Lukács Bence

Dezinformációs támadások társadalmi hatásai, lehetséges ellenintézkedések azonosítása

Bevezetés

A digitális kommunikációs platformok elterjedése az információs hadviselés egy típusának, a dezinformációs támadásoknak a reneszánszát hozta, amelyek jelentős fenyegetést jelentenek az egyénekre, szervezetekre és társadalom egészére. A jelen szakirodalmi összefoglaló célja, hogy átfogó áttekintést nyújtson a dezinformációs támadásokról, feltárva a különböző támadástípusokat, az alkalmazott taktikákat és a javasolt ellenintézkedéseket. A meglévő kutatások szintetizálásával ez a dokumentum hozzájárul a dezinformáció fejlődésének megértéséhez, és betekintést nyújt káros hatásainak mérséklésébe.

Az információs korszak beköszöntével soha nem látott mértékű összekapcsolódás jött létre, de a rosszindulatú szereplők számára is új lehetőségeket teremtett az információterjesztés sebezhetőségének kihasználására. A dezinformáció, amelyet a hamis vagy félrevezető információk szándékos terjesztése jellemez, erőteljes eszközzé vált azok kezében, akik a közvélemény manipulálására, a politikai eredmények befolyásolására és az intézményekbe vetett bizalom aláásására törekszenek. Emellett a dezinformáció definíciójának kiterjesztése a történelmi, hatalmi és politikai dimenziókra is, rávilágít a hatalmi hierarchiák megerősítésére szolgáló elsődleges médiastratégiaként való használatára, hangsúlyozva a kritikai dezinformációs tanulmányok

fontosságát a dezinformáció hatásának megértésében és az ellene való küzdelemben.[1]

A dezinformáció a félretájékoztatás és az álhírek előfordulása jelentősen megnőtt az elmúlt években, amely szignifikáns hatást gyakorol a társadalmakra.[2] A dezinformáció az egyének szándékos megtévesztésére előállított hamis vagy a valóságtól eltérő környezetbe ágyazott információ, míg a félretájékoztatás hamis és/vagy félrevezető információként definiálható.[3] A dezinformáció lehet kiberművelet (hackelés) vagy nyílt tevékenység (hamis információ terjesztése).[4] Az álhíreknek több definíciója létezik, általánosságban elmondható, hogy az interneten hírformátumban megjelenő hamis történetek, melyek célja a szándékos félrevezetés és/vagy egyéb haszonszerzés tekinthetők álhíreknek.

1. Dezinformációs támadások jellemzői

1.1 Támadástípusok

A dezinformációs támadások kifejezés számos olyan szándékos manipulatív taktikát foglal magában, amelyek célja az egyének és rendszerek megtévesztése és félrevezetése.[5] A dezinformációt

1 Rachel Kuo – Alice Marwick: Critical disinformation studies: History, power, and politics, *Harvard Kennedy School Misinformation Review*, 2021. 2.4: 1–11.

2 Pythagoras N. Petratos – Alessio Faccia: Fake news, misinformation, disinformation and supply chain risks and disruptions: risk management and resilience using blockchain, *Annals of Operations Research*, 2023. 1–28.

3 Hunt Allcott – Matthew Gentzkow: Social media and fake news in the 2016 election, *Journal of economic perspectives*, 2017. 31.2: 211–236.

4 Pythagoras N. Petratos: Misinformation, disinformation, and fake news: Cyber risks to business, *Business Horizons*, 2021. 64.6: 763–774.

5 Mahmoud Abbasi, et al.: Security in the Internet of Things Application Layer: Requirements, Threats, and Solutions, *IEEE Access*, 2022. 10: 97197–97216.

többek között hibrid eszközként használják a demokratikus államok érdekei és polgáraik biztonsága elleni támadásra.[6] Jellemzője a célzott megtévesztés, amely gyakran magában foglalja az információk gyártását vagy manipulálását konkrét politikai célok elérése érdekében.[7] Emellett a dezinformációs támadásokról ismert, hogy a közösségi médiaplatformokat használják fel, ami egyre nagyobb igényt támaszt az olyan mesterséges intelligenciaeszközök iránt, amelyek képesek az ilyen támadások korai szakaszában történő azonosítására és az azokra való reagálásra.[8]

1.2 Taktikák

A támadók a dezinformációs kampányokban különböző taktikákat alkalmaznak céljaik eléréséhez. E taktikák közé tartozik a hamis vagy félrevezető információk terjesztése, a közvélemény manipulálására szolgáló számítógépes propaganda alkalmazása, valamint a társadalmon belüli viszály és polarizáció megteremtése.[9] A dezinformációs támadások magukban foglalhatják az

6 Dávid Kollár, et al.: Dezinformácie ako kľúčová bezpečnostná výzva súčasnosti v kontexte rusko-ukrajinského konfliktu, *Politické vedy*, 2022. 25.3: 87–109.

7 Michael Hameleers, et al.: Mistake or manipulation? Conceptualizing perceived mis-and disinformation among news consumers in 10 European countries, *Communication Research*, 2022. 49.7: 919–941.

8 Barry Cartwright, et al.: Detecting and responding to hostile disinformation activities on social media using machine learning and deep neural networks, *Neural Computing and Applications*, 2022. 34.18: 15141–15163.

9 Joao VS Ozawa, et al.: How Disinformation on WhatsApp Went From Campaign Weapon to Governmental Propaganda in Brazil, *Social Media+ Society*, 2023. 9.1: 20563051231160632.

álhírek terjesztését és a közösségi média használatát is a megtévesztő narratívák felerősítésére, amelyek gyakran konkrét közösségeket céloznak meg vagy politikai zavargásokat szítanak.[10] Egy a Twitter-en végzett felmérés alapján az álhírek jobban és gyorsabban terjednek, mint a valós hírek, az álhírek retweetelése (újramegosztása) akár 70%-kal valószínűbb, mint a valós híreknél.[11]

A személyre szabható internetes szolgáltatások (pl. közösségi médiák) szűrői korlátozhatják az új tartalmak megjelenését, így a fogyasztó figyelmen kívül hagyja (személyes szándékán kívűl is) az eltérő nézőpontokat, ami a saját előítéleteit növelheti.[12] Figyelembe véve, hogy az emberek az identitásukat, ideológiájukat részesítik előnyben, mint az attól eltérő véleményeket, ez a jelenség veszélyesnek tekinthető.[13] A közösségi média személyre szabott tartalmai a felhasználók meggyőződéseinek megerősítésében nagy szerepet játszanak, a szűrőbuborékok (filter-bubbles) és a visszhangkamrák (echo chambers) jelenségek révén. A szűrőbuborékok lényegében, olyan algoritmusok, amelyek a felhasználó által kedvelt tartalmakhoz hasonló tartalmakkal próbálják fenntartani a felhasználó figyelmét. A visszhangkamrák jelensége a felhasználók által kiválasztott személyek, csoportok, tartalmak követése által jön létre, tehát a kiválasztott tartalmakkal ellen-

10 Michael Hameleers: The (un) intended consequences of emphasizing the threats of mis-and disinformation, *Media and Communication*, 2023. 11.2: 5–14.

11 Soroush Vosoughi – Deb Roy – Sinan Aral: The spread of true and false news online, *Science*, 2018. 359.6380: 1146–1151.

12 Jonathan Clarke, et al.: Fake news, investor attention, and market reaction, *Information Systems Research*, 2020. 32.1: 35–52.

13 Cameron Martel – Gordon Pennycook – David G. Rand: Reliance on emotion promotes belief in fake news, *Cognitive research: principles and implications*, 2020. 5: 1–20.

tétes tartalmak megjelenése erősen korlátozott, amely elősegíti a saját vélemény folytonos megerősítését.[14]

A támadók továbbá olyan taktikákat alkalmazhatnak, mint a hamisítás és a megtévesztő kommunikációs technikák használata a célpontok megtévesztése és manipulálása érdekében.[15]

Ezek a kampányok gyakran a dezinformáció szándékos és stratégiai felhasználását jelentik politikai, társadalmi vagy ideológiai célok elérése érdekében, mind belföldön, mind nemzetközi szinten.[16] A támadók emellett kifinomult technikákat alkalmazhatnak, beleértve a számítási módszerek és a mesterséges intelligencia használatát a dezinformáció hatásának maximalizálása és a közvélemény manipulálása érdekében. E taktikák ellen különösen nagy kihívás, mivel gyakran kihasználják a közösségi média és a digitális kommunikációs platformok összekapcsolt jellegét, hogy széles közönséget érjenek el és befolyásoljanak.[17] A dezinformációs támadások taktikáinak megértése kulcsfontosságú a dezinformáció hatásának mérséklésére és a káros hatások elleni védelemre irányuló hatékony stratégiák kidolgozásához.

14 Samuel C. Rhodes: Filter bubbles, echo chambers, and fake news: how social media conditions individuals to be less critical of political misinformation, *Political Communication*, 2022. 39.1: 1–22.

15 Martin Innes – Diyana Dobreva – Helen Innes: Disinformation and digital influencing after terrorism: Spoofing, truthing and social proofing, *Contemporary Social Science*, 2021. 16.2: 241–255.

16 Martin Innes, et al.: The normalisation and domestication of digital disinformation: On the alignment and consequences of far-right and Russian state (dis) information operations and campaigns in Europe, *Journal of Cyber Policy*, 2021. 6.1: 31–49.

17 Aaron Erlich, et al.: Does analytic thinking insulate against pro-Kremlin disinformation? Evidence from Ukraine, *Political Psychology*, 2023. 44.1: 79–94.

1.3 Ellenintézkedések

A dezinformációs támadások megelőzésére és kezelésére számos stratégia és megközelítés létezik. Ilyen a tényellenőrző (fact-checking) újságírás a hamis információk terjesztése elleni kulcsfontosságú enyhítő eszköz. A tényellenőrzők releváns újságírói együttműködéseket és stratégiákat hoztak létre a dezinformáció elleni küzdelem érdekében.[18] A főbb ellenintézkedések közé tartoznak továbbá a számítási módszerek és a mesterséges intelligencia alkalmazások a közösségi médiaplatformokon megjelenő dezinformáció felderítésére és mérséklésére.[19]

A dezinformációs támadások elleni hatékony fellépéshez elengedhetetlen a különböző érdekelt felek bevonásával megvalósított sokoldalú stratégia. Mindenekelőtt a médián belüli műveltség és az oktatási kezdeményezések előmozdítása kulcsfontosságú, hogy az egyének képessé váljanak az információforrások kritikus értékelésére, az állítások tényellenőrzésére és az elfogult tartalmak kiszűrésére. Emellett a jó hírű tényellenőrző szervezetek támogatása elengedhetetlen az információk ellenőrzéséhez és a hamis állítások leleplezéséhez. Kulcsfontosságú az online platformok átláthatóságának és elszámoltathatóságának szorgalmazása, beleértve az algoritmusokra, a tartalom moderálására vonatkozó irányelvekre és a politikai hirdetésekre vonatkozó információk közzétételét. Állami oldalról továbbá a kormányok szerepet játszhatnak a hamis információkat szándékosan terjesztőkre vonatkozó jogi következményekkel járó szabályozások

18 Luisa Martínez-García – Iliana Ferrer: Fact-Checking Journalism: A Palliative Against the COVID-19 Infodemic in Ibero-America, *Journalism & Mass Communication Quarterly*, 2023. 100.2: 264–285.

19 Noémi Bontridder – Yves Poullet: The role of artificial intelligence in disinformation, *Data & Policy*, 2021. 3: e32.

meghozatalával és betartatásával. Nemzeti és nemzetközi szinten egyaránt szükség van az együttműködésre az információk, erőforrások és a dezinformáció elleni küzdelem legjobb gyakorlatainak megosztása érdekében. A közösségi médiaplatformoknak szigorú irányelveket kell érvényesíteniük, beleértve a tényellenőrzési mechanizmusokat és a tartalom moderálását, míg az algoritmikus megoldások felhasználhatók a dezinformáció terjedésének felderítésére és korlátozására. További intézkedéseket jelenthet a polgárok ösztönzése a gyanús tartalmak aktív bejelentésére, a sokszínű médiatér előmozdítása és a dezinformációs kampányok elleni válságkommunikációs tervek kidolgozása. A közvéleményt tudatosító kampányok, a digitális infrastruktúra védelmét szolgáló kiberbiztonsági intézkedések, valamint a felelős újságírói gyakorlatok – beleértve a pontos tudósításokat és az etikai normákat – előmozdítása szerves részét képezik ennek az átfogó stratégiának. Ezek az ellenintézkedések együttesen az információs ökoszisztéma megerősítését és a hamis narratívák társadalomra gyakorolt hatásának mérséklését célozzák.[20]

A nemcsak oktatási tevékenységgel való védekezés rávilágít annak fontosságára, hogy a digitális korban a dezinformáció jelentette kihívások kezelése érdekében ki kell használni a technológiai fejlődést. Az információbiztonsággal összefüggésben a hatékony sebezhetőség-ellenőrzés és a funkcióellenőrzés ellenintézkedései, például a javítás és a vírusvédelem, kritikus szerepet játszanak a támadások előrehaladásának korai szakaszban történő megállításában. Ezen túlmenően a támadások összetettségének növelése és a titkosítási algoritmusok elleni hibatámadások megelőzése érdekében olyan hibavédelmi technikák alkalmazása javasolt, mint a hamis körök és a konzisztenciaellenőrzéssel

20 Xichen Zhang – Ali A. Ghorbani: An overview of online fake news: Characterization, detection, and discussion, *Information Processing & Management*, 2020. 57.2: 102025.

ellátott redundáns számítások alkalmazása. A kriptográfia területén az állandó idejű titkosítás javasolt a távoli gyorsítótár időzítési támadások ellenintézkedéseként, ami jól mutatja a különböző kibertámadásokkal szemben ellenálló kriptográfiai technikák kifejlesztésének fontosságát. Emellett a robusztus kiberfizikai rendszerek alkalmazása és az irányítórendszerek elleni támadások meghiúsításához szükséges feltételek megfogalmazása aláhúzza a proaktív védelmi mechanizmusok jelentőségét a kritikus infrastruktúra dezinformációs alapú fenyegetésekkel szembeni védelmében.[21]

1.4 Hatások

A közösségi médián és online platformokon keresztül terjesztett dezinformáció bizonyítottan befolyásolja a közvélemény megítélését és meggyőződését, ami potenciálisan olyan valós következményekhez vezethet, mint a belföldi terrorizmus.[22] A félretájékoztatás és dezinformáció hatásainak ellensúlyozására stratégiai kommunikációs beavatkozások javasoltak, amelyek enyhítik az ilyen események által kiváltott szélesebb körű közkárokat. Továbbá a dezinformáció szándékos terjesztése bizonyítottan valós következményekkel jár az emberek hiedelmeire és viselkedésére nézve, amint azt COVID-19 járvány kitörése is bizonyította.[23] A politikai elitek által használt álhír-diskurzusoknak való kitettség csökkentheti az emberek valós információkba

21 Saeed Jamalzadeh, et al.: Weaponized disinformation spread and its impact on multi-commodity critical infrastructure networks, *Reliability Engineering & System Safety*, 2023. 109819.

22 James A. Piazza: Fake news: The effects of social media disinformation on domestic terrorism, *Dynamics of Asymmetric Conflict*, 2022. 15.1: 55–77.

23 Alyt Damstra, et al.: What does fake look like? A review of the literature on intentional deception in the news and on social media, *Journalism Studies*, 2021. 22.14: 1947–1963.

vetett bizalmát, és károsíthatja a dezinformációval szembeni ellenálló képességüket. A dezinformáció és propaganda terjesztése aláásható a nemzetközi biztonságot és a nemzeti érdekeket.[24] A propaganda eszközei a közvélemény befolyásolása, meggyőzése, olyan információkkal, amelyek objektívnek tűnnek viszont torzítanak a preferált oldal irányában.[25] Elengedhetetlen a dezinformáció elleni küzdelem és a nemzetbiztonság védelme hatékony információs politikák végrehajtásával és a dezinformáció elleni küzdelemmel szabályozási szinten. Például a kanadai kormány elismerte a külföldi dezinformáció fenyegetését, és intézkedéseket hozott annak érdekében, hogy ezt biztonsági aggályként kezelje.[26]

A digitális dezinformáció, azaz álhírek terjedése az egyik legjelentősebb fenyegetésnek számít az interneten, amely nagymértékben okoz egyéni és társadalmi károkat. Emellett a dezinformációs kampányokat a demokrácia elleni támadásokkal összefüggésben is elemezték, a kommunikáció pedig központi szerepet játszik az ilyen támadások megvalósulásában és azok következményeiben.[27]

A dezinformáció a kiberfenyegetés lencséjén keresztül elemezhető, kiemelve a kiberfenyegetésként való besorolást, amely olyan megkülönböztetett elemekkel rendelkezik, mint a fenyegető ágensek, támadási vektorok, célpontok, hatások és védelmi me-

24 Edward Deverell – Charlotte Wagnsson – Eva-Karin Olsson: Destruct, direct and suppress: Sputnik narratives on the Nordic countries, *The Journal of International Communication*, 2021. 27.1: 15–37.

25 Edson C. Tandoc Jr. – Zheng Wei Lim – Richard Ling: Defining "fake news" A typology of scholarly definitions, *Digital journalism*, 2018. 6.2: 137–153.

26 Nicole J. Jackson: The Canadian government's response to foreign disinformation: Rhetoric, stated policy intentions, and practices, *International Journal*, 2021. 76.4: 544–563.

27 Spencer McKay – Chris Tenove: Disinformation as a threat to deliberative democracy, *Political Research Quarterly*, 2021. 74.3: 703–717.

chanizmusok.[28] Elmondható, hogy a dezinformációt hivatalos és tényleges kiberfenyegetésként kellene felvenni a kiberbiztonsági szabványokba, mivel hasonló jellemzőkkel rendelkezik, mint a már létező fenyegetések.

1.5 Hibrid-hadviselés

A kibertámadásokban a dezinformáció veszélye jelentős aggodalomra ad okot a kiberbiztonság területén. A hibrid hadviselés, amely katonai és nem katonai akciókat kombinál, dezinformációt, kibertámadásokat és más nem katonai eszközöket használ fel a káosz és az instabilitás megteremtésére.[29] A fekete-tengeri régió nagyszabású kibertámadások és folyamatos dezinformációs kampányok célpontja volt, ami e tevékenységek széles körű hatását jelzi. Emellett a kibertér a kereskedelmi forgalomban kapható technológiákkal való lehetséges visszaélés a terrorista csoportok részéről, valamint az online közösségi médián keresztül zajló, ismétlődő politikai dezinformációs kampányok miatt az egyéni és a kollektív biztonság szempontjából is kritikussá vált. Az államilag támogatott „piszkos játékosok" (bad actors) egyre inkább a közösségi médiaplatformokat használják kibertámadások és dezinformációs kampányok indítására a választások idején. Továbbá bizonyíték van arra, hogy ellenséges és rosszindulatú szereplők hibrid háborús intézkedésekkel, többek között kibernetikai

28 Kevin Matthe Caramancion, et al. The missing case of disinformation from the cybersecurity risk continuum: A comparative assessment of disinformation with other cyber threats, *Data*, 2022. 7.4: 49.

29 Khorram-Amir Manesh – Krzysztof Goniewicz – Frederick M. Burkle: Social and healthcare impacts of the Russian-led hybrid war in Ukraine – a conflict with unique global consequences, *Disaster medicine and public health preparedness*, 2023. 17: e432.

behatolásokkal és dezinformációval manipulálják és kihasználják a sebezhető régiókat.[30]

Az információs hadviselés olyan stratégiai megközelítés, amelyet az információk manipulálására és befolyásolására használnak politikai, katonai vagy ideológiai célok elérése érdekében. Szorosan összefonódik az állambiztonsággal. Az államközpontú online propaganda az információs hadviselés jelentős eleme. A politikusok és az állambiztonsági erők dezinformációt és propagandát alkalmazhatnak a közvélemény formálására, erőszakra vagy az ellenzék elnyomására buzdítanak.[31] A dezinformáció elterjedése és a közösségi média platformok használata a nemzetbiztonsági rendszerek fő aggályai közé kerültek. A szélsőséges csoportok propaganda terjesztésével befolyásoljak a közvéleményt, amely hatalmas veszélyt jelent a nemzetbiztonságra.[32] A kiberbiztonság dinamikájának szintetizálása kulcsfontosságú a globális kiberbiztonsági környezet, valamint a kibertámadások és a védekezés közötti kölcsönhatások megértéséhez.[33] Emiatt a védelmi kutatások elengedhetetlenek az AI/ML modellek ellenséges támadásokkal szembeni ellenálló képességének elemzéséhez a kiberbiztonság területén.

A dezinformációnak a hibrid hadviselés eszközeként való felhasználása nem korlátozódik a katonai műveletekre, hanem

30 Flemming Splidsboel Hansen: *Russian hybrid warfare: A study of disinformation*, DIIS Report, 2017.

31 Hannah Smidt: Mitigating election violence locally: UN peacekeepers' election-education campaigns in Côte d'Ivoire, *Journal of peace research*, 2020. 57.1: 199–216.

32 Soufia Kausar – Bilal Tahir – Muhammad Amir Mehmood: ProSOUL: a framework to identify propaganda from online Urdu content, *IEEE access*, 2020. 8: 186039–186054.

33 Ren Zheng – Wenlian Lu – Shouhuai Xu: Preventive and reactive cyber defense dynamics is globally stable, *IEEE Transactions on Network Science and Engineering*, 2017. 5.2: 156–170.

kiterjed a politikai és társadalmi szférára is, pénzügyi és politikai haszonszerzés, valamint kísérleti manipuláció céljából.[34] Az ellenséges külföldi szereplők hibrid módszereket, köztük dezinformációs kampányokat használnak fel a nyugati országok ellen, felfedve felkészületlenségüket és sebezhetőségüket ezekkel a fenyegetésekkel szemben.[35] A hibrid fenyegetésekben a nemzetközi határok elmosódása és a kibertechnológia használata a dezinformációt életképes eszközzé teszi, ami hozzájárul a betudhatóság kétértelműségéhez és a rosszindulatú akciók lehetőségéhez.[36]

A dezinformációs támadások hibrid hadviselési aspektusai a taktikák széles spektrumát foglalják magukban, beleértve a kiber- és információs hadviselést, a civil intézmények célba vételét és a kétértelműség kihasználását a stratégiai célok elérése érdekében. Ezek a taktikák túlmutatnak a hagyományos katonai műveleteken, és képesek jelentősen befolyásolni a közvéleményt, a társadalmi stabilitást és a nemzetközi kapcsolatokat.

Összefoglalás

A dezinformációs támadások komoly fenyegetést jelentenek, és az álhírek terjedése káros társadalmi hatásokkal jár. A támadások közé tartoznak a hamis információk terjesztése és a közvélemény manipulálása, különösen a közösségi médiaplatformokon keresztül. Az ellenintézkedések között szerepel a tényellenőrzés, a mesterséges intelligencia alkalmazása és az oktatási kezdeményezések.

34 Marc Owen Jones: Disinformation superspreaders: the weaponisation of COVID-19 fake news in the Persian Gulf and beyond, *Global Discourse*, 2020. 10.4: 431–437.

35 Sandra Kalniete – Tomass Pildegovičs: Strengthening the EU's resilience to hybrid threats, *European View*, 2021. 20.1: 23–33.

36 B. Poornima: Cyber Threats and Nuclear Security in India, *Journal of Asian Security and International Affairs*, 2022. 9.2: 183–206.

A dezinformáció nagy mértékben befolyásolja a közvéleményt és a hibrid hadviselési stratégiák részeként jelentős nemzetbiztonsági kihívásokat vet fel. Kiemelten fontos a nemzetközi együttműködések, az átláthatóság, az oktatási kezdeményezések, és az információs ökoszisztéma megerősítése a dezinformációs kampányok hatásainak mérséklése érdekében. Mivel a dezinformációs támadások egyre összetettebbé és kifinomultabbá válnak, elengedhetetlen az interdiszciplináris kutatás és együttműködés előmozdítása a szilárd ellenintézkedések kifejlesztése érdekében. Jelen szakirodalmi áttekintés megalapozza a dezinformáció sokrétű természetének megértését, és olyan meglátásokat kínál, amelyek a jövőbeni kutatás, a szakpolitika-fejlesztés és a technológiai fejlesztések alapjául szolgálhatnak az információs manipuláció elleni folyamatos küzdelemben.