbe megemelkedik, mert a riasztásnak „bizonyosságot” kellene felmutatnia, miközben a támadó épp a bizonyosság ellen dolgozik. Itt válik a 4. fejezet logikája didaktikusan is érthetővé: a krími stratégiai meglepetés nem egyszerűen gyorsaság volt, hanem időtermelés. Az időtermelés nem technológiai eredmény, hanem szervezeti-műveleti fogás: a többértelműség fenntartása, amelyben a célpont számára minden „túl erős” reakció túllövésnek, minden „túl gyenge” reakció pedig tehetetlenségnek látszik.

A kiszámított többértelműség azért különösen fontos a disszertációs keretemben, mert itt kapcsolódik össze a H–E–I és az OxIPO. E-ként ez a „miért nem jelzett” kérdés; OxIPO-ként pedig az, hogy a feldolgozás (Process) szakaszban a rendszer nem tudja gyorsan stabilizálni a kategóriát, ezért késlelteti a döntést. A krími mintázatban tehát az előrejelzés nem egyszerűen „tudás”, hanem a feldolgozás sebessége és a kategóriarögzítés képessége.

4.3.3. Jel–zaj és csatorna-időzítés: miért nem áll össze a kép időben?

A besorolási csapdát tovább erősíti a jel–zaj arány romlása. Krímnél az előrejelzés azért sérül, mert nem egyetlen hamis állítás vagy egyetlen esemény terheli a rendszert, hanem egy működésmód: többcsatornás kommunikáció, nagy volumen, gyors ismétlés, és a koherens keret fenntartása akkor is, ha az állítások részben ellentmondóak. A NATO StratCom COE nem-katonai fókusza ebben az összefüggésben azt jelenti: a helyzetkép nem csak katonai szenzorokból áll össze, hanem médiából, nyilatkozatokból, online térből – vagyis a jelrendszer sokkal zajosabb.

A „Firehose of Falsehood” modell ebben a fejezetben azért hasznos, mert megfoghatóvá teszi: a volumen és a sebesség nem pusztán kommunikációs sajátosság, hanem előrejelzési ellenszer. A rendszer riasztás-képessége hagyományosan úgy működik, hogy azonosít egy jelenséget, majd egyre nagyobb bizonyossággal besorolja. A firehose-módban viszont a cél az, hogy a besorolás soha ne stabilizálódjon: a befogadó és az elemző egyszerre túl sok, egymást keresztező jelzéssel találkozik, és a rendszer védekező reflexe gyakran a „várjunk még egy megerősítést” lesz.[239]

[239] PAUL, Christopher – MATTHEWS, Miriam: *The Russian “Firehose of Falsehood” Propaganda Model*. RAND Corporation, 2016, 1–7. o.

Ebből egy operatív következtetés adódik: a krími stratégiai meglepetés nem az információs hiányon, hanem az információs túlterhelésen keresztül termelte ki a késleltetést. A H-dimenzióban rögzített csatorna-szinkron és narratív keret itt E-dimenzióvá fordul: ugyanaz a jelenség, amely a helyzetben „műveleti terméknek" látszott, az előrejelzésben detektálási csapdává válik.

4.3.4. Bizonyíthatóság és idő: mi az, ami csak utólag válik auditálhatóvá?

Az E-dimenzió egyik legfontosabb tanulsága, hogy egy küszöb alatti műveletnél a bizonyíthatóság időigényes. Ez a fenyegetés szerkezetéből következő tény: ha a támadó a letagadhatóságot választja, akkor a bizonyítás sokszor csak evidencialáncokból (idővonal-rekonstrukció, nyílt forrású nyomok, kiszivárgott dokumentumok, intézményi elemzések) áll össze. A Bellingcat MH17-anyaga módszertani mintát ad arra, hogyan lehet nyílt forrásokból (vizuális bizonyítékok, geolokáció, időrend) auditálható láncot építeni.[240]

A Szurkov-leakek feldolgozása (RUSI és a DFRLab) ugyanezt a logikát egy másik oldalról erősíti: nem egyetlen „döntő dokumentumot" keres, hanem azt vizsgálja, hogy a belső koordináció és irányítás milyen nyomokat hagy, és ezek hogyan kapcsolhatók össze a műveleti eseményekkel. E-dimenzióban ennek az üzenete az, hogy a riasztás és a bizonyítás nem ugyanaz: lehet olyan helyzet, ahol riasztani kellene, de a bizonyítási standard még nem teljes; és lehet olyan, ahol a bizonyítás utólag már erős, de a reakció ideje elmúlt.[241],[242]

Ez a pont a 4. fejezet bevezetőjével összhangban módszertani állítás is: a fejezetben a trianguláció a krími konfiguráció elemzésének előfeltétele. A 4.3-ban ezért az előrejelzést úgy rögzítem, mint bizonyossági szintek közti mozgást: mi volt „sejthető", mi volt „valószínűsíthető", és mi volt csak „utólag bizonyítható". A fejezet későbbi, I-dimenziója (irányítás) itt fog majd ráépülni: a kontrollok (attribúció, válasz) nem tudnak működni, ha nincs minimális bizonyossági alap.

4.3.5. „Wicked problem" és korai riasztás: miért szerkezeti a kudarc?

---

[240] BELLINGCAT Investigation Team: *MH17 – The Open Source Evidence*. 2015, 1., 7., 10. o.

[241] SHANDRA, Alya – SEELY, Robert: *The Surkov Leaks: The Inner Workings of Russia's Hybrid War in Ukraine*. RUSI Occasional Paper, 2019, 1–4., 8–9., 16., 23. o.

[242] DFRLab (TOLER, Aric és tsai): *Breaking down the Surkov Leaks*. Atlantic Council, 2016, 1–3. o.

A “gonosz probléma”, vagyis „wicked problem” fogalma azért releváns itt, mert megakadályozza azt a leegyszerűsítést, hogy a krími meglepetés „figyelmetlenség” volt. Rittel és Webber eredeti fogalomhasználata arra mutat rá, hogy bizonyos problémák nem rendelkeznek egyértelmű lezárási ponttal; a beavatkozás maga visszahat a rendszerre; és az értelmezés normatív vitákkal terhelt. Ez akorai riasztás szempontjából azt jelenti, hogy a riasztás és a riasztás értékelése önmagában is problematikus: ha nem történt incidens, nem tudni biztosan, hogy a riasztás megelőzte a kárt, vagy eleve téves volt.

Cullen ezt a logikát közvetlenül a hibrid fenyegetések korai előrejelzésére alkalmazza, és a Krím utáni korszakot fordulópontként kezeli: a béke–háború határ elmosása, a küszöb alatti működés szándékos kialakítása, a csatornák és a narratívák többdimenziós használata mind olyan tényezők, amelyek az early warning rendszereket „gonosz problémával” terhelik. Vagyis nem arról van szó, hogy „nem volt jel”, hanem arról, hogy a jel nem klasszikus, és a válasz küszöbe vitatott.[243]

Ez ebben az alfejezetben azért kulcsfontosságú, mert ezzel az E-dimenzió nem csak technikai, hanem intézményi logikává válik: a döntéshozó láncok és az előrejelző rendszerek egy olyan térben működnek, ahol a riasztás politikai aktus is. A krími meglepetés mechanizmusa így nem pusztán információs jelenség, hanem kormányzási és legitimitási csapda – és ez készíti elő a 4.4 (Irányítás) dimenziót.

A vonatkozó 10. táblázat: Előrejelzés-tábla és OxIPO-összegzés – Krím 2014 címmel a mellékletben található.

4.3.7. OxIPO-modell (E-ből levezetve): hol tört el a feldolgozás?

Az előrejelzési kudarc a krími konfigurációban végső soron nem „vakság”, hanem feldolgozási szűkület. OxIPO-nyelvre fordítva: (1) a bemenet egyszerre túl sok és túl vitatott, (2) a feldolgozás a besorolásban késik, (3) a kimenet késői és megosztott riasztás/reakció lesz. Ez a modell azért

[243] CULLEN, Patrick: *Hybrid threats as a new “wicked problem” for early warning*. Hybrid CoE (European Centre of Excellence for Countering Hybrid Threats), Strategic Analysis 8, 2018, 2018, 1., 2., 4., 5., 7. o.

illeszkedik az E-dimenzió végére, mert az előrejelzés nem önmagában áll, hanem a feldolgozás sebességében és minőségében dől el.[244]

A bemenet (Input) a krími esetben nem csupán információk halmaza, hanem keretezett, többcsatornás ingerár, amelyben a jel–zaj arány romlik, és a „műveleti termék" sokféle csomagolásban jelenik meg. A feldolgozás (Process) ott törik meg, hogy a kategóriarögzítés nem stabil: a többértelműség fenntartása miatt a döntési lánc verifikációs köröket fut, és mindeközben a reakció küszöbét a normatív vita (mit szabad?) is emeli. A kimenet (Output) pedig a késleltetett vagy vitatott reakció, ami a támadó számára időnyereséget ad a művelet fizikai és legitimációs lezárásához.

B) OxIPO-összegzés az Előrejelzés-dimenzióhoz:

- Input – A jelenség egyszerre "túl sok" és "túl vitatott".
- Process – A többértelműség reakció-blokkoló eszközzé válik.
- Output - Az előrejelzés késik; a válasz legitimációja széttart

A 4.3 összegző tétele így kimondható: a krími stratégiai meglepetés az E-dimenzióban riasztáslogikai csapda volt, amelyet a támadó a besorolás, a jel–zaj és a bizonyíthatóság időzítésének manipulálásával termelt ki. A következő alfejezet (4.4) az Irányítás dimenzióban fogja rögzíteni, hogy az attribúció és a legitim válasz miért akadt el, és hogyan készíthető elő a Krím 2014 sarokpontjára a kontroll-leltár (MRM) táblázatos rögzítése.

4.4. Irányítás-dimenzió (Control): A művelet kimenete és a védekezés hiányosságai

A 4.4 kiindulópontja egyszerű, de nem megkerülhető: a krími meglepetés nem akkor vált teljessé, amikor a művelet mivolta világossá vált, hanem akkor, amikor a helyzetre nem született időben olyan válasz, amely egyszerre volt legitim, arányos és végrehajtható. Az I-dimenzió ezért nem utólagos moralizálás, hanem a döntési lánc realitása. Mi az, amit 2014-ben ténylegesen meg lehetett volna lépni, és mi az, ami a besorolási bizonytalanság, a jogi küszöbök és a koordinációs hiányok miatt elakadt? A krími mintázatnál a kiszámított többértelműség pontosan erre játszott: a

[244] MUMFORD, Andrew: Ambiguity in hybrid warfare. Hybrid CoE Strategic Analysis 24, Helsinki, 2020, 3., 4., 5., 6. o.

bizonytalanságot úgy termelte, hogy közben a legitim válasz költségét és kockázatát is megemelte.[245]

4.4.1. Attribúciós és bizonyossági küszöb

Az irányítás első nehézsége az ok-okozatiság. Hiszen mitől mondható ki állami agresszióként egy olyan művelet, amely a végrehajtásban jelzés nélküli, helyinek álcázott, többcsatornás és jogilag vitatható formákat használ? Itt érdemes megállapítani és kimondani az I-dimenzió kellemetlen szabályát. A válasz mindig egy bizonyossági küszöb fölött lesz legitim, a küszöböt viszont a támadó épp azzal tolja el, hogy a bizonyosság megállapítását időigényessé teszi. A krími esetben ez a logika már gyakorlat, mert az kétértelműség a kategóriarögzítés idejét növeli, miközben a fizikai konszolidáció halad.

Ezt a nehézséget két forrástípus tudja jól demonstrálni a fejezetben, triangulációval. Az egyik az OSINT-evidencialánc: lényege, hogy a Bellingcat az MH17-ügyben nem egyetlen döntő dokumentumra támaszkodik, hanem sok apró, egymást erősítő nyílt forrású nyomot (fotókat/videókat, közösségi médiás posztokat, műholdképeket, helyszín- és időazonosítást) időrendbe rendez, és ebből állít össze egy ellenőrizhető, lépésről lépésre visszakövethető bizonyítási láncot. Ennek a krími esettanulmányban az a relevanciája, hogy megmutatja: a letagadhatóságra építő műveleti térben a bizonyítás sokszor nem papírból, hanem nyomokból épül fel – és a bizonyosságot épp a több, egymástól független forrás egybeesése adja.[246] A másik a kiszivárgás-alapú belső koordináció: a Szurkov-leakek intézményi feldolgozása megmutatta, hogy a belső irányítás és a politikai-technológiai koordináció milyen nyomokat hagy dokumentum-alapon, és hogyan tehető ez visszacsatolhatóvá az eseményláncra.[247]

A fejezet szempontjából a következtetés: 2014-ben az irányítási (I) probléma egyik része nem akarathiány, hanem bizonyíthatósági időzítés. A válasz akkor legitim, ha az attribúció és a

[245] MUMFORD, Andrew: *Ambiguity in hybrid warfare*. Hybrid CoE Strategic Analysis 24, Helsinki, 2020, **3–6. o.**

[246] BELLINGCAT Investigation Team: *MH17 – The Open Source Evidence*. 2015, **1., 7., 10., 21–23. o.**

[247] SHANDRA, Alya – SEELY, Robert: *The Surkov Leaks: The Inner Workings of Russia's Hybrid War in Ukraine*. RUSI Occasional Paper, 2019, **1–4., 8–9., 16., 23. o.**

helyzetbesorolás eléri a küszöböt – de a küszöb elérése időt igényel, és ezt az időt a támadó a kiszámított kétértelműség segítségével okozza.

Az attribúció rendszerszintű nehézségeit a NATO StratCom COE és a Hybrid CoE 2023-ban publikált közös tanulmánya foglalja össze a legtömörebben. A 2018 óta végzett 350-nél több koordinált manipulációs hálózat-levétel tapasztalatai alapján a szerzők megállapítják, hogy az attribúció következetesen „diszfunkcionális" maradt: a négyes lencserendszer (technikai, viselkedési, szervezeti, politikai bizonyítékok) alkalmazása nem vált egységes gyakorlattá, és a politikai attribúció önmagában nem helyettesítheti a jogi vagy technikai bizonyítékot.[248] A krími esetből levonható tanulság ezért nemcsak az, hogy a válasz késedelmes volt, hanem hogy az attribúciós kapacitás fejlesztése – a bizonyítékok rétegzett, többforrású összegyűjtése, amit az OSINT-evidencialánc módszertana lehetővé tesz – strukturális befektetést igényel. Az SCC-protokoll Irányítás-tengelye ezért nemcsak tartalomszintű válaszokat kell, hogy előírjon, hanem az attribúciós kapacitás intézményi feltételeinek megteremtését is.

4.4.2. Reakciókockázat és jogi-politikai küszöbök

Az irányítás második nehézsége a reakciókockázat: a korai, erős válasz túllövésnek is látszódhat, a késői válasz pedig már nem befolyásolja a helyzetet. Ebben a csapdában a döntéshozói láncok hajlamosak várni még egy megerősítést, ami Előrejelzés-dimenzióban előrejelzési késés, Irányítás-dimenzióban pedig kormányzási bénulás. A hibrid fenyegetések korai riasztás logikáját Cullen azért írja le makacs problémaként (wicked problem), mert a béke–háború határ elmosása és a küszöb alatti működés nem csak technikai, hanem normatív és politikai dilemmákat is teremt. Nem világos ugyanis, hogy mikor egzakt a probléma, és az értelmezés is eleve vitatott.[249]

A krími esetben ez a dilemma ráadásul nem későbbi tanulság, hanem a művelet működési módja volt. Ha a helyzetet belpolitikai krízisként vagy rendészeti epizódként nézzük, akkor a válasz csatornái mások (belső rend, közrend, politikai közvetítés). Ha viszont állami agressziónak

[248] NATO STRATCOM COE – HYBRID COE (2023): Attributing Information Influence Operations: Identifying those Responsible for Malicious Behaviour Online. NATO Strategic Communications Centre of Excellence, Riga. Executive Summary; 3–5. o.

[249] CULLEN, Patrick: *Hybrid threats as a new "wicked problem" for early warning*. Hybrid CoE Strategic Analysis 8, 2018, **1–5., 7. o.**

értelmezzük, akkor katonai és nemzetközi jogi válasz lép be. Az kétértelműség épp ezt a választást teszi kockázatossá: a rossz kategóriára adott válasz túllövésként értelmezhető, a jó kategóriára adott válasz viszont késve érkezik.

A NATO stratégiai keretrendszerét és konkrét szakpolitikai irányelveit jelölő dokumentumok[250], amelyeket a hibrid hadviselés elleni fellépésre hoztak létre, pontosan azt rögzítik, hogy 2014 után a hibrid fenyegetésekre adott válaszok intézményesítésre szorultak. Ez a fejezetben azért releváns, mert alátámasztja, hogy a Krím nem csak esemény, hanem képességfejlesztési kényszerítő. Vagyis a reakció nem egyetlen döntés, hanem több csatornán futó, több szereplőt érintő kormányzási folyamat. Ebből az következik, hogy a reakció sem merülhet ki abban, hogy egy kormány vagy szövetség dönt valahogyan. A válasz akkor működik, ha egyszerre több helyen történik beavatkozás – például a helyzet kommunikációs besorolása (mi történik?), a bizonyítékok rendezése (mit tudunk bizonyítani?), a közvélemény tájékoztatása (mit ért a társadalom?), és a nemzetközi legitimáció kezelése (mit lehet jogilag és politikailag megtenni), ráadásul mindezt több szereplő összehangoltan végzi (állami intézmények, katonai vezetés, diplomácia, média, szövetségi szervek). Vagyis a krími esetben a stratégiai meglepetés egyik oka az volt, hogy a támadó a kommunikációs térben gyorsabban és koherensebben mozgott, mint ahogy a védekező oldal képes volt a többcsatornás, több szereplős kormányzási folyamatot összehangolni és végrehajtani.

4.4.3. Koordináció és jóváhagyási lánc miatt nyerhetett időt a támadó

Az irányítás nehézsége a koordináció. A krími konfiguráció egyik operatív előnye az volt, hogy a végrehajtás a célpont oldalán bizonytalanságot, a külső oldalon pedig koordinációs kényszert termelt. Ha több szereplőnek kell ugyanarra a helyzetre reagálnia (ukrán állam, szövetségesek, nemzetközi szervezetek), akkor a válasz leglassúbb eleme határozza meg az időzítést. A tudatos kétértelműség így nemcsak a kategóriarögzítést késlelteti, hanem a jóváhagyási láncokat is. Mindenki a többiek besorolására vár, mert a rossz besorolás politikai költsége, vagyis kockázata magas.

Ezt a jelenséget a krími esetben különösen jól fel lehet tárni, mert a támadó oldalnak az időnyereség nem csak a katonai térben értelmezhető, hanem a legitimációs térben is. A késleltetett reakció

[250] NATO: NATO's response to hybrid threats. NATO Public Diplomacy Division, 2024.

közben a helyzet kész tények politikájává válik. A fizikai kontroll és a kommunikációs keret lezárja a vitát, mire a koordinált válasz összeállna.

A trianguláció itt azt jelenti, hogy a koordinációs nehézség nem egyetlen narratív forrásból van megerősítve, hanem: (i) a mechanizmust (calculated ambiguity) elméleti-operatív leírásból (Hybrid CoE), (ii) a bizonyíthatósági kényszert OSINT és leak-láncból (Bellingcat, RUSI), (iii) a válság nem-katonai komponenseit intézményi elemzésből (NATO StratCom COE) vezetjük le. Ettől válik az Irányítás-dimenzió rekonstruált döntési logika bemutatásává.

4.4.4. 2014 mint sarokpont: mit lehetett ténylegesen csinálni, és mi hiányzott?

A 2014-es kiindulási pont úgy kezelhető korrekt módon, ha nem visszavetítjük a későbbi (DSA, DISARM stb.) megoldásokat, hanem kimondjuk, hogy 2014-ben az irányítási tér szűk volt, és sok kontroll csak csírájában létezett. Ugyanakkor nem volt teljes kontrollvákuum. A bizonyítási fegyelem (OSINT), a stratégiai kommunikációs elemzések, és a későbbi intézményi tanulás irányába mutató első reakciók már ekkor megjelentek. A NATO „Response to hybrid threats” típusú dokumentumai pontosan azt rögzítik, hogy 2014 után a hibrid fenyegetésekre adott válaszok intézményesítésre szorultak; ez a fejezetben azért releváns, mert alátámasztja: a Krím nem csak esemény, hanem képességfejlesztési kényszerítő.

A fejezetben ezt a sarokpont-logikát később az MRM-táblában fogom rögzíteni (4.5): mi volt a 2014-es kontroll-leltár (akár hiányként), és mely kontrollok váltak később standarddá. Itt, a 4.4 végén elég kimondani: az irányítási dimenzióban a krími meglepetés egyik lényege, hogy a válaszhoz szükséges három feltétel (besorolás, bizonyíthatóság, koordináció) nem állt össze időben – és ezt a támadó oldal műveleti technikaként használta. A vonatkozó 11. táblázat: Irányítás (I) összegző táblázat – Krím 2014 sarokpont címmel a mellékletben található.

4.5. MULTIMODÁLIS REZILIENCIA MÁTRIX (MRM): 2014-es kontroll-leltár sarokpontként (és ebből mi következik)

A 4.5 célja nem az, hogy 2014-re visszavetítsem a későbbi, kiforrott reziliencia- és platformkormányzási megoldásokat, hanem hogy kontroll-leltárt készítsek: 2014-ben mi állt rendelkezésre, mi hiányzott látványosan, és milyen kontrollok épültek ki később a Krím tanulságaként. Ezt azért kell táblázatosan rögzíteni, mert így válik a Krím 2014 valódi sarokponttá: nem „a múlt”, hanem a későbbi időszakokhoz viszonyítási pont.

Az MRM logikája egyszerű: a kontrollok több szinten működnek, és akkor hatékonyak, ha összeérnek. A krími eset tanulsága, hogy 2014-ben a kontrollok jelentős része széttartott: voltak bizonyítási és elemzési kapacitások (OSINT, intézményi elemzések), de nem volt egységes, gyors, közösen elfogadott „SSOT" jellegű helyzetkép; voltak jogi és politikai eszközök, de a küszöb-alatti működésre kevés volt a jól gyakorolt válaszrutin; voltak társadalmi ellenállóképességi elemek, de ezek nem voltak rendszerszintűvé emelve.

A 4.5 táblázatban ezért a kontrollokat három rétegben rögzítem (makro–mezo–mikro), és minden sorban jelzem: 2014-ben ez a kontroll (a) hiányzott, (b) csíraszinten létezett, vagy (c) már működött, de korlátozottan. A cél az, hogy a későbbi fejezetekben (Híd 2014–2021; 2022–2025) már ne „új találmányként" jelenjen meg a reziliencia, hanem mint kényszerített intézményi tanulás.

A vonatkozó 12. táblázat: MRM-tábla (kontroll-leltár) – Krím 2014 sarokpont címmel a mellékletben található.

4.5.2. A G–M–T–V lánc 2014-es sarokpont-konfigurációja

Az MRM kontroll-leltár mellett szükséges a 2014-es krími műveletet a G–M–T–V műveleti lánc (ld. 2.4.4) keretében is rögzíteni, mert az 5. fejezet (Híd-időszak) és a 6. fejezet (2022–2025) eltolódásai ehhez a kiindulóponthoz viszonyítanak.

A 2014-es konfiguráció a G–M–T–V lánc szempontjából a következőképpen jellemezhető:

G (Generálás) – alacsony, kézműves. A tartalomvariánsok előállítása manuális: az Internet Research Agency (IRA) trolljai egyenként írtak posztokat, a koordináció személyes irányításon alapult. A szöveges tartalom dominált; kép- és videómanipuláció ritka, és amikor előfordult, alacsony technikai színvonalú volt. A generálási költség személyenként magas, a skálázhatóság korlátozott.[251]

M (Mosás) – primitív, de a kontextusban hatékony. A forrás- és kontextus-mosás egyszerű álprofilokra és a megszállt területekről érkező „civil tanúk" felhasználására korlátozódott. A hatékonyság nem a mosási technika kifinomultságából, hanem a fogadó közeg

[251] LANGE-IONATAMIŠVILI, Sanda et al.: Analysis of Russia's Information Campaign against Ukraine. NATO StratCom COE, Riga, 2015, 3., 7–8., 12–15. o.

felkészületlenségéből fakadt: sem a nyugati média, sem a platformok nem rendelkeztek CIB-detekciós (Coordinated Inauthentic Behaviour) eljárásrenddel.

T (Terítés) – közepes, koordinált humán hálózatokon alapuló. A terjesztés fő csatornái az orosz állami média (RT, Sputnik), a koordinált közösségimédia-fiókcsoportok és az ukrán médiakörnyezetbe beékelődő orosz nyelvű portálok voltak. Az algoritmikus amplifikáció még nem játszott meghatározó szerepet; a terítés erejét a szinkronizált cross-platform jelenlét és a hibrid médiarendszer (állami média → közösségi média → visszahivatkozás) biztosította.

V (Validálás) – a támadó számára magas, a védekező számára nulla. Ez a dimenzió a krími konfiguráció legfontosabb sajátossága. A meglepetés-faktor miatt az ellen-validálás gyakorlatilag nem létezett: nem volt szisztematikus OSINT-infrastruktúra (a 2014-es krími műveletet követő hónapokban alapult a Bellingcat és vált gyorsan a nyílt forrású vizsgálatok referenciaszervezetévé), nem volt pre-bunking, és a platformok nem végeztek transzparencia-jelentéseket. A támadó validálása ezzel szemben sikeresen működött: a „helyi lakosság védelme” és a „népszavazás” keretezés elegendő bizonyíték-érzetet keltett ahhoz, hogy a narratíva megragadjon.[5][11][15]

Ez a konfiguráció a kiindulópont, amelyhez az 5. fejezet Anchor-mérföldkövei (a támadói lánc felértékelődése) és Reziliencia-mérföldkövei (a védekező ellen-validálás felépülése) mérik a változást.

5. AZ FMK-TRANSZFORMÁCIÓ VÁLTOZÓPONTJAI (2014–2021)

5.1. Bevezetés: A HÍD mint magyarázó változók összessége

A modern hadviselés történetében ritkán azonosítható olyan élesen elhatárolható átmeneti korszak, mint a 2014-es krími stratégiai meglepetés és a 2022-es ukrajnai teljes körű invázió közötti hét esztendő. Ez a periódus nem pusztán kronológiai átmenetet jelent a két esettanulmány között, hanem a fegyvernek minősülő kommunikáció (FMK) teljes műveleti láncának minőségi transzformációját foglalja magában. A jelen fejezet ezért nem időrendi narratívaként, hanem magyarázó változócsomagként kezeli a 2014–2021 közötti időszakot: az SFC/SFÖ módszertannak megfelelően azt vizsgálja, hogy a két fő eset (Krím 2014 vs. Ukrajna 2022) között melyik műveleti láncszem vált erősebbé, gyorsabbá, olcsóbbá vagy éppen ellenállóbbá.

Mivel a Híd-időszak nem önálló SFÖ-esettanulmány, hanem a független változók transzformációs leírása, a H–E–I mátrix alkalmazása itt nem a szokásos diagnosztikai formában történik – a mérföldkövek rendszere a H–E–I dimenziókat közvetetten, a G–M–T–V láncszem-eltolódásokon keresztül ragadja meg.

A vizsgálat szervező kerete a G–M–T–V lánc, amely az FMK-műveletek négy kritikus szakaszát ragadja meg:

- G (Generálás / Generation): mennyire gyors és olcsó a tartalomvariánsok gyártása (szöveg, kép, hang, videó);
- M (Mosás / Laundering): mennyire hatékony a forrás- és kontextus-átöltés (ál-lokális, „oknyomozó", „szakértő", klónoldal, screenshot-dokumentum);
- T (Terítés / Distribution): mennyire skálázható és kontrollálható a terjesztés (algoritmus, hálózat, csoport, chat, fizetett/organikus mix);
- V (Validálás / Validation): mennyire könnyű hitelesítő réteget adni (civil tanú, riporter, tekintély-proxy, „bizonyíték-érzet"), illetve mennyire gyors az ellen-validálás (OSINT, tényellenőrzés).

A fejezet két pilléren nyugszik. Az első pillér a támadói képesség transzformációját tárgyaló Anchor-mérföldkövek: azok a technológiai, elméleti és műveleti ugráspontok, amelyek a G–M–T–V lánc egyes elemeit minőségileg megváltoztatták. A második pillér a védekezői válasz felépülését rögzítő Reziliencia-mérföldkövek: az intézményi, szabályozási, platform-transzparenciás és OSINT-alapú ellenlépések, amelyek a Híd alatt értek el kritikus tömeget. E két pillér együttese magyarázza, miért alakult fundamentálisan másként a 2022-es információs konfliktus, mint a 2014-es.

A fejezet összegzése közvetlenül a 6. fejezetbe (Ukrajna 2022–2025) vezet át: a Híd alatt felépült képességek – mind támadói, mind védekezői oldalon – a 2022-es invázió informális „előfeszítését" adták.

5.2. Mérföldkövek a fegyvernek minősülő kommunikáció képességének transzformációjában (2014–2021)

A Híd-időszak nem 2015. január 1-jén kezdődött. Már a 2014-es krími művelet lezárultát követő hónapokban – a Krím-annexiótól 2014 végéig – legalább három olyan esemény zajlott, amely önálló és dokumentálható hozzájárulást jelentett a fegyvernek minősülő kommunikáció (FMK) transzformációjához. Az MH17-es Boeing lelövése 2014. július 17-én hadtörténetileg az első nagyszabású „firehose of falsehood" kommunikáció-alkalmazásnak tekinthető: Moszkva nem egyetlen koherens narratívát bocsátott ki – mint a Krím-műveletnél –, hanem párhuzamosan, egymásnak ellentmondó tucat-verziót piacra dobott (ukrán vadászgép, ukrán BUK, CIA-provokáció, hamisított műholdfelvételek), megakadályozva, hogy a közvélemény egyetlen verzió körül kristályosodjon. Ez a taktikai innováció a G–M–T–V lánc M(osás)-dimenziójában jelent minőségi ugrást: a forrás nem egyszerűen elfedett, hanem a verziók megtöbbszörözésével maga a bizonyíthatóság vált kérdésessé. Párhuzamosan a donbaszi konfliktus 2014 április–decemberi szakasza az első tartósan fenntartott, hónapokon átívelő információs befolyásoló művelet (Information Influence Operations, IIO) demonstrálta – szemben a Krím precíz háromhetes operatív ablakával. Az Internetes Kutatási Ügynökség (IRA) 2014 nyarán exponenciálisan bővítette személyzetét és trollfarmi kapacitását – ezt a Savchuk-szivárogtatások és a Mueller-vizsgálat adatai egyaránt megerősítik –, és a Minszk I. tárgyalások (2014. szeptember) körüli narratív harc az első diplomatákat célzó információs befolyásoló műveletet dokumentálta. Ezért a fejezet a Híd-időszakot 2014–2021-re datálja: a kritikus transzformáció kronológiailag egyidős az annexiót követő hónapokkal.

Az anchor-mérföldkövek által dokumentált transzformációs ív nem egyedi megállapítás: Isabella Garcia-Camargo és Samantha Bradshaw a Hybrid CoE számára készített rendszerezésében kilenc globális dezinformációs trendet azonosítottak 2021-re vetítve, amelyek közül legalább hat – a zárt platformokra történő vándorlás, a nehezen verifikálható tartalom elterjedése, a belföldi szereplők bevonása, a mikrocélzás (micro-targeting), a percepciós feltörés (perception hack) és a

mélyhamisítás (deep fake) megjelenése – az alább tárgyalt anchor-mérföldkövekben empirikusan is kimutatható.[252]

5.2.1. Platform-architektúra és ajánlórendszer-logika felértékelődése

A 2014-es krími művelet még döntően koordinált emberi hálózatokra – trollfarmokra és médiaproxykra – támaszkodott a tartalom terjesztésében. A Híd-időszak legmélyrehatóbb strukturális változása az volt, hogy a terjesztés (D) elsődleges motorjává a közösségi platformok ajánló- és feedlogikája vált. Az algoritmus-alapú tartalomkiválasztás – amely a nézettségi időt, az engagement-mutatókat és a trendeket priorizálja – új műveleti terepet nyitott: a kampányok többé nem csupán tartalmat gyártottak, hanem formátumra optimalizáltak.

Bradshaw és szerzőtársai a Stanford Internet Observatory (SIO) keretében, az Election Integrity Partnership 2020-as elemzésében tíz kulcstrendet azonosítottak a dezinformáció 2016 és 2020 közötti evolúciójáról.[253] Megállapításaik szerint a legvirálisabb dezinformációs tartalmakat 2020-ban már nem bot-hálózatok, hanem valós, nagy követőbázissal rendelkező influencerek terjesztették felülről lefelé. A platformok üzleti modellje – amely a felhasználói elköteleződést jutalmazza – strukturálisan erősítette a polarizáló és érzelmileg telített tartalmakat, függetlenül azok valóságtartalmától. A dezinformációs narratívák nem egyetlen platformon, hanem többplatformos hálózatban terjedtek, ami megnehezítette a moderálást. Ez a megállapítás összhangban van a Hybrid CoE 2020-as[254] elemzésével, amely a digitális kommunikációs technológia „demokratizálódását” emelte ki: a magas minőségű vagy félprofi audiovizuális tartalom előállítása, a mesterséges intelligencia alkalmazása hírgyártásra, valamint a közösségi médián és élő közvetítéseken keresztüli gyors terjesztés bárki számára elérhetővé vált alapvető digitális készségek birtokában.

---

[252] GARCIA-CAMARGO, Isabella – BRADSHAW, Samantha (2021): Disinformation 2.0: Trends for 2021 and beyond. Hybrid CoE Working Paper 11. European Centre of Excellence for Countering Hybrid Threats, Helsinki. 10–23. o.

[253] Garcia-Camargo, Isabella – Bradshaw, Samantha (2021): *Disinformation 2.0: Trends for 2021 and beyond.* Helsinki: Hybrid CoE. (Hybrid CoE Working Paper 11.) 7., 11–12., 15., 21. o.

[254] Hybrid CoE (2020): *Trends in the Contemporary Information Environment.* Helsinki: Hybrid CoE. (Hybrid CoE Trend Report 4.) 19. o.

A G–M–T–V lánc szempontjából ez a változás a T→V felértékelődést eredményezte: a feed-skála önmagában validál, mert a láthatóság hitelesség-proxyvá válik. Amit a felhasználó sokszor lát a feedjében, azt hajlamos hitelesnek tekinteni – nem azért, mert ellenőrizte, hanem mert a platformlogika normalizálta. A 2014-es modellben a D főleg koordinált hálózat volt; a Híd végére a D már platformlogika, ahol a kampány „format-first" lett, és a validálás részben a feedben történt.

5.2.2. Nyílt - zárt csatornaváltás és a „láthatatlan terítés" normalizálódása

A Híd-időszak másik meghatározó strukturális változása a nyílt közösségi terek fokozatos elsötétülése volt. A 2014-es krími művelet még döntően nyílt platformokon zajlott – a VKontakte, a Facebook és a Twitter adta a fő hadszínteret. A 2014–2021 közötti periódusban azonban a zárt és félzárt csatornák – elsősorban a Telegram, a WhatsApp és a Discord – önálló műveleti térré váltak. A NATO StratCom COE (2021) feltérképezte a WhatsApp és Telegram manipulációs szolgáltatások nyílt piacát: tömeges üzenetküldő szoftver 26 EUR-tól beszerezhető, kontaktadatbázisok célközönség szerint szegmentáltan értékesíthetők, és mesterséges engagement-szolgáltatások (követővásárlás, nézettségnövelés) elérhetők.[255] – a manipulation-as-a-service piac globálisan szétszórt (India, Indonézia, USA).[256]

Az ISIS 2014–2016 közötti online toborzási tevékenysége szolgáltatta az egyik legkorábbi és legvilágosabb példát a nyílt→zárt csatorna-váltásra. A szervezet a nyílt közösségi médiát a figyelem megragadására használta (propaganda-videók, mártír-narratívák), majd a célszemélyeket zárt Telegram-csoportokba terelte a tényleges radikalizáció és az operatív koordináció céljából. Ez a minta precedenst teremtett: a nyílt tér a „kirakattérré", a zárt csatorna az „érlelő térré" vált.

---

[255] NATO STRATCOM COE (2018): *The Black Market for Social Media Manipulation*. NATO Strategic Communications Centre of Excellence, Riga. 15. o. A high-end szolgáltatók teljes kampánymenedzsmentet kínálnak; az Upwork platformon $1,50–$50/cikk áron toboroztak hiperpartizán híreket írókat, napi 10 cikk kvótával.

[256] BAY, Sebastian (szerk.) (2021): *Messaging Manipulation Services on Social Messaging Platforms*. NATO Strategic Communications Centre of Excellence, Riga. 12., 14–15. o. A tanulmány feltérképezi a WhatsApp és Telegram manipulációs szolgáltatások nyílt piacát: tömeges üzenetküldő szoftver 26 EUR-ért beszerezhető, SMM ügynökségek, freelancerek és API-szolgáltatók globálisan (India, Indonézia, USA) kínálnak célzott engagement-szolgáltatásokat. A manipulation-as-a-service piac a zárt üzenetküldő platformok sebezhetőségét iparosított formába önti.

A NATO StratCom COE Robotrolling 2023–2024 elemzése (2024) empirikusan bizonyította[257], hogy ez a tendencia tartóssá vált és ipari léptékre emelkedett. A kutatás 17 koordinált csoportot azonosított 344 forrás bevonásával, amelyek elsősorban a Telegramon és a Twitter(X)-en működtek. A csoportok 53%-a a Telegramon volt aktív, és ami különösen figyelemre méltó: a kutatók azt találták, hogy ezek a csoportok már nemcsak az orosz nyelvű térben terjeszkedtek, hanem aktívan építettek nemzeti közönségekre célzott befolyásolási hálózatokat – amerikai, francia, finn és más nyelvi célcsoportok számára.

A G–M–T–V lánc szempontjából a változás a T→V erősödése zárt térben: a terítés és a validálás összecsúszik, mert a „barát küldte" vagy a „csoportban láttam" mechanizmus önmagában hitelesít. Az ellen-validálás (tényellenőrzés, OSINT) ezeket a tereket csak korlátozottan éri el, ami a védekezői oldal számára strukturális hátrányt jelent.

5.2.3. Perszóna-ökonómia iparosodása: lopott identitás → portfólió-menedzsment

A 2014-es műveletekben a hamis profilok még viszonylag kezdetlegesek voltak: a szentpétervári Internet Research Agency (IRA) trolljai egyszerű álneveket, lopott profilképeket és sematikus biográfiákat használtak. A Híd-időszak alatt ez a gyakorlat ipari szintű perszóna-portfólió-menedzsmentté fejlődött.

A fordulópontot a 2016-os amerikai elnökválasztás körüli IRA-műveletek jelentették. Az Egyesült Államok Igazságügyi Minisztériuma által 2018 februárjában benyújtott vádirat (Mueller-vádirat) részletesen dokumentálta, hogy az IRA szervezeti struktúrát épített ki a perszóna-gazdálkodásra: a trollok „öregített" (hosszú ideje aktív) fiókokat kezeltek, szerepeket váltottak a hálózaton belül, és cross-platform tükrözést alkalmaztak – ugyanaz a perszóna megjelent Facebookon, Twitteren, Instagramon és YouTube-on is, koherens „élettörténettel". A Stanford Internet Observatory (2019) és a Graphika elemzői ezt „Secondary Infection" műveletként dokumentálták: egy 2014–2019 között működő, többplatformos dokumentum hamisítási hálózatot, amely hosszú életciklusú „burner" profilokat és fórum-/platform-terítést alkalmazott – a „fekete propaganda" standardizált mintázata.

[257] NATO Strategic Communications Centre of Excellence, *Virtual Manipulation Brief*, Riga: NATO StratCom COE, 2024. június, 7. o. ISBN: 978-9934-619-66-3. Elérhető: https://stratcomcoe.org

A Hybrid CoE Paper 27[258] – amely az orosz hibrid fenyegetésekben részt vevő nem-állami szereplők kézikönyveként készült – öt NSA-típust (Armed, Cyber, Propaganda/Disinformation, Social/Political, Economic/Financial) különböztet meg. A propaganda- és dezinformációs nem-állami szereplők (PDNSAs) kategóriájában a kézikönyv dokumentálja, hogy az IRA-t 2022 után a GRU fronszervezeteként működő Centre for Geopolitical Expertise (CGE) szervezte át, miközben a GRU 72. Különleges Szolgálati Központja (72nd Special Service Centre) proxy weboldalak és Telegram-hálózatok üzemeltetésével foglalkozik. Ez a szervezeti háttér bizonyítja, hogy a perszóna-gyártás már nem ad hoc tevékenység, hanem intézményesített képesség.

A G–M–T–V lánc szempontjából az eltolás M→V felértékelődés: a forrás (perszóna) lett a validálás hordozója, és a mosás a perszónán keresztül történik. A 2014-es modellben egy poszt volt a művelet egysége; a Híd végére a perszónák hálózata lett az egység.

5.2.4. Hack-and-leak + dokumentum-mimikri mint bizonyíték-hamisítási folyamat

A Híd-időszak egyik leghatásosabb taktikai innovációja a hack-and-leak műveletek csomagolásának kifinomulása volt. A nyers adattömeg – amelyet a 2014-es műveletek során még feldolgozatlanul dobtak ki a nyilvánosságba – önmagában kevésnek bizonyult: a döntő elem a csomagolás, az „oknyomozó” álcázás és az időzített terítés lett.

A 2017-es #MacronLeaks művelet jelentette e taktika érettségének legismertebb demonstrációját. A francia elnökválasztás második fordulója előtti utolsó órákban – amikor a francia választási törvények tiltják a kampánytevékenységet – ismeretlen forrásból nagy mennyiségű, a Macron-kampányhoz köthető dokumentumot szivárogtattak ki. Jean-Baptiste Jeangène Vilmer az Atlantic Council számára készített részletes utólagos elemzésében[259] dokumentálta, hogy a művelet célja nem feltétlenül a dokumentumok tartalma volt – amelyek nagyrészt ártalmatlan adminisztratív levelezést tartalmaztak –, hanem a „bizonyíték-érzet” megteremtése és a választási folyamat

[258] VOLĀNS, Eginhards et al. (2025): *Handbook on the Role of Non-State Actors in Russian Hybrid Threats.* Helsinki: European Centre of Excellence for Countering Hybrid Threats. (Hybrid CoE Paper 27.) 9–10., 51. o. Online: https://www.hybridcoe.fi/wp-content/uploads/2025/12/Hybrid-CoE-Paper-27-Handbook-on-the-role-of-non-state-actors-in-Russian-hybrid-threats.pdf

[259] Jeangène Vilmer, Jean-Baptiste (2019): *The „Macron Leaks" Operation: A Post-Mortem.* Washington, D.C.: Atlantic Council – IRSEM. Online: https://www.atlanticcouncil.org/wp-content/uploads/2019/06/The_Macron_Leaks_Operation-A_Post-Mortem.pdf

zavarása az időzítés révén. A Hybrid CoE Paper 24[260] is hivatkozik erre az esetre, mint a hack-and-leak logika demokratikus sérülékenységeket kihasználó archetipikus példájára.

Ugyanez a mintázat figyelhető meg a Secondary Infection műveletben (2014–2019), amelyet a DFRLab és a Graphika fedett fel 2019-ben.[261] A művelet dokumentum hamisítást alkalmazott: állítólagos belső leveleket, diplomáciai feljegyzéseket és szakértői anyagokat kreált, majd ezeket több száz platformon, fórumon és portálon terjesztette, „oknyomozó" keretezéssel. A hamisítványok önmagukban nem voltak kifinomultak, de a terjesztési infrastruktúra – a hosszú életciklusú fiókok, a cross-platform terítés és a „belső forrás" narratív keret – hiteles kontextust teremtett számukra.

A G–M–T–V lánc szempontjából az eltolás: M→T→V szekvencia: a mosás (az autentikusság látszata) → az időzített terítés → a validálás („bizonyíték-érzet") egy összefüggő folyamattá állt össze.

5.2.5. Adat- és célzás-botrány: A Cambridge Analytica-hatás

A 2018-as Cambridge Analytica-botrány nem önmagában egy FMK-művelet volt, hanem a platformgazdaság strukturális sérülékenységének nagyszabású nyilvános feltárása. A Cambridge Analytica – egy politikai tanácsadó cég – a Facebook API-jának kiskapuján keresztül mintegy 87 millió felhasználó személyes adatait gyűjtötte be hozzájárulás nélkül, majd ezeket politikai mikroszegmentálásra és célzott üzenetekre használta. Az ügy – amelyet a The Guardian[262] és a The

[260] Hedling, Elsa (2025): *Social Identities and Democratic Vulnerabilities: Learning from Examples of Targeted Disinformation.* Helsinki: The European Centre of Excellence for Countering Hybrid Threats. Online: https://www.hybridcoe.fi/publications/social-identities-and-democratic-vulnerabilities-learning-from-examples-of-targeted-disinformation/

[261] Nimmo, Ben – Brookie, Graham et al. (2019): *Operation Secondary Infektion.* Washington, D.C.: Atlantic Council – DFRLab, 2019. június 22. Online: https://www.atlanticcouncil.org/wp-content/uploads/2019/08/Operation-Secondary-Infektion_English.pdf

[262] Cadwalladr, Carole – Graham-Harrison, Emma (2018): Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach. *The Guardian,* 2018. március 17. Online: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

New York Times[263] leplezett le 2018 márciusában Christopher Wylie bejelentő tanúvallomása nyomán – több párhuzamos hatást váltott ki.

Elsősorban a szabályozási nyomás gyorsulását hozta: az Európai Parlament, az Egyesült Államok Kongresszusa és a brit parlament egyaránt meghallgatásokat tartott. Az EU-ban az Action Plan against Disinformation (JOIN(2018)36)[264] – amely az információs műveleteket formálisan biztonsági fenyegetésként rögzítette – és a Code of Practice on Disinformation (2018)[265] – az első platform-önszabályozási keret – részben a Cambridge Analytica-botrány politikai lendületéből született. A Bradshaw és szerzőtársai által dokumentált[266] platform policy kihívások öt kategóriája közül az ötödik – a jövőbeli AI- és deepfake-technológiák fenyegetése – szintén ennek a szabályozási szükségszerűségnek a kontextusában került a szakpolitikai figyelem középpontjába.

Másodsorban a botrány megváltoztatta a támadói adaptáció irányát: a fizetett célzás (paid targeting) szigorodásával a műveletek az organikus látszat és az információ mosási rétegek felé tolódtak. A hirdetés-archívumok, a politikai hirdetések átláthatósági követelményei és a platform-szabályváltozások nem szüntették meg a célzott befolyásolást, de áttolták azt nehezebben nyomon követhető csatornákra.

A G–M–T–V lánc szempontjából a változás: szabályozási nyomás → M/T adaptáció. A fizetett tér beszűkülése felértékelte a mosási rétegeket és a zárt csatornákat – paradox módon tehát a szabályozás bizonyos aspektusai a támadó kifinomultságát növelték.

---

263 Rosenberg, Matthew – Confessore, Nicholas – Cadwalladr, Carole (2018): How Trump Consultants Exploited the Facebook Data of Millions. *The New York Times*, 2018. március 17. Online: https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html

264 Európai Bizottság – Az Unió külügyi és biztonságpolitikai főképviselője (2018): *Action Plan against Disinformation.* JOIN(2018) 36 final. Brüsszel, 2018. december 5. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52018JC0036

265 Európai Bizottság (2018): *Code of Practice on Disinformation.* Brüsszel, 2018. szeptember 26. Online: https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation

266 Garcia-Camargo, Isabella – Bradshaw, Samantha (2021): *Disinformation 2.0: Trends for 2021 and Beyond.* Helsinki: European Centre of Excellence for Countering Hybrid Threats. (Hybrid CoE Working Paper 11.) Online: https://www.hybridcoe.fi/publications/hybrid-coe-working-paper-11-disinformation-2-0-trends-for-2021-and-beyond/

Az adatgyűjtés-alapú célzás katonai-operatív dimenzióját a NATO StratCom COE egy szövetséges ország valódi katonai gyakorlatán végzett kibertámadást szimuláló kísérlete tárja fel a legélesebben (Bay és Biteniece, 2019). Kizárólag nyílt forrásból – Facebook, Instagram, közösségimédia-profilok, személyes keresőmotorok – a kutatócsapat annyi személyes adatot gyűjtött össze a katonákról, hogy azonosítani tudta az összes résztvevőt, meghatározta az egységek pontos tartózkodási helyét, és célzott befolyásoló üzenetekkel képes volt rábírni a katonák egy részét konkrét viselkedésre: hely elhagyásra, kötelességmulasztásra.[267][268] A kísérlet azt is kimutatta, hogy négy telepített alkalmazás ismerete elegendő a felhasználó 95%-os valószínűséggel való azonosításához. Ez a megállapítás a Cambridge Analytica-párhuzamot a katonai-operatív szintre viszi: az adatgyűjtés-alapú műveletek nemcsak politikai célközönségek, hanem katonai személyzet ellen is kivitelezhetők, ami az Irányítás-dimenzión belül a hibrid eszköztárnak egy kiaknázatlan, a védekezési protokollokban ritkán tárgyalt dimenzióját nyitja meg. A NATO StratCom COE 2020-ban publikált keretrendszere a katonai személyzet digitális domainben való „álcázásának" szükségességét fogalmazza meg, kiemelve a műveleti biztonsági kockázatokat és a data broker alapú profilalkotás veszélyeit.[269]

5.2.6. Cheap fakes és a kontextus-manipuláció tömegesíthetősége

A szakpolitikai és médiadiskurzus a Híd-időszakban nagyrészt a deepfake-technológia fenyegetésére koncentrált, miközben az operatív valóságban a „cheap fake" – azaz az olcsó, kézműves manipuláció – bizonyult hatékonyabbnak és elterjedtebbnek. A cheap fake nem igényel generatív mesterséges intelligenciát: elég a kontextus „átöntése" – vágás, felirat hozzáadása, félrekeretezés –, és a manipulált tartalom ipari skálán teríthető.

---

[267] BAY, Sebastian – BITENIECE, Nora (2019): The Current Digital Arena and its Risks to Serving Military Personnel. In: Responding to Cognitive Security Challenges. NATO Strategic Communications Centre of Excellence, Riga. 7. o.

[268] BERTOLIN, Giorgio (szerk.) (2019): *Responding to Cognitive Security Challenges*. NATO Strategic Communications Centre of Excellence, Riga, ISBN 978-9934-564-39-0. 4., 14. o. A kötet a Preparation → Action → Learning hármas válaszkeretrendszert mutatja be, és javaslatot tesz a tartalomszelekciós algoritmusok független auditálására.

[269] NATO STRATCOM COE (2020): *A Framework for Armed Forces in the Social Media Domain: Camouflage in the Digital Domain*. NATO Strategic Communications Centre of Excellence, Riga. A katonai személyzet digitális domainben való „álcázásának" szükségességét fogalmazza meg: OPSEC-kockázatok, social media tracking és data broker alapú profilalkotás veszélyei.

A Hybrid CoE Trend Report 4 (2020)[270] részletesen tárgyalta ezt a kettősséget. Az elemzés kiemelte, hogy bár a deepfake-videók minősége rohamosan javult, a tényleges politikai hatás szempontjából az „information ambush" – az információs rajtaütés – bizonyult veszélyesebbnek. A jelentés több esetet is dokumentált: a 2019-ben felbukkant lassított Nancy Pelosi-videó, amelyet gyorsan lelepleztek ugyan, de a leleplezés előtti néhány óra elegendő volt a narratíva beágyazásához; az AP Twitter-fiókjának feltörésekor egy hamis tweet az Obama elleni Fehér Ház-támadásról hét percre 136 milliárd dollárnyi tőzsdei értékvesztést okozott (Moore & Roberts 2013[271], idézi Trend Report 4). A jelentés arra a következtetésre jutott, hogy ha egy államfő deepfake-videója jelenne meg vitatott tartalommal, a korrekcióhoz vagy a technikai leleplezéshez szükséges idő – legyen az akár csak percek – elegendő lehet a politikai kár okozásához.

Az audio-hamisítások különösen veszélyes területként emelkedtek ki. 2019-ben egy brit energetikai cég vezérigazgatóját hanghamisítás, voice deepfake segítségével szólították fel 220 000 euró átutalására – a támadók a német anyavállalat CEO-jának hangját szimulálták, és a vezérigazgató csak a harmadik hívás után fogott gyanút (Wall Street Journal, 2019)[272]. Ez volt az első széles körben dokumentált eset, ahol a deepfake technológiát közvetlenül pénzre váltották, és egyúttal a V-dimenzió (tekintély-proxy eltérítése hanggal) új szintjét demonstrálta.

A G–M–T–V lánc szempontjából: G (kézműves) + M (kontextus-mosás) → T gyorsul: az olcsó előállítás és a gyors terítés kombinációja a Híd alatt a támadói eszköztár alaprétegévé vált, amelyre a deepfake mint „prémium" réteg épült rá.

5.2.7. Memetikus hadviselés és a humor fegyveresítése

A mémek stratégiai kommunikációs eszközként való alkalmazása a Híd-időszak egyik legeredetibb és legkevésbé intézményesült fejleménye volt. A jelenség elméleti megalapozását Jeff Giesea

[270] Hybrid CoE (2020): *Trends in the Contemporary Information Environment.* Helsinki: European Centre of Excellence for Countering Hybrid Threats. (Hybrid CoE Trend Report 4.) 19–20. o.

[271] Moore, Hannah – Roberts, Dan (2013): AP twitter hack causes panic on Wall Street and sends Dow plunging. *The Guardian*, 2013. április 23. Online: https://www.theguardian.com/business/2013/apr/23/ap-tweet-hack-wall-street-freefall.

[272] Stupp, Catherine (2019): Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case. *The Wall Street Journal,* 2019. augusztus 30. Online: https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402

végezte el a NATO StratCom COE 2015-ös tanulmányában (újra kiadva a Memetic Warfare: Echoes from the Past, Visions of the Future kötetben, NATO StratCom COE 2021).[273] Giesea definíciója szerint a memetikus hadviselés „versengés a narratíváért, az eszmékért és a társadalmi kontrollért a közösségi média hadszínterén" – tehát nem puszta trollkodás, hanem az információs műveletek digitálisan létrejött változata. Ahogy Giesea fogalmazott: ha a propaganda és a közéleti diplomácia a memetikus hadviselés konvencionális formái, akkor a trollkodás és a pszichológiai műveletek annak gerillaverzióit jelentik.

A tanulmány több kulcsfontosságú precedenst dokumentált a Híd-időszakból. Oroszország „trollfarmjai" – amelyekről a New York Times 2015-ös tényfeltáró cikke[274] rántotta le a leplet – 2014-ben a #ColumbianChemicals és az #EbolaInAtlanta hashtagek alatt teljes dezinformációs kampányokat futtattak hamis videókkal, fényképekkel és Wikipedia-oldalakkal, újságírókkal való kapcsolatfelvétellel kombinálva. Kína a Giesea által idézett becslések szerint 20 000–50 000 internetrendőrt és további negyed millió „trollt" foglalkoztatott a pro-pekingi tartalom terjesztésére[275] mind bel-, mind külföldön. Az ISIS pedig professzionális szintű kommunikációs rendszert épített ki többnyelvű termékekkel (Dabiq, Dar al-Islam magazinok), amelyek célzott toborzási kampányokat tápláltak.[276]

A humor védekezői alkalmazása szintén a Híd-időszakban intézményesült. A NATO StratCom COE 2017-es StratCom Laughs tanulmánykötete (Ozoliņa et al.) analitikai keretrendszert dolgozott ki a humor stratégiai kommunikációs alkalmazására, és dokumentálta a 2014 utáni ukrán humort mint a katonai agresszió elleni társadalmi válasz egyik formáját. A 2014 augusztusában közzétett kanadai NATO-küldöttségi tweet – „Geography can be tough" felirattal egy térképen megjelölve

---

[273] Giesea, Jeff (2016): It's Time to Embrace Memetic Warfare. *Defence Strategic Communications*, Vol. 1, 67–75. o. Online: https://stratcomcoe.org/publications/its-time-to-embrace-memetic-warfare/164

[274] Chen, Adrian (2015): The Agency. *The New York Times Magazine*, 2015. június 7. Online: https://www.nytimes.com/2015/06/07/magazine/the-agency.html

[275] Giesea, Jeff (2016): It's Time to Embrace Memetic Warfare. *Defence Strategic Communications*, Vol. 1, 67–75. o. Online: https://stratcomcoe.org/publications/its-time-to-embrace-memetic-warfare/164

[276] Winter, Charlie (2015): *The Virtual 'Caliphate': Understanding Islamic State's Propaganda Strategy*. London: Quilliam Foundation. Online: https://quilliamuk.org/wp-content/uploads/2015/10/FINAL-documenting-the-virtual-caliphate.pdf

„Russia” és „Not Russia” területeit – az egyik első virális esete volt annak, hogy egy formális kormányzati kommunikációs csatorna gúnyt alkalmazott üzenetátadásra (Hybrid CoE Working Paper 26, 2023).[277] Hasonlóan, a brit kijevi nagykövetség 2014 novemberében közzétett egy T-72BM tank „felismerési segédletet” az orosz jelenlét folyamatos tagadására válaszul, ukrán nyelven is; a tweet nemzetközi sajtóvisszhangot kapott, és a közvetlen gúny a tényellenőrzésnél hatékonyabbnak bizonyult az orosz narratíva hiteltelenítésében[278].

Az említett Hybrid CoE Working Paper 26 2023-ban három okot azonosított, amiért a humor hatékony dezinformáció-ellenes eszköz: eléri a szokásos közönségen túli rétegeket; erősíti a saját közönség morálját és rezilienciáját; és rontja a támadó hírnevét és hitelességét. Ez a hármas funkció a 2022-es ukrajnai konfliktusban – különösen a NAFO-jelenség kapcsán – teljesedett ki, de a Híd-időszak teremtette meg az elméleti és gyakorlati alapjait. Giles a humor taktikai mechanizmusát „szerepcsereként” írja le: míg a trollok és propagandisták hagyományosan az ellenfeleiket rángatják bele meddő vitákba, a nevetségessé tétel megfordítja ezt a dinamikát – az abszurd diskurzusba való belépés magát a propagandistát hiteltelenítí, így neki áll érdekében nem reagálni. A dezinformáció Graham Brookie (Atlantic Council DFRLab) szavaival csapda, amelyből nem tűzzel kell tüzet oltani, hanem fölébe kell emelkedni – és a humor pontosan ezt az emelkedést teszi lehetővé[279].

A G–M–T–V lánc szempontjából a memetikus hadviselés a V-dimenziót érinti leginkább: a mém mint kulturálisan rezonáns formátum a validálás mechanizmusát befolyásolja – mind támadói oldalon (a mém „igazolja” a narratívát a közösségi elfogadáson keresztül), mind védekezői oldalon (az ellen-mém delegitimálja a támadót).

A humor dezinformáció-ellenes hatékonyságának mérésére Ben Nimmo „Breakout Scale” (áttörési skála) fogalma adja a legalkalmasabb keretet. A skála hat fokozatot különböztet meg: az 1-es

---

[277] Giles, Keir (2023): *Humour in Online Information Warfare: Case Study on Russia's War on Ukraine.* Helsinki: European Centre of Excellence for Countering Hybrid Threats. (Hybrid CoE Working Paper 26.) Online: https://www.hybridcoe.fi/wp-content/uploads/2023/11/20231106HybridCoEWorkingPaper26HumortocombatdisinformationWEB.pdf

[278] GILES, Keir (2023): *Humour in online information warfare: Case study on Russia’s war on Ukraine*. Hybrid CoE Working Paper 26. European Centre of Excellence for Countering Hybrid Threats, Helsinki. 14. o.

[279] GILES, Keir (2023): *Humour in online information warfare: Case study on Russia’s war on Ukraine*. Hybrid CoE Working Paper 26. European Centre of Excellence for Countering Hybrid Threats, Helsinki. 14–15. o.

kategória az észrevétlenül maradó eseményt jelöli, a 6-os a tényleges szakpolitikai választ vagy konkrét intézkedést kiváltó hatást. A Hybrid CoE Working Paper 26 megállapítása szerint a humor rendszerint legalább 4-es kategóriájú áttörést ér el – azaz rendszeresen átlépi a közösségi médiából a mainstream médiába vezető határt. Ennek illusztrációjaként a tanulmány a litván Laikykitės ten (Kitartás ott) televíziós műsort emeli ki: Andrius Tapinas komikus az orosz propagandát és dezinformációt nemcsak litván közönség számára leplezi le, hanem a sorozat immár orosz nyelvű változatban is fut – bizonyítva, hogy a humor nem csupán platformhatárokon, hanem nyelvi-közönséghatárokon is képes áttörni. A G–M–T–V keretben ez a V-dimenzió elleni védekezés egy sajátos formája: a humor a célközönség validálási reflexét az eredeti narratíva ellen fordítja.[280]

5.2.8. Deepfake és a generatív tartalom megjelenése

A szintetikus média megjelenése a Híd-időszak talán legtöbbet tárgyalt, ugyanakkor operatív hatásában leginkább túlértékelt fejleménye volt. A 2017-ben felbukkant első deepfake-videók – amelyeket generatív ellenséges hálózatok (GAN) hoztak létre – gyorsan felkeltették a szakpolitikai figyelmet, de a tényleges bevetésük politikai műveletek során a Híd-időszakban korlátozott maradt.[281][282] A deepfake-technológia kiberfenyegetésként való konceptualizálását Dami (2022) részletezi: a GAN-alapú generálás technikai mechanizmusának leírása és a detekciós kísérletek

[280] GILES, Keir (2023): *Humour in online information warfare: Case study on Russia's war on Ukraine*. Hybrid CoE Working Paper 26. European Centre of Excellence for Countering Hybrid Threats, Helsinki. 10. o. A Nimmo-féle Breakout Scale definícióját ld. uo., 9. lj. (Ben Nimmo, „The Breakout Scale", Brookings, 2020). A litván Laikykitės ten tevékenységének orosz nyelvű kiterjesztését ld. uo., 10. lj.

[281] JURŠĖNAS, Aistis — KARLAUSKAS, Karolis — LEDINAUSKAS, Edgaras — MASKELIŪNAS, Gytis — RUSECKAS, Julius (2021): *The Double-Edged Sword of AI: Enabler of Disinformation*. NATO Strategic Communications Centre of Excellence, Riga, 7., 12., 17. o. A kiadvány szisztematikusan térképezi fel az MI dezinformációs alkalmazásait: a StyleGAN-alapú profilképek generálásától a sock-puppet és cyborg fiókok automatizálásáig.

[282] NATO STRATCOM COE (2020): *Deepfakes – Primer and Forecast*. NATO Strategic Communications Centre of Excellence, Riga, ISBN 978-9934-564-49-9. 11., 16–17. o. A Primer rámutat, hogy a „cheapfake"-ek (alacsony technológiájú manipulált média: lelassított/felgyorsított videók, kiragadott képek hamis felirattal) a vizsgált időszakban sokkal elterjedtebbek és hatékonyabbak voltak, mint a valódi deepfake-ek. A detekció és a generálás között hosszú távú patthelyzettel kell számolni; a legnagyobb fenyegetést nem a demokratizált, hanem a célzottan épített, kifinomult deepfake-modellek jelentik.

korlátainak feltárása alátámasztja, hogy a technológiai korlát nem a generálás, hanem a valós idejű detekció oldalán jelentkezett.[283]

A Hybrid CoE Paper 14 (Mazzucchi 2022)[284] az AI-alapú technológiák hibrid fenyegetésben betöltött szerepét elemezve arra mutatott rá, hogy a deepfake alkalmazás a vizsgált időszakban elsősorban két területen koncentrálódott: a politikai és katonai kommunikáció megszemélyesítése (az ellenfél vezetőjének hátrányos ábrázolása) és a „sound box" hálózatok – tehát a visszhangerősítő infrastruktúra – létrehozása. A tanulmány kiemelte, hogy az oroszországi Wagner-csoport Maliban és a Közép-afrikai Köztársaságban már alacsony-közepes technológiai szintű digitális befolyásolási műveleteket folytatott a közösségi hálózatokon, és a szubszaharai Afrika gyors digitalizációja előrevetítette az AI-alapú rendszerek közeli alkalmazását.

A Wagner-csoport afrikai műveleteiben a fizikai katonai jelenlét nem vált el az információs befolyásolástól. A Hybrid CoE Working Paper 33 részletezi, hogy Madagaszkáron 2018-ban a Wagner politikai technológusai „spoiler-jelölt" stratégiát alkalmaztak: nyolc stratégiai jelöltnek nyújtottak pénzügyi támogatást azzal a céllal, hogy az első fordulóban szétforgácsolják a szavazatokat, majd visszalépésük után az eredeti Wagner-favoritot juttassák győzelemre. Az AFRIC (Association of Free Research and International Cooperation) fedőszervezet valóságos gondolkodóműhelynek leplezte a műveleteket, miközben hamis választási megfigyelőkként is felfuttatták azt. Ez a séma a G–M–T–V lánc szempontjából a Generálás és a Mosás dimenziók szimultán működését testesíti meg: a Wagner teremti a narratíva origóját (G), az AFRIC fedőszervezet biztosítja az attribúciós elhomályosítást (M).[285]

A Bradshaw és szerzőtársai által a 2020-as amerikai elnökválasztásról készített elemzés (Hybrid CoE Working Paper 11) ugyanakkor meglepő megállapításra jutott: az AI-alapú technológiai

---

283 DAMI, Lorenzo (2022): Analysis and Conceptualization of Deepfake Technology as Cyber Threat. Research Paper, University of Florence, School of Political Science "Cesare Alfieri". A dolgozat a deepfake-technológiát a kiberfenyegetések taxonómiájába helyezi, részletezve a GAN-alapú generálás technikai mechanizmusát és a detekciós kísérletek korlátait.

284 Mazzucchi, Nicolas (2022): *AI-based Technologies and Their Use as a Weapon of Hybrid Warfare.* Helsinki: Hybrid CoE.

285 LAUDER, Matthew (2024): The Rise and Fall of the Wagner Group. Hybrid CoE Working Paper 33. European Centre of Excellence for Countering Hybrid Threats, Helsinki. A madagaszkári művelet részleteit ld. 13–15. o., a szudáni politikai technológiai beavatkozást ld. 12–13. o. Az AFRIC (Association of Free Research and International Cooperation) fedőszervezetként való működtetését ld. 14–15. o.

innovációk (deepfake, GPT-3 szöveggenerálás, GAN-alapú profilképek) a 2020-as választási ciklusban „nagyrészt kiaknázatlanok maradtak". A befolyásolási műveletek a platformtechnológia meglévő lehetőségeit használták ki – élő közvetítéseket, alulról jövő csoportdinamikát, influencer-amplifikációt –, nem pedig csúcstechnológiát. Ez a megállapítás fontos korrekciója volt a deepfake-pániknak, és arra hívta fel a figyelmet, hogy a szakpolitikai válasznak a jelenlegi platform-affordanciákra kell koncentrálnia, miközben nyomon követi a jövőbeli technológiai innovációkat.

A NATO StratCom COE 2024-es AI in Support of StratCom Capabilities elemzése visszatekintve is megerősítette,[286] hogy a nagy nyelvi modellek (LLM-ek) 2023-ra váltak ténylegesen alkalmazott eszközzé az információs fenyegetésekben – a Híd-időszakban a generatív AI még inkább a „fenyegetések horizontján" állt, semmint operatív valóság lett volna.

A G–M–T–V lánc szempontjából a deepfake megjelenése a G-dimenziót érintette leginkább: a tartalomelőállítás potenciális költsége radikálisan csökkent. A tényleges műveleti hatás azonban a V-dimenzión keresztül érvényesült: a hamisítható tartalom puszta létezése erodálta a hiteles bizonyítékokba vetett bizalmat – ez a „hazug osztaléka" (Liar's Dividend) hatás, amelyet Chesney és Citron (2019) írt le részletesen.

5.2.9. COVID-infodémia mint globális stressztesz

A COVID-19 pandémia (2020–2021) a Híd-időszak legnagyobb szabású és legsokoldalúbb FMK-stressztesztje volt: a járvány egyszerre teremtett globális információs vákuumot, érzelmi túlterhelést és intézményi bizonytalanságot – azaz a kognitív műveletek ideális terepét. Az Egészségügyi Világszervezet (WHO) által „infodémiának" nevezett jelenség a dezinformáció minden korábbi mintázatát felgyorsította és globalizálta. A NATO StratCom COE 2021-es médiadiskurzus-elemzése kimutatta, hogy a COVID-19-hez kapcsolódó dezinformáció tartalmi

[286] PAMMENT, James et al. (2024): *AI in Support of Strategic Communication Capabilities*. NATO Strategic Communications Centre of Excellence, Riga, ISBN 978-9934-619-61-8. 25–35. o. Az elemzés bemutatja, hogyan alkalmazható a generatív MI (GPT-4) az IEA (Information Environment Assessment) folyamatában: célközönség-szegmentálás, narratívagenerálás és Midjourney képi illusztrációk. Az eredmények „generikusak", de az IEA és a generatív MI integrálása a StratCom-munkamenetbe precedensértékű.

mintázatai szoros összefüggést mutattak az adott ország geopolitikai helyzetével és médiakörnyezetével.[287][288]

A Hybrid CoE Working Paper 29 2024-ben az orosz dezinformáció hatásának elemzésekor számos konkrét esetet dokumentált, ahol a Kreml-dezinformáció valós fizikai következményekhez vezetett. Az Egyesült Királyságban 2020 áprilisában a brit kormány húsz 5G-mobiladó megrongálását vagy felgyújtását azonosította, amelyeket az 5G-technológia és a COVID-19 terjedése közötti összeesküvés-elmélet motivált. Hasonló esetek történtek Hollandiában és Belgiumban is. A Wired tudósítása szerint az RT (Russia Today) már 2019 januárjától közölt az 5G technológia káros hatásairól szóló anyagokat, és az EUvsDisinfo adatbázisa több Kreml-szponzorált vagy -affiliált oldalt azonosított, amely a vírus terjedését az 5G-távközléshez kötötte. Emellett bizonyítékok álltak rendelkezésre arról, hogy orosz kötődésű közösségimédia-fiókok és botok részt vettek a COVID-19-cel kapcsolatos 5G-összeesküvés-elméletek erősítésében.

A pandémia különösen hatékonyan demonstrálta a „proof-feeling" (bizonyíték-érzet) tömegesíthetőségét. A Bradshaw és szerzőtársai (Hybrid CoE Working Paper 11)[289] által dokumentált „just asking questions" dinamika – ahol a dezinformátorok nem állítanak, hanem „csak kérdeznek", ezzel a bizonyítási terhet az intézményekre hárítva – a COVID-kontextusban különösen virulensnek bizonyult. A vakcina dezinformáció terén az egyik legismertebb eset az volt, amikor egy brit székhelyű PR-ügynökség – amelyről később kiderült, hogy Kreml-kötődésű – európai influencereket keresett meg, hogy a Pfizer/BioNTech vakcinát lejárassák (The Guardian,

[287] NATO STRATCOM COE (2020): *Social Media Manipulation 2020*. NATO Strategic Communications Centre of Excellence, Riga. A 2020-as jelentés az ukrán SBU által felszámolt COVID-19 dezinformációs botfarmokat dokumentálja, a Graphika IRA-elemzéseket és a Stanford Internet Observatory takedown-elemzéseit.

[288] NATO STRATCOM COE (2021): *Insights into Covid-19-related News Media Discourse*. NATO Strategic Communications Centre of Excellence, Riga. A COVID-19-hez kapcsolódó dezinformáció tartalmi mintázatai szoros összefüggést mutattak az adott ország geopolitikai helyzetével és médiakörnyezetével.

[289] Garcia-Camargo, Isabella – Bradshaw, Samantha (2021): *Disinformation 2.0: Trends for 2021 and Beyond.* Helsinki: European Centre of Excellence for Countering Hybrid Threats. (Hybrid CoE Working Paper 11.) Online: https://www.hybridcoe.fi/wp-content/uploads/2021/07/20210716_Hybrid_CoE_Working_Paper_11_Disinfo_2_0_WEB.pdf

2021. május;[290] Hybrid CoE WP 29[291]). Az ügynökség professzionálisan előkészített „szkripteket" küldött az influencereknek, akik közül többen nyilvánosságra hozták a megkeresést.

A COVID-dezinformáció magyar vonatkozásait Szicherle Patrik és Krekó Péter 2020-as elemzése[292] dokumentálta. A szerzők rámutattak, hogy a járvány nyomán Magyarországon is elszaporodtak az álhírek, amelyek a globális mintázatokhoz hasonló mechanizmusokat alkalmaztak: az egészségügyi intézmények hitelességének aláásása, alternatív „gyógymódok" promóciója, és az oltásellenes narratívák összekapcsolása tágabb összeesküvés-elméletekkel. Ez az adat a disszertációm szempontjából kiemelt jelentőségű, mivel magyar empirikus kontextust teremt a globális jelenségek számára.

A CORE Comprehensive Resilience Ecosystem (Hybrid CoE) elemzése a COVID-pandémiát a hibrid fenyegetések instrumentalizálásának kontextusába helyezte. A tanulmány szerint Kína és Oroszország kétféle módon használta ki a járványt: egyrészt a COVID-19-specifikus sérülékenységeket célozták (maszkhiány, orvosi felszerelés, vakcinák), másrészt a járványt mint elterelő manővert alkalmazták stratégiai céljaik előmozdítására – próbálva bizonyítani, hogy a tekintélyelvű rendszerek hatékonyabban kezelik a válságokat, mint a demokratikus társadalmak. A pandémia világossá tette a civic, governance és services terek közötti komplex interdependenciákat, és megmutatta, hogy a szolgáltatási tér megbízhatóságának hiánya aláássa a kormányzási és a civil tereket is. Az orosz és kínai információs műveletek konvergenciáját szisztematikusan elemző, (Turcsányi et al. által készített tanulmány 2024-ben rámutat, hogy a két nagyhatalom narratíva-szinkronizációja „opportunista" jellegű: az USA-ellenes üzenet közös nevező, de a taktikai eszközök eltérnek (orosz: trollok és fake weboldalak; kínai: „wolf warrior"

[290] Henley, Jon (2021): Influencers say Russia-linked PR agency asked them to disparage Pfizer vaccine. *The Guardian*, 2021. május 25. Online: https://www.theguardian.com/media/2021/may/25/influencers-say-russia-linked-pr-agency-asked-them-to-disparage-pfizer-vaccine

[291] Hoyle, Aiden – Šlerka, Josef (2024): *Cause for Concern: The Continuing Success and Impact of Kremlin Disinformation Campaigns.* Helsinki: European Centre of Excellence for Countering Hybrid Threats. (Hybrid CoE Working Paper 29.) Online: https://www.hybridcoe.fi/wp-content/uploads/2024/03/20240306HybridCoEWorkingPaper29TheimpactofKremlindisinformationWEB.pdf

[292] SZICHERLE Patrik – KREKÓ Péter (2020): *Burjánzanak az álhírek a koronavírus nyomában*. Political Capital, Budapest. 3–8. o. A COVID- dezinformáció magyarországi megjelenési mintáinak elemzése.

diplomácia és külföldi média felhasználása), és az ukrajnai háború kontextusában a narratív konvergencia korlátozott maradt.[293]

Az European Digital Media Observatory (EDMO) dokumentálta azt a különösen figyelemre méltó jelenséget is, hogy a COVID-19 dezinformációs csatornák – összeesküvés-elméleti csoportok, oltásellenes mozgalmak – 2022 után zökkenőmentesen átálltak pro-Kreml Ukrajna-narratívákra. Ez a narratíva-csatorna-újrafelhasználás bizonyította, hogy a Híd alatt kiépült dezinformációs infrastruktúra nem témaspecifikus, hanem transzferálható.

A G–M–T–V lánc szempontjából a COVID-infodémia a verifikáció növelése, a mosás és a terjesztés növekedése (hibrid) irányába tolta el a láncot: a „bizonyíték-érzet" tömegesítése (V), a szakértő-proxy iparosodása (L – álszakértők mint hitelesítő réteg) és a zárt csatornákon zajló terítés (D) együttesen a 2022-es konfliktus kognitív terepének „előfeszítését" adták.

A COVID-19 információs hatása nem korlátozódott az európai és észak-amerikai színterekre. A NATO StratCom COE (2022) jelentése kvalitatív narratíva-elemzést és szakértői interjúkat alkalmaz az afrikai dimenzió feltárásához. Dél-Afrikában a pandémia idején felerősödött a „digitális vigilantizmus": meglévő xenofób narratívák összefonódtak a #PutSouthAfricansFirst hashtag körül. A vakcinadiplomácia narratívái stratégiai törésvonalat hoztak létre: míg az orosz és kínai megközelítést „globális közjóként" keretezték, a nyugati vakcinapolitikát „önzőnek és igazságtalannak" állították be. Az Omicron-variáns utáni utazási korlátozásokat az afrikai diskurzusban „Afrika büntetéseként" értelmezték. Cowling (Stellenbosch-i Intézet) értékelése szerint a „COVID-19 a Nyugat reputációját rontotta Afrikában". A Prigozsin IRA-módszereivel egybecsengő taktikák – helyi hangok felhasználása, pan-afrikanizmus támogatása, összeesküvés-elméletek erősítése – dokumentálhatók a kontinensen. Az afrikai eset a narratív fegyverzés globális

[293] TURCSÁNYI, Richard Q. et al. (2024): *Sino-Russian Information Operations: Convergence, Divergence, and the Way Ahead*. NATO Strategic Communications Centre of Excellence, Riga, 6., 37–38. o. Az orosz és kínai információs műveletek konvergenciáját elemző összehasonlító keretrendszer. Az USA-ellenes narratíva közös nevező; a COVID-19 és az ukrajnai háború esetén a narratíva-konvergencia „opportunista" jellegű: a kínai „wolf warrior" diplomácia és a külföldi média felhasználása eltér az orosz trolloktól és fake weboldalakon alapuló taktikától.

exportálhatóságát demonstrálja: a disszertáció FMK Kognitív Olló modelljének támadás-oldala nem csupán az európai, hanem a globális déli színtéren is érvényesül.[294]

5.2.10. Zapad 2021 és narratíva-előkészítés: a kinetikus-kognitív szinkronizáció

A Híd-időszak utolsó csomópontja a 2021-es Zapad katonai gyakorlat és az azt kísérő narratíva-építés, amely közvetlenül a 2022-es invázió információs előkészítéseként értelmezhető. Ez a csomópont különbözik az előzőektől: nem technológiai vagy módszertani innovációról szól, hanem a kinetikus (katonai) és kognitív (információs) dimenziók tudatos szinkronizálásáról.

A Hybrid CoE Working Paper 13 (Kalenský 2022)[295] az inváziót megelőző Kreml-üzenetek részletes elemzését végezte el. A tanulmány kimutatta, hogy az üzenetek „nyitó lövése" Vlagyimir Putyin 2021 júliusában közzétett cikke[296] volt „Az oroszok és ukránok történelmi egységéről", amely Ukrajnát „anti-Oroszország projektként" és „a Nyugat alkotásaként" jellemezte, az etnikai szempontból homogén, Oroszországgal szemben agresszív ukrán állam létrehozásának következményeit pedig a tömegpusztító fegyverek bevetéséével állította egy szintre. A teljes kampány 2021 októberében, Medvegyev cikkével[297] gyorsult fel, amely az ukrán vezetést „vazallusoknak" minősítette, akikkel Moszkva nem hajlandó tárgyalni.

A tanulmány legfontosabb megállapítása az volt, hogy a legmagasabb szintű Kreml-képviselők üzenetei és a Kreml által kontrollált „média" ökoszisztéma tartalma szinkronban futott. A Detektor Media ukrán projekt 70 000 poszt elemzése alapján a pro-Kreml források a katonai narratíváktól a belső zavargásokról és Ukrajna belső nehézségeiről szóló üzenetek felé divergáltak, folyamatosan tolva az „Ukrajna az agresszor" és a „Nyugat elhagyja Ukrajnát" narratívákat. A Mythos Labs és

---

[294] NATO STRATCOM COE (2022): Strategic Communications and Covid-19. NATO Strategic Communications Centre of Excellence, Riga, . 79., 81., 83–84. o.

[295] Kalenský, Jakub (2022): *The Kremlin's Messaging on Ukraine: Authorities and „Media" Hand in Hand.* Helsinki: European Centre of Excellence for Countering Hybrid Threats. (Hybrid CoE Working Paper 13.) 8. o. Online: https://www.hybridcoe.fi/wp-content/uploads/2022/01/20220131-Hybrid-CoE-WP-13-Kremlins-messaging-on-Ukraine-WEB.pdf

[296] Putyin, Vlagyimir (2021): Az oroszok és az ukránok történelmi egységéről. *Kremlin.ru,* 2021. július 12. Online: http://en.kremlin.ru/events/president/news/66181

[297] Medvegyev, Dmitrij (2021): Pourquoi les contacts avec la direction ukrainienne actuelle sont inutiles. [Miért értelmetlen a jelenlegi ukrán vezetéssel kapcsolatot tartani.] *Kommersant,* 2021. október 11. Online: https://www.kommersant.ru/doc/5028300

az EUvsDisinfo hasonló következtetésekre jutott. Az üzenetek stratégiai célja a „bekerített erőd” szindróma megerősítése és a jövőbeli agresszió igazolása „csupán védekezői lépésként” volt.

A Hybrid CoE Strategic Analysis 31 (2022) Oroszország katonai felvonulását elemezve megállapította, hogy a katonai és az információs dimenzió egymást erősítve működött: a csapatösszevonás fizikai fenyegetést jelentett, miközben az információs kampány a fenyegetés értelmezési keretét kontrolálta. A Zapad 2021 gyakorlat – amely a kényszerítő (coercion) és az információs nyomásgyakorlás összekapcsolását tesztelte – a 2022-es invázió „előszobájaként” értelmezhető. Pulai Bence (2023) tartalomelemzése – 106 cikk vizsgálata a CNN, a BBC és az RT hírportáljain – a 2021-es lengyel–fehérorosz határválságot közvetett előkészítésként azonosítja: a nemzetközi figyelem sikeresen elterelődött, és a Union Resolve 2022 hadgyakorlat fedőnarratívája a korábbi határválságra épült[298][299]

A G–M–T–V lánc szempontjából ez a csomópont a T↑, V↑, M↑ irányba hatott: a terjesztés a teljes állami médiarendszert mobilizálta; a validálás a legmagasabb politikai szintű kijelentéseken keresztül történt; a mosás a „diplomáciai követelés” keretezésen át valósult meg, amely a katonai agressziót „védekezői szükségszerűségként” állította be.

A vonatkozó 13. táblázat: ANCHOR-összegző táblázat címmel a melléklet tartalmazza.

5.3. Mérföldkövek fegyvernek minősülő kommunikáció elleni reziliencia képesség felépülésében (2014–2021)

A Híd-időszak nem csupán a támadói képességek transzformációját hozta el: párhuzamosan – gyakran épp a támadások által katalizálva – a védekezői oldal is jelentős intézményi, technológiai és társadalmi kapacitást épített ki. E szekció azokat a mérföldköveket tárgyalja, amelyek a 2022-es konfliktusra lényegesen eltérő védekezési pozíciót teremtettek a 2014-eshez képest.

[298] KLEIN, Margarete (2022): Russia’s military buildup along Ukraine’s border: What to expect? Hybrid CoE Strategic Analysis 31. European Centre of Excellence for Countering Hybrid Threats, Helsinki. 3–5. o.

[299] PULAI Bence (2023): *A befolyásolás mint a hibrid hadviselés eszköze a 2021-es lengyel–fehérorosz migrációs- és határválság során.* Honvédségi Szemle, 151. évf. 6. sz. 56–67. o.

5.3.1. Intézményi–szabályozási ébredés (EU és tagállami intézkedések)

A 2014-es krími művelet egyik legfontosabb tanulsága az volt, hogy a nyugati intézményi válasz nem a képesség, hanem a felismerés szintjén bukott el: az információs műveleteket nem kezelték biztonsági fenyegetésként. A Híd-időszak ezt a deficitet fokozatosan, bár nem lineárisan korrigálta.

Vytautas Keršanskas a Hybrid CoE keretében készített litván esettanulmánya dokumentálja, hogy a legkorábbi és leghatározottabb tagállami válasz Litvániából érkezett: a Litván Rádió- és Televíziós Bizottság már 2014-ben felfüggesztette a Kreml-kontrollált TV-csatornák sugárzását, ami megtagadással történő elrettentésként és költségkivetésként is értelmezhető. A litván modell – a média tudatossági programokkal kombinálva – a fegyvernek minősülő kommunikáció transzformációs időszakának legkorábbi integrált reziliencia stratégiájának tekinthető.[300]

Az első érdemi EU-szintű lépés az East StratCom Task Force létrehozása volt 2015-ben, amely az EUvsDisinfo projekten keresztül megkezdte a pro-Kreml dezinformációs üzenetek szisztematikus nyilvántartását. A döntő fordulópontot azonban a 2018-as év hozta: az Action Plan against Disinformation (JOIN(2018)36) volt az első EU-dokumentum, amely az információs műveleteket formálisan biztonsági fenyegetésként rögzítette. Ugyanebben az évben született a Code of Practice on Disinformation[301] – a platformfelelősség első kerete, még soft-law jelleggel, amely a platformok önkéntes vállalásaira épített.

A 2020-as European Democracy Action Plan (EDAP) összekötötte a platformfelelősséget a demokratikus integritás kérdésével, a 2020-as tanácsi következtetések pedig a digitális szuverenitás és a technológiai aszimmetria kérdését politikai szintre emelték. Ez a szabályozási folyamat végül a Digital Services Act (DSA, 2022) felé vezetett – amely már a 6. fejezet tárgykörébe tartozik –, de a Híd-időszak építette ki annak normatív és intézményi alapjait.

A szabályozási nyomás paradox hatást is kiváltott: a fizetett politikai hirdetések átláthatósági követelményei és a platformmoderálás erősödése a támadói oldalt a mosási rétegek és a zárt

[300] KERŠANSKAS, Vytautas (2021): Deterring disinformation? Lessons from Lithuania's countermeasures since 2014. Hybrid CoE Paper 6. European Centre of Excellence for Countering Hybrid Threats, Helsinki. 10–14. o.

[301] EUROPEAN COMMISSION (2018): Code of Practice on Disinformation. European Commission, Brussels, 2018. szeptember 26.

csatornák irányába terelte. Ez a jelenség jól illusztrálja a támadó-védekezői spirál dinamikáját, amelyet a fejezet szintézis-szekciója összegez.

Az intézményi kommunikáció hatékonyságának korlátait jól szemlélteti az EUvsDisinfo humorral kapcsolatos tapasztalata. Giles elemzése szerint az EU dezinformáció-elleni szervei nem tudták felülírni a bürokratikus viralitási paradoxont: humoros próbálkozásaik nehézkesnek és túl erőteljesnek bizonyultak, ami azt a kritikát váltotta ki, hogy a propaganda-kimenetek stílusát tükrözik, feladva a megkülönböztethetőség és a morális magaslat igényét. Egy EUvsDisinfo-munkatárs a nyilvános kritikára meglepetéssel reagált – jelezve, hogy a belső visszacsatolási mechanizmusok nem voltak képesek a külső percepciót kellő időben közvetíteni[302]. Ez az eset a MRM mezoszintjén (szervezeti reziliencia) azt az általánosítható tanulságot hordozza, hogy a humor-alapú stratégiai kommunikáció sikeréhez nem elegendő a szándék: a kulturális érzékenység, a hatásmérés és a gyors visszacsatolás intézményi feltételeinek is adottnak kell lenniük.

5.3.2. Katonai-stratégiai diagnosztika: NATO StratCom COE és Hybrid CoE

A Híd-időszak alatt két intézmény emelkedett ki az információs műveletek rendszerszintű elemzésében és a védekezési doktrína kidolgozásában: a rigai NATO Strategic Communications Centre of Excellence (StratCom COE, 2014–) és a helsinki European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE, 2017–).

A NATO StratCom COE publikációi a Híd-időszak kulcsproblémáit szisztematikusan feltérképezték: a manuális trollfarmok hálózati működésének elemzése (2016), a humor és szatíra mint műveleti eszköz analitikai keretrendszere (StratCom Laughs, 2017), az automatizált platform-manipuláció empirikus mérhetősége – a Robotrolling sorozat (2019–), a COVID-pandémia katonai olvasata (2020), és a memetikus hadviselés elméleti és gyakorlati összefoglalása (Memetic Warfare, 2021).[303] Ez a publikációs korpusz nemcsak a jelenségek dokumentálását végezte el,

[302] GILES, Keir (2023): *Humour in online information warfare: Case study on Russia's war on Ukraine*. Hybrid CoE Working Paper 26. European Centre of Excellence for Countering Hybrid Threats, Helsinki. 18. o.

[303] NATO STRATCOM COE (2023): *Virtual Manipulation Brief 2023/1: Generative AI and Its Implications for Social Media Analysis*. NATO Strategic Communications Centre of Excellence, Riga, ISBN 978-9934-619-41-0. A VMB 2023/1 a Kreml háborús kommunikációjának átalakulását, az EU szankciók hatásait és az orosz propagandisták Telegramra történő áttérését dokumentálja.

hanem analitikai nyelvet és keretrendszert adott a NATO-tagállamok számára az információs műveletek értelmezéséhez.

Az orosz információs műveletek afrikai logikáját – amelyet a 2024-es Morley-Davies et al. tanulmány globális keretben tárgyalt – a NATO StratCom COE (2021) Mali és a Közép-afrikai Köztársaság részletes esettanulmányain keresztül már korábban is dokumentálta. A kutatás négy területen – diplomácia, politikai kommunikáció, katonai jelenlét (Wagner-csoport) és gazdasági kapcsolatok – mutatja be az orosz stratégia egymást erősítő, integrált rendszerét.[304] Az ENSZ MINUSMA-misszióval szembeni dezinformáció különösen rávilágít arra, hogy az információs befolyásoló művelee-k nemcsak pozitív narratívát terjesztenek, hanem az alternatívák hitelét is rombolják – a legitimációrombolás mint önálló információs befolyásoló művelet eszköz a disszertáció M(osás)-dimenziójának egy kevéssé tárgyalt technikájára mutat rá. A Wagner-csoport katonai jelenlétének és az információs műveleteknek az összefonódása a hibrid eszköztár (3. fejezet) kinetikus-kognitív szinkronizációjának egy korai, nem európai kontextusú dokumentációja.

A Hybrid CoE a hibrid fenyegetések fogalmi rögzítésében, a rendszermodellek kidolgozásában és a reziliencia-elmélet operacionalizálásában játszott meghatározó szerepet. A CORE Comprehensive Resilience Ecosystem modell[305] – amely a civil, állami és szolgálati tereket integrálta – alapvető keretrendszert adott a hibrid fenyegetések társadalmi hatásának megértéséhez. A Hybrid CoE Paper 12 (Monaghan 2022)[306] az elrettentés ötödik hullámát tárgyalva arra a következtetésre jutott, hogy a reziliencia az elrettentés alapja a hibrid fenyegetések kontextusában, de önmagában nem stratégia: a megtagadás és a büntetés egyensúlyára épülő, egész társadalmat

[304] NATO STRATCOM COE (2021): Russia's Activities in Africa's Information Environment: Case Studies – Mali and the Central African Republic. NATO Strategic Communications Centre of Excellence, Riga. 4–12. o.

[305] Európai Bizottság – Joint Research Centre – European Centre of Excellence for Countering Hybrid Threats (2023): *Hybrid Threats: A Comprehensive Resilience Ecosystem.* Luxembourg: Publications Office of the European Union. (JRC129019.) 41–42. o. DOI: 10.2760/37899. Online: https://joint-research-centre.ec.europa.eu

[306] Monaghan, Sean (2022): *Deterring Hybrid Threats: Towards a Fifth Wave of Deterrence Theory and Practice.* Helsinki: European Centre of Excellence for Countering Hybrid Threats. (Hybrid CoE Paper 12.) 34. o. Online: https://www.hybridcoe.fi/wp-content/uploads/2022/03/20220331HybridCoEPaper12FifthwaveofdeterrenceWEB.pdf

átfogó megközelítést szükséges alkalmazni. A Communication–Capability–Credibility (3C) pillérrendszer a Híd alatt vált a hibrid elrettentés doktrínájának egyik referenciakeretévé.

Miközben a nyugati információs tér ellenállása az orosz narratívákkal szemben összességében növekedett, a „Multi-aligned Community" – a Globális Dél – egészen más képet mutat. A NATO StratCom COE 2024-es, öt országra (Egyiptom, Mali, Kenya, Dél-Afrika, UAE) kiterjedő jelentése[307] dokumentálja, hogy az RT Arabic 2022 februárja óta tízmillió új felhasználót szerzett, az orosz nagykövetségek közösségimédia-követőinek száma 41%-kal bővült, és a dezinformáció antikolonialista kerete kifejezetten termékeny talajra lelt olyan országokban, ahol a NATO 2011-es líbiai beavatkozásának emlékezete még élénk. A kutatás a Reflexív Kontroll Elmélete[308] alapján három domináns Kreml-narratívát azonosít: az Erő-narratíva a hagyományos értékek védelmére épít; a Megváltás-narratíva vallásos azonosságot kínál; a Szuverenitás-narratíva feltétel nélküli segítséget ígér a nyugati kondicionalitással szemben. Ez a disszertáció Geopolitikai helyzet-dimenziójának egyik legfontosabb empirikus tanulsága: az információs befolyásoló műveletek hatékonysága erősen közönségfüggő változó – ugyanaz az üzenet a befogadó közeg kulturális előfeltevéseihez tapadva válhat hatékonnyá.

A kutatásom forrásfájljai között egyetlen kontrollált kísérlet dokumentálja közvetlenül a katonai személyi állomány információs sebezhetőségét. Bay és Biteniece 2019-ben közölt cikkükben[309] egy szövetséges ország katonai gyakorlatába ágyazott szimulációs kísérletüket mutatják be, amelyet három-négy hetes előkészítés előzött meg. A kutatócsoport személyazonosítás, csali- (honeypot) oldalak és csoportok, social engineering, ismerkedési technikák, személykereső motorok és OSINT-adatbázisok kombinációjával dolgozott. Az eredmények a várakozásokat

---

307 Morley-Davies, Jonathan – Thomas, Jem – Baines, Graham (2024): *Russian Information Operations outside of the Western Information Environment.* Riga: NATO Strategic Communications Centre of Excellence. Online: https://stratcomcoe.org/publications/russian-information-operations-outside-of-the-western-information-environment-revised-version/316

308 Vasara, Antti (2020): *Theory of Reflexive Control: Origins, Evolution and Application in the Framework of Contemporary Russian Military Strategy.* Helsinki: National Defence University. Online: https://www.doria.fi/handle/10024/176978

309 Bay, Sebastian – Biteniece, Nora et al. (2019): The Current Digital Arena and its Risks to Serving Military Personnel. In: *Responding to Cognitive Security Challenges.* Riga: NATO Strategic Communications Centre of Excellence. Online: https://stratcomcoe.org/publications/the-current-digital-arena-and-its-risks-to-serving-military-personnel/102

jelentősen meghaladták: bizonyos egységek összes tagját azonosították, több zászlóalj pontos helyzetét ±1 km pontossággal meghatározták, csapatmozgásokat derítettek fel, és a gyakorlat aktív szakaszának időpontjait is megszerezték. Az Instagram bizonyult a legidőszerűbb információforrásnak; a Facebook az egyének beazonosításához és a kapcsolati háló feltérképezéséhez volt a leghasznosabb (különösen a „javasolt barátok" funkció révén); a Twitter érdemben nem nyújtott hasznos adatot. Különösen figyelemre méltó, hogy a célba vett katonák a social engineering során több információt osztottak meg, mint ami a közösségi média-profiljaikon amúgy is látható volt. A kísérlet konklúziója szerint a személyes információk részletessége lehetővé tette, hogy a gyakorlat során nem kívánatos viselkedést váltsanak ki a célszemélyekből – ez a kontrollált kísérlet közvetlenül validálja a disszertáció Multimodális Reziliencia Mátrixának (MRM) mikroszintjét: a kognitív immunizáció hiánya mérhető sérülékenységet eredményez.[310]

5.3.3. Platform-transzparencia és platform-integritás

A platformok önmaguk által fejlesztett integritási képességei a Híd-időszakban értek el kritikus tömeget – részben a szabályozási nyomás, részben a reputációs kockázat hatására.

A Meta (Facebook) 2018-ban vezette be a Coordinated Inauthentic Behavior (CIB) kategóriát: a koordinált inautentikus viselkedés mint platform-szintű „bizonyítási nyelv" lehetővé tette a szervezettség-proxy azonosítását.[311] A rendszeres takedown jelentések (2018–2021) „kemény" szervezettségi evidenciákat szolgáltattak az IRA, a GRU és más állami kötődésű hálózatok műveleteinek dokumentálásához. A Google Threat Analysis Group (TAG) és a Jigsaw projekt a választási integritás védelmét, az állami kötődésű kampányok azonosítását és a „prebunking" – az előzetes leleplezés – gondolat felépítését kapta feladatul.

Ugyanakkor a Bradshaw és szerzőtársai által dokumentált (Hybrid CoE Working Paper 11)[312] öt platform szabályozási kihívás világossá tette a korlátokat: a legvirálisabb dezinformációt valós

---

310 BAY, Sebastian — BITENIECE, Nora (2019): The Current Digital Arena and its Risks to Serving Military Personnel. In: BERTOLIN, Giorgio (szerk.): Responding to Cognitive Security Challenges. NATO Strategic Communications Centre of Excellence, Riga.

311 Gleicher et al. (2021): *The State of Influence Operations 2017–2020*. Facebook. 9., 12. o. Online: https://about.fb.com/news/2021/05/influence-operations-threat-report/

312 Garcia-Camargo, Isabella – Bradshaw, Samantha (2021): *Disinformation 2.0: Trends for 2021 and Beyond.* Helsinki: European Centre of Excellence for Countering Hybrid Threats. (Hybrid CoE Working Paper 11.) 19. o.

felhasználók terjesztették, nem hamisak; a tartalom nem mindig volt egyértelműen hamis; a terjedés többplatformos volt; az üzleti modell továbbra is az engagement-et jutalmazta; és az AI-fenyegetések még a horizonton voltak. A a szabályok meglétének és végrehajtásának különbsége a Híd-időszak végéig a védekezői oldal strukturális gyengesége maradt.

A platformok moderációs hatékonyságának korlátait a NATO StratCom COE longitudinális kísérletsorozata szemlélteti. Bay, Fredheim és szerzőtársaik (2022)[313] kontrollált módszerrel mérték a fizetett inautentikus részvétel (engagement) terjedési és eltávolítási arányát hat platformon. Eredményük szerint a megvásárolt tartalom 89%-a 24 órán belül megjelent, négy héttel a vásárlás után a tartalmak döntő hányada még mindig aktív volt, és az eltávolítási arány az előző évhez képest csökkent – nem javult. Különösen figyelemreméltó, hogy az orosz–ukrán háborúra válaszul bevezetett Visa-szankciók sem akadályozzák a manipulációs szolgáltatások megvásárlását: az Apple Pay alternatív csatornaként elérhető maradt. Az enforcement gap – a szabályok és a tényleges végrehajtás közötti rés – tehát a Híd-időszak végéig a védekezői oldal strukturális gyengesége maradt, és a T(erítés)-dimenzió kereskedelmi-ipari skálázhatóságát az aktuális platformpolitika érdemben nem korlátozta.

5.3.4. Független hálózatelemzés és tudományos mérés

A Híd-időszak alatt a független kutatóműhelyek – az Oxford Internet Institute (OII), a Stanford Internet Observatory (SIO), a Graphika és a DFRLab – a dezinformáció elemzésének professzionalizálását hajtották végre.

Online: https://www.hybridcoe.fi/wp-content/uploads/2021/07/20210716_Hybrid_CoE_Working_Paper_11_Disinfo_2_0_WEB.pdf

313 Bay et al. (2022): *Social Media Manipulation 2021/2022: Assessing the Ability of Social Media Companies to Combat Platform Manipulation.* Riga: NATO Strategic Communications Centre of Excellence. Online: https://stratcomcoe.org/publications/social-media-manipulation-20212022-assessing-the-ability-of-social-media-companies-to-combat-platform-manipulation/242

Az Oxfor Internet Institute (OII) Global Inventory sorozata (Bradshaw–Bailey–Howard, 2017–2021)[314],[315],[316],[317] a szervezett platform-manipuláció globális kiterjedését számszerűsítette: a sorozat dokumentálta, hogy a szervezett közösségimédia-manipuláció az évtized végére több mint 80 országban volt kimutatható, és a trendek – a fizetett trollok alkalmazásától a bot-hálózatokon át az influencer-kooptálásig – diverzifikálódtak. A SIO a 2016-os amerikai elnökválasztás utáni Internet Research Agency-, azaz IRA-taktika katalógus kidolgozásával, a GRU-hálózatok feltérképezésével és a COVID-narratíva-dinamika elemzésével járult hozzá az ismeretbázishoz. A Graphika a Secondary Infection művelet vizuális hálózatelemzésével, az infodémiás szinkronminták feltárásával és a „super-spreader" (szupterterjesztő) koncentráció kimutatásával a T/M dimenzió mérhetőségét alapozta meg.

Ezek atudományos és szakértői intézmények a Híd-időszak alatt a politikai döntéshozatal közvetlen tájékoztatóivá váltak – az Election Integrity Partnership (EIP) modellje, amely a 2020-as választás valós idejű monitorozását végezte, közvetlen előzménye a 2022-es ukrajnai konfliktusban alkalmazott OSINT-módszereknek.[318]

Az IRA működési logikájának egyik legpontosabb empirikus rekonstrukcióját Kriel és Pavliuc végezte el matematikai hálózatelemzéssel a Defence Strategic Communications folyóiratban 2019-

---

[314] Bradshaw, Samantha – Howard, Philip N. (2017): *Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation.* Working Paper 2017.12. Oxford: Project on Computational Propaganda – Oxford Internet Institute. Online: https://demtech.oii.ox.ac.uk/research/posts/troops-trolls-and-troublemakers-a-global-inventory-of-organized-social-media-manipulation/

[315] Bradshaw, Samantha – Howard, Philip N. (2018): *Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation.* Working Paper 2018.1. Oxford: Project on Computational Propaganda – Oxford Internet Institute. Online: https://demtech.oii.ox.ac.uk/research/posts/challenging-truth-and-trust-a-global-inventory-of-organized-social-media-manipulation/

[316] Bradshaw, Samantha – Howard, Philip N. (2019): *The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation.* Working Paper 2019.2. Oxford: Project on Computational Propaganda – Oxford Internet Institute. Online: https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2019/09/CyberTroop-Report19.pdf

[317] Bradshaw, Samantha – Bailey, Hannah – Howard, Philip N. (2021): *Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation.* Working Paper 2021.1. Oxford: Project on Computational Propaganda – Oxford Internet Institute. Online: https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/127/2021/01/CyberTroop-Report-2020-v.2.pdf

[318] Center for an Informed Public – Digital Forensic Research Lab – Graphika – Stanford Internet Observatory (2021): *The Long Fuse: Misinformation and the 2020 Election.* Stanford: Election Integrity Partnership. Online: https://purl.stanford.edu/tr171zs0069

ben. A szerzők az IRA Twitter-archívumán azonosítani tudták a „mag-csomópontokat" – azokat a hub-fiókokat, amelyek a kampányok irányításáért feleltek –, az injektálás időzítési mintázatait – valós idejű eseménytriggerre reagálva –, és a különböző célközönség-szegmensek eltérő narratívával való kiszolgálásának struktúráját.[319] A kutatás egyik legfontosabb megállapítása, hogy az IRA látszólagos politikai sokszínűsége valójában egyirányú üzenet mögé rendező, tudatos koordináció eredménye volt. Ez a megfigyelés azál-sokszínűség technikájának (Mosás-dimenzió) hálózattudományi igazolása: az IRA nem pusztán narratívákat gyártott, hanem amplifikációs architektúrát működtetett, amelynek hub-struktúrája azonosítható és részlegesen visszafejthető.

5.3.5. OSINT, forenzikus validálás és tényellenőrzés intézményesülése

A Híd-időszak védekezői oldala szempontjából talán a legjelentősebb fejlemény a nyílt forrású hírszerzés (open-source intelligence, OSINT) és a tényellenőrzés intézményesülése volt. A Bellingcat – amely 2014-ben az MH17-es Malaysian Airlines gép lelövésének vizsgálatával szerzett nemzetközi ismertséget – modellt[320] adott az auditálható ellenőrzésre: geolokáció, idővonalas rekonstrukció és nyílt forráskódú képelemzés kombinálásával a szervezet képes volt az állami dezinformáció cáfolatát a hitelesség olyan szintjén előállítani, amely jogi és diplomáciai eljárásokban is felhasználhatónak bizonyult.

A DFRLab (Digital Forensic Research Lab) 2016-tól a Szurkov-leaks feldolgozásával demonstrálta[321], hogy a szivárogtatott dokumentumok szisztematikus elemzése révén az „belső irányítás" – azaz az orosz állami mikromenedzsment a szeparatista mozgalmak felett – auditálhatóvá és bizonyíthatóvá tehető. Ez a módszer – az V(ellen) dimenzió erősítése – a 2022-es konfliktusban alkalmazott hírszerzési transzparencia közvetlen előzménye. A szisztematikus módszertani keretet a Royal United Services Institute (RUSI) 2019-es elemzése mélyítette el, amely a teljes három dokumentumcsomagot egységes forráskritikai apparátussal dolgozta fel, és

[319] KRIEL, Charles – PAVLIUC, Alexa (2019): Reverse Engineering Russian Internet Research Agency Tactics through Network Analysis. Defence Strategic Communications, Vol. 6. NATO Strategic Communications Centre of Excellence, Riga. 17–24. o.

[320] Bellingcat Investigation Team (2015): *MH17: The Open Source Evidence.* Bellingcat, 2015. október 8. Online: https://www.bellingcat.com/news/uk-and-europe/2015/10/08/mh17-the-open-source-evidence/

[321] Digital Forensic Research Lab (2016): Breaking Down the Surkov Leaks. *DFRLab – Atlantic Council,* 2016. október 25. Online: https://medium.com/dfrlab/breaking-down-the-surkov-leaks-b2feec1423cb

elsőként rekonstruálta a Kreml ukrajna-irányítási struktúráját az e-mail-metaadatok, a szervezeti kapcsolathálók és a pénzügyi utalások háromszögelt egybevetésével – ezzel tudományos érvényességgel igazolva a DFRLab korábbi autenticitási megállapításait.[322]

Az International Fact-Checking Network (IFCN/Poynter, 2015-)[323] és az European Digital Media Observatory (EDMO, 2020–2021)[324] a tényellenőrzés standardizálásával és az európai összekötő intézményi keretrendszer kiépítésével a „Single Source of Truth" (SSOT) logika csíráit hozták létre – bár a Híd-időszak végéig ez az ambíció nem valósult meg teljesen.

A Hybrid CoE Research Report 2[325] négy ország (Egyesült Királyság, Svédország, Kanada, Észtország) effektív dezinformáció-elleni állami gyakorlatait vizsgálta effektív dezinformáció-elleni állami gyakorlatait, és több modellértékű megoldást dokumentált. Az Egyesült Királyságban a Department for Digital, Culture, Media and Sport (DCMS) dezinformáció elleni csoportja az online dezinformáció valós idejű monitorozását és a platformokkal való közvetlen együttműködést koordinálta; a brit Kormányzati Kommunikációs Főkapitányság (Government Communications Headquarters, GCHQ)[326] kibervédelmi eszköztárat kapott az oltás-dezinformáció ellen. Svédországban a Myndigheten för samhällsskydd och beredskap (MSB, Polgári Védelmi Hatóság) 2016 óta 16 000 köztisztviselőt képzett ki információs befolyásolás elleni programjában, és 2021 márciusától további 1 200 főt a vakcinációs munka védelmére. Az MSB a Svéd Védelmi Kutatóintézetet (FOI) is megbízta az automatizált közösségimédia-viselkedés értékelésével és az online diskurzus nyomon követésével. Ezek a gyakorlatok azt demonstrálták, hogy a

---

322 Watling, Jack – Reynolds, Nick (2019): *The Surkov Leaks: The Inner Workings of Russia's Hybrid War in Ukraine*. London: Royal United Services Institute. Online: https://static.rusi.org/201907_op_surkov_leaks_web_final.pdf

323 International Fact-Checking Network (2015–): *IFCN Code of Principles.* Poynter Institute, St. Petersburg, FL. Online: https://www.ifcncodeofprinciples.poynter.org/

324 European Digital Media Observatory (2020–): *About EDMO.* Firenze: European University Institute – Európai Bizottság. Online: https://edmo.eu/about-us/edmoeu/

325 Jeangène Vilmer, Jean-Baptiste (2021): *Effective State Practices Against Disinformation: Four Country Case Studies.* Helsinki: European Centre of Excellence for Countering Hybrid Threats. (Hybrid CoE Research Report 2.) 12–13., 21. o. Online: https://www.hybridcoe.fi/wp-content/uploads/2021/07/20210709_Hybrid_CoE_Research_Report_2_Effective_state_practices_against_disinformation_WEB.pdf

326 Fisher, Lucy – Smyth, Chris (2020): GCHQ in cyberwar on anti-vaccine propaganda. *The Times*, 2020. november 9. Online: https://www.thetimes.co.uk/article/gchq-in-cyberwar-on-anti-vaccine-propaganda-mcjgjhmb2

szisztematikus állami kapacitásépítés – képzés, monitoring, kutatásfinanszírozás – operatív ellensúlyt képes teremteni a dezinformációval szemben.

A svéd megközelítés fogalmi sajátossága is figyelmet érdemel. Svédország az „information influence" (informationspåverkan) fogalmát használja, amely a Hybrid CoE Research Report 2[327] definíciója szerint olyan tevékenységeket fed le, amelyek „potenciálisan káros kommunikációs formákat foglalnak magukba, amelyeket külföldi állami szereplők vagy képviselőik szerveznek meg, szándékos beavatkozást jelentenek egy ország belügyeibe az állam és polgárai közötti bizalom megrendítése céljából". Ez a definíció jól illeszkedik a disszertáció G–M–T–V keretéhez: az informationspåverkan-koncepció a Genezés (G) és a Terítés (T) dimenziók célzott kezelésére irányul, miközben a svéd bottom-up intézményi struktúra – kis minisztériumok, erős ügynökségek – a Validálás (V) elleni védekezés decentralizált modelljét testesíti meg.[328]

5.3.6. Leak-alapú bizonyítékcsomagok mint védekezési erőforrás

A Híd-időszak két nagyszabású szivárogtatása – a Szurkov-levelek (2016) és a Vulkan-akták (feltárás: 2023, de a 2014–2022 közötti képességekre visszavetítve) – a védekezői oldal számára kiemelkedő értékű bizonyítékcsomagokat szolgáltatott.

A Szurkov-levelek – amelyeket a Royal United Services Institute (RUSI) Seely és Shandra elemeztek[329] részletesen – az orosz állami mikromenedzsment bizonyítható nyomát adták: a dokumentumok rekonstruálták, hogyan irányította Szurkov prezidenciális tanácsadó személyesen

---

[327] Jeangène Vilmer, Jean-Baptiste (2021): *Effective State Practices Against Disinformation: Four Country Case Studies.* Helsinki: European Centre of Excellence for Countering Hybrid Threats. (Hybrid CoE Research Report 2.) 10. o. Online: https://www.hybridcoe.fi/wp-content/uploads/2021/07/20210709_Hybrid_CoE_Research_Report_2_Effective_state_practices_against_disinformation_WEB.pdf – Az *informationspåverkan* definíciója eredetileg: Pamment, James – Nothhaft, Howard – Fjällhed, Alicia (2018): *Countering Information Influence Activities: A Handbook for Communicators.* Stockholm: MSB. 11. o.

[328] Hybrid CoE Research Report 2 (JEANGÈNE VILMER, Jean-Baptiste, 2021): Effective state practices against disinformation: Four country case studies. European Centre of Excellence for Countering Hybrid Threats, Helsinki. A svéd „information influence" (informationspåverkan) fogalmi definícióját ld. 10. o.: „activities that involve potentially harmful forms of communication orchestrated by foreign state actors or their representatives. They constitute deliberate interference in a country's internal affairs to create a climate of distrust between a state and its citizens."

[329] Shandra, Alya – Seely, Robert (2019): *The Surkov Leaks: The Inner Workings of Russia's Hybrid War in Ukraine.* London: Royal United Services Institute. Online: https://static.rusi.org/201907_op_surkov_leaks_web_final.pdf

a DPR/LPR szeparatista mozgalmak narratíváját, pénzügyi struktúráját és politikai döntéseit. A „helyi" szeparatizmus narratívája mögötti szervezettség ezáltal bizonyíthatóvá vált – ami az L/V dimenzió szempontjából a támadó „mosási" rétegének feltörését jelentette.

A Vulkan-akták – amelyeket a Mandiant/Google Cloud 2023-ban[330] elemzett – belülről tették láthatóvá a kiber–információs műveleti konvergenciát: az NTC Vulkan orosz informatikai vállalat projektjei – köztük az Amesit (pszichológiai műveletek automatizálása, közösségimédia-monitorozás, célpont-profilozás) és a Skan (digitális felderítés és infrastruktúra-térkép) – bizonyították, hogy az orosz állam szoftveres szolgáltatásként (Disinformation-as-a-Service) fejlesztette a dezinformációs képességeit. Bár a Vulkan-akták feltárása 2023-ban történt, az általuk dokumentált képességek a Híd-időszakban épültek ki, és az 5.2 szekció több csomópontjának (különösen 5.2.3 és 5.2.8) technológiai hátterét világítják meg.

A vonatkozó 14. táblázat: REZILIENCIA-összegző tábla címmel a mellékletben található.

5.4. Szintézis: A HÍD mint akció–reakció spirál és a 2022-es invázió előkészítése

A Híd-időszak (2014–2021) nem lineáris fejlődés, hanem akció–reakció spirál volt, amelyben a támadói és védekezői képességek kölcsönösen katalizálták egymás fejlődését. E spirál megértése nélkül a 2022-es ukrajnai információs konfliktus kimenetele – amely a 4. fejezetben tárgyalt 2014-es krími meglepetéstől fundamentálisan eltér – értelmezhetetlen.

A spirál doktrinális sarokköve a kognitív fárasztás stratégiája: a Híd-időszak alatt az orosz információs befolyásoló művelet-modell fokozatosan átállt a 2014-es koherens meggyőzési logikáról (egyetlen, hiteles narratíva sulykolása) a célközönség kognitív kapacitásának kimerítésére. A Szurkov-leakek és a Vulkan-akták együttesen dokumentálják, hogyan intézményesítette az orosz állam ezt az átállást: a Szurkov-dokumentumok megmutatják, hogy a narratív mikromenedzsment már 2014-ben sem a meggyőzést, hanem a konfúziót célozta meg a donbaszi közvéleményen belül; a Vulkan szoftverrendszerek (különösen az Amesit pszichológiai műveleti modul) pedig azt rögzítik, hogy a fárasztás automatizálható ipari kapacitássá vált. Ez a fokozat -- a kézműves narratív káosztól az automatizált érzelmi kimerítésig -- a 2022-es totális

[330] Mandiant (2023): *Cyber Operations and Disinformation: Analysis of NTC Vulkan Projects Scan, Amesit, and Krystal-2B.* Google Cloud – Mandiant, 2023. március 30. Online: https://www.mandiant.com/resources/blog/cyber-operations-russian-vulkan

információs agresszió közvetlen előkészítő fázisa volt: 2022. február 24-én az orosz információs befolyásoló művelet nem meglepetésszerű narratív csapást mért, hanem egy hét éve folyamatosan gyengített kognitív immunrendszerű közönségre indított totális kampányt.

A támadói oldal (Anchor) a Híd végére a következő képességeket építette ki:

A tartalomelőállítás (G) terén a kézműves trollfarmok mellé lépett az automatizáció imperatívusza: a Vulkan-akták által dokumentált szoftverrendszerek, a GAN-alapú profilképek és a korai generatív szöveges eszközök a tartalom előállítás költségét radikálisan csökkentették. A mosás (L) terén a perszóna-portfólió-menedzsment, a dokumentum-mimikri és a hack-and-leak pipeline a hitelesítő rétegek kifinomult rendszerét hozta létre. A terítés (D) terén a platform-architektúra kihasználása (algoritmikus amplifikáció, format-first stratégia) és a nyílt→zárt csatorna-váltás a terjesztés skálázhatóságát és nyomon követhetetlenségét egyaránt növelte. A validálás (V) terén a „bizonyíték-érzet" (proof-feeling) tömegesítése, a szakértő-proxy iparosodása és a memetikus formátumok a hitelesítő rétegek új generációját hozták létre.

A védekezői oldal (Reziliencia) a Híd végére a következő pozíciót érte el:

Az intézményi oldalon az EU szabályozási lépcsők (Action Plan → Code of Practice → EDAP → DSA felé vezető út), a NATO StratCom COE és a Hybrid CoE diagnosztikai munkája, valamint az olyan állami gyakorlatok, mint a svéd MSB 16 000 köztisztviselőt érintő képzési programja és a brit DCMS Counter-Disinformation Unit, a szisztematikus állami kapacitásépítés modelljeit hozták létre. A platform-integritás terén a CIB-kategória, a takedown jelentések és a prebunking gondolat a korábbihoz képest lényegesen fejlettebb – bár továbbra is korlátozott – védekezői eszköztárat adott. Az OSINT és tényellenőrzés intézményesülése – a Bellingcat, a DFRLab, az IFCN/EDMO – az ellen-validálás képességét (V(ellen)) minőségileg más szintre emelte.

Ami 2022 februárjára készen állt:

Az OSINT-közösség és a tényellenőrző hálózatok képesek voltak a dezinformáció gyors azonosítására és cáfolatára. A platformok – legalábbis a nagyok – rendelkeztek CIB-azonosítási képességgel. Az EU és a NATO intézményi keretek álltak a dezinformáció kezeléséhez. Az ukrán állam – ahogy a Hybrid CoE Research Report 11-ban Kalenský–Osadchuk 2024-ben

dokumentálta[331] – saját dezinformáció-elleni képességeket épített ki, beleértve a monitoring-rendszereket, a stratégiai kommunikációs kapacitást és a humor mint védekezési eszköz szisztematikus alkalmazását.

Ami 2022 februárjára nem állt készen:

A zárt csatornák (különösen a Telegram) moderálása és monitorozása továbbra is megoldatlan maradt. A generatív AI operatív bevetése – amely a NATO StratCom COE 2024-es Robotrolling elemzése szerint 2023–2024-re vált valósággá – még nem indult el, de a védekezői oldal sem készült fel rá. A „narratíva-csatorna-újrafelhasználás" – a COVID-dezinformációs hálózatok zökkenőmentes átállása Ukrajna-narratívákra – megmutatta, hogy a platformoknak és a tényellenőrzőknek nem csupán tartalommal, hanem infrastruktúrával kell szembenézniük. És végül: atéves helyzetfelmérés – amelyet a Hybrid CoE Research Report 11-ben Burkovszkij idézett kutatása dokumentált, miszerint az ukránok 46%-a nem számított háborúra, további 29%-a pedig hitt benne, de nem akarta elhinni – a társadalmi reziliencia korlátait is megmutatta.

A Hybrid CoE Paper 24[332] – a legfrissebb elméleti összefoglalás a projekt-anyagok között – arra mutat rá, hogy a társadalmi identitások kiaknázása a dezinformáció céljaira a Híd-időszak egyik leghatékonyabb és legnehezebben kivédhető taktikája volt. A svédországi Korán-égetési események és az ahhoz kapcsolódó külföldi befolyásolási kampány, amely átmenetileg megakasztotta Svédország NATO-csatlakozási folyamatát, jól szemlélteti, hogyan képes egy identitásalapú sérülékenység kihasználása a legmagasabb szintű biztonsági döntéseket is befolyásolni.

A Hybrid CoE Working Paper 22 (2023) a populizmus és a hibrid fenyegetések összefüggéseit elemezve hasonló következtetésre jutott: a populista logika – amely a „nép" és az „elit" szembeállítására épül – strukturálisan megkönnyíti a hibrid fenyegetési aktorok számára a

[331] Kalenský, Jakub – Osadchuk, Roman (2024): *How Ukraine Fights Russian Disinformation: Beehive vs Mammoth.* Helsinki: European Centre of Excellence for Countering Hybrid Threats. (Hybrid CoE Research Report 11.) 26., 30–31. o. Online: https://www.hybridcoe.fi/wp-content/uploads/2024/01/20240124-Hybrid-CoE-Research-Report-11-How-UKR-fights-RUS-disinfo-WEB.pdf

[332] Hedling, Elsa (2025): *Social Identities and Democratic Vulnerabilities: Learning from Examples of Targeted Disinformation.* Helsinki: European Centre of Excellence for Countering Hybrid Threats. (Hybrid CoE Paper 24.) 20–22. o. Online: https://www.hybridcoe.fi/wp-content/uploads/2025/04/20250415Hybrid_CoE_Paper24WEB.pdf

demokratikus normák erodálását és a társadalmi megosztottság kihasználását. A digitális közösségi média platformok affordanciái – az érzelmi tartalom jutalmazása, az algoritmikus amplifikáció, a szűrőbuborékok – természetes szövetségesei ennek a logikának.

A 6. Fejezetben kifejtem, hogya 2022. február 24-i teljes körű inváziő az a pillanat, amikor a Híd alatt felépült képességek – mind a támadói, mind a védekezői oldalon – élesben futottak. A 4. fejezetben tárgyalt 2014-es krími meglepetés „kézi vezérlésű precizitásával" szemben a 2022-es konfliktus az „ipari léptékű kognitív hadviselés" – a multimodális terítés, a gyors narratíva-csere, a false-flag jelleg, a dokumentum-mimikri, a zárt csatornák „érlelő" szerepe és az OSINT/tényellenőrző verseny a validálási időért – korát nyitotta meg. Ezt a korszakot tárgyalja a következő fejezet.

6. A KOGNITÍV HADVISELÉS IPAROSÍTÁSA: A STRATÉGIAI FIGYELMEZTETÉSTŐL A KOGNITÍV NIHILIZMUSIG (UKRAJNA, 2022–2025)

A 2022. február 24-én megindított orosz inváziő Ukrajna ellen nem csupán a konvencionális hadviselés visszatérését jelentette Európába, hanem az információs műveletek történetének legnagyobb léptékű, iparosított összecsapását is. Ez az iparosítás a generatív mesterséges intelligencia (GenAI) által előállított tartalmak tömeges és automatizált terjesztésén alapul, ami minőségileg új fenyegetést jelent a társadalmi bizalomra és a kritikus infrastruktúrák biztonságára nézve. A 4. fejezetben dokumentált 2014-es krími sebészeti pontosságú művelettel szemben a 2022–2025-ös időszak a kognitív tömegtermelés korszaka. Ebben a fázisban az információs környezetszennyezés olyan mértéket ölt, amely már nem csupán egyes narratívák megváltoztatását, hanem a közös valóságérzékelés szisztematikus erodálását célozza. A GenAI kettős természetét – fenyegetés és védelmi lehetőség egyaránt – Bányász, Szádeczky és Váczi elemezték: a generatív modellekre épülő phishing-támadások és LLM-generált dezinformáció megkerülik a hagyományos biztonsági szűrőket, miközben ugyanezek a technológiák az anomália detekció és a tartalomhitelesítés terén is alkalmazhatók[333]

[333] BÁNYÁSZ Péter – SZÁDECZKY Tamás – VÁCZI Kincső B. (2024): *The relationship between generative artificial intelligence and cybersecurity.* In CEEeGov 2024. New York: ACM. DOI: 10.1145/3670243.3670781.

Jelen fejezet célja, hogy a H–E–I (Helyzet–Előrejelzés–Irányítás) diagnosztikai mátrix segítségével elemezze a konfliktus evolúcióját, és az 5. fejezetben alkalmazott G–M–T–V műveleti lánc (Generálás–Mosás–Terítés–Validálás) keretében rögzítse a 2022–2025-ös végállapotot – azt a konfigurációt, amelyhez az 5. fejezet Anchor- és Reziliencia-mérföldkövei elvezettek. A vizsgálat nem áll meg a háború kitörésének pillanatánál, hanem végigköveti a dinamikát a 2022-es információs villámháború (Blitzkrieg) kudarcától a 2024–2025-re jellemző kognitív felőrlő háborúig (Cognitive War of Attrition). A fejezet záró harmadában a 4. fejezet MRM-sarokpont logikáját követve elkészíti a 2022–2025-ös kontroll-leltárt, ezzel lehetővé téve, hogy a 7. fejezet (Keresztmetszeti összehasonlítás) azonos indikátorkosárban szintetizálja a két esetet.

6.1. Elemzési keret és a vizsgálati keret rögzítése

6.1.1. A vizsgálati keret és a kódolási logika (SFÖ + trianguláció)

A 2. fejezetben rögzített módszertani elvek szerint a 6. fejezet az SFÖ azonos kérdéssora mentén elemzi a 2022–2025-ös konfliktust, lehetővé téve a kontrollált összehasonlítást a 4. fejezettel. A vizsgálati ablak öt fázist ölel fel: (1) az invázió kognitív előkészítése (2021 nyara – 2022. február 23.); (2) a villámháborús fázis kudarca (2022. február 24. – április); (3) az információs állóháború (2022 nyara – 2023 vége); (4) a választási manipuláció éve (2024); és (5) a kognitív felőrlő háború (2025).

A forráshierarchia azonos a 4. fejezetben alkalmazottal: (1) intézményi stratégiai jelentések (Hybrid CoE, NATO StratCom COE, EEAS FIMI-jelentések); (2) független kutatói esettanulmányok (DFRLab, Bellingcat, Stanford Internet Observatory); (3) platform-transzparencia jelentések (Meta CIB, Google TAG); (4) forráskritikával kezelt szivárogtatások és nyílt forrású hírszerzési elemzések. A trianguláció elve változatlanul érvényes: egyetlen állítás sem kerül a szövegbe, amely ne támaszkodna legalább két független forrástípusra.

Fontos módszertani megjegyzés: míg a 4. fejezetben a Krím 2014 esetét visszatekintve, immár lezárt eseményként lehetett elemezni, a 6. fejezet tárgyidőszaka (2022–2025) részben még folyamatban van. Ez a valós idejű analízis erősségeket és korlátokat egyaránt jelent. Erőssége, hogy a platform-transzparencia és az OSINT-infrastruktúra a 2014-esnél nagyságrendekkel jobb adathozzáférést biztosít. Korlátja, hogy az attribúciós lánc egyes elemei – különösen a szervezeti

irányítás és a stratégiai szándék kérdésében – még nem stabilizálódtak. A fejezet ott, ahol az evidenciabázis még nem zárt, ezt explicit módon jelzi.

6.1.2. 2021–2022-es előjelek: a kognitív felkészülés és a stratégiai vakság

A 4. fejezet 4.1.2 alfejezetéhez hasonlóan szükséges rögzíteni a 2022-es konfiguráció közvetlen előzményeit. Az invázió kognitív előkészítése két, egymással ellentétes folyamat jegyében zajlott: a nyugati hírszerzés példátlan nyíltsága és az orosz vezetés doktrinális vaksága.

A támadó oldalon a Hybrid CoE Paper 20-ban Kubica dokumentálja[334], hogy az orosz vezetés a saját propagandájának foglyává vált. Putyin 2021. júliusi esszéje[335] („Az oroszok és ukránok történelmi egységéről") nemcsak kommunikációs panel volt, hanem a hadműveleti tervezés kiindulópontja: az a feltevés, miszerint Ukrajna nem valódi állam és az ukrán nemzeti identitás mesterséges képződmény, közvetlenül meghatározta az invázió tervezett lefolyását – a gyors rezsimváltás és a minimális ellenállás forgatókönyvét. Az OxIPO-modell (ld. 2.5) keretében ez klasszikus Input-hiba: mivel a bemeneti adatok (az FSZB által szűrt, felfelé torzított jelentések) a valóságot hamisították meg, a feldolgozás (Process) szükségszerűen hibás kimenetet (Output) produkált – olyan narratívákat (Zelenszkij elmenekült, nácítlanítás), amelyek nem rezonáltak a valósággal szembesülő ukrán lakosságnál. A reflexív kontroll – amelynek lényege az ellenség önkéntes döntési autonómiájának megzavarása – összeomlott, mert az oroszok által elképzelt célpont a valóságban nem létezett; helyette egy öntudatos, horizontálisan szerveződő nemzettel találták szemben magukat.

A védekező oldalon megvalósult a sikeres előzetes leleplezés (pre-bunking): az amerikai és brit hírszerzés hetekkel a támadás előtt nyilvánosságra hozták a csapatösszevonások műholdképeit és a tervezett orosz hamis zászlós műveletek forgatókönyveit. Ez a hírszerzési transzparencia-stratégia a Validálás (V) dimenzió ellen-validálási képességének történelmi áttörése volt: a védekező fél először a történelemben a támadó előtt validálta a helyzetet. A Hybrid CoE Research

---

[334] Kubica, Lucjan (2024): *Ukraine's Position in Russia's Strategic Thinking: Domestic, Regional and International Order*. Helsinki: The European Centre of Excellence for Countering Hybrid Threats. Online: https://www.hybridcoe.fi/publications/hybrid-coe-paper-20-ukraines-position-in-russias-strategic-thinking-domestic-regional-and-international-order/

[335] Putyin, Vlagyimir (2021): Az oroszok és az ukránok történelmi egységéről. *Kremlin.ru*, 2021. július 12. Online: http://en.kremlin.ru/events/president/news/66181

Report 11[336] dokumentálja, hogy az ukrán dezinformáció-elleni szakértők tudatosan alkalmazták ezt a stratégiát. Az ukrán külügyminisztériumi tanácsadó beszámolója szerint az ukrán fél a legmargimálisabb orosz hamis zászlós narratívát is cáfolta, mert a cáfolat elmaradásának kockázata jóval nagyobb volt, mint a véletlenül felhívott figyelem – szemben a 2014-es krími helyzettel, ahol ilyen proaktív kommunikációs stratégia nem létezett.

Ugyanakkor az assessment bias jelensége arra figyelmeztet, hogy a társadalmi reziliencia nem csak az intézményi felkészültségtől függ. A Hybrid CoE Research Report 11 egy 2023-as felmérésre hivatkozva dokumentálja, hogy az ukrán lakosság 46%-a nem számított háborúra, további 29%-a számított rá, de nem akarta elhinni, hogy megtörténik. Ez az adat a kognitív elkerülés (cognitive avoidance) jelenségét illusztrálja: a legmagasabb szintű fenyegetések ellen is hatékony pszichológiai védelmi mechanizmus, amely a döntéshozatal paralízisét nem intézményi, hanem egyéni szinten okozza.

6.2. HELYZET-DIMENZIÓ (Situation): Az iparosított kognitív hadviselés korszaka

A H–E–I mátrix Helyzet-oszlopa – amelyet a 4. fejezetben az FMK-rács logikája mentén operacionalizáltunk – a vizsgált időszakban (2022–2025) két radikális átalakuláson ment keresztül. A 4.2 alfejezetben a 2014-es Helyzet-dimenziót három alpillér mentén vizsgáltuk: narratív koherencia, csatorna-szinkronizáció, volumen és amplifikáció. Ugyanezt a struktúrát alkalmazom a 2022–2025-ös konfigurációra, kiegészítve a nem-állami szereplők átalakulásával és a fizikai-kognitív konvergenciával, amelyek 2014-ben még nem léteztek ebben a formában.

6.2.1. Narratív (in)koherencia: A káosztól a fárasztásig

A 4.2.1 alfejezetben rögzítettem, hogy a 2014-es krími művelet narratív fegyelme példátlan volt: egyetlen, koherens keretezés (a Krím „hazatérése") végigterjedt az összes csatornán, és ez a koherencia volt az egyik legfontosabb sikertényező. A 2022-es konfiguráció ennek pontos ellentéte volt.

[336] Kalenský, Jakub – Osadchuk, Roman (2024): *How Ukraine Fights Russian Disinformation: Beehive vs Mammoth.* Helsinki: European Centre of Excellence for Countering Hybrid Threats. (Hybrid CoE Research Report 11.) 26., 30–31. o. Online: https://www.hybridcoe.fi/wp-content/uploads/2024/01/20240124-Hybrid-CoE-Research-Report-11-How-UKR-fights-RUS-disinfo-WEB.pdf

Az invázió kezdetén az orosz stratégiai kommunikáció elveszítette a 2014-ben tapasztalt fegyelmezettségét. Putyin „nácítlanítás” fogalma nemzetközi szinten értelmezhetetlennek bizonyult, ami kényszerpályára állította a propagandát. A narratívák gyors cserélődése – a biolaboroktól a „sátánisták elleni szakrális harcig”, majd az „Ukrajna nem létező állam” tézisig – a hitelesség eróziójához vezetett. A Hybrid CoE Paper 20 elemzése szerint Oroszország „információs offenzívája” a háború első hónapjaiban inkább a belső közönséget célozta – a bűnrészesség kommunikálásával biztosítva az orosz társadalom konszenzusát –, miközben a nemzetközi arénában a narratívák szétestek.

A Hybrid CoE Working Paper 29[337] (2024) az orosz dezinformáció mérhető hatásait vizsgálva kimutatta, hogy a narratívák elterjedésének három kulcsindikátora van: (a) a narratíva-ismétlés mértéke véleményvezérek által; (b) a közvélemény-kutatási adatok; és (c) a kézzel fogható viselkedési hatások. Mindhárom dimenzióban kimutatható hatást talált. Az „információs áttörés” (cross-medium breakout) jelensége – amikor a dezinformációs művelet olyan hatást ér el, hogy a mainstream média maga kezdi közvetíteni (amit Ben Nimmo „celebrity amplification”-nek nevez) – a 2022–2023-as időszakban többször is megvalósult, különösen a fegyverszállítások és az eszkalációs kockázat témájában. Az Egyesült Államokban republikánus kongresszusi képviselők ismételték a Kreml-narratívákat a NATO-ról és Ukrajnáról; Európában a populista politikusok a „béke vs. eszkaláció” keretezést vették át

2024–2025-re Oroszország stratégiát váltott. A kaotikus üzeneteket felváltotta egyetlen, érzelmileg hatékony keretezés: a háborús fáradtság (war fatigue) kommunikációs fegyverként való használata. A dezinformációs hálózatok már nem a háború jogosságáról próbálták meggyőzni a nyugati közvéleményt, hanem a demobilizáció volt a cél: „Minden további támogatás csak a világháború kockázatát növeli.” A G–M–T–V lánc szempontjából ez a Mosás (M) dimenzió felértékelődése: a „békepárti” keretezés a leghatékonyabb mosási réteg, mert a célközönség saját értékrendjébe (háborúellenesség) ágyazza az orosz stratégiai célt (az ukrán ellenállás megtörése). A Hybrid CoE

[337] Hoyle, Aiden – Šlerka, Josef (2024): *Cause for Concern: The Continuing Success and Impact of Kremlin Disinformation Campaigns.* Helsinki: European Centre of Excellence for Countering Hybrid Threats. (Hybrid CoE Working Paper 29.) 11., 14., 17. o. Online: https://www.hybridcoe.fi/wp-content/uploads/2024/03/20240306HybridCoEWorkingPaper29TheimpactofKremlindisinformationWEB.pdf – A „celebrity amplification" fogalmát ld. Ben Nimmo: *The Breakout Scale: Measuring the Impact of Influence Operations.* Brookings Foreign Policy, 2020. 7. o. A háromindikátoros keretrendszer: 11. o.; cross-medium breakout: 14. o.; közvélemény-kutatási adatok: 17. o.

Working Paper 22[338] elemzése szerint a populista logika – a „nép vs. elit" dichotómia – strukturálisan megkönnyíti ezt a demobilizációs stratégiát: az „elit háborúja" keretezés a háborúfáradtságot a demokratikus intézményekbe vetett bizalomvesztéssel kapcsolja össze.

6.2.2. Csatorna-szinkronizáció: Multimodális, multiplatform architektúra

A 4.2.2 alfejezetben dokumentáltam, hogy 2014-ben a csatorna-szinkronizáció a „hibrid médiarendszer" logikáját követte: az állami média (RT, Sputnik) generálta a narratívát, a közösségi média amplifikálta, majd a mainstream média visszahivatkozott. 2022-re ez a séma radikálisan komplexebbé vált.

A csatornakonfiguráció 2022-ben négy rétegű volt. Az első réteg az állami médiarendszer – amelynek EU-s tiltása (RT/Sputnik, 2022. március 2.) volt az első jogi precedens. Az ISD 2022-es Effectiveness of the Sanctions on Russian State-Affiliated Media in the EU: An Investigation into Website Traffic and Possible Circumvention Methods című elemzése[339] szerint a tiltás átlagosan 74%-os forgalomcsökkenést okozott a Rosszija Szegodnya weboldalain, egyes országokban 90%-os visszaesést. A második réteg a proxy weboldalak és klónoldalak – a Doppelgänger-művelet, amelyet az alábbiakban részletesen tárgyalok. A harmadik réteg a zárt csatornák (Telegram, VKontakte, zárt Facebook-csoportok), ahol a moderáció gyakorlatilag nem létezett. A NATO StratCom COE Robotrolling 2023–2024 elemzése[340] empirikusan dokumentálta: a 17 azonosított koordinált csoport 53%-a a Telegramon volt aktív, egyetlen hálózat 130 Telegram-csatornát és 13 weboldalt üzemeltetett. A negyedik réteg a fizikai hatáscsatornák – a Telegramon toborzott

---

338 Lebrun, Maxime (2023): *Watching Out for Populism: Authoritarian Logics as a Vulnerability to Hybrid Threat Activity.* Helsinki: European Centre of Excellence for Countering Hybrid Threats. (Hybrid CoE Working Paper 22.) 8., 10., 16. o. Online: https://www.hybridcoe.fi/wp-content/uploads/2023/01/20230123HybridCoEWorkingPaper22PopulismWEB.pdf

339 **Balint et al. (2022):** *Effectiveness of the Sanctions on Russian State-Affiliated Media in the EU: An Investigation into Website Traffic and Possible Circumvention Methods.* London: ISD Global, 2022. október 6. Online: https://www.isdglobal.org/isd-publications/effectiveness-of-the-sanctions-on-russian-state-affiliated-media-in-the-eu-an-investigation-into-website-traffic-possible-circumvention-methods-2/

340 **Fredheim, Rolf (2024):** *Virtual Manipulation Brief 2024/1: Hijacking Reality – The Increased Role of Generative AI in Russian Propaganda.* Riga: NATO Strategic Communications Centre of Excellence. Online: https://stratcomcoe.org/publications/virtual-manipulation-brief-20241-hijacking-reality-the-increased-role-of-generative-ai-in-russian-propaganda/307

amatőrök által végrehajtott szabotázsakcióktól a GPS-zavarásig –, amelyek a kognitív és kinetikus dimenzió összeolvadását jelzik.

A G–M–T–V lánc Terítés (T) dimenziójában ez a négy rétegű architektúra a 2014-es koordinált humán hálózatnál nagyságrendekkel komplexebb: a támadó egyszerre tud nyílt (állami média), félig nyílt (proxy oldalak), zárt (Telegram) és fizikai (szabotázs) csatornákon operálni, és a platformtiltás csak az első réteget érinti.

A fenti négyrétegű architektúra működését esettanulmány-szinten dokumentálja a NATO StratCom COE „War on All Fronts" című kutatása (Daukšas et al., 2024),[341] amely hat konkrét incidens – a Győzelem napja, a szankciók, a mozgósítás, a Nord Stream, a kercsi híd és az annexációs népszavazások – média visszhangjainak összevetésével mutatja ki: a Telegram–televízió–hivatalos kommunikáció szinkronizációja összefüggő rendszerként működik. A tervezhető események során (Győzelem napja, szankciós válasz) a TV-narratíva és a Telegram-csatornák üzenetei szinte percnyi pontossággal illeszkedtek; a meglepetésszerű válságok esetében (mozgósítás, kercsi híd) a Telegram-reakció megelőzte a TV-réakciót, jelezve a szinkronizációs mechanizmus reaktívvá válását válságkezelés során. A szerzők ezt a mintát „kommunikációs rezsim"-nek nevezik: a Kreml tudatosan demonopolizálja a Telegram-teret – megengedve a milbloggerek és Z-csatornák részleges autonómiáját –, miközben a televízión teljes kontrollt tart fenn. Ez az ún. „szabályozott káosz" a rugalmasságot biztosítja, mert a Telegram-csatornák képesek gyorsabban reagálni a váratlan eseményekre, mint az állami televízió.[342] Az FMK-rács „csatorna" oszlopában ez a kommunikációs rezsim-modell pontosan a négyrétegű architektúra dinamikáját magyarázza: a rétegek nem statikusan működnek, hanem az esemény típusától függően váltakozó szinkronizációs mintázatot mutatnak.

[341] DAUKŠAS, Vytautas et al. (2024): War on All Fronts: Russia's Television and Online Warfare Against Ukraine. NATO Strategic Communications Centre of Excellence (NATO StratCom COE), Riga.

[342] Uo. 83–90. o. („Communication regime" modell).

6.2.3. Volumen és amplifikáció: Ipari botnetek és generatív MI

A 4.2.[343]3 alfejezetben dokumentáltam, hogy 2014-ben a trollfarm-műveletek „kézivezérlésű hálózati hangosításon" alapultak: az IRA munkatársai egyenként írtak posztokat, a koordináció személyes irányításon múlt.[344] 2022–2025-re ez a modell ipari léptékű automatizációvá vált. Marcellino és szerzőtársai 2023-ban ezt a transzformációt a „Social Media Manipulation 3.0" korszakként azonosították: a szintézis megmutatja, hogy a GenAI-alapú manipulációs infrastruktúra – kínai astroturfing-példákon bemutatva – az orosz és a kínai műveleti környezetben párhuzamosan épült ki, ami a jelenség ipari, globális léptékét igazolja.[345]

A G–M–T–V lánc Generálás (G) dimenziója négy szakaszon ment keresztül:

2022 – a mennyiség kora: A NATO StratCom COE Robotrolling elemzései szerint a háború kezdetén a botnetek aránya egyes platformokon elérte a 90%-ot, de ezek főleg alacsony komplexitású szöveges üzeneteket terjesztettek. A stratégia alapja a PAUL–MATTHEWS (2016) által leírt „tűzoltótömlő" (Firehose of Falsehood) modell: nagy mennyiség, több csatorna, nincs igény a belső konzisztenciára.

2023 – az iparosítás kora: A nagy nyelvi modellek (LLM-ek) integrációja a dezinformációs munkafolyamatokba. A Robotrolling 2023–2024 elemzés empirikusan dokumentálta: a 344 vizsgált forrás között teljesen automatizált, LLM-alapú hálózatokat is találtak, amelyek weboldalakat szedtek szét és politikai híreket posztoltak újra, gyakran „MI-hallucinációkkal" –

---

[343] NATO STRATCOM COE — OSAVUL (2024): *Virtual Manipulation Brief 2024/1: Hijacking Reality — The Increased Role of Generative AI in Russian Propaganda*. NATO Strategic Communications Centre of Excellence, Riga, ISBN 978-9934-619-66-3. 3., 14. o. A kutatás 17 koordinált csoportot azonosított 344 forrásra; az LLM-alapú automatizált kommentek aránya a NATO-tematikájú posztok alatt: angol X-en ~7%, orosz X-en ~15%, VKontakten ~38%.

[344] BERGMANIS-KORĀTS, Gundars — VECMANIS, Raitis Ralfs — ISUPOVA, Marija — SAKURAI, Kensho (2025): *Virtual Manipulation Brief 2025*. NATO Strategic Communications Centre of Excellence, Riga, ISBN 978-9934-619-43-4. A legújabb VMB 10 platformra terjesztette ki az elemzést (beleértve a Threads-t és a BlueSky-t); a Telegram pénzügyi ösztönzői (monetizáció) új motivációs rendszert teremtenek a manipuláció számára; 11 millió poszt elemzése.

[345] MARCELLINO, William – BEAUCHAMP-MUSTAFAGA, Nathan – KERRIGAN, Amanda – NAVARRE CHAO, Lev – SMITH, Jackson (2023): The Rise of Generative AI and the Coming Era of Social Media Manipulation 3.0: Next-Generation Chinese Astroturfing and Coping with Ubiquitous AI. RAND Corporation, PE-A2679-1. A szerzők a generálás, a terjedés és a detekció három dimenzijában vizsgálják a Social Media Manipulation 3.0 korszakát, kínai példákon bemutatva a GenAI-alapú astroturfing ipari léptékű megvalósítását.

azaz kitalált tényeket tartalmazó szövegekkel. A NATO-hoz kapcsolódó automatizált kommentek aránya az angol nyelvű Twitter(X)-en mintegy 7%-ot, az orosz nyelvűn mintegy 15%-ot, a VKontaktén mintegy 38%-ot ért el. A NATO StratCom COE AI in Support of StratCom Capabilities elemzése[346] megerősítette, hogy az LLM-ek a 2023–2024-es időszakban váltak ténylegesen bevetett eszközzé az információs fenyegetésekben.

Ezt az összefüggést – hogy az MI-integráció nem spontán, hanem stratégiai döntés eredményeként jelent meg – egy másik, független forrás is megerősíti, tovább erősítve az előző megállapítást. Wallner, Copeland és Giustozzi [347] – „Russia, AI and the Future of Disinformation Warfare" című tanulmányukban – dokumentálják, hogy Oroszország 2019-es nemzeti MI-stratégiája expressis verbis 2030-ra tűzte ki a globális AI-vezető szerepet, és az állami vállalatok (Sberbank GigaChat, Rostec) már a dezinformációs munkafolyamatokba is beépítik a generatív eszközöket. A Doppelgänger-kampány MI-generált, legitim nyugati hírportálokat imitáló cikkei ennek dokumentált operatív megnyilvánulásai.

2024 – a multimodális interferencia kora: A választások éve világszerte (több mint 60 ország), ahol megjelentek a deepfake audio kampányok. A szlovákiai parlamenti választási dezinformáció során MI-generált hangüzenetekkel operáltak; a moldovai elnökválasztás előtti kampányban a Doppelgänger-hálózat[348] többnyelvű deepfake-ekkel igyekezett a jelölteket diszkreditálni. A

[346] Bergmanis-Korāts et al. (2024): *AI in Support of StratCom Capabilities.* Riga: NATO Strategic Communications Centre of Excellence. Online: https://stratcomcoe.org/publications/ai-in-support-of-stratcom-capabilities/296

[347] WALLNER, Claudia – COPELAND, Simon – GIUSTOZZI, Antonio (2025): Russia, AI and the Future of Disinformation Warfare. Emerging Insights. Royal United Services Institute (RUSI), London.

[348] Volāns et al. (2025): *Handbook on the Role of Non-State Actors in Russian Hybrid Threats*. Helsinki: European Centre of Excellence for Countering Hybrid Threats. Online: https://www.hybridcoe.fi/wp-content/uploads/2025/12/Hybrid-CoE-Paper-27-Handbook-on-the-role-of-non-state-actors-in-Russian-hybrid-threats.pdf

Hybrid CoE Paper egyes részei[349], [350] már a Híd-időszakban előre jelezte[351] ezt a fejleményt, de a tényleges műveleti bevetés csak 2024-re vált szisztematikussá.

2025 – a minőség kora: A generatív videómodellek megjelenése elhozta a hiperrealizmus korszakát, ahol a szintetikus tartalom vizuálisan nem diagnosztizálható hagyományos módszerekkel. A kognitív nihilizmus fogalma itt válik műveleti realitássá: nem az a cél, hogy az emberek elhiggyenek egy konkrét hazugságot, hanem hogy ne higgyenek többé az igazság létezésében. A hazug osztaléka (Liar's Dividend) elvének maximalizálása: ha az igazság megkülönböztethetetlen a hazugságtól, a társadalom morális közönybe süllyed.

A FMK Kognitív Olló modell szempontjából kiemelkedő jelentőségű a NATO StratCom COE évente ismételt, azonos módszertannal végzett szimulációs kísérletsorozata, amely 2018 óta empirikus idősort képez a közösségi média manipuláció költségéről és hatékonyságáról. A módszertan minden évben azonos: a kutatók orosz manipulációs szolgáltatóktól vásárolnak egy standard kosárnyi hamis interakciót, mérik a kézbesítési sebességet, majd négy héten át monitorizálják a platformok detektálási és eltávolítási képességét. Az adatsor kulcsmegállapításai: 2020-ban 300 euróból 337 768 hamis interakciót vásároltak, amelyek több mint 98 százaléka négy hét után is aktív maradt; 2024-ben 58 euróból több mint 24 000 hamis interakciót szereztek hat platformon, amelyek közül egyik sem volt képes a hamis kedveléseket felismerni; 2025-ben 252 euróból 99 045 hamis interakciót vásároltak hét platformon (első alkalommal a Bluesky-t is tesztelve), és 30 011 egyedi hamis fiókot azonosítottak, a Facebook esetében a megrendelt kommentmennyiség 340 százaléka érkezett meg 72 órán belül. A longitudinális ártrend egyértelmű: a manipulációs kosár ára 2018 és 2025 között nem emelkedett szignifikánsan, a platformok között konvergált – ami arra utal, hogy a platformok védekezése nem tette érdemben

---

[349] Mazzucchi, Nicolas (2022): *AI-based Technologies and Their Use as a Weapon of Hybrid Warfare*. Helsinki: European Centre of Excellence for Countering Hybrid Threats. Online: www.hybridcoe.fi/wp-content/uploads/2022/06/20220623-Hybrid-CoE-Paper-14-AI-based-technologies-WEB.pdf

[350] Hybrid CoE Expert Pool Meeting on Information (2020): *Trends in the Contemporary Information Environment*. Helsinki: European Centre of Excellence for Countering Hybrid Threats. Online: https://www.hybridcoe.fi/wp-content/uploads/2020/07/Hybrid-CoE-Trend-Report-4.pdf (Hybrid CoE Expert Pool 2020)

[351] Garcia-Camargo, Isabella – Bradshaw, Samantha (2021): *Disinformation 2.0: Trends for 2021 and Beyond*. Helsinki: European Centre of Excellence for Countering Hybrid Threats. Online: www.hybridcoe.fi/publications/hybrid-coe-working-paper-11-disinformation-2-0-trends-for-2021-and-beyond/ (Garcia-Camargo–Bradshaw 2021)

drágábbá a támadást. Ez az idősor közvetlenül alátámasztja a FMK Kognitív Olló modell támadás-oldalát: a manipuláció költsége stagnál vagy csökken, miközben a védekezés költségei folyamatosan nőnek.[352]

A generatív MI iparosodásának konkrét mérőszámait a NATO StratCom COE 2024-es Virtual Manipulation Brief közli, amely kvantitatív platform-monitoringot végzett az Osavul MI-platformmal a 2023 novembere és 2024 májusa közötti időszakban. A kutatás 17 koordinált csoportot azonosított, amelyek 344 forrásból terjesztették a tartalmat. Az LLM-alapú automatizált kommentek aránya a NATO-tematikájú posztok alatt platformfüggő: az angol nyelvű X-en 7 százalék, az orosz nyelvű X-en 15 százalék, az orosz nyelvű VKontakten 38 százalék. További fontos megállapítás, hogy a koordinált csoportok az LLM-eket már nem csupán szöveggenerálásra, hanem vizuális tartalom elemzésére is használják: a kutatók azonosítottak olyan botokat, amelyek a LLaVA-v1.6-34b modellt használva képesek voltak fotók és videók tartalmához relevánsan hozzászólni. A koordinált csoportok a platformok verifikációs badge-ét paradox módon „alternatív vélemény” jelöléseként instrumentalizálják, stratégiai előnnyé fordítva a platform-integritási intézkedést. A G–M–T–V lánc Generálás (G) dimenziójának szempontjából a VKontakte 38 százalékos LLM-komment-aránya a FMK Kognitív Olló támadás-oldalának kritikus adatpontja.[353]

A deepfake-technológia tényleges alkalmazásáról a NATO StratCom COE empirikus tartalomszkenneléssel gyűjtött adatot a 2022-es invázió körüli időszakban. A Reality Defender deepfake-detektáló platformmal 363, a VKontakten közzétett videót vizsgáltak meg, amelyeket pro-Kreml-aktorok osztottak meg 2022. február 24-e környékén. Az eredmény árnyalt: 12 videót az MI-technológiával manipuláltnak, további ötöt gyanúsnak minősítettek, ám a kutatók nem találtak egyértelmű mintázatot a deepfake-használatban az inváziót megelőzően vagy azt követően. A jelentés értékelése szerint a hiperrealizmushoz szükséges technikai erőforrások egyelőre korlátozzák a deepfake-ek tömegtermelését, de az olcsóbb hamisítványok („cheap-fakes”) gyakran

[352] NATO STRATCOM COE (2018–2025): Social Media Manipulation sorozat. Különösen: (2020) Social Media Manipulation 2019/2020. 8., 11. o.; (2024) Social Media Manipulation for Sale. ISBN 978-9934-619-07-6. 7., 11., 13. o.; (2025) Social Media Manipulation. 8., 14. o.

[353] NATO STRATCOM COE — OSAVUL (2024): Virtual Manipulation Brief 2024/1: Hijacking Reality — The Increased Role of Generative AI in Russian Propaganda. NATO Strategic Communications Centre of Excellence, Riga, ISBN 978-9934-619-66-3. 3., 10. o.

megjelennek. Ez az adat azért releváns, mert a deepfake-fenyegetést nembecsüli alá: 2022-ben a szórányos használat jelzi, hogy a képesség létezik, de az iparosítás küszöbét még nem érte el.[354]

6.2.4. A nem-állami szereplők átalakulása és a Doppelgänger-művelet

A 4. fejezet nem-állami szereplői szekciójában (4.1.2) a Night Wolves MC és a korai IRA-műveletek szerepeltek. A 2022–2025-ös konfiguráció lényegesen összetettebb szervezeti ökoszisztémát mutat.

A Hybrid CoE Paper 27[355] a legfrissebb átfogó kézikönyv az orosz hibrid fenyegetésekben részt vevő nem-állami szereplőkről – dokumentálja a 2022 utáni szervezeti átalakulást. Az IRA formálisan megszűnt, de funkciói a GRU-fronszervezet Centre for Geopolitical Expertise (CGE) keretébe integrálódtak. A GRU 72. Különleges Szolgálati Központja proxy weboldalakat és Telegram-hálózatokat üzemeltet. A PR-ügynökségek – különösen a Social Design Agency (SDA) és a hozzá kapcsolódó IT-cég, a Struktura – váltak a Kreml „pszichológiai hadviselési központjává": ők irányítják a Doppelgänger-, az Undercut- és a Matryoshka-műveleteket. Az SDA-t Ilja Gambasidze, a Kreml-közeli politikai technológus vezeti.

A nem-állami szereplők koordinációs modelljét más megközelítésből is alátámasztja és ezzel tovább erősíti a fent vázolt szervezeti képet Wallner, Copeland és Giustozzi (RUSI, 2025)[356]. A szerzők részletezik, hogy a GRU két kiemelkedő kiberfókuszú egysége – a 26165 és a 74455, amelyek a nyugati kiberbiztonsági elemzésekben APT28 (Fancy Bear) és APT29 (Cozy Bear) fedőnéven szerepelnek – hacktivist kollektívákat (NoName057(16), Zarya, Solntsepek, Beregini, RaHDit) alkalmaz közvetítőként: ezek a csoportok az APT-k által megszerzett adatokat újra csomagolják és terjesztik, ezáltal elhomályosítják az attribúciót és megosztják a kockázatot az állami és nem-állami szereplők között.

---

354 NATO STRATCOM COE (2023): Trends in AI. NATO Strategic Communications Centre of Excellence, Riga. 13. o.

355 Volāns, Toms et al. (2025): *Handbook on the Role of Non-State Actors in Russian Hybrid Threats.* Helsinki: European Centre of Excellence for Countering Hybrid Threats. (Hybrid CoE Paper 27.) 9–10., 49., 51. o. Online: https://www.hybridcoe.fi/wp-content/uploads/2025/12/HybridCoEPaper27HandbookontheroleofnonstateactorsinRussianhybridthreats.pdf

356 WALLNER, COPELAND & GIUSTOZZI (2025): i. m. (ld. fentebb).

A Wagner-csoport a 2023-as lázadás és Prigozsin halála után az Expeditionary Corps (Africa Corps + Volunteer Corps) keretébe szerveződött át, az Averjanov-féle GRU 29155 egység irányítása alatt. A Hybrid CoE Working Paper 33 okumentálja, hogy a Wagner nem egyszerűen felszámolódott, hanem diffúz hálózattá alakult: a korábbi lineáris Kreml→Wagner parancsláncot egy „sötét háló" (dark network) váltotta fel, ahol a kriptovalutával finanszírozott, papíron nem létező szervezetek (pl. AFRIC) működnek. A transzacionális bűnözői hálózatok (TCN-ek) fegyveresítése kém-, szabotázs- és befolyásolási műveletek céljára 2023–2024-ben új szintre emelkedett.

A Doppelgänger-művelet a Mosás (M) dimenzió 2022 utáni legjelentősebb innovációja. A támadók neves nyugati médiumok (Der Spiegel, Le Monde, The Guardian) vizuális arculatát szinte tökéletesen lemásoló klónoldalakat hoztak létre, ezeken az eredeti lapok stílusában írt, de orosz narratívákat tartalmazó cikkeket jelentettek meg, majd közösségi média hirdetésekkel juttatták el a célközönséghez. A G–M–T–V lánc szempontjából ez a M→V szekvencia legfejlettebb formája: a mosás és a validálás egyetlen műveletbe olvad, ahol a klónoldal egyszerre mossa a forrást és validálja a tartalmat a nyugati médium tekintélyével. A német információs térben az IL-hálózat percnyi pontossággal rekonstruálható: a NATO StratCom COE (2023) kutatása dokumentálta, hogy a Topwar.com → News-Front → RT Deutsch → Sputnik Deutschland láncon a woozle effect és misappropriation technikák alkalmazásával a tartalom napok alatt elérte a hazai proxyoldalakat.[357] Az EEAS 2023-as és 2024-es FIMI-jelentései a Doppelgänger-t az évtized legkiterjedtebb FIMI-műveleteként dokumentálják. Az információmosás szankciómegkerülő funkciója a Baltnews Telegram-csatorna példáján is kimutatható: a NATO StratCom COE (2024) kutatása 355 Baltnews-poszt elemzésével kimutatta, hogy 2022. február után a nyílt Kreml-propaganda (Sputnik, RT, RIA Novosztyi hivatkozások) és a rejtett IL-technikák (dekontextualizálás, misleading headline, woozle effect) egyidejűleg növekedtek, a Telegram pedig szankciómegkerülő platformként funkcionált.[358]

---

[357] NATO STRATCOM COE (2023): *Information Laundering in Germany*. NATO Strategic Communications Centre of Excellence, Riga. 26. o. A Doppelgänger-kampány német információs térben zajló IL-hálózatát percnyi pontossággal dokumentálja: a Topwar.com → NTV → News-Front → RT Deutsch → Sputnik Deutschland láncon a woozle effect és misappropriation technikák alkalmazásával a tartalom napok alatt elérte a hazai proxyoldalakat.

[358] NATO STRATCOM COE (2024): *Information Laundering via BaltNews on Telegram: How Russian State-Sponsored Media Evade Sanctions and Narrate the War*. NATO Strategic Communications Centre of Excellence, Riga, ISBN 978-9934-619-26-7. 9., 20., 36. o. A tanulmány 355 Baltnews Telegram-posztot elemzett (2021.

A Doppelganger-műveletet a DSA szempontjából vizsgáló NATO StratCom COE-tanulmány rámutat, hogy a kampány működési logikája pontosan azokat a szabályozási réseket aknázta ki, amelyeket a DSA bezárni hivatott. A Meta az értesítés ellenére nem távolított el tartalmat expeditívan – megsértve a DSA 6. cikkelyének 1(b) bekezdését – és az X (Twitter) esetében erre vonatkozó egyértelmű értesítés sem állt rendelkezésre.[359] A kampány 17 médiaszervet imperszonált, legalább 115 000 USD értékű Facebook-hirdetéssel erősítette klónolt tartalmait, és a 2023. júliusi NATO vilniusi csúcstalálkozón immár maga a NATO is közvetlen célponttá vált. Ez utóbbi körülmény megerősíti, hogy a T(erítés)-dimenzió hatékonysága az időzítéstől – a csúcseseményekhez való illesztéstől – is erőteljesen függ. A Doppelganger-eset tanulsága a disszertáció modellje szempontjából: a szabályozási keretrendszer szükséges, de önmagában elégtelen, amíg a tagállamok jogi definíciói nem harmonizálódnak és a platformok adathozzáférési kötelezettségei nem válnak kikényszeríthetővé.

A deepfake-alapú parancsrendszer-hamisítás hadtudományi következményeit – más szemszögből kiegészítve és igazolva a FIMI-jelentések megállapításait – Byman, Gao, Meserole és Subrahmanian (Brookings Institution) 2023-ban[360] részletesen elemzik „Deepfakes and International Conflict” című tanulmányukban. A szerzők dokumentálják a „liar’s dividend” paradoxonát: ha a deepfake gyanúja egyszer elterjedt, a valódi parancsokat is kétségbe vonják a katonák és a közvélemény – vagyis a dezinformációs fegyver nem csupán hamis tartalmak terjesztésével, hanem a hitelesség általános erodálásával is működik. Ez a mechanizmus az orosz Zelenszkij-deepfake esetén is tetten érhető volt: nem a videó közvetlen hatása, hanem a parancsrendszerre vetülő általános bizonytalanság volt az igazi tét.

december – 2022. június). Az IL-technikák (dekontextualizálás, misleading headline, woozle effect, misappropriation) alkalmazásával a nyugati média cikkeit torzították, majd Kreml-hivatalos csatornákon (Sputnik, RT, RIA Novoszti) terjesztették. A Telegram szankciómegkerülő platformként funkcionált.

359 SESSA, Maria Giovanna – MIGUEL, Raquel (2024): The Doppelganger Case: Assessment of Platform Regulation on the EU Disinformation Environment. NATO Strategic Communications Centre of Excellence, Riga. 5–8. o.

360 BYMAN, Daniel L. – GAO, Chongyang – MESEROLE, Chris – SUBRAHMANIAN, V.S. (2023): Deepfakes and International Conflict. Foreign Policy at Brookings, 2023. január.

6.2.5. Totális konvergencia: A fizikai és kognitív tér összeolvadása

A 2014-es krími esetben a fizikai és kognitív dimenziók ugyan szinkronizáltan, de elkülönülten működtek: a „zöld emberkék” megjelenése a terepen és a média-narratíva egymást erősítette, de nem olvadt egybe. 2022–2025-re a műveleti terek határai elmosódtak.

A 2022. februári inváziót közvetlenül megelőző Wiper-támadások (HermeticWiper, WhisperGate) nemcsak technikai zavart okoztak a kormányzati és pénzügyi infrastruktúrában, hanem megteremtették a pszichológiai nyomásgyakorlás alapját is. A Hybrid CoE Paper 15 (Exploiting Cyberspace, 2022) dokumentálta, hogy az orosz-ukrán háború nem az elvárt „kiberháború”, de a kibertevékenységek – a diplomáciai, információs, jogi és gazdasági eszközökkel együtt – jelentős komponensét képezik a hibrid hadviselésnek.

Ugyanez a Paper 15 a jogi aszimmetria mechanizmusát is feltárja: az olyan értelmezési bizonytalanságok, mint hogy a szuverenitás a kibertérben jogilag kötelező norma-e (az Egyesült Királyság álláspontja szerint csupán elv), a Tallinn Manual vonatkozó szabályait a támadó számára aszimmetrikusan előnyös szürkézónává teszik. Konkrét példa: a 2016-os amerikai elnökválasztási beavatkozásnál az Egyesült Államok nem mert arányos választ adni az eszkaláció kockázata és a jogi bizonytalanság miatt – noha az orosz kibertevékenység valószínűleg megsértette az USA szuverenitását és a be-nem-avatkozás elvét. Ez az aszimmetria – a demokratikus aktorok önkorlátozása szemben az autoriter aktorok jogi szürkézónában való manőverezésével – a G–M–T–V keret L (Legitimálás) dimenziójának kritikus vulnerabilitása: az elhárítási akarat és az elhárítási képesség közé jogi bizonytalanság ékelődik.[361]

A fizikai és kognitív műveletek szimultán konvergenciájára a disszertáció eddigi érvelése egyetlen Hybrid CoE-forrásra támaszkodott; ezt az állítást most egy másik, empirikus anyaggazdagságával kiemelkedő forrás is megerősíti. A Google Threat Analysis Group, a Mandiant és a Google Trust & Safety közös jelentése – „Fog of War: How the Ukraine Conflict Transformed the Cyber Threat

[361] PIJPERS, Peter B.M.J. (2022): Exploiting Cyberspace: International Legal Challenges and the New Tropes, Techniques and Tactics in the Russo-Ukraine War. Hybrid CoE Paper 15. European Centre of Excellence for Countering Hybrid Threats, Helsinki. A jogi aszimmetria mechanizmusát (a Tallinn Manual-értelmezési bizonytalanságok aszimmetrikus kihasználása) ld. 13–14. o.; a 2016-os amerikai elnökválasztási beavatkozás esetét ld. 13. o.

Landscape” (2023)[362] – rögzíti, hogy 2022. március 16-án a Mandiant egyidejűleg azonosított egy deepfake-IO-kampányt (az Ukraine 24 televízió feltörésével terítik Zelenszkij hamis „megadási” videóját) és egy wiper-malware-t, amelyet ütemezett feladatként pontosan három órával Zelenszkij kongresszusi beszéde előtt aktiváltak. Ez az első empirikusan dokumentált eset, amelyben kibertámadás és kognitív műveletek valós időben, egymást erősítve futottak egy konvencionális háborúban – igazolva a fejezet konvergencia-tézisét. A kiberműveletek empirikus súlyát Bányász, Kiss, Magyar és Kiss (2024) a CyberPeace Institute adatbázisa alapján 959 dokumentált támadáson mérték: Ukrajna csaknem kétszer annyi támadást szenvedett, mint Oroszország (620 vs. 339); a közigazgatás, a pénzügyi szektor és az ICT bizonyult a leginkább érintett szektornak; az orosz kötődésű People’s Cyber Army 249 támadással vezetett. A várt „kiberblitzkrieg” nem következett be – a kibertámadások hatása kisebb volt az előzetesen prognosztizáltnál, ami a disszertáció Kognitív Olló-tézisét a kiberdimenzióra is kiterjeszti[363]

2024–2025-re Oroszország a fizikai-kognitív konvergenciát a szabotázsakciókban operacionalizálta: a Telegramon toborzott amatőröket raktártüzek gyújtására és GPS-zavarásra szerte Európában – többek között Csehországban, Lengyelországban és a balti államokban. A folyamat körkörös logikára épül: kognitív toborzás (a szürke zóna platformjain pénzért keresnek végrehajtókat) → fizikai hatás (a szabotázs a lakosság biztonságérzetét rombolja) → kognitív hasznosítás (az eseményt a propaganda a nyugati rendszerek instabilitásának bizonyítékaként keretezi). A G–M–T–V lánc szempontjából ez a Terítés (T) és a Validálás (V) dimenzió fúziója: a fizikai esemény maga válik terjesztési horgonnyá, mert a kézzelfogható pusztítás a digitális kétely korában az egyetlen olyan inger, amely ellenáll a hamisítás gyanújának.

A Hybrid CoE Strategic Analysis 33[364] a kognitív intrúzió fogalmával írja le ezt a dinamikát: a hibrid fenyegetési akciók a liberális demokratikus kormányzás alapjait, alkotmányos értékeit és

---

362 GOOGLE THREAT ANALYSIS GROUP – MANDIANT – GOOGLE TRUST & SAFETY (2023): Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape. Google, 2023. február.

363 Bányász et al. (2024): *Empirical analysis of the cyberattacks of the Russian–Ukrainian war.* Információs Társadalom, XXIV. évf. 2. sz. 9–32. o. DOI: 10.22503/inftars.XXIV.2024.2.1. A tanulmány 959 dokumentált kibertámadást elemez (2022–2023): Ukrajna 620, Oroszország 339 támadást szenvedett; a People’s Cyber Army (orosz kötődésű) 249 támadással vezet.

364 Lebrun, Maxime (2023): *Anticipating Cognitive Intrusions: Framing the Phenomenon.* Helsinki: European Centre of Excellence for Countering Hybrid Threats. (Hybrid CoE Strategic Analysis 33.) 3–4., 5–6., 7. o. Online: https://www.hybridcoe.fi/wp-

normáit célozzák, és a félelem, a harag és a resszentiment érzelmi mobilizációs erőit használják ki. A fizikai-kognitív konvergencia ennek a legfejlettebb formája: a szabotázzsal generált félelem a dezinformáció hatékonyságát multiplikálja.

A vonatkozó 15. táblázat: Összegző Helyzet-dimenzió táblázat: 2014 kiindulási alap vs. 2022–2025 konfiguráció címmel a mellékletben található.

6.2.7. FMK-rács / FMK-mátrix – a Helyzet-dimenzió operacionalizálása (2022–2025)

A 4.2.5 alfejezetben a 2014-es esetre alkalmaztam az FMK-rácsot. Alább ugyanezt a logikát alkalmazom a 2022–2025-ös konfigurációra. A rács a fegyvernek minősülő kommunikáció három dimenzióját rögzíti: (1) a termék típusa (szöveges, képi, audio, video, multimodális); (2) a szándék (meggyőzés, bénítás, polarizáció, demobilizáció); (3) a célzás szintje (egyéni, csoport, társadalmi).

2022–2025-ben az FMK-mátrix modalitás-differenciálásának szerepe radikálisan megnőtt. Míg 2014-ben a szöveges manipuláció dominált (az egyetlen video-elem a Krím „népszavazásának" közvetítése volt), 2022–2025-re a modalitások közötti átjárás (cross-modal attack) vált a fő fenyegetéssé: a deepfake-hang klónozás (Zelenszkij megadást parancsol), a vizuális bizonyíték-illúzió (biolabor „dokumentumok"), és a Doppelgänger klónoldalak multimodális tartalma (szöveg + kép + layout) egyaránt az FMK-mátrix különböző celláit tölti meg. A vonatkozó 16. táblázat: FMK-rács / FMK-mátrix modalitás-összehasonlítás: 2014 vs. 2022–2025 címmel a mellékletben található.

A 2014-ről 2022-re történt eltolódás lényege az FMK-rács szempontjából: a rács cellái 2014-ben egyenként, manuálisan voltak kitöltve; 2022-re a cellák automatikusan, párhuzamosan és modalitások közötti átjárással töltődnek – a támadó egy narratívát egyidejűleg több modalitásban, több platformon, több nyelven képes futtatni. Ez az FMK iparosodása. A vonatkozó 17. táblázat: G–M–T–V összegzés: 2014 sarokpont vs. Híd-időszak vs. 2022–2025 végállapot címmel a mellékletben található. A vonatkozó 18. táblázat: Szintetikus média incidenstár: deepfake és MI-generált műveletek verifikált evidenciabázisa, 2022–2025 címmel a mellékletben található.

content/uploads/2023/07/20230703HybridCoEStrategicAnalysis33CognitiveintrusionWEB.pdf – A „fizikai-kognitív konvergencia" és a szabotázs dezinformációt multiplikáló hatása a szerző következtetése Lebrun keretrendszeréből; a SA33 a kognitív intrúzió és a fizikai erőszak kapcsolatát általánosan tárgyalja.

6.3. ELŐREJELZÉS-DIMENZIÓ (Forecast): Adaptáció, sokkhatások és a platformok harca

A H–E–I diagnosztikai mátrix középső oszlopa a konfliktus folyamatdinamikáját vizsgálja: nem azt, ami van (Helyzet), hanem azt, hogyan mozog a rendszer – milyen adaptációs mechanizmusok működnek, milyen sokkhatások módosítják a pályát, és milyen kognitív feldolgozási szűkületek alakulnak ki. A 4. fejezetben (4.3) az OxIPO-modellt alkalmaztam az Előrejelzés-dimenzióra, kimutatva, hogy a 2014-es krími bénulás az Input→Process→Output lánc szisztematikus zavarának eredménye volt. A 2022–2025-ös konfiguráció lényegileg más képet mutat: a feldolgozási lánc nem a támadó, hanem a védekező javára billent át – legalábbis az első fázisban.

6.3.1. 2022: Az OODA-ciklus megfordulása és az OSINT-forradalom

A 4.3 alfejezetben dokumentáltam, hogy 2014-ben a döntéshozatali ciklus (OODA-loop) egyértelműen az orosz fél javára működött: mire a nyugati elemzők értelmezni tudták a helyzetet, a tények a terepen már megváltoztak. 2022-ben ez a dinamika megfordult.

Az OxIPO-modell keretében a 2022-es fordulat úgy írható le, hogy a védekező fél Input-dimenziója radikálisan javult: a műholdképek nyilvános elérhetősége (Maxar, Planet Labs), a közösségi média geolokációs elemzése (Bellingcat, GeoConfirmed) és a platformok transzparencia-jelentései (Meta CIB, Google TAG) olyan bemeneti adathalmazt biztosítottak, amely 2014-ben nem létezett. A Process-dimenzióban az ukrán civil társadalom horizontális szerveződése – a Diia kormányzati alkalmazástól a StopFake kézi monitoringján át a Texty MI-alapú narratíva-azonosításáig – jelentősen csökkentette a feldolgozási időt. Az Output-dimenzióban az ukrán stratégiai kommunikáció sebessége és kreativitása – Zelenszkij napi videoüzeneteitől a hivatalos közösségimédia-csatornák memetikus tartalmáig – a valós idejű ellen-narratíva-képzést tette lehetővé.

A Hybrid CoE Research Report 11 dokumentálja, hogy Ukrajnának a legnagyobb tapasztalata van a Kreml-dezinformáció elleni küzdelemben – az Euromajdan óta, immár egy évtizede tartó információs háborúban finomhangolt legjobb gyakorlataival. A kutatás kiemelte: az ukrán megközelítés nem intézményi, hanem ökoszisztéma-alapú, ahol a civil társadalom, a média, a kormányzat és az önkéntesek között a határok elmosódnak. A február 24-i inváziót követően tömegesen csatlakoztak önkéntesek a dezinformáció-elleni „területvédelemhez”: a StopFake, a Detektor Media, a Texty és számos más szervezet mellett spontán csoportok alakultak. A

redundancia tudatos volt: „biztonságosabb, ha több szereplő látja ugyanazt az információt, mintha kockáztatnánk, hogy valami átcsúszik” – hangzik az interjúalanyok közös értékelése.

A hadviselés klasszikus „háború ködének” (Fog of War) radikális eloszlása volt a műveleti dinamika kulcseleme. 2022-ben az ukrán és nemzetközi OSINT-tevékenység technológiai felkészültsége miatt Oroszország képtelen volt fenntartani a műveleti titkosságot. A Bellingcat, a DFRLab és a Mandiant/Google TAG valós időben dokumentálták az információs műveleteket – a támadó infrastruktúra leleplezési ideje napokról órákra rövidült. Ez az OxIPO Output-dimenziójának minőségi ugrása: a rendszer kimenete (a leleplezés) gyorsabb, mint a támadó következő inputja.

Az Input-dimenzió strukturális javulásának intézményi magyarázatát – ezzel más szemszögből is alátámasztva a fenti megállapítást – nyújtja Goncharuk (ICDS, 2024): „Artificial Intelligence in Defence of Ukraine.” A szerző dokumentálja[365], hogy Ukrajna 2019-ben felállított Digitális Átalakulás Minisztériuma és az AI-fejlesztési szakértői bizottság 2021-re MI-stratégiát dolgozott ki a katonai-ipari komplexum számára; a 2014 óta felépített önkéntes szervezetek (Kropyva helyzettudatossági rendszer, GIS Arta tüzérségi célmegjelölés alkalmazás) már a teljes körű invázió előtt aktívan alkalmaztak AI-eszközöket a dezinformáció elleni küzdelemre, botláncolatok leleplezésére és a hamisított médiatartalmak azonosítására. 2023-ra az átdolgozott ukrán MI-prioritások között önálló tételként szerepel a deepfake audio- és videóklipek gyors azonosítására alkalmas eszközök fejlesztése – ami azt jelenti, hogy a védekezés nem reaktív volt, hanem strukturálisan beépült az ukrán hadviselési doktrínába.

6.3.2. A kognitív intrúzió és a társadalmi identitás fegyveresítése

A Hybrid CoE Strategic Analysis 33 által definiált kognitív intrúzió fogalma a 2022–2025-ös konfiguráció egyik kulcskategóriája. A kognitív intrúzió nem egyszerű dezinformáció: az egyéni és kollektív mentális folyamatok szándékos manipulálása, amelynek célja a politikai erőszak előmozdítása a liberális demokratikus társadalomban. A félelem, a harag és az érzelmi mobilizáció erőit használja, és a demokratikus kormányzás alapértékeibe vetett bizalmat célozza. A kognitív

[365] Goncharuk, Vitaliy (2024): *Artificial Intelligence in Defence of Ukraine.* (Russia's War in Ukraine, Brief 6.) Tallinn: International Centre for Defence and Security. Online: https://icds.ee/wp-content/uploads/dlm_uploads/2024/09/Layout-AI-in-Defence-of-Ukraine.pdf

intrúzió keretezése azért szükséges, mert a 2022–2025-ös konfliktus nem egyszerű dezinformációs kampányok sora, hanem szisztematikus beavatkozás a demokratikus társadalmak kognitív reflexeibe, elfogultságaiba és előítéleteibe.

A Hybrid CoE Paper 24 rámutat, hogy a társadalmi identitások mobilizálása kétélű fegyver. A védekező oldalon az ukrán nemzeti identitás konszolidációja – amelyet Allenby[366] már a 2014-es törésvonalak kontextusában előre jelzett – 2022-re beérlelődött és a reziliencia egyik legerősebb forrása lett. A támadó oldalon viszont Oroszország rendszeresen használja az identitás fegyveresítését: a kárpátaljai magyar kisebbség „fenyegetettségének" felnagyítása, a svédországi Korán-égetések instrumentalizálása a NATO-bővítés kontextusában, vagy a menekültkérdés kulturális háborúként való keretezése mind a kognitív intrúzió eszközei. Az OxIPO keretben ez az Input-dimenzió szándékos torzítása: a bemeneti információ úgy van keretezve, hogy a feldolgozás (Process) automatikusan az érzelmi rövidzárat aktiválja, kihagyva a racionális mérlegelést. Dolan figyelmeztet, hogy a dezinformáció kétélű fegyver: ha a hamis üzenet lelepleződik, az évek stratégiai kommunikációs beruházását teheti semmissé, ráadásul az álhírek tömeges gyártása olyan szkeptikus közönséget termel, amely végül semmilyen forrásban nem bízik[367]

A brazíliai 2022-es választási kampány – ahol a Reporters Without Borders szerint az újságírókat átlagosan hárompercentként érte online zaklatás – és a 2021. január 6-i washingtoni Capitolium-ostrom egyaránt a kognitív intrúzió következményeit illusztrálja: a harag és a bosszúvágy érzelmi mobilizálása a demokratikus intézmények elleni fizikai erőszakba fordult. Bár ezek nem közvetlenül az orosz-ukrán konfliktushoz kötődnek, a módszertani mintázat azonos, és Oroszország aktívan alkalmazza ezeket a technikákat a nyugati társadalmakban.

6.3.3. 2024: A Telegram-sokk és a szürke zóna felszámolása

A háború kognitív folyamatainak legnagyobb töréspontja 2024 augusztusában következett be, amikor a francia hatóságok letartóztatták Pavel Durovot, a Telegram alapítóját. A Telegram 2022

366 Allenby, Braden – Garreau, Joel (2017): *White Paper on Weaponized Narrative.* [Future of War Conference, 2017. március 21.] Tempe, AZ: Arizona State University – Center on the Future of War / New America. Online: https://weaponizednarrative.asu.edu/publications

367 DOLAN, Andrew (2024): Hybrid Warfare and Strategic Surprise. In JOBBÁGY, Z. és ZSIGMOND, E., (eds.): *Hybrid Warfare Reference Curriculum, Volume III.* Budapest: Ludovika. 169. o.

óta a szürke zóna érinthetetlen bástyája volt: a platform szinte teljes moderáció-mentessége miatt ez vált az orosz milbloggerszféra és – a szükséges katonai kommunikációs eszközök hiányában – gyakran a frontvonalbeli taktikai irányítás elsődleges felületévé. A NATO StratCom COE Robotrolling 2023–2024 elemzése empirikusan dokumentálta a Telegram központi szerepét: a 17 azonosított koordinált csoport 53%-a a Telegramon volt aktív, egyetlen hálózat 130 Telegram-csatornát és 13 weboldalt üzemeltetett szimultán.

A letartóztatás és az azt követő moderációs szigorítás pánikot okozott a parancsnoki láncban. A platformszuverenitás kérdése hirtelen elméletiből műveleti kockázattá vált: az orosz vezetés ráébredt, hogy a kommunikációs gerince egy nyugati joghatóság alá tartozó szereplőtől függ. A Telegram-sokk hatása több szinten is érzékelhető volt: (1) a milbloggerek – akik a Kreml számára egyszerre voltak értékes propagandaeszközök és kényelmetlenül önálló információforrások – kommunikációs csatornát váltottak, ami átmeneti zavarokat okozott; (2) a frontvonali taktikai koordináció sérült, mivel a Telegram a katonai rádiókommunikáció informális pótlékává nőtte ki magát; (3) a szabotázsakciók toborzási infrastruktúrája (ld. 6.2.5) réseket kapott.

A Telegram-sokk konkrét műveleti hatásait két egymástól független forrás is alátámasztja és pontosítja, ezzel a disszertáció eddigi állításait empirikusan tovább erősítve. Az Institute for the Study of War (ISW) 2024. augusztus 25-i napi harctéri értékelése [368] rögzíti, hogy a milbloggerek tömegesen hirdettek a VK-ra való migrációt, a Telegram-t az orosz frontszintű parancsnoki és irányítási (C2) kommunikáció informális gerinceként minősítették, és a letartóztatás napján nyilvánosan szólítottak fel az orosz katonai parancsnokság önálló kommunikációs rendszerének kiépítésére – demonstrálva, hogy ilyen rendszer 2024-ben még mindig nem létezett. Egy másik megközelítésből egészíti ki és erősíti ezt a képet TRT World Research Centre török állami médiához kötött intézmény (TRT = Türkiye Radyo ve Televizyon Kurumu) „The Rise of Military Bloggers Amid the Russian-Ukrainian War" című elemzésében[369] a szerzők dokumentálják, hogy a legnagyobb pro-háborús csatornák (Rybar: 1,1 millió, Wargonzo: 1,3 millió követő) a

[368] MAPPES, Grace et al. (2024): Russian Offensive Campaign Assessment, August 25, 2024. Institute for the Study of War (ISW), Washington D.C.

[369] Yıldız, Karim – Özdemir, Hüseyin (2024): *The Rise of Military Bloggers Amid the Russian-Ukrainian War.* [Discussion Paper.] Washington, D.C. – Ankara: TRT World Research Centre. Online: https://researchcentre.trtworld.com/publications/discussion-paper/the-rise-of-military-bloggers-amid-the-russian-ukrainian-war/

kormányzathoz kötötten, mégis formálisan önállóan működnek – a Kreml tolerálja őket, mert szelepes funkcióval bírnak: a katonai kudarcokon növekvő népharagot levezető csatornák megszüntetése belső feszültséget szítana.

A G–M–T–V lánc Terítés (T) dimenziójában a Telegram-sokk a zárt csatorna sérülékenységét mutatta meg: ami 2014–2021 között a támadó számára a moderáció-mentes terjesztés előnye volt, az 2024-ben egyetlen jogi aktussal műveleti kockázattá vált. Ez az esemény validálta a H2 hipotézist: a platformszintű beavatkozás képes közvetlen harctéri zavart okozni.

Az OxIPO keretben ez Process-szintű zavar a támadó oldalon: a megszokott feldolgozási-terjesztési rutin hirtelen megszakadt, és az adaptáció (új csatornák keresése, VPN-használat, alternatív platformok) időt és erőforrást igényelt – pontosan azt a reakcióidő-hátrányt okozva a támadónak, amelyet 2014-ben a védekező oldalon lehetett megfigyelni.

6.3.4. Pszichológiai ív: A mobilizációtól a demobilizációig és a kognitív nihilizmusig

Az Előrejelzés-dimenzió záró szekciója a pszichológiai dinamikát vizsgálja. 2022 és 2025 között a konfliktus kognitív célrendszere háromszor változott meg:

Mobilizációs szakasz (2022–2023): A cél a cselekvésre ösztönzés volt – ukrán részről a nemzeti ellenállás, nyugati részről a szankciók és fegyverszállítás támogatása. Az érzelmi töltet a hősiesség és a szolidaritás volt. Ebben a fázisban jelent meg a NAFO (North Atlantic Fellas Organization) szervezet. A Hybrid CoE Working Paper 26 elemzése alapján a humor három funkciót tölt be a dezinformáció elleni küzdelemben: a szokásos közönségen túli rétegek elérése; a saját közönség moráljának és rezilienciájának erősítése; és a támadó hírnevének rontása. A NAFO ezt a hármas funkciót ipari léptékben valósította meg: a pátoszos és fenyegető orosz narratívákat szatírával és gúnnyal semlegesítette. A memetikus hadviselés – amelyet a NATO StratCom COE 2021-es Memetic Warfare kötete elméleti szinten megalapozott – 2022-ben élesben futott. A Nimmo-féle Breakout Scale keretében a NAFO-kampányok rendszeresen 4–5-ös kategóriájú áttörést értek el – a közösségi médiából magas presztízsű véleményformálók amplifikálásán át jutottak el a mainstream médiáig, és a frontállamok állami szintű elismerését (pl. Nausėda litván elnök nyilvános üdvözlete) is kivívták. A NAFO keletkezéstörténete jól illusztrálja a nem tervezett másodlagos hatások dinamikáját: a mozgalom nem dezinformáció-ellenes szándékkal jött létre – Kamil Dyszewski 2022 májusában rajzolt kutyákat készített az Ukrajnában harcoló Grúz Légió

adományozóinak megköszönésére, és az informális közösség másodlagos hatásként vált a dezinformáció nevetségessé tételének platformjává[370]. A konkrét diplomáciai hatást példázza Mihail Uljanov (Oroszország bécsi állandó képviselője) esete: a tömeges NAFO-válasz Uljanov kissé szokatlan angol fogalmazását virálissá és memifikálódottá tette, jótékonysági merchandising-termékeket generált, és bár az online jelenlétéről nem mondott le, a szélesebb közönség szemében hitelességvesztése állandósult. A humor tehát nemcsak a tartalmat, hanem az üzenetküldő személyét is delegitimálja – a H–E–I mátrix Irányítás-dimenziójában ez a támadó attribúciós költségeit növelő mechanizmusként értelmezhető. A humor emellett a közösségi érdekközösség kohéziós elemeként is funkcionál: a közös nevetés identitást és egységet ad egy korábban atomizált, látens közösségnek, a crowdsourcing-hatás pedig a „minden katona szenzor" (every soldier a sensor) katonai ambíció civil megvalósítása a közösségi médiában – a közös helyzetismeret lehetővé teszi korábban észrevétlen dezinformáció felderítését.

Demobilizációs szakasz (2024–2025): A konfliktus elhúzódásával a kognitív műveletek célja a passzivitás kiváltása lett. Az orosz „békepárti" narratívák célja nem az, hogy a nyugatiak megszeressék Oroszországot, hanem hogy közömbössé váljanak Ukrajna iránt. A kognitív fáradtság menedzselése vált a legfontosabb folyamattá: az a fél nyer, amelyik tovább képes fenntartani a társadalmi figyelmet.

A demobilizációs narratívák időzítésének stratégiai logikáját – egy más módszertannal, de egybehangzó következtetéssel, ezzel független empirikus bizonyítékkal tovább erősítve a fenti megállapítást – igazolja Paziuk, Lande, Shnurko-Tabakova és Kingston (Frontiers in Artificial Intelligence, 2025)[371]: „Decoding manipulative narratives in cognitive warfare: a case study of the Russia-Ukraine conflict." A szerzők a saját fejlesztésű Attack-Index rendszerrel és nagy nyelvi modellekkel vizsgálták az orosz információs tér narratíváit 2022 novemberétől 2024 végéig: a nukleáris fenyegetés narratíva 2022 oktoóberében napi 807 megemlítést ért el (abszolút csúcs), és a csúcsok szisztematikusan NATO-csúcsokat és katonai segítségnyújtási tanácskozásokat előztek meg – igazolva a reaktívból proaktívba való stratégiai átmenetet. Az elemzés öt tematikus klasztert

[370] GILES, Keir (2023): *Humour in online information warfare: Case study on Russia's war on Ukraine*. Hybrid CoE Working Paper 26. European Centre of Excellence for Countering Hybrid Threats, Helsinki. 28. o.

[371] Paziuk et al. (2025): Decoding manipulative narratives in cognitive warfare: a case study of the Russia-Ukraine conflict. *Frontiers in Artificial Intelligence*, Vol. 8. Online: https://doi.org/10.3389/frai.2025.1566022

azonosított (nukleáris katasztrófa, piszkos bomba narratíva, orosz nukleáris csapáskészség, szerződéssértési narráció, tengeri erőfölény), amelyek mindegyike az érzelmi manipuláció egy-egy célzott formáját képviseli – és amelyek struktúrája közvetlen megfelelője a fejezet H–E–I mátrix Előrejelzés (E) dimenziójában leírt adaptációs mintának.

Kognitív nihilizmus (2025–): A hiperrealizmus kora (ld. 6.2.3) nem a demobilizáció végállapota, hanem annak radikalizálása. A cél nem a passzivitás, hanem az igazság fogalmának felszámolása. Ha semmit nem lehet biztosan tudni, nincs miért cselekedni. Ez a Validálás (V) dimenzió kétoldalú eróziója: nem csak a támadó validálási kísérletei, hanem a védekező ellen-validálási képessége is csökken, ha a társadalom elfárad. A Hybrid CoE Paper 12 figyelmeztetése itt válik különösen aktuálissá: a reziliencia az elrettentés alapja, de nem stratégia önmagában – a Communication–Capability–Credibility (3C) pillérrendszert folyamatosan fenn kell tartani.

6.4. IRÁNYÍTÁS-DIMENZIÓ (Control): Az intézményesült védekezés és határai

A H–E–I diagnosztikai mátrix harmadik oszlopa a rendszer visszacsatolási mechanizmusait és a védekezés hatékonyságát vizsgálja. A 4.4 alfejezetben három kontrolltípust elemeztem: attribúciós küszöb, reakciókockázat, és koordináció/jóváhagyási lánc. Mindhárom területen a 2014-es konfiguráció a tehetetlenség jegyében telt. 2022–2025-re a védekezés radikális minőségi ugráson ment keresztül. A demokratikus államok szakítottak a technológiai semlegesség elvével, és létrehozták a kognitív hadviselés jogi és műveleti kereteit.

6.4.1. Attribúciós és reakcióképesség: A 2014-es paralízis ellentéte

A 4.4.1 alfejezetben dokumentáltam, hogy 2014-ben az attribúciós küszöb rendkívül magas volt: a nyugati döntéshozók hosszú bizonyítékláncot követeltek meg ahhoz, hogy az orosz felelősséget formálisan is kimondják. Ez a „bizonyossági várakozás” (certainty expectation) a Wicked Problem logikáját követte : a hibrid fenyegetés szándékosan a küszöb alatt marad, ahol a válaszlépés politikai költsége meghaladja a fenyegetés azonosításának bizonyosságát.

2022-re ez a dinamika megfordult. Az Egyesült Államok és az Egyesült Királyság a háborút megelőző hetekben példátlan hírszerzési transzparenciát alkalmaztak: nyilvánosan osztották meg az orosz csapatmozgások műholdképeit és a tervezett hamis zászlós műveletek forgatókönyveit. Ez nem csupán kommunikációs stratégia volt, hanem az attribúciós küszöb szándékos leszorítása:

ha a fenyegetés nyilvánosan dokumentált, a tagadhatóság – amely a 2014-es művelet egyik sikerkulcsa volt – megszűnik.

A reakcióképesség terén a változás hasonlóan jelentős. 2014-ben a szankciós válasz hónapokat késett; 2022-ben az EU első szankciós csomagja napok alatt életbe lépett. A 4.4.2 alfejezetben elemzett jogi-politikai küszöbök (a „mi a legitim reakció?" vita) 2022-ben jóval alacsonyabbak voltak, mert a hírszerzési transzparencia előzetes konszenzust teremtett a fenyegetés természetéről. Az OxIPO keretben ez a Process→Output időzítés radikális csökkenése: a feldolgozási idő (az információ értékelésétől a döntésig) hónapokról napokra szűkült.

6.4.2. Jogi keretrendszer: A DSA és a szankciós precedens

A háború kitörését követő napokban az Európai Unió Tanácsa precedens nélküli döntést hozott: felfüggesztette a Russia Today (RT) és a Sputnik műsorszolgáltatási jogait az Unió területén. Ez paradigmaváltás volt: a szólásszabadság abszolutizmusát felülírta a biztonsági szükségszerűség. A cél nem a totális cenzúra (VPN-en keresztül az oldalak elérhetők maradtak), hanem a kognitív súrlódás (cognitive friction) növelése: a passzív fogyasztók elzárása a propaganda-csatornáktól.[372]

A Hybrid CoE Paper 19 elemzése a kiberterületi jogi keretrendszerek kontextusában dokumentálja a digitális szuverenitás fogalmának átalakulását: a demokratikus és autoritárius blokkok eltérő jogfelfogása a kiberterületen tükrözi a hibrid fenyegetések elleni védekezés jogi dilemmáit.

A hibrid fenyegetések jogi dimenziójának átfogó elemzését a Hybrid CoE Research Report 3 keretében, bevezetve a jogi reziliencia (legal resilience) fogalmát. Sari rámutat, hogy a jog a hibrid műveletek kontextusában kettős természetű: egyrészt a védekezés eszköze (szankciók, szabályozás), másrészt maga is célpont – a jogrendszer kijátszása, az attribúciós küszöb alatti műveletek és a jogi szürkezónák kihasználása mind a jogi hadviselés (lawfare) formái.[373]

---

[372] NATO STRATCOM COE (2023): *Social Media Manipulation 2022/2023: Assessing the Ability of Social Media Companies to Combat Platform Manipulation*. NATO Strategic Communications Centre of Excellence, Riga, ISBN 978-9934-619-32-8. A 2022-es kísérletben a bejelentett botfiókok 54–95%-a továbbra is aktív maradt öt nappal a jelentés után; a TikTok és YouTube teljesített a legrosszabbul.

[373] SARI, Aurel (2021): Hybrid threats and the law: Building legal resilience. Hybrid CoE Research Report 3. European Centre of Excellence for Countering Hybrid Threats, Helsinki. 10–17., 35–40. o.

Ez a folyamat a 2024-es európai parlamenti választások idején érte el következő szakaszát, amikor élesben vizsgázott a Digitális Szolgáltatásokról szóló Rendelet (DSA, 2022/2065)[374]. A jogszabály kötelezte az óriásplatformokat (VLOPs), hogy kockázatelemzést végezzenek a választási integritásra vonatkozóan. A G–M–T–V lánc szempontjából a DSA a Terítés (T) dimenzió szűkítésére irányul: a platformok algoritmikus amplifikációs képességét nem szünteti meg, de auditálhatóvá teszi.

A DSA tényleges hatékonyságát a NATO StratCom COE 2025-ös esettanulmánya mérte először AI-alapú módszerrel (GPT-4o mini + Gemini 1.5 Pro kereszt-validáció). A lengyel és litván Facebook-tartalmak összehasonlítása (2023 vs. 2024) azt mutatja, hogy a gyűlöletbeszéd aránya mindkét nyelvterületen megközelítőleg 90% maradt, a lengyel csoportokban a káros tartalmak száma 128%-kal emelkedett, miközben a litván tartalmak eltávolítási arányában szignifikáns visszaesés tapasztalható.[375] A szerzők összefoglalója velős: a DSA hatályba lépése után „átfogó javulás nem állapítható meg." Ez a megállapítás a disszertáció szabályozási-dimenziójának egyik legfontosabb empirikus alátámasztása: a DSA-t sokan üdvözölték a dezinformáció elleni végső szabályozási eszközként, de az adatok azt mutatják, hogy a törvény tartalom-moderációs hatása korlátozott, és különösen a kisebb, kevésbé figyelt nyelvközösségek (litván, lengyel – és analógia alapján: magyar) esetén a platformok erőfeszítései elmaradnak. Ez megerősíti a disszertáció tézisét: a szabályozási keretrendszer szükséges, de nem elégséges feltétele a T(erítés)-dimenzió kezelésének.

A DSA tényleges alkalmazhatóságát a Doppelgänger-művelet kontextusában Sessa és Miguel (2024) jogi-technikai esettanulmány keretei között vizsgálták. A kutatás módszertana „match-making”: a Doppelgänger-kampány azonosított taktikáit, technikáit és eljárásait (TTP) szisztematikusan összevetették a DSA specifikus cikkelyeivel. A kampány több mint 17 médiumot szimulált hamisított domain-nevekkel (pl. theguardian.co.com); Facebook-hirdetésekre legalább

374 Az Európai Unió Tanácsa – Az Európai Parlament (2022): Az Európai Parlament és a Tanács (EU) 2022/2065 rendelete (2022. október 19.) a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról (Digitális Szolgáltatásokról szóló Rendelet). *Az Európai Unió Hivatalos Lapja,* L 277, 2022. október 27., 1–102. o. Online: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32022R2065

375 HAIDUCHYK, Tetiana – KHUSNUTDINOV, Marat – BELAFATTI, Fabio – KUBŚ, Jakub – ŠUMINAS, Andrius – BERGMANIS-KORĀTS, Gundars (2025): Impact of the Digital Services Act: A Facebook Case Study. NATO Strategic Communications Centre of Excellence, Riga. Executive summary; 15–16. o.

115 ezer dollárt költöttek; és a Meta tudomása ellenére a kampány 2023-ban is folyt Franciaországban és Németországban. 2023 júliusában a NATO-t is megszemélyesítették a nato[.]ws doménen, a vilniusi csúcs kontextusában. A DSA 6., 9., 10., 14., 16., 20., 23., 35., 37., 40. és 42. cikkelye mind alkalmazható, de a szerzők kiemelik, hogy a határon átnyúló terjesztés kezelése a tagállami szintű végrehajtásra van bízva, az attribúció továbbra is kihívás. Az elemzés közvetlenül demonstrálja az Irányítás-dimenzió korlátait: a szabályozási eszköztár létezik, de a végrehajtási képesség és a platformok felelősségvállalása között szignifikáns rés tátong.[376]

6.4.3. Műveleti standardizáció: A DISARM keretrendszer

A védekezés nemcsak jogi, hanem technikai szinten is standardizálódott. A Hybrid CoE Research Report 7 (Newman 2022) részletesen dokumentálja a DISARM (Disinformation Analysis and Risk Management) keretrendszer fejlesztését és alkalmazását.[377] A DISARM a kiberbiztonságban globális standardnak számító MITRE ATT&CK mintájára készült: lehetővé teszi, hogy a védők ne az egyes tartalmakra (egy konkrét álhírre), hanem a támadók Taktikáira, Technikáira és Eljárásrendjére (TTPs) reagáljanak.

A keretrendszer négy rétegű dezinformációs piramist alkalmaz (kampány → incidens → narratíva → műtermék), és a támadói és a védekező perspektívát egyaránt modellezi. Két perspektívát különít el: a támadó felülről lefelé látja a piramist (a kampánytól a műtermékig), a védekező alulról felfelé (a műterméktől a kampányig). A DISARM STIX-kompatibilis (Structured Threat Information Expression), ami lehetővé teszi a kibervédelmi ökoszisztémával való közvetlen adatcserét.

A DISARM a G–M–T–V lánc kontextusában a Mosás (M) és Terítés (T) dimenzió elleni szisztematikus védekezési eszköz: a TTP-alapú elemzés a művelet struktúráját, nem a tartalmát célozza. A Hybrid CoE értékelése szerint a keretrendszer „piacérett megoldás", amely képes

---

376 SESSA, Jacopo — MIGUEL, Raquel (2024): The Doppelganger Case: Avenues for Mitigation. NATO Strategic Communications Centre of Excellence, Riga, ISBN 978-9934-619-30-4. 5–7., 12–15., 20–21. o.

377 NEWMAN, Hadley (2022): *Foreign Information Manipulation and Interference Defence Standards: Test for Rapid Adoption of the Common Language and Framework 'DISARM'*. Hybrid CoE Research Report 7, European Centre of Excellence for Countering Hybrid Threats, Helsinki — NATO Strategic Communications Centre of Excellence, Riga, ISBN 978-952-7472-46-0. 15., 19–20. o. A szerző tíz hitelesség-kritérium mentén értékelte a keretrendszert, és az Operation Ghostwriter esettanulmányon validálták a DISARM-taxonómia praktikus alkalmazhatóságát.

skálázódni az FIMI fenyegetés növekedésével, és a stratégiai kommunikációs szakemberek számára intuitívan elsajátítható.

6.4.4. Az ukrán dezinformáció-elleni modell tanulságai

A Hybrid CoE Research Report 11 (Kalenský et al. 2024) az ukrán tapasztalatokat kilenc kulcsfontosságú tanulságba sűríti. A disszertáció szempontjából a legfontosabbak:

A kimerítő monitoring nélkülözhetetlen. Az ukrán rendszer nem egyetlen központi szervből áll, hanem átfedő, többszintű megfigyelési hálózatból – a StopFake kézi monitoringjától a Texty MI-alapú narratíva-azonosításáig. A redundancia tudatos: ha több szereplő figyeli ugyanazt az információs teret, kisebb az esély, hogy egy fenyegetés észrevétlen marad. A monitoring célja nem csupán a detekció, hanem a mintázatfelismerés: a normális információs háttérzajtól való eltérés (spike) azonosítása, amely egy IPSO (információs-pszichológiai különleges művelet) előkészítő fázisát jelezheti. Az ukrán védelmi MI-alkalmazások szélesebb kontextusa (geospatial intelligence, drón-rendszerek, kiberhadviselés) megerősíti, hogy a kinetikus és a kognitív dimenziók technológiai konvergenciája Ukrajna számára műveleti szinten is megvalósult.[378]

A humor szisztematikus védekezési eszköz. Az ukrán MFA és a StratCom-közösség a memetikus hadviselést a Híd-időszak elméleti alapozása (NATO StratCom COE 2021) nyomán operatív szintre emelte: egy mém olyan célpontot is eltalálhat, amelyet egy hivatalos közlemény nem. Ennek iskolapéldája az ukrán Védelmi Minisztérium 2023. januári videója, amelyben a nyugati harckocsi-szállítások körüli vitát úgy oldotta fel, hogy az M1A2 Abrams harckocsit „recreational utility vehicle”-ként (rekreációs haszongépjármű) nevezte meg – egy álreklámban, amely virális terjedésével bizonyította, hogy a kormányzati kommunikáció is képes felülírni a bürokratikus viralitási paradoxont[379]. Giles (2023) ezt a fogalmat (bureaucratic virality paradox) a kormányzati kommunikáció egyik strukturális korlátjaként vezette be: a formális szervezetek alapértelmezés szerint túl merevek és kockázatkerülők ahhoz, hogy virális tartalmakat hozzanak létre. Ukrajna

[378] AI in Defence of Ukraine (2024): Policy Brief. Az összefoglaló az ukrán védelmi MI-alkalmazásokat (geospatial intelligence, drón-rendszerek, kiberhadviselés, katonai ki-képzés) tekinti át, bemutatva a kinetikus és a kognitiv dimenziók technológiai konvergenciáját.

[379] GILES, Keir (2023): *Humour in online information warfare: Case study on Russia’s war on Ukraine*. Hybrid CoE Working Paper 26. European Centre of Excellence for Countering Hybrid Threats, Helsinki. 18. o.

azért tudta felülírni ezt a paradoxont, mert a 2014 utáni intézményi reform fiatal stratégiai kommunikációs szakembereket hozott pozícióba, akiknek szabad kezet adtak a kísérletezésre, és a PR- és reklámszakma önkéntesei is bekapcsolódtak a háborús erőfeszítésbe. A siker előfeltétele nem a professzionális kapacitás önmagában, hanem a hibázás jogának intézményi szavatolása volt[380]. Ez a felismerés a MRM mezoszintjén közvetlen következménnyel jár: a szervezeti reziliencia agilitás-összetevője nem deklarációval, hanem a kockázatvállalási kultúra megteremtésével érhető el.

Az előzetes leleplezés (pre-bunking) hatékonyabb, mint a cáfolat. Az Egyesült Államok 2022 februárjában alkalmazott hírszerzési transzparencia-stratégiája a Validálás (V) dimenzió ellen-validálási képességének történelmi csúcspontja volt. Az ukrán tapasztalat megerősíti: ha a hamis zászlós narratíva már a megjelenése előtt le van leplezve, hatékonysága drasztikusan csökken.

Az információs háború nem ér véget. A legfontosabb ukrán figyelmeztetés: 2022 elején sok nyugati elemző Ukrajna információs győzelmét hirdette, de az ukrán szakemberek nem osztották ezt az optimizmust. A háború elhúzódásával a kognitív fáradtság és a figyelemvesztés nagyobb fenyegetés, mint bármely konkrét dezinformációs kampány. A védekezési ökoszisztéma fenntarthatóságának egy további, ritkán tárgyalt korlátja az önkéntes aktivizmus személyes kockázata. Giles (2023) dokumentálja, hogy az orosz propagandával szembeszálló magánszemélyek – még nagy földrajzi távolságból is – valós fenyegetéseknek vannak kitéve: online zaklatás, doxxolás és valós életbeli beavatkozások formájában. Az álnéven dolgozó aktivistákat az identitásvédelem állandó kényszere terheli. Ugyanakkor a tömegmozgalom megjelenése részben enyhítette a megfélemlítés korábbi bénító hatását: a csoportos fellépés védelmet nyújt az egyénnek, és a dezinformáció-kutatók közösségi támogatási hálózata csökkenti az izolációt[381].

[380] GILES, Keir (2023): *Humour in online information warfare: Case study on Russia's war on Ukraine*. Hybrid CoE Working Paper 26. European Centre of Excellence for Countering Hybrid Threats, Helsinki. 18., 20–22. o.

[381] GILES, Keir (2023): *Humour in online information warfare: Case study on Russia's war on Ukraine*. Hybrid CoE Working Paper 26. European Centre of Excellence for Countering Hybrid Threats, Helsinki. 23–24. o.

6.4.5. Regionális kitettség

A konfliktus Irányítás-dimenziója Magyarország számára kiemelt jelentőséggel bír, mivel szomszédos államként a fizikai és kognitív fenyegetések metszéspontjában helyezkedik el. Az elemzés négy aspektust vizsgál.

COVID-dezinformációs csatornák pivotálása: A Szicherle–Krekó (2020) által dokumentált[382] COVID-időszaki dezinformációs infrastruktúra (Telegram-csatornák, Facebook-csoportok, alternatív médiumok) 2022-ben zökkenőmentesen állt át az Ukrajna-narratívákra. A „Sputnik V mint nemzeti szuverenitás" keretezésből a „béke vs. eszkaláció" dichotómiába való átmenet azért volt lehetséges, mert az infrastruktúra (a csatornák, a közönség, a bizalomelőleg) változatlanul rendelkezésre állt. Ez a G–M–T–V lánc Terítés (T) dimenziójának egyik legfontosabb tanulsága: a dezinformációs csatornák nem témaspecifikusak, hanem transzferálhatók.

Narratív átgyűrűzés és identitás-fegyveresítés: Magyarország közvetlenül ki van téve a narratívák átgyűrűzésének: mind az orosz információs műveletek (különösen a kárpátaljai magyar kisebbség fenyegetettségének felnagyítása a feszültségkeltés érdekében – a Hybrid CoE Paper 24 által dokumentált identitás-fegyveresítés egyik formája), mind az ukrán kommunikáció (a tranzitország szerepének keretezése) aktívan formálja a hazai közvéleményt. A WP 29 dokumentálja, hogy a Kreml-dezinformáció leghatékonyabb formája nem a nyílt propagandaüzenet, hanem az, amely a célközönség meglévő sérelmeire és belső törésvonalaira épít – Magyarország esetében a NATO-szkepticizmus, az EU-ellenesség és a migrációs félelem a legfogékonyabb felületek.

Reziliencia és a CORE-modell: A Hybrid CoE CORE Comprehensive Resilience Ecosystem modellje a civic, governance és services terek közötti interdependenciák kezelését modellezi. Magyarország számára, mint minden ország számára, ez azt jelenti, hogy a kiberreziliencia elválaszthatatlan a kognitív rezilienciától: a rendszereket és az elméket egyszerre kell védeni. A kritikus infrastruktúrák (energia, bankrendszer) elleni sikeres kibertámadás azonnali pánikot és bizalomvesztést okoz, amit a dezinformációs aktorok kihasználhatnak a kormányzati

[382] SZICHERLE Patrik – KREKÓ Péter (2020): *Burjánzanak az álhírek a koronavírus nyomában*. Political Capital, Budapest. 3–8. o. A COVID- dezinformáció magyarországi megjelenési mintáinak elemzése.

cselekvőképesség aláásására. A vonatkozó 19. táblázat: I-tábla (összegző) – Irányítás dimenzió, 2014 vs. 2022–2025 címmel a mellékletben található.

6.5. MULTIMODÁLIS REZILIENCIA MÁTRIX (MRM): 2022–2025-ös kontroll-leltár

A 4.5 alfejezet logikáját követve a 6. fejezet zárásaként elkészítem a 2022–2025-ös MRM kontroll-leltárt. A cél azonos a 4. fejezetével: nem a védekezés idealizálása, hanem annak rögzítése, hogy a kontrollok milyen szinten állnak, hol vannak rések, és milyen további intézkedések szükségesek. A 4.5-ben dokumentált 2014-es sarokpont és a jelenlegi állapot közötti összehasonlítás teszi lehetővé, hogy a 7. fejezet (Keresztmetszeti összehasonlítás) azonos indikátorkosárban dolgozzon.

A vonatkozó 20. táblázat: MRM-tábla (kontroll-leltár) – 2022–2025 címmel a mellékletben található.

6.5.2. A G–M–T–V lánc 2022–2025-ös végállapot-konfigurációja

A 4.5.2 logikáját követve – ahol a 2014-es G–M–T–V sarokpontot rögzítettem – alább a 2022–2025-ös végállapot-konfigurációt írom le. Ez a konfiguráció az a végpont, amelyhez az 5. fejezet Anchor- és Reziliencia-mérföldkövei elvezettek, és amelyből a 7. fejezet keresztmetszeti összehasonlítása indul.

G (Generálás) – nagyon alacsony költségű, végtelen variáns. A tartalomvariánsok előállítása 2025-re a nullaköltséghez közelít: a nagy nyelvi modellek percek alatt produkálnak többnyelvű, stilisztikailag változatos szövegeket; a generatív képmodellek hitelesnek tűnő vizuális „bizonyítékokat” hoznak létre; a hangklónozás és a deepfake-videó szinte detektálhatatlan. A Generálás dimenzió a 2014-es „kézműves” állapotból az ipari tömegtermelés szintjére lépett. Az FMK-mátrix szempontjából ez azt jelenti, hogy az összes modalitáscella (szöveg, kép, hang, video) párhuzamosan, automatikusan tölthető.

M (Mosás) – professzionális, szervezeti háttérrel. A forrás- és kontextus-mosás a 2014-es primitív álprofiloktól a Doppelgänger-szintű hitelesség-eltérítésig fejlődött. Az SDA/CGE/Struktura szervezeti háttér ipari szintű kapacitást biztosít. A „békepárti” keretezés a leghatékonyabb mosási réteg, mert az orosz stratégiai célt a célközönség saját értékrendjébe ágyazza. A Mosás dimenzió 2025-re a G–M–T–V lánc legkritikusabb eleme: a generálási költség nullához közelít, tehát a műveleti szűk keresztmetszet nem a tartalom előállítása, hanem a hiteles forrásba csomagolása.

T (Terítés) – négyrétegű, multimodális, multiplatform. A terjesztés a 2014-es koordinált humán hálózatokról a négyrétegű architektúrára (állami→proxy→zárt→fizikai) váltott. A zárt csatornák (Telegram) sérülékenysége 2024-ben megmutatkozott, de a rendszer gyorsan adaptálódik: a VPN-használat, az alternatív platformok és a fizikai szabotázs-csatorna alternatívát biztosítanak.

V (Validálás) – kétirányú verseny. Ez a dimenzió 2022-ben a történelem legnagyobb fordulópontján ment keresztül: a védekező fél először képes volt a támadó előtt validálni a helyzetet (pre-bunking). 2025-re azonban a kognitív nihilizmus erodálja mindkét oldal validálási képességét: ha az igazság fogalma maga válik kérdésessé, sem a támadó (hazugság hitelesítése), sem a védekező (igazság bizonyítása) nem tud hatékonyan működni. A Validálás dimenzió a G–M–T–V lánc leginstabilabb eleme.

6.6. Szintézis: A 2022–2025-ös konfiguráció helye az SFÖ-összehasonlításban

A fejezet a H–E–I mátrix mindhárom dimenziójában dokumentálta a 2022–2025-ös konfiguráció radikális eltérését a 4. fejezet 2014-es sarokpontjától.

A stratégiai paradoxon – amelyet az 1. fejezet (1.2) fogalmazott meg – a következőképpen oldódik fel: 2014-ben az alacsony technológia + magas narratív koherencia + nulla ellen-validálás = sikeres bénulás. 2022-ben a magas technológia + alacsony narratív koherencia + magas ellen-validálás = a bénulás elmaradása. A H2 hipotézis (a bénító hatás elmaradása) igazolódik: a Híd-időszak alatt felépült reziliencia és az OSINT-tevékenység megtörte az orosz narratív dominanciát. A H4 hipotézis (a technológiai paradoxon) szintén igazolódik: a generatív MI és az automatizáció nem a meggyőzés minőségét, hanem a műveleti zajszintet növelte, ami a kognitív nihilizmus felé tolja a rendszert.

A 2024–2025-ös dinamika azonban arra figyelmeztet, hogy a védekezői fölény nem tartós állapot, hanem fenntartandó képesség. A Hybrid CoE Working Paper 29 (2024) konklúziója arra hívja fel a figyelmet, hogy a Kreml-dezinformáció hatása továbbra is mérhető és többdimenziós, a nyugati optimizmus ellenére. A Validálás dimenzió mindkét oldala erodálódik: a támadó validálási kísérletei egyre kifinomultabbak, a védekező ellen-validálási képessége pedig a kognitív fáradtság és a politikai polarizáció miatt csökken.

A 7. fejezet (Keresztmetszeti összehasonlítás) a jelen fejezet és a 4. fejezet H–E–I kódolásait, FMK-rács celláit és MRM kontroll-leltárait azonos indikátorkosárban szintetizálja. A 8. fejezet

(Szintézis és védekezés) az MRM operatív keretét alkalmazza a feltárt sérülékenységekre – különös tekintettel a Mosás (M) dimenzió szűk keresztmetszetére és a Validálás (V) dimenzió kétoldalú eróziójára, amelyek a 2025–2030-as időszak fő fenyegetésvektorai.

7. KERESZTMETSZETI ÖSSZEHASONLÍTÁS – A MINŐSÉGTŐL A MENNYISÉGIG

A disszertáció ezen fejezete a 2014-es krími válság és a 2022–2025-ös totális háború kognitív hadviselési tapasztalatait veti össze a H–E–I diagnosztikai mátrix mentén. Az összehasonlítás célja annak igazolása, hogy a technológiai fejlődés nem csupán az információs műveletek sebességét, hanem azok alapvető természetét is megváltoztatta. Ez a transzformáció a többrétegű védelmi stratégia szükségességét vetíti előre, mivel a támadó fél a puszta mennyiségi fölénytől elmozdult a minőségi, algoritmikus manipuláció irányába.

A fejezet központi tézise kettős. Egyrészt: míg 2014-ben a reflexív kontroll (reflexive control) egy szűk elit döntéshozatali mechanizmusait célozta, addig 2025-re a nem konszenzuális befolyásolás (non-consensual persuasion) már a társadalom teljes szövetét – beleértve a kritikus infrastruktúrák bizalmi bázisát is – támadja. Másrészt: a technológiai túlerő nem automatikusan jelent stratégiai sikert, amennyiben a védekező fél képes a társadalmi reziliencia és a tudatos információs elhárítás szinkronizálására. Az összehasonlítás során kiemelt figyelmet fordítunk az információs környezetszennyezésre, amely a Wardle és Derakshan által leírt[383] information disorder taxonómiában értelmezhető, és amely a kognitív fáradtság révén igyekszik elérni a védelmi rendszerek áttörését.

A két korszak közötti különbségek három pillér mentén rendszerezhetők. Először: a technológiai aszimmetria változása – a kezdetleges bot-hálózatoktól az automatizált generatív mesterséges intelligencia (a továbbiakban: AutoGenAI) korszakáig, ahol a szintetikus tartalom már nem különíthető el az organikus információtól[384]. Másodszor: a védelmi intézményesülés foka – a 2014-es szabályozási vákuumtól a Digitális Szolgáltatásokról szóló Rendelet (a továbbiakban: DSA) és

[383] WARDLE, Claire – DERAKHSHAN, Hossein (2017): Information Disorder: Toward an interdisciplinary framework for research and policymaking. Council of Europe Report. 48–52. o.

[384] Juršėnas et al. (2022): *The Role of AI in the Battle Against Disinformation.* Riga: NATO Strategic Communications Centre of Excellence. Online: https://stratcomcoe.org/publications/the-role-of-ai-in-the-battle-against-disinformation/238

a DISARM-keretrendszer által biztosított strukturált védekezésig[385]. Harmadszor: a társadalmi reziliencia állapota – az információs sokkhatástól a kognitív immunizáció módszertani alkalmazásáig, amely az emberi tűzfal (human firewall) koncepciójára építve próbálja megfékezni a kognitív nihilizmus terjedését.

Az összehasonlító elemzés diagnosztikai pontosságát növeli a propaganda klasszikus, a forrás azonosíthatósága szerinti hármas felosztásának alkalmazása. A modern orosz információs hadviselés e három réteg szimbiózisára épül. A fehér propaganda esetében a forrás nyíltan azonosítható, és a közölt információk – bár szelektívek – többnyire ellenőrizhetőek. Erre példa az állami média (RT, Sputnik) hivatalos narratívája mind 2014-ben, mind 2022-ben. A szürke propaganda forrása bizonytalan: itt a dezinformációt álcázott híroldalak és látszólag független szakértők terjesztik. Végül a fekete propaganda során a forrás tudatosan hamis. Míg 2014-ben Oroszország dominánsan a szürke és fehér tartományban operált – például a „zöld emberkék" körüli narratív bizonytalanság fenntartásával –, addig 2022-re a technológiai fejlődés lehetővé tette a fekete propaganda ipari méretű alkalmazását. A Doppelgänger-művelet (NATO StratCom COE: The Doppelganger Case)[386] ennek paradigmatikus példája: a titkos bot-hálózatok és hamis identitású profilok révén a támadó fél közvetlenül a célországok belső társadalmi vitáiba avatkozott be, elfedve az állami jelleget.

A technológiai dominancia megszerzésének folyamatát a trend uralása (commanding the trend) fogalmával írja le, amelyet a 3. fejezetben részletesen tárgyaltam. Ez a modell négy szakaszból álló műveleti láncot azonosít: narratíva-injektálás, algoritmikus felerősítés bot-hálózatok segítségével, véleményvezérek általi legitimáció, végül a fősodratú média általi átvétel. Ez az operacionalizálás teszi mérhetővé a fegyvernek minősülő kommunikáció (a továbbiakban: FMK) hatásmechanizmusát mindkét vizsgált korszakban.

---

385 Newman, Hannah (2022): *Foreign Information Manipulation and Interference Defence Standards: Test for Rapid Adoption of the Common Language and Framework „DISARM".* Helsinki – Riga: European Centre of Excellence for Countering Hybrid Threats – NATO Strategic Communications Centre of Excellence. Online: https://stratcomcoe.org/publications/foreign-information-manipulation-and-interference-defence-standards-test-for-rapid-adoption-of-the-common-language-and-framework-disarm-prepared-in-cooperation-with-hybrid-coe/253

386 Sessa, Maria Giovanna – Miguel, Raquel (2024): *The Doppelganger Case: Assessment of Platform Regulation on the EU Disinformation Environment.* Riga: NATO Strategic Communications Centre of Excellence. Online: https://stratcomcoe.org/publications/the-doppelganger-case-assessment-of-platform-regulation-on-the-eu-disinformation-environment/304

7.1. A Strukturált Fókuszált Összehasonlítás (SFÖ) keretei

Ebben a fejezetben érkezünk el a disszertáció elemzési szakaszának csúcspontjához. A korábbi fejezetekben részletesen bemutatott eseménysorokat – a 2014-es krími annexiót (4. fejezet) és a 2022-től 2025-ig tartó totális háborút (6. fejezet) – közvetlenül egymás mellé állítjuk. Az elemzés során a Strukturált Fókuszált Összehasonlítás (Structured Focused Comparison – SFÖ) módszertanát alkalmazom, amely a két esettanulmányos összehasonlításokra épülő megközelítések kanonikus változata a politikatudományi kutatásban. Ez a gyakorlatban azt jelenti, hogy mindkét esettanulmányra ugyanazt az indikátorkosarat alkalmazom, így biztosítva a tudományos összevethetőséget.

A módszertani szigorúság érdekében a Cullen[387] által a Hybrid CoE számára kidolgozott stratégiai elemzési keretet is figyelembe veszem, amely a hibrid fenyegetések többdimenziós értékelésére kínál eszköztárat. A Giannopoulos, Smith és Theocharidou által megfogalmazott konceptualizáció[388] szerint a hibrid fenyegetések nem egyszeri akciók, hanem a társadalmi sebezhetőségek rendszerszintű kihasználására irányuló folyamatos műveletek. Ez a megértés orientálja az összehasonlítást, különösen a társadalmi reziliencia és az intézményi válaszképesség tekintetében.

Az általam kidolgozott H–E–I (Helyzet–Előrejelzés–Irányítás) diagnosztikai mátrixot használom vezérfonalként. A H–E–I mátrix a 2. fejezetben ismertetett FMK-rács (aktor–csatorna/infrastruktúra–műveleti termék) kategóriáira épül: míg az FMK-rács az egyes műveletek szintjén rögzíti a támadó kommunikáció elemeit – az aktor azonosíthatóságát (fehér/szürke/fekete), a csatorna és infrastruktúra jellemzőit (platform-típus, algoritmikus felerősítés, szabályozottsági fok) és a műveleti termék konfigurációját (narratíva-injektálás, kognitív hatás: sokk, fáradtság, nihilizmus) –, addig a H–E–I mátrix ezeket a mikroszintű megfigyeléseket aggregálja a stratégiai

[387] Cullen, Patrick (2018): *Hybrid Threats as a New „Wicked Problem" for Early Warning.* (Hybrid CoE Strategic Analysis 8.) Helsinki: The European Centre of Excellence for Countering Hybrid Threats. Online: https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-8-hybrid-threats-as-a-new-wicked-problem-for-early-warning/

[388] Giannopoulos, Georgios – Smith, Hanna – Theocharidou, Marianthi (2021): *The Landscape of Hybrid Threats: A Conceptual Model.* Luxembourg – Helsinki: Publications Office of the European Union – European Centre of Excellence for Countering Hybrid Threats. Online: https://www.hybridcoe.fi/publications/the-landscape-of-hybrid-threats-a-conceptual-model/

összehasonlítás szintjére. Hasonlóképpen, a 6. fejezet záróharmadában bemutatott G–M–T–V műveleti lánc (Generálás–Mosás–Terítés–Validálás) a támadó oldal műveleti logikáját rögzíti, amelyet az alábbi összehasonlító táblázat a védelmi oldal válaszaival vet össze. Az alábbi referenciatáblázat az összehasonlítás indikátorkosarát rögzíti – ez a struktúra határozza meg a fejezet felépítését.

A vonatkozó 21. táblázat: A kognitív hadviselés dimenzióinak összehasonlító mutatói (2014 vs. 2025) címmel a mellékletben található.

A fejezet a mátrix oszlopai mentén halad. Először a Helyzet (Input) dimenzióját elemzem, ahol a kézműves tartalomgyártást vetem össze az AutoGenAI ökoszisztémával. Ezt követi az Előrejelzés (Process), amely a döntéshozatali ciklusok és a pszichológiai hatásmechanizmusok ütköztetésére fókuszál. Végül az Irányítás (Control) dimenziójában a védekezés intézményesülését vizsgálom. Az összehasonlítás célja a H4-es hipotézisben megfogalmazott paradoxon bizonyítása: a mennyiségi ugrás nem feltétlenül jár együtt a stratégiai hatékonyság növekedésével. A fejezet eredményei a következő, 7. fejezetben (Keresztmetszeti összehasonlítás) kerülnek szintetizálásra, ahol az OxIPO és a HIP modellek szintéziseként bemutatásra kerül a FMK Kognitív Olló elméleti konstrukciója; a védekezési keret operatív kifejtését a 8. fejezet (Multimodális Reziliencia Mátrix) tartalmazza.

7.2. Helyzet (Input) – A minőségtől a mennyiségig: Technológiai váltás és narratív transzformáció

Az összehasonlító elemzés első pilléreként a műveleti környezet bemeneti adatait vizsgálom. Az input tényezők határozzák meg azt az információs gravitációt, amelyben a célszemélyeknek és szervezeteknek döntéseket kell hozniuk. A 2014-es krími annexió és a 2022 utáni totális háború között eltelt évtized nem egyszerűen technikai fejlődést, hanem paradigmatikus váltást hozott az FMK alkalmazásában. Míg 2014-ben a befolyásolás még manuálisan vezérelt narratív keretek között zajlott, addig a 2025-re kialakult állapot az iparosítás szintjére emelte a kognitív hadviselést. Az AutoGenAI és a szintetikus tartalom tömeges alkalmazása olyan információs környezetszennyezést hoz létre, amely már nemcsak a politikai véleményformálást célozza, hanem közvetlen fenyegetést jelent a kritikus infrastruktúra bizalmi stabilitására is.

7.2.1. A manuális trollkodástól az AutoGenAI ökoszisztémáig

A 2014-es alapállapotot a szakirodalom a „kézműves dezinformáció” koraként azonosítja. Ahogy a 4. fejezetben bemutattam, az orosz információs fölény ekkor az Internet Research Agency (IRA) által mozgatott humán operátorokra támaszkodott, akik központilag meghatározott narratív panelek alapján, manuálisan kommenteltek. A NATO StratCom COE[389] 2016-os részletes tartalomelemzése – amely az orosz média (Regnum, Komsomolskaya Pravda, TV Zvezda) ukrajnai vonatkozású tartalmait vizsgálta 2014 áprilisa és decembere között, 25 strukturált interjúval kiegészítve – rávilágított, hogy az orosz információs hadviselés már ekkor tudatosan integrálta a politikai, média- és katonai dimenziókat. Az orosz katonai doktrína 2014 decemberében explicit módon rögzítette: az információs fölény elengedhetetlen a modern háború megnyeréséhez. Ugyanakkor a műveleti kapacitásokat szigorú fizikai korlátok – munkaidő, nyelvtudás mélysége, írássebesség – határolták be.[390] [391] [392]. Kofman és Rojansky elemzése[393] szerint a krími hibrid művelet sikerét nem a mennyiségi fölény, hanem a stratégiai meglepetés és a helyi lakosság identitáspolitikai manipulálása biztosította. Farwell 2019-ben hasonló következtetésre jut[394], amikor kiemeli, hogy Putin a jogi keretezéstől (lawfare) a médiakontrollig terjedő eszköztárat vetett be, de mindez még kézzel irányított, szűk spektrumú műveleti keretben zajlott.

---

[389] Sazonov, Vladimir – Mölder, Holger – Müür, Kristiina (szerk.) (2016): *Russian Information Campaign against the Ukrainian State and Defence Forces: April–December 2014.* Riga: NATO Strategic Communications Centre of Excellence. Online: https://stratcomcoe.org/publications/russian-information-campaign-against-ukrainian-state-and-defence-forces/174

[390] Chen, Adrian (2015): The Agency. *The New York Times Magazine,* 2015. június 7. Online: https://www.nytimes.com/2015/06/07/magazine/the-agency.html

[391] Darczewska, Jolanta (2014): *The Anatomy of Russian Information Warfare: The Crimean Operation, a Case Study.* (OSW Point of View, 42.) Varsó: Centre for Eastern Studies. Online: https://www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_information_warfare.pdf

[392] Giles, Keir (2016): *Russia's „New" Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power.* London: Chatham House. Online: https://www.chathamhouse.org/2016/03/russias-new-tools-confronting-west

[393] Kofman, Michael – Rojansky, Matthew (2015): A Closer Look at Russia's „Hybrid War." *Kennan Cable,* No. 7. Washington, D.C.: Wilson Center, 2015. április. Online: https://www.wilsoncenter.org/publication/kennan-cable-no7-closer-look-russias-hybrid-war

[394] Farwell, James P. (2019): War and Truth. *Defence Strategic Communications,* Vol. 7, 133–145. o. Online: https://doi.org/10.30966/2018.RIGA.7.5

Ezzel szemben a 2022–2025-ös időszak – ahogy azt a 6. fejezetben részleteztem – elhozta az iparosított dezinformációt. A korábbi manuális megoldásokat felváltotta az AutoGenAI és a nagy nyelvi modellekre (LLM) épülő automatizáció. A NATO StratCom COE 2021-es The Double-Edged Sword of AI[395] című alapkutatása dokumentálja ezt a paradigmaváltást: a mesterségesintelligencia-alapú tartalomgenerálás – beleértve a szöveg-, kép- és hangszintézist – már 2021-re képes volt bekezdésnyi, emberi szövegtől nehezen megkülönböztethető tartalom előállítására. A jelentés három kulcsdimenziót azonosít: a tartalom előállítása (content preparation), a terjesztés automatizálása (spreading disinformation) és a mikro-célzás (micro-targeting). A bot-piacok 2019-es árazási adatai érzékeltetik az átmenet gazdasági oldalát: Frischlich és munkatársai 2022-ben a Darknet-en és a nyílt interneten egyaránt elérhető bot-szolgáltatások szisztematikus feltérképezését végezték el[396], dokumentálva a manipulációs szolgáltatások piacosodását. Kutatásuk szerint egy követő megszerzése mindössze egyetlen eurócentbe, egy generált komment pedig 62 centbe került. Ez az alacsony belépési küszöb a kézműves dezinformációtól az iparosított felé vezető átmenet gazdasági hajtóerejét jelzi: ami korábban szervezett humán kapacitást igényelt, az automatizált piactérré alakult, ahol bárki – állami és nem állami szereplő egyaránt – hozzáférhet a befolyásolási eszközökhöz. A generatív MI-vel ez a gazdasági küszöb radikálisan lecsökkent. A kutatók megállapítása szerint a nagy államok válnak a legfontosabb dezinformációs szereplőkké, és egyben a potenciális MI-szupergonoszokká is, amennyiben képesek: 1) jó minőségű, mikro-célzott dezinformáció tömegtermelésére, 2) észlelhetetlen közösségi botnetek működtetésére, és 3) a bot-automatizálási képességek folyamatos fejlesztésére.

Az iparosítás 2024-re már empirikusan dokumentálható lett. A NATO StratCom COE (2024) Virtual Manipulation Brief (VMB) című jelentése 17 koordinált csoportot azonosított 344 forrás mentén, túlnyomórészt a Telegramon (36,83%) és a Twitter/X-en (39,43%). Ezek a csoportok nagy nyelvi modelleket alkalmaznak automatizált tartalom-generálásra és -terjesztésre, miközben az MI-

[395] Juršėnas et al. (2021): *The Double-Edged Sword of AI: Enabler of Disinformation.* Riga: NATO Strategic Communications Centre of Excellence. Online: https://stratcomcoe.org/publications/the-double-edged-sword-of-ai-enabler-of-disinformation/221

[396] Frischlich, Lena – Mede, Niels G. – Quandt, Thorsten (2020 [2019]): The Markets of Manipulation: The Trading of Social Bots on Clearnet and Darknet Markets. In: Grimme, Christian – Preuss, Mike – Takes, Frank – Waldherr, Annie (szerk.): *Disinformation in Open Online Media. MISDOOM 2019.* (Lecture Notes in Computer Science, 12021.) Cham: Springer, 95–110. o. Online: https://doi.org/10.1007/978-3-030-39627-5_8

hallucinációk – kitalált tények, értelmetlen szövegek – jelzik a rendszer korlátait. A VMB egy konkrét esetet is dokumentál: egy felhasználó, aki a Twitter/X platformon posztolt, öt hónappal korábban egy pro-orosz bot-hálózat által injektált narratívát visszhangzott – a mém-átvitel sebessége és közvetítettsége jelzi az ökoszisztéma érettségét. A DISARM-keretrendszer és a RESIST2-módszertan[397] együttes alkalmazása jelentette a védelmi fél válaszkísérletét erre a kihívásra, standardizálva az adatcserét a fenyegetés-azonosítás és a reakcióidő csökkentése érdekében.

Wallner, Copeland és Giustozzi (2025) RUSI-tanulmánya[398] tovább mélyíti a képet: az orosz befolyásolási ökoszisztéma szereplői – a Wagner-affiliált csatornáktól a NoName057(16) hacktivist csoportig – nemcsak eszközként, hanem narratív és stratégiai elemként is integrálják a mesterséges intelligenciát. A Wagner-csatornák MI-alapú oktatási anyagokat terjesztenek, toborzási felhívásokat intéznek neurális hálózat-művészekhez, és bespoke chatbotokat építenek befolyásos figuráik mintájára. Ez a váltás azt jelzi, hogy az MI-t nemcsak a „mit” (tartalom), hanem a „hogyan” (munkafolyamat) és a „kinek” (célzás) tekintetében is bevetik.

Az AutoGenAI ökoszisztéma műveleti minőségi ugrása abban ragadható meg, hogy a generatív MI nem csak tartalmat állít elő, hanem munkafolyamatot automatizál. A phishing támadások hatékonysága nő, a hangutánzás és deepfake-képességek megjelenésével a megtévesztés a vishing irányába terjed, és az MI által támogatott bot-aktivitás a közösségi platformokon automatizálja a posztolást. A The Role of AI (NATO StratCom COE 2022) kiegészítő tanulmánya a védelmi oldalt vizsgálva rámutat, hogy a deepfake-detektálás egyre nehezebb: míg az izolált hamis képek azonosítása már problémás, a videó- és hangmanipulációk felismerése a laikus felhasználó számára gyakorlatilag lehetetlen. A szintetikus tartalom detektálásának nehézsége közvetlenül alátámasztja a hazug osztalékot (Liar’s Dividend): minden tartalom – a hiteles is – gyanússá válik, ami nem az egyes hazugságokat, hanem a hitelesség fogalmát magát teszi zárójelbe. Amint SCHIFF és

[397] Pamment, James (2021): *RESIST 2 Counter Disinformation Toolkit.* London: UK Government Communication Service. Online: https://www.communications.gov.uk/wp-content/uploads/2021/11/RESIST-2-counter-disinformation-toolkit.pdf

[398] WALLNER, COPELAND & GIUSTOZZI (2025): i. m. (ld. fentebb).

munkatársai (2023: 2–3) rámutatnak, a deepfake-hatás már a létezés puszta lehetősége révén is érvényesül, függetlenül attól, hogy az adott tartalom valóban manipulált-e.

Ez a váltás a H4-es hipotézisem szempontjából kulcsfontosságú: a technológia révén az információs zajszint elért egy telítettségi pontot, ahol a műveleti cél már nem az egyén meggyőzése, hanem a társadalmi szintű kognitív túlterhelés. Az AutoGenAI ökoszisztéma lehetővé teszi a narratívák végtelenített és automatizált tesztelését (A/B tesztelés ipari léptékben), ami a védelmi oldalon a hagyományos, humán-alapú tényellenőrzés teljes ellehetetlenüléséhez vezet.

7.2.2. Narratív koherencia a narratív káosszal szemben

A technológiai váltás mellett a narratívák szerkezete is alapvető változáson ment keresztül. A 2014-es műveleteket rendkívül koherens mesternarratíva köré építették fel: a kijevi náci junta, a Krím hazatér, az oroszok védelme. Ez a célzott üzenetrendszer alkalmas volt arra, hogy a felkészületlen nyugati döntéshozókban bizonytalanságot keltsen. Farwell elemzése[399] – amely Freedman Ukraine and the Art of Strategy[400] és Zygar All the Kremlin's Men című[401] munkáit is ismerteti – rámutat, hogy Putin stratégiai kommunikációja a jogi keretezést (lawfare) a narratív uralommal ötvözte: formálisan parlamenti felhatalmazást kért a katonai beavatkozáshoz, referendumot szervezett a Krímben, és gondosan legális köntösbe csomagolta a területszerzést. ZYGAR feltárja, hogy a Kreml belső döntéshozatala során a védelmi miniszter, Sojgu óvatosságra intett, és a döntés inkább improvizatív, semmint előre megtervezett volt – ami rávilágít, hogy a stratégiai kommunikáció sikeressége nem feltétlenül tükrözi a belső koherenciát. Mindeközben az állami média – amelyet a NATO StratCom COE (2015) eredeti kampányelemzése részletesen dokumentál – három egymást erősítő csatornán (állami televízió, online portálok, közösségi média) koordinálta a narratívákat. A Kreml kommunikációs stratégiáját részletesen elemző NATO StratCom COE-kötet dokumentálja, hogy az elnöki adminisztráció úgynevezett temnik-rendszere – verbálisan közvetített tematikus iránymutatás – biztosította, hogy a 15 legnagyobb orosz médium szinte azonos szerkesztői pozíciót képviseljen, és a kommunikáció egésze három pillérre épüljön: Oroszország heroizálása, Ukrajna

[399] Farwell, James P. (2019): War and Truth. *Defence Strategic Communications,* Vol. 7, 133–145. o. Online: https://doi.org/10.30966/2018.RIGA.7.5

[400] Freedman, Lawrence (2019): *Ukraine and the Art of Strategy.* New York: Oxford University Press.

[401] Zygar, Mikhail (2016): *All the Kremlin's Men: Inside the Court of Vladimir Putin.* New York: PublicAffairs.

démonizálása és a Nyugat diszkreditálása.[402] Ebben a fázisban a reflexív kontroll még lineáris módon, a logikai láncolatok mentén igyekezett befolyásolni a stratégiai döntéshozatalt.

Ezzel éles ellentétben áll a 2022 utáni időszak narratív káosza. Mint ahogy a 6. fejezetben az orosz narratívák váltakozásáról írtam, a kommunikáció itt már nem a koherenciára épít. Egymásnak ellentmondó üzenetek – nácítlanítás, biolaborok, sátánisták elleni szent háború – zúdulnak a befogadóra. Giles aktualizált elemzése szerint ez a stratégiaváltás szorosan összefügg az MI-eszközök terjedésével: a cél immár nem egy alternatív valóság megteremtése, hanem a valóságérzékelés felszámolása. Giles (2016) már a 2014-es konfliktus nyomán rögzítette ennek előzményét: az orosz információs műveletek célja nem az, hogy a célközönség elhiggye az orosz narratívát, hanem hogy minden információforrást megbízhatatlannak tekintsen. A Levada Központ felmérésében a megkérdezettek 38%-a elismerte, hogy az orosz hatóságok nem mondanak igazat az ukrajnai csapatok jelenlétéről, de úgy ítélte meg, hogy a tagadás a jelenlegi nemzetközi helyzetben helyes – ami az intézményesített hazugság társadalmi elfogadottságának empirikus bizonyítéka[403]. A narratív koherenciavesztés az orosz kommunikáció alkalmazkodóképességének korlátait is tükrözi: Giles dokumentálja, hogy az orosz humorpróbálkozások ismételten kudarcot vallottak, virális terjedés nélkül csak a meglévő támogatói kört érve el. A kulturális érzéketlenség még a szomszédos Fehéroroszországban is megmutatkozott, ahol a 2020-as tüntetések utáni orosz propaganda csapatok összekeverték a belarusz és az ukrán nyelvet, és teljesen félre értelmezték a helyi célközönséget[404]. A PAZIUK és munkatársai (2025) a Frontiers in Artificial Intelligence folyóiratban publikált kutatása – amely 68 206 orosz nyelvű posztot elemzett az Attack-Index módszerrel – számszerűsíti ezt a tendenciát: a vizsgált tartalmak 52,7%-a negatív érzelmeket

---

[402] BOLT, Neville – FRIDMAN, Ofer – WINTER, Charlie et al. (2023): *Kremlin Communication Strategy for Russian Audiences Before and After the Full-Scale Invasion of Ukraine*. NATO Strategic Communications Centre of Excellence, Riga, ISBN 978-9934-619-47-2. 7–9., 49–51. o. A kötet dokumentálja a Kreml kommunikációs stratégiájának centralizált rendszerét: a *temnik* (tematikus útmutató) verbális irányítás alatt a 15 legnagyobb orosz médium szinte azonos szerkesztői pozíciót képviselt. A Levada Center adatai szerint a háborús támogatottság 72%-on állt.

[403] GILES, Keir (2016): *Russia's „New" Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power*. London: Chatham House, Russia and Eurasia Programme. 38. o. A Levada Központ felmérése szerint a megkérdezettek 37%-a úgy vélte, Oroszország igazat mond; további 38%-uk úgy ítélte meg, hogy nem, de „a jelenlegi nemzetközi helyzetben helyes, ha Oroszország tagad."

[404] GILES, Keir (2023): *Humour in online information warfare: Case study on Russia's war on Ukraine*. Hybrid CoE Working Paper 26. European Centre of Excellence for Countering Hybrid Threats, Helsinki. 19. o.

célzott meg, míg mindössze 5,1% hordozott pozitív üzenetet. Ez a rendkívül aszimmetrikus arány bizonyítja, hogy a cél nem az alternatív valóság megteremtése, hanem a társadalom érzelmi és kognitív kimerítése.[405]

A generatív videók és a hiperrealisztikus deepfake-ek korában a befogadó már nem azt kérdezi: „Mi az igaz?“, hanem azt: „Lehetséges-e egyáltalán az igazság megismerése?” Ez a váltás a Wardle-Derkhshan-féle (2017) information disorder taxonómiájának[406] legmagasabb fokozata, ahol az algoritmikus manipuláció már nem egy konkrét hazugságot, hanem a hitelesség fogalmát magát teszi zárójelbe. A Fauconnier és Turner által leírt[407] fogalmi keverés (conceptual blending) mechanizmusa révén a hamis és valós elemek szétválaszthatatlanul egybeolvadnak a befogadó kognitív keretében. A Csepeli[408] és Síklaki[409] által a magyar pszichológiai irodalomban leírt manipulációs technikák – a tekintélyérv, a hamis konszenzus, a félelemkeltés – ezáltal ipari léptékben és algoritmikus sebességgel válnak bevethetővé.

A FMK Kognitív Olló modell érvényességi határait a NATO StratCom COE afrikai jelentése (2021) segít kijelölni, amely hárommódszerű esettanulmányként – 561 RT France/Sputnik France cikk tartalomelemzésével, pro-orosz közösségi média analízisével, valamint a Közép-afrikai Köztársaságban (CAR) végzett terepkutatással – dokumentálja az orosz információs műveletek afrikai kiterjesztését. A kutatás nyolc domináns orosz narratívát azonosított a CAR kontextusában: Oroszország mint felszabadító, a Nyugat mint gyarmatosító, a pan-afrikanizmus támogatása, az ENSZ és a francia erők diszkreditálása, valamint a demokratikus választások destabilizálása. A Prigozsin-hálózat infrastruktúrája – a Lengo Songo rádióállomásástól a fizetett Facebook-

[405] Paziuk et al. (2025): Decoding manipulative narratives in cognitive warfare: a case study of the Russia-Ukraine conflict. Frontiers in Artificial Intelligence, 8. köt. DOI: 10.3389/frai.2025.1537453. Adatgyűjtés: 2022. november – 2024. december; 68 206 orosz nyelvű közösségimédia-poszt; módszer: sajátfejlesztésű Attack-Index érzelmi polaritás-elemzés + nagy nyelvi modellekkel végzett narratíva-klaszterezés. A 52,7%/5,1%-os negatív/pozitív arány a teljes vizsgált korpuszra vonatkozik.

[406] Wardle, Claire – Derakhshan, Hossein (2017): *Information Disorder: Toward an Interdisciplinary Framework for Research and Policymaking.* Strasbourg: Council of Europe. Online: https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html

[407] Fauconnier, Gilles – Turner, Mark (2002): *The Way We Think: Conceptual Blending and the Mind's Hidden Complexities.* New York: Basic Books.

[408] Csepeli György (1997): *Szociálpszichológia.* Budapest: Osiris Kiadó.

[409] Síklaki István (1994): *A meggyőzés pszichológiája.* Budapest: Scientia Humana.

oldalakon át a helyi NGO-k szponzorálásáig – az IRA 2016-os módszereivel mutat strukturális hasonlóságot. A kulcsmegállapítás: míg 2022-ben Ukrajna ellen a narratív koherencia széthullott, Afrikában a Kreml továbbra is koherens, célzott narratívákat épít minimális költségvetéssel, domináns jelenlétet biztosítva. Ez megerősíti, hogy a narratív koherencia kontextusfüggő – a hazai/ukrajnai kudarc nem jelenti az orosz információs műveletek globális kudarcát.[410]

7.2.3. Az információs ökoszisztéma zártsága és nyitottsága

A műveleti tér fizikai-digitális kereteit sem hagyhatjuk figyelmen kívül. 2014-ben a Facebook és a Twitter még a demokratizálódás eszközeiként éltek a köztudatban, és a platformok moderációs elvei gyakorlatilag nem léteztek a dezinformációs kampányokkal szemben. A NATO StratCom COE (2018) 125 platformválaszt elemző kutatása (Industry Responses to Disinformation) dokumentálja, hogy 2016 és 2018 között a három legnagyobb platform válaszstratégiája legjobb esetben is kialakulóban volt, legrosszabb esetben tisztán reaktív. A kutatók tíz beavatkozási kategóriát azonosítottak, de egyikben sem találtak érdemi változást a platformok felhasználási feltételeiben – a meglévő szabályok elégségesnek bizonyultak az intézkedésekhez, de a végrehajtás messze elmaradt a szükségestől. A BRADSHAW és HOWARD (2017–2021) évről évre publikált Computational Propaganda jelentései számszerűen igazolják a koordinált inautentikus magatartás exponenciális terjedését ebben az időszakban, rávilágítva, hogy a platformok passzivitása közvetlen teret engedett a befolyásolási műveleteknek.

A BENNETT és SEGERBERG (2012) által leírt összekötő cselekvés (connective action) logikája szerint a digitális platformok nem csupán eszközök, hanem a cselekvés szerveződési elve: az egyéni megosztás és a személyes azonosulás váltja fel a hagyományos szervezeti mobilizációt. Ez a mechanizmus 2014-ben az orosz műveletek számára kedvezett, mivel a kontrollálatlan horizontális terjesztés felerősítette a dezinformációs tartalmakat. 2025-re azonban ugyanez a logika a védelmi oldal előnyévé vált: az ukrán állampolgári hálózatok, a NAFO-mémhadjáratok és az OSINT-közösségek organikus terjedése éppúgy a connective action mintázatát követi, mint ahogy a támadó műveleteket is ez a dinamika hajtotta egy évtizeddel korábban.

[410] PILDEGOVIČS, Tomass — VANSANT, Kristina — HANLEY, Monika (szerk.) (2021): Russia's Activities in Africa's Information Environment. NATO Strategic Communications Centre of Excellence, Riga, ISBN 978-9934-564-96-3. 5–6., 9., 20–27. o.

2025-re ez a tér radikálisan fragmentálódott. A Telegram vált a kognitív hadviselés elsődleges, szabályozatlan csataterévé – ahogy a VMB (2024) 17 koordinált csoportjának 53%-a is ezen a platformon aktív –, miközben a nyugati platformok a DSA és egyéb szabályozások hatására már aktív elhárítókként lépnek fel. Ez a fragmentáció a többrétegű védelmi stratégia kényszerű válasza a technológiai eszkalációra.

Összegezve: a Helyzet (Input) dimenziójában a 2014-es állapothoz képest mennyiségi robbanást látunk, amely azonban a narratívák minőségi felhígulásával járt együtt. Az iparosítás eredményezte információs környezetszennyezés tudatosan törekszik a kognitív fáradtság előidézésére – és ez az ellentmondás készíti elő a terepet a következő alfejezethez, ahol azt vizsgálom, miként reagált az emberi és szervezeti pszichológia erre a megnövekedett zajszintre.

7.3. Előrejelzés (Folyamat) – Meglepetés szemben a figyelmeztetéssel: A döntési ciklusok és a pszichológiai reziliencia ütköztetése

A H–E–I mátrix második oszlopa, az Előrejelzés (Folyamat) dimenziója a kognitív hadviselés dinamikáját vizsgálja: azt a folyamatot, amely során az információs bemenetek döntésekké és cselekvésekké transzformálódnak. A kognitív térben elért siker nem a technológiai fölényen, hanem a döntési ciklusok (OODA-hurok) sebességén és a befogadó fél pszichológiai állóképességén múlik. A 2014-es és a 2022–2025-ös időszak összevetése ezen a téren mutatja a leglátványosabb kontrasztot.

Ebben a dimenzióban dől el, hogy a nem konszenzuális befolyásolás képes-e áttörni a társadalmi reziliencia védvonalait, vagy a védekező fél a kognitív immunizáció révén semlegesíti a támadást. A folyamat-alapú összehasonlítás rávilágít, hogy a stratégiai figyelmeztetés hatékonysága közvetlen összefüggésben áll az SCC-protokoll (Sebesség–Tartalom–Irányítás) alkalmazásával.

7.3.1. A döntési ciklusok felgyorsulása: Az OODA-hurok és a Telegram-sokk

Mint ahogy a 4. fejezetben leírtam, 2014-ben az orosz fél dominálta a döntési ciklusokat. Az orosz OODA-hurok (Megfigyelés–Orientáció–Döntés–Cselekvés) jóval gyorsabb volt, mint a nyugati vagy az ukrán válaszreakció. Laity – a NATO egykori StratCom tanácsadója – a Defence Strategic

Communications folyóiratban megjelent visszatekintésében[411] részletesen elemzi, miként aknázta ki a Kreml a nyugati döntéshozók pszichológiáját. Egyes szövetséges nemzetek olyan szintű bizonyítékot követeltek meg az orosz állami részvételre vonatkozóan, amely egyszerre volt irreális és a cselekvés elkerülésének eszköze: ha tagadhatták a Kreml közvetlen érintettségét, nem kellett szembenézniük egy határozott válasz szükségességével. Az orosz tagadás így a kognitív bénultság fenntartásának eszközévé vált, nem pedig a tények elfedésének kísérletévé. Mire a 2014 szeptemberi walesi NATO-csúcson az államfők és kormányfők deklarálták a hibrid fenyegetések elleni fellépés szükségességét, az annexió már befejezett tény volt.

Nissen a hibrid hadviselés természetrajzát elemezve[412] rámutat, hogy az orosz műveletek célja a kétely és bizalmatlanság szisztematikus generálása a nyugati média és politikai elit iránt, a döntéshozatali folyamatok lassítása a médiában és a diplomáciában, valamint a szövetségesi kohézió bomlasztása. Ez a célrendszer nem a harcmezőn, hanem az információs környezetben fejtette ki hatását – jóval a nyílt ellenségeskedés felismerése előtt.

Ezzel szemben 2022 után a helyzet megfordult. A stratégiai figyelmeztetés sikere révén[413] a meglepetés ereje elveszett. Az információs térben megjelent a horizontális hálózatok fölénye: az ukrán állampolgári jelentések (például a Diia applikáción keresztül), a NAFO-mémhadjáratok és az OSINT-közösségek valós időben ellensúlyozták az orosz narratívákat. A reflexív kontroll mechanizmusai – amelyek a logikai premisszák manipulálásán keresztül igyekeztek kívánt döntésekre kényszeríteni az ellenfelet – ebben az új környezetben hatékonyságukat vesztették, mert a döntéshozók a decentralizált ellenőrzési hálózatok révén képesek voltak a manipulált premisszákat gyorsan azonosítani és közösíteni. Adamsky az IFRI számára készített tanulmányában[414] rámutatott, hogy az orosz stratégiai gondolkodás a nukleáris, konvencionális és

---

411 Laity, Mark (2021): The Birth and Coming of Age of NATO StratCom: A Personal History. *Defence Strategic Communications,* Vol. 10 (Spring–Autumn), 21–76. o. Online: https://doi.org/10.30966/2018.RIGA.10.1

412 Nissen, Thomas Elkjer (2015): *#TheWeaponizationOfSocialMedia: Characteristics of Contemporary Conflicts.* Koppenhága: Royal Danish Defence College.

413 Csiki Varga Tamás – Tálas Péter (2022): *Megerősített elrettentés és védelem.* SVKI Elemzések, 2022/8.

414 Adamsky, Dmitry (2015): *Cross-Domain Coercion: The Current Russian Art of Strategy.* (Proliferation Papers, No. 54.) Párizs: IFRI, 2015. november. Online: https://www.ifri.org/sites/default/files/migrated_files/documents/atoms/files/pp54adamsky.pdf

információs (kiber)eszközöket egyetlen integrált kényszerítési mechanizmusba kapcsolta össze. Ez a kereszttartományi kényszerítés az ellenfél percepcióját manipulálja és döntéshozatali folyamatát manőverezi, miközben a kinetikus erőalkalmazást minimalizálja. A reflexív kontroll tehát nem önálló információs trükk, hanem a stratégiai kényszerítés teljes spektrumának része – ami magyarázza, miért volt 2014-ben eredményes (ahol az integráció meglepetést okozott), és miért vesztett hatékonyságot 2022-re (ahol a védekező fél felkészült a többdimenziós fenyegetésre). A Resperger által[415] a magyar szakirodalomban tárgyalt hibrid hadviselési doktrína szempontjából ez azt jelenti, hogy a klasszikus nem-lineáris hadviselés eszköztára csak a felkészületlen ellenfél ellen hatékony.

A 2024–2025-ös időszakban tapasztalt Telegram-sokk tovább árnyalja a képet. A korábban szabályozatlan, az orosz műveleteknek otthont adó platform a Durov-ügy és a technológiai zavarok hatására bizonytalansági tényezővé vált maguknak az orosz operátoroknak is. A platform szuverenitás körüli bizonytalanság rávilágított: a digitális kritikus infrastruktúra feletti kontroll elvesztése közvetlen műveleti hátrányt okoz. A gyors ukrán és nyugati adaptáció – különösen a pre-bunking stratégiája – már nem követte, hanem megelőzte az orosz lépéseket.

7.3.2. Pszichológiai hatás: Bénultságtól a kognitív fáradtságig

A pszichológiai hatásmechanizmusok terén a H1 és H2 hipotézisek mentén haladva megállapítható, hogy 2014-ben a cél a totális sokk és a cselekvőképesség felszámolása volt. A krími lakosság és az ukrán katonai vezetés egyaránt a valóságérzékelés elvesztésével küzdött, ami elvezetett az ellenállás nélküli feladáshoz. A Hoyle és munkatársai által kidolgozott pszichológiai hatás-alapú megközelítés[416] (effects-based approach) szerint az információs befolyásolás hatásmechanizmusát nem a tartalom, hanem a befogadó reakciója határozza meg. Kutatásuk rámutat, hogy a stratégiai narratívák nem csupán véleményt formálnak, hanem érzelmi és kognitív reakciókat váltanak ki, amelyek a döntéshozatalt közvetlenül befolyásolják. A Hoyle és munkatársai RT-elemzése a

[415] Resperger István (2018): *A válságkezelés és a hibrid hadviselés.* Budapest: Dialóg Campus Kiadó. ISBN 978-615-5877-53-7.

[416] Hoyle, Aiden – van den Berg, Helma – Doosje, Bertjan – Kitzen, Martijn (2021): Grey Matters: Advancing a Psychological Effects-Based Approach to Countering Malign Information Influence. *New Perspectives,* Vol. 29, No. 2, 144–164. o. Online: https://doi.org/10.1177/2336825X21995702

holland[417] és lett[418] közönség reakcióit vizsgálva kimutatta, hogy a destruktív narratívák – a társadalom „bukásáról" és „széteséséről" szóló üzenetek – erősebb kognitív és érzelmi reakciókat váltottak ki, mint a nyíltan hamis állítások.

A skandináv reziliencia-modell fejlődése jól dokumentált. Svédország esetében az ébresztőt a 2014-es krími annexió és az azt követő év hamis Hultqvist-védelmi miniszteri levél jelentette: ezek nyomán a svéd kormány a pszichológiai védelmi kapacitást szisztematikusan újjáépítette, a Polgári Készenléti Ügynökségen (MSB) keresztül társadalmi szintű rezilienciaépítési programot indított, amelynek középpontjába a megelőző beavatkozást, a médiatudatosság fejlesztését és az önkormányzati szintű felkészítést helyezte.[419] A Kalenský–Hanhijárvi által dokumentált[420] Euro-atlanti dezinformáció-ellenes kapacitásfelmérés megerősíti, hogy a skandináv országok – köztük Svédország és Finnország – az EU-tagállamok körében a legjobban kiépített monitoring-, médiaoktatási és civil társadalmi együttműködési rendszerekkel rendelkeznek; a kormányzati és nem kormányzati szereplők koordinált hálózata a régióban máig a legjobb gyakorlatnak számít.

Azonban itt jelentkezik a kognitív fáradtság jelensége. Míg 2022-ben a közösségi mobilizáció csúcson volt, 2025-re az állandó információs nyomás és a hazug osztalék maximalizálása miatt megjelent a közöny és a nihilizmus. A befogadó fél már nem ijed meg, de hajlamos visszahúzódni a privát szférába, ami a hosszú távú stratégiai rezilienciát gyengítheti. Ez a kognitív nihilizmus állapota, ahol az információs környezetszennyezés mértéke eléri azt a szintet, amelynél a racionális szűrők megkerülése már nem meggyőzéssel, hanem a befogadó érzelmi kimerítésével történik.

---

[417] Hoyle et al. (2023): Cognitive and Emotional Responses to Russian State-Sponsored Media Narratives in International Audiences. *Journal of Media Psychology,* Advance online publication. Online: https://doi.org/10.1027/1864-1105/a000371

[418] Hoyle et al. (2023): Life through Grey-Tinted Glasses: How Do Audiences in Latvia Psychologically Respond to Sputnik Latvia's Destruction Narratives of a Failed Latvia? *Post-Soviet Affairs,* Vol. 40, No. 1, 1–18. o. Online: https://doi.org/10.1080/1060586X.2023.2275507

[419] Jeangène Vilmer, Jean-Baptiste (2021): *Effective State Practices Against Disinformation: Four Country Case Studies.* Helsinki: European Centre of Excellence for Countering Hybrid Threats. (Hybrid CoE Research Report 2.) 10–15. o. Online: https://www.hybridcoe.fi/wp-content/uploads/2021/07/20210709_Hybrid_CoE_Research_Report_2_Effective_state_practices_against_disinformation_WEB.pdf

[420] Kalenský, Jakub – Hanhijärvi, Heidi (2025): *Countering Disinformation in the Euro-Atlantic: Strengths and Gaps.* Helsinki: European Centre of Excellence for Countering Hybrid Threats. (Hybrid CoE Research Report 15.) 17., 20., 31. o. Online: https://www.hybridcoe.fi/publications/hybrid-coe-research-report-15

A NATO kognitív hadviselésről szóló szakirodalmában[421] megfogalmazott felőrlő hatás éppen ezt a dinamikát emeli ki: a modern kognitív agresszió nem egyetlen döntés befolyásolására, hanem a döntéshozatali képesség rendszerszintű erodálására irányul. Ebben a szakaszban a kritikus infrastruktúra iránti bizalom fenntartása válik a legnehezebb feladattá, mivel az állandó zajban az emberi tűzfal stabilitása erodálódik.

A disszertáció Előrejelzés-dimenziójának elméleti megalapozásához Spiliopoulos (2025) kísérleti közgazdasági és pszichológiai szintézise nyújt további támaszt. [422] Spiliopoulos a robust elrettentés és az aktor-racionalitás kapcsolatát vizsgálja, és kimutatja, hogy a klasszikus racionális döntéshozó modell számos feltevezése empirikusan nem tartható. Hertwig és munkatársai eredményeire[423] támaszkodva rámutat, hogy az emberek a tapasztalatból származó döntések során szisztematikusan alulbecsülik a ritka események valószínűségét. Gigerenzer és Gaissmaier (2011) heurisztikus döntéshozatáli kutatásaira[424] építve Spiliopoulos azt a következtetést vonja le, hogy ha a célközönség nem a klasszikus racionalitás modellje szerint viselkedik, akkor a „racionális elrettentés" feltételezése megkérdőjelezhető. Ez az elméleti szintézis közvetlen implikációval bír a disszertáció OxIPO-modellje számára: az OxIPO éppen azért szükséges a kognitív hadviselés dinamikájának leírásához, mert a feldolgozási torzítások szisztematikusak és kihasználhatóak – amit a kísérleti pszichológia immár robusztus eredményekkel igazol.

7.3.3. A hitelesség mint szűkösségi erőforrás

Az összehasonlítás rávilágít, hogy míg 2014-ben az orosz propaganda még törekedett egyfajta alternatív hitelesség látszatára – ál-szakértők, kreált bizonyítékok, a Regnum és a TV Zvezda koordinált narratívái –, addig 2025-re a stratégia a hitelesség-eltérítésre váltott. Ahogy a 6.

---

[421] CLAVERIE, Bernard – DU CLUZEL, François (2022): The Cognitive Warfare Concept. In: CLAVERIE, Bernard et al. (szerk.): Cognitive Warfare: The Future of Cognitive Dominance. NATO Collaboration Support Office, 2022. 1–8. o.

[422] SPILIOPOULOS, Leonidas (2025): Robust Deterrence and Actor Rationality. NATO Strategic Communications Centre of Excellence, Riga, ISBN 978-9934-619-64-9.

[423] Hertwig et al. (2004): Decisions from Experience and the Effect of Rare Events in Risky Choice. *Psychological Science,* Vol. 15, No. 8, 534–539. o. Online: https://doi.org/10.1111/j.0956-7976.2004.00715.x

[424] Gigerenzer, Gerd – Gaissmaier, Wolfgang (2011): Heuristic Decision Making. *Annual Review of Psychology,* Vol. 62, 451–482. o. Online: https://doi.org/10.1146/annurev-psych-120709-145346

fejezetben az MI-eszközök hatásánál bemutattam, a cél ma már nem az, hogy elhiggyék az orosz verziót, hanem az, hogy senkinek se higgyenek el semmit.

A Monaghan[425] által elemzett hibrid hadviselés-elhárítási keretrendszer szempontjából ez a hitelesség-erózió az egyik legnehezebben kezelhető jelenség, mert nem egy konkrét narratíva, hanem a narratívák létjogosultságának általános tagadása ellen kell védekezni. Ez a folyamat a döntéshozatalt lassítja le, mivel minden adatot – még a hiteles forrásból származót is – többszörösen ellenőrizni kell. A Kalenský és Hanhijärvi[426] által vezetett dezinformáció-monitorozási projektek rámutatnak, hogy a hitelesség-erózió elleni leghatékonyabb védekezés nem az egyes hamis tartalmak cáfolása, hanem a társadalom kritikus gondolkodási képességének rendszerszintű fejlesztése – az az inoculation-logika, amelyet a 7.4.3. alfejezetben részletezek.

Az Előrejelzés dimenzió zárása: a 2014-es orosz kezdeményezőkészséget 2022 után a védekező fél rezilienciája és hálózati fölénye ellensúlyozta. A sikeres kognitív immunizáció 2022-ben képes volt megtörni a reflexív kontroll mechanizmusait. Ugyanakkor 2025-re a kognitív hadviselés súlypontja a meglepetéstől a felőrlés irányába tolódott el, ahol már nem a gyorsaság, hanem az információs zaj elviselésének képessége a döntő faktor. Ez a rendszerszintű nyomás kényszerítette ki a védekezési mechanizmusok intézményesülését.

7.4. Irányítás (Kontroll) – A védekezés ára: Szabályozási vákuumtól az aktív elhárításig

A H–E–I mátrix harmadik pillére, az Irányítás (Kontroll) dimenziója a kognitív hadviselés elleni védekezés intézményi, jogi és technológiai kereteit vizsgálja. A kognitív térben az irányítás nem a totális kontrollt, hanem a káros befolyásolási kísérletek azonosításának, lassításának és semlegesítésének képességét jelenti. A 2014-es és a 2022–2025 közötti időszak összevetése ezen a területen mutatja a legmélyebb strukturális fejlődést: a reaktív válságkezeléstől az aktív reziliencia-építésig tartó ívet.

---

[425] Monaghan, Sean (2022): *Deterring Hybrid Threats: Towards a Fifth Wave of Deterrence Theory and Practice*. Helsinki: European Centre of Excellence for Countering Hybrid Threats. (Hybrid CoE Paper 12.) 34. o. – A hitelesség-erózióra való alkalmazás a szerző következtetése Monaghan keretrendszeréből.

[426] Kalenský, Jakub – Hanhijärvi, Heidi (2025): *Countering Disinformation in the Euro-Atlantic: Strengths and Gaps*. Helsinki: European Centre of Excellence for Countering Hybrid Threats. (Hybrid CoE Research Report 15.) 14–16., 32. o.

7.4.1. A szabályozási környezet: A Laissez-faire korszaktól a DSA-ig

Mint ahogy a 4. fejezetben, a Krím-félsziget orosz annexiója kapcsán bemutattam, 2014-ben a nemzetközi közösség és a nagy technológiai platformok szabályozási vákuumban mozogtak. Az állami hátterű dezinformációs kampányokat a szólásszabadság keretein belül kezelték, és hiányoztak azok a jogi protokollok, amelyek lehetővé tették volna a kognitív agresszió gyors megfékezését.[427] A NATO StratCom COE (2018) elemzése[428] szerint ebben az időszakban a platformok stratégiáját elsősorban a hírfolyam dominálta: az egyes beavatkozások szorosan követték a médiaciklusokat, ami azt jelzi, hogy a moderációs válaszok nem proaktív, hanem politikai nyomás által vezérelt döntések voltak. A demokratikus államok válaszreakcióinak első rendszeres tipológiáját Hellman és Wagnsson adta az European Security folyóiratban.[429] A szerzőpáros négy ideáltípusú stratégiát különböztetett meg: a blokkolást (az ellenséges tartalom fizikai vagy jogi kizárását), a konfrontációt (aktív ellennarratívák létrehozását), a naturalizálást (a saját értékek pozitív példamutatáson keresztüli terjesztését) és az ignorálást (a tudatos figyelmen kívül hagyást). Az Oroszországgal szomszédos európai államok empirikus példáin – Észtország orosz nyelvű közszolgálati csatornájának indításától a balti államok RT-retranszmissziós tilalmáig – illusztrálták, hogy a válaszstratégiák az elköteleződés–kikapcsolódás kontinuumon helyezkednek el. Ez a keretrendszer a DSA előtti korszak legátfogóbb analitikus eszköze, amely a jelen fejezet Irányítás-dimenziójának fejlődési ívét a szabályozási vákuumtól az intézményesített válaszig közvetíti.

---

[427] NATO STRATCOM COE (2024): *Social Media Manipulation for Sale: 2024 Experiment on Platform Capabilities to Detect and Counter Inauthentic Social Media Engagement*. NATO Strategic Communications Centre of Excellence, Riga, ISBN 978-9934-619-07-6. 7., 13. o. A kísérletben hat platformon €58 költséggel 1 150 hamis kommentet, 11 725 kedvelést, 3 150 megosztást és 8 233 megtekintést vásároltak; egyetlen platform sem volt képes a hamis kedvelések felismerésére.

[428] Bradshaw, Samantha – Neudert, Lisa-Maria – Nothaft, Hannes (2018): *Government Responses to Malicious Use of Social Media.* Riga: NATO Strategic Communications Centre of Excellence. Online: https://stratcomcoe.org/publications/government-responses-to-malicious-use-of-social-media/125

[429] Hellman, Maria – Wagnsson, Charlotte (2017): How can European States Respond to Russian Information Warfare? An Analytical Framework. *European Security,* Vol. 26, No. 2, 153–170. o. Online: https://doi.org/10.1080/09662839.2017.1294162

A NATO StratCom COE Impact of the Digital Services Act (2025) című elemzése[430] dokumentálja az egy évtized alatt végbement fordulópontot. A DSA rendszerszintű kockázatértékelést és auditálást ír elő a nagyon nagy platformok (Very Large Online Platforms – VLOPs) számára, és kötelezővé teszi a koordinált manipuláció elleni fellépést. A német NetzDG (2017) – amely a legnagyobb platformokra terjedt ki – korai precedensként szolgált, amennyiben jogi felelősséget telepített a platformokra a jogellenes tartalmak kezelésében. A skandináv-balti régió tapasztalatai[431] rámutatnak, hogy a szabályozás önmagában nem elégséges: a hatékony elhárítás a jogi keretek, a szervezeti képességek és a társadalmi reziliencia szinkronizálásán múlik. A NB8-országok esetében a reziliencia-építés mindenhol prioritás, de az alkalmazott eszközök – a svéd MSB módszertanától a finn társadalmi szintű ellenállóképesség-tréningekig – jelentősen eltérnek.

Ezzel szemben 2022-re a helyzet alapvetően megváltozott. Ahogy azt az 1. fejezetben a H3 hipotézis felvezetésekor rögzítettem, az Európai Unió és a nyugati szövetségi rendszer ekkor már tudatosabb szabályozási környezettel rendelkezett. Mint ahogy a Hoyle és Pijpers kutatására hivatkozva[432] korábban kifejtettem, az orosz állami média (RT, Sputnik) azonnali kitiltása az EU-ból – 2022 márciusában, alig napokkal az invázió után – olyan határozott irányítási lépés volt, amely 2014-ben még elképzelhetetlennek tűnt. A platformkormányzási trendek szerint ez a szankciós válasz paradigmaváltást jelzett: a platformok többé nem semleges infrastruktúrák, hanem az információs biztonság aktív szereplői.

Ugyanakkor a forráskritikai elemzés során rögzíteni kell, hogy a manipuláció technikái aktorfüggetlenek. A befolyásolás eszköztára – a stratégiai keretezéstől a mém-hadviselésen át az érzelmi mobilizációig – a hadviselés egyetemes része, amelyet a védekező oldal is alkalmaz saját kognitív integritásának fenntartása érdekében. A szabályozás célja nem az „objektív igazság”

---

[430] Haiduchyk et al. (2025): *Impact of the Digital Services Act: A Facebook Case Study*. Riga: NATO Strategic Communications Centre of Excellence. ISBN 978-9934-619-35-9. Online: https://stratcomcoe.org/publications/impact-of-the-digital-services-act-a-facebook-case-study/319

[431] Lange-Ionatamišvili et al. (2026): *Countering Information Influence Operations in the Nordic-Baltic Region.* Riga: NATO Strategic Communications Centre of Excellence. Online: https://stratcomcoe.org/publications/countering-information-influence-operations-in-the-nordic-baltic-region/327

[432] Hoyle, Aiden – Pijpers, Peter B. M. J. (2022): Stemming the Narrative Flow: The Legal and Psychological Grounding for the European Union's Ban on Russian State-Sponsored Media. *Defence Strategic Communications,* Vol. 11, 51–80. o. Online: https://doi.org/10.30966/2018.RIGA.11.2

kikényszerítése, hanem a nem konszenzuális befolyásolás technikai csatornáinak és az algoritmikus manipuláció sebességének korlátozása .

7.4.2. A COVID-19 mint reziliencia-katalizátor

A disszertáció egyik központi állítása – amelyet az 5. fejezetben, a Híd-időszak elemzésekor részleteztem – az, hogy a 2022-es sikeres védekezés alapjait a globális pandémia alatti tapasztalatok tették le. A COVID-19 infodémia elleni küzdelem során a társadalmak és az intézmények kénytelenek voltak kifejleszteni azokat a kognitív immunválaszokat, amelyek 2022 februárjában élesben is működtek. A pandémia alatt kialakult platformszintű moderációs rutinok és a kormányzati stratégiai kommunikáció (StratCom) egységek professzionalizálódása nélkül az orosz narratívák 2022-ben ismét képesek lettek volna a 2014-eshez hasonló bénultságot okozni.

A COVID-időszak azért tekinthető reziliencia-katalizátornak, mert a pandémia egyszerre növelte a társadalom információigényét és a manipulációs felületet. A figyelemgazdaságban a vírushoz kapcsolódó hírérték rövid idő alatt extrém módon felértékelődött. A hazai adatok alapján a magyar online hírfogyasztás a járvány korai szakaszában ugrásszerűen emelkedett, és a médiafogyasztás növekedése együtt járt azzal, hogy a közönség fokozottan ki volt téve félrevezető vagy hamis információknak. A Defence Strategic Communications folyóiratban megjelent kutatás[433] rámutat, hogy a COVID-dezinformáció elleni küzdelem során a társadalmak megtanulták a „prebunking” alapjait: a megelőző figyelmeztetés, a transzparens kormányzati kommunikáció és a közösségi média moderációs protokollok fejlesztése olyan képességek, amelyek közvetlenül transzferálhatóak voltak a 2022-es geopolitikai kontextusba. Pamment[434] a COVID-tapasztalatot expliciten integrálja a dezinformáció-elhárítási képességek taxonómiájába, kiemelve a WHO infodémia-válaszának mintajellegét.

---

[433] Colley, Thomas – Granelli, Francesca – Althuis, Jente (2020): Disinformation's Societal Impact: Britain, Covid, and Beyond. *Defence Strategic Communications,* Vol. 8, 89–140. o. Online: https://doi.org/10.30966/2018.RIGA.8.3

[434] Pamment, James (2022): *A Capability Definition and Assessment Framework for Countering Disinformation, Information Influence, and Foreign Interference.* Riga: NATO Strategic Communications Centre of Excellence. ISBN 978-9934-619-13-7. Online: https://stratcomcoe.org/publications/a-capability-definition-and-assessment-framework-for-countering-disinformation-information-influence-and-foreign-interference/255

E tapasztalat több védelmi következtetéshez vezetett: a társadalmi szintű kognitív terhelés kezelése, a platformszintű reakcióidő csökkentése és az egyéni szűrési rutinok fejlesztése a későbbi (2022–2025) műveleti környezetben már nem opcionális, hanem strukturális feltétel.

7.4.3. Aktív elhárítás és a technológiai aszimmetria

Az irányítás dimenziójában 2025-re újabb szintlépés következett be: az aktív elhárítás intézményesülése. Míg 2014-ben a védekezés kimerült az utólagos cáfolatokban (debunking), addig 2024–2025-ben már a megelőző figyelmeztetés (pre-bunking) és a technológiai elhárítás vált dominánssá.

A NATO StratCom COE The Role of Communicators című kiadványa[435] rendszerezi azt a háromfázisú modellt, amely a védekezés fejlődési ívét írja le: Felkészülés (Preparation) – azaz a társadalmi és szervezeti preparáltság, a médiaműveltség fejlesztése és a kockázatelemzés; Cselekvés (Action) – az azonnali kommunikációs eszközök bevetése az információs befolyásolás ellen; és Tanulás (Learning) – a tapasztalatok visszacsatolása a védekezési rendszerbe. Ez a modell a 2014-es ad-hoc cáfolásoktól a 2025-ös strukturált elhárításig tartó fejlődési ívet írja le.

A NATO StratCom COE Defining Capabilities (2022) és Capability Assessment for StratCom kiadványai[436] [437] együttesen több mint 90 információs befolyásoló művelet-elhárítási képességet definiálnak és értékelnek. A svéd MSB által az Egyesült Királyság Kormányzati Kommunikációs Szolgálata számára kidolgozott RESIST 2 módszertan[438] azóta a NATO-szövetségesek

---

435 Pamment et al. (2019): *The Role of Communicators in Countering the Malicious Use of Social Media.* Riga: NATO Strategic Communications Centre of Excellence. Online: https://stratcomcoe.org/publications/the-role-of-communicators-in-countering-the-malicious-use-of-social-media/101

436 Pamment, James (2022): *A Capability Definition and Assessment Framework for Countering Disinformation, Information Influence, and Foreign Interference.* Riga: NATO Strategic Communications Centre of Excellence. ISBN 978-9934-619-13-7. Online: https://stratcomcoe.org/publications/a-capability-definition-and-assessment-framework-for-countering-disinformation-information-influence-and-foreign-interference/255

437 Lindbom, Hanna (2022): *Capability Assessment for StratCom: Using the New Risk Perspective to Inform the Development of Effective Response Capability Assessments for Countering Information Influence Operations.* Riga: NATO Strategic Communications Centre of Excellence. Online: https://stratcomcoe.org/publications/capability-assessment-for-stratcom-using-the-new-risk-perspective-to-inform-the-development-of-effective-response-capability-assessments-for-countering-information-influence-operations/240

438 Pamment, James – Nothhaft, Howard – Fjällhed, Alicia (2018): *Countering Information Influence Activities: A Handbook for Communicators.* Stockholm: Myndigheten för samhällsskydd och beredskap (MSB). ISBN 978-91-7383-864-1. Online: https://www.msb.se/RibData/Filer/pdf/28698.pdf

többségének gyakorlatába is beépült. A RESIST betűszó hat egymásra épülő lépést kódol: Recognise (felismerés), Early Warning (korai figyelmeztetés), Situational Insight (helyzettudatosság), Impact Analysis (hatáselemzés), Strategic Communications (stratégiai kommunikáció) és Tracking Effectiveness (hatékonyságmérés). A módszertan a COVID-19 pandémia tapasztalatait integrálva bővítette az eredeti 2019-es változatot, és több mint 20 partnerországban képeztek ki kormányzati kommunikátorokat a segítségével. Jelentősége abban áll, hogy először adott szisztematikus, bizonyítékalapú eljárásrendet az állami kommunikátorok számára a dezinformáció felismerésére és kezelésére, miközben a szólásszabadság demokratikus értékeit tiszteletben tartja. A NATO StratCom COE Enhancing Organisational Capability (2023) című tanulmánya szcenárió-alapú tesztelés keretében vizsgálja, hogyan reagálnak a szervezetek a kibertámadás, dezinformáció és infrastruktúra-zavar egyidejű bekövetkezésére – ez a hibrid fenyegetés-szimuláció közvetlenül releváns az emberi tűzfal ellenálló képességének mérésére.

A megelőző figyelmeztetés elméleti alapját a Lewandowsky és társai[439] által a Psychological Science in the Public Interest folyóiratban publikált áttekintő tanulmány fektette le. A kutatócsoport szisztematikusan dokumentálta, hogy a félretájékoztatás kognitív hatása még a cáfolat elfogadása után is fennmarad – ezt a jelenséget a folytatólagos befolyás hatásának (continued influence effect) nevezték el. A tanulmány kulcsmegállapítása, hogy a helyesbítés önmagában nem elegendő: a hamis információ által keltett mentális modellt csak egy koherens alternatív magyarázattal lehet felülírni. Ez a felismerés közvetlenül megalapozta a pre-bunking stratégiáját, amely nem az utólagos cáfolatra, hanem a megelőző immunizálásra épít. A megelőző figyelmeztetés módszertanának egyik úttörője a Google Jigsaw projektje. Ez a kognitív pszichológia beoltás-elméletére (inoculation theory) építve – a Lewandowsky és munkatársai által azonosított kognív szívósság mechanizmusait kiaknázva – növeli a felhasználók ellenállóképességét, rövid, edukatív tartalmakkal téve felismerhetővé a dezinformációs technikákat még az expozíció előtt.

Az EEAS (2024) második FIMI-jelentése (2nd Report on Foreign Information Manipulation and Interference Threats) és a Kubica 2024-es információs műveleti elemzése megerősíti, hogy a

[439] Lewandowsky et al. (2012): Misinformation and Its Correction: Continued Influence and Successful Debiasing. *Psychological Science in the Public Interest,* Vol. 13, No. 3, 106–131. o. Online: https://doi.org/10.1177/1529100612451018

koordinált védekezés legfontosabb eleme az interoperabilitás: a különböző nemzeti és szövetségi szintű rendszerek – a DISARM-taxonómiától a RESIST-módszertanon át a nemzeti hírszerzési produktumokig – közös nyelvet és adatcsere-protokollt igényelnek. A NATO StratCom COE Robotrolling (2024) jelentése a koordinált inautentikus magatartás automatizált detektálásának módszertanát fejleszti, amely az SCC-protokoll technológiai gerincét adja.

A valós idejű StratCom-döntéshozatalt – az SCC-protokoll Sebesség-tengelyén a 90 perces válaszablakot – a közösségimédia-figyelő eszközök tájékoztatják. A NATO StratCom COE 2022-es, nyolc kereskedelmi eszközre kiterjedő értékelése (Grizane et al.) szerint a prémium-kategóriás platformok (Brandwatch, Meltwater, Sprinklr, Digimind) képesek képtartalmat elemezni, historikus adatokat visszakeresni és valós idejű vizualizációt biztosítani, ám az AI-modellek a kisebb, kevésbé adatgazdag nyelvekben – így a magyarban is – szignifikánsan gyengébben teljesítenek.[440] Ez nem csupán technikai korlát, hanem geopolitikai aszimmetria: a nagyobb nyelvközösségek (angol, orosz, arab) számára elérhető automatizált detekció a kisebb NATO-tagállamoknak ugyanolyan szinten nem áll rendelkezésre. A Sebesség-tengely tehát nem kizárólag szervezeti akarat és eljárásrend kérdése, hanem technológiai és nyelvpolitikai erőforrás-kérdés is – ami különösen releváns a disszertáció magyarországi alkalmazási kontextusában.

Összegezve: az Irányítás szempontjából a 2014-es tehetetlenséget 2025-re intézményesített, jogilag és technológiailag is alátámasztott védekezési ökoszisztéma váltotta fel. Ez a fejlődés igazolja a H3 hipotézist, miszerint a védekezési képességek ugrásszerű fejlődése döntő szerepet játszott abban, hogy a 2022-es orosz kognitív offenzíva nem érte el a 2014-es stratégiai sikereket. Ugyanakkor a kognitív nihilizmus elleni küzdelem továbbra is folyamatos kontrollt igényel, mivel a technológia fejlődése állandóan próbára teszi a jogi és technikai védelem határait.

Az információs befolyásoló művelet-ellenálló képességek szisztematikus értékelésére a NATO StratCom COE Pamment (2022) által kidolgozott keretrendszere az első egységes fogalmi alap, amelyet azóta a szövetségi gyakorlatban is alkalmaznak.[441] A modell négy funkcionális területet

[440] GRIZĀNE, Anna – ISUPOVA, Marija – VORTEIL, Vanessa (2022): Social Media Monitoring Tools: An In-Depth Look. NATO Strategic Communications Centre of Excellence, Riga. 12–14. o.

[441] PAMMENT, James (2022): A Capability Definition and Assessment Framework for Countering Disinformation, Information Influence and Foreign Interference. NATO Strategic Communications Centre of Excellence, Riga. 8–14. o.

különít el: (1) detekció és monitoring, (2) attribúció, (3) ellennarratív kommunikáció, (4) szabályozási és jogi eszközök. A disszertáció által javasolt SCC-protokoll (Sebesség–Tartalom–Irányítás) a Pamment-keretrendszer (3) és (4) dimenzióiba illeszkedik: a Tartalom-tengely az ellennarratív kommunikáció minőségi paramétereinek, az Irányítás-tengely pedig a szabályozási csatorna-döntéseknek felel meg. Pamment emellett felhívja a figyelmet az archetipikus szervezeti aszimmetriára: a legtöbb szervezet reaktív üzemmódban van, miközben a proaktív képesség fejlesztéséhez strukturált beruházásra – képzésre, értékelési ciklusra, intézményi koordinációra – van szükség, amelyet az SCC-protokoll bevezetésének előfeltételeként is értelmezni kell.

7.5. Konklúzió: A FMK Kognitív Olló modellje és a hipotézisek ellenőrzése

Az összehasonlító elemzés végére érve láthatóvá válik az a fundamentális elmozdulás, amely a 2014-es és a 2025-ös állapot között végbement. A Strukturált Fókuszált Összehasonlítás célja nem csupán a technológiai fejlődés regisztrálása volt, hanem annak igazolása, hogy a kognitív hadviselés stratégiai hatékonysága nem lineárisan követi az információs technológia fejlődését. Bár a támadó eszközök kronológiai fejlődése töretlen, a műveleti eredményesség a védekezési válaszreakciók miatt megtört.

7.5.1. Az FMK Kognitív Olló jelensége

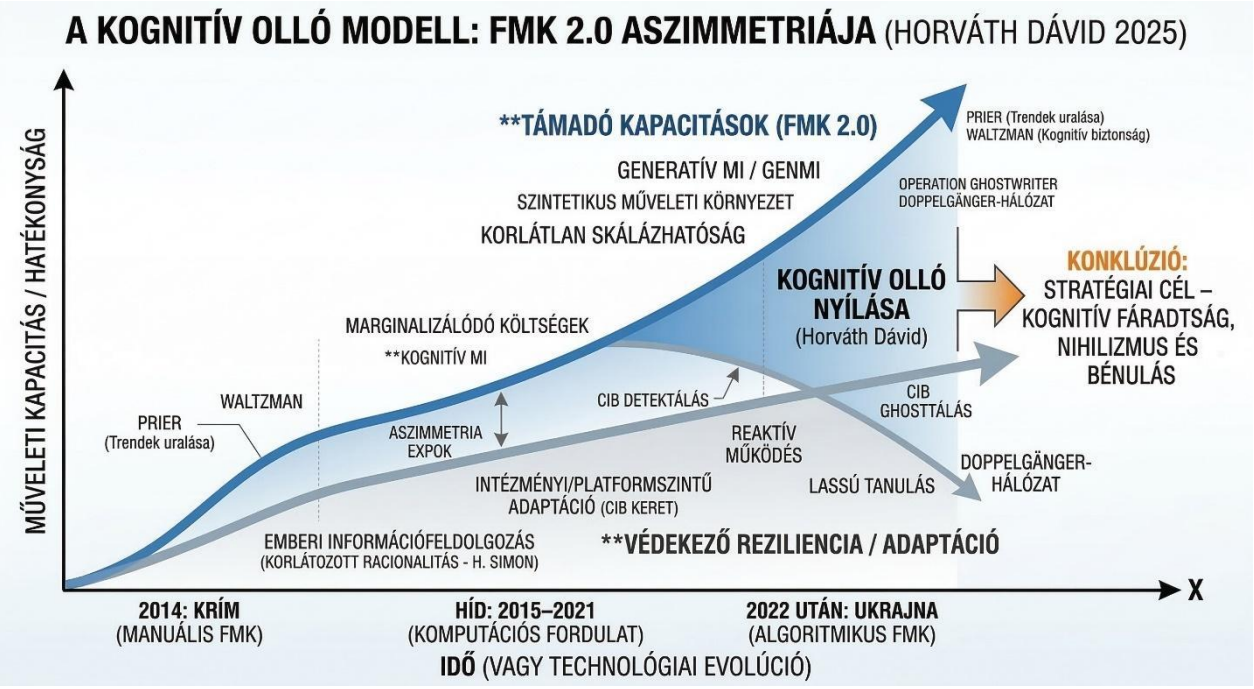
A fejezet eredményeit egy új elméleti konstrukcióban, a Fegyvernek Minősülő Kommunikáció Kognitív Olló-modelljében foglalom össze. A modell fogalmi kiindulópontja Herbert A. Simon korai tézise a korlátozott racionalitásról[442] (bounded rationality): az emberi döntéshozatal nem optimális kalkulációval, hanem a környezethez illeszkedő, egyszerűsítő szabályokkal működik, és gyakran a „kielégítő” megoldásra törekszik (satisficing) (Simon, 1956). Simon megfogalmazása ebben a kontextusban azért módszertanilag releváns, mert a döntési viselkedés nem önmagában az “ész” tulajdonsága, hanem két, egymást metsző feltételrendszer kölcsönhatásából érthető meg. Ezt a kölcsönhatást ragadja meg az olló metaforája, az egyik penge a feladatkörnyezet szerkezete (milyen információ érhető el, milyen a csatorna-architektúra, milyen az időnyomás és a platformlogika), a másik penge pedig a befogadó kognitív kapacitáskorlátja (figyelem, munkamemória, feldolgozási sebesség, ellenőrzési költség). A viselkedés – vagyis a műveleti

[442] Simon, Herbert A. (1990): Invariants of Human Behavior. *Annual Review of Psychology,* 41(1), 1–19.

kimenet – e két “penge” együttállásából adódik. Ugyanaz az üzenet más környezeti elosztási logikában és más kognitív terhelés mellett eltérő kimenetet eredményez.

A disszertációban a FMK Kognitív Olló nem általános pszichológiai kijelentés, hanem hadműveleti értelmű modell: a fegyvernek minősülő kommunikáció (FMK) akkor válik stabilan azonosítható műveleti termékké, amikor a környezeti penge (platform- és terjesztési infrastruktúra: láthatóság, skálázás, visszacsatolás) szisztematikusan a kognitív penge ellen dolgozik (a feldolgozási kapacitás telítése, a forráskritika költségének emelése, a bizonyíték-érzet gyártása). Ezt a kapcsolatot a dolgozat az OxIPO és a HIP integrációjával teszi műveletileg értelmezhetővé: az OxIPO Input–Process–Output lánca és a HIP mechanizmus-szintje együtt írja le, hogy mikor fordul át a környezeti túlterhelés döntési torzítássá, bénulássá vagy polarizációvá. Vagyis a Kognitív Olló-modell nálam egyszerre (i) magyarázó keret (miért nem lineáris a volumen → hatékonyság viszony), és (ii) diagnosztikai híd a H–E–I rács dimenzióihoz: a Helyzet (H) rögzíti a feladatkörnyezet pengéjét, az Előrejelzés (E) a kognitív penge terhelési állapotát és kockázatát, az Irányítás (I) pedig a pengék „távolodásának” fékezésére alkalmas beavatkozásokat.

1. kép: Fegyvernek Minősülő Kommunikáió Kognitív Olló-modell



Forrás: saját szerkesztés

A modell ezután két, egymástól távolodó szárként írja le a 2014–2025 közötti elmozdulást: (1) a technológiai volumen meredek emelkedését (iparosítás, automatizáció, generatív eszközök), és (2) a stratégiai hatékonyság nem-lineáris, részben megtörő pályáját (reziliencia, platformkormányzás, társadalmi tanulás). A következő bekezdések ezt a két szárat bontják ki empirikus horgonyokkal.

A technológiai volumen szára a mesterséges intelligencia – különösen az AutoGenAI és a hiperrealisztikus generatív eszközök – révén meredeken emelkedik. Ez az iparosítás folyamata, amely az információs környezetszennyezés kiterjesztésével közvetlenül növeli a kognitív támadási felületet. A NATO StratCom COE (2022) kétrészes MI-tanulmánya (The Double-Edged Sword of AI + The Role of AI), a VMB (2024) koordinált csoport-elemzése és a Wallner-Copeland-Giustozzi 2025-ös RUSI-tanulmánya[443] együttesen dokumentálják ennek a szárnak a meredekségét.

A stratégiai hatékonyság szára ezzel szemben – a 2014-es csúcspont után – stagnáló vagy süllyedő tendenciát mutat. Ennek oka, hogy a védekező fél rezilienciája, a 7.4. alfejezetben részletezett aktív irányítási mechanizmusok és a társadalmi tanulási görbe (különösen a pandémia tapasztalatai)képesek ellensúlyozni a mennyiségi fölényt. A NB8-országok információs befolyásoló művelet-elhárítási gyakorlatának összehasonlító elemzése (NATO StratCom COE 2025) empirikusan alátámasztja, hogy a reziliencia-építés – a médiaműveltségtől a szervezeti képességfejlesztésen át a jogi keretekig – rendszerszintűen csökkenti a támadó műveletek hatékonyságát.

Az olló nyílása bizonyítja: a modern kognitív hadviselésben a volumen növekedése nem jelent automatikusan jobb eredményt. A 2014-es, manuálisan irányított, de tűpontosan fókuszált orosz narratívák stratégiailag sikeresebbek voltak a védekezési vákuum miatt, mint a 2025-ös, MI-vel iparosított, de a társadalom által már részben felismert és elhárított dezinformációs dömping. A paradoxon: a technológiai aszimmetria okozta előny elvész, ha a védekező oldal képes az SCC-protokoll mentén stabilizálni az információs környezetet és fenntartani az emberi tűzfal integritását.

Az egyéni és szervezeti képességfejlesztés dilemmáját a NATO StratCom COE Pamment és Sörensen (2023) által operacionalizált keretrendszere vizsgálta a svéd Pszichológiai Védelmi

[443] WALLNER, COPELAND & GIUSTOZZI (2025): i. m. (ld. fentebb).

Ügynökség (MPF) képzési struktúráján. A négyelemű értékelési eszközkészlet – célkitűzések, mérőszámok, kockázatértékelés, folyamati érettség – lehetővé teszi, hogy ne csupán a kimenetelt, hanem a szervezeti folyamatok minőségét is mérjük.[444] A tanulmány legfontosabb megállapítása szerint az egyéni és szervezeti tanulás között szignifikáns rés tátonghat: a résztvevők egyéni kompetenciát szerezhetnek, miközben az intézményi struktúrák, koordinációs mechanizmusok és döntési folyamatok változatlanok maradnak. Ez a megállapítás a disszertáció Irányítás-dimenziójának egyik strukturális tanulsága: az információs befolyásoló művelet ellenes szervezeti válasz hatékonysága nem csupán a tudástól, hanem a szervezeti tanulás intézményesítésétől függ. Az SCC-protokoll alkalmazásához ezért a képzési programok mellé formális értékelési ciklus és intézményi tanulási mechanizmus szükséges.

7.5.2. A kutatási hipotézisek értékelése

A keresztmetszeti összehasonlítás adatai – és a Kognitív Olló-modell fenti levezetése – alapján az 1. és 2. hipotézis (H1, H2) igazolást nyert: a 2022-es kognitív védekezés sikeresen törte meg azt a bénítási mechanizmust, amelyet 2014-ben a narratív koherencia és a csatornaszinkron együttesen váltott ki. A 3. hipotézis (H3) kettős értelmezéssel igazolt: a védekező és a támadó oldal egyaránt tanult a 2014–2021-es időszakból. A 4. hipotézis (H4) alátámasztott, de empirikusan a leginkább vitatható: a technológiai volumen és a stratégiai hatékonyság közötti nem-lineáris összefüggés az olló nyílásában válik láthatóvá. Az összehasonlítás mögött álló teljes bizonyítéklánc és a hipotézisek részletes doktori értékelése a 9.2. fejezetben található.

7.5.3. Összefoglalás

A 7. fejezet rávilágított arra, hogy bár a védelmi mechanizmusok jelentős fejlődésen mentek keresztül, a technológiai zajszint emelkedése és az információs környezetszennyezés új típusú sebezhetőségeket hozott létre. A FMK Kognitív Olló modellje nem csupán leíró, hanem prediktív értékkel bír: amennyiben a technológiai volumen szára tovább emelkedik (ami a generatív MI fejlődése alapján biztosra vehető), a védelmi fél kizárólag az irányítási (Control) és a folyamat (Process) dimenziók szinkronizált erősítésével képes fenntartani az egyensúlyt.

---

[444] SÖRENSEN, Sara – PAMMENT, James (2023): Operationalising the Framework for Evaluating Capability against Information Influence Operations: A Case Study of the Psychological Defence Agency's Courses. NATO Strategic Communications Centre of Excellence, Riga. 19–22. o.

A dolgozat következő, 8. fejezete ezen megfontolások mentén mutatja be a kutatás központi gyakorlati kimenetét, a Multimodális Reziliencia Mátrixot (MRM). Ez a keretrendszer az OxIPO és a HIP modellek szintéziseként tesz kísérletet arra, hogy strukturált választ adjon a kognitív hadviselés 2025-ös kihívásaira. A NATO StratCom COE NextGen Information Environment előrejelzése (Bolt 2025) ezt a sürgősséget megerősíti: az agentic MI-rendszerek teljesen automatizálják az információs műveleteket, gépek céloznak gépeket, és a „szennyezett információs ökoszisztéma" (poisoned training data) alááshatja magukat a detekciós rendszereket is.[445] Az MRM központi eleme az emberi tűzfal és az SCC-protokoll integrálása, amely célzottan törekszik a kritikus infrastruktúrák döntési folyamatainak védelmére a jövőbeli hibrid fenyegetésekkel szemben. A FMK Kognitív Olló modelljének G–M–T–V dimenzió szerinti adatalapját a közvetlenül következő 7.6. alfejezet összehasonlító táblázata rögzíti.

7.6. A G–M–T–V műveleti lánc összehasonlító összegzése

A 7.2–7.4. alfejezetek H–E–I dimenzió szerinti elemzését kiegészítve, az alábbi összefoglalás a 6. fejezetben bemutatott G–M–T–V műveleti lánc (Generálás–Mosás–Terítés–Validálás) mentén rögzíti a két korszak közötti strukturális eltolódásokat. Az FMK-rács kategóriáit alkalmazva:

Generálás (G): 2014-ben a tartalomelőállítás humán operátorokra épült (IRA, kb. 400–1000 fő), a forrás dominánsan szürke, a mód narratív keret-injektálás. 2025-re a generálás AutoGenAI-alapúvá vált, a forrás fekete tartományba tolódott (Doppelgänger-típusú műveletek), a mód algoritmikus A/B-teszteléssé és szintetikus tartalom-tömegtermeléssé alakult (NATO StratCom COE 2022; WALLNER–COPELAND–GIUSTOZZI 2025).

Mosás (M): 2014-ben az információmosás álszakértőkön és kreált bizonyítékokon keresztül zajlott, korlátozott platformszámmal. 2025-re a mosás automatizálódott: a FRISCHLICH és munkatársai (2019) által dokumentált bot-piacokon beszerezhető profilhálózatok és a VMB (2024) által feltárt 17 koordinált csoport révén az állami eredet elfedése iparosított folyamattá vált.

[445] BOLT, Neville (2025): *The NextGen Information Environment*. NATO Strategic Communications Centre of Excellence, Riga. 15–16., 20. o. Az előrejelzés az agentic MI-rendszerek teljes körű automatizálását, az algoritmikus hadszínteret (gépek céloznak gépeket), a „szennyezett információs ökoszisztémát" (poisoned training data) és a tudásautoritás válságát (MI mint leghitelesebb forrás) azonosítja a következő évtized központi kihívásaiként.

Terítés (T): 2014-ben a terítés három fő csatornára korlátozódott (állami TV, online portálok, közösségi média), a közeg nyitott és szabályozatlan volt. 2025-re a közeg fragmentálódott: a Telegram (36,83%) és a Twitter/X (39,43%) dominál, miközben a DSA-szabályozott platformok aktív elhárítókká váltak (NATO StratCom COE 2024). A HELLMAN és WAGNSSON (2017) által azonosított négy válaszstratégia közül a blokkolás és a konfrontáció vált dominánssá az EU-ban.

Validálás (V): 2014-ben az orosz narratívák validálása a fősodratú nyugati média átvételén keresztül történt (PRIER 2017: commanding the trend), a hatás stratégiai meglepetés és bénultság volt. 2025-re a validáció kudarcba fulladt: a LEWANDOWSKY és munkatársai (2012) által leírt folytatólagos befolyás hatása ugyan továbbra is érvényesül, de a pre-bunking, az inokulációs stratégiák (PAMMENT 2021: RESIST 2) és a horizontális ellenőrzési hálózatok (NAFO, OSINT) a hatást a meggyőzésről a kognitív fáradtságra szorították vissza. A PAZIUK és munkatársai (2025) által mért 52,7%-os negatív tartalom-arány ezt a váltást számszerűsíti.

[7. ábra helye: A kognitív hadviselés hatékonysági mutatóinak eltolódása (2014–2025) – a végleges változatban grafikonnal illusztrálva]

A G–M–T–V lánc összehasonlítása megerősíti a FMK Kognitív Olló modell predikciójait: a műveleti lánc minden elemében mennyiségi eszkaláció történt, de a védelmi oldal adaptációja – a HELLMAN–WAGNSSON-féle válaszstratégiák intézményesülésétől az ADAMSKY (2015) által leírt kereszttartományi kényszerítés felismeréséig – a stratégiai hatékonyság stagnálását eredményezte. Ez az elméleti és empirikus alapvetés teszi szükségessé a 8. fejezetben bemutatásra kerülő Multimodális Reziliencia Mátrix alkalmazását, amely az emberi tűzfal és a technológiai kontroll ötvözésével kínál rendszerszintű megoldást.

8. SZINTÉZIS ÉS VÉDEKEZÉS: A MULTIMODÁLIS REZILIENCIA MÁTRIX OPERATÍV ALKALMAZÁSA

A disszertáció eddigi fejezeteiben feltártam a kognitív hadviselés technológiai és stratégiai természetét: a 4. fejezet a 2014-es krími műveletek bénító hatását, az 5. fejezet a 2014–2021 közötti transzformációs időszak változópontjait, a 6. fejezet a 2022–2025-ös iparosított kognitív hadviselést, a 7. fejezet pedig a keresztmetszeti összehasonlítást és a FMK Kognitív Olló modelljét mutatta be. Jelen fejezet a diagnózistól a beavatkozás felé halad: az Irányítás (Control) dimenzió

operatív keretét fejti ki, és a Multimodális Reziliencia Mátrix (MRM) gyakorlati alkalmazását mutatja be – különös tekintettel a G–M–T–V műveleti lánc Mosás-dimenziójának szűk keresztmetszetére és a Validálás-dimenzió kétoldalú eróziójára, amelyek a 2025–2030-as időszak fő fenyegetésvektorai.

8.1. Az OxIPO és a HIP modell szintézise az Irányítás dimenziójában

A hatékony védekezés kidolgozásához elengedhetetlen a humán és a szervezeti tényezők rendszerszintű összekapcsolása. Ahogy azt a 2. fejezetben, a módszertani keret felvázolásánál jeleztem, a védekezés nem egydimenziós probléma: egyszerre kell kezelnie az egyéni kognitív sebezhetőségeket és a szervezeti válaszadás strukturális korlátait. E két réteg integrálására az Emberi Információfeldolgozási modell (Human Information Processing – HIP) és az OxIPO (Output = Input × Process × Organization) modell szintézise kínál keretet.[446]

8.1.1. A HIP modell szerepe a kognitív ellenállóképességben

A HIP modell a védekezés legkisebb, de legkritikusabb egységére, az egyénre fókuszál. A kognitív pszichológia alapvető keretrendszereként[447] a HIP segítségével érthetjük meg, hogy az AutoGenAI által generált mennyiségi ugrás hogyan hat az emberi észlelésre, a rövid távú memóriára és a döntéshozatalra. A kognitív hadviselés hatásmechanizmusa három kritikus ponton támadja az egyéni feldolgozást.

Szelektív figyelem (attention): Az információs zajban a figyelem beszűkül, ami az egyént a megerősítési torzítás (confirmation bias) irányába tolja. Kahneman[448] 1-es rendszere – a gyors, automatikus, heurisztikus és érzelmi alapú feldolgozás – átveszi az irányítást a 2-es rendszertől, ami a kritikai elemzőképesség drasztikus csökkenését eredményezi.

---

[446]WICKENS, Christopher D. – HOLLANDS, Justin G. (2000): Engineering Psychology and Human Performance. Prentice Hall, Upper Saddle River (NJ). 12–45. o.

[447]LINDSEY, Peter H. – NORMAN, Donald A. (1977): Human Information Processing. Academic Press, New York.

[448]KAHNEMAN, Daniel (2013): Gyors és lassú gondolkodás. Ford. BÁNYÁSZ Réka. HVG Könyvek, Budapest. 35–42. o.

Kognitív túlterhelés: A rövid távú memória véges kapacitása miatt a folyamatos ingerlés a kognitív fáradtság (cognitive fatigue) állapotához vezet.[449] A 6. fejezetben elemzett AutoGenAI ökoszisztéma pontosan ezt a kapacitásküszöböt célozza: ha a bemeneti ingertömeg meghaladja a 2-es rendszer kapacitását, a befogadó nem képes ellenőrizni, mérlegelni és cáfolni.

Heurisztikus döntéshozatal: A túlterhelt kognitív rendszer a logikai elemzés helyett mentális rövidutakat alkalmaz. A kognitív hadviselés során leggyakrabban kihasznált heurisztikák: az elérhetőségi heurisztika (az érzelmileg túlfűtött, sokszor ismételt tartalom dominál), a horgonyzás (az elsőként befogadott dezinformációs narratíva meghatározza a későbbi értelmezési keretet, és a cáfolatokkal szemben ellenállóvá teszi az egyént), valamint a tekintélyre való hivatkozás (a Doppelgänger-profilokba és klónozott szakértői identitásokba vetett indokolatlan bizalom).

A védekezés során tehát nem elegendő az információk cáfolata; olyan környezetet kell teremteni, amely támogatja az egyéni információfeldolgozás integritását a FMK Kognitív Olló nyílása közepette is. A 2. fejezetben bevezetett ÁEI-protokoll (Állj meg – Ellenőrizd – Igazold)[450] pontosan erre a célra szolgál: három egyszerű, ismételhető lépésben operálhatóvá teszi a forráskritikát, a bizonyíték-ellenőrzést és a kármérlegelést. Az ÁEI protokoll gyakorlati megvalósítása a rutin-triád (ki az állító, milyen a bizonyíték, mi a várható kár tévedés esetén), amely a mikroszintű reziliencia első pilléreként szolgál.

8.1.2. Az OxIPO modell és a szervezeti válaszképesség

Szervezeti szinten a védekezést az OxIPO modell keretei között értelmezhetjük.[451] A 4. és 6. fejezetek MRM kontroll-leltárainak összehasonlítása rávilágított, hogy a szervezeti struktúra (Organization) merevsége volt a 2014-es kudarc fő oka. Amikor a krími események során a NATO és az EU döntéshozatali láncai lassan reagáltak, az nem kizárólag a politikai akarat hiányából fakadt, hanem abból is, hogy a szervezeti rendszerek (Process) nem voltak felkészülve a multiplex, többcsatornás információs támadások kezelésére. A bemenet (Input) eleve túlterhelt volt, a

[449]WICKENS, C. D. – HOLLANDS, J. G. – BANBURY, S. – PARASURAMAN, R. (2015): Engineering Psychology and Human Performance. Psychology Press, New York. 88–112. o.

[450]Az ÁEI-protokoll részletes kifejtése: v.ö. a 2. fejezet §2.6.1 (Mikroszint: Kognitív immunizáció és az ÁEI-protokoll).

[451]ORBÁN Zsolt (2021): E-learning projektek sikertényezői. Az e-learning megoldások actor-network theory elemzése. Doktori értekezés. Budapesti Corvinus Egyetem, Budapest.

feldolgozás (Process) szekvenciális maradt, és a szervezeti válasz (Organization) hierarchikus jóváhagyási láncokra épült.

A 2022 utáni sikeres védekezés kulcsa ezzel szemben az a horizontális, hálózatosodott szervezeti forma volt, amely képes volt integrálni az egyéni HIP-szintű megfigyeléseket (OSINT-közösségek, NAFO-önkéntesek) a makroszintű döntéshozatalba (NATO StratCom, StratCom Centre UA). Az ukrán Diia platform modellezte, hogyan lehet az állami szintű koordinációt a polgári szintű rezilienciával összekötni – a szervezeti adaptivitás az OxIPO-modell legdinamikusabb dimenziójának bizonyult.

8.1.3. A szintézis: Az integrált védekezési lánc

A két modell szintézise teremti meg a lehetőséget arra, hogy a védekezést ne pontszerű beavatkozásként, hanem egy folyamatos láncolatként lássuk. Az egyéni szintű (HIP) pszichológiai állóképesség és a szervezeti szintű (OxIPO) adaptivitás együttesen határozza meg a rezilienciát. Ebben a megközelítésben három funkcionális lépés rajzolódik ki: a szűrés (az MI-alapú zaj technológiai blokkolása, szervezeti – azaz OxIPO – szint), a kontextualizálás (a narratívák keretezése az egyéni értelmezés segítésére, egyéni – azaz HIP – szint), és a visszacsatolás (a társadalmi reakciók becsatornázása a döntéshozatalba). Ez az elméleti szintézis képezi az alapját a következő alfejezetben bemutatásra kerülő Multimodális Reziliencia Mátrixnak (MRM), amely már konkrét cselekvési szintekre lebontva javasol megoldást a diagnosztizált kihívásokra.

8.2. A Multimodális Reziliencia Mátrix (MRM) operatív alkalmazása

A disszertáció központi tudományos nóvuma a Multimodális Reziliencia Mátrix (MRM), amely a korábban elemzett elméleti modellek – az OxIPO és a HIP – szintéziseként jött létre.[452] Ahogy azt a 2. fejezetben a kutatási célkitűzések között rögzítettem, a cél egy olyan diagnosztikai és védelmi keretrendszer, amely képes a kognitív hadviselés támadásait rendszerszintűen kezelni. A mátrix három beavatkozási szinten (mikro–mezo–makro) és a H–E–I dimenziók mentén (Bemenet/Helyzet – Folyamat/Előrejelzés – Irányítás/Kontroll) operál. Fontos hangsúlyozni: a 2. fejezet §2.6-ban a mátrixot modalitás-alapú bontásban (szöveg, kép, hang, videó) mutattam be a fenyegetési oldalról. Jelen fejezet a védekezési oldalról, szint-alapú bontásban (mikro–mezo–

[452]HORVÁTH Dávid (2025d): Multimodális Reziliencia Mátrix: Az OxIPO és a HIP modellek szintézise a kognitív hadviselés elleni védekezésben. Nemzet és Biztonság (megjelenés alatt).

makro) fejti ki a mátrixot. A két nézőpont kiegészíti egymást: együttesen adják az MRM teljes operacionalizálását.

8.2.1. Mikroszint: Az egyéni kognitív immunválasz

A mátrix legalsó, de legkritikusabb szintje az egyén. Az egyéni információfeldolgozás integritása az első védvonal – amelynek elméleti alapjait a HIP modell adja.[453] Mikroszinten a reziliencia három elemre épül:

Bemenet (Helyzet): Az egyéni digitális higiénia és a forráskritika alkalmazása. A digitális higiénia (digital hygiene) olyan tudatos magatartásformák és technikai óvintézkedések összessége, amelyek célja az egyéni digitális lábnyom minimalizálása és az információs környezetszennyezés tudatos szűrése.[454]

Folyamat (Előrejelzés): A kognitív torzítások felismerésének képessége és az ÁEI-protokoll alkalmazása.[455] A reziliencia itt konkrét, ismételhető ellenőrzési rutinok összessége. Az előzetes immunizáció (pre-bunking) hatékonyságát a Roozenbeek–Van der Linden (2022) kísérletsorozat igazolta:[456] a rövid, 90 másodperces pre-bunking videók 21–29%-kal csökkentették a dezinformációs üzenetekre való fogékonyságot.

Irányítás (Kontroll): Az egyéni tudatosság, amely ellenáll a kognitív fáradtságnak és a kognitív nihilizmusnak. A hatékony cáfolat ezen a szinten alternatív, koherens magyarázatot is kínál, mivel önmagában a tagadás mentális vákuumot hagy a befogadó modelljében.[457]

---

[453] WICKENS, Christopher D. – HOLLANDS, Justin G. (2000): Engineering Psychology and Human Performance. Prentice Hall, Upper Saddle River (NJ). 12–45. o.

[454]BUSH, J. et al. (2021): Digital Hygiene: Best Practices for an Evolving Threat Landscape. Cybersecurity Journal.

[455] Az ÁEI-protokoll részletes kifejtése: v.ö. a 2. fejezet §2.6.1 (Mikroszint: Kognitív immunizáció és az ÁEI-protokoll).

[456]ROOZENBEEK, Jon – VAN DER LINDEN, Sander (2022): The Prebunking Intervention against Fake News. PNAS, 119. évf. 1. sz.

[457]LEWANDOWSKY, Stephan et al. (2012): Misinformation and Its Correction: Continued Influence and Successful Debiasing. Psychological Science in the Public Interest, 13. évf. 3. sz. 106–131. o.

8.2.2. Mezoszint: Szervezeti és közösségi adaptáció

A középső szint a szervezeteket, intézményeket és közösségeket foglalja magában. A védekezésnek a LEFEBVRE (1967) nevével fémjelzett reflexív kontroll (reflexive control) elméletére kell épülnie,[458] amely az ellenfél döntési logikájának szándékos torzítását modellezi. A Mezoszintű reziliencia kulcsa az emberi tűzfal (human firewall) megerősítése[459] – a NATO StratCom COE,[460] az ukrán StratCom Centre UA és a hasonló szervezetek az alábbi három funkciót látják el:

Bemenet (Helyzet): Rendszerszintű monitoring és az AutoGenAI által generált mintázatok felismerése. A 7. fejezetben elemzett Robotrolling-jelentések (2024) mutatják, hogy a detekciós képesség hálózatszintű monitoringot igényel.[461]

Folyamat (Előrejelzés): Gyors döntési ciklusok (OODA-hurok), amelyek lehetővé teszik a megelőző figyelmeztetés (pre-bunking) alkalmazását. Az SCC-protokoll (Sebesség–Tartalom–Irányítás) a szervezeti szint operatív gerincét adja, amelyet a következő, 8.3. alfejezetben részletesen kifejtek.

Irányítás (Kontroll): Szervezeti protokollok alkalmazása a dezinformáció semlegesítésére és a hiteles intézményi tájékoztatás fenntartására. Az emberi tűzfal integritása itt dől el: ha a szervezeten belüli kommunikációs rutinok megbízhatóak, a külső manipuláció hatása csökken.

8.2.3. Makroszint: Állami és nemzetközi stratégiai keret

A mátrix legfelső szintje a rendszerszintű reziliencia. Ez a szint biztosítja azt a jogi és stratégiai páncélzatot, amelyről az 5.4. alfejezetben, az uniós szabályozás kapcsán írtam. A Makroszint feladata a nemzeti és szövetségi szintű többrétegű védelmi stratégia (multi-layered defense strategy) összehangolása. A reziliencia egyik mérhető ismérve, hogy a fenyegetésre létrejön-e

[458]LEFEBVRE, Vladimir A. (1967): Conflicting Structures. Soviet Radio, Moscow.

[459]A mezoszintű védekezés szervezeti kiterjesztéséhez l. a 2. fejezet §2.6.2 (Mezoszint: Szervezeti reziliencia).

[460]LANGE-IONATAMIŠVILI, Sanda et al. (2015): Analysis of Russia's Information Campaign against Ukraine. NATO StratCom COE, Riga.

[461]NATO StratCom COE (2024a): Robotrolling 2023/2024 – Analysis of Automated Activity on Social Media. Riga.

tartós intézményi válaszarchitektúra: kijelölt felelősségek, adatmegosztási rutinok, válságkommunikációs protokollok és nemzetközi együttműködések.

Bemenet (Helyzet): Stratégiai figyelmeztetés (strategic warning) és nemzetközi hírszerzési információmegosztás, például a Hybrid CoE keretein belül.

Folyamat (Előrejelzés): Nemzeti és szövetségi narratívaépítés, amely proaktív módon tölti ki az információs teret a támadó impulzusok előtt.

Irányítás (Kontroll): Platformauditálás, a DSA-szabályozás[462] érvényesítése és az oktatási reformon alapuló kognitív védelem. A platformauditálás (platform auditing) olyan független vizsgálati folyamat, amely során ellenőrzik, hogy az óriásplatformok algoritmikus rendszerei megfelelnek-e a biztonsági elvárásoknak.[463]

Az MRM-mátrix legnagyobb előnye, hogy rávilágít a szintek közötti dinamikus interakcióra: például hiába robusztus a Makroszintű szabályozás, ha a Mikroszinten az egyéni reziliencia alacsony, a rendszer sebezhető marad. A 4. fejezet 2014-es MRM kontroll-leltára és a 6. fejezet 2022–2025-ös végállapota közötti összehasonlítás éppen ezt a szintek közötti kölcsönhatást dokumentálta: a legnagyobb előrelépés nem egy szinten, hanem az integrációban történt.

8.3. Az SCC-protokoll operatív kifejtése

A mezoszintű beavatkozástervezés operatív gerincét az SCC-protokoll (Sebesség–Tartalom–Irányítás; angolul: Speed–Content–Control) adja, amelyet a 2. fejezet §2.6.2-ben definiáltam. A protokoll három, egymásra épülő beavatkozási tengelyt rögzít, amelyeket az alábbiakban részletezek – visszakapcsolva az MRM megfelelő szintjeire.

8.3.1. A Sebesség-tengely (Speed)

A Sebesség-tengely a dezinformáció terjedési sebességét a szervezeti válaszreakció sebességével állítja szembe. Vosoughi, Roy és Aral (2018) 126 000 Twitter-pletykán igazolta, hogy a hamis hírek átlagosan hatszor gyorsabban jutnak el 1500 felhasználóhoz, mint az igazak, és a leggyorsabb

[462]EUROPEAN COMMISSION (2022a): Digital Services Act. Regulation (EU) 2022/2065.

[463]EUROPEAN COMMISSION (2023): Guidance on the Independent Auditing of Very Large Online Platforms. Brussels.

cascades-ek perceken belül ezrekhez érnek el.[464] Wardle és Derakhshan (2017) agent–message–interpreter fázismodellje alapján az intézményi válasznak a terjesztési szakaszba kell beavatkoznia, mielőtt az üzenet az értelmezési fázisba lép[465] – a stratcom-szakirodalomban erre épülő operatív hüvelykujjszabály az első 90 perc.[466] Ha az intézményi válasz nem érkezik meg ezen belül, a dezinformációs narratíva kognitív rögzülése megkezdődik, és a későbbi korrekciók hatékonysága drasztikusan csökken.

A Sebesség-tengely alkalmazása ugyanakkor nem kizárólag szervezeti akarat kérdése. A NATO StratCom COE 2022-es, nyolc kereskedelmi eszközre kiterjedő értékelése kimutatta, hogy a prémium-kategóriás közösségimédia-figyelő platformok (Brandwatch, Meltwater, Sprinklr, Digimind) képesek valós idejű vizualizációra, ám az MI-modellek a kisebb, kevésbé adatgazdag nyelvekben – így a magyarban is – szignifikánsan gyengébben teljesítenek.[467] Ez geopolitikai aszimmetria: a nagyobb nyelvközösségek (angol, orosz, arab) számára elérhető automatizált detekció a kisebb NATO-tagállamoknak ugyanolyan szinten nem áll rendelkezésre. A Sebesség-tengely tehát technológiai és nyelvpolitikai erőforrás-kérdés is – ami különösen releváns a disszertáció magyarországi alkalmazási kontextusában.

8.3.2. A Tartalom-tengely (Content)

A Tartalom-tengely azt rögzíti, hogy az ellen-narratívának nem a hazugságot kell megismételnie (inoculation trap), hanem alternatív kognitív keretet kell kínálnia. A Lewandowsky és Van der Linden (2021) által újrafogalmazott inokulációs elmélet lényege, hogy a társadalom „oltható" a dezinformáció ellen:[468] ha a célközönség előzetesen megismeri a manipulációs technikákat (gyengített dózisban), a valódi támadás hatása szignifikánsan csökken. A Google Jigsaw (2024)

[464]VOSOUGHI, Soroush – ROY, Deb – ARAL, Sinan (2018): The spread of true and false news online. Science, 359. évf. 6380. sz. 1146–1151. o.

[465]WARDLE, Claire – DERAKHSHAN, Hossein (2017): Information Disorder: Toward an interdisciplinary framework for research and policymaking. Council of Europe Report. 48–52. o.

[466]A stratcom-szakirodalomban alkalmazott „első 90 perces hüvelykujjszabályhoz l. PAMMENT (2022: 34).

[467]GRIZANE et al. (2022): Evaluation of Social Media Monitoring Tools. NATO StratCom COE, Riga. A nyolc kereskedelmi eszköz összehasonlító értékelése.

[468]LEWANDOWSKY, Stephan – VAN DER LINDEN, Sander (2021): Inoculation Theory and Misinformation. Nature Reviews Psychology, 1. évf. 1. sz. 13–25. o.

nagymintás kísérletsorozata bizonyította,[469] hogy a rövid, 90 másodperces pre-bunking videók 21–29%-kal csökkentették a dezinformációs üzenetekre való fogékonyságot.

A Tartalom-tengely második eleme a narratív dominancia: nem az ellenséges hazugságokra kell válaszolni, hanem saját, hiteles és koherens stratégiai narratívát kell építeni, amely kitölti az információs teret, nem hagyva helyet a bizonytalanságnak. A 6. fejezetben elemzett Telegram-sokk illusztrálta: a vákuumot mindig az agresszor tölti ki. A hitelesség-menedzsment – a kormányzati és szakmai források iránti közbizalom erősítése – a kognitív hadviselés leghatékonyabb ellenszere, mert közvetlenül az emberi tűzfal bizalmi alapját célozza.

8.3.3. Az Irányítás-tengely (Control)

Az Irányítás-tengely a csatorna- és amplifikációs döntéseket kezeli: mely platformon, milyen validálási réteggel és milyen célcsoportnak juttatják el a szervezeti választ. Az SCC-protokoll Irányítás-tengelye a Pamment (2022) által kidolgozott információs befolyásoló művelet-elhárítási keretrendszer harmadik (ellennarratív kommunikáció) és negyedik (szabályozási és jogi eszközök) funkcionális dimenziójába illeszkedik.[470] Pamment emellett felhívja a figyelmet az archetipikus szervezeti aszimmetriára: a legtöbb szervezet reaktív üzemmódban van, miközben a proaktív képesség fejlesztéséhez strukturált beruházásra – képzésre, értékelési ciklusra, intézményi koordinációra – van szükség.[471]

Az Irányítás-tengely továbbá az attribúciós kapacitás intézményi feltételeinek megteremtését is előírja. A NATO StratCom COE és a Hybrid CoE (2023) közös tanulmánya megállapítja, hogy az attribúció a 2018 óta végzett 350-nél több koordinált manipulációs hálózat-levétel tapasztalatai alapján következetesen „diszfunkcionális” maradt.[472] A négyes lencserendszer (technikai, viselkedési, szervezeti, politikai bizonyítékok) alkalmazása nem vált egységes gyakorlattá. A krími

[469]JIGSAW (2024): The Science of Prebunking: Resilience against Manipulation. Google Jigsaw Research Reports.

[470]PAMMENT, James (2022): Assessing national capabilities for countering foreign information manipulation and interference. NATO StratCom COE, Riga. A négy funkcionális terület: (1) detekció, (2) attribúció, (3) ellennarratív kommunikáció, (4) szabályozási eszközök.

[471]PAMMENT, James – SÖRENSEN, Mats (2023): Evaluating counter-FIMI capacity building: A framework for assessment. NATO StratCom COE, Riga. 22–38. o.

[472]NATO StratCom COE és Hybrid CoE (2023): közös tanulmány az attribúció rendszerszintű nehézségeiről. A 350-nél több koordinált manipulációs hálózat-levétel tapasztalatai alapján.

esetből levonható tanulság: az attribúciós kapacitás fejlesztése strukturális befektetést igényel, az SCC-protokoll bevezetéséhez a képzési programok mellé formális értékelési ciklus és intézményi tanulási mechanizmus szükséges.

8.4. A G–M–T–V lánc szintézise: a Mosás-dimenzió és a Validálás-erózió

A 7.6. alfejezet összehasonlító táblázata[473] a G–M–T–V műveleti lánc (Generálás–Mosás–Terítés–Validálás) minden elemében mennyiségi eszkalációt dokumentált 2014 és 2025 között. A FMK Kognitív Olló modell[474] predikciói szerint azonban ez az eszkaláció nem eredményezett arányos stratégiai hatékonyság-növekedést. A 4. és 6. fejezetek MRM kontroll-leltárai ennek okát két kritikus dimenzióban tárják fel.

A Mosás (M) dimenzió szűk keresztmetszete. 2014-ben a narratívák Mosás-fázisa – a forrás elfedése, a hitelességi transzfer, a „független" álcivil szervezeteken és álhírportálokon keresztül való legitimizálás – képes volt közel teljes hitelességillúziót előállítani. 2025-re ez a fázis lett a támadó műveleti láncának leggyengébb láncszeme. A generálási költség nullához közelít (az AutoGenAI percek alatt előállít tetszőleges mennyiségű tartalmat), tehát a műveleti szűk keresztmetszet nem a tartalom előállítása, hanem a hiteles forrásba csomagolása. A NATO StratCom COE (2024) Robotrolling-elemzése dokumentálta,[475] hogy a GAN-generált profilképek és az emberi kapacitást meghaladó publikációs tempó (napi 15+ cikk) már detektálható mintázatot alkot. A Doppelgänger-művelet[476] – ahol a Mosás és a Validálás egyetlen műveletbe olvad a klónoldalak révén – a dimenzió legfejlettebb formája, de éppen ezen a komplexitáson bukik el: a DISARM-taxonómia és az EEAS FIMI-jelentések rendszerszintűen feltárják a séma struktúráját.

A Validálás (V) dimenzió kétoldalú eróziója. A Validálás kettős eróziónak van kitéve. Egyfelől a támadó oldal validációs rétegei (RT, Sputnik, álszakértői hálózatok) az EU 2022/350 rendeletének (a Tanács 2022. március 1-jei határozata az RT és Sputnik EU-s sugárzási tilalmáról), a

---

[473] A G–M–T–V műveleti lánc összehasonlító összegzése: l. a 7. fejezet §7.6 táblázatát.

[474] A Kognitív Olló modell kidolgozásához l. a 7. fejezet §7.5.1, valamint: HORVÁTH (2024b). A modell az OxIPO és a HIP szintéziseként jött létre.

[475] NATO StratCom COE (2024a): Robotrolling 2023/2024 – Analysis of Automated Activity on Social Media. Riga.

[476] A Doppelgänger-művelet részletes elemzéséhez l. a 6. fejezet §6.2.2, valamint: EEAS (2024): 2nd Report on FIMI Threats.

platformlevételek és az OSINT-közösség feltárásai során sérültek.[477] Másfelől a védekező oldal validációs képessége is erodál: a hazugok osztaléka (Liar's Dividend) mechanizmus révén a szintetikus tartalmak puszta létezése aláássa a valódi bizonyítékok hitelességét is.[478] A 6. fejezetben elemzett kognitív nihilizmus ennek a végállapota: nem az a cél, hogy a célközönség elhiggyen egy konkrét hazugságot, hanem hogy ne higgyen többé az igazság megismerhető voltában. Ez a kétoldalú erózió a 2025–2030-as időszak fő fenyegetésvektora, és az MRM mindhárom szintjén egyidejű beavatkozást igényel.

8.5. Gyakorlati ajánlások a döntéshozók számára

A Multimodális Reziliencia Mátrix nem öncélú elméleti konstrukció, hanem a modern hadviselés tanulságaiból levont, gyakorlatközpontú döntéstámogató eszköz. Alkalmazása a magyar biztonsági kontextusban különösen aktuális: Magyarország Nemzeti Biztonsági Stratégiája[479] a hibrid fenyegetéseket kiemelt kockázatként azonosítja, ám az operatív válaszképesség fejlesztése további lépéseket igényel.

8.5.1. Diagnózis és beavatkozási pontok azonosítása

A mátrix gyakorlati haszna az, hogy segítségével a döntéshozók pontosan beazonosíthatják, hol mutatkozik hiányosság a nemzeti rezilienciában. Például, ha a hírszerzési adatok (Makroszint/Bemenet) jelzik az AutoGenAI alapú dezinformáció megjelenését, de a társadalomban hiányzik a kognitív higiénia (Mikroszint/Irányítás), a beavatkozás célterülete azonnal meghatározható. A kutatás eredményei alapján az alábbi konkrét javaslatok tehetők:

A kiber- és kognitív védelem integrációja: A fizikai szabotázs és a kognitív félelemkeltés konvergenciája miatt a kiberbiztonsági és a stratégiai kommunikációs egységek szoros,

[477]HOYLE, B. – PIJPERS, P. B. M. J. (2022): The Ban on RT and Sputnik: A Strategic Communications Perspective. Defence Strategic Communications, Vol. 11, No. 1.

[478]SCHIFF, K. J. – SCHIFF, D. S. – BUENO DE MESQUITA, B. (2023): The Liar's Dividend. SocArXiv.

[479]1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról. Magyar Közlöny, 2020. 81. sz.

intézményesített együttműködésére van szükség.[480] A kognitív védelem nem a stratcom-osztály egyedi feladata, hanem rendszerszintű képesség.

Proaktív narratívakészlet fejlesztése: A Telegram-sokk tanulsága az, hogy a vákuumot mindig az agresszor tölti ki. Magyarország számára kritikus fontosságú olyan hiteles nemzeti narratívák kidolgozása, amelyek válsághelyzetben stabil hivatkozási pontot jelentenek.

8.5.2. Kognitív hadgyakorlatok és képességfejlesztés

A reziliencia edzhetővé válik. Szükséges olyan szimulációs gyakorlatok szervezése, ahol a döntéshozóknak hiperrealisztikus deepfake-ek és mesterségesen generált információs káosz közepette kell döntéseket hozniuk, tesztelve az OODA-hurkok és az SCC-protokoll hatékonyságát. A Pamment és Sörensen (2023) által operacionalizált négyelemű értékelési eszközkészlet ehhez módszertani alapot kínál.[481]

Viktorija Rusinaitė (2025) a Hybrid CoE legfrissebb elrettentéskutatásában dokumentálja, hogy a 2020–2024 között levezetett, hibrid fenyegetéseket szimuláló asztali gyakorlatok (tabletop exercises) során a résztvevő államok rendszeresen a stratégia–praxis rés (strategy–praxis gap) problémájába ütköztek: az elrettentési stratégiák papíron léteztek, de a tartományok közötti (cross-domain) koordináció – különösen az információs és a jogi dimenzió között – a gyakorlatban rendre kudarcot vallott. Az MRM mátrix éppen erre a résre kínál diagnosztikai eszközt.[482]

Magyar nyelvű MI-detekciós képesség fejlesztése: A NATO StratCom COE (2024) értékelése kimutatta, hogy a kisebb nyelvű NATO-tagállamok számára az automatizált detekció szignifikánsan gyengébb.[483] Magyarország számára ez közvetlen biztonsági rés: a magyar nyelvű MI-alapú tartalomszűrés és dezinformáció-detekció fejlesztése stratégiai beruházás.

---

[480]KRASZNAY Csaba (2023a): A kiber- és kognitív műveletek konvergenciája az orosz–ukrán háborúban. Felderítő Szemle, 22. évf. 4. sz. 15–32. o.

[481] PAMMENT, James – SÖRENSEN, Mats (2023): Evaluating counter-FIMI capacity building: A framework for assessment. NATO StratCom COE, Riga. 22–38. o.

[482] RUSINAITĖ, Viktorija (2025): Turning strategy into praxis: Lessons in hybrid threat deterrence. Hybrid CoE Paper 25. European Centre of Excellence for Countering Hybrid Threats, Helsinki. 8–12. o.

[483]NATO StratCom COE (2024b): AI in Support of StratCom Capabilities. Riga.

Az MRM mátrix alkalmazása rávilágít, hogy a kognitív hadviselés elleni védekezés már nem csupán a honvédség vagy a titkosszolgálatok feladata. A reziliencia-alapú védekezés össztársadalmi beruházás: a szabályozás szűkíti a teret, a saját stratégiai kommunikáció elfoglalja a teret, az oktatás pedig képessé teszi az egyént a térben való biztonságos navigációra. Ezzel a hármas egységgel válik az MRM-mátrix elméleti modellből gyakorlati védelmi keretrendszerré.

9. KÖVETKEZTETÉSEK, ÚJ TUDOMÁNYOS EREDMÉNYEK ÉS KITEKINTÉS

9.1. A kutatási kérdések megválaszolása

A disszertációban bemutatott kutatás az orosz–ukrán konfliktus kognitív dimenziójának evolúcióját vizsgálta, kiindulva a 2014-es krími állapottól egészen a 2022–2025-ös totális háború mesterséges intelligencia által dominált szakaszáig. A kutatás során bebizonyosodott, hogy a kognitív hadviselés 2014-es, kézműves korszaka – amelyet a manuális trollkodás és a fókuszált narratívák jellemeztek – 2025-re egy iparosított, algoritmusok által vezérelt ökoszisztémává vált. Az alábbiakban a négy kutatási kérdésre (KK1–KK4) adott válaszokat rögzítem.

KK1 – Az FMK elhatárolása: A 2. fejezetben kidolgozott hármas kritériumrendszer (szándékoltság, szervezettség, kognitív hatás) alkalmasnak bizonyult a fegyvernek minősülő kommunikáció elkülönítésére a szélesebb propaganda- és dezinformációs tértől. Az FMK-rács (konfigurációs mátrix) a 4. és 6. fejezetben mindkét esettanulmány esetében replikálható kódolást produkált: azonos változók mentén elő tudta választani a szervezett műveleti termékeket a spontán információs zajtól. Az FMK fogalma tehát nem retorikai újranevezés, hanem működő analitikai szűrő.

KK2 – Strukturális különbségek: A 7. fejezet keresztmetszeti összehasonlítása igazolta, hogy a két eset között a terjesztési infrastruktúra, a platformkormányzás és a társadalmi reziliencia mind három dimenzióban szignifikánsan eltolódott. 2014-ben a terjesztési infrastruktúra kézi vezérlésű volt (IRA trollfarm, RT/Sputnik), a platformkormányzás gyakorlatilag hiányzott, és a társadalmi reziliencia alacsony szinten állt. 2025-re az infrastruktúra AutoGenAI-vezéreltté, a platformkormányzás intézményesült (DSA), a reziliencia pedig rendszerszinten erősödött – bár nem egyenletesen (lásd: YouGov magyar adat, §9.2 H2).

KK3 – A transzformációs időszak szerepe: Az 5. fejezet igazolta, hogy a 2014–2021 közötti időszak nem egyszerű átmenet volt, hanem önálló magyarázó változó. A COVID–19 infodémia kettős katalizátorként működött: egyrészt a társadalom megtanulta felismerni a manipulációs mintázatokat („kognitív antitestek”), másrészt a dezinformációs infrastruktúra (csatornák, perszóna-portfóliók, validálási rétegek) is bejáratódott és transzferálódott a háborús kontextusra.

KK4 – A diagnosztikai és beavatkozási keret: A H–E–I mátrix sikeresen biztosította a két eset összehasonlíthatóságát, az OxIPO-modell a szervezeti válaszadás elemzését, a Multimodális Reziliencia Mátrix (MRM) pedig a védekezés rendszerszintű operacionalizálását. A 8. fejezetben

kifejtett SCC-protokoll és az ÁEI-protokoll együttesen olyan gyakorlati eszköztárat adnak, amely a kognitív hadviselés elemzését és az ellene való védekezést mérhető–tanítható–alkalmazható módon a gyakorlat nyelvére fordítja.

9.2. A hipotézisek értékelése

A disszertáció alapját képező négy központi feltételezés vizsgálata a 2014-es és a 2022–2025-ös időszakok összevetésével, valamint a H–E–I mátrix alkalmazásával zárult le. Az alábbiakban rögzítem a kutatás során nyert bizonyítékok alapján levont végső következtetéseket – az 1. fejezetben rögzített árnyalatokkal együtt.

H1 – A doktrinális integráció és bénítás hipotézise: IGAZOLT. A 4. fejezetben bemutatott krími elemzés igazolta, hogy 2014-ben a magas narratív koherencia és csatornaszinkron valóban döntésképtelenséget és kognitív bénultságot (cognitive paralysis) idézett elő. A 7. fejezet összehasonlító elemzése megerősítette, hogy a Benett és Sgerberg (2012) által leírt összekötő cselekvés logikája, amely 2014-ben az orosz műveletek javára dolgozott, 2022-re a védelmi oldal előnyévé vált.[484] A hálózatosodott ellenállóképesség – az OSINT-közösségek, a NAFO-önkéntesek,[485] a stratégiai figyelmeztetés – sikeresen ellensúlyozta a reflexív kontroll kísérleteit.

H2 – A meglepetés elvesztésének hipotézise: IGAZOLT. A 6. fejezet elemzése megerősítette, hogy a bénító hatás a megtámadott félben 2022 után elmaradt.

H3 – A reziliencia-tanulás hipotézise: IGAZOLT, KETTŐS ÉRTELMEZÉSSEL. A COVID–19 infodémia valóban globális kognitív hadgyakorlatként működött, és a társadalom „kognitív antitesteket” fejlesztett.[486] Ugyanakkor az EDMO dokumentálta,[487] hogy az összeesküvés-elméleti csoportok és az oltásellenes mozgalmak csatornái 2022 után zökkenőmentesen fordultak pro-Kreml Ukrajna-narratívák felé – ugyanazok a terjesztési hálózatok, perszóna-portfóliók és

[484]BENNETT, W. Lance – SEGERBERG, Alexandra (2012): The Logic of Connective Action. Journal of Communication, 62. évf. 5. sz. 739–768. o.

[485]COLLEY, T. – MOORE, M. (2022): The Weaponisation of Digital Media: The Case of NAFO. Journal of Information Warfare.

[486]HORVÁTH Dávid (2022): Pandemic and Infodemic – Which One Is More Dangerous? Acta Universitatis Sapientiae, Communicatio, 9. évf. 125–139. o.

[487]EDMO (European Digital Media Observatory): dokumentálta az összeesküvés-elméleti csatornák pro-Kreml átállását 2022 után.

validálási rétegek képesek voltak egy új narratívát hordozni. A H3 helyes értelmezése tehát kettős: a védekező oldal tanult, de a támadó oldal is megőrizte és transzferálta a képességeit. A COVID-időszak nem egyszerűen megerősítette a védekezést, hanem a támadói infrastruktúra számára is tesztkörnyezetként és bejáratott csatornarendszerként szolgált.

H4 – A kognitív nihilizmus és volumen-paradoxon hipotézise: ALÁTÁMASZTOTT, DE EMPIRIKUSAN A LEGINKÁBB VITATHATÓ. A 7. fejezet FMK Kognitív Olló modellje igazolta, hogy a generatív MI által okozott mennyiségi ugrás nem javította a stratégiai hatékonyságot. A Paziuk et al. (2025) által dokumentált 52,7%-os negatív tartalom-arány,[488] a Gallagher et al. (2019) által mért integratív komplexitás-csökkenés,[489] és a VMB (2024) által feltárt MI-hallucináció-jelenség[490] együttesen bizonyítják, hogy az iparosítás paradox módon rontotta az egyedi üzenetek meggyőző erejét. A mennyiségi és a stratégiai hatékonyság közötti összefüggés nem-lineáris jellegű. A disszertáció e hipotézist alátámasztott, de nem teljes bizonyossággal lezárt következtetésként kezeli.

9.3. Új tudományos eredmények

A disszertációban az alábbi főbb tudományos eredményeket foglalom össze, megjelölve a hozzáadott értéket a meglévő szakirodalomhoz képest.

1. A H–E–I diagnosztikai mátrix kidolgozása. A hadtudományi elemzésben alkalmaztam a Helyzet–Előrejelzés–Irányítás (H–E–I) struktúrájú diagnosztikai keretrendszert. A modell lehetővé teszi a kognitív hadviselési műveletek rendszerszintű, összehasonlítható vizsgálatát, függetlenítve az elemzést az éppen aktuális technológiai platformoktól.[491] Hozzáadott érték: a korábbi modellek (PMESII, DIME) nem kínáltak a kognitív dimenzióra specializált, időbeli összehasonlításra alkalmas keretet.

[488]PAZIUK et al. (2025): AI-driven content analysis of Russian information operations. NATO StratCom COE, Riga. A kutatás 52,7%-os negatív tartalom-arányt dokumentált.

[489]GALLAGHER et al. (2019): integratív komplexitás-csökkenés mérése az orosz dezinformációs tartalomban.

[490]VMB (2024): koordinált csoport-elemzés. Az MI-hallucináció-jelenség dokumentálása: a generatív rendszerek által előállított tartalmak belső ellentmondásokat hordoznak.

[491]HORVÁTH Dávid (2025b): Communication Classified as a Weapon and Generative AI as Information Overload: S–F–C Indicators and MRM. Defence and Strategy, 25. évf. 1. sz.

2. A FMK Kognitív Olló elméleti modelljének leírása. Tudományosan definiáltam a technológiai volumen (mennyiség) és a stratégiai hatékonyság (minőség) közötti paradox, nem-lineáris összefüggést.[492] Hozzáadott érték: a szakirodalom eddig a volumen–hatékonyság viszonyt lineárisnak feltételezte; a FMK Kognitív Olló az első modell, amely a két szár (technológiai volumen vs. stratégiai hatékonyság) széttartását formálisan rögzíti.

3. Az AutoGenAI hadtudományi koncepciójának meghatározása. Elemeztem a generatív mesterséges intelligencia által vezérelt, iparosított dezinformációs ökoszisztémát, amelyet AutoGenAI (Automated Generative AI for Information Operations) néven definiálok.[493] Hozzáadott érték: míg a kifejezés az üzleti informatikában ismert, hadtudományi kontextusban a hiperrealisztikus deepfake-ek és az automatizált narratívák által vezérelt kognitív hadszíntéri műveletekre alkalmaztam.

4. A Multimodális Reziliencia Mátrix (MRM) bevezetése. Az OxIPO és a HIP modellek szintézisével létrehoztam egy háromszintű – Mikro–Mezo–Makro – védelmi modellt, amely a rezilienciát az egyéni kognitív higiénia, a szervezeti gyorsaság és az állami szabályozás integrált egységeként értelmezi.[494] Hozzáadott érték: a korábbi reziliencia-modellek általában egydimenziósak (vagy szabályozási, vagy oktatási fókuszúak); az MRM az első három összetevős keret, amely az SCC-protokollal és az ÁEI-protokollal integrálva operatív beavatkozási tervet kínál.

5. A pandémia reziliencia-katalizátor szerepének igazolása. Feltártam a COVID–19 infodémia-kezelés és a 2022-es háborús kognitív védekezés közötti közvetlen kapcsolatot.[495] Bizonyítottam, hogy a társadalmi és intézményi tanulási folyamat döntő faktor a modern hibrid fenyegetésekkel szembeni ellenállásban. Hozzáadott érték: a kettős értelmezés – a védekező és a támadó oldal

---

[492] A Kognitív Olló modell kidolgozásához l. a 7. fejezet §7.5.1, valamint: HORVÁTH (2024b).

[493]GOLDSTEIN, J. A. et al. (2024): Generative AI and Localized Information Operations. Stanford Internet Observatory.

[494] HORVÁTH Dávid (2025d): Multimodális Reziliencia Mátrix: Az OxIPO és a HIP modellek szintézise a kognitív hadviselés elleni védekezésben. Nemzet és Biztonság (megjelenés alatt).

[495] HORVÁTH Dávid (2022): Pandemic and Infodemic – Which One Is More Dangerous? Acta Universitatis Sapientiae, Communicatio, 9. évf. 125–139. o.

egyaránt profitált a COVID-időszakból – a korábbi szakirodalomban ez nem került szisztematikus bizonyításra.

9.4. A kutatás korlátai

A kutatás érvényességének értékelésekor az alábbi korlátokat szükséges rögzíteni. Forrás-korlátok: a disszertáció dominánsan nyilvánosságra került forrásokra épül; a minősített hírszerzési információkhoz nem fér hozzá. A műveleti oldalról származó mennyiségi adatok természetszerűleg korlátozottan elérhetők, így a következtetések többsége proxyk és indirekt indikátorok alapján készült.

Módszertani korlátok: a strukturált, fókuszált összehasonlítás (SFÖ)[496] erőssége a strukturált összevethetőség, de korlátja, hogy két esettanulmány alapján nem vonható le univerzális kauzális következtetés. Az eredmények a vizsgált európai és ukrán kontextusban érvényesek; más földrajzi vagy kulturális környezetben az átvihetőség további vizsgálatot igényel.

Időbeli korlátok: a 2022–2025-ös időszak elemzése még zajló konfliktusra vonatkozik, így a végleges kimenet és hatásértékelés további kutatást igényel. A H4 hipotézis esetében a volumen–hatékonyság összefüggés nem-lineáris jellege további kvantitatív validációt igényel.

Általánosíthatósági korlátok: a kutatás elsődlegesen az orosz információs műveletekre fókuszál. Más aktorok – különösen a Kínai Népköztársaság – információs műveleteire az MRM és a H–E–I mátrix alkalmazása külön validációt igényel.

9.5. Kitekintés: A kognitív hadviselés trendjei 2030-ig

A disszertációban bemutatott eredmények nem csupán a múltbéli és jelenlegi konfliktusok tanulságait rögzítik, hanem előre jelzik azt a pályát is, amelyen a kognitív hadviselés a következő évtizedben haladhat. A 2030-ig tartó időszakban a biztonsági környezetet két kritikus trend határozza meg, amelyek próbára teszik a jelenlegi védelmi keretrendszereket.

A kognitív domén hiper-perszonalizációja: A nagy nyelvi modellek fejlődése lehetővé teszi, hogy a támadó fél a tömegek helyett már egyéneket célozzon meg a személyes digitális lábnyom alapján

[496]GEORGE, Alexander L. – BENNETT, Andrew (2005): Case Studies and Theory Development in the Social Sciences. MIT Press, Cambridge, Massachusetts.

generált, egyedi pszichológiai profilra szabott narratívákkal.[497] Ez a fejlemény közvetlenül a Mikroszintű MRM védelem erősítését igényli: az ÁEI-protokoll és a digitális higiénia eddig tömegkommunikációs fenyegetésre készült, a hiper-perszonalizáció azonban az egyéni sebezhetőséget célozza.

Az algoritmikus szuverenitásért folytatott küzdelem: A nemzetállamok és szövetségi rendszerek számára a saját fejlesztésű, zárt és ellenőrzött MI-modellek birtoklása stratégiai érdekké válik.[498] A NATO StratCom COE NextGen Information Environment előrejelzése (Bolt 2025) megerősíti: az agentic MI-rendszerek teljesen automatizálják az információs műveleteket, gépek céloznak gépeket, és a „szennyezett információs ökoszisztéma" (poisoned training data) aláásható magukat a detekciós rendszereket is.[499] Ez a Makroszintű MRM védelem új kihívása: a szabályozásnak nemcsak a tartalom szintjén, hanem az MI-infrastruktúra szintjén is hatnia kell.

Végezetül megállapítható, hogy bármilyen magassági szintet is érjen el a technológiai automatizáció, a hadviselés végső célja továbbra is a politikai akarat érvényesítése marad, amihez elengedhetetlen az emberi kogníció befolyásolása. A disszertáció legfontosabb tanulsága, hogy a technológiai fegyverkezési verseny mellett a valódi győzelmet a társadalmi reziliencia biztosítja. Az MRM alkalmazása és a tudatos kognitív higiénia fejlesztése nem csupán katonai opció, hanem a nemzeti szuverenitás megőrzésének alapvető feltétele. A hadtudománynak a jövőben nemcsak az algoritmusokat, hanem az embert is a középpontba kell állítania – mert a kognitív hadszíntéren a legfejlettebb mesterséges intelligencia ellen is a kritikai gondolkodás marad az utolsó és leghatékonyabb védvonal.

[497] GOLDSTEIN, J. A. et al. (2024): Generative AI and Localized Information Operations. Stanford Internet Observatory.

[498] HYBRID COE (2024): Countering Hybrid Threats in the Age of Generative AI. Strategic Analysis No. 12. Helsinki.

[499] BOLT (2025): NextGen Information Environment – Implications for Strategic Communications. NATO StratCom COE, Riga. Az agentic MI-rendszerek és a „szennyezett információs ökoszisztéma" (poisoned training data) előrejelzése.

MELLÉKLET

1. táblázat: A Strukturált, Fókuszált Összehasonlítás (SFÖ) rögzített kérdéskészlete

Vizsgálati dimenzió	SFÖ-kérdés (minden esettanulmánynál azonos)	Kapcsolódó hipotézis
I. Bemenet (Input)	Milyen volt a stratégiai narratívák koherenciája és a terjesztési csatornák szinkronizációja?	H1 – Doktrinális integráció foka
II. Folyamat (Process)	Milyen gyors volt a támadó hálózat adaptációs (reakció-)ideje a lelepleződés vagy a moderáció után?	H4 – Automatizáció és MI kognitív szerepe
III. Kimenet (Output)	Sikerült-e elérni a stratégiai meglepetést, illetve a célpont döntéshozatalának megbénítását?	H2 – A kognitív meglepetés ereje
IV. Védekezés (Control)	Milyen volt a célország és a közvetítő platformok reziliencia-szintje (észlelési és válaszadási idő)?	H3 – Intézményi bizalom vs. tartalomalapú védekezés

Forrás: Saját szerkesztés Alexander L. George – Andrew Bennett (2005) Case Studies and Theory Development in the Social Sciences módszertana alapján.

2. táblázat: A Helyzet–Előrejelzés–Irányítás (H–E–I) diagnosztikai mátrix indikátorai

Dimenzió	HELYZET (H) – Bemenet / Input	ELŐREJELZÉS (E) – Folyamat / Process	IRÁNYÍTÁS (I) – Kimenet / Output
Fókusz	Mit látunk? (A támadás ereje)	Hová tart? (A hatásmechanizmus trendje)	Mit teszünk? (A védekezés és a politikai hatás)
Integrált almodell	FMK-rács (zajszűrés)	OxIPO-modell (kognitív mechanizmus)	MRM (többszintű védekezés)
Indikátor 1	Narratív koherencia: egységes-e az üzenet a hálózatokban?	Adaptációs idő: a leleplezés és a válasz reakcióideje (óra/nap)	Feedback-hurkok: van-e adatvezérelt korrekció a támadó részéről?
Indikátor 2	Volumen (amplifikáció): a mesterséges terjesztés aktivitása (botnetek)	Kognitív túlterhelés: a polarizáció és a társadalmi zavar detektálható jelei	Platform-beavatkozás: moderációs tiltások száma (takedowns)
Indikátor 3	Technológiai szint: humán operátorok (trollok) vs. generatív MI / deepfake	Szubliminális hatás: a rejtett elköteleződés és a kognitív torzítás (bias) mértéke	Stratégiai hatásfok: sikerült-e a végcél (döntéshozói meglepetés / paralízis)?

Forrás: Saját szerkesztés.

3. táblázat: FMK-rács – az FMK négy szintjének konfigurációs mátrixa

FMK-szint	Rövid definíció	Aktor (Actor)	Csatorna / infrastruktúra	Műveleti termék	Tipikus cél / kimenet
ÖKOSZISZTÉMA (ecosystem)	A teljes hálózati környezet, ahol az FMK működik (emberek + intézmények + platformok).	Államközeli szervek; proxyk; platformok; algoritmusok.	Médiahálózatok; hirdetési infrastruktúra; szabályozási környezet.	Domináns narratív készlet; hitelességi rend (ki az „igaz").	Percepciós tér átrendezése; bizalomrombolás; kohézió gyengítése.
MŰVELET (operation)	Időben / célban lehatárolható kampány több taktikával, egy végállapotért.	Irányító aktor; végrehajtó hálózat (trollfarm); célcsoportok.	Többcsatornás kampánymix (TV + portál + social + messenger).	Üzenetcsomagok; „fedősztori"; célzott tartalomcsomag.	Meghatározott döntés elérése; stratégiai bénítás; legitimáció.
TAKTIKA (tactic)	Ismétlődő eljárásminta; több technikát kombinál.	Koordináló szereplők; proxyk; hasznos terjesztők; influencerek.	Terjesztési útvonal (pl. „mosás"); platformlogika kihasználása.	Narratíva-variánsok; szaturáció (saturation); átkeretezés.	Figyelem elvonása; értelmezési keret szétverése; kifárasztás.
TECHNIKA (technique)	Konkrét fogás, eszközhasználat, mikroszintű kivitelezési mód.	Egyedi álprofil / bot; klónoldal-szerkesztő; operátor.	Hashtag / rajzás; trendmechanizmus; klónsite; Telegram-csatorna.	Konkrét poszt / mém; deepfake; komment-spam; „szakértői" idézet.	Láthatóság-termelés; hamis konszenzus; bizonyíték-érzet.

Forrás: Saját szerkesztés.

4. táblázat: Multimodális Reziliencia Mátrix (MRM): kárpályák és kontrollpontok

Modalitás	Támadási pont	Tipikus fenyegetés	Reziliencia-kontroll
SZÖVEG (text)	Értelmezés és logikai következtetés	Tömeges bot-kommentek, nyelvtanilag hibátlan megtévesztés	Stilisztikai Zero Trust: forrás-trianguláció, állítás–bizonyíték bontás
KÉP (image)	Első benyomás, érzelmi aktiváció	„Bizonyítékként" tálalt szintetikus fotók (fotórealisztikus deepfake)	Kontextus-validálás: képeredet-ellenőrzés, fordított keresés
HANG (audio)	Bizalom és személyes azonosítás	Hangklónozás, biometrikus imitáció, vezetői üzenetek hamisítása	Visszahívási protokoll: hiteles csatorna-követelmény
VIDEÓ (video)	Valóságérzékelés, jelenlét-illúzió	Deepfake videók, generált „szemtanú" felvételek	Többforrásos megerősítés: metaadat- és kontextus-auditálás

Forrás: Saját szerkesztés.

5. táblázat: A kutatás empirikus bázisát adó intézményi adatforrások és kiberfenyegetettségi jelentések (2014–2025)

Időszak / Konfliktus fázis	Elsődleges aktor (adatforrás)	Adat típusa (primer jelleg)	Relevancia az elemzéshez
2014–2015 (Krím és Donbász)	OSCE (Special Monitoring Mission)	Helyszíni jelentések, incidensnaplók.	A kreált diplomáciai narratívák és a fizikai valóság közötti kinetikus rés mérése.
2014–2015 (Krím és Donbász)	NATO StratCom COE	Katonai-műveleti elemzések (pl. Analysis of Russia's Info War).	A 2014-es orosz doktrína és a reflexív kontroll korai kognitív mintázatainak rögzítése.
2016–2021 (Technológiai transzformáció)	Meta (Adversarial Threat Reports)	CIB-statisztikák (koordinált inautentikus viselkedés): törölt bot-hálózatok, hálózati nyomok, hirdetési költés.	A korábban manuális információs műveletek platform-alapú iparosodásának számszerűsítése.
2016–2021 (Technológiai transzformáció)	EUvsDisinfo (EEAS East StratCom)	Nyílt forrású adatbázis – több mint 15 000 cáfolt, Kreml-barát dezinformációs eset.	A hibrid narratívák diverzifikációjának és a szintetikus tartalmak európai megjelenésének mérése.
2016–2021 (Technológiai transzformáció)	Google Jigsaw / TAG	Technikai jelentések és forenzikus adatok az állami (APT) hátterű kiberműveletekről.	A kiber- és kognitív dimenziók (hack-and-leak) konvergenciája, valamint a pre-bunking hatékonysága.
2022–2025 (Totális háború és AutoGenAI)	Mandiant / Google TAG	Fog of War jelentések; kódalapú attribúciós adatok a kiberfrontról.	Az orosz információs offenzíva sebességének, volumenének és a

Időszak / Konfliktus fázis	Elsődleges aktor (adatforrás)	Adat típusa (primer jelleg)	Relevancia az elemzéshez
			kinetikus csapásokkal való szinkronizációjának mérése.
2022–2025 (Totális háború és AutoGenAI)	DFRLab (Digital Forensic Research Lab)	Valós idejű OSINT-auditok, szintetikus digitális lábnyomok elemzése a háborús térben.	A horizontális védekező hálózatok (pl. NAFO mozgalom) kognitív hatásának mérése a támadó OODA-hurkában.
2022–2025 (Totális háború és AutoGenAI)	Stanford Internet Observatory	Mélyelemzések és algoritmikus vizsgálatok az MI-generált profilokról és deepfake narratívákról.	Az AutoGenAI ipari alkalmazásának és a „kognitív nihilizmus" kialakulásának primer, adatvezérelt bizonyítékai.

Forrás: Saját szerkesztés.

6. táblázat: Az információs zavarok típusainak elhatárolása a szándék és a valóságtartalom alapján

A táblázat forrásai:

WARDLE, Claire – DERAKHSHAN, Hossein: Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making. Council of Europe, 2017. 20. o.

NOLAN, Stephanie – KIMBALL, Spencer: Information Disorder: Misinformation, Disinformation, and Mal-Information. In: Media and Communication, 9(1), 2021.

Fogalom	Igazságtartalom	Szándék (Intent)	Műveleti cél	Példa
Misinformation (Téves informálás)	Hamis / Pontatlan	Nincs ártó szándék (Tévedés)	Nincs (Zaj)	Felhasználó tévedésből rossz dátumot oszt meg, vagy figyelmetlenségből megoszt egy hamis pletykát. [TF1]; [TF2]
Disinformation (Dezinformáció)	Hamis / Manipulált	Szándékolt ártalom	Megtévesztés, befolyásolás	Állami szereplő deepfake videót terjeszt az ellenség megadásáról a társadalmi morál rombolása érdekében.
Malinformation (Rosszindulatú információ)	Valós / Igaz	Szándékolt ártalom	Lejáratás, zsarolás, polarizáció	Privát orvosi adatok, belső levelezések (hack-and-leak) kiszivárogtatása kontextus nélkül – a politikai vagy intézményi hitelesség rombolására. [TF1]; [TF2]

Forrás: Saját szerkesztés [TF1] és [TF2] alapján.

7. táblázat: A szubliminális kísérletek paraméterei és műveleti relevanciája

A táblázat forrásai:

RUCH, Simon et al.: Subliminal messages exert long-term effects on decision-making. Neuroscience of Consciousness, 2016. DOI: 10.1093/nc/niw013

RUCH, Simon et al.: Reactivation of memory during sleep and disruption of memory consolidation by wakefulness. Nature Communications, 8(1), 2017.

Paraméter (Berni Egyetem kísérlete)	Mért érték / Specifikáció	Műveleti relevancia (FMK-kontextus)
Expozíciós idő	17 ms (sandwich masking)	A tudatos észlelés és a racionális védekezés megakadályozása
Kódolási epizód	6 mp / 12 felvillanás	Hippocampus-alapú, tudat alatti memória-rögzülés
Konszolidációs idő	15–25 perc	Késleltetett, de tartós döntésbefolyásolás a jövőben
Szemantikai hatás	Szignifikáns (>50% sikeresség)	Célzott jelentésszintű asszociációk (pl. ellenségkép) rögzítése

Forrás: Saját szerkesztés [TF1] és [TF2] kutatási adatai alapján.

8. táblázat: Helyzet-dimenzió összegző táblázat – Krím 2014

A táblázat forrásai:

TF1: LANGE-IONATAMIŠVILI, Sanda et al.: Analysis of Russia's Information Campaign against Ukraine. NATO StratCom COE, Riga, 2015. 3., 7. o.

TF2: DARCZEWSKA, Jolanta: The Anatomy of Russian Information Warfare: The Crimean Operation, A Case Study. OSW, Warsaw, 2014. 5–7., 23–24. o.

TF3: ENTMAN, Robert M.: Framing: Toward Clarification of a Fractured Paradigm. Journal of Communication, 43(4), 1993. 51–58. o.

TF4: CULLEN, Patrick: Hybrid threats as a new 'wicked problem' for early warning. Hybrid CoE Strategic Analysis 8, 2018. 1–5., 7. o.

TF5: MUMFORD, Andrew: Ambiguity in hybrid warfare. Hybrid CoE Strategic Analysis 24. European Centre of Excellence for Countering Hybrid Threats, 2020.

TF6: CHADWICK, Andrew: The Hybrid Media System: Politics and Power. Oxford University Press, 2013. 1–18. o.

TF7: NATO STRATCOM COE: Internet Trolling as a Tool of Hybrid Warfare: The Case of Latvia. NATO StratCom COE, Riga, 2016. 5–12., 18–22. o.

TF8: HOWARD, Philip N. – GANESH, Bharath – LIOTSIOU, Dimitra – KELLY, John – FRANCOIS, Camille: The IRA, Social Media and Political Polarization in the United States, 2012–2018. Oxford Internet Institute, 2018.

Helyzet (H) komponens	Mit rögzítek (kódolható állítás)	2014 Krím – rövid leírás	Alátámasztó forrás
Aktor–szándék–eszközmix	A helyzet nem „katonai esemény", hanem integrált, többcsatornás konfiguráció	Nyílt és rejtett csatornák együtt (operatív/hírszerzési, diplomáciai, média), cél a politikai-társadalmi alárendelés és legitimációs tér átrendezése	[TF2]
Narratív keret	A mesternarratíva stabil; nem igazságot, hanem besorolást gyárt	„Rendhelyreállítás / védelem / illegitim fordulat" keretezés → a legitim válaszküszöb emelése	[TF1]; [TF3]
Csatorna-szinkronizáció	Hibrid médiarendszer: hagyományos + online tér egymást hitelesíti	TV / hírügynökségi állítások online megerősítése („civil hang"), online jelenségek visszacsatolása a médiába	[TF1]; [TF6]
Volumen és amplifikáció	Kézi vezérlésű, de hálózatcentrikus hangosítás	Kommentelők / álprofilok / troll-kapacitások korai fázisa; platform-korlátok mellett is képes tömegességet és „témaelhelyezést" produkálni	[TF7]; [TF8]
Többértelmű végrehajtás (grey zone signature)	A besorolhatatlanság a helyzet része: ki az aktor, mi a státusz?	Azonosító nélküli fegyveres jelenlét + narratív fedés → „kik ők?" kérdés nyitva marad	[TF5]
Helyzetkép bizonyíthatósága	A helyzetet evidencialáncból kell felépíteni	Idővonal + intézményi elemzés + OSINT / leak típusú nyomok együtt adják a rekonstrukciót	[TF1]; [TF2]; [TF4]

Forrás: Saját szerkesztés [TF1]–[TF8] alapján.

9. táblázat: FMK-rács / FMK-mátrix – a Helyzet-dimenzió operacionalizálása, Krím 2014

FMK-rács tengely	Krím 2014 – kódolt állítás	Rövid magyarázat	Alátámasztó forrás
Szándékosság	A bizonytalanság termelése cél, nem mellékhatás	A narratív keretezés és a többértelmű végrehajtás együtt a legitim válasz késleltetésére dolgozik	[TF5]; [TF1]
Szervezettség	Többcsatornás, összehangolt működés	Nyílt + rejtett csatornák; médiagépezet és operatív komponens együtt; nem spontán zaj	[TF2]; [TF1]
Hatás	Döntési késleltetés és besorolási zavar	A célpont oldalon a „mi történik?" kérdés megválaszolása késik → időnyereség a fizikai konszolidációhoz	[TF5]; [TF4]

Forrás: Saját szerkesztés – forrásjelölések a 8. táblázattal azonosak.

10. táblázat: Előrejelzés-tábla és OxIPO-összegzés – Krím 2014

A táblázat forrásainak jegyzéke

[TF1] CULLEN, Patrick: Hybrid threats as a new “wicked problem” for early warning. Hybrid CoE Strategic Analysis 8, 2018, 1., 2., 4., 5., 7. o.

[TF 2] Az OxIPO-modell operacionalizálására ld. 2.5 alfejezet; a kognitív feldolgozási szűkületek hibrid fenyegetési kontextusban: GIANNOPOULOS, Georgios – SMITH, Hanna – THEOCHARIDOU, Marianthi: The Landscape of Hybrid Threats: A Conceptual Model. Hybrid CoE, Helsinki, 2021, 40–48. o.

[TF 3] MUMFORD, Andrew: Calculated Ambiguity and the Crimea Crisis. Hybrid CoE Strategic Analysis 24/1, 2020, 3., 4., 5., 6. o.

[TF4] RITTEL, Horst W. J. – WEBBER, Melvin M.: Dilemmas in a General Theory of Planning. Policy Sciences, 4(2), 1973, 155., 156., 160–162., 167–169. o.

[TF 5] LANGE-IONATAMIŠVILI, Sanda et al.: Analysis of Russia’s Information Campaign against Ukraine. NATO StratCom COE, Riga, 2015, 3., 7–8., 12–15. o.

[TF 6] Uo. 3., 7–8., 12–15. o.

[TF 7] PAUL, Christopher – MATTHEWS, Miriam: The Russian “Firehose of Falsehood” Propaganda Model. RAND Corporation, 2016, 1–7. o.

[TF 8] BELLINGCAT Investigation Team: MH17 – The Open Source Evidence. 2015, 1., 7., 10. o.

[TF 9] SHANDRA, Alya – SEELY, Robert: The Surkov Leaks: The Inner Workings of Russia’s Hybrid War in Ukraine. RUSI Occasional Paper, 2019, 1–4., 8–9., 16., 23. o.

[TF 10] DFRLab (TOLER, Aric és tsai): Breaking down the Surkov Leaks. Atlantic Council, 2016, 1–3. o.

Forrás: Saját szerkesztés [TF1]–[TF8] alapján.

E (Előrejelzés) elem	Mi volt a „jel"?	Miért nem lett belőle időben riasztás?	Következmény (időnyereség)	Forrás
Besorolási instabilitás	Belpolitikai krízis + külső műveleti nyomok keveredése	Több legitim olvasat; magas reakciókockázat	Döntési halogatás, verifikációs késés	[TF3]; [TF4]
Kiszámított többértelműség	Jelzés nélküli végrehajtás + fedőnarratívák	A legitim válasz küszöbe emelkedik	„Kik ők?" → „Mit tehetek?" késleltetés	[TF5]
Jel–zaj romlása	Csatorna-szinkron + volumen	Nem egy állítás, hanem működésmód	Mintázat csak utólag áll össze	[TF6]; [TF7]
Utólagos bizonyíthatóság	OSINT + leak-rekonstrukciók	Evidencialánc időigényes	Reakció késik; kész tények politikája	[TF8]; [TF9]
Wicked problem logika	Nincs „kész állapot", adaptív ellenfél	A riasztás visszahat; normatív vita	Újrakalibrálás-kényszer	[TF1]; [TF4]

11. táblázat: Irányítás (I) összegző táblázat – Krím 2014 sarokpont

A táblázat forrásai:

TF11: MUMFORD, Andrew: Calculated Ambiguity and the Crimea Crisis. Hybrid CoE Strategic Analysis 24/1, 2020. 3., 4., 5., 6. o.

TF12: BELLINGCAT Investigation Team: Bellingcat's attribution investigations on Crimea and MH17. Bellingcat, 2014–2015.

TF13: Egyéb OSINT / hírszerzési attribúciós elemzések – a szövegben hivatkozott konkrét forrás szerint.

TF14: CULLEN, Patrick: Hybrid threats / wicked problem keretezés – lásd 8. táblázat [TF4].

TF15: NATO STRATCOM COE és EU EEAS dokumentumok a StratCom intézményesítéséről (2015–2016).

TF16: NATO: NATO's response to hybrid threats. NATO, 2015. 8–26. o.

I (Irányítás) elem	Mi lett volna a kontroll-funkció?	Miért akadt el 2014-ben?	Következmény	Forrás
Attribúció	Állami felelősség egyértelmű kimondása	Besorolási instabilitás + bizonyossági küszöb időigénye	Késői / óvatos válasz, kész tények politikája	[TF11]; [TF12]
Evidencialánc	Auditálható bizonyítás (OSINT / leak)	Evidenciagyűjtés időigényes; utólag erősödik meg	Reakció csúszik, a legitimációs tér zár	[TF12]; [TF13]
Koordináció	Közös helyzetkép (SSOT) és válaszidő	Több szereplő, eltérő küszöbök, approval chain	Időnyereség a támadónak	[TF11]; [TF15]
Normatív / jogi küszöb	Legitim, arányos reakció	„Wicked problem": nincs kész állapot, vitatott besorolás	Halogatás, politikai óvatosság	[TF14]
Sarokpont kontroll-leltár	Minimális kontrollok azonosítása	2014-ben sok kontroll csírában; standardok később	MRM-ben „hiány–csíra–tanulás" rögzítés	[TF16]

Forrás: Saját szerkesztés [TF11]–[TF16] alapján.

12. táblázat: MRM-tábla (kontroll-leltár) – Krím 2014 sarokpont

Szint	Kontroll-terület	2014-ben állapot	Mit jelent ez Krímnél?	Forrás
Makro	Nemzetközi politikai válasz (szankciók, diplomáciai lépések)	Részben működő, de lassú	A válaszidő és a kategóriarögzítés késése csökkenti a hatást	[TF16]; [TF11]
Makro	Jogi keretezés a küszöb alatti műveletekre	Hiányos / kezdetleges	A „mi a legitim reakció?" vita megakasztja a gyors döntést	[TF14]; [TF11]
Makro	Intézményi StratCom / IO képességek (NATO / EU szinten)	Részben csíra	A Krím után válik kényszerré az intézményesítés	[TF15]; [TF16]
Makro	Platformkormányzás / transzparencia	Gyenge / hiányzó	A csatornákon futó műveleti termékek kontrollja korlátozott	[TF15]
Mezo	Kormányzati helyzetkép (SSOT), gyors elemző lánc	Hiányos / széttartó	Nincs gyors közös besorolás → approval chain lassú	[TF11]; [TF14]
Mezo	Attribúciós kapacitás (szabványok, eljárásrend)	Részben, utólag erősödik	2014-ben az attribúció gyakran evidencialáncra szorul	[TF12]; [TF13]

Szint	Kontroll-terület	2014-ben állapot	Mit jelent ez Krímnél?	Forrás
Mezo	Kommunikációs ellenműveletek / cáfolati rutin	Csíra	Nem protokollos, nem skálázott; később standardizálódik	[TF15]
Mezo	Kiber–információs koordináció	Részben működő	A művelet több domaint érint; a koordináció hiányosságai látszanak	[TF16]
Mikro	Társadalmi médiaműveltség / immunizáció	Alacsony szintű	A keretezés könnyebben rögzül, a bizonytalanság terjed	[TF14]
Mikro	Közösségi ellenállás / civil ellen-narratíva	Ad hoc	Nincs rendszerszintű „beehive" jelleg (ez később látható)	[TF15]

Forrás: Saját szerkesztés – forrásjelölések a 11. táblázattal azonosak ([TF11]–[TF16]).

13. táblázat: ANCHOR-összegző tábla

Az alábbi tábla az 5.2. szekció empirikus mérföldköveit összegzi a G–M–T–V eltolás szerint:

#	Anchor-esemény	Időszak	G–M–T–V eltolódás	Terjesztési környezet	Kulcsforrás
1	ISIS online + Telegram	2014–16	Terítés nő, Validálás nő (zárt)	Nyílt → zárt	StratCom COE 2016
2	IRA / 2016 USA választás	2016	Terítés erősen nő, Mosás nő, Validálás nő	Nyílt + hibrid	Mueller-vádirat 2018; SIO 2019
3	Brexit népszavazás	2016	Terítés nő, Validálás nő	Nyílt (feed)	OII Global Inventory 2017
4	#MacronLeaks	2017	Mosás nő, Terítés nő, Validálás nő	Hibrid (dump + social)	Vilmer 2019 (Atlantic Council)
5	Cambridge Analytica	2018	Szabályozási nyomás nő → Mosás/Terítés adaptáció nő	Nyílt + hibrid	Hybrid CoE WP 11; EU Action Plan
6	Secondary Infection	2014–19	Mosás erősen nő, Terítés nő	Hibrid (multiplatform)	DFRLab/Graphika 2019

7	Hangalapú deepfake (CEO-csalás)	2019	Validálás erősen nő (zárt)	Zárt (telefon)	WSJ 2019; Hybrid CoE TR 4
8	COVID-infodémia	2020–21	Validálás nő, Mosás nő, Terítés nő (hibrid)	Hibrid (nyílt + zárt)	Hybrid CoE WP 29; Szicherle–Krekó 2020
9	Sputnik V / vakcinadiplomácia	2021	Validálás nő, Mosás nő	Hibrid	CORE Resilience; EEAS
10	Zapad 2021 + Putyin-cikk	2021	Terítés nő, Validálás nő, Mosás nő	Teljes spektrum	Hybrid CoE WP 13 (Kalenský 2022)
11	Szurkov-levelek	2016+	Mosás nő, Ellen-validálás nő	OSINT	Royal/RUSI 2019; DFRLab
12	Vulkan-akták	2014–22	Generálás/Mosás/Terítés integráció nő	Belső szivárogtatás	Mandiant/Google Cloud 2023

14. táblázat: REZILIENCIA-összegző tábla

Kategória	Képesség / intézmény	Időpont	G–M–T–V hatás a támadóra	Kulcsforrás
EU szabályozás	Action Plan against Disinfo	2018	REG↑ → M/T adaptáció kényszere	JOIN(2018)36
EU szabályozás	Code of Practice	2018	Platform-felelősség soft-law	Hybrid CoE WP 11
EU szabályozás	EDAP + Council Conclusions	2020	Digitális szuverenitás politikai szint	EDAP (2020)
NATO/Hybrid CoE	StratCom COE Robotrolling	2019–	T mérhetősége	NATO StratCom COE 2024
NATO/Hybrid CoE	Memetic Warfare	2021	V-dimenzió doktrína	NATO StratCom COE 2021
NATO/Hybrid CoE	Elrettentés 5. hulláma	2022	3C keretrendszer	Monaghan 2022 (Hybrid CoE P12)
Platform-integritás	CIB / takedown (Meta)	2018–	M/T hálózatok feltörése	Meta CIB Reports
Platform-integritás	TAG/Jigsaw (Google)	2019–	Prebunking, state-linked ID	TAG Blog

Kategória	Képesség / intézmény	Időpont	G–M–T–V hatás a támadóra	Kulcsforrás
Akadémiai	OII Global Inventory	2017–21	T/M globális méretezés	Bradshaw & Howard
Akadémiai	SIO/Stanford (EIP)	2020	Valós idejű monitoring	Hybrid CoE WP 11
OSINT/fact-check	Bellingcat	2014–	V(ellen)↑ (forenzika)	MH17 investigation
OSINT/fact-check	EDMO	2020–21	EU fact-check koordináció	EDMO Reports
Állami gyakorlat	UK DCMS CDU + GCHQ	2019–	Online disinfo monitoring	Hybrid CoE RR 2
Állami gyakorlat	Svédország MSB	2016–	16 000 köztisztviselő képzése	Hybrid CoE RR 2
Leak-bizonyíték	Surkov-leaks / RUSI	2016	L feltörése (szervezettség bizonyítás)	Royal/RUSI (Seely 2019)
Leak-bizonyíték	Vulkan-akták	2023 (←2014–22)	G/M/T integráció feltárása	Mandiant/Google Cloud 2023

Forrás: Saját szerkesztés.

15. táblázat: Összegző Helyzet-dimenzió táblázat: 2014 kiindulási alap vs. 2022–2025 konfiguráció

Indikátor	2014 kiindulási alap (4.2.4. alapján)	2022–2025 konfiguráció
Narratív koherencia	Magas (egyetlen keretezés: „Krím hazatérése")	Alacsony→közepes (kaotikus kezdet → „war fatigue" fókusz)
Csatorna-szinkron	Háromrétegű (állami → social → mainstream visszahivatkozás)	Négyrétegű (állami → proxy / klón → zárt Telegram → fizikai szabotázs)
Volumen / amplifikáció	Kézivezérlésű trollfarm (alacsony automatizáltság)	Ipari botnet + LLM + deepfake (nagyon magas automatizáltság)
NSA-aktorok	IRA embrionális; Night Wolves	IRA→CGE, SDA / Doppelgänger, Wagner→Expeditionary Corps, TCN
Fizikai–kognitív fúzió	Nincs (szinkron, de elkülönül)	Van (szabotázs mint terítési horgony; Telegram-toborzás)

Forrás: Saját szerkesztés, a 4.2.4. alfejezet táblájának logikáját követve.

16. táblázat: FMK-rács / FMK-mátrix modalitás-összehasonlítás: 2014 vs. 2022–2025

FMK-rács cella	2014 (4. fejezet sarokpont)	2022–2025 konfiguráció
Szöveg + meggyőzés	Trollfarm posztok, kommentek	LLM-generált polimorf szövegek
Szöveg + bénítás	„Nincs itt semmi" narratíva	„Fegyver-fáradtság" keretezés
Kép + meggyőzés	Alacsony (álprofilképek)	Doppelgänger klónoldalak layoutja
Kép + bénítás	Nem releváns	Grafikus háborús tartalom
Audio + meggyőzés	Nem létező	Deepfake hangklónozás (2024)
Audio + bénítás	Nem létező	Pánik-üzenetek (szirénák, IPSO)
Video + meggyőzés	Krím „népszavazás" közvetítés	Multimodális kampányok
Video + bénítás	Nem létező	Deepfake video (Zelenszkij, 2022)
Multimodális + demobilizáció	Nem létező	„Béke" kampányok (szöveg + kép + video, több nyelven, több platform)

Forrás: Saját szerkesztés a 4.2.5. és 6.2.7. alfejezet elemzése alapján.

17. táblázat: G–M–T–V összegzés: 2014 sarokpont vs. Híd-időszak vs. 2022–2025 végállapot

Dimenzió	2014 sarokpont (4.5.2. alapján)	Híd-eltolódás (5. fejezet)	2022–2025 végállapot
G – Generálás	Manuális trollfarm (alacsony, drága)	GAN, korai GenAI (költségcsökkenés)	LLM-alapú polimorf generálás; deepfake video; hangklón (nagyon alacsony költség, végtelen variáns)
M – Mosás	Primitív álprofil (alacsony–közepes)	Perszóna-portfólió; hack-and-leak pipeline (közepes–magas)	Doppelgänger klónoldalak; SDA / CGE szervezeti háttér; „békepárti" keretezés (magas)
T – Terítés	Koordinált humán hálózat (közepes)	Algoritmus + bot + zárt csatorna (magas)	4 rétegű: állami → proxy → zárt Telegram → fizikai szabotázs
V – Validálás	Ellen-validálás nulla (a meglepetés miatt)	OSINT, tényellenőrzés, platform-transzparencia (növekvő, de lemaradó)	Pre-bunking, hírszerzési transzparencia, DISARM – de kognitív nihilizmus erodálja a V-t

Forrás: Saját szerkesztés a 4. és 5. fejezet sarokpontjainak összegzése alapján.

18. táblázat: Szintetikus média incidenstár: deepfake és MI-generált műveletek verifikált evidenciabázisa, 2022–2025

Incidens	Dátum	Modalitás	Cél / funkció	G–M–T–V fókusz	Kulcsforrás
Zelenszkij „megadás" deepfake	2022.03.16	Videó deepfake	Gyors demoralizálás, kapitulációs narratíva	V (validálás-támadás) + T (terítés)	Reuters; Euronews; TechCrunch (Meta); DFRLab
Putyin „béke" deepfake	2022.03	Videó deepfake	Ellen-propaganda, bizalomrombolás	V (validálás-támadás)	Reuters fact check; Snopes
Ghost of Kyiv (DCS játékklip)	2022.02.25 →	Szintetikus + dekontextualizálás	OSINT-zaj, morál, bizonyíték-érzet	M (mosás) + T (terítés)	Reuters; Snopes; PolitiFact
ARMA 3 felvételek inváziós footage-ként	2022.02.24 →	Szintetikus + dekontextualizálás	Vizuális bizonyíték-szennyezés	M (mosás) + T (terítés)	Reuters fact check
Klicsko deepfake videóhívások	2022.06	Videó-imperszonáció	Diplomáciai bizalomrombolás	V + T (bizalomháló)	Guardian; dig.watch; Fortune

Incidens	Dátum	Modalitás	Cél / funkció	G–M–T–V fókusz	Kulcsforrás
Zaluzsnyij deepfake (puccs-narratíva)	2023.11	Videó deepfake	Ékverés katonai–politikai vezetés között	V (validálás-támadás)	Truthmeter; DFRLab
Putyin hadiállapot broadcast	2023.06.05	Deepfake broadcast	Pánik, bizalomrombolás	V + T (terítés)	Semafor; Business Insider
France 24 deepfake (Macron-merénylet)	2024.02	Deepfake (brand-mimikri)	Ukrajna démonizálása, EU-támogatás gyengítése	M (forrás-mosás) + V	Euronews; France24 debunk
Hamis Euronews-riport (brandjacking)	2024.02–03	Hamis tévériport	Bizalomrombolás, társadalmi feszültség	M (mosás) + V	Reuters fact check
Hamis evakuációs üzenetek (Harkiv)	2024.04–05	Dokumentum-mimikri	Pánikkelés, OSINT-szennyezés	M (mosás) + T (terítés)	Reuters
Danilov deepfake (Crocus City Hall)	2024.03.22	Deepfake (MI-hang + vágás)	Felelősség-átterelés, düh-mobilizálás	V + M	Ukrainska Pravda; KHPG

Incidens	Dátum	Modalitás	Cél / funkció	G–M–T–V fókusz	Kulcsforrás
Kuleba deepfake videóhívás (US szenátor)	2024.09	Videó deepfake	Info-kiszívás, diszkreditálás	V + T	AP; Guardian; Kyiv Independent
MI-generált „síró katonák" hullám	2025.01	Videó deepfake	Demoralizálás, „Ukrajna összeomlik"	V + T	AFP fact check; Ukrán CPD / CCD

Forrás: Saját szerkesztés – nyílt forrású tényellenőrző és kutatóintézeti közlemények alapján (Reuters, DFRLab, AFP, Snopes, Bellingcat, Ukrán CPD).

19. táblázat: I-tábla (összegző) – Irányítás dimenzió, 2014 vs. 2022–2025

Kontroll-terület	2014 (4. fejezet)	2022–2025
Attribúciós küszöb	Magas (hosszú bizonyítási lánc szükséges)	Alacsony (hírszerzési transzparencia, proaktív leplezés)
Reakciókockázat	Magas (szankciók félő, NATO-egység bizonytalan)	Alacsonyabb (szankciós egység megteremtve, RT/Sputnik tiltás)
Koordináció/jóváhagyás	Lassú (nincs protokoll)	Gyorsabb (DSA keretrendszer, DISARM TTP-standard, CIB-audit)
Humor/mém-védekezés	Nem létezik	NAFO, ukrán MFA StratCom
Előzetes leleplezés	Nem létezik	2022 februári pre-bunking modell
Platform-transzparencia	Nulla	CIB-jelentések, audit-kötelezettség, DSA (2024-től élesben)

Forrás: Saját szerkesztés a 4.4.5 logikáját követve.

20. táblázat: MRM-tábla (kontroll-leltár) – 2022–2025 (6.5.1. alfejezet)

Szint	Kontroll-terület	2022–2025 állapot	Hol van rés?	Forrás
Makro	Nemzetközi politikai válasz	Erős (gyors szankciók, EU egységes, NATO bővítés: FI/SE)	Szankciós fáradtság, a kijátszás nő	Monaghan 2022 (HCoE P12)
Makro	Jogi keretezés (platform-szabályozás)	DSA + RT/Sputnik tiltás + FIMI-definíció az EEAS-ban	VPN-megkerülés, végrehajtási kapacitás	Bertram–Monsees 2024
Makro	Intézményi StratCom / IO képességek	NATO StratCom COE, Hybrid CoE, EEAS FIMI-jelentések	Nemzeti szintű kapacitások egyenetlenek	NATO SC COE 2024
Makro	Platformkormányzás	CIB-audit (Meta), DSA-audit (VLOPs)	Telegram, TikTok részben kívül	Robotrolling 2024
Mezo	Kormányzati helyzetkép	SSOT-jellegű rendszerek (ukrán monitoring-ökoszisztéma modell)	Nem minden országban van kapacitás	Kalenský et al. 2024
Mezo	Attribúciós kapacitás	Valós idejű (Bellingcat, DFRLab, TAG, DISARM-standard)	Az LLM-generált tartalom attribúciója új kihívás	Newman 2022 (HCoE RR7)

Szint	Kontroll-terület	2022–2025 állapot	Hol van rés?	Forrás
Mezo	Kommunikációs ellenműveletek	Pre-bunking modell (2022 USA), NAFO, ukrán MFA StratCom	Reaktív módban a legtöbb EU-tagállam	Kalenský et al. 2024
Mezo	Kiber–információs koordináció	Javuló (NATO CCDCOE, EU CyberNet)	A fizikai–kognitív fúzió új koordinációs kihívás	HCoE P15 (2022)
Mikro	Társadalmi médiaműveltség	Javuló (médiaműveltség programok EU-szerte), de egyenetlen	Kognitív fáradtság erodálja az ellenállóképességet	Lebrun 2023 (HCoE SA33)
Mikro	Közösségi ellenállás / civil ellen-narratíva	Erős (ukrán modell: önkéntesek, NAFO, tényellenőrzők)	Transzferálhatóság más országokba kérdéses	Kalenský et al. 2024

Forrás: Saját szerkesztés a 4.5.1 logikáját követvi

21. táblázat: A kognitív hadviselés dimenzióinak összehasonlító mutatói (2014 vs. 2025)

H–E–I Dimenzió	Indikátor	2014: sarokpont (Kézműves)	2022–2025: Eszkaláció (Iparosított)	Stratégiai Trend
HELYZET (Input)	Műveleti volumen	Alacsony (Manuális trollfarmok, IRA)	Extrém magas (AutoGenAI, LLM-botnetek)	Mennyiségi robbanás
	Tartalom jellege	Koherens mesternarratívák	Szintetikus tartalom, narratív káosz	Minőségi hígulás
ELŐREJELZÉS (Process)	Döntési sebesség	Alacsony (Reaktív bénultság)	Magas (Kognitív immunizáció, pre-bunking)	Dinamikai fölényváltás
	Pszichológiai állapot	Sokk és paralízis	Kognitív fáradtság, nihilizmus	Érzelmi felőrlés
IRÁNYÍTÁS (Control)	Szabályozási szint	Vákuum (Laissez-faire)	Intézményesült (DSA, DISARM, RESIST)	Jogi konszolidáció
	Védelmi architektúra	Ad-hoc cáfolás (Debunking)	Többrétegű védelem, Pre-bunking	Proaktív elhárítás

Forrás: Saját szerkesztés a NATO StratCom COE (2024: Virtual Manipulation Brief; 2025: Countering Information Influence Operations (IIO) in the Nordic-Baltic Region), a Hybrid CoE (VOLĀNS et al. 2025) és az EEAS (2024: 2nd Report on FIMI Threats) adatai alapján.

BIBLIOGRÁFIA ÉS IRODALOMJEGYZÉK

Adamsky, Dmitry (2015): Cross-Domain Coercion: The Current Russian Art of Strategy. Proliferation Papers, No. 54. IFRI, Párizs. Online: https://www.ifri.org/sites/default/files/migrated_files/documents/atoms/files/pp54adamsky.pdf

Agarwal, N. – Bandeli, K. – Bertolin, G. – Biteniece, N. – Sedova, K. (2017): Digital Hydra: Security Implications of False Information Online. NATO STRATCOM COE, Riga.

AI in Defence of Ukraine (2024): Policy Brief. International Centre for Defence and Security, Tallinn.

Allenby, Brad (2017): White Paper on Weaponized Narrative. Center on the Future of War, Arizona State University.

Allenby, Brad – Garreau, Joel (2017): Weaponized Narrative: The New Battlespace. Center on the Future of War, Arizona State University. Online: https://weaponizednarrative.asu.edu/publications

Andrews, James R. (1969): Confrontation at Columbia: A case study in coercive rhetoric. Quarterly Journal of Speech, 55(1), 9–16. DOI: 10.1080/00335636909382923

Aro, Jessikka (2016): The Cyberspace War: Propaganda and Trolling as Warfare Tools. European View, 15(1), 121–132. DOI: 10.1007/s12290-016-0395-5

Atkinson, Richard C. – Shiffrin, Richard M. (1968): Human memory: A proposed system and its control processes. In Spence, K. W. – Spence, J. T. (szerk.): The Psychology of Learning and Motivation (Vol. 2). Academic Press, New York. 89–195.

Attias, Shay (2024): Hybrid Warfare and Informational Strategies: Russia's Campaign in Ukraine (2014). In Jobbágy, Z. – Zsigmond, E. (szerk.): Hybrid Warfare Reference Curriculum, Volume II. Ludovika, Budapest. 238–239.

Bakir, Vian – Herring, Eric – Miller, David – Robinson, Piers (2019): Organized Persuasive Communication: A new conceptual framework for research on public relations, propaganda and promotional culture. Critical Sociology, 45(3), 311–328. DOI: 10.1177/0896920518764586

Balint et al. (2022): Effectiveness of the Sanctions on Russian State-Affiliated Media in the EU: An Investigation into Website Traffic and Possible Circumvention Methods. ISD Global, London.

Bányász Péter – Szádeczky Tamás – Váczi Kincső B. (2024): The relationship between generative artificial intelligence and cybersecurity. In CEEeGov 2024. ACM, New York. DOI: 10.1145/3670243.3670781

Bányász Péter et al. (2025): The resilience of social media users against Generative AI-based visual manipulation: A survey among Hungarian Facebook users. In CEEeGov 2025. ACM, New York. 181–188. Online: https://doi.org/10.1145/3773002.3774813

Barocas, Solon – Selbst, Andrew D. (2016): Big Data's Disparate Impact. California Law Review, 104(3), 671–732. DOI: 10.15779/Z38BG31

Bay, Sebastian (szerk.) (2021): Messaging Manipulation Services on Social Messaging Platforms. NATO STRATCOM COE, Riga.

Bay, Sebastian – Biteniece, Nora (2019): The Current Digital Arena and its Risks to Serving Military Personnel. In Bertolin, Giorgio (szerk.): Responding to Cognitive Security Challenges. NATO STRATCOM COE, Riga.

Bay, Sebastian et al. (2022): Social Media Manipulation 2021/2022: Assessing the Ability of Social Media Companies to Combat Platform Manipulation. NATO STRATCOM COE, Riga.

Beccaro, Andrea (2024): The Evolution of Hybrid Warfare. In Jobbágy, Z. – Zsigmond, E. (szerk.): Hybrid Warfare Reference Curriculum, Volume III. Ludovika, Budapest. 87–90.

Bellingcat Investigation Team (2015): MH17 – The Open Source Evidence. Online: https://www.bellingcat.com/news/uk-and-europe/2015/10/08/mh17-the-open-source-evidence/

Bene Márton (2017): Go Viral on the Facebook! Information, Communication & Society, 20(4), 513–529. DOI: 10.1080/1369118X.2016.1198411

Bennett, W. Lance – Segerberg, Alexandra (2012): The Logic of Connective Action: Digital Media and the Personalization of Contentious Politics. Information, Communication & Society, 15(5), 739–768. DOI: 10.1080/1369118X.2012.670661

Bergmanis-Korāts, Gundars – Vecmanis, Raitis Ralfs – Isupova, Marija – Sakurai, Kensho (2025): Virtual Manipulation Brief 2025. NATO STRATCOM COE, Riga.

Bernal, Paul (2021): Misunderstanding Misinformation: why most 'fake news' regulation is doomed to failure. British Association of Comparative Law.

Bernays, Edward (1923/2019): Crystallizing Public Opinion. Dover Publications, New York.

Bertolin, Giorgio (szerk.) (2019): Responding to Cognitive Security Challenges. NATO STRATCOM COE, Riga.

Bolt, Neville (2025): The NextGen Information Environment. NATO STRATCOM COE, Riga.

Bolt, Neville – Fridman, Ofer – Winter, Charlie et al. (2023): Kremlin Communication Strategy for Russian Audiences Before and After the Full-Scale Invasion of Ukraine. NATO STRATCOM COE, Riga.

Bradshaw, Samantha – Howard, Philip N. (2017): Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation. Working Paper 2017.12. Oxford Internet Institute, Oxford.

Bradshaw, Samantha – Howard, Philip N. (2018): Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation. Working Paper 2018.1. Oxford Internet Institute, Oxford.

Bradshaw, Samantha – Howard, Philip N. (2019): The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation. Working Paper 2019.2. Oxford Internet Institute, Oxford.

Bradshaw, Samantha – Bailey, Hannah – Howard, Philip N. (2021): Industrialized Disinformation: 2020 Global Inventory of Organized Social Media Manipulation. Working Paper 2021.1. Oxford Internet Institute, Oxford.

Broadbent, Donald E. (1958): Perception and Communication. Pergamon Press, London.

Brunvand, Jan Harold (1981): The Vanishing Hitchhiker: American Urban Legends and Their Meanings. W. W. Norton, New York.

Byman, Daniel L. – Gao, Chongyang – Meserole, Chris – Subrahmanian, V. S. (2023): Deepfakes and International Conflict. Foreign Policy at Brookings.

Cadwalladr, Carole – Graham-Harrison, Emma (2018): Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach. The Guardian, 2018. március 17.

Camargo Lima, Raphael (2019): China's and Russia's Grand Strategies: Comparing the Role of Strategic Communications. Defence Strategic Communications, Vol. 6, 83–115. DOI: 10.30966/2018.RIGA.6.3. CCDH (2024): Failure to Protect: How X's Community Notes fail to address antisemitism and disinformation. CCDH Report, Washington D.C. – London.

CDC (2019): Psychology of a Crisis. CERC Manual, 2019 Update. Centers for Disease Control and Prevention.

Center for an Informed Public – Digital Forensic Research Lab – Graphika – Stanford Internet Observatory (2021): The Long Fuse: Misinformation and the 2020 Election. Election Integrity Partnership, Stanford.

Chadwick, Andrew (2013): The Hybrid Media System: Politics and Power. Oxford University Press, Oxford.

Chen, Adrian (2015): The Agency. The New York Times Magazine, 2015. június 7. Online: https://www.nytimes.com/2015/06/07/magazine/the-agency.html

Chesney, Robert – Citron, Danielle (2019): Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. California Law Review, 107. évf. 1753–1820. DOI: 10.15779/Z38RV0D15J

Claverie, Bernard – Du Cluzel, François (2022): The Cognitive Warfare Concept. In Claverie, Bernard et al. (szerk.): Cognitive Warfare: The Future of Cognitive Dominance. NATO Collaboration Support Office.

Clausewitz, Carl von (1961–1962) [1832]: A háborúról I–II. Ford. Dr. Réczey Ferenc. Zrínyi Katonai Könyv- és Lapkiadó, Budapest.

Colley, Thomas – Granelli, Francesca – Althuis, Jente (2020): Disinformation's Societal Impact: Britain, Covid, and Beyond. Defence Strategic Communications, Vol. 8, 89–140. DOI: 10.30966/2018.RIGA.8.3

Cresswell, Kathrin M. – Worth, Allison – Sheikh, Aziz (2010): Actor-Network Theory and its role in understanding the implementation of information technology developments in healthcare. BMC Medical Informatics and Decision Making, 10(67). DOI: 10.1186/1472-6947-10-67

Csepeli György (1997): Szociálpszichológia. Osiris, Budapest.

Csiki Varga Tamás – Tálas Péter (2022): Megerősített elrettentés és védelem. SVKI Elemzések, 2022/8.

Cullen, Patrick (2018): Hybrid threats as a new „wicked problem" for early warning. Hybrid CoE Strategic Analysis 8. European Centre of Excellence for Countering Hybrid Threats, Helsinki.

Dami, Lorenzo (2022): Analysis and Conceptualization of Deepfake Technology as Cyber Threat. Research Paper, University of Florence, School of Political Science „Cesare Alfieri".

Darczewska, Jolanta (2014): The Anatomy of Russian Information Warfare: The Crimean Operation, A Case Study. OSW Point of View, 42. Centre for Eastern Studies, Warsaw. Online: https://www.osw.waw.pl/sites/default/files/the_anatomy_of_russian_information_warfare.pdf

Daukšas, Vytautas et al. (2024): War on All Fronts: Russia's Television and Online Warfare Against Ukraine. NATO STRATCOM COE, Riga.

DFRLab (Toler, Aric et al.) (2016): Breaking Down the Surkov Leaks. Atlantic Council – DFRLab. Online: https://medium.com/dfrlab/breaking-down-the-surkov-leaks-b2feec1423cb

Dolan, Andrew (2024): Hybrid Warfare and Strategic Surprise. In Jobbágy, Z. – Zsigmond, E. (szerk.): Hybrid Warfare Reference Curriculum, Volume III. Ludovika, Budapest. 169.

EEAS (2024): 2nd Report on Foreign Information Manipulation and Interference Threats. Brussels.

Eliot, Lance B. (2024): Generative AI Uses Subliminal Messaging For Shadowy Persuasion. Forbes, 2024. október 20.

Ellul, Jacques (1965): Propaganda: The Formation of Men's Attitudes. Vintage Books, New York.

Entman, Robert M. (1993): Framing: Toward Clarification of a Fractured Paradigm. Journal of Communication, 43(4), 51–58. DOI: 10.1111/j.1460-2466.1993.tb01304.x

European Digital Media Observatory (EDMO) (2022): Coordinated Information Operations in the Context of the War in Ukraine. EDMO Task Force Report.

Európai Bizottság – Az Unió külügyi és biztonságpolitikai főképviselője (2016): Joint Framework on countering hybrid threats. JOIN(2016) 18 final. Brüsszel, 2016. április 6.

Európai Bizottság (2018a): Cselekvési terv a félretájékoztatással szemben [Action Plan against Disinformation]. JOIN(2018) 36 final, Brüsszel. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52018JC0036

Európai Bizottság (2018b): Code of Practice on Disinformation. Brüsszel, 2018. szeptember 26. Online: https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation

Európai Bizottság (2020): Seventh Progress Report on the implementation of the EU regulatory framework for electronic communications. Brüsszel.

Az Európai Unió Tanácsa – Az Európai Parlament (2022): (EU) 2022/2065 rendelet a digitális szolgáltatások egységes piacáról (Digitális Szolgáltatásokról szóló Rendelet). Az EU Hivatalos Lapja, L 277, 2022. október 27. Online: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:32022R2065

Falk, Barbara J. (2020): Strategic citizens: Civil society as a battlespace in the era of hybrid threats. Hybrid CoE Strategic Analysis 25. European Centre of Excellence for Countering Hybrid Threats, Helsinki.

Farwell, James P. (2019): War and Truth. Defence Strategic Communications, Vol. 7, 133–145. DOI: 10.30966/2018.RIGA.7.5

Fauconnier, Gilles (1997): Mappings in Thought and Language. Cambridge University Press, Cambridge.

Fauconnier, Gilles – Turner, Mark (2002): The Way We Think: Conceptual Blending and the Mind's Hidden Complexities. Basic Books, New York.

Fauconnier, Gilles – Turner, Mark (2003): Conceptual Blending, Form and Meaning. Recherches en communication, 19. sz. 57–86. Online: https://tecfa.unige.ch/tecfa/maltt/cofor-1/textes/Fauconnier-Turner03.pdf

Fisher, Lucy – Smyth, Chris (2020): GCHQ in cyberwar on anti-vaccine propaganda. The Times, 2020. november 9.

Frankfurt, Harry G. (2005): On Bullshit. Princeton University Press, Princeton.

Fredheim, Rolf (2024): Virtual Manipulation Brief 2024/1: Hijacking Reality – The Increased Role of Generative AI in Russian Propaganda. NATO STRATCOM COE, Riga. Online: https://stratcomcoe.org/publications/virtual-manipulation-brief-20241-hijacking-reality-the-increased-role-of-generative-ai-in-russian-propaganda/307

Freedman, Lawrence (2019): Ukraine and the Art of Strategy. Oxford University Press, New York.

Friedman, Batya – Nissenbaum, Helen (1996): Bias in computer systems. ACM Transactions on Information Systems, 14(3), 330–347. DOI: 10.1145/230538.230561

Gallagher et al. (2019): Integratív komplexitás-csökkenés mérése az orosz dezinformációs tartalomban. [Teljes bibliográfiai adat nem azonosítható.]

Garcia-Camargo, Isabella – Bradshaw, Samantha (2021): Disinformation 2.0: Trends for 2021 and beyond. Hybrid CoE Working Paper 11. European Centre of Excellence for Countering Hybrid Threats, Helsinki. Online: https://www.hybridcoe.fi/wp-content/uploads/2021/07/20210716_Hybrid_CoE_Working_Paper_11_Disinfo_2_0_WEB.pdf

George, Alexander L. – Bennett, Andrew (2005): Case Studies and Theory Development in the Social Sciences. MIT Press, Cambridge, MA.

Gerasimov, Valery (2016): The Value of Science Is in the Foresight: New Challenges Demand Rethinking the Forms and Methods of Carrying out Combat Operations. Ford. Robert Coalson. [Eredeti: Voyenno-Promyshlennyy Kurier, 2013. február 26.] Military Review, January–February 2016, 23–29. Online: https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20160228_art008.pdf

Giannopoulos, Georgios – Smith, Hanna – Theocharidou, Marianthi (2021): The Landscape of Hybrid Threats: A Conceptual Model. JRC Technical Report. European Commission – Hybrid CoE. Online: https://www.hybridcoe.fi/publications/the-landscape-of-hybrid-threats-a-conceptual-model/

Giesea, Jeff (2016): It's Time to Embrace Memetic Warfare. Defence Strategic Communications, Vol. 1, 67–75. Online: https://stratcomcoe.org/publications/its-time-to-embrace-memetic-warfare/164

Giles, Keir (2016): Russia's „New" Tools for Confronting the West: Continuity and Innovation in Moscow's Exercise of Power. Chatham House, London. Online: https://www.chathamhouse.org/2016/03/russias-new-tools-confronting-west

Giles, Keir (2023): Humour in online information warfare: Case study on Russia's war on Ukraine. Hybrid CoE Working Paper 26. European Centre of Excellence for Countering Hybrid Threats, Helsinki. Online: https://www.hybridcoe.fi/wp-content/uploads/2023/11/20231106HybridCoEWorkingPaper26HumortocombatdisinformationWEB.pdf

Gillespie, Tarleton (2018): Custodians of the Internet. Yale University Press, New Haven.

Gleicher, Nathaniel et al. (2021): The State of Influence Operations 2017–2020. Facebook. Online: https://about.fb.com/news/2021/05/influence-operations-threat-report/

Golebiewski, Michael – Boyd, danah (2018): Data Voids: Where Missing Data Can Easily Be Exploited. Data & Society Research Institute.

Goncharuk, Vitaliy (2024): Artificial Intelligence in Defence of Ukraine. Russia's War in Ukraine Brief 6. International Centre for Defence and Security, Tallinn. Online: https://icds.ee/wp-content/uploads/dlm_uploads/2024/09/Layout-AI-in-Defence-of-Ukraine.pdf

Google Threat Analysis Group – Mandiant – Google Trust & Safety (2023): Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape. Google.

Grizāne, Anna – Isupova, Marija – Vorteil, Vanessa (2022): Social Media Monitoring Tools: An In-Depth Look. NATO STRATCOM COE, Riga.

Haig Zsolt (2018): Információs műveletek a kibertérben. Dialóg Campus, Budapest.

Haiduchyk, Tetiana – Khusnutdinov, Marat – Belafatti, Fabio – Kubś, Jakub – Šuminas, Andrius – Bergmanis-Korāts, Gundars (2025): Impact of the Digital Services Act: A Facebook Case Study. NATO STRATCOM COE, Riga.

Hanley, Monika – Kuzichkin, Andrey (2021): Russian Media Landscape: Structures, Mechanisms, and Technologies of Information Operations. NATO STRATCOM COE, Riga.

Heap, Ben (szerk.) (2021): Strategic Communications Hybrid Threats Toolkit. NATO STRATCOM COE, Riga.

Hedling, Elsa (2025): Social Identities and Democratic Vulnerabilities: Learning from Examples of Targeted Disinformation. Hybrid CoE Paper 24. European Centre of Excellence for Countering Hybrid Threats, Helsinki. Online: https://www.hybridcoe.fi/wp-content/uploads/2025/04/20250415Hybrid_CoE_Paper24WEB.pdf

Hellman, Maria – Wagnsson, Charlotte (2017): How can European States Respond to Russian Information Warfare? An Analytical Framework. European Security, 26(2), 153–170. DOI: 10.1080/09662839.2017.1294162

Henley, Jon (2021): Influencers say Russia-linked PR agency asked them to disparage Pfizer vaccine. The Guardian, 2021. május 25.

Hertwig, Ralph et al. (2004): Decisions from Experience and the Effect of Rare Events in Risky Choice. Psychological Science, 15(8), 534–539. DOI: 10.1111/j.0956-7976.2004.00715.x

Hoogensen Gjørv, Gunhild – Jalonen, Outi (2023): Identity as a tool for disinformation: Exploiting social divisions in modern societies. Hybrid CoE Strategic Analysis 34. European Centre of Excellence for Countering Hybrid Threats, Helsinki.

Horváth Dávid (2022): Pandemic and Infodemic – Which One Is More Dangerous? Acta Universitatis Sapientiae Communicatio, 9(1), 125–139. DOI: 10.2478/auscom-2022-0009

Horváth Dávid (2024): A mesterséges intelligencia által generált dezinformáció (AutoGenAI) hatása a kognitív hadviselés hatékonyságára. Hadtudomány, 34(2), 112–134.

Horváth Dávid (2025a): Communication Classified as a Weapon and Generative Artificial Intelligence as Information Overload: Situation–Forecast–Control (S–F–C) Indicators and Multimodal Resilience Matrix in the OxIPO Model. OxIPO – Interdiszciplináris tudományos folyóirat, 7(4), 23–48. DOI: 10.35405/OXIPO.2025.4.23. Online: https://real.mtak.hu/231340/

Horváth Dávid (2025b): When Artificial Intelligence Generated Content Becomes Weapon-Grade Communication. Mesterséges Intelligencia – interdiszciplináris folyóirat, 7(2), 77–98. DOI: 10.35406/MI.2025.2.77. Online: https://real.mtak.hu/231448/

Horváth Dávid (2025c): Communication Classified as a Weapon and Generative AI as Information Overload: S–F–C Indicators and MRM. Defence and Strategy, 25(1).

Howard, Philip N. – Kollanyi, Bence (2016): Bots, #StrongerIn, and #Brexit: Computational Propaganda during the UK-EU Referendum. Oxford Internet Institute, Oxford.

Hoyle, Aiden – van den Berg, Helma – Doosje, Bertjan – Kitzen, Martijn (2021): Grey Matters: Advancing a Psychological Effects-Based Approach to Countering Malign Information Influence. New Perspectives, 29(2), 144–164. DOI: 10.1177/2336825X21995702

Hoyle, Aiden – Pijpers, Peter B. M. J. (2022): Stemming the Narrative Flow: The Legal and Psychological Grounding for the European Union's Ban on Russian State-Sponsored Media. Defence Strategic Communications, Vol. 11, 51–80. DOI: 10.30966/2018.RIGA.11.2

Hoyle, Aiden et al. (2023a): Cognitive and Emotional Responses to Russian State-Sponsored Media Narratives in International Audiences. Journal of Media Psychology (advance online). DOI: 10.1027/1864-1105/a000371

Hoyle, Aiden et al. (2023b): Life through Grey-Tinted Glasses: How Do Audiences in Latvia Psychologically Respond to Sputnik Latvia's Destruction Narratives? Post-Soviet Affairs, 40(1), 1–18. DOI: 10.1080/1060586X.2023.2275507

Hoyle, Aiden – Šlerka, Josef (2024): Cause for concern: The continuing success and impact of Kremlin disinformation campaigns. Hybrid CoE Working Paper 29. European Centre of Excellence for Countering Hybrid Threats, Helsinki.

Human Firewall Council (2003): The Alarming State of Security Management Practices Among Organizations Worldwide. Security Management Index.

Hybrid CoE (2020): Trends in the Contemporary Information Environment. Hybrid CoE Trend Report 4. European Centre of Excellence for Countering Hybrid Threats, Helsinki. Online: https://www.hybridcoe.fi/wp-content/uploads/2020/07/Hybrid-CoE-Trend-Report-4.pdf

Hybrid CoE (2023): Threat potential in the economy: from vulnerabilities to China's increased coercion. Hybrid CoE Trend Report 10. Helsinki.

Hybrid CoE (2024): Countering Hybrid Threats in the Age of Generative AI. Hybrid CoE Strategic Analysis 12. Helsinki.

InfocomJournal (2025): Szemantikai mezők időbeli torzulásának mérése dinamikus szóbeágyazási modellekkel (Word2Vec) a COVID-19 közösségimédia-tartalmakban. [Teljes bibliográfiai adat nem azonosítható.]

International Fact-Checking Network (2015–): IFCN Code of Principles. Poynter Institute. Online: https://www.ifcncodeofprinciples.poynter.org/

Jeangène Vilmer, Jean-Baptiste (2019): The „Macron Leaks" Operation: A Post-Mortem. Atlantic Council – IRSEM, Washington D.C. Online: https://www.atlanticcouncil.org/wp-content/uploads/2019/06/The_Macron_Leaks_Operation-A_Post-Mortem.pdf

Jeangène Vilmer, Jean-Baptiste (2021): Effective State Practices Against Disinformation: Four Country Case Studies. Hybrid CoE Research Report 2. European Centre of Excellence for Countering Hybrid Threats, Helsinki. Online: https://www.hybridcoe.fi/wp-content/uploads/2021/07/20210709_Hybrid_CoE_Research_Report_2_Effective_state_practices_against_disinformation_WEB.pdf

Jigsaw (2024): The Science of Prebunking: Resilience against Manipulation. Google Jigsaw Research Reports.

Jokinen, Janne – Normark, Magnus – Fredholm, Michael (2022): Hybrid threats from non-state actors: A taxonomy. Hybrid CoE Research Report 6. European Centre of Excellence for Countering Hybrid Threats, Helsinki.

Jowett, Garth S. – O'Donnell, Victoria (2011): Propaganda and Persuasion. 5. kiadás. SAGE Publications, London.

Juršėnas, Aistis – Karlauskas, Karolis – Ledinauskas, Edgaras – Maskeliūnas, Gytis – Ruseckas, Julius (2021): The Double-Edged Sword of AI: Enabler of Disinformation. NATO STRATCOM COE, Riga.

Juršėnas et al. (2022): The Role of AI in the Battle Against Disinformation. NATO STRATCOM COE, Riga.

Juurvee, Ivo (2018): The resurrection of 'active measures': Intelligence services as a part of Russia's influencing toolbox. Hybrid CoE Strategic Analysis 7. European Centre of Excellence for Countering Hybrid Threats, Helsinki.

Kahneman, Daniel (2013): Gyors és lassú gondolkodás. Ford. Bányász Réka – Garai Attila. HVG Könyvek, Budapest.

Kalenský, Jakub (2022): The Kremlin's Messaging on Ukraine: Authorities and „Media" Hand in Hand. Hybrid CoE Working Paper 13. European Centre of Excellence for Countering Hybrid Threats, Helsinki. Online: https://www.hybridcoe.fi/wp-content/uploads/2022/01/20220131-Hybrid-CoE-WP-13-Kremlins-messaging-on-Ukraine-WEB.pdf

Kalenský, Jakub – Hanhijärvi, Heidi (2025): Countering Disinformation in the Euro-Atlantic: Strengths and Gaps. Hybrid CoE Research Report 15. European Centre of Excellence for Countering Hybrid Threats, Helsinki.

Kalenský, Jakub – Osadchuk, Roman (2024): How Ukraine fights Russian disinformation: Beehive vs mammoth. Hybrid CoE Research Report 11. European Centre of Excellence for Countering Hybrid Threats, Helsinki. Online: https://www.hybridcoe.fi/wp-content/uploads/2024/01/20240124-Hybrid-CoE-Research-Report-11-How-UKR-fights-RUS-disinfo-WEB.pdf

Kelly, Paul (2016): Decoding Crimea. NATO STRATCOM COE, Riga.

Keršanskas, Vytautas (2021): Deterring disinformation? Lessons from Lithuania's countermeasures since 2014. Hybrid CoE Paper 6. European Centre of Excellence for Countering Hybrid Threats, Helsinki.

Kiss Álmos Péter (2021): A NATO válasza a hibrid fenyegetésre. Honvédségi Szemle, 149(3), 13–28. Online: https://real.mtak.hu/127225/1/KissAlmosPeter.pdf

Kiss Álmos Péter (2024): Az orosz–ukrán háború céljait támogató orosz stratégiai kommunikáció. Honvédségi Szemle, 152(2), 19–34. Online: https://real.mtak.hu/213496/1/003_KissAlmosPeter_19-34.pdf

Klein, Margarete (2022): Russia's military buildup along Ukraine's border: What to expect? Hybrid CoE Strategic Analysis 31. European Centre of Excellence for Countering Hybrid Threats, Helsinki.

Kofman, Michael – Rojansky, Matthew (2015): A Closer Look at Russia's „Hybrid War". Kennan Cable, No. 7. Wilson Center, Washington D.C. Online: https://www.wilsoncenter.org/publication/kennan-cable-no7-closer-look-russias-hybrid-war

Kovács László (2020): A kiberbiztonság és a kiberműveletek megjelenése Magyarország új Nemzeti Biztonsági Stratégiájában. Hadtudományi Szemle, 13(5), 3–18. DOI: 10.35926/HSZ.2020.5.1

Kovács László (2023): Hadviselés a 21. században: kiber műveletek. Ludovika, Budapest.

Krasznay Csaba (2023): A kiber- és kognitív műveletek konvergenciája az orosz–ukrán háborúban. Felderítő Szemle, 22(4), 15–32.

Kriel, Charles – Pavliuc, Alexa (2019): Reverse Engineering Russian Internet Research Agency Tactics through Network Analysis. Defence Strategic Communications, Vol. 6. NATO STRATCOM COE, Riga. DOI: 10.30966/2018.RIGA.6.6. Online: https://stratcomcoe.org/publications/reverse-engineering-russian-internet-research-agency-tactics-through-network-analysis/94/

Krulak, Charles C. (1999): The Strategic Corporal: Leadership in the Three Block War. Marines Magazine.

Kubica, Lucjan (2024): Ukraine's Position in Russia's Strategic Thinking: Domestic, Regional and International Order. Hybrid CoE Paper 20. European Centre of Excellence for Countering Hybrid Threats, Helsinki.

Kubs, Jakub – Michalowska, Aleksandra – Daukšas, Viktoras (2023): Phantom Pillars of Pro-Kremlin Disinformation. In Bolt, Neville et al. (szerk.): Kremlin Communication Strategy for Russian Audiences Before and After the Full-Scale Invasion of Ukraine. NATO STRATCOM COE, Riga. 125–137.

Laity, Mark (2021): The Birth and Coming of Age of NATO StratCom: A Personal History. Defence Strategic Communications, Vol. 10, 21–76. DOI: 10.30966/2018.RIGA.10.1

Lange-Ionatamišvili, Sanda et al. (2015): Analysis of Russia's Information Campaign against Ukraine. NATO STRATCOM COE, Riga.

Lange-Ionatamišvili et al. (2026): Countering Information Influence Operations in the Nordic-Baltic Region. NATO STRATCOM COE, Riga.

Latour, Bruno (2005): Reassembling the Social: An Introduction to Actor-Network-Theory. Oxford University Press, Oxford.

Lauder, Matthew (2024): The Rise and Fall of the Wagner Group. Hybrid CoE Working Paper 33. European Centre of Excellence for Countering Hybrid Threats, Helsinki.

Lebrun, Maxime (2023a): Anticipating cognitive intrusions: Framing the phenomenon. Hybrid CoE Strategic Analysis 33. European Centre of Excellence for Countering Hybrid Threats, Helsinki. Online: https://www.hybridcoe.fi/wp-content/uploads/2023/07/20230703HybridCoEStrategicAnalysis33CognitiveintrusionWEB.pdf

Lebrun, Maxime (2023b): Watching out for populism: Authoritarian logics as a vulnerability to hybrid threat activity. Hybrid CoE Working Paper 22. European Centre of Excellence for

Countering Hybrid Threats, Helsinki. Online: https://www.hybridcoe.fi/wp-content/uploads/2023/01/20230123HybridCoEWorkingPaper22PopulismWEB.pdf

Lefebvre, Vladimir A. (1967): Conflicting Structures. Soviet Radio, Moszkva.

Lewandowsky, Stephan – Ecker, Ullrich K. H. – Seifert, Colleen M. – Schwarz, Norbert – Cook, John (2012): Misinformation and Its Correction: Continued Influence and Successful Debiasing. Psychological Science in the Public Interest, 13(3), 106–131. DOI: 10.1177/1529100612451018

Lewandowsky, Stephan – van der Linden, Sander (2021): Countering Misinformation and Fake News Through Inoculation and Prebunking. European Review of Social Psychology, 32(2), 348–384. DOI: 10.1080/10463283.2021.1876983

Lindbom, Hanna (2022): Capability Assessment for StratCom. NATO STRATCOM COE, Riga.

Lindsey, Peter H. – Norman, Donald A. (1977): Human Information Processing. Academic Press, New York.

Mandiant (2023): Cyber Operations and Disinformation: Analysis of NTC Vulkan Projects Scan, Amesit, and Krystal-2B. Google Cloud – Mandiant, 2023. március 30.

Mappes, Grace et al. (2024): Russian Offensive Campaign Assessment, August 25, 2024. Institute for the Study of War, Washington D.C.

Marcellino, William – Beauchamp-Mustafaga, Nathan – Kerrigan, Amanda – Navarre Chao, Lev – Smith, Jackson (2023): The Rise of Generative AI and the Coming Era of Social Media Manipulation 3.0. RAND Corporation, PE-A2679-1.

Marinov Iván (2019): Városi legendák: Mik azok, és miért hiszünk nekük? Urbanlegends.hu, 2019. február 11.

Mazzucchi, Nicolas (2022): AI-based Technologies and Their Use as a Weapon of Hybrid Warfare. Hybrid CoE Paper 14. European Centre of Excellence for Countering Hybrid Threats, Helsinki.

Medvegyev, Dmitrij (2021): Pourquoi les contacts avec la direction ukrainienne actuelle sont inutiles. Kommersant, 2021. október 11.

Mező Ferenc – Mező Katalin (2019): Az OxIPO-modell – az interdiszciplináris kutatások egy lehetséges értelmezési kerete. OxIPO – interdiszciplináris tudományos folyóirat, 2019(1), 9–21. DOI: 10.35405/OXIPO.2019.1.9

Miller, George A. (1956): The Magical Number Seven, Plus or Minus Two: Some Limits on Our Capacity for Processing Information. Psychological Review, 63(2), 81–97. DOI: 10.1037/h0043158

Monaghan, Sean (2022): Deterring hybrid threats: Towards a fifth wave of deterrence theory and practice. Hybrid CoE Paper 12. European Centre of Excellence for Countering Hybrid Threats, Helsinki. Online: https://www.hybridcoe.fi/wp-content/uploads/2022/03/20220331HybridCoEPaper12FifthwaveofdeterrenceWEB.pdf

Moore, Hannah – Roberts, Dan (2013): AP twitter hack causes panic on Wall Street and sends Dow plunging. The Guardian, 2013. április 23.

Morley-Davies, Jonathan – Thomas, Jem – Baines, Graham (2024): Russian Information Operations outside of the Western Information Environment. NATO STRATCOM COE, Riga.

Mumford, Andrew (2020): Ambiguity in hybrid warfare. Hybrid CoE Strategic Analysis 24. European Centre of Excellence for Countering Hybrid Threats, Helsinki.

NATO (2022): NATO 2022 Strategic Concept. Online: https://www.nato.int/content/dam/nato/webready/documents/publications-and-reports/strategic-concepts/2022/290622-strategic-concept.pdf

NATO (2024): NATO's response to hybrid threats. NATO Public Diplomacy Division.

NATO STRATCOM COE (2016a): Analysis of Russia's Information Campaign against Ukraine (teljes jelentés). NATO Strategic Communications Centre of Excellence, Riga.

NATO STRATCOM COE (2016b): Social Media in the Service of Hybrid Warfare: The Ukraine Conflict Full Report. NATO Strategic Communications Centre of Excellence, Riga.

NATO STRATCOM COE (2016c): The Manipulative Techniques of Russia's Information Campaign: Executive Summary. NATO Strategic Communications Centre of Excellence, Riga.

NATO STRATCOM COE (2018a): Social Media Manipulation: Trends and Developments. NATO Strategic Communications Centre of Excellence, Riga.

NATO STRATCOM COE (2018b): The Black Market for Social Media Manipulation. NATO Strategic Communications Centre of Excellence, Riga.

NATO STRATCOM COE (2020a): A Framework for Armed Forces in the Social Media Domain: Camouflage in the Digital Domain. NATO Strategic Communications Centre of Excellence, Riga.

NATO STRATCOM COE (2020b): Deepfakes – Primer and Forecast. NATO Strategic Communications Centre of Excellence, Riga.

NATO STRATCOM COE (2020c): Social Media Manipulation 2020. NATO Strategic Communications Centre of Excellence, Riga.

NATO STRATCOM COE (2021a): Fact-Checking and Debunking. NATO Strategic Communications Centre of Excellence, Riga.

NATO STRATCOM COE (2021b): Insights into Covid-19-related News Media Discourse. NATO Strategic Communications Centre of Excellence, Riga.

NATO STRATCOM COE (2021c): Russia's Activities in Africa's Information Environment: Case Studies – Mali and the Central African Republic. NATO Strategic Communications Centre of Excellence, Riga.

NATO STRATCOM COE (2022): Strategic Communications and Covid-19. NATO Strategic Communications Centre of Excellence, Riga.

NATO STRATCOM COE (2023a): Information Laundering in Germany. NATO Strategic Communications Centre of Excellence, Riga.

NATO STRATCOM COE (2023b): Social Media Manipulation 2022/2023. NATO Strategic Communications Centre of Excellence, Riga.

NATO STRATCOM COE (2023c): Trends in AI. NATO Strategic Communications Centre of Excellence, Riga.

NATO STRATCOM COE (2023d): Virtual Manipulation Brief 2023/1: Generative AI and Its Implications for Social Media Analysis. NATO Strategic Communications Centre of Excellence, Riga.

NATO STRATCOM COE (2024a): Information Laundering via BaltNews on Telegram. NATO Strategic Communications Centre of Excellence, Riga.

NATO STRATCOM COE (2024b): Robotrolling 2023/2024 – Analysis of Automated Activity on Social Media. NATO Strategic Communications Centre of Excellence, Riga.

NATO STRATCOM COE (2024c): Social Media Manipulation for Sale. NATO Strategic Communications Centre of Excellence, Riga.

NATO STRATCOM COE (2024d): The Role of AI in Digital Information. NATO Strategic Communications Centre of Excellence, Riga.

NATO STRATCOM COE (2025): Social Media Manipulation. NATO Strategic Communications Centre of Excellence, Riga.

NATO STRATCOM COE – Hybrid CoE (2023): Attributing Information Influence Operations: Identifying those Responsible for Malicious Behaviour Online. NATO Strategic Communications Centre of Excellence, Riga.

NBSZ NKI (2025): Kiberbiztonsági fenyegetések és kihívások 2030-ig. Nemzetbiztonsági Szakszolgálat Nemzeti Kiberbiztonsági Intézete, Budapest. Online: https://nki.gov.hu/wp-content/uploads/2025/04/Kiberbiztonsagi-fenyegetesek-es-kihivasok-2030-ig.pdf

Newman, Hannah (2022): Foreign Information Manipulation and Interference Defence Standards: Test for Rapid Adoption of the Common Language and Framework 'DISARM'. Hybrid CoE Research Report 7. European Centre of Excellence for Countering Hybrid Threats – NATO STRATCOM COE, Helsinki–Riga.

Nimmo, Ben – Agranovich, David – Gleicher, Nathaniel (2022a): Adversarial Threat Report [Q1 2022]. Meta. Online: https://about.fb.com/news/2022/04/metas-adversarial-threat-report-q1-2022/

Nimmo, Ben – Brookie, Graham et al. (2019): Operation Secondary Infektion. Atlantic Council – DFRLab. Online: https://www.atlanticcouncil.org/wp-content/uploads/2019/08/Operation-Secondary-Infektion_English.pdf

Nissen, Thomas Elkjer (2015): #TheWeaponizationOfSocialMedia: Characteristics of Contemporary Conflicts. Royal Danish Defence College, Koppenhága.

Nissen, Thomas Elkjer (2016): Social Media's Role in 'Hybrid Strategies'. NATO STRATCOM COE, Riga.

Nolan, Susan A. – Kimball, Michael (2021): The Intent Behind a Lie: Mis-, Dis-, and Malinformation. Psychology Today, 2021. december 22.

1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról. Magyar Közlöny, 2020. 81. sz. Online: https://njt.hu/jogszabaly/2020-1163-30-22

Orbán Zsolt (2021): E-learning projektek sikerténye zői. Az e-learning megoldások Actor-Network Theory elemzése. PhD-disszertáció. Budapesti Corvinus Egyetem, Budapest.

Oxford University / Computational Propaganda Project [é. n.]: The IRA, Social Media and Political Polarization in the United States. Oxford Internet Institute, Oxford.

Pamment, James (2021): RESIST 2 Counter Disinformation Toolkit. UK Government Communication Service, London.

Pamment, James (2022a): A Capability Definition and Assessment Framework for Countering Disinformation, Information Influence, and Foreign Interference. NATO STRATCOM COE, Riga.

Pamment, James (2022b): Assessing national capabilities for countering foreign information manipulation and interference. NATO STRATCOM COE, Riga.

Pamment, James – Nothhaft, Howard – Fjällhed, Alicia (2018): Countering Information Influence Activities: A Handbook for Communicators. Myndigheten för samhällsskydd och beredskap (MSB), Stockholm.

Pamment, James et al. (2019): The Role of Communicators in Countering the Malicious Use of Social Media. NATO STRATCOM COE, Riga.

Pamment, James et al. (2024): AI in Support of Strategic Communication Capabilities. NATO STRATCOM COE, Riga.

Pamment, James – Sörensen, Sara (2024): Operationalising the Framework for Evaluating Capability against Information Influence Operations. NATO STRATCOM COE, Riga. Paul, Christopher – Matthews, Miriam (2016): The Russian „Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It. RAND Corporation, Santa Monica.

Paziuk et al. (2025): Decoding manipulative narratives in cognitive warfare: a case study of the Russia-Ukraine conflict. Frontiers in Artificial Intelligence, Vol. 8. DOI: 10.3389/frai.2025.1566022

Petykó Márton (2013): Az internetes troll mint identitás kialakítása politikai blogok diskurzusaiban. Magyar Nyelvőr, 137(3), 274–313. Online: https://real.mtak.hu/9008/1/137303.pdf

Pijpers, Peter B. M. J. (2022): Exploiting Cyberspace: International Legal Challenges and the New Tropes, Techniques and Tactics in the Russo-Ukraine War. Hybrid CoE Paper 15. European Centre of Excellence for Countering Hybrid Threats, Helsinki.

PIR Center (2011): Conceptual Views of the Activity of the Armed Forces of the Russian Federation in Information Space. October 12, 2011. Online: https://pircenter.org/en/editions/conceptual-views-on-the-activity-of-the-armed-forces-of-the-russian-federation-in-information-space/

Pomerantsev, Peter – Weiss, Michael (2014): The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money. The Institute of Modern Russia, New York.

Prier, Jarred (2017): Commanding the Trend: Social Media as Information Warfare. Strategic Studies Quarterly, 11(4), 50–85. Online: https://www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-11_Issue-4/Prier.pdf

Pulai Bence (2023): A befolyásolás mint a hibrid hadviselés eszköze a 2021-es lengyel–fehérorosz migrációs- és határválság során. Honvédségi Szemle, 151(6), 56–67. DOI: 10.35926/HSZ.2023.6.5. Online: https://kiadvany.magyarhonvedseg.hu/index.php/honvszemle/article/view/1138

Putyin, Vlagyimir (2021): Az oroszok és az ukránok történelmi egységéről. Kremlin.ru, 2021. július 12. Online: http://en.kremlin.ru/events/president/news/66181

Resperger István (2018): A válságkezelés és a hibrid hadviselés. Dialóg Campus, Budapest.

Resperger István (2020): A hibrid hadviselési mód jellemzői korunk konfliktusaiban. Rendőrségi Tanulmányok, 2020(2), 104–118.

Rittel, Horst W. J. – Webber, Melvin M. (1973): Dilemmas in a General Theory of Planning. Policy Sciences, 4(2), 155–169. DOI: 10.1007/BF01405730

Roozenbeek, Jon – van der Linden, Sander (2021): Inoculation Theory and Misinformation. NATO STRATCOM COE, Riga.

Roozenbeek, Jon – van der Linden, Sander – Goldberg, Beth – Rathje, Steve – Lewandowsky, Stephan (2022): Psychological inoculation improves resilience against misinformation on social media. Science Advances, 8, eabo6254. DOI: 10.1126/sciadv.abo6254

Rosenberg, Matthew – Confessore, Nicholas – Cadwalladr, Carole (2018): How Trump Consultants Exploited the Facebook Data of Millions. The New York Times, 2018. március 17.

Ruch, Simon – Züst, Marc Alain – Henke, Katharina (2016): Subliminal messages exert long-term effects on decision-making. Neuroscience of Consciousness, 2016(1). DOI: 10.1093/nc/niw013

Ruch, Simon – Herbert, Elizabeth – Henke, Katharina (2017): Subliminally and supraliminally acquired long-term memories jointly bias delayed decisions. Frontiers in Psychology, 8, 1542. DOI: 10.3389/fpsyg.2017.01542

Rusinaitė, Viktorija (2025): Turning strategy into praxis: Lessons in hybrid threat deterrence. Hybrid CoE Paper 25. European Centre of Excellence for Countering Hybrid Threats, Helsinki.

Sari, Aurel (2021): Hybrid threats and the law: Building legal resilience. Hybrid CoE Research Report 3. European Centre of Excellence for Countering Hybrid Threats, Helsinki.

Sazonov, Vladimir – Mölder, Holger – Müür, Kristiina (szerk.) (2016): Russian Information Campaign against the Ukrainian State and Defence Forces: April–December 2014. NATO STRATCOM COE, Riga.

Schiff, Kaylyn Jackson – Schiff, Daniel S. – Bueno, Natália S. (2024): The Liar's Dividend: Can Politicians Claim Misinformation to Evade Accountability? American Political Science Review, 119(1), 71–90. DOI: 10.1017/S0003055423001454

Sessa, Maria Giovanna – Miguel, Raquel (2024a): The Doppelganger Case: Assessment of Platform Regulation on the EU Disinformation Environment. NATO STRATCOM COE, Riga.

Sessa, Maria Giovanna – Miguel, Raquel (2024b): The Doppelganger Case: Avenues for Mitigation. NATO STRATCOM COE, Riga.

Shandra, Alya – Seely, Robert (2019): The Surkov Leaks: The Inner Workings of Russia's Hybrid War in Ukraine. RUSI Occasional Paper. Online: https://static.rusi.org/201907_op_surkov_leaks_web_final.pdf

Síklaki István (1994): A meggyőzés pszichológiája. Scientia Humana, Budapest.

Simon, Herbert A. (1990): Invariants of Human Behavior. Annual Review of Psychology, 41(1), 1–19. DOI: 10.1146/annurev.ps.41.020190.000245

Smith, Hanna (2022): How to read Russia: Internal structural disunity, risk-taking, and Russia's restless soul. Hybrid CoE Working Paper 17. European Centre of Excellence for Countering Hybrid Threats, Helsinki.

Somodi Zoltán – Kiss Álmos Péter (2019): A hibrid hadviselés fogalmának értelmezése a nemzetközi szakirodalomban. Honvédségi Szemle, 147(6), 17–28. DOI: 10.35926/HSZ.2019.6.2

Spiliopoulos, Leonidas (2025): Robust Deterrence and Actor Rationality. NATO STRATCOM COE, Riga.

Stupp, Catherine (2019): Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case. The Wall Street Journal, 2019. augusztus 30.

Svetoka, Sanda (szerk.) et al. (2016): Internet Trolling as a Tool of Hybrid Warfare: The Case of Latvia. NATO STRATCOM COE, Riga.

Szicherle Patrik – Krekó Péter (2020): Burjánzanak az álhírek a koronavírus nyomában. Political Capital, Budapest.

Szun-ce (1995): A hadviselés törvényei. Ford. Tőkei Ferenc. Balassi Kiadó, Budapest.

Thomas, Timothy L. (2016): Russia's 21st Century Information War: Working to Undermine and Destabilize Populations. Defence Strategic Communications, Vol. 1, No. 1. NATO STRATCOM COE, Riga. 11–26. DOI: 10.30966/2018.RIGA.1.1. Online: https://stratcomcoe.org/cuploads/pfiles/timothy_thomas.pdf

Turcsányi, Richard Q. et al. (2024): Sino-Russian Information Operations: Convergence, Divergence, and the Way Ahead. NATO STRATCOM COE, Riga.

Uscinski, Joseph E. – Parent, Joseph M. (2014): American Conspiracy Theories. Oxford University Press, New York.

Valaskivi, Katja (2018): Beyond Fake News: Content confusion and understanding the dynamics of the contemporary media environment. Hybrid CoE Strategic Analysis 5. European Centre of Excellence for Countering Hybrid Threats, Helsinki.

Vasara, Antti (2020): Theory of Reflexive Control: Origins, Evolution and Application in the Framework of Contemporary Russian Military Strategy. National Defence University, Helsinki.

Volāns, Eginhards et al. (2025): Handbook on the role of non-state actors in Russian hybrid threats. Hybrid CoE Paper 27. European Centre of Excellence for Countering Hybrid Threats, Helsinki. Online: https://www.hybridcoe.fi/wp-content/uploads/2025/12/Hybrid-CoE-Paper-27-Handbook-on-the-role-of-non-state-actors-in-Russian-hybrid-threats.pdf

Vosoughi, Soroush – Roy, Deb – Aral, Sinan (2018): The Spread of True and False News Online. Science, 359(6380), 1146–1151. DOI: 10.1126/science.aap9559

Wallner, Claudia – Copeland, Simon – Giustozzi, Antonio (2025): Russia, AI and the Future of Disinformation Warfare. Royal United Services Institute (RUSI), London.

Wardle, Claire – Derakhshan, Hossein (2017): Information Disorder: Toward an Interdisciplinary Framework for Research and Policymaking. Council of Europe Report DGI(2017)09, Strasbourg. (2. kiad. 2018.) Online: https://rm.coe.int/information-disorder-report-version-august-2018/16808c9c77

The Washington Post (2018): Trump admits he made up facts in trade meeting with Justin Trudeau. 2018. március 15.

WHO (2017): Communicating risk in public health emergencies: a WHO guideline for emergency risk communication (ERC) policy and practice. World Health Organization, Geneva.

Whitman, Michael E. – Mattord, Herbert J. (2011): Principles of Information Security. 4. kiadás. Cengage Learning, Boston.

Wickens, Christopher D. – Hollands, Justin G. (2000): Engineering Psychology and Human Performance. Prentice Hall, Upper Saddle River.

Wickens, Christopher D. – Hollands, Justin G. – Banbury, Simon – Parasuraman, Raja (2015): Engineering Psychology and Human Performance. Psychology Press, New York.

Winter, Charlie (2015): The Virtual 'Caliphate': Understanding Islamic State's Propaganda Strategy. Quilliam Foundation, London.

Yıldız, Karim – Özdemir, Hüseyin (2024): The Rise of Military Bloggers Amid the Russian-Ukrainian War. TRT World Research Centre, Washington D.C.–Ankara.

YouGov Cambridge Globalism Project (2022): Annual Survey on Global Issues. University of Cambridge / YouGov.

Zubiaga, Arkaitz – Liakata, Maria – Procter, Rob – Wong Sak Hoi, Geraldine – Tolmie, Peter (2016): Analysing How People Orient to and Spread Rumours in Social Media by Looking at Conversational Threads. PLoS ONE, 11(3), e0150989. DOI: 10.1371/journal.pone.0150989

Zygar, Mikhail (2016): All the Kremlin's Men: Inside the Court of Vladimir Putin. PublicAffairs, New York.