Hadtudományi Szemle
19. évfolyam (2026) 1. szám 141–156. • DOI: 10.32563/hsz.2026.1.8

Horváth Dávid[1]

A kommunikációs fenyegetések kezelése a kritikusinfrastruktúra-szektorokban

Managing Information-Driven Threats in Critical Infrastructure Sectors

Absztrakt

A tanulmány kiindulópontja nem a szektorok felsorolása, hanem az a felismerés, hogy a megtévesztésre épülő kommunikáció képes a működési döntéseket torzítani, így ellátásbiztonsági zavarokhoz és bizalomvesztéshez vezetni. Magyarországi példákon vizsgálom, miként alakul ki a narratíva által kiváltott kockázat, amikor a hitelességi jelek manipulálása (márkautánzás, domainklónok, personaalapú közösségi támadások, audiovizuális hamisítás) és a csatornaátterjesztés együtt növeli az incidensek valószínűségét. Az értelmezési keret az OPC fogalma, de a fókusz a szervezett meggyőzés döntéstorzító mechanizmusain van, nem az „álhír" kategóriáján. A védekezést háromszintű, visszacsatolt gyakorlatként ragadom meg: felhasználói jelértelmezési készségek (mikroszint), szervezeti gyorsciklusú cáfolat és riasztás (mezoszint), valamint platform- és hatósági kooperációs protokollok (makroszint). Eredményeim szerint a kommunikációs fenyegetések kezelése ott hatékony, ahol a szolgáltatásfolytonosság mérőszámai összekapcsolódnak a tényellenőrzés és a válaszlépések mérhető idejével; e kapcsolat teszi lehetővé a reziliencia célzott növelését és a döntéshozatali zaj mérséklését.

Kulcsszavak: álhír, kritikus infrastruktúra, dezinformáció, hibrid hadviselés, információs műveletek

Abstract

Rather than offering a sectoral inventory, the paper starts from the recognition that deception-based communication can distort operational decision-making, producing

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola, e-mail: netminiszter@gmail.com, david@netokracia.hu

supply-security disruptions and loss of trust. Using Hungarian case vignettes, it examines how narrative-induced risk emerges when manipulation of credibility cues (brand impersonation, cloned domains, persona-based social attacks, audiovisual falsification) combines with cross-channel amplification to raise the likelihood of incidents. The analytical frame is organised persuasive communication (OPC), with emphasis on the decision-distorting mechanisms of organised persuasion rather than the narrower category of "fake news". Defence is conceptualised as a three-level, feedback-driven practice: user-level cue-interpretation skills (micro), organisational fast-cycle rebuttal and alerting (meso), and platform- and regulator-level cooperation protocols (macro). Findings indicate that communication threats are mitigated most effectively where service-continuity metrics are tied to measurable fact-checking and response times; this linkage enables targeted resilience gains and reduces decision-making noise.

Keywords: fake news, critical infrastructure, disinformation, hybrid warfare, information operations

Bevezetés

A korszerű ellátási rendszerek sérülékenysége ma már nem kizárólag műszaki vagy fizikai kockázatokból fakad: a megtévesztésre épülő kommunikáció képes a működtetők és a felhasználók döntéseit is elbillenteni. Amikor a bizalom infrastruktúrája meginog, a hiba nem feltétlenül a kábelben vagy a vezérlőben keletkezik, hanem a jelentésadás folyamatában: a terjedő narratívák döntéstorzítást válthatnak ki, amely végső soron szolgáltatásfolytonossági zavarokhoz vezethet.

A tanulmány azt vizsgálja, miként keletkezik és terjed a narratíva által kiváltott kockázat (narratívaindukált kockázat) a magyarországi környezetben. Kiindulópontunk, hogy a hitelességi jelek célzott manipulációja (márkautánzás, domainklónozás, personaalapú közösségi támadások, audiovizuális hamisítás) és a csatornaátterjesztés egymást erősítve képes növelni az incidensek valószínűségét. Az elemzési keret az *organized persuasive communication* (OPC) fogalma: nem az „álhír" szűk kategóriájára koncentrálunk, hanem a szervezett meggyőzés döntéstorzító mechanizmusaira, amelyek az információs műveletek (IO) logikájába illeszkednek.

A gyakorlat felől közelítünk: esetvázlatokkal mutatjuk be, hogyan fordíthatók át a kommunikációs ingerek működési kockázattá – a lakossági percepció változásától a vállalati incidenskezelés döntési pontjaiig. Külön figyelmet kapnak a jelmanipuláció elleni mintázatok (például vizuális/nyelvi „hitelességi" díszletek) és azok a platformdinamikák, amelyek rövid idő alatt képesek amplifikálni a félrevezető tartalmak hatását.

A védekezést háromszintű, visszacsatolt gyakorlatként értelmezzük. Mikroszinten a felhasználói jelértelmezési készségek döntik el, hogy a megtévesztő tartalom elakad-e. Mezoszinten a gyorsciklusú cáfolat és riasztás szabja meg, milyen hosszú ideig marad hatásban a téves narratíva. Makroszinten a platform- és hatósági kooperációs protokollok jelölik ki a beavatkozás ütemét és eszköztárát. E három szint akkor a leghatékonyabb, ha a rezilienciacélok és a válaszidő-metrikák mérhetően összekapcsolódnak a szolgáltatásfolytonosság indikátoraival.

Hozzájárulásunk kettős. Egyrészt fogalmi hidat építünk az OPC-alapú megközelítés és a kritikus szolgáltatások működtetési realitásai közé; másrészt bemutatjuk, hogyan illeszthető a kommunikációs kockázatkezelés a szervezeti döntéshozatal napi rutinjaihoz. Módszertanunk *structured-focused comparison:* minden esetre azonos kérdéskészletet alkalmazunk, és csak a tézishez szükséges változókra fókuszálunk. A cikk felépítése: 1. elméleti és módszertani háttér; 2. esettérkép és elemzés; 3. védekezési mintázatok és kooperációs protokollok; 4. következtetések és mérhető beavatkozási pontok.

A tanulmány szerkezete

Cikkemben először a releváns szakirodalom alapján kijelölöm a magyarországi kritikus infrastruktúrák körét, majd elkülönítem azokat a fegyvernek minősülő kommunikációs technikákat, amelyek kifejezetten közmű-, telekommunikációs és pénzügyi szereplők nevével, arculati elemeivel visszaélve célozzák az ügyfeleket; ezeket elhatárolom más megtévesztési formáktól. Ezt követően hazai esettanulmányokon mutatom be, hogyan szereznek adatot vagy anyagi javakat megtévesztő üzenetekkel, és milyen reziliencia-elemek (észlelés, riasztás, gyorsciklusú cáfolat) működnek a közintézményeknél, közszolgáltatóknál és piaci szereplőknél. A téma uniós szinten is kiemelt: az Európai Bizottság 2018-as dezinformáció-ellenes cselekvési terve a tagállami együttműködés erősítését és összehangolt válaszlépéseket ír elő.[2]

Elméleti keretek

Kritikus infrastruktúrák keretrendszere

Ebben a fejezetben a kritikus infrastruktúrák meghatározásának főbb megközelítéseit térképezem fel. A 2009-es *A kritikus információs infrastruktúrák meghatározásának módszertana* kiadvány a fogalom definíciós kérdéseit rendszerezi, és összeveti több állam és nemzetközi szervezet (például USA, Egyesült Királyság, EU, NATO) felfogását, majd összegzi a hazai gyakorlat sarokpontjait. A hivatkozott áttekintés alapján röviden bemutatom a Magyarországon akkor érvényes keretrendszert, kiemelve azokat az elemeket, amelyek a jelen tanulmány eseteinek értelmezéséhez szükségesek.

A 2112/2004. (V. 7.) Korm. határozat[3] a kritikus infrastruktúrák közé sorolja többek között az energiaellátást, a közműveket, a közlekedést-szállítást, a távközlést/elektronikus adatforgalmat és informatikai hálózatokat, a bankrendszert, a szolgáltatásokat, a médiát, az ivóvíz- és élelmiszer-ellátást, valamint az egészségbiztosítást. Ez a kör ugyanakkor – az uniós és több állami gyakorlatnál – nem tartalmazza a közigazgatást, a segélyszolgálatokat és a védelmi-készenléti szervezeteket. Ezt módosítva a 2080/2008. (VI. 30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról az ágazatokat már az alábbi fő csoportokba rendezi: energetika; infokommunikációs

[2] Európai Bizottság 2018; 2022.
[3] 2112/2004. (V. 7.) Korm. határozat a terrorizmus elleni küzdelem aktuális feladatairól.

technológiák; közlekedés; víz; élelmiszer; egészségügy; pénzügy; ipar; jogrend-kormányzat; közbiztonság-védelem.

A 2019-es kiadású *Kritikus infrastruktúrák védelme I.* című könyv szerzői (Bognár Balázs, Bonnyai Tünde és Vámosi Zoltán) a kritikus infrastruktúrák védelmének fontosságát hangsúlyozzák,[4] kiemelve azokat az infrastruktúrákat, amelyek elengedhetetlenek a társadalom biztonságos és zavartalan működéséhez. Az infrastruktúra értelmezése többféle szempontból is történik, figyelembe véve azokat az eszközöket, intézményeket és létesítményeket, amelyek nélkülözhetetlen feltételei a termelési és szolgáltatási folyamatoknak. A könyv alapján a kritikus infrastruktúrákat többek között az energetikai szektorban található elemek alkotják, mint a villamosenergia-termelés, átviteli és elosztó hálózatok, a kőolajipar és a földgázszállítás és -termelés. Ezek az infrastruktúrák kulcsfontosságúak a nemzetgazdaság és az állampolgárok mindennapi életének biztonságához, így védelmük kritikus fontosságú a nemzetbiztonság szempontjából. A villamosenergia-termelés esetében például azokat az elemeket tekintik kritikusnak, amelyek kiesése jelentős teljesítménycsökkenést okozna a belföldi villamosenergia-termelésben. Az átviteli hálózatban olyan elemek számítanak kritikusnak, amelyek kiesése esetén nem pótolható módon csökkenne a rendelkezésre álló teljesítmény. Az elosztó hálózat, a kőolajipar, a földgázszállítás és -termelés szintén tartalmaz olyan elemeket, amelyek kiesése súlyos hatással lenne az ország energiaellátására és gazdasági stabilitására. Összességében a mű a kritikus infrastruktúrák széles körét tárgyalja, különös tekintettel azokra az infrastruktúrákra, amelyek elengedhetetlenek az ország gazdasági stabilitásának és az állampolgárok biztonságának fenntartásához. Magyarországi és magyar vonatkozásban a kritikus infrastruktúra definiálását a szerzők szerint a hazai Zöld Könyv által megfogalmazottak írják le a legpontosabban:

> „kritikus infrastruktúrának minősülnek azon hálózatok, erőforrások, szolgáltatások, termékek, fizikai vagy információtechnológiai rendszerek, berendezések, eszközök és azok alkotó részei, melyek működésének meghibásodása, megzavarása, kiesése vagy megsemmisítése, közvetlenül vagy közvetetten, átmenetileg vagy hosszútávon súlyos hatást gyakorolhat az állampolgárok gazdasági, szociális jólétére, a közegészségre, közbiztonságra, a nemzetbiztonságra, a nemzetgazdaság és a kormányzat működésére."[5]

Lazari és Mikac könyvében részletesen foglalkozik az Európai Unió létfontosságú infrastruktúráinak védelmével. Elemzésük az EU azon törekvésére összpontosít, hogy hogyan védi meg azokat az infrastruktúrákat, amelyek létfontosságúak a tagállamok biztonsága, gazdasági stabilitása és az állampolgárok jóléte szempontjából. Általában az alábbi létfontosságú infrastruktúrákat tekintik kritikusnak az EU-ban:

- Az energia-infrastruktúra, beleértve az elektromos hálózatokat, gázvezetékeket és olajvezetékeket, amelyek létfontosságúak a mindennapi élet fenntartásához, a gazdaság működéséhez és az országok közötti energiaellátás biztonságához.
- A közlekedési infrastruktúra, mint a repülőterek, kikötők, vasúti és közúti hálózatok, amelyek kulcsfontosságúak az emberek és áruk mozgásának biztosításában,

[4] Bognár–Bonnyai 2019: 36, 42.

[5] Zöld könyv a kritikus infrastruktúrák védelmére vonatkozó nemzeti programról. A Kritikus Infrastruktúra Védelem Nemzeti Programjáról szóló 2080/2008. (VI. 30.) kormányhatározat 1. sz. melléklete.

valamint az EU belső és külső kereskedelmében. Az információs és kommunikációs technológia (IKT) infrastruktúrák, beleértve az internetet, a telekommunikációs hálózatokat és az adatközpontokat, amelyek nélkülözhetetlenek a modern társadalom működéséhez, az információáramláshoz és a kritikus szolgáltatások fenntartásához.
- A vízellátás és -kezelés infrastruktúrái, beleértve a víztisztító és -szétosztó rendszereket, amelyek létfontosságúak az emberi egészség, higiénia és az ökoszisztémák védelme szempontjából.
- Az élelmiszer-ellátási lánc, beleértve a mezőgazdasági termelést, feldolgozást és disztribúciót, ami kulcsfontosságú az élelmiszer-biztonság és az állampolgárok élelmezésének biztosítása szempontjából.
- Az egészségügyi infrastruktúra, beleértve a kórházakat, laboratóriumokat és gyógyszerellátási láncokat, ami létfontosságúak az emberi élet védelme és a betegségek elleni küzdelem szempontjából.

A *The External Dimension of the European Union's Critical Infrastructure Protection Programme: From Neighbouring Frameworks to Transatlantic Cooperation* című írásban Lazari és Mikac az Európai Unió *Kritikus Infrastruktúra Védelmi Program*jának (CIP) külső dimenzióival foglalkoznak,[6] különös tekintettel arra, hogy az EU hogyan működik együtt nemzetközi partnereivel és harmadik országokkal a kritikus infrastruktúrák védelme érdekében. Az alábbiakban vázolok egy általános keretet, amely segíthet megérteni, milyen témákat és kérdéseket tárgyalnak a kritikus infrastruktúrák globális dimenziójában:
- A nemzetközi együttműködés jelentősége fontos, a kritikus infrastruktúrák védelme ugyanis globális kihívás, amely nem korlátozódik egyetlen ország vagy régió határaira. Az EU együtt dolgozik más országokkal, nemzetközi szervezetekkel és többoldalú fórumokkal a közös biztonsági kihívások kezelése érdekében.
- Kiemelt a közös stratégiák kidolgozása, így az EU és nemzetközi partnerei közötti stratégiák és politikák kidolgozása, amelyek célja a kritikus infrastruktúrák védelmének összehangolása, beleértve a legjobb gyakorlatok megosztását, a kockázatkezelési módszerek harmonizálását és a válaszadási kapacitások fejlesztését.
- Nélkülözhetetlen a jogi és szabályozási különbségek kezelése. A különböző jogi és szabályozási rendszerek kihívásokat jelentenek az együttműködésben, és ezeket az akadályokat le kell küzdeni.
- Fókuszban vannak a jövőbeli együttműködési lehetőségek és azok a területek, ahol további erőfeszítésekre van szükség a kritikus infrastruktúrák globális védelmében.

Összességében a *The External Dimension of the European Union's Critical Infrastructure Protection Programme: From Neighbouring Frameworks to Transatlantic Cooperation* című írás átfogóan elemezi az EU kritikus infrastruktúrák védelmében végzett nemzetközi

[6] Lazari–Mikac 2022.

együttműködésének stratégiáit, kihívásait és lehetőségeit, különös tekintettel arra, hogy ez a munka hogyan járul hozzá a globális biztonsághoz és stabilitáshoz.

A hibrid hadviselés

A hibrid hadviselésben a fizikai, kiber- és információs műveletek egymást erősítve célozzák a döntéshozatalt és a közbizalmat, miközben a médiatér önálló műveleti környezetté válik. Szun-ce már több mint két évezreddel ezelőtt megfogalmazta, hogy minden háború a megtévesztésen alapul.[7] Ma ez a logika a dezinformáció, az álhír-ökoszisztéma és a hitelességi jelek manipulációja révén érvényesül:[8] personaalapú megtévesztések, klónozott felületek és célzott terjesztési mechanizmusok befolyásolják a percepciót. A digitális térben mindezt gyakran kísérik összehangolt kiberműveletek (például túlterheléses támadások), amelyek átmeneti szolgáltatáskiesést idézhetnek elő, s ezzel felerősítik a kommunikációs hatást. Az adathalász kampányok és hamis riasztások további kockázatot jelentenek a nagy rendszerekre és a társadalmi stabilitásra, a politikai nyomásgyakorlás pedig a narratívák szintjén zárja össze a hatásláncot.

Fegyvernek minősülő kommunikációs technikák és taktikák, avagy az álhírek

Nincs egységes, minden helyzetre alkalmazható „álhír-definíció"; a jelenséget egy tágabb ernyőfogalom, a szervezett meggyőző kommunikáció (*organized persuasive communication,* OPC) keretében tárgyalom, amely a befolyásolási gyakorlatokat – többek között propagandát, PR-t és marketinget – közös rendszerbe rendezi.[9] A dezinformációt az Európai Bizottság olyan igazolhatóan hamis vagy félrevezető közlésként írja le, amelyet haszon- vagy szándékos megtévesztési céllal állítanak elő és terjesztenek, s amely a közérdeket sértheti; a tévedések, szatírák és nyíltan pártkötődésű közlések nem ide tartoznak.[10] A félretájékoztatás ezzel szemben szándéktól függetlenül terjesztett hamis információ,[11] míg a rosszindulatú torzítás *(malinformation)* valós tények kártékony célú terjesztése.

A befolyásolás intézményes módozatai közül a PR klasszikus értelmezését Bernays munkája szemlélteti,[12] a marketing pedig a célcsoportigények kielégítésére szolgáló marketingmix szervezőelve köré rendeződik.[13] A propaganda célja a megismerés, attitűd és viselkedés irányítása; megkülönböztethető „fehér", „szürke" és „fekete" változata – az önfeltártság és igazságtartalom viszonya szerint.[14]

[7] Szun-ce 2020.
[8] Aro 2016.
[9] Bakir et al. 2019.
[10] European Commission 2018.
[11] The Britannica Dictionary [é. n.].
[12] Bernays 2019 [1923].
[13] Kotler–Levy 1969.
[14] Jowett–O'Donnell 2011: 7.

A kritikus infrastruktúrák szempontjából e kategóriák nem elméleti finomságok: a *weapon-grade* (fegyvernek minősülő) kommunikációs eljárások konkrét műveleti kockázatot teremtenek (hitelességi jelek manipulálása, csatornaamplifikáció), amelyet az OPC-keret segít rendszerezni.

Dezinformációból félretájékoztatás, avagy a viralitás természete

Az NMHH tájékoztatása szerint az sms-, spam- és e-mail-alapú megtévesztő tartalmak tiltottak. Ide sorolhatók azok a megoldások is, amelyek a felhasználók befolyásolására, illetve életkori vagy fogyatékosságból eredő sebezhetőségük kihasználására épülnek. Tilosak továbbá a személyek „megbízhatóságát" értékelő/osztályozó alkalmazások, ha ez hátrányos megkülönböztetést eredményez. Az ilyen álhírek terjesztése és manipulatív használata súlyos következményekkel járhat.

Ugyanakkor az NMHH nem sorolja közvetlenül az sms-, spam- és e-mail-tartalmakat az álhírek kategóriájába. Ezeket a kommunikációs formákat inkább a kéretlen hirdetésekkel kapcsolatos problémaként kezeli,[15] és tanácsokat ajánl a felhasználóknak a védekezés leghatékonyabb módjairól, mint például a levélszűrők használata. A hatóság jogköre csak a természetes személyeknek küldött elektronikus hirdetésekkel kapcsolatos bejelentések kezelésére terjed ki.

Tehát a szándékoltan hamis információkat tartalmazó sms-ek és e-mailek, egyéb csetüzenetek mint disztribúciós felület, vagyis terjesztési csatorna állnak rendelkezésre, de ide sorolható a közösségi média is, azon belül álhírek linkjeit tartalmazó posztok, azok terjesztésére alkalmas csoportok. A már megtévesztett és lelkes felhasználók maguk terjesztik a hamis információt, álhírt, amely ekkor már jóindulatú, de félretájékoztatásként funkcionál.

Esetek az álhír fajtáira és felhasználási módjára a kritikus infrastruktúrák elleni támadáskor

A kritikus infrastruktúrák területén az álhírek és dezinformáció különböző módon okozhatnak pánikot és társadalmi befolyásolást.

Az energiaellátás területén hamis hírekkel az energiahiányról vagy katasztrófákról befolyásolhatják az energiaárakat vagy okozhatnak pánikvásárlást. Amikor kibertámadás érte a Colonial Pipeline-t,[16] egy úgynevezett *ransomware* támadás 2021-ben, az esemény az egyik legjelentősebb kibertámadás volt az amerikai energia-infrastruktúra történetében. A DarkSide *ransomware* csoport támadása során a Colonial Pipeline egy alkalmazottja felfedezett egy zsarolóvírust, ami miatt a cég leállította az üzemanyag-szállítást, napi több mint 2,5 millió hordó finomított benzint érintve. Az eseményről szóló hírek hosszú üzemanyagsorokat és pánikvásárlást okoztak

[15] Nemzeti Média- és Hírközlési Hatóság [é. n.].
[16] Vojinovic 2023.

az Egyesült Államok keleti partján, ami jelentős üzemanyaghiányt és áremelkedést eredményezett. De ebbe a körbe sorolható még általánosságban a hamis információk terjedése a megújuló energiáról. A megújuló energiaforrások, mint a nap- és szélenergia kapacitásainak félreértelmezése gyakori célpontja a dezinformációs kampányoknak, amelyek azt állítják, hogy ezek a technológiák önmagukban nem képesek fenntartani az energiaellátást. Ezek a hamis állítások befolyásolhatják a közvéleményt és a politikai döntéshozatali folyamatokat, potenciálisan gátolva a zöldenergia fejlesztését. Dezinformáció-kampányok a vízenergia-projektekről is vannak. Hamis hírek terjedhetnek egyes nagy vízenergia-projektekről, amelyek állítólag káros hatással lehetnek a környezetre és a helyi közösségekre. A téves információk erős ellenállást válthatnak ki, ami befolyásolhatja a projektek előrehaladását és a kapcsolódó politikai támogatást.

A vízellátás és vízkezelés területén a téves információk a vízminőségről vagy -szennyeződésről pánikot kelthetnek a lakosság körében. 2018-ban a Donbasz vízellátásának mérgezési összeesküvése is erről szólt.[17] Egy proorosz hackercsoport, a CyberBerkut állította, hogy Ukrajna nukleáris hulladékkal akarja mérgezni a Donbasz régió vízellátását, és ezt az amerikai titkosszolgálatokkal karöltve tervezik megvalósítani. Ezeket az állításokat széles körben terjesztették orosz médiumok, de később kiderült, hogy a történet teljes mértékben kitalált volt.

A közlekedés területén a dezinformáció az infrastruktúra állapotáról vagy balesetekről is zavart okozhat a közlekedési és ellátási láncokban. Például 2019-ben az Egyesült Királyságban terjedtek hamis jelentések közlekedési balesetekről a közösségi médiában, amelyek valójában nem történtek meg, mégis zavart keltettek az utazási döntésekben, és aláásták a közlekedési rendszerekbe vetett bizalmat.[18] Ez a típusú hamis információ fokozza a közlekedési láncok sebezhetőségét, és növeli a kockázatot a közlekedési infrastruktúra szempontjából. Más hamis hírek a közlekedési infrastruktúráról, például hidak és alagutak állapotáról terjesztettek téves információkat,[19] ami negatívan befolyásolta az emberek biztonságérzetét és a közlekedési tervezést. Amikor hamis jelentések terjedtek tömegközlekedési sztrájkokról, amelyek valójában nem történtek meg,[20] zavart okoztak az utasok között, és potenciálisan aláásták a közlekedési szolgáltatásokba vetett bizalmat.

Magyarországon a Magyar Telekom az egyik legnagyobb telekommunikációs szolgáltató. A vállalat biztosítja a mobil- és vezetékes telefon, valamint az internetszolgáltatásokat, amelyek alapvető fontosságúak a kommunikációs infrastruktúra szempontjából. 2019-ben több esetben is előfordult, hogy hamis számlákat küldtek ki a Magyar Telekom nevében, amelyek valósnak tűnő logókkal és formátummal rendelkeztek. Ezek a számlák arra ösztönözték az embereket, hogy fizessenek olyan szolgáltatásokért, amelyeket valójában nem vettek igénybe. 2020-ban *phishing e-mailek* terjedtek a Magyar Telekom nevében, amelyek célja az volt, hogy megszerezzék a felhasználók személyes és banki adatait. Ezek az e-mailek gyakran tartalmaztak megtévesztő linkeket, amelyek a felhasználókat hamis bejelentkezési oldalakra irányították. 2021-ben a közösségi médiában hamis közlemények jelentek meg, amelyek arról számoltak be,

[17] Fake: Kyiv to Poison Donbas Water Supply and Blame Russia 2018.
[18] Bekker-Nielsen 2021.
[19] Baptista–Gradim 2020.
[20] Columbia SPS 2024.

hogy a Magyar Telekom bizonyos szolgáltatásait ingyenesen biztosítja a pandémia ideje alatt. Ezek az információk zavart okoztak az ügyfelek körében és megnövelték a vállalatra nehezedő nyomást.

Léteznek hamis információk egészségügyi válságokról vagy gyógyszerek hatékonyságáról, amelyek torzíthatják a közegészségügyi rendszereket. A WHO jelentése szerint az infodémiák és az egészségügyi téves információk súlyosan befolyásolják az emberek mentális egészségét, növelik a vakcinaellenességet, és késleltetik az egészségügyi ellátást. Ez a fajta dezinformáció jelentős mértékben növeli az egészségügyi krízisek során az egészségügyi intézkedésekkel szembeni ellenállást, ami hátrányosan befolyásolja a közegészségügyi válaszokat.[21] A DelveInsight jelentése[22] szerint az egészségügyi ágazatban terjedő hamis hírek, különösen a vakcinákkal kapcsolatos téves információk, jelentősen növelik a vakcinázással szembeni ellenállást. Az ilyen típusú hamis hírek befolyásolják a betegek döntéshozatalát, késleltetik a szükséges orvosi kezelést, és felesleges kiadásokat okozhatnak. A pandémia alatt terjedő hamis hírek jelentősen növelték a vakcinaellenességet.[23] Ezek a téves információk gyakran nem tudományos forrásokból származtak, és különböző tévhiteket terjesztettek a vakcinák hatékonyságáról és biztonságáról, ami globálisan akadályozta a vakcinázási erőfeszítéseket és növelte a közegészségügyi válság súlyosságát.

Téves információk pénzügyi válságról vagy a bankrendszer instabilitásáról pánikeladásokhoz vezethetnek a piacokon. A Yale Egyetem kutatása[24] kimutatta, hogy a befektetési weboldalakon megjelenő promóciós cikkek, amelyeket gyakran hamis hírként közzétevő PR-cégek írnak, ideiglenesen megemelhetik a kisvállalatok részvényárait. Ezek az írások sok esetben megtévesztők lehetnek, és ha elegendő befektető vásárol részvényeket a hamis hírek alapján, az árfolyam emelkedhet, majd a piaci korrekció hatására visszaeshet. 2019-ben a Metro Bank részvényárfolyama jelentősen esett, miután WhatsAppon és Twitteren hamis pletykák terjedtek arról, hogy a bank az összeomlás szélén áll, és az ügyfeleknek azonnal ki kellene venniük a pénzüket. Ez a pánik jelentős hatással volt a bank részvényárára és általánosan is rontotta a pénzügyi szektorba vetett bizalmat.[25] Egy hamis „Kedves Ügyvezető Igazgató" levél, amely állítólag a BlackRock vezérigazgatójától származott, számos médiumban megjelent és valótlan állításokat tartalmazott az assetmenedzsmentcég tevékenységéről. Ez a levél hamis információkat terjesztett, és jelentős zavart okozott a piacon, ami példázza, hogy a hamis hírek milyen könnyen befolyásolhatják a pénzügyi piacokat.[26]

Álhírekkel az élelmiszer-biztonságban is ellátási zavarokat és pánikvásárlást lehet okozni. A Covid–19-járvány idején széles körben terjedtek hamis információk arról, hogy élelmiszerhiányok lesznek, ami több helyen pánikvásárlást indított el. Ez a jelenség többletkeresletet generált bizonyos alapvető élelmiszerek iránt, ami időszakos hiányokhoz és áremelkedésekhez vezetett, különösen a tartós élelmiszerek piacán.[27] A génmódosított szervezetekkel (GMO) kapcsolatos hamis információk szintén

[21] WHO 2022.
[22] DelveInsight 2021.
[23] Gagnon-Dufresne et al. 2023.
[24] Niessner 2018.
[25] Nish–Naumaan–Muir 2020.
[26] Nish–Naumaan–Muir 2020.
[27] Komócsin–Csernátony 2021; Felix et al. 2020.

befolyásolták a fogyasztói magatartást. Bizonyos hamis állítások szerint a GMO-élelmiszerek egészségügyi kockázatokat jelentenek, ami növelte a GMO-mentes termékek iránti keresletet, annak ellenére, hogy a tudományos közösség általánosságban biztonságosnak találta ezeket a termékeket.[28] Hogy hogyan befolyásolhatják az élelmiszer-fogyasztási szokásokat a félrevezető információk, jó példa a mikrohullámmal pattogatott kukorica fogyasztásával kapcsolatos tévhitek terjedése. Hamis hírek szerint a mikrohullámmal pattogatott kukorica fogyasztása komoly egészségügyi kockázatokkal jár, ami az értékesítés csökkenéséhez vezetett, bár tudományos bizonyítékok ezt nem támasztották alá.[29]

Álhíreket lehet terjeszteni a kormányzati válaszokról vagy vészhelyzeti intézkedésekről, amelyek befolyásolhatják a lakosság reakcióit és a társadalmi rendet. Ezek a példák azt mutatják, hogy az álhírek jelentős zavart okozhatnak a kritikus infrastruktúrák működésében, ami közvetlen hatással van a társadalomra és a gazdaságra. A brexit folyamata során a hamis hírek jelentős hatást gyakoroltak a közvéleményre, és befolyásolták a szavazók döntéseit, különösen az Egyesült Királyság Európai Unióból való kilépésének politikai és gazdasági következményeivel kapcsolatban. A félrevezető információk között szerepeltek téves állítások a brexit gazdasági előnyeiről, amelyek a valós tényekkel ellentétben álltak.[30] Az USA-ban a 2016-os elnökválasztási ciklus alatt terjedő hamis hírek számos alkalommal befolyásolták a politikai diskurzust. Ezek a hírek gyakran a jelöltekkel és politikai kérdésekkel kapcsolatos téves információkat tartalmaztak, amelyek célja a nyilvános vélemény manipulálása volt. A hamis hírek nemcsak a választói magatartást befolyásolták, hanem az amerikai demokratikus intézményekbe vetett bizalmat is aláásták.[31] 2018-ban az Egyesült Államokban több iskolát, kormányépületet és rendőrségi központot ért hamis bombariadó, amelyek híre a közösségi médián terjedt. Ezek az álhírek azonnali pánikot és evakuálásokat okoztak, és jelentős erőforrásokat vontak el a hatóságoktól, amelyek így valós veszélyhelyzetek kezelésére kevésbé voltak felkészülve. Ezek az incidensek rámutatnak arra, hogy a hamis információk milyen gyorsan és széles körben terjedhetnek, komoly zavart okozva az állami funkciókban.[32]

Nagy teljesítményű szerverparkok működését is meg lehet zavarni, amelyek weboldalak, felhőalapú szolgáltatások és nagy adatmennyiségek tárolását biztosítják. Hamis hírek terjedtek a Google és a Facebook adatközpontjainak állítólagos környezeti hatásairól, amelyek azt állították, hogy ezek az adatközpontok jelentős mértékben hozzájárulnak a helyi vízhiányhoz és energiafogyasztáshoz. Ezek a téves információk növelték a helyi lakosság és politikusok aggodalmait, és ellenállást váltottak ki az új adatközpontok építésével szemben, különösen vízhiányos területeken, mint például Arizona és Utah.[33] 2018-ban hamis hír terjedt el egy Facebook-adatközpont elleni kibertámadásról és annak leállásáról, ami pánikot okozott a felhasználók körében, és növelte a Facebook részvényeinek volatilitását. A hír később hamisnak bizonyult, de

[28] Petratos–Faccia 2023.
[29] Petratos–Faccia 2023.
[30] Rodny-Gumede 2018.
[31] Ordway 2017.
[32] Morrow 2019.
[33] Gonzales 2022.

addigra már jelentős kárt okozott a vállalat imázsában és a piaci bizalomban.[34] Az NSA Utah adatközpontjáról szóló hamis hírek szerint az intézmény hatalmas mennyiségű vizet használ fel, ami a helyi vízhiányhoz vezetett. Ezek a hírek feszültségeket szítottak a helyi lakosság körében és ellenállást váltottak ki az adatközpont működésével szemben. Az NSA később cáfolta ezeket az állításokat, de addigra már jelentős közösségi ellenállás alakult ki.[35]

Reziliencia és tudatos tartalomfogyasztás

Az álhír elleni fellépés intézményrendszere

Annak ellenére, hogy az álhírek a média térnyerésével csak az utóbbi években kezdtek el komolyabb, újfajta veszélyforrássá válni, már léteznek intézményi törekvések a megfékezésükre. A *Magyar Nemzeti Biztonsági Stratégia* 68. pontja így fogalmaz:

> „Az állami és nem állami szereplők által szponzorált politikai, gazdasági és társadalmi folyamatok befolyásolására irányuló stratégiák száma, változatossága és hatásfoka növekszik. A befolyásolás egyik eszköze lehet a nemzetközi közvélemény szervezett és módszeres Magyarország ellen hangolása. Az információs műveletek hatásfokát az emeli, hogy az álhírek a közösségi platformokon villámgyorsan képesek eljutni a célközönséghez. A befolyásolási technikák a politikai térben és az üzleti döntéshozatalban egyaránt nyomásgyakorló szerepet kaphatnak, amely során az ellenérdekelt nemzetközi szereplők korlátozni próbálhatják hazánk cselekvőképességét."[36]

A NATO 2018 óta stratégiai prioritásként kezeli azokat az álhírjelenségeket, amelyek a hibrid fenyegetések körébe tartoznak.[37] Ehhez szükséges és kívánatos intézményrendszert építtett ki:

- Hibrid Fenyegetéseket Elhárító Európai Kiválósági Központ (The European Centre of Excellence for Countering Hybrid Threats) Helsinkiben, a nem NATO-tag Finnországban jött létre, és az Európai Unióval közösen működtetik;
- Stratégiai Kommunikációs Kiválósági Központ (Strategic Communications Centre of Excellence) Rigában, Lettországban;
- Kibervédelmi Együttműködési Kiválósági Központ (Cooperative Cyber Defence Centre of Excellence) Tallinnban, Észtországban.

[34] Linklaters [é. n.].
[35] Gonzales 2022.
[36] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról 2107.
[37] NATO's Response to Hybrid Threats.

Az Európai Unió védelem okán történt fellépése a kritikus infrastruktúrákért

Az Európai Unió a kritikus infrastruktúrák védelmét, beleértve a kockázatkezelést, a reziliencia építését és a tagállamok közötti együttműködést az alábbi politikákkal és intézkedésekkel közelíti meg:

- Jogszabályok és szabályozások: az EU különféle jogszabályokat és szabályozásokat fogadott el a kritikus infrastruktúrák védelmének megerősítésére. Ezek közé tartozik a kritikus infrastruktúra védelméről szóló irányelv, amely előírja a tagállamok számára, hogy azonosítsák és védelmezzék azokat az infrastruktúrákat, amelyek elengedhetetlenek a társadalom és a gazdaság számára.
- Kockázatkezelés: az EU hangsúlyozza a kockázatkezelési stratégiák alkalmazását, amely magában foglalja a fenyegetések, sebezhetőségek és a potenciális hatások felmérését. A cél az, hogy csökkentsék az infrastruktúrák elleni támadások vagy természeti katasztrófák valószínűségét és hatásait.
- Reziliencia építése: az EU a reziliencia építését prioritásként kezeli, ami a kritikus infrastruktúrák ellenálló képességének növelését jelenti váratlan eseményekkel szemben. Ez magában foglalja az újjáépítési és helyreállítási tervek kidolgozását, valamint a redundancia és sokféleség biztosítását az infrastruktúra elemeiben.
- Közös válaszmechanizmusok: az EU ösztönzi a tagállamok közötti együttműködést a közös válaszmechanizmusok kialakításában, ami segít a határokon átnyúló fenyegetések kezelésében. Ez magában foglalja az információmegosztást, a legjobb gyakorlatok cseréjét és a közös gyakorlatok lebonyolítását.
- Tudatosság és képzés: az EU fontosnak tartja a tudatosság növelését és a képzést a kritikus infrastruktúra védelme terén. Ez magában foglalja az érdekelt felek tájékoztatását a legújabb fenyegetésekről, valamint azok képzését, akik felelősek a kritikus infrastruktúrák védelméért.
- Nemzetközi együttműködés: miközben az EU ösztönzi a tagállamok közötti együttműködést, szintén hangsúlyozza a nemzetközi együttműködés fontosságát, különösen azokkal az országokkal és szervezetekkel, amelyekkel közösen a kritikus infrastruktúrák védelmében érdekelt.

Hazai civil és hivatalos védekezés az álhírekkel szemben

Magyarországon több platform és jó gyakorlat is működik, amelyek célja az álhírek gyors bejelentése és az ilyen jellegű információk terjedésének megakadályozása. Az *Urban Legends* magyar nyelvű weboldal a közösségi médiában és az interneten terjedő álhírek, összeesküvés-elméletek és *hoaxok* leleplezésével foglalkozik. Az oldal rendszeresen publikál cikkeket, amelyek elemzik és cáfolják a terjedő hamis információkat.[38] Az NMHH is foglalkozik a médiában terjedő álhírek kezelésével.

[38] Lásd: https://www.urbanlegends.hu/

A hatóság rendszeresen figyeli a médiatartalmakat, és jelentéseket készít az álhírek terjedéséről. Bár nem közvetlenül az álhírek bejelentésére szolgáló platform, szerepe fontos a dezinformáció elleni küzdelemben. Ezek a platformok és gyakorlatok segítik az álhírek gyors bejelentését és a közvélemény tájékoztatását a hamis információk elleni küzdelemben. Fontos, hogy a lakosság is aktívan részt vegyen ebben a folyamatban, és kritikusan kezelje a médiában megjelenő tartalmakat.

Egyéni védekezés az álhírekkel szemben

Az EPRS szerint a legelső lépés a tartalom, a szerző, a forrás és a képi bizonyítékok külön ellenőrzése; megosztás előtt érdemes a saját érzelmi elfogultságot is tudatosítani.[39] Az NMHH kutatásai arra figyelmeztetnek, hogy a puszta forráskritika nem mindig elég: az is számít, hol és hogyan ellenőrizzük az információt.[40] Gyakorlati jelzők azonosításához az NMHH útmutatója ajánl listát (például szenzációhajhász cím, régi/hamis illusztráció, ismeretlen domain, szerző és hivatkozások átláthatatlansága, kirívó helyesírás, hirdetéstúlsúly) – ezek együttese különösen gyanús.[41] Uniós szinten a 2019–2024-es stratégiai menetrend a polgárok védelmét és a hibrid fenyegetések kezelését tűzi ki,[42] a dezinformáció elleni lépések fókusza az összehangolt megelőzés, közös fellépés és a reziliencia erősítése.[43]

Összegzés

A felsorolt cégek gyakorlataiból kiderült, hogy hiába próbálkoznak mind fellépni a kiberbiztonsági veszélyekkel szemben, mégis egyfajta tehetetlenségben vannak. Az ügyfelek edukációját sokkal inkább előtérbe kell helyezni, azonban kellenek újabb formák a figyelem fenntartására, hogy ne vesszen el az üzenet. Emellett megfelelő, célszerűen kialakított platformokat kell biztosítani az esetleges visszaélések gyors bejelentésének lehetőségére. Nagy segítség minden cégnek, hogy a sajtó szereti felkapni a negatív és sok kattintást hozó információkat, így a csalásokról való beszámolás még mindig húzó témának számít. Azonban az információ eljutásának gyorsasága kritikus: sokkal jobb lenne minél előbb közzétenni a visszaéléseket, még mielőtt a csalássorozat hulláma a csúcsára ér, de ez nem mindig kivitelezhető. Az egy-egy szektoron belül lévő versenytársak összefogása és tudásmegosztása a kiberbiztonság érdekében lehet a legnagyobb előny.

[39] Európai Parlament 2019.
[40] Nemzeti Média- és Hírközlési Hatóság 2021.
[41] Nemzeti Média- és Hírközlési Hatóság 2022.
[42] Európai Tanács 2019.
[43] Európai Tanács 2020.

Felhasznált irodalom

1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról
2112/2004. (V. 7.) Korm. határozat a terrorizmus elleni küzdelem aktuális feladatairól
Aro, Jessikka (2016): The Cyberspace War: Propaganda and Trolling as Warfare Tools. *European View,* 15(1), 121–132. Online: https://doi.org/10.1007/s12290-016-0395-5
Bakir, Vian et al. (2019): Organized Persuasive Communication: A New Conceptual Framework for Research on Public Relations, Propaganda and Promotional Culture. *Critical Sociology,* 45(3), 1–18. Online: https://doi.org/10.1177/0896920518764586
Baptista, João Pedro – Gradim, Anabela (2020): Understanding Fake News Consumption: A Review. *Social Sciences,* 9(10), 185. Online: https://doi.org/10.3390/socsci9100185
Bekker-Nielsen, Tønnes (2021): Fake News from the Past – Lessons For the Future. *Public History Weekly,* 2021. december 9. Online: https://public-history-weekly.degruyter.com/9-2021-10/fake-news-from-the-past-lessons-for-the-future/
Bernays, Edward L. (2019) [1923]: *Crystallizing Public Opinion.* New York: Liveright. Online: https://www.gutenberg.org/files/61364/61364-h/61364-h.htm
Bognár Balázs – Bonnyai Tünde szerk. (2019): *Kritikus infrastruktúrák védelme I.* Budapest: Dialóg Campus. Online: http://hdl.handle.net/20.500.12944/12450
Columbia SPS (2024): *The Real Impact of Fake News: The Rise of Political Misinformation and How We Can Combat Its Influence.* Online: https://sps.columbia.edu/news/real-impact-fake-news-rise-political-misinformation-and-how-we-can-combat-its-influence
DelveInsight (2021): *Fake News in the Healthcare Sector. A Misinformation Crisis in the Era of Digitalization.* Online: https://www.delveinsight.com/blog/fake-news-in-the-healthcare-sector
Európai Bizottság (2018): *A dezinformáció elleni 2018. évi cselekvési terv.* Online: https://ec.europa.eu/info/publications/action-plan-disinformation-commission-contribution-european-council-13-14-december-2018_hu
Európai Bizottság (2022): *Küzdelem a dezinformáció ellen.* Online: https://www.consilium.europa.eu/hu/policies/coronavirus/fightingdisinformation/
Európai Parlament (2019): *Hogyan ismerjük fel az álhíreket?* Online: https://www.europarl.europa.eu/RegData/etudes/ATAG/2017/599386/EPRS_ATA(2017)599386_HU.pdf
Európai Tanács (2019): *A 2019–2024-es időszakra szóló új stratégiai menetrend.* Online: https://www.consilium.europa.eu/media/39917/a-new-strategic-agenda-2019-2024-hu.pdf
Európai Tanács (2020): *A Tanács következtetései a reziliencia megerősítéséről és a Covid–19-világjárvány összefüggésében felmerülő hibrid fenyegetések, többek között a dezinformáció elleni küzdelemről.* Online: https://data.consilium.europa.eu/doc/document/ST-14064-2020-INIT/hu/pdf
European Commission (2018): *Communication from The Commission to The European Parliament, The Council, The European Economic and Social Committee and The Committee of The Regions.* COM (2018) 236 final. Online: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018DC0236

Fake: Kyiv to Poison Donbas Water Supply and Blame Russia (2018). *Stopfake.org,* 2018. augusztus 28. Online: https://www.stopfake.org/en/fake-kyiv-to-poison-donbas-water-supply-and-blame-russia/

Felix, Ignacio et al. (2020): US Food Supply Chain: Disruptions and Implications from COVID-19. *McKinsey and Company,* 2020. július 2. Online: https://www.mckinsey.com/industries/consumer-packaged-goods/our-insights/us-food-supply-chain-disruptions-and-implications-from-covid-19

Gagnon-Dufresne, Marie-Catherine et al. (2023): Social Media and the Influence of Fake News on Global Health Interventions: Implications for a Study on Dengue in Brazil. *International Journal of Environmental Research and Public Health,* 20(7), 5299. Online: https://doi.org/10.3390/ijerph20075299

Gonzales, Steven (2022): Inside the Physical Footprint of the Cloud. *Popular Science,* 2022. február 14. Online: https://www.popsci.com/environment/data-centers-environmental-impacts/

Jowett, Garth S. – O'Donnell, Victoria (2011): *Propaganda and Persuasion.* SAGE. Online: https://csmeyns.github.io/propaganda-everyday/pdf/odonnell-jowett-2018-what-is-propaganda.pdf

Komócsin Sándor – Csernátony Csaba (2021): Visszatér pánikvásárlás, kiürülnek a polcok az áruházakban. *Economx,* 2021. szeptember 26. Hozzáférés: https://www.economx.hu/nemzetkozi-gazdasag/buksza-vasarlas-hiany-koronavirus-jarvany-bolt.737122.html

Kotler, Philip – Levy, Sidney J. (1969): Broadening the Concept of Marketing. *Journal of Marketing,* 33(1), 10–15. Online: https://doi.org/10.1177/002224296903300103

Lazari, Alessandro – Mikac, Robert szerk. (2022): *The External Dimension of the European Union's Critical Infrastructure Protection Programme: From Neighbouring Frameworks to Transatlantic Cooperation.* Boca Ranton: CRC Press. Online: https://doi.org/10.4324/9781003273769

Linklaters [é. n.]: *The Impact of Fake News. Part of Our Series on Tackling Erosion of Trust and the Spread of Fake News.* Online: https://web.archive.org/web/20220125020906/www.linklaters.com/en/insights/publications/crisis-ready/crisis-ready/tackling-erosion-of-trust-and-the-spread-of-fake-news/the-impact-of-fake-news

Morrow, Shawn (2019): Social and News Media's Effects on Law Enforcement. *Global Journal of Forensic Science & Medicine,* 4(1). Online: https://irispublishers.com/gjfsm/pdf/GJFSM.MS.ID.000516.pdf

NATO's Response to Hybrid Threats. Online: https://www.nato.int/cps/en/natohq/topics_156338.htm

Nemzeti Média- és Hírközlési Hatóság (2021): *NMHH-kutatás: Védekeznénk az álhírekkel szemben, de ez nem mindig sikerül.* Online: https://nmhh.hu/cikk/224768/NMHHkutatas_Vedekeznenk_az_alhirekkel_szemben_de_ez_nem_mindig_sikerul

Nemzeti Média- és Hírközlési Hatóság (2022): *Élesedik az álhírek elleni küzdelem: mi sem maradhatunk ki belőle.* Online: https://nmhh.hu/cikk/229831/Elesedik_az_alhirek_elleni_kuzdelem_mi_sem_maradhatunk_ki_belole

Nemzeti Média- és Hírközlési Hatóság [é. n.]: *Spam és kéretlen e-mailes hirdetések bejelentése.* Online: https://nmhh.hu/cikk/187271/Spam_es_keretlen_emailes_hirdetesek_bejelentese

Niessner, Marina (2018): Does Fake News Sway Financial Markets? *Yale Insights,* 2018. június 27. Online: https://insights.som.yale.edu/insights/does-fake-news-sway-financial-markets

Nish, Adrian – Naumaan, Saher – Muir, James (2020): Enduring Cyber Threats and Emerging Challenges to the Financial Sector. *Carnegie Endowment for International Peace,* 2020. november 18. Online: https://carnegieendowment.org/research/2020/11/enduring-cyber-threats-and-emerging-challenges-to-the-financial-sector?lang=en

Ordway, Denise-Marie (2017): Fake News and the Spread of Misinformation. A Research Roundup. *The Journalist's Resource,* 2017. szeptember 1. Online: https://journalistsresource.org/politics-and-government/fake-news-conspiracy-theories-journalism-research/

Petratos, Pythagoras – Faccia, Alessio (2023): Fake News, Misinformation, Disinformation and Supply Chain Risks and Disruptions: Risk Management and Resilience Using Blockchain. *Annals of Operations Research,* 327, 735–762. Online: https://doi.org/10.1007/s10479-023-05242-4

Rodny-Gumede, Ylva (2018): Fake It till You Make It. The Role, Impact and Consequences of Fake News. In Mutsvairo, Bruce – Karam, Beschara (szerk.): *Perspectives on Political Communication in Africa.* Cham: Palgrave Macmillan, 203–219. Online: https://doi.org/10.1007/978-3-319-62057-2_13

Szun-Ce (2020): *A háború művészete.* Ford. Tokaji Zsolt. Budapest: Helikon.

The Britannica Dictionary [é. n.]: *Misinformation.* Online: https://www.britannica.com/dictionary/misinformation

Vojinovic, Ivana (2023): *Critical Infrastructure Cyber Attacks. A New Form of Warfare.* DataProt, 2023. július 14. Online: https://dataprot.net/articles/critical-infrastructure-cyber-attacks/

WHO (2022): *Infodemics and Misinformation Negatively Affect People's Health Behaviours, New Who Review Finds.* Online: https://www.who.int/europe/news/item/01-09-2022-infodemics-and-misinformation-negatively-affect-people-s-health-behaviours--new-who-review-finds

Zöld könyv a kritikus infrastruktúrák védelmére vonatkozó nemzeti programról. A Kritikus Infrastruktúra Védelem Nemzeti Programjáról szóló 2080/2008. (VI. 30.) kormányhatározat 1. sz. melléklete.