Jog-Állam-Politika, 2024/3.229
DOI: 10.58528/JAP.2024.16-3.229

FARKAS ÁDÁM – PAPP JÁNOS TAMÁS

Az internet- és médiaszabályozás kihívásai a terrorizmus, valamint a hibrid fenyegetések elleni európai fellépés tükrében[1]

ABSTRACT

This paper examines the rise of cyber threats and the manipulation of public consciousness through information, as well as the role of the media in these dynamics. The resurgence of international terrorism, highlighted by ISIS's online presence and sophisticated use of media, underscores the pivotal role of the internet and media platforms in modern non-traditional security threats. Furthermore, technological advancements have reshaped state rivalries, elevating the role of non-military factors in global security. Consequently, hybrid threats have become increasingly significant in the 21st century, blending conventional and unconventional methods, often overlapping with terrorist propaganda and online extremist content.

The media, as both a tool and target of hybrid threats, plays a critical role in the dissemination of information and the shaping of public opinion, making it vulnerable to manipulation through tactics such as disinformation campaigns, cyberattacks, and algorithmic exploitation on social media platforms. This paper reviews the EU's evolving regulatory framework, including measures to combat disinformation, enhance media transparency, and protect democratic processes from manipulation. The study highlights key initiatives, such as the Digital Services Act (DSA) and the Terrorist Content Regulation (TERREG), which aim to strengthen media resilience against hybrid threats while balancing the protection of fundamental rights like freedom of expression.

Keywords: hybrid threats ■ media regulation ■ cybersecurity ■ Digital Services Act ■ TERREG ■ EMFA ■ disinformation

[1] A mű a Katonai Nemzetbiztonsági Szolgálat TKP2021-NVA-24 azonosító számú „A mesterséges intelligencia alkalmazásának kutatása a katonai nemzetbiztonsági célú adatszerző, adatfeldolgozó és vizualizációs eljárásokban, és kapcsolódó fejlesztések elvégzése" elnevezésű projektje keretében, az Innovációs és Technológiai Minisztérium Nemzeti Kutatási Fejlesztési és Innovációs Alapból nyújtott támogatásával valósult meg.

I. BEVEZETÉS

A 21. századnak a biztonság terén is meghatározója az információs tér és az infokommunikációs technológia. Az e téren átélt fejlődés felgyorsította életünket, redukálta a fizikai távolságok jelentőségét, növelte a kutatási, fejlesztési és gazdasági hatékonyságot, illetve átalakította az egyéni és társas interakciók jelentős részét.

A szakirodalom már széles körben vizsgálja az infokommunikációval is szoros összefüggésben kialakult valódi globális gazdaságra építve a világ részeinek összekapcsoltságát,[2] az információs társadalom kérdéseit,[3] a kibertér technikai vonatkozásán túl annak szociológiai és pszichológiai sajátosságait, amiből érezhetjük, hogy az információs korszak jelentős hatással van az egyéni, társas, társadalmi kognitív folyamatokra.

Nem meglepő, hogy az előzőekből következően az infokommunikációs robbanás a biztonság terén is jelentős változásokat hozott magával. A hagyományosnak mondható katonai és a bűnözési tevékenységek infokommunikációval való felvértezése mellett e körben külön érdemes figyelmet fordítani a kibertérben végzett különféle veszélyeztető, fenyegető, bűnös cselekményekre,[4] illetve a tudat információs tartalmakkal való befolyásolására.[5]

A nemzetközi terrorizmus újbóli megerősödése, különösen az Al-Kaida nyomán kibontakozó ISIS és annak gazdasági, pszeudo-állami és nem utolsó sorban onlinemarketing-tevékenysége egyértelművé tette az internet és média kulcsszerepét a nem hagyományos biztonsági kihívások és fenyegetések tekintetében. Ezt a megítélést pedig hatványozta az a felismerés, hogy az állami rivalizálás tekintetében is jelentős változást hozott a technika fejlődése, hiszen a korábban is használt nem katonai tényezők szerepe jelentős mértékben felértékelődik ezek által. Ennek eredményeként lett a hibrid fenyegetések témaköre igazán fajsúlyos a 21. században, amelynek azonban eszköz- és módszerrendszere sok tekintetben átfedést mutat a terrormarketing és az internetes terrorista tartalmak témakörével.

Jelen tanulmány célja ezen alapvetések mentén az információs térben is aktív terrorista és hibrid fenyegetési tendenciák európai internet- és médiaszabályozásra gyakorolt egyes hatásait áttekinteni és felhívni a figyelmet az elmúlt időszak változásaira, illetve a további potenciális beavatkozási irányokra a biztonság fokozása érdekében.

[2] Vö. Khanna, 2016; Wallerstein, 2010; Csizmadia, 2016.

[3] Lásd: Juhász – Pintér, 2006; Mattelart, 2004; Castells, 2005; Castells, 2007; Buckland, 2017.

[4] Cornish, 2022; Cho, 2022; Stengel, 2019; Vikman, 2022a, 91-108.; Vikman, 2022b.

[5] A téma kapcsán lásd: McIntyre, 2018; Peters – Rider – Hyvönen – Besley, 2018; Aczél – Veszelszki, 2023; Szitás, 2019, 249-275.; Krekó, 2018.

II. A HIBRID FENYEGETÉSEKRŐL ÁLTALÁBAN

Egy olyan korban, amikor az internet és a médiaplatformok az információterjesztés elsődleges csatornáivá váltak, a hibrid fenyegetések és a terrorizmushoz hasonló, káros tartalmak szabályozása kulcsfontosságúvá válik a nemzetbiztonság, a demokrácia védelme és a társadalmi jólét, illetőleg stabilitás szempontjából.

A hibrid fenyegetések olyan többdimenziós, összehangolt stratégiákat jelentenek, amelyeket állami vagy nem állami szereplők alkalmaznak, és amelyekben hagyományos és nem hagyományos eszközök és eljárások, katonai és nem katonai tényezők, nyílt és rejtett műveletek keverednek.[6] Ezek a fenyegetések gyakran politikai, gazdasági, társadalmi vagy technológiai gyengeségeket használnak ki.[7] E tekintetben osztjuk azt a – hazánkban még bevettnek nem nevezhető – megközelítést, amely fontosnak tartja elkülöníteni egymástól a hibrid fenyegetések, a hibrid konfliktusok és a hibrid hadviselés kategóriáit.[8] Ezek ugyanis eltérő szintjeit jelölik a hibrid képletben megoszló tényezők arányának és alkalmazásának, ami jelen téma szempontjából is fontos. Ha ezt a kategorizálást elfogadjuk, akkor azt mondjuk, hogy a hibrid fenyegetésektől a hibrid hadviselés felé haladó lépcsőkben növekszik a katonai szemléletmód és stratégia fajsúlya az alkalmazott eszközök és módszerek körében. Ez az internet és média felhasználása körében is érvényesül, hiszen ezen a skálán haladva a jellemzően nem katonai tartalmak dominanciájától a katonai műveleteket közvetlenül érintő vagy azokat közvetve – de mégis szorosan – támogató tartalmak irányába mozog a beavatkozás. Fogalmazhatnánk úgy is, hogy más társadalmi hangulat kialakítása a cél a hibrid fenyegetés nem közvetlenül katonai determináltságú fázisában, mint a félutat képező és már katonai szembenállással is fenyegető hibrid fenyegetés, majd a dominánsan katonai jellemzőkkel áthatott hibrid hadviselés szakaszában. Bárhonnan nézzük azonban, a média, amely a közvélemény befolyásolásának és a politikai tájkép alakításának és a legitim államműködésnek is hatékony platformjaként szolgál, nem lehet mentes a hibriditásból következő, különféle fenyegetésektől.

A média és az internet nemcsak, hogy nem lehet mentes a hibrid fenyegetésekből következő hatásoktól, hanem e területek lényegében kulcsszerepet játszottak a hibrid biztonsági környezet kialakulásában. A nem katonai tényezők konfliktusos alkalmazása ugyanis nem újszerű. Erről Farkas és Kelemen a következőket írja: „A hibrid konfliktusok képében bizonyos szempontból egy régi ismerős tekint vissza ránk, egy valóban újszerű formában. Ha csak a fogalommal szinte összemosott orosz állam 20. századi történelmét nézzük, akkor azt látjuk, hogy a Szovjetunióban óriási hagyományai voltak a sokrétű, nem tisztán katonai lépésekre építkező stratégiai érdekérvényesítésnek és eszközrendszernek.

[6] Európai Tanács: A Tanács a reziliencia megerősítésére..., 2020.
[7] Európai Bizottság - Sajtóközlemény, 2016.
[8] Vö: Farkas – Kelemen, 2022; Farkas, 2023.

A maszkirovka katonai alkalmazása, majd ennek a szemléletmódnak a kiszélesítése több mint százéves múltra tekint vissza. Ehhez persze hozzá kell tenni, hogy önmagában véve a nem katonai tényezők hadászati-stratégiai célokat megalapozó vagy előkészítő, illetve konkrét katonai műveleteket kísérő alkalmazása messze nem újdonság a világtörténelemben, mivel Sun Ce, Taj Kung vagy Vej Liao-Ce óta ismertek. Az állami, társadalmi sajátosságok katonai műveletekkel összefüggő kiaknázása, a kémek alkalmazása, az ellenséges területek lakosságához való viszonyulása, az ellátási láncokra való hatásgyakorlás mind-mind olyan témakör, amely már az antikvitás óta jelen van a hadviselésre, stratégiai gondolkodásra vonatkozó irodalomban. Ez a komplex, a katonai és a nem katonai elemeket vegyítő – és ilyenként hibrid – megközelítés aztán egyre markánsabban átszivárgott a katonai gondolkodástól különváló politikai filozófiai és államtudományi gondolkodásba is Niccolò Machiavellitől Napóleonon át Carl Schmittig, hogy aztán visszahasson a hadviselés elméletére, és abban szélesebb horizontot tárjon fel, mint maga a háború megvívásának katonai dimenziója, ahogy ez Carl von Clausewitz abszolút háború felfogásában, majd Erich Ludendorff totális háborújában megjelent."[9] Innen nézve tehát, a média és az internet terrénumai ma jelentős mértékben azokat a technikai-társadalmi-tudati metszethalmazokat jelölik, amelyek napi szinten, sőt pillanatról-pillanatra terjedően képesek tömegek világlátását, valóságképét, biztonságpercepcióját és ezek által állami szervezetek működését befolyásolni. A 21. századi infokommunikációra épülő gazdasági, társadalmi, politikai működés az, ami tehát hatványozni tudta olyan mértékben a nem katonai tényezők jelentőségét a biztonság és védelem horizontján, hogy érdemes legyen immár elkülönülten beszélni a hibrid fenyegetések súlyáról.

A hibrid fenyegetések egyre nagyobb aggodalomra adnak okot a médiaágazatban. Ezek a fenyegetések a hagyományos és nem hagyományos módszerek stratégiai keverékét jelentik a társadalmi struktúrák és intézmények, köztük a média megzavarása és manipulálása érdekében. A médiát érintő hibrid fenyegetések jellemzően olyan taktikákat foglalnak magukban, mint a dezinformációs kampányok, a médiainfrastruktúra elleni kibertámadások és a közösségi média algoritmusainak manipulálása.[10] A közösségimédia-platformok széles hatókörükkel és hálózati algoritmikus struktúráikkal termékeny talajt biztosítanak az ilyen fenyegetések számára. Manipulálhatók bizonyos üzenetek felerősítésére, visszhangkamrák létrehozására és a polarizáció ösztönzésére.[11] A médiainfrastruktúra elleni kibertámadások továbbá megzavarhatják a műsorszóró rendszereket, érzékeny információkat szivárogtathatnak ki, vagy manipulálhatják a terjesztett tartalmakat.[12]

A hibrid fenyegetések egyik legelterjedtebb formája a dezinformáció vagy „álhírek" terjesztése. A médiát, amelynek kulcsszerepe van a közvélemény alakításában, gyakran használják ki arra, hogy kitalált narratívákat terjesszenek,

[9] Farkas – Kelemen, 2022, 96.
[10] Bergh, 2019, 23.
[11] A visszhangkamrákról lásd még részletesen: Papp, 2023.
[12] Slavan, 2016, 738-752., 741-742.

amelyek célja zavart kelteni, megosztottságot szítani vagy közösségeket destabilizálni. A dezinformációs kampányok jelentős károkat okozhatnak, különösen akkor, ha megkérdőjelezik a demokratikus intézmények hitelességét vagy társadalmi feszültségeket gerjesztenek.[13] A hibrid fenyegetések a médiumok elleni kibertámadások formájában is megjelenhetnek. Ezek a támadások a médiavállalkozások honlapjainak leállítását célzó DDoS-támadásoktól kezdve az érzékeny adatok ellopására vagy a belső hálózatok megzavarására irányuló kifinomultabb behatolásokig terjedhetnek.[14] Egyes esetekben a kibertámadások célja akár a közzétett tartalom megváltoztatása is lehet, ami befolyásolja a média hitelességét, és széles körű félretájékoztatáshoz vezet. Ez a másnéven információs hadviselésnek nevezett folyamat a hibrid fenyegetések egy másik dimenzióját jelenti, amikor az ellenfelek stratégiai előny megszerzése érdekében manipulálják az információkat. Az állami szereplők például „trollfarmokat" alkalmazhatnak[15] az online narratívák ellenőrzésére vagy megváltoztatására, vagy részt vehetnek az „astroturfing"-ban,[16] vagyis abban a gyakorlatban, hogy egy adott kérdésben a tömeges támogatás vagy ellenállás illúzióját keltik.[17] Az ilyen taktikák drámaian befolyásolhatják a közhangulatot és felhasználhatók arra, hogy a politikai diskurzust az agresszor javára irányítsák.[18]

A mesterséges intelligencia utóbbi években megfigyelhető, rohamos mértékű fejlődése pedig további lehetőségeket biztosít a hasonló támadások elkövetői számára. A mesterséges intelligenciát hiperrealisztikus, de teljesen szintetikus audiovizuális tartalmak létrehozására használó deepfake technológia térhódítása különösen aggasztó forgatókönyvet jelent. A megtévesztő videók felhasználhatók a közvélemény manipulálására, erőszakra való felbujtásra vagy a jó hírnév megrontására, és ahogy a mesterséges intelligencia technológia egyre kifinomultabbá válik, úgy nő a visszaélések lehetősége ezen a területen.[19]

Összefoglalva, a hibrid fenyegetések jelentős kihívást jelentenek a médiaágazat számára, és folyamatos éberséget és alkalmazkodást igényelnek az információk pontosságának és hitelességének biztosítása érdekében a digitális korban. Ezen hibrid fenyegetések befolyásolják és kihasználják az adott társadalomban felfedezhető sebezhetőségeket, hogy a nyílt agresszió küszöbértéke alatti károkat okozzanak, és következményei messzire mutatóak lehetnek.[20] Az azonnali hatásokon túl, mint például a félretájékoztatás vagy a pánikkeltés, ezek a taktikák idővel alááshatják a média iránti közbizalmat is. Ahogy az emberek elveszí-

[13] OECD Going Digital Toolkit - Policy Note.

[14] Pierozzi, 2017.

[15] WhatsthePONT Blog: Can You Really Trust Social Media in a Crisis?, 2015.

[16] The New York Times Magazine: The Agency, 2015.

[17] García-Orosa, 2021.

[18] OECD Policy Responses: Ukraine Tackling the Policy Challenges…, 2022.

[19] Bontridder – Poullet, 2021.

[20] European Union External Action – The Diplomatic Service of the European Union: Countering hybrid threats, 2024.

tik a hírforrásaikba vetett bizalmukat, úgy válnak fogékonyabbá a további dezinformációra és manipulációra, ami egy olyan mérgező körforgást eredményez, amely aláássa a demokráciát és a társadalmi kohéziót.[21] Ez teszi a hibrid fenyegetéseket az egyik legnagyobb folyamatos kihívássá a 21. században, újszerűségük pedig a sokrétű formájukban, új technológiák alkalmazásában és terjedésük exponenciális sebességében rejlik.[22]

E kihívásokra válaszul kormányok, technológiai vállalatok és nem kormányzati szervezetek dolgoznak a hibrid fenyegetések elhárításán. A megoldások közé tartozik a specifikus jogi szabályozás bevezetése, a kiberbiztonsági infrastruktúra javítása, valamint az álhírek és a deepfake felismerésére és leküzdésére szolgáló mesterségesintelligencia-rendszerek fejlesztése.[23] A média jelentős csatatér a hibrid fenyegetések elleni küzdelemben.[24] Mivel ezek a fenyegetések egyre összetettebbé válnak, az Európai Unió megközelítésének is alkalmazkodnia kell, hangsúlyozva az együttműködést, a rugalmasságot, a tudatosságot és a technológiai vállalatok döntő szerepét. A kihívások ellenére az EU többirányú stratégiája mintát kínál a politika, az oktatás és a technológia integrálására a médiát fenyegető hibrid fenyegetések elleni küzdelemben.

Az Európai Unió, felismerve, hogy ezek a fenyegetések komoly hatással lehetnek tagállamai biztonságára, gazdaságára és demokratikus intézményeire és felmérve a fenyegetések kifinomultságát, proaktívan lépett fel az ellenük való küzdelem mechanizmusainak létrehozásában. Az EU megközelítése az ellenálló képesség kiépítésén, a tudatosság növelésén, valamint a tagállamok közötti és a NATO-val való együttműködés előmozdításán alapul.[25] Az uniós jogszabályok és szakpolitikák az ilyen fenyegetések elleni hatékony küzdelem érdekében fejlődtek, és különböző ágazatokra összpontosítanak, többek között a kibernetikai, az információs és kommunikációs, a pénzügyi és a kritikus infrastruktúrára.[26]

III. A HAGYOMÁNYOS MÉDIA EU-MEGKÖZELÍTÉSE A HIBRIDITÁSSAL LEÍRHATÓ BIZTONSÁGI KÖRNYEZETBEN

A médiaszolgáltatások területén az elsődleges jogszabály az audiovizuális médiaszolgáltatásokról szóló irányelv,[27] mely támogatja a média igazságos el-

[21] Wijnja, 2022.

[22] Sanz-Caballero, 2023, 7.

[23] Mazucchi, 2022, 16.

[24] Bless, 2011, 283.

[25] Az Európai Parlament és a Tanács közös közleménye a hibrid fenyegetésekkel szembeni fellépés közös keretéről. JOIN/2016/018.

[26] Argomaniz, 2015.

[27] Az Európai Parlament és a Tanács 2010/13/EU irányelve (2010. március 10.) a tagállamok audiovizuális médiaszolgáltatások nyújtására vonatkozó egyes törvényi, rendeleti vagy közigazgatási rendelkezéseinek összehangolásáról (Audiovizuális médiaszolgáltatásokról szóló irányelv).

osztását és a médiatulajdonlás átláthatóságát, megállapítja a médiaszolgáltatások európai tartalmi kvótáira vonatkozó szabályokat, és támogatja a nemzeti médiaszabályozók függetlenségét.

A 2020 végén meghirdetett Európai Demokrácia Cselekvési Terv az Európai Bizottság által kidolgozott keretrendszer, amelynek célja a demokrácia megerősítése az Európai Unióban.[28]

A terv célja többek között a választások és a politikai hirdetések integritásának biztosítása, az átláthatóság fokozása, a független újságírás támogatása, valamint, hogy javítsa az EU dezinformációs felderítési és reagálási képességeit.[29] A cselekvési terv részeként jelentette be[30] Ursula von der Leyen 2021-ben az Európai Médiaszabadságról szóló törvényre (European Media Freedom Act – EMFA) vonatkozó kezdeményezést, mely az audiovizuális médiaszolgáltatásokról szóló irányelvre épül, és különböző szabályokat állapít meg a médiaszabályozók függetlenségére vonatkozóan, előmozdítja a médiatulajdonlás átláthatóságát, és megerősíti a szerkesztői döntésekbe függetlenségét. A kezdeményezés a médiaszolgáltatások létrehozása és működtetése előtt álló akadályok felszámolására összpontosít, és célja, hogy közös keretet hozzon létre a médiaágazat belső piacának előmozdítására, tekintettel a média szabadságának és pluralizmusának védelmére ezen a piacon.[31]

Az Európai Unió végül 2024. április 11-én fogadta el a jogszabályt. Az április 17-én kihirdetett EMFA[32] a médiaszabályozás területére tartozó heterogén területeket gyűjt egybe, köztük a közszolgálati médiára, a nemzeti szabályozó hatóságok együttműködésére, a médiatulajdonosi viszonyok átláthatóságára vagy az állami hirdetések elosztására vonatkozó rendelkezéseket. Noha a jogszabály 2024. május 7-én hatályba lépett, egyes rendelkezései eltérő időpontokban válnak alkalmazhatóvá. A javaslat 17. cikke az Unión kívüli médiaszolgáltatásokra vonatkozó intézkedések összehangolásával foglalkozik, és előírja, hogy a Médiaszolgáltatások Európai Testülete „legalább két tagállam nemzeti szabályozó hatóságának vagy szervének kérésére összehangolja az érintett nemzeti szabályozó hatóságok vagy szervek azon releváns intézkedéseit, amelyek az Unión kívülről származó olyan médiaszolgáltatások vagy az Unión kívül letelepedett médiaszolgáltatók által nyújtott olyan médiaszolgáltatások terjesztésével vagy az azokhoz való hozzáféréssel kapcsolatosak, amelyek a terjesztés vagy a hozzáférés módjától függetlenül az Unión belüli közönséget céloznak vagy érnek el, amennyiben az ilyen médiaszolgáltatások – többek között a harmadik országok által felettük gyakorolt eset-

[28] European Commission: European Democracy Action Plan: making EU democracies stronger.

[29] European Commission: Shaping Europe's digital future: Tackling online disinformation.

[30] European Commission: State of the Union 2021.

[31] European Commission: European Media Freedom Act: Commission launches public consultation, 2022.

[32] 2024/1083 rendelet a belső piaci médiaszolgáltatások közös keretének létrehozásáról és a 2010/13/EU irányelv módosításáról (a tömegtájékoztatás szabadságáról szóló európai rendelet), HL L, 2024/1083, 2024.04.17.

leges ellenőrzésre tekintettel – sértik a közbiztonságot, vagy az annak sérelmével fenyegető komoly és súlyos kockázatot jelentenek".[33]

A cikkhez kapcsolódó preambulumbekezdések a médiahatóságok különleges gyakorlati szakértelmét emelik ki annak érdekében, hogy megvédjék a belső piacot az Unión kívülről érkező médiaszolgáltatások olyan tevékenységeitől, amelyek az Unión belüli közönséget célozzák meg vagy érik el, és amelyek „sérthetik vagy veszélyeztethetik a közbiztonságot". Ilyen kockázatot jelenthetnek például a külföldi információmanipulációval és beavatkozással kapcsolatos szisztematikus nemzetközi kampányok, amelyek célja az egész Unió vagy egyes tagállamok destabilizálása.[34] Ennek érdekében a jogszabály a preambulum szerint össze kívánja hangolni azokat a nemzeti intézkedéseket, amelyeket az Unión kívülről származó vagy letelepedett, de az uniós közönséget megcélzó médiaszolgáltatások által a közbiztonságot fenyegető veszélyek elhárítására lehet elfogadni.[35] Ennek érdekében a jogszabály javasolja az EMFA által felállítandó Médiaszolgáltatások Európai Testülete által összeállított kritériumlista létrehozását, mely segítené a nemzeti szabályozó hatóságokat vagy testületeket olyan helyzetekben, amikor egy érintett médiaszolgáltató joghatóságot kér valamely tagállamban, vagy amikor egy tagállam joghatósága alá tartozó médiaszolgáltató súlyos és súlyos közbiztonsági kockázatot jelent. Az ilyen jegyzékben szereplő elemek vonatkozhatnak többek között a „tulajdonviszonyokra, a vezetésre, a finanszírozási struktúrákra, a harmadik országoktól való szerkesztői függetlenségre, vagy a szerkesztés szakmai normáit szabályozó, egy vagy több tagállamban működő társ- vagy önszabályozási mechanizmusban való részvételre".[36]

A szabályozást egyértelműen az orosz–ukrán konfliktus hívta életre. Az Európai Unió Tanácsa 2022. március 1-jén tanácsi rendeletet fogadott el, amely előírta, hogy az Oroszország által indított hibrid hadviselés miatt az Európai Unióban korlátozni kell egyes, az államhoz kötődő orosz médiumok működését és sugárzását.[37] Ebben azt írták elő, hogy tilos a gazdasági szereplők számára a Russia Today és bármely hozzá kapcsolódó szolgáltató tartalmának sugárzása, vagy annak lehetővé tétele, ideértve a „kábelen, műholdon, IPTV-n, internetszolgáltatókon, internetes videomegosztó platformokon vagy alkalmazásokon keresztül történő átvitelt vagy terjesztést".[38] A csatorna felfüggesztése komoly vitát váltott ki újságíró szervezetek, valamint jogászok és szakértők körében egyaránt.[39]

[33] EMFA 17. cikk.

[34] EMFA (47) preambulumbekezdés.

[35] EMFA (48) preambulumbekezdés.

[36] EMFA (49) preambulumbekezdés.

[37] A Tanács (EU) 2022/350 rendelete (2022. március 1.) az ukrajnai helyzetet destabilizáló orosz intézkedések miatt hozott korlátozó intézkedésekről szóló 833/2014/EU rendelet módosításáról.

[38] A Tanács (EU) 2022/350 rendelete (2022. március 1.) az ukrajnai helyzetet destabilizáló orosz intézkedések miatt hozott korlátozó intézkedésekről szóló 833/2014/EU rendelet módosításáról, 1. cikk.

[39] A témában lásd bővebben: Lendvai, 2023.

IV. AZ ONLINE KÖRNYEZET ÉS A HIBRID FENYEGETÉSEK EU-SZINTŰ SZABÁLYOZÁSA

Az Európai Unió is felismerte, hogy a dezinformáció egyre növekvő fenyegetést jelenthet a társadalmi diskurzusokra nézve, és hogy a demokratikus folyamatok és intézmények manipulációval szembeni védelme "hosszú távú kihívást jelent és folyamatos erőfeszítéseket tesz szükségessé".[40] Az Európai Unió Európai Külügyi Szolgálat (EKSZ) keleti stratégiai kommunikációval foglalkozó munkacsoportot (East StratCom) hozott létre a dezinformáció visszaszorítására,[41] amely többek között az EU v. Disinfo honlapot üzemelteti, ahol összegyűjtik az Unióval kapcsolatos hamis híreket, és információkat szolgáltatnak a leleplezett hamishír-hálózatokról.[42] A munkacsoportot eredetileg 2015-ben, az orosz befolyás elleni fellépés miatt hozták létre, 2019 májusáig pedig több mint 5455 orosz eredetű hamis hírt azonosítottak be és léptek fel ellenük.[43]

Az Európai Bizottság 2017 végén magas szintű szakértői csoportot hozott létre az üggyel kapcsolatos tanácsadás biztosítása érdekében, "hamis hírekkel és az internetes félretájékoztatással foglalkozó magas szintű munkacsoport" néven. A munkacsoport feladata a probléma feltérképezése volt, valamint, hogy megfelelő ajánlásokat fogalmazzon meg az Unió számára a dezinformáció visszaszorításának érdekében. A Bizottság széles körű nyilvános konzultációs folyamatot is elindított a témában, amely a 2986 választ kapott online kérdőívekből, az érdekelt felekkel folytatott strukturált párbeszédekből, valamint egy, mind a 28 tagállamra kiterjedő Eurobarométer közvélemény-kutatásból áll.[44] A szakértői csoport 2018. március 12-én terjesztette elő jelentését,[45] melyben elsődlegesen az önszabályozás mellett tették le voksukat. A jelentés ajánlásai között szerepel még emellett a médiatudatosság előmozdítása, olyan eszközök kifejlesztése, melyekkel a felhasználók és az újságírók egyaránt hatékonyabban tudnák kezelni a dezinformációt, a hírekkel foglalkozó európai média sokszínűségének és fenntarthatóságának védelme, valamint az Európán belül megfigyelhető félretájékoztatással kapcsolatos kutatások folytatása.[46] A szakértői csoport ezen felül egy alapelveket tartalmazó kódex megalkotását javasolta, melynek használata mellett az online platformok és a közösségi oldalak egyaránt elköteleznék magu-

[40] Jelentés az Európai Parlamentnek, az Európai Tanácsnak, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának a dezinformációval szembeni közös cselekvési terv végrehajtásáról. Brüsszel, 2019.6.14. JOIN (2019) 12 final.

[41] European Union External Action - Questions and Answers about the East StratCom Task Force, 2021.

[42] Az oldal elérhetősége: https://euvsdisinfo.eu/.

[43] Index, Arató, 2019.05.25.

[44] European Commission: Shaping Europe's digital future: Tackling online disinformation.

[45] European Commission: Shaping Europe's digital future: Final report of the High Level Expert Group on Fake News and Online Disinformation, 2018.

[46] Európai Bizottság: Online félretájékoztatás: az internetes platformok fokozott átláthatóságára van szükség, 2018.

kat. Az alapelvek olyan követelményeket fogalmaztak meg, mint az átláthatóság az információk forrása, előállítása, szponzorálása, terjesztése és célzottsága tekintetében, az online elszámoltathatóság előmozdítása, vagy a magas színvonalú újságírás és a médiaműveltség támogatása.[47]

Az EU által kitűzött célok tehát főként a dezinformációval kapcsolatos tudatosságnövelés, a médiaműveltség javítása, a civil társadalom szerepének erősítése, a kiberfenyegetésekkel szembeni védelem javítása és a fizetett online politikai hirdetések átláthatóságának növelése volt.[48] 2018 októberében meg is született a dezinformáció visszaszorítását célzó gyakorlati kódex,[49] amely önszabályozás keretében igyekezett megoldani a kérdést. Az önszabályozó kódexet a Facebook, a Google, a Twitter, a Mozilla és a Microsoft is aláírta, melyet így magukra nézve kötelezőnek ismertek el. A kódex értelmében a platformoknak átláthatóbbá kell tenniük szabályzataikat, szorosabb együttműködést kell kialakítaniuk a kutatói szférával, tényellenőrzőkkel és a tagállamokkal. A platformok legfontosabb kötelezettségei azonban a politikai hirdetések átláthatóságára, a dezinformáció szűrésére és önértékelő jelentések[50] (az EU-s választásokat megelőző hónapokban havi, később éves rendszerességgel történő) benyújtására vonatkoztak. Az Európai Unió ezzel tehát az önszabályozás felé terelte a platformokat, arra ösztönözve őket, hogy a korábbinál még nagyobb mértékben végezzenek monitorozási tevékenységet, átadva nekik a szabályozást. A magatartási kódexben foglaltakat így nem maga az Európai Unió tartatja be, hanem maguk a techcégek, az Unió kezében csupán az általuk rendelkezésre bocsátott jelentések értékelésének lehetősége van.

1. DSA

A digitális közvetítők szerepe alapvető fontosságú, mivel egy olyan, a gyakorlatban nem létező terjesztési hálózatot biztosítanak, amely a propagandatartalmakat messzire és széles körben terjeszti. Emellett az ilyen típusú tartalmakat alátámasztó cikkek és érzelmek összefoglalóit a közösségi média felhasználói visszhangozzák, amelyek aztán felerősítenek bizonyos összeesküvés-elméleteket, amelyeket ezek a propaganda-csatornák indítottak el.[51]

A DSA témánk szempontjából különösen érdekes része a platformok átláthatósági jelentései, az online óriásplatformok szisztematikus problémáinak kocká-

[47] Európai Bizottság: Európai megközelítés az online félretájékoztatás kezelésére. COM (2018) 236 final, Brüsszel, 2018.4.26. 1.

[48] Jelentés az Európai Parlamentnek, az Európai Tanácsnak, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának a dezinformációval szembeni közös cselekvési terv végrehajtásáról. Brüsszel, 2019.6.14. JOIN(2019) 12 final.

[49] Európai Bizottság: A dezinformáció visszaszorítását célzó uniós gyakorlati kódex.

[50] European Commission: Shaping Europe's digital future: Annual self-assessment reports of signatories to the Code of Practice on Disinformation 2019.

[51] EDRi: Disinformation and propaganda: It's all political!, 2021.

zatértékelése valamint a válságreagálási mechanizmusa. A platformoknak éves jelentéseket kell majd közzétenniük, amelyekben ismertetik a tartalommoderálási gyakorlatukat.[52] A platformoknak emellett egységes panaszmechanizmust is be kell vezetniük, hogy a felhasználók megtámadhassák a platformok azon döntéseit, melyekkel korlátozzák a szólásszabadságukat, vagy pont ellenkezőleg, figyelmen kívül hagyja a tartalommal kapcsolatos panaszt.[53] Mindemellett fel kell mérniük néhány, a szolgáltatásaik kialakításából és használatából eredő kockázatot, és csökkenteniük is kell ezeket a kockázatokat.[54] Ebbe beletartozik a rendelet szerint a "a polgári közbeszédre, valamint a választási folyamatokra és a közbiztonságra gyakorolt bármely tényleges vagy várható negatív hatás".[55]

A DSA emellett válságreagálási mechanizmusok kidolgozását is előírja. Válsághelyzetnek tekinti azokat a helyzeteket, amikor "olyan rendkívüli körülmények merülnek fel, amelyek az Unióban vagy annak jelentős részében a közbiztonságot vagy a közegészséget érintő komoly fenyegetéshez vezethetnek".[56] Ilyen helyzetekben pedig a Bizottság olyan határozatokat fogadhat el, melyekben az online óriásplatformokat különböző intézkedésekre kötelezheti, mint például a szolgáltatásaik működéséből eredő veszélyek érékelése, valamint arányos, konkrét és eredményes intézkedések bevezetése ezek megelőzése, megszüntetése vagy korlátozása érdekében.[57]

2. TERREG

A technológiai ipar összehangolt kezdeményezésekkel próbálja kezelni a terrorista vagy szélsőséges harmadik féltől származó tartalmak okozta problémákat, amelyek célja az egyedi intézkedések hatékonyságának fokozása. Az összehangolt kezdeményezések közé tartozik többek között a terrorizmus elleni globális internetes fórum,[58] az uniós szerveket, kormányokat és technológiai vállalatokat tömörítő uniós internetes fórum,[59] az illegális online gyűlöletbeszéddel szembeni fellépésről szóló magatartási kódex,[60] valamint a közös ipari hash-adatbázis.[61] A vállalatok külön-külön vállalták, hogy további intézkedé-

[52] DSA 14. cikk.

[53] DSA 20. cikk.

[54] DSA 34-35. cikkek.

[55] DSA 34. cikk (1) c) pont.

[56] DSA 36. cikk (2) bek.

[57] DSA 36. cikk (1) bek.

[58] Microsoft Corporate Blogs: Facebook, Microsoft, Twitter and YouTube announce formation of the Global Internet Forum to Counter Terrorism, 2017.

[59] European Commission: EU Internet Forum: a major step forward in curbing terrorist content on the internet, 2016.

[60] European Commission: Your rights in the EU.

[61] Google Blog - Around he Globe: Partnering to help curb the spread of terrorist content online, 2016.

seket tesznek annak érdekében, hogy a mesterséges intelligencia és az „emberi szakértelem" alkalmazásával fellépjenek a platformjaik terrorista és egyéb jogellenes célokra történő felhasználása ellen, hogy azonosítsák a „szélsőséges és terrorizmussal kapcsolatos" tartalmakat.[62]

Az ezzel a problémával foglalkozó, mérföldkőnek számító jogszabály az online terrorista tartalmak elleni fellépésről szóló rendelet.[63] Ezt a jogszabályt az Európai Parlament és az Európai Unió Tanácsa 2021-ben fogadta el azzal a szándékkal, hogy korlátozza a terrorista tartalmak egyénekre és társadalmakra gyakorolt hatását.[64] A rendelet szigorú szabályokat ír elő az EU-ban szolgáltatásokat nyújtó tárhelyszolgáltatók számára, függetlenül azok letelepedési helyétől. Kötelezi az ilyen szolgáltatókat, hogy az illetékes hatóságoktól kapott eltávolítási utasítástól számított egy órán belül távolítsák el vagy tiltsák le az azonosított terrorista tartalmakhoz való hozzáférést.[65] Emellett megkönnyíti a határokon átnyúló együttműködést, lehetővé téve bármely tagállam számára, hogy eltávolítási végzést küldjön egy másik tagállamban működő tárhelyszolgáltatónak.[66] A tagállamoknak továbbá ki kell jelölniük az illetékes hatóságokat az online terrorista tartalmak felderítésére, azonosítására és eltávolítására vonatkozó utasítások kiadására.[67]

A rendelet tágan határozza meg a terrorista tartalmak fogalmát, beleértve (1) a terrorista bűncselekmények elkövetésére való felbujtás vagy uszítást, (2) a terrorista bűncselekményekhez való hozzájárulás ösztönzését, (3) a terrorista csoport tevékenységeinek előmozdítását vagy (4) a terrorista bűncselekmények elkövetése céljából alkalmazott módszerekre vagy technikákra vonatkozó oktatást.[68] A rendelet súlyos szankciókat ír elő a szabályok be nem tartása esetén, beleértve a szolgáltató előző üzleti évi globális forgalmának 4%-áig terjedő bírságot.[69] Emellett a rendelet szilárd átláthatósági és elszámoltathatósági keretet hoz létre, amely előírja a szolgáltatók számára, hogy tegyenek jelentést a tevékenységükről, a tagállamoknak pedig, hogy ellenőrizzék a rendelet alkalmazását.[70]

3. Ön- és társszabályozás

Az EU-s szabályozás mellett az önszabályozás és a társszabályozás szerves

[62] Hassan, 2022.
[63] Az Európai Parlament és a Tanács rendelete az online terrorista tartalom terjesztésének megelőzéséről.
[64] Bellanova – de Goede, 2022, 1316-1334.
[65] TERREG 4. cikk.
[66] TERREG 13. cikk.
[67] TERREG 17. cikk.
[68] TERREG 2. cikk 5. pont.
[69] TERREG 18. cikk.
[70] Hassan, 2022.

stratégiák lehetnek a hibrid fenyegetések elleni küzdelemben, mivel olyan rugalmas és innovatív módszereket kínálnak, amelyek gyorsan alkalmazkodnak e kockázatok dinamikus jellegéhez.

Az önszabályozás azt a gyakorlatot jelenti, amikor iparágak vagy ágazatok saját normákat és gyakorlatokat határoznak meg egy bizonyos szintű magatartás fenntartása vagy meghatározott célok elérése érdekében.[71] A digitális ágazat vállalatai például különböző kiberbiztonsági protokollokat és szabványokat alakíthatnak ki a kibertámadások kivédésére, szigorú auditokat hajthatnak végre, és védelmi rendszereiket olyan gyakorlatokon keresztül tesztelhetik, mint a red teaming.[72] A digitális platformok, beleértve a közösségi médiát is, létrehozhatnak továbbá olyan irányelveket, amelyek segítségével felismerhetik, elemezhetik és eltávolíthatják a dezinformációt, ugyanakkor szigorú büntetéseket szabhatnak ki az ezeket az irányelveket gyakran megsértő felhasználókra. Ezen túlmenően a vállalkozások minden ágazatban önszabályozást vezethetnek be a gazdasági kényszerítés ellen, amely magában foglalja a külföldi befektetések és partnerségek szigorú ellenőrzési folyamatainak elfogadását.

Másrészt a társszabályozás olyan együttműködési modellt jelent, amelyben az iparágon belüli önszabályozás összehangolódik a törvényi szabályozással. Olyan együttműködési környezetet alakít ki, amelyben az iparág és a kormányzat együtt dolgozik egy adott kérdés megoldásán. A társszabályozás sikeres példája a kiberbiztonságban figyelhető meg. Itt a kormányzat és az ipar együttműködik a szilárd kiberbiztonsági szabványok kialakításában, a fenyegetésekkel kapcsolatos kritikus információk megosztásában és a nagyobb kiberincidensekre adott válaszlépések összehangolásában.[73] Hasonlóképpen, a dezinformáció elleni küzdelemben a társszabályozás elősegítheti a digitális platformok, a hírszervezetek és a kormányok közös erőfeszítéseit, hogy a problémát a gyökerénél kezeljék. Ez magában foglalhatja a dezinformációs kampányokkal kapcsolatos adatok megosztását, a közös válaszlépések megszervezését és a tartalom moderálására vonatkozó iránymutatások közös kidolgozását.

Miközben azonban az ön- és társszabályozás értékes eszközként szolgál a hibrid fenyegetésekkel szembeni fellépésben, fontos biztosítani, hogy ezek a megközelítések tiszteletben tartsák a demokratikus értékeket és az alapvető jogokat, például a véleménynyilvánítás szabadságát és a magánélet védelmét. Ennek az egyensúlynak a megtalálása kulcsfontosságú a hatékony és etikus kockázatcsökkentés szempontjából. A média ugyanis nem csak a terroristák potenciális eszköze. A terrorizmus elleni küzdelemben döntő szerepet játszik azáltal, hogy létfontosságú közérdekű információkat terjeszt, oknyomozó riportokon keresztül feltárja a terrorizmus rideg valóságát, és felhívja a figyelmet a terrorizmus veszélyeire és az ellene tett erőfeszítésekre. Végső soron a média a szabad véleménynyilvánítás egyik pillére, egy olyan alapvető emberi jog, amelyet a terroristák gyakran igye-

[71] Bellanova – de Goede, 2022, 1320.
[72] Trend Micro: What is Red Teaming & How it Benefits Orgs, 2023.
[73] Tropina – Callanan, 2015.

keznek aláásni. Ezért a média szerepe létfontosságú a terrorizmus elleni küzdelemben, miközben fenntartja a szabad társadalom elveit.[74]

V. ÖSSZEGZÉS

Az internet és a média szabadságát kihasználó terrorista tevékenységek, illetőleg a hasonlóan kihasználó jellegű hibrid fenyegetések egyértelműen markáns jellemzői és egyben kihívásai a 21. századi biztonsági környezetnek. Fordítva szemlélve, a kortárs terrorizmus és extrémizmus, illetve a hibrid fenyegetések médiát és internetet eszközként használó jellege magától értetődően komoly fenyegetést jelent ezen területek megbízhatóságára, ezáltal pedig társadalmi megítélésére és szabályozására nézve is. Ez a kapcsolódás mélyebb összefüggést – és egyben kihívást is – tár elénk, ha osztjuk azt a megközelítést, miszerint a hibrid fenyegetésekben nem a nem katonai tényezők alkalmazása az újszerű, hanem az a tényszerűség, hogy a technikafejlődés révén ezek a nem katonai tényezők – különösen a kortárs média és internet – geopolitikai, illetve biztonsági hatóképessége soha nem látott mértékben növekedett meg. Ekkor ugyanis láthatjuk, hogy a média- és internetszabályozás terén jelentkező kihívások nemcsak egy tiszta okozati viszonyt tükröznek, hanem e területek fejlődése lényegében oka is a hibrid környezet és eszköztár kialakulásának. E megközelítésből nézve a különféle európai válaszok jelentősége az internet- és médiaszabályozás értékeinek megóvása és a társadalmi hasznok biztosítása mellett a hibrid fenyegetések elleni fellépés stratégiai mátrixában is kiemelt jelentőséggel bír.

Tanulmányunkban áttekintésre került a hibrid fenyegetések alapvetései nyomán a hagyományos médiára és az online közegre gyakorolt hatás fő tendenciája, illetve mindazok a lépések, amelyeket Európa annak érdekében tett, hogy ezek a platformok továbbra is elsősorban az európai értékek érvényesülési terei és ne a visszaélések domináns eszközparkjai legyenek. Az áttekintett döntések és szabályozási megoldások rávilágítanak az EU változási képességére, amelynek még lehet további fejlődése és dinamizálódása a jövőben, azonban tükrözi a reagálás szükségszerűségét is. A terrorista- és a hibrid fenyegetésekre reagáló európai média- és internetszabályozás alapvető európai jogi értékeket érint, melyekre a demokratikus berendezkedés épül. Egyértelműen tükrözi azonban az e téren tapasztalt változás azt is, hogy az új típusú biztonsági kihívások és fenyegetések a különféle jogok és értékek visszaélésszerű és illegitim alkalmazásával vagy végérvényesen aláássák ezen értékek működését vagy kikényszerítik e téren a változást az intézmények, a megoldások és a szükség szerinti korlátozások terén.

Figyelemmel a média és az internet világát érintő szakadatlan technológiai fejlődésre, magától értetődő, hogy e kérdéskör még nem jutott nyugvópontra. Tanulmá-

[74] Bless, 2011, 283.

nyunk célja erre figyelemmel egy olyan áttekintés volt, amely a hibrid fenyegetések sajátosságaihoz közelítve e tárgykört, alapot kíván adni a későbbi változások mélyebb értelmezéséhez és olyan elemzések elkészítéséhez a reagálás terén, amelyek megfelelően tudják szintetizálni a biztonsági és a médiatudományi aspektusokat.

IRODALOM

- Aczél Petra – Veszelszki Ágnes (szerk.) (2023): *Deepfake: A valótlan valóság.* Gondolat Kiadó, Budapest.
DOI: https://doi.org/10.1556/2065.185.2024.6.13.
- Argomaniz, Javier (2015): European Union responses to terrorist use of the Internet. In: *Cooperation and Conflict.* 2015/2. sz.
DOI: https://doi.org/10.1177/0010836714545690.
- Bakhtiar Ul Hassan, Muhammad (2022): *The EU Legal Framework and National Strategies for Monitoring Terrorist Content Online.* Nova School of Law, Lisbon.
- Bellanova, Rocco – de Goede, Marieke (2022): Co-Producing Security: Platform Content Moderation and European Security Integration. In: *JCMS.* 2022/5. sz.
DOI: https://doi.org/10.1111/jcms.13306.
- Bergh, Arild (2019): *Social network centric warfare - understanding influence operations in social media*. Norwegian Defence Research Establishment (FFI) 4 October.
- Bless, Roland (2011): Countering Terrorism while Protecting Freedom of the Media: A Crucial Balance for Governments. In: Ifsh (ed.): *OSCE Yearbook 2010*. Baden-Baden.
DOI: https://doi.org/10.5771/9783845229584-283.
- Bontridder, Noémi – Poullet, Yves (2021): The role of artificial intelligence in disinformation. In: *Data & Policy.* 2021/3. sz.
- Buckland, Michael (2017): *Information and Society.* MIT Press, Cambridge.
- Castells, Manuel (2005): *A hálózati társadalom kialakulása.* Gondolat-Infonia, Budapest.
- Castells, Manuel (2007): *Az évezred vége. Az információ kora.* Gondolat kiadó, Budapest.
- Cho, Sungbaek et. al. (2022): *Recent Cyber Events: Considerations for Military and National Security Decision Makers*. CCD CoE, Tallinn.
- Cornish, Paul (ed.) (2022): *The Oxford Handbook of Cyber Security.* Oxford University Press, Oxford.
DOI: https://doi.org/10.1093/oxfordhb/9780198800682.001.0001.
- Csizmadia Norbert (2016): *Geopillanat. A 21. század megismerésének térképe.* L'Harmattan, Budapest.
- Farkas Ádám – Kelemen Roland (2022): A közösségimédia-platformok és a hibrid konfliktusok kapcsolata. In: *In Medias Res.* 2022/1. sz., 96-108.
- Farkas Ádám (2023): Gondolatok a történeti tapasztalatok hasznosíthatóságáról a hibrid fenyegetések korában. In: Bódiné Beliznai Kinga – Gosztonyi Gergely (szerk.) (2023): *Jogtörténeti Parerga III. Ünnepi tanulmányok Mezey Barna 70. születésnapja tiszteletére*. ORAC kiadó, Budapest.
- García-Orosa, Berta L. (2021): *Disinformation, social media, bots, and astroturfing: the fourth wave of digital democracy*. (Elérhető: https://revista.profesionaldelainformacion.com/index.php/EPI/article/view/86730. Letöltés ideje: 2023.09.26.).
DOI: https://doi.org/10.3145/epi.2021.nov.03.
- Juhász Lilla – Pintér Róbert (2006): *Információs társadalom, információs stratégiák.* L'Harmattan, Budapest.

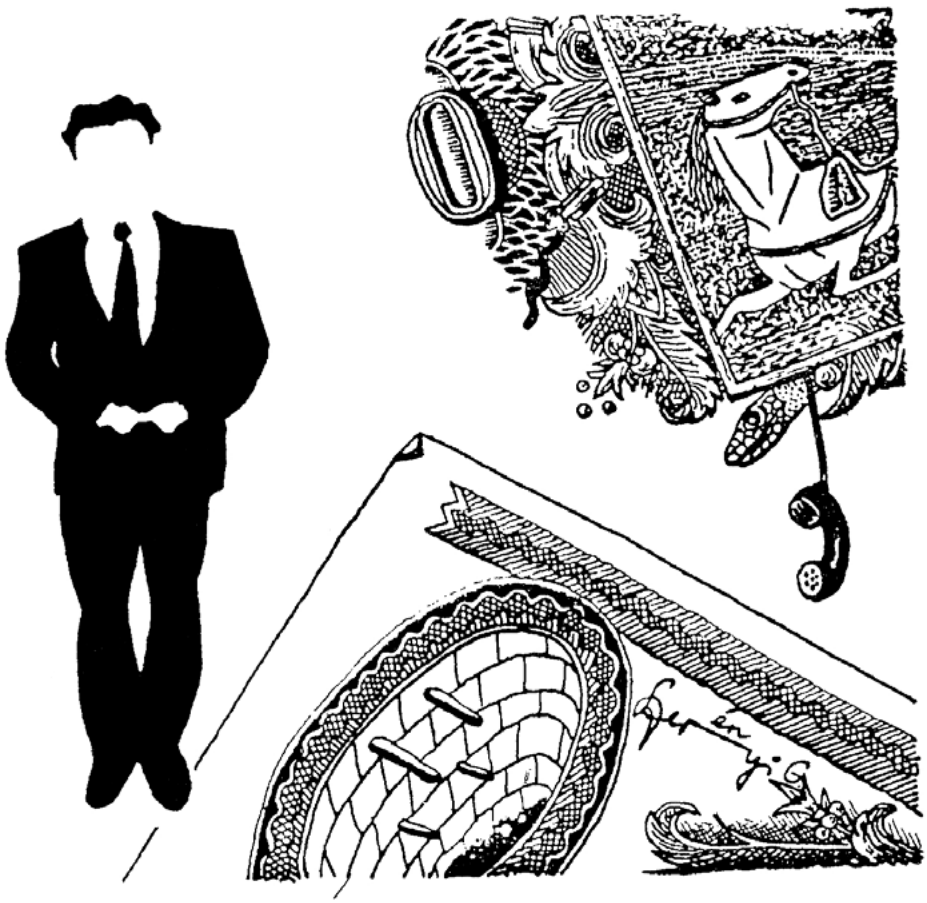
- Krekó Péter (2018): *Tömegparanoia – Az összeesküvés-elméletek és álhírek szociálpszichológiája.* Athenaeum Kiadó, Budapest.
- Lendvai Gergely Ferenc (2023): Media in war – a comprehensive overview of the European restrictions on Russian media. In: *European Papers, Special Focus on Ukraine.* 2023/3. sz.
- Mattelart, Armand (2004): *Az információs társadalom története.* Gondolat Kiadó, Budapest.
- Mazucchi, Nicolas (2022): *AI-based technologies in hybrid conflict: The future of influence operations*. Hybrid CoE Paper 14. (Elérhető: https://www.hybridcoe.fi/wp-content/uploads/2022/06/20220623-Hybrid-CoE-Paper-14-AI-based-technologies-WEB.pdf. Letöltés ideje: 2023.09.26.).
- McIntyre, Lee (2018): *Post-Truth.* MIT Press, Cambridge.
- Papp János Tamás (2023): A szűrőbuborék kipukkasztása – Gondolatok az online szűrőbuborékok és visszhangkamrák koncepciójának újraértelmezéséhez. In: Török Bernát – Ződi Zsolt (szerk.) (2023): *Digitalizálódó társadalom: Tanulmányok az új technológiák társadalmi-jogi hatásairól*. Ludovika Kiadó, Budapest.
- Parag Khanna (2016): *Konnektográfia. A globális civiláció jövőjének feltérképezése.* HVG Könyvek, Budapest.
- Peters, Michael A. – Rider, Sharon – Hyvönen, Mats – Besley, Tina (eds.) (2018): *Post-Truth, Fake News.* Springer Nature Singapore, Singapore.
DOI: https://doi.org/10.1007/978-981-10-8013-5_1.
- Pierozzi, Filippo (2017): *EU and Cyberterrorism. Added Value or Chimera?* Universitá Degli Studi Firenze, Firenze.
- Sanz-Caballero, Susana (2023): The concepts and laws applicable to hybrid threats, with a special focus on Europe. In: *Humanities and Social Sciences Communications.* 2023/10. sz.
DOI: https://doi.org/10.1057/s41599-023-01864-y.
- Slavan, Vladislav (2016): *Media Manipulation and Psychological War in Ukraine and the Republic of Moldova*. Centre for European Studies, Iasi. Vol. 8/2016, Iss. 4.
- Stengel, Richard (2019): *Information wars. How We Lost the Global Battle Against Disinformation and What We Can Do About It.* Atlantic Monthly Press, New York.
- Szitás Péter (2019): Paradigmaváltás a tömegmédia manipulációban: a post-truth korszak eszközei és stratégiái. In: Kiss Mária Rita – Sánta Tamás – Balogh Péter – Laki Ildikó – Szabó Péter (szerk.) (2019): *Tanulmányok a társadalomról IV.* A Szegedi Tudományegyetem Polgáraiért Alapítvány, Szeged.
- Tropina, Tatiana L. – Callanan, Cormac (2015): *Self- and Co-regulation in Cybercrime, Cybersecurity and National Security*. Springer, London, 2015.
DOI: https://doi.org/10.1007/978-3-319-16447-2.
- Vikman László (2022): Az aktuális kibertéri fenyegetések jogi kihívástérképe. In: *Katonai Jogi és Hadijogi Szemle.* 2022/3. sz.
- Vikman László (2022): Szempontok a kibertér egyes aktuális fenyegetéseinek jogi értékeléséhez. In: *Military and Intelligence CyberSecurity Research Paper.* 2022/4. sz.
- Wallerstein, Immanuel (2010): *Bevezetés a világrendszer-elméletbe.* L'Harmattan, Budapest.
- Wijnja, Kim (2022): Countering hybrid threats: does strategic culture matter? In: *Defence Studies.* 2022/1. sz..
DOI: https://doi.org/10.1080/14702436.2021.1945452.

JOGFORRÁSOK

- Az Európai Parlament és a Tanács 2010/13/EU irányelve (2010. március 10.) a tagállamok audiovizuális médiaszolgáltatások nyújtására vonatkozó egyes törvényi, rendeleti vagy közigazgatási rendelkezéseinek összehangolásáról (Audiovizuális médiaszolgáltatásokról szóló irányelv).
- Az Európai Parlament és a Tanács közös közleménye a hibrid fenyegetésekkel szembeni fellépés közös keretéről. JOIN/2016/018. https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52016JC0018. (Elérhető: https://www.eeas.europa.eu/eeas/countering-hybrid-threats_en. Letöltés ideje: 2023.09.26.).
- Az Európai Parlament és a Tanács rendelete az online terrorista tartalom terjesztésének megelőzéséről. (TERREG) (Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52018PC0640. Letöltés ideje: 2023.09.26.).
- EBU: European Parliament took an important step towards strengthening the European Media Freedom Act and ensuring media freedom in the digital sphere, 2023. (Elérhető: https://www.ebu.ch/news/2023/06/important-step-towards-european-media-freedom-act. Letöltés ideje: 2023.09.26.).
- EDRi: Disinformation and propaganda: It's all political!, 2021. (Elérhető: https://edri.org/our-work/disinformation-and-propaganda-it-is-all-political/. Letöltés ideje: 2023.09.26.).
- EU vs Disinfo. (Elérhető: https://euvsdisinfo.eu/. Letöltés ideje: 2023.09.26.).
- Európai Bizottság – Sajtóközlemény. Biztonság: az EU megerősíti a hibrid fenyegetésekkel szembeni válaszintézkedéseket, 2016. (Elérhető: https://ec.europa.eu/commission/presscorner/api/files/document/print/hu/ip_16_1227/IP_16_1227_HU.pdf. Letöltés ideje: 2023.09.26.).
- Európai Bizottság: Online félretájékoztatás: az internetes platformok fokozott átláthatóságára van szükség, 2018. (Elérhető: https://ec.europa.eu/commission/presscorner/detail/hu/IP_18_1746. Letöltés ideje: 2023.09.26.).
- Európai Bizottság: A dezinformáció visszaszorítását célzó uniós gyakorlati kódex. (Elérhető: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=59115. Letöltés ideje: 2023.09.26.).
- Európai Bizottság: Európai megközelítés az online félretájékoztatás kezelésére. COM (2018) 236 final, Brüsszel, 2018.4.26. 1.
- Európai Tanács: A Tanács a reziliencia megerősítésére és a hibrid fenyegetések, többek között a dezinformáció elleni küzdelemre szólított fel, 2020. (Elérhető: https://www.consilium.europa.eu/hu/press/press-releases/2020/12/15/council-calls-for-strengthening-resilience-and-countering-hybrid-threats-including-disinformation-in-the-context-of-the-covid-19-pandemic/. Letöltés ideje: 2023.09.26.).
- European Commission: EU Internet Forum: a major step forward in curbing terrorist content on the internet, 2016. (Elérhető: https://ec.europa.eu/commission/presscorner/detail/en/IP_16_4328. Letöltés ideje: 2023.09.26.).
- European Commission: European Democracy Action Plan: making EU democracies stronger. (Elérhető: https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2250. Letöltés ideje: 2023.09.26.).
- European Commission: European Media Freedom Act: Commission launches public consultation, 2022. (Elérhető: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_85. Letöltés ideje: 2023.09.26.).

- European Commission: Shaping Europe's digital future: Annual self-assessment reports of signatories to the Code of Practice on Disinformation 2019. (Elérhető: https://digital-strategy.ec.europa.eu/en/news/annual-self-assessment-reports-signatories-code-practice-disinformation-2019 Letöltés ideje: 2023.09.26.).
- European Commission: Shaping Europe's digital future: Final report of the High Level Expert Group on Fake News and Online Disinformation, 2018. (Elérhető: https://digital-strategy.ec.europa.eu/en/library/final-report-high-level-expert-group-fake-news-and-online-disinformation. Letöltés ideje: 2023.09.26.).
- European Commission: Shaping Europe's digital future: Tackling online disinformation. (Elérhető: https://digital-strategy.ec.europa.eu/en/policies/online-disinformation. Letöltés ideje: 2023.09.26.).
- European Commission: State of the Union 2021. (Elérhető: https://state-of-the-union.ec.europa.eu/state-union-2021_en. Letöltés ideje: 2023.09.26.).
- European Commission: Your rights in the EU. (Elérhető: https://commission.europa.eu/aid-development-cooperation-fundamental-rights/your-rights-eu_en. Letöltés ideje: 2023.09.26.).
- European Union External Action - The Diplomatic Service of the European Union: Countering hybrid threats, 2024. (Elérhető: https://www.eeas.europa.eu/eeas/countering-hybrid-threats_en. Letöltés ideje: 2023.09.26.).
- European Union External Action - The Diplomatic Service of the European Union: Questions and Answers about the East StratCom Task Force, 2021. (Elérhető: https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en. Letöltés ideje: 2023.09.26.).
- Google Blog - Around he Globe: Partnering to help curb the spread of terrorist content online, 2016. (Elérhető: https://blog.google/around-the-globe/google-europe/partnering-help-curb-spread-terrorist-content-online/. Letöltés ideje: 2023.09.26.).
- Jelentés az Európai Parlamentnek, az Európai Tanácsnak, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának a dezinformációval szembeni közös cselekvési terv végrehajtásáról. Brüsszel, 2019.6.14. JOIN (2019) 12 final. (Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52019JC0012&from=EN. Letöltés ideje: 2023.09.26.).
- Jelentés az Európai Parlamentnek, az Európai Tanácsnak, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának a dezinformációval szembeni közös cselekvési terv végrehajtásáról. Brüsszel, 2019.6.14. JOIN(2019) 12 final. (Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52019JC0012&from=EN. Letöltés ideje: 2023.09.26.).
- Microsoft Corporate Blogs, 'Facebook, Microsoft, Twitter and YouTube announce formation of the Global Internet Forum to Counter Terrorism' (26 June 2017). (Elérhető: https://blogs.microsoft.com/on-the- issues/2017/06/26/facebook-microsoft-twitter-youtube-announce-formation-global-internet-forum-counter- terrorism/. Letöltés ideje: 2018.01.15.).
- OECD Going Digital Toolkit - Policy Note. Disentangling untruths online: Creators, spreaders and how to stop them. (Elérhető: https://goingdigital.oecd.org/data/notes/No23_ToolkitNote_UntruthsOnline.pdf. Letöltés ideje: 2023.09.26.).
- OECD Policy Responses: Ukraine Tackling the Policy Challenges. Disinformation and Russia's war of aggression against Ukraine: Threats and governance responses, 2022. (Elérhető: https://www.oecd-ilibrary.org/docserver/37186bde-en.pdf?expires=1721931768&id=id&accname=guest&checksum=DBC308E087F87702BD95BA-32A94145B9. Letöltés ideje: 2023.09.26.).

• The New York Times Magazine: The Agency, 2015. (Elérhető: https://www.nytimes.com/2015/06/07/magazine/the-agency.html?smid=pl-share. Letöltés ideje: 2023.09.26.).
• Trend Micro: What is Red Teaming & How it Benefits Orgs, 2023. (Elérhető: https://www.trendmicro.com/en_se/research/23/a/what-is-red-teaming.html?irclickid=1ycwobwLxxyKWKCTV1wxR1%3AiUkC2u92NhTBsR00&irgwc=1. Letöltés ideje: 2023.09.26.).
• WhatsthePONT Blog: Can You Really Trust Social Media in a Crisis? The Rise of Troll Farms, 2015. (Elérhető: https://whatsthepont.blog/2015/09/09/the-rise-of-troll-farms-can-you-really-trust-social-media-in-a-crisis/. Letöltés ideje: 2023.09.26.).



Szerényi Gábor grafikája