Horváth Dávid[1]

Infrastruktúra és identitás a köztes kognitív hadviselési ökoszisztéma korszakában

A fegyvernek minősülő kommunikáció operatív bázisértékei

A tanulmány a fegyvernek minősülő kommunikáció (FMK) műveleti alaprétegeit vizsgálja a 2013–2015 közötti „köztes kognitív hadviselési ökoszisztéma korszakban", a generatív mesterséges intelligencia előtti manuális kampányok időszakában. A kutatás a strukturált és fókuszált összehasonlítás (SFC) módszertanával négy horgonyesetet elemez: a 2013-as AP-incidensben az alacsony eszközigényű hitelességbitorlást; a 2014-es krími kampányban a teljes G–M–T–V támadási lánc rendszerszintű alkalmazását; a 2014-es ebola-infodémiában az ideológiai vállalkozók validációorientált műveleti logikáját; a 2015-ös migrációs válságban a zárt csoportokba szorított dezinformáció protokollját. Az összehasonlító elemzést a H–E–I diagnosztikai rács (helyzetértékelés–előrejelzés–irányítás) táblázatos formában vizualizálja. Fő megállapítás: a vizsgált időszak az FMK operatív bázisértéke – azon műveleti rutinok rögzített készlete, amelyeket a 2016 utáni dezinformációs hullámok már csak technológiai úton skáláztak fel.

Kulcsszavak: *kognitív hadviselés, fegyvernek minősülő kommunikáció, operatív bázisérték, G–M–T–V támadási lánc, köztes kognitív hadviselési ökoszisztéma*

Infrastructure and Identity in the Intermediate Cognitive Warfare Ecosystem Era

Operational Baseline Values of Weapon-Grade Communication

This study examines the operational foundations of weapon-grade communication (WGC) during the 2013–2015 intermediate cognitive warfare ecosystem period, before the emergence of generative AI. Using structured and focused comparison (SFC), the G–L–D–V kill chain model, and the H–E–I (Situation–Forecast–Control) diagnostic grid, the research analyses four anchor-case events: the 2013 AP incident (low-resource credibility hijacking), the 2014 Crimea annexation (full kill-chain state operation), the 2014 Ebola infodemic (validation-oriented non-state actors), and the 2015 migration crisis (closed-group disinformation logic). The H–E–I profiles of each case are presented in tabular form. The central argument is that manually coordinated campaigns had fully established their core operational routines – persona masking, coordinated amplification, network density – by 2015. The 2013–2015 period thus constitutes the operational baseline (bázisérték) without which the later AI-scaled disinformation waves, including operations such as Ghostwriter (2021), cannot be fully understood.

Keywords: *cognitive warfare, weapon-grade communication, operational baseline, G–L–D–V kill chain, intermediate cognitive warfare ecosystem*

[1] Horváth Dávid az NKE Hadtudományi Doktori Iskolájának doktori hallgatója.

Bevezetés

Jelen tanulmány a 2013–2015 közötti, úgynevezett „köztes kognitív hadviselési ökoszisztéma" korszak információs műveleteinek elemzésén keresztül azonosítja a modern kognitív hadviselés automatizáció előtti, örökölt mintázatait. A kutatás központi tézise szerint az ekkor manuálisan koordinált kampányok rögzítették azokat a műveleti rutinokat, amelyeket a 2016-os évet követő rendszerszintű dezinformációs hullámok már csak technológiai úton skáláztak fel.

A kutatás elméleti alapvetése a fegyvernek minősülő kommunikáció terminológiájára épül. Az FMK olyan rendszerszintű és koordinált befolyásolási műveleteket *(influence operations)* jelöl, amelyek túlmutatnak a klasszikus meggyőzésen: elsődleges funkciójuk az emberi információfeldolgozás szisztematikus megzavarása, a helyzetértékelés *(situational awareness)* torzítása, valamint a döntéshozatali képesség *(decision-making capacity)* lassítása vagy teljes megbénítása. A terminológia elméleti gyökerei az információs hadviselés korai, kilencvenes évekbeli megalapozásáig nyúlnak vissza. Arquilla és Ronfeldt (1993) úttörő munkája szakított azzal a megközelítéssel, amely a kommunikációt csupán a kinetikus műveletek kiegészítőjeként kezelte; helyette az adatfolyamokat olyan önálló stratégiai erőforrásként definiálták, amelyek közvetlen csapásmérő képességgel bírnak.[2] Ez az evolúció vezetett a fegyverré tett narratíva *(weaponized narrative)* koncepciójához, amely a keretezést és a történetmesélést már egyfajta stratégiai fegyverrendszerként értelmezi.[3] Ebben a dimenzióban a cél az ellenfél valóságérzékelésének szisztematikus erodálása és a befogadó belső logikájának önmaga ellen fordítása. A fogalom operatív mélységét a pszichológiai és kognitív tudományok vívmányait ötvöző precíziós nyelvi eszközök *(weapon-grade tools)* adják, amelyek kontrollt biztosítanak a befogadó érzelmi és racionális válaszreakciói felett.[4] Ez a megközelítés szervesen illeszkedik a hibrid fenyegetések *(hybrid threats)* elleni fellépés korszerű NATO-doktrínáihoz, ahol az információs egységek már nem passzív üzenetként, hanem a kognitív folyamatokat célzó, aktív műveleti elemekként jelennek meg.[5]

A kutatás központi tézise szerint a 2013 és 2015 közötti periódus nem csupán elszigetelt incidensek sorozata volt, hanem a kognitív hadviselés manuális iparosításának kora. Ebben az értelemben a vizsgált időszakot operatív bázisértékként határozom meg: ez az a minimális képesség- és rutinkészlet (például koordinált amplifikáció, online profilmaszkolás), amely 2016-tól kezdve már stratégiai szinten skálázhatóvá vált. A kutatás rávilágít arra, hogy az FMK hatékonysága nem a technológiai fejlettségtől, hanem a kognitív sérülékenységek *(cognitive vulnerabilities)* – vagyis az emberi információfeldolgozás azon belső torzításai és mentális rövidútjai (például kognitív torzítások vagy érzelmi heurisztikák),

[2] Arquilla, John – Ronfeldt, David (1993): Cyberwar is Coming! *Comparative Strategy,* 12(2), 141–165.

[3] Allenby, Brad – Garreau, Joel: *Weaponized Narrative: The New Battlespace.* [online], 2017. 01. 03. Forrás: Defense One [2026. 01. 26.].

[4] Voss, Chris – Raz, Tahl (2016): *Never Split the Difference: Negotiating as if Your Life Depended on it*. New York: HarperBusiness.

[5] du Cluzel, François: *Cognitive Warfare*. [online], 2021. Forrás: innovationhub-act.org [2026. 01. 10.].

amelyeket az információs műveletek a befogadó valóságérzékelésének manipulálására használnak fel[6] – és a médiarendszerek hibriditásának pontos kiaknázásától függ.[7]

A téma aktualitása és a kutatási hézag

Bár a szakirodalom bőségesen foglalkozik a 2016-os amerikai elnökválasztás vagy a 2020-as világjárvány alatti dezinformációs kampányokkal, viszonylag kevés figyelem irányul a 2013–2015-ös időszakra mint önálló, bázisértékkel bíró korszakra. A kutatási hézagot az a kérdés jelöli ki, hogy miként jöttek létre és rögzültek azok a terjesztési infrastruktúrák *(distribution infrastructures)* és online profil-ökonómiák *(online profile economies),* amelyek ma is a befolyásolási műveletek gerincét alkotják.

A forrásmennyiség korlátait a terület legelismertebb hazai és nemzetközi szakértőinek mélyfúrásszerű beemelésével kompenzáltuk. A szövegben kontextualizáltam és ütköztettem a hibrid hadviselés elméletének magyarországi alapvetéseit (Resperger István[8] és Marton Péter[9]), valamint a nemzetközi kognitív hadviselési diskurzus meghatározó alakjait, köztük a RAND Corporation kutatóit (Christopher Paul, Rand Waltzman), illetve a számítógépes propaganda elismert szakértőit (Samuel Woolley, Philip N. Howard). Ez a szelektív, de szakmailag fajsúlyos hivatkozási háló biztosítja a kutatás elméleti és empirikus érvényességét.

Kutatási kérdések és hipotézisek

A kutatás az alábbi központi kérdésekre keresi a választ:

1. kutatási kérdés: Milyen típusú műveleti rutinok jellemezték a fegyvernek minősülő kommunikációt a köztes kognitív hadviselési ökoszisztéma korszakában?
2. kutatási kérdés: Hogyan érvényesült a kommunikáció, tartalmi generálás–mosás–terjesztés–validálás (G–M–T–V) támadási lánc a manuális korszak meghatározó eseményei során?
3. kutatási kérdés: Mennyiben tekinthető a 2015-ös esztendő a szabályozási és intézményi immunválasz fordulópontjának?

A vizsgálat során az alábbi hipotéziseket (H) tesztelem:

1. hipotézis: A fegyvernek minősülő kommunikáció műveleti rutinjai, úgymint az online profilmaszkolás és a koordinált amplifikáció, már 2015-re teljeskörűen rögzültek, függetlenül a későbbi automatizációs technológiáktól.
2. hipotézis: A köztes kognitív hadviselési ökoszisztéma korszakában a támadási lánc súlypontja a terjesztési *(distribution)* és a validálási *(validation)* fázisokra helyeződött, kihasználva a médiarendszerek hibriditását.

---

[6] Lewandowsky, Stephan – Cook, John – Lombardi, Doug (2020): *The Debunking Handbook 2020*. [H. n.]: [K. n.], 4.
[7] Marton Péter (2018): A hibrid hadviselés előfordulásának feltételeiről. *Nemzet és Biztonság,* 11(3), 95–105.
[8] Resperger István (2018): *A válságkezelés és a hibrid hadviselés*. Budapest: Dialóg Campus, 24.
[9] Marton 2018: 95.

3. hipotézis: A 2013–2015 közötti események hullámdinamikája közvetlen hatást gyakorolt a nyugati intézményi védekezési stratégiák *(east stratcom task force)* megalapozására.

A kutatás tárgya és korlátai

A kutatás tárgya a 2013. áprilisi Associated Press-incidens[10] és a 2015. végi európai intézményi válaszreakciók közötti időszak információs műveleteinek elemzése. A vizsgálat fókusza a kognitív hadviselés operatív szintje, nem pedig a politikai ideológiák tartalmi elemzése. A kutatás korlátját a platform-transzparencia retrospektív hiányosságai jelentik,[11] amit a módszertan visszatekintő digitális vizsgálati eljárásokkal és szigorú, auditálható forrásküszöbökkel igyekszik kompenzálni.[12]

Fogalmi keretrendszer és kutatási módszertan

Hibrid hadviselés és válságkezelés

A modern biztonsági környezetben a hibrid hadviselés fogalma olyan komplex műveleti formát jelöl, amelyben a támadó aktor a katonai és nem katonai eszközöket szinkronizált módon alkalmazza a célország stratégiai bénultságának előidézésére. Resperger István rámutat, hogy ebben a rendszerben az információs műveletek *(information operations)* szerepe kritikus, mivel a bizonytalanság szisztematikus fenntartása közvetlenül a válságkezelési mechanizmusok *(crisis management)* hatékonyságát ássa alá.[13]

A hibrid fenyegetések egyik legfontosabb eszköze a reflexív kontroll *(reflexive control),* amelynek során a támadó olyan információkkal – vagy dezinformációval *(disinformation)* – látja el a célpontot, amelyek hatására az alany a támadó érdekeinek megfelelő döntést hoz. Az elméleti keret szerint a sikeres válságkezelés alapfeltétele a helyzetértékelési képesség *(situational awareness)* megőrzése, amit a fegyvernek minősülő kommunikáció az információs zaj és a kognitív túlterhelés *(cognitive overload)* útján igyekszik ellehetetleníteni. Ebből a szempontból a 2013–2015-ös időszak eseményei nem csupán elszigetelt incidensek, hanem a válságkezelési rutinok kognitív tesztelésének folyamataiként értékelhetők.[14]

Svetoka és szerzőtársai a NATO StratCom COE elemzésében az internetes trollkodást *(internet trolling)* mint a hibrid hadviselés operatív eszközét azonosítják, amely a válságkezelés akadályozásának egyik legaktívabb módszere. Kutatásuk alátámasztja, hogy a szervezett befolyásolás hatékonysága az organikus társadalmi párbeszéd és a mesterségesen

[10] Paul, Christopher – Matthews, Miriam: *The Russian „Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It*. [online], 2016. 07. 11. Forrás: RAND [2026. 06. 17.].

[11] Matos Alves, Artur de: *A Short History of Online Platform Transparency*. [online], 2023. 02. Forrás: demontages.phllab.uliege.be [2026. 01. 10.].

[12] Prier, Jarred (2017): Commanding the Trend: Social Media as Information Warfare. *Strategic Studies Quarterly,* 11(4), 50–85. 52.

[13] Resperger 2018: 24–25.

[14] Resperger 2018: 31.

generált narratívák közötti határvonal szándékos elmosásában rejlik. Ez a gyakorlatban a legsebezhetőbb társadalmi csoportok célzott elérését és a meglévő információs buborékok *(information bubbles)* kihasználását jelenti, ami tovább mélyíti a Resperger által leírt stratégiai bizonytalanságot.[15]

A médiarendszerek hibriditása és a kognitív sérülékenység

A befolyásolási műveletek hatékonysága a támadó szándékán túl a befogadó közeg strukturális jellemzőitől is függ. Marton Péter rávilágít, hogy a médiarendszerek hibriditása *(hybrid media systems)* – vagyis a hagyományos szerkesztőségi média és a hálózatosodott közösségi média logikájának összefonódása – alapjaiban változtatta meg az információ terjedési dinamikáját.[16] Ez a hibriditás teszi lehetővé, hogy az FMK behatolási pontokat találjon a célközönség információs buborékaiba.

A kognitív sérülékenység *(cognitive vulnerability)* egyik legmeghatározóbb faktora a kulturális közelség *(cultural proximity)*. Joseph Straubhaar elmélete szerint a befogadók ösztönösen azokat a tartalmakat és forrásokat részesítik előnyben, amelyek nyelvi, kulturális és szociális kódrendszere megegyezik a sajátjukkal.[17] Az FMK operatív alaprétegét ezen elméleti tétel gyakorlati alkalmazása, a fiktív perszónák *(fictional personas)* hálózatba szervezett, stratégiai működtetése adja. Ebben a környezetben a perszóna már nem egyszerűen egy hamisított felhasználói fiók, hanem egy módszeresen felépített, valós személyiséget imitáló szereplő, amely saját névvel, koherens vizuális identitással és egyedi viselkedési rutinnal rendelkezik. A „helyi hangként" fellépő maszkok a kulturális közelséget kihasználva válnak a célközönség információs környezetének szerves részévé, megkerülve az intézményi forrásokkal szembeni kognitív fenntartásokat.

Ebben a folyamatban a médiarendszerek sebezhetősége abban rejlik, hogy a sebességre és a figyelemgazdaság *(attention economy)* mechanizmusaira optimalizált algoritmusok kritika nélkül segítik elő a sablonizált dezinformáció terjedését. Jarred Prier kutatása a trendek uralásáról *(commanding the trend)* rávilágít, hogy a közösségi média algoritmusaival való visszaélés végső célja a fősodratú média napirendjének *(agenda-setting)* irányítása.[18] A mesterségesen generált interakciók – a belső megosztások és kedvelések rendszere – a tartalmakat olyan algoritmuspályára helyezik, amely folyamatos nyomás alatt tartja a figyelmi szűrőket *(agenda-pressure).* Az információs művelet akkor ér el stratégiai áttörést, amikor a professzionális média tekintélye által nyeri el végső legitimációját.

Ez a mechanizmus a kognitív sérülékenység egyik legsúlyosabb formáját, a megerősítési torzítást *(confirmation bias)* használja ki. A cél egyrészt a többségi látszat *(illusion of majority)* előállítása, amely a hamisított társadalmi bizonyíték *(social proof)* erejével azt sugallja a felhasználónak, hogy a narratíva mögött széles körű egyetértés áll. Másrészt

[15] Svetoka, Sanda et al. (2016): *Social Media as a Tool of Hybrid Warfare*. Riga: NATO Strategic Communications Centre of Excellence, 33.

[16] Marton 2018: 95.

[17] Straubhaar, Joseph D. (1991): Beyond Media Imperialism: Asymmetrical Interdependence and Cultural Proximity. *Critical Studies in Mass Communication,* 8(1), 39–59.

[18] Prier 2017: 52.

a folyamat a hitelességbitorláson *(credibility hijacking)* keresztül vagy éles társadalmi polarizációt, vagy kognitív bénultságot *(cognitive paralysis)* eredményez.[19] Utóbbi esetben a cinizmus és a döntésképtelenség válik uralkodóvá, ami a médiarendszer hibriditását közvetlenül a demokratikus válságkezelési folyamatok ellen fordítja.

A fegyvernek minősülő kommunikáció és a kognitív hadviselés fogalmi elkülönítése

A tudományos pontosság megköveteli a technikai eszköztár és a műveleti tartomány éles elhatárolását. A jelen kutatás keretei között az FMK és a kognitív hadviselés (*cognitive warfare,* CW) két különböző, de egymást feltételező dimenziót jelöl.

Az FMK magát az ökoszisztémát jelenti: olyan tudatosan szerkesztett információs egységet, amelynek célja nem a klasszikus meggyőzés, hanem a döntéshozatali funkciók megbénítása.[20] Az FMK-tartalom jellemzője a nagyfokú célzottság és a pszichológiai kiváltó okok *(triggers)* tudatos kiaknázása. Ezzel szemben a kognitív hadviselés a műveleti teret és a stratégiai célt definiálja: ez az a domén, ahol a támadó a célpont döntéshozatali mechanizmusait és valóságérzékelését támadja. Resperger István értelmezésében a valódi reziliencia a befogadói tudatosság szintjén dől el.[21]

Módszertan

A kutatás módszertani kerete: a strukturált és fókuszált összehasonlítás

A fegyvernek minősülő kommunikáció operatív mintázatainak és örökölt rutinjainak feltárásához a tanulmány a strukturált és fókuszált összehasonlítás (*structured, focused comparison,* SFC) módszertanát alkalmazza.[22] Ez az eljárás lehetőséget teremt arra, hogy a látszólag eltérő természetű eseményeket egy közös elméleti és elemzési keretben vessük össze. A módszer strukturált jellege abban nyilvánul meg, hogy a kiválasztott incidensek – úgynevezett *anchor* esetek – vizsgálata során minden esetben ugyanazokat a rögzített kutatási kérdéseket alkalmazzuk. Ez a megközelítés biztosítja az adatok szisztematikus összevethetőségét, a gyűjtött információk auditálhatóságát és a levonható következtetések tudományos érvényességét.

A vizsgálat ugyanakkor fókuszált is, mivel figyelmét kizárólag a kognitív hadviselés operatív aspektusaira, a technikai infrastruktúra sajátosságaira, valamint a támadási láncra irányítja. A kutatás tudatosan eltekint az egyes incidensek politikai vagy ideológiai kontextusának részletes elemzésétől, hogy az információs műveletek „műveleti

[19] Resperger 2018: 31.
[20] NATO Strategic Communications Centre of Excellence (2015): *Analysis of Russia's Information Campaign against Ukraine*. Riga: NATO StratCom COE, 40.
[21] Resperger 2018: 31.
[22] George, Alexander L. – Bennett, Andrew (2005): *Case Studies and Theory Development in the Social Sciences*. Cambridge: MIT Press, 67.

tervrajzai" *(operational blueprints)* váljanak láthatóvá. Ez a szelektív fókusz teszi lehetővé a 2013–2015 közötti, az információs ökoszisztéma kialakulását megelőző időszakban rögzült rutinok azonosítását, amelyek a későbbi, automatizált korszakok technológiai skálázásának alapjául szolgáltak.

Az SFC-modell alkalmazása során az elemzés minden vizsgált eseménynél standardizált változókat rögzít. Ezek közé tartozik a műveleti kiváltó ok *(trigger)* pontos meghatározása, az aktorok rendszertani besorolása, az igénybe vett kommunikációs csatornák jellege, valamint a célzott kognitív kimenet azonosítása. Ez a módszertani következetesség garantálja, hogy a vizsgált korszak heterogén eseményei egyetlen, egységes diagnosztikai rácson váljanak értelmezhetővé.

A kutatás folyamatmodellje: a G–M–T–V támadási lánc

Az FMK elemzéséhez alkalmazott keretrendszer az információs műveleteket négy, egymást feltételező szakaszra bontja. Ez a folyamatmodell – amelyet a kutatás generálás–mosás–terjesztés–validálás (*generation, laundering, distribution, validation,* G–M–T–V) támadási láncként *(kill chain)* definiál – teszi lehetővé a kognitív hadviselés során alkalmazott funkcionális lépések elkülönítését. A modell rávilágít arra, hogy az információs ökoszisztéma kialakulását megelőző időszakban rögzült manuális műveleti rutinok miként képezik a későbbi technológiai skálázás alapját.

A láncolat első fázisa a generálás (*generation,* G), amely az operatív célokat szolgáló narratívák és üzenetpanelek előállítását jelenti. Az automatizáció előtti korszakban ez a szakasz dominánsan manuális jellegű volt, ahol a tartalmakat emberi aktorok – például szervezett trollfarmok munkatársai – hozták létre.[23]

A második szakasz az információs mosás (*laundering,* L), amely az üzenetek eredetének elrejtését és a hitelesség szimulálását szolgálja. A művelet célja itt az, hogy a tartalom elveszítse közvetlen kötődését a támadó aktorhoz, és látszólag organikus információként vagy kiszivárgott tényként jelenjen meg a célközönség információs terében.

A harmadik fázis a terjesztés (*distribution,* D), vagyis az üzenetek nagy volumenű eljuttatása a kiválasztott célcsoportokhoz. Ebben a szakaszban a hálózati sűrűség és az elárasztás sebessége válik prioritássá, szisztematikusan építve a „hazugság tűzoltótömlője" *(firehose of falsehood)* elvére.[24]

A láncolat utolsó eleme a validálás (*validation,* V), amely a befogadói elfogadás és a társadalmi bizonyíték megteremtését célozza. Ez a fázis az automatizáció előtti időszakban elsősorban identitásalapú hitelességkölcsönzés és fiktív perszónák hálózatos alkalmazása útján valósult meg.[25]

---

[23] NATO Strategic Communications Centre of Excellence 2015: 39–40.

[24] Paul–Matthews 2016: 2.

[25] Horváth Dávid (2026): *A fegyvernek minősülő kommunikáció operatív alaprétegei.* (Interpretáció).

A H–E–I diagnosztikai rács alkalmazása

A H–E–I diagnosztikai rács három tengelyen méri az FMK műveleti hatását: a helyzetérzékelés (H) tengelye azt rögzíti, mennyire torzult a célközönség valóságérzékelése; az előrejelzés (E) tengelye azt méri, mennyire romlott a döntés-előkészítési képesség; az irányítás (I) tengelye azt azonosítja, miből fakadt a cselekvőképesség-kiesés. Az 1. táblázat az *anchor* esetek H–E–I profiljait foglalja össze a G–M–T–V-súlyponttal együtt.

1. táblázat: Az anchor esetek H–E–I diagnosztikai profilja

Eset	**H: Helyzetértékelés torzítása**	**E: Döntés-előkészítés rontása**	**I: Cselekvőképesség-kiesése**	**G–M–T–V-súlypont**
AP-incidens (2013)	Hamis válsághelyzet percepciója (Fehér Ház-támadás)	Algoritmikus tőzsdei reakció megelőzte a cáfolatot (23 perc)	Befagyott döntéshozatal a hitelesítési vákuum idején	V (validálás)
Krím-annexió (2014)	„Helyi szemtanú" narratíva elfedi a katonai jelenlétet	A NATO-döntéshozók bizonytalansága, késleltetett válasz	Az összehangolt katonai és narratív nyomás megbénítja az intézményi reakciót	Teljes G–M–T–V-lánc
Ebola-infodémia (2014)	Hamis gyógymódok felülírják a WHO-ajánlásokat	Karanténellenes magatartás, egészségügyi kockázat alábecslése	Közvetlen fizikai kár; közegészségügyi karanténintézkedések hatástalansága	V (validálás dominál)
Migrációs válság (2015)	Manipulált képek és hamis statisztikák torzítják a közbeszédet	Polarizált közvélemény döntésképtelensége zárt csoportokban	A visszhangkamra-logika kizárja a cáfolatot; hatósági monitorozás vakfolt	M–T (zárt platformon)

Forrás: a szerző szerkesztése

Az információs ökoszisztéma kialakulásának operatív jellemzői (2013–2015)

A terjesztési infrastruktúra sajátosságai és a hálózati sűrűség

Az FMK ökoszisztémájának kialakulását megelőző időszak egyik meghatározó felismerése, hogy a befolyásolási műveletek hatékonysága elsősorban nem a tartalom belső koherenciáján, hanem a terjesztési infrastruktúra *(distribution infrastructure)* sűrűségén és az algoritmikus láthatóságon alapult. Ebben a környezetben a stratégiai súlypont a támadási lánc terjesztési (*distribution,* D) fázisára tolódott el: a mennyiségi elárasztás módszeresen kompenzálta a generált (*generation,* G) tartalom esetleges logikai hiányosságait.

A terjesztési dominancia alapköve a számítógépes propaganda *(computational propaganda),* amely az algoritmusok és a humán erőforrás szisztematikus ötvözését jelenti

a diskurzus manipulálása érdekében.[26] Az operatív bázisértékek rögzítése során az alábbi aktortaxonómia azonosítható a terjesztési hálózatokban:

- állami aktorok: a közvetlen műveleti irányítást végző szervek (például trollfarmok);
- proxyszervezetek: látszólag függetlennek mutatkozó, de irányított intézetek vagy médiumok;
- bűnözői hálózatok: a technikai infrastruktúra (például botnetek) bérbeadására szakosodott csoportok;[27]
- ideológiai vállalkozók: alapvetően monetizációs célú, de az FMK-narratívákat felerősítő szereplők.

Christopher Paul és Miriam Matthews a „hazugság tűzoltótömlője" *(firehose of falsehood)* modellje mentén alátámasztják, hogy a hálózati sűrűség önmagában a hitelesség helyettesítőjévé *(proxy)* válik: a befogadó számára az információ azért tűnik valósnak, mert rövid időn belül több, látszólag független forrásból találkozik vele.[28]

Kiemelendő a műveleti fenntarthatóság gazdasági aspektusa is. A 2015-re kiépült monetizációs ösztönzők – úgymint a kattintásvadász *(clickbait)* hálózatok és a hirdetési rendszerek – olyan önfinanszírozó üzleti motort biztosítottak, amely az állami forrásoktól függetlenül is fenntartotta az FMK-infrastruktúrát. Marton Péter rávilágít, hogy amennyiben a terjesztési hálózat képes a célközönség platformnatív rutinjait utánozni, a dezinformáció tisztára mosása *(laundering)* már a terjesztési fázisban megkezdődik.[29] Ez a mechanizmus rögzítette a skálázhatóság azon alapelveit, amelyeket a 2016 utáni korszak technológiai automatizációja már kész mintaként vett át.

A koordinált álszemélyiség-hálózatok és a hitelességszimuláció operatív mintázatai

Az identitás-gazdaságtan *(identity economy)* keretrendszerében a hitelességkölcsönzés *(credibility lending)* vált a manipuláció elsődleges validáló eszközévé, rögzítve azokat a pszichológiai és műveleti mintázatokat, amelyeket a későbbi korszakok már technológiai úton automatizáltak. Az FMK hatékonysága az információs ökoszisztéma kialakulásának fázisában alapvetően a befogadói bizalom morfológiájára épült. Míg a támadási lánc *(kill chain)* terjesztési szakaszában a mennyiségi elárasztás dominált, a validálás (*validation,* V) fázisában a minőségi hitelességszimuláció vált döntő faktorrá. Ebben a kontextusban az identitás-gazdaságtan az emberi percepció módszeres megtévesztését jelentette ellopott *(stolen identities)* és hibrid identitások *(hybrid identities)* segítségével.

A korszak egyik meghatározó dokumentuma a NATO Stratégiai Kommunikációs Kiválósági Központ (NATO Strategic Communications Centre of Excellence) 2014-es elemzése, amely rögzítette a „helyi szemtanú" és a „bennfentes" maszkok rendszerszintű

[26] Woolley, Samuel C. – Howard, Philip N. szerk. (2018): *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media*. Oxford: Oxford University Press, 3–6.
[27] Europol (2015): *Internet Organised Crime Threat Assessment (iOCTA) 2015*. Hága: Europol, 48.
[28] Paul–Matthews 2016: 2.
[29] Marton 2018: 95.

alkalmazását.[30] A műveleti tervezők felismerték, hogy a forrás társadalmi beágyazottsága kritikusabb tényező, mint az információ tényszerűsége. A bizalombitorlás *(trust hijacking)* során olyan profilokat aktiváltak, amelyek a célközönség kulturális és szociális normáit tükrözték. Marton Péter rávilágít, hogy a kulturális közelség lehetővé teszi a támadó számára, hogy a célközönség információs buborékaiba „helyi hangként" épüljön be, hatékonyan megkerülve a hivatalos narratívák védvonalait.[31]

J. M. Berger és Jonathon Morgan az Iszlám Állam (ISIS) tevékenységét vizsgálva alátámasztották, hogy a hálózatosodott szélsőségesség sikere a hiperaktív perszónahálózatok koordinált tevékenységén alapult.[32] Ez a jelenség a többségi látszat *(illusion of majority)* megteremtésével a validálási fázist a „társadalmi bizonyíték" *(social proof)* szintjére emelte. Resperger István hangsúlyozza, hogy a hibrid hadviselés ezen szakaszában a válságkezelési mechanizmusok hatékonyságát éppen ez a kognitív bizonytalanság ásta alá.[33] Rand Waltzman a kognitív biztonság *(cognitive security)* hiányával magyarázza e műveletek sikerét, ahol a „személyes vallomás" ereje képes volt felülírni a technikai cáfolatokat.[34]

Az iparszerű sablonizáció és az információs mosás folyamatai

A tartalomgyártás (*generation,* G) ebben a szakaszban még döntően manuális jellegű volt, azonban az információs mosás (*laundering,* L) fázisa már ipari léptékű sablonokat *(templates)* alkalmazott a dezinformáció legitimizálásához, megteremtve a befolyásolási műveletek fenntartható üzleti modelljét. A mosási fázis felelős azért, hogy a generált üzenet elveszítse közvetlen kötődését az eredeti forráshoz, és látszólag organikus információként jelenjen meg. Az ökoszisztéma kialakulásának ezen időszakában a fő innovációt a sablonizáció *(templating)* és a figyelemgazdaság *(attention economy)* mechanizmusainak tudatos kiaknázása jelentette.

Az Europol 2015-ös jelentése rávilágított, hogy a közösségi mérnökösködés *(social engineering)* technikái szoros szimbiózisba léptek a monetizációs ösztönzőkkel.[35] A kattintásvadász *(clickbait)* megoldások terjedése során olyan sablonizált tartalmi panelek jöttek létre, amelyek az érzelmi alapú hírfogyasztást célozták meg. A programozott hirdetésvásárlás *(programmatic advertising)* lehetővé tette, hogy a dezinformációs szereplők automatizált módon jussanak bevételhez, ahol a kattintásszám-alapú profit és a politikai hatáskiváltás kölcsönösen erősítette egymást.

A tartalmi mosás egyik leghatékonyabb eszköze a „mosási rétegsor" *(laundering stack)* kiépítése volt, amely ál helyi hírportálokból és hírgyűjtő (aggregátor) oldalakból állt. Marton Péter rámutat, hogy a médiarendszerek töredezettsége lehetővé tette a hírmosás *(news laundering)* sikeres végrehajtását, ahol a bizonytalan eredetű információ több

[30] NATO Strategic Communications Centre of Excellence 2015: 39–40.
[31] Marton 2018: 96.
[32] Berger, J. M. – Morgan, Jonathon (2015): *The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter*. Washington, D.C.: The Brookings Institution.
[33] Resperger 2018: 31.
[34] Waltzman, Rand (2017): *The Weaponization of Information. The Need for Cognitive Security*. Santa Monica: RAND, 3–4.
[35] Europol 2015: 37.

áttéten keresztül vált „hírértékűvé".[36] Resperger István kiemeli, hogy a támadó ebben a fázisban nem feltétlenül az igazság megdöntésére, hanem a bizonytalanság iparszerű fenntartására törekedett, amelyhez a sablonizált tartalomgyártás biztosította a szükséges volument.[37] Az adatvezérelt profilozás *(data-driven profiling)* korai formái pedig lehetővé tették, hogy a tartalmat a célcsoport pszichológiai profiljához igazítsák, tovább növelve a validálás sikerességét.[38]

Műveleti kiváltó okok és a hullámlogika dinamikája

Az FMK az információs ökoszisztéma kialakulását megelőző időszakban nem folytonos jelenlétként, hanem eseményvezérelt hullámokban *(wave-logic)* jelentkezett. Ezen információs hullámok műveleti kiváltó okait *(operational triggers)* a fizikai tér válsághelyzetei szolgáltatták. A hullámlogika alapvetése, hogy a támadás intenzitása és módszertana a válság jellegéhez igazodik: a hirtelen megugró információs igény olyan kognitív réseket nyit a társadalmi percepcióban, amelyek lehetőséget teremtenek a kognitív sérülékenység módszeres kihasználására.[39]

A kutatás négy fő kategóriába sorolja a kiváltó okokat, amelyek mentén a vizsgált korszak műveleti mintázatai rögzíthetők:

KONF (konfliktus): A 2014-es ukrajnai válság alátámasztotta, hogy a Krím félsziget annexiója során az információs hadviselés már a kinetikus hadmozdulatokkal szinkronizált, önálló műveleti dimenziót alkotott. Resperger István rámutat, hogy ebben a szakaszban a bizonytalanság fenntartása és a döntéshozatali ciklusok megbénítása volt az elsődleges cél, építve a reflexív kontroll *(reflexive control)* gyakorlatára.[40]

EÜ (egészségügyi): A 2014-es ebolajárvány szolgált alapul az infodémia *(infodemic)* mintázatainak rögzítéséhez. A *British Medical Journal* elemzése rávilágított, hogy az orvosi dezinformáció *(medical misinformation)* terjedési sebessége gyakran meghaladta a hiteles szakmai tájékoztatását, ami a validálás kudarcán keresztül közvetlen károkat okozott.[41]

MIG (migrációs): A 2015-ös európai migrációs válság során a dezinformáció a társadalmi polarizáció *(social polarization)* és az intézményi bizalom eróziójának eszközévé vált.[42] Ebben a hullámban rögzült az operatív eltolódás a zárt csoportok irányába, ahol a hitelesítés már a visszhangkamra-hatáson *(echo chamber effect)* alapult, megnehezítve a hatósági monitorozást.

SZAB (szabályozási): Az intézményi immunválasz kezdetét a 2015. márciusi európai tanácsi következtetések jelentették, amelyek elvezettek az East StratCom Task Force

[36] Marton 2018: 95.
[37] Resperger 2018: 31.
[38] Information Commissioner's Office: *Investigation into the Use of Data Analytics in Political Campaigns*. [online], 2018. 11. 06. Forrás: ICO [2026. 06. 17.].
[39] Marton 2018: 95–96.
[40] Resperger 2018: 31.
[41] Oyeyemi, Sandra – Gabarron, Elia – Wynn, Rolf (2014): Ebola, Twitter, and Misinformation. A Dangerous Combination? *BMJ,* 349, g6178.
[42] Svetoka 2016: 47–48.

felállításához.[43] Ez a lépés jelezte az ökoszisztéma-építés előtti korszak lezárulását és a dezinformáció elleni védekezés doktrinális prioritássá emelését.[44]

A kiválasztott események operatív elemzése

A 2013. április 23-i Associated Press-incidens az FMK alacsony eszközigényű, magas reputációs hatású paradigmaesete. Az aktor a szíriai állami érdekeket képviselő Syrian Electronic Army (SEA) volt – ideológiai vállalkozói profil, amelyet a szír állami hírszerzés közvetve irányított, de közvetlen állami irányítást nem lehetett bizonyítani. A platform: az AP hivatalos Twitter-fiókja, amelynek hozzáférési adatait *phishing* útján szerezték meg. A konkrét művelet: a fiókból egyetlen hamis *tweetet* posztoltak – „Breaking: Two Explosions in the White House and Barack Obama is Injured" – amely 23 percig volt látható. A G–M–T–V-láncon belül a súlypont a validálás (V) fázisán volt: a tartalom generálása minimális erőforrást igényelt, de az AP tekintélyének hitelességbitorlása révén a befogadói szűrők kritika nélkül engedték át az üzenetet. A Dow Jones-index 143 pontot esett percek alatt, igazolva, hogy az algoritmikus médiarendszerben a forrás hitelessége képes helyettesíteni a tényszerűséget.

A 2014-es ukrajnai Krím-annexió az FMK első, teljes G–M–T–V-láncot alkalmazó, állami szintű művelete. Az aktor az orosz katonai hírszerzés (GRU) által koordinált trollfarmhálózat volt, amelyet a kijevi Euromajdan-tüntetések elleni narratívák generálására aktiváltak. A platform: VKontakte- és Twitter-koordinált módon, kiegészítve orosz állami és álhírportálok hálózatával. A konkrét művelet: több száz, „helyi szemtanú" maszkban működő álprofil egyidejűleg posztolt a krími szeparatista önvédelmi csapatok legitimitásáról, a NATO-csapatmozgások fenyegetéséről és az ukrán kormány nácipárti jellegéről. A NATO StratCom COE dokumentálta, hogy a terjesztés (T) és a validálás (V) fázisa volt a legintenzívebb: az egyszerre több forrásból érkező, egymást erősítő narratívák a többségi látszat illúzióját teremtették meg, miközben az információs mosás (M) a VK-n virális megosztásokon és orosz hírportálokon keresztül zajlott.

Az ebolajárvány (2014) idején kibontakozó infodémia az FMK ideológiai vállalkozói típusának tankönyvi esete. Az aktorok nem egy koordinált állami apparátus, hanem szétszórt, monetizációs és ideológiai motivációjú szereplők hálózata volt: természetgyógyász szervező oldalak, összeesküvés-elméleti profilok és „jóindulatú tanácsadó" maszkban működő közösségimédia-fiókok. A platform elsősorban Twitter és Facebook volt. Oyeyemi, Gabarron és Wynn BMJ-elemzése dokumentálta, hogy az ebolajárvány csúcsán a releváns tweetek több mint 40%-a félrevezető vagy teljesen hamis egészségügyi információt tartalmazott – hamis gyógymódokat, oltásellenes narratívákat és összeesküvés-elméleteket. A G–M–T–V-láncon belül a súlypont a validálás (V) fázisán volt: a „jóindulatú tanácsadó" perszóna a befogadói bizalmat csapolja le úgy, hogy az üzenet látszólag nem politikai, hanem egészségügyi segítségnyújtásként érkezik. A terjesztési sebesség rendszeresen meghaladta a WHO hivatalos kommunikációjáét.

---

[43] *Európai Tanács (2015. március 19–20.) – Következtetések (ST 11/15)*. Brüsszel: Európai Tanács.

[44] *Questions and Answers about the East StratCom Task Force*. [online], 2021. 10. 27. Forrás: European External Action Service [2026. 01. 10.].

A 2015-ös európai migrációs válság az FMK zárt csoportokba szorított, validációorientált alkalmazásának prototípusa. Az aktorok részben orosz állami érdekeket képviselő proxyszervezetek, részben organikus ideológiai vállalkozók voltak; a *Political Capital* és a *Svetoka* szerkesztette NATO StratCom COE-jelentés egyaránt dokumentálta mindkét típus jelenlétét. A platform: zárt Facebook-csoportok és Twitter. A konkrét műveletek: koordinált álprofilok manipulált képeket, valótlan statisztikákat (például hamis bűnügyi adatokat) és uszító tartalmakat terjesztettek zárt, jobboldali tematikájú Facebook-csoportokban, ahol a visszhangkamra-logika megakadályozta a cáfolat behatolását. A G–M–T–V-láncon belül az információs mosás (M) és a terjesztés (T) fázisa volt a súlypont: a tartalmak több álhírportálon és privát csoporton keresztül jutottak el a végfelhasználóhoz, mire a hatósági monitorozás reagálni tudott. Ez a hullám rögzítette az operatív eltolódást a nyilvános platformoktól a nehezebben monitorozható zárt digitális terek irányába.

A fegyvernek minősülő kommunikációs műveletek operatív bázisértékei

A kognitív hadviselés operatív küszöbe

Az FMK műveleti küszöbe az a határ, ahol az információ áramlása kilép a hagyományos meggyőzés kereteiből, és stratégiai szintű befolyásolási műveletté transzformálódik. Ez az operatív küszöb *(operational threshold)* az a választóvonal, amely felett a kognitív hadviselés *(cognitive warfare)* már nem csupán a véleményformálást célozza, hanem a célközönség valóságérzékelését és döntéshozatali autonómiáját támadja. A 2013–2015-ös időszak tapasztalatai alátámasztják, hogy ez a küszöbérték nem technológiai, hanem rendszerszintű és kognitív tényezők függvénye.

Resperger István a válságkezelés és a hibrid hadviselés összefüggéseit vizsgálva rámutat, hogy az információs műveletek célja a bizonytalanság szisztematikus fenntartása.[45] Az operatív bázisérték *(baseline)* alátámasztja, hogy a kognitív hadviselés operatív küszöbe a döntéshozatali ciklusok *(OODA-loop)* sebességaszimmetriájának kihasználásával léphető át. Amennyiben a dezinformáció terjedése és befogadása – a kulturális rezonancia miatt – gyorsabb, mint az intézményi ellenőrzés és cáfolat képessége, kognitív bénultság *(cognitive paralysis)* következhet be.

Az operatív küszöb átlépését az információs ökoszisztéma kialakulása során a „hazugság tűzoltótömlője" *(firehose of falsehood)* modell tette lehetővé, amely a mennyiségi elárasztás útján erodálta az objektív igazságba vetett hitet.[46] Ez a mechanizmus igazolja, hogy a kulturálisan illesztett, de auditálható forrásmegjelölés nélküli információ olyan aktív fegyverré válik, amely képes a társadalmi kohézió megbontására és stratégiai meglepetés okozására. A 2013–2015-ös bázisértékek technológiai skálázásának egyik legtisztább példája a 2021-ben feltárt Operation Ghostwriter (UNC1151), amely az AP-incidensben

[45] Resperger 2018: 31.
[46] Paul–Matthews 2016: 2.

rögzített hitelességbitorlás logikáját állami szintre emelte: feltört tisztviselői közösségi-média-profilokból terjesztett hamis katonai tartalmakat Lengyelország és a balti államok célközönségének.[47]

Az intézményi immunválasz és a szabályozási vákuum

A fegyvernek minősülő kommunikáció ökoszisztémájának kialakulását megelőző korszak lezárultát a demokratikus intézményrendszer felismerése és az arra adott első, rendszerszintű válaszreakció jelölte ki. 2013 és 2015 között a támadó szereplők egyfajta szabályozási vákuumban *(regulatory vacuum)* tevékenykedtek, ahol a nemzetközi jogi keretek még nem kezelték prioritásként az információs térben zajló destabilizációs törekvéseket. Ez az átmeneti védettségi hiány tette lehetővé a kognitív hadviselés eszköztárának zavartalan fejlesztését.

A fordulatot az Európai Tanács 2015. márciusi csúcstalálkozója hozta el, amelynek következtetései politikai szinten rögzítették az igényt az orosz dezinformációs kampányokkal szembeni közös fellépésre. Ez a dokumentum az európai intézményi immunválasz *(institutional immune response)* alapkövének tekinthető.[48] Ennek közvetlen operatív következményeként jött létre az East StratCom Task Force, amelynek feladata a dezinformáció monitorozása és a tényalapú narratívák erősítése lett.[49]

Az intézményi válasz megjelenése rávilágított a kognitív biztonság megteremtésének nehézségeire is. Míg a támadó szereplők a hihető tagadás *(plausible deniability)* elve mentén mozogtak, addig az állami válaszreakcióknak a demokratikus alapértékek és a transzparencia keretei között kellett maradniuk. Resperger István hangsúlyozza, hogy a válságkezelés ezen új dimenziójában a stratégiai kommunikáció a nemzeti reziliencia részévé vált.[50] Az East StratCom Task Force létrehozása tehát lezárta a gátlástalan műveleti kísérletezés időszakát, és megnyitotta az utat a 2016-tól datált, tudatosabb védekezéssel kísért iparosítás időszaka felé.

Összefoglalás és következtetések

A hipotézisek és kutatási kérdések értékelése

A kutatás mindhárom hipotézisét megerősítette. H1: Az FMK műveleti rutinjai – online profilmaszkolás, koordinált amplifikáció, hálózati sűrűség – már 2015-re teljeskörűen rögzültek, függetlenül a későbbi automatizációtól. H2: A támadási lánc súlypontja a terjesztési (D) és a validálási (V) fázisokra esett, kihasználva a médiarendszerek hibriditását és a kulturális közelséget. H3: A 2013–2015-ös hullámdinamika közvetlen hatással volt az intézményi védekezési stratégiákra: az East StratCom Task Force létrehozása igazolta, hogy az FMK nemzetbiztonsági prioritássá vált. A vizsgált időszak operatív bázisértékként

[47] Paul–Matthews 2016: 2.
[48] *Európai Tanács (2015. március 19–20.) – Következtetések (ST 11/15).*
[49] *Questions and Answers about the East StratCom Task Force* 2021.
[50] Resperger 2018: 31.

(baseline) azonosítható: a 2016 utáni, mesterséges intelligencia által skálázott dezinformációs műveletek ezekre az örökölt rutinokra épültek.

Korlátok és jövőbeli irányok

A kutatás egyik legjelentősebb korlátja a visszatekintő vizsgálatoknál tapasztalható adatgyűjtési aszimmetria, amely a platformarchívumok töredékességéből fakad. A jövőbeli kutatások számára a kognitív biztonság *(cognitive security)* területén a manuális bázisértékek *(baseline values)* és az MI-alapú automatizáció közötti interakciók vizsgálata jelölheti ki az irányt. A védekezési stratégiáknak a technológiai moderáción túlmutatva a társadalmi ellenálló képesség *(social resilience)* és az intézményi bizalommenedzsment *(trust management)* megerősítésére kell fókuszálniuk, megvalósítva egy többrétegű védelmi stratégiát *(multi-layered defense strategy)*.

Felhasznált irodalom

Allenby, Brad – Garreau, Joel: *Weaponized Narrative: The New Battlespace.* [online], 2017. 01. 03. Forrás: Defense One [2026. 01. 26.].

Arquilla, John – Ronfeldt, David (1993): Cyberwar is Coming! *Comparative Strategy,* 12(2), 141–165. Online: https://www.doi.org/10.1080/01495939308402915

Berger, J. M. – Morgan, Jonathon (2015): *The ISIS Twitter Census: Defining and Describing the Population of ISIS Supporters on Twitter.* Washington, D.C.: The Brookings Institution. Online: https://www.brookings.edu/wp-content/uploads/2016/06/isis_twitter_census_berger_morgan.pdf

du Cluzel, François: *Cognitive Warfare*. [online], 2021. Forrás: innovationhub-act.org [2026. 01. 10.].

Európai Tanács (2015. március 19–20.) – Következtetések (ST 11/15). [online], 2015. Forrás: Európai Tanács [2026. 01. 10.].

Europol (2015): *The Internet Organised Crime Threat Assessment (iOCTA) 2015.* Hága: Europol. Online: https://doi.org/10.2813/03524

George, Alexander L. – Bennett, Andrew (2005): *Case Studies and Theory Development in the Social Sciences*. Cambridge: MIT Press.

Horváth Dávid (2026): *A fegyvernek minősülő kommunikáció operatív alaprétegei*. (Interpretáció).

Information Commissioner's Office: *Investigation Into The Use Of Data Analytics In Political Campaigns.* [online], 2018. 11. 06. Forrás: ICO [2026. 06. 17.].

Juhász, Attila – Szicherle, Patrik (2017): *The Political Effects of Migration-Related Fake News, Disinformation and Conspiracy Theories in Europe*. Budapest: Political Capital – Friedrich-Ebert-Stiftung.

Lewandowsky, Stephan – Cook, John – Lombardi, Doug (2020): *The Debunking Handbook 2020.* [H. n.]: [K. n.]. Online: https://doi.org/10.17910/b7.1182

Marton Péter (2018): A hibrid hadviselés előfordulásának feltételeiről. *Nemzet és Biztonság,* 11(3), 95–105. Online: https://www.matarka.hu/klikk.php?cikkmutat=3138019&mutat=http://www.nemzetesbiztonsag.hu/cikkek/nb_2018_3_09_marton.pdf

Matos Alves, Artur de: *A Short History of Online Platform Transparency*. [online], 2023. 02. Forrás: demontages.phl-lab.uliege.be [2026. 01. 10.].

NATO Strategic Communications Centre of Excellence (2015): *Analysis of Russia's Information Campaign against Ukraine.* Riga: NATO StratCom COE. Online: https://stratcomcoe.org/cuploads/pfiles/russian_information_campaign_public_12012016fin.pdf

Oyeyemi, Sandra – Gabarron, Elia – Wynn, Rolf (2014): Ebola, Twitter, and Misinformation: A Dangerous Combination? *BMJ,* 349, g6178. Online: https://doi.org/10.1080/01495939308402915

Paul, Christopher – Matthews, Miriam: *The Russian „Firehose of Falsehood" Propaganda Model.* [online], 2016. 07. 11. Forrás: RAND [2026. 06. 17.].

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

Questions and Answers about the East StratCom Task Force. [online], 2021. 10. 27. Forrás: European External Action Service [2026. 01. 10.].

Resperger István (2018): *A válságkezelés és a hibrid hadviselés*. Budapest: Dialóg Campus. Online: https://bit.ly/4gqRvMd

Straubhaar, Joseph D. (1991): Beyond Media Imperialism: Asymmetrical Interdependence and Cultural Proximity. *Critical Studies in Mass Communication,* 8(1), 39–59. Online: https://doi.org/10.1080/15295039109366779

Svetoka, Sanda szerk.: *Social Media as a Tool of Hybrid Warfare.* [online], 2016. 07. 07. Forrás: NATO StratCom [2026. 01. 10.].

Voss, Chris – Raz, Tahl (2016): *Never Split the Difference: Negotiating as if Your Life Depended on It.* New York: HarperBusiness.

Waltzman, Rand (2017): *The Weaponization of Information: The Need for Cognitive Security.* Santa Monica: RAND. Online: https://doi.org/10.7249/CT473

Woolley, Samuel C. – Howard, Philip N. szerk. (2018): *Computational Propaganda. Political Parties, Politicians, and Political Manipulation on Social Media.* Oxford: Oxford University Press. Online: https://doi.org/10.1093/oso/9780190931407.001.0001

World Health Organization: *Ebola at End-2014: Getting to Zero. Special Session of the Executive Board on the Ebola Emergency.* [online], 2015. 01. 19. Forrás: WHO [2026. 01. 10.].