KELEMEN ROLAND[1]

Radikalizálás, dezinformálás és tömegpszichózis modern köntösben: a hibrid konfliktus kibertérben

A radikalizálás, a dezinformálás, a tömegpszichózis alakítása egyik sem újkeletű fogalom, a hadviselés történetében mindegyik számtalanszor alkalmazott, használt eszköznek tekinthető. Ha mellé emeljük a hibrid hadviselést, és elhelyezzük benne a fenti fogalmakat, akkor még mindig azt kell mondani, hogy régi ismerős tekint vissza ránk. Ha csak a fogalommal szinte összemosott orosz állam 20. századi történelmét nézzük, akkor azt látjuk, hogy a Szovjetunióban óriási hagyományai voltak ennek a harcmodornak és a fenti eszközöknek. A két világháború közötti időszakban a balti államok, a hidegháborús időszakban pedig mi, magyarok, de a csehszlovákok, az afgánok és a grúzok is saját testükön érezhették azt a szovjet narratívát, hogy miként lehet elfoglalni más államok területét, vagy ott katonai műveleteket végrehajtani úgy, hogy annak megalapozását politikai, gazdasági nyomásgyakorlás tette lehetővé.[2]

A hibrid fenyegetések metódusa és a mögöttes fogalomrendszer a 2000-es évek második felétől váltak ismét széleskörben vizsgálat tárgyává, annak hatására, hogy a Hezbollah 2006-ban kézzelfogható katonai sikereket ért el Libanonban az Izraeli Védelmi Erők ellen.[3] Tovább fokozta ezt az Iszlám Állam tevékenysége, valamint Oroszország Ukrajnával szembeni műveletei és a Krím félsziget annexiója.

Feltehető a kérdés, hogy mi eredményezte a régi ismerős forradalmi átalakulását? A válasz szinte kézzelfogható: újszerűsége, reneszánsza „a korábban is alkalmazott nem katonai tényezők tárházának robbanásszerű gyarapodásának és ezáltal kialakulni látszó stratégiai dominanciájából, illetve ezek hatóerejének a társadalom- és technológiafejlődés miatti megerősödéséből következik”.[4] A mögöttes technológia- és társadalomfejlődés origóját pedig a kibertér és annak térnyerése jelenti. A kibertér alapjaiban szabta újra az állam működését és a társadalmi, gazdasági folyamatokat. A kibertér nem hozott létre önmagában új

[1] Jelen tanulmány megjelenése az Emberi Erőforrások Minisztériuma megbízásából az Emberi Erőforrás Támogatáskezelő által meghirdetett NTP-NFTÖ-20-B-0063 kódszámú pályázati támogatásból valósult meg.

[2] A hibrid hadviselés szovjet gyökereit lásd: Kilinskas, 2016, 139-158.

[3] Hoffman, 2007, 37.

[4] Farkas – Resperger, 2020, 132.

konfliktus-kategóriákat, hanem a meglévőket fejlesztette tovább, tette azokat hatékonyabbá és sokszorozta meg a korábbi erőhatásokat, fokozta végletekig a műveleti képességeket. Lehetővé tette ugyanis a hagyományos és nem hagyományos, katonai és nem katonai eszközök integrált alkalmazását, mégpedig valós idejű nyomon követéssel, visszacsatolással, koordinációval. Jelen tanulmány azt kívánja körbejárni, hogy a hibrid konfliktusok eszközparkjához tartozó radikalizálás, dezinformálás, tömegpszichózis formálásának területén a kibertér megjelenése miben jelentett forradalmian új perspektívát a támadó fél számára, mitől váltak oly hatékonnyá ezek a pszichológiai műveletek, és velük szemben milyen jogi jellegű fellépési lehetőségek vannak.

I. A KIBERTÉR SZINDIKALIZÁLÓ ÉS RADIKALIZÁLÓ HATÁSAI

A kibertér kiépülésének köszönhetően váltak ténylegesen globálissá az emberi interakciók, a gazdaság,[5] a kultúra. Eme változások jelentős hatást gyakoroltak az egyénre is, ugyanis a kibertér és annak használata egyértelműen képes befolyásolni az éntudatot, képes azt módosítani, „átprogramozni". Mindezt úgy, hogy új esélyt kínál az egyénnek: egy más közösséghez tartozást, a lehetőségek tárházát, akár úgy is, hogy látszatra a hagyományos létezése nem változik, valójában azonban teljesen felülírja azt. A „cyberkörnyezetben csökken az ítélőképesség és nő az impulzivitás, némileg hasonlóan ahhoz, ahogyan az alkohol hat ránk. A cyberközeg sajátos jellemzői – a külső kontroll vagy felügyelet hiánya, a névtelenség, a távolság, a fizikai elkülönültség érzete – elősegítik a gátlások levetkőzését."[6] Ez a kontrollvesztés önmagában növeli az ismeretlenek közötti szindikalizáció lehetőségét. Az új hálózatok méretüket tekintve minden korábbi társadalmi kapcsolati hálót meghaladnak, és számuk folyamatosan gyarapodik. Ehhez hozzájárul, hogy míg korábban a közösség egy földrajzilag jól lehatárolható területre összpontosult, és ezen belül tudtak kialakulni az azonos elvek mentén cselekvő személyek kapcsolatrendszerei is, mára ez teljesen átalakult. Így bár hagyományos térben az egyéni kapcsolatok visszaszorulása, elsorvadása figyelhető meg, addig a kibertérben az emberi létezés fokmérője a hálózathoz tartozás lett.[7] Az egyén mindent megtesz, hogy egy-egy közösség részese lehessen, míg mások céljaik eléréséhez használják az általuk vagy mások által kialakított hálózatokat.

A kibertér növeli a kialakított hálózatok testreszabottságát is, mivel a kialakult közösségek tagjai közötti interakciók a kibertérnek köszönhetően már országhatárokat, sőt kontinenseket is átlépnek. A hasonlóan gondolkodó egyé-

[5] Ennek hálózati és biztonsági hatásait lásd bővebben: Pongrácz, 2018, 41-61.; Németh, 2020, 23-41.; Németh, 2019, 307-325.
[6] Aiken, 2020, 35.
[7] Pintér, 2007, 25.

nek határok nélkül tudnak kommunikálni, egymással információkat megosztani, csoportokat létrehozni, hálózatokat szervezni.

Ezzel párhuzamosan pedig fokozódik ezeknek a hálózatoknak a közösségformáló szerepe. Hozzájárul ehhez a hálózatok hiperdiadikus jellege is. A hagyományos térben a viselkedési minták átvétele családtagok, barátok, osztálytársak, kollégiumi szobatársak stb. szokásainak másolásával történik meg, vagyis egy-egy viselkedési minta terjedése a legtöbbször lineárisan valósul meg. Ha ez a lineáris lánc megszakad, akkor ennek az új magatartási formának az átadása is meghiúsul. Ez a hiperdiadikus terjedés egy szervezetben, így például egy munkahelyen, kollégiumi közösségben, egyetemen már horizontálissá válik, bonyolultabb, és nehezebben visszakövethetőbbek a hatások, viszonthatások. Akkor ezt most helyezzük át a kibertérbe, ahol a hálózat tagjainak száma több ezerre, tízezerre, sőt akár millióra is emelkedhet. Itt egy-egy viselkedési minta átadásához, vírusszerű terjedéséhez nem kell az, hogy minden szereplő azt magáévá tegye, támogassa, elsajátítsa.[8] Az így kialakított hálózatoknak létrejönnek olyan tulajdonságai és funkciói, amelyek az egyéntől elszakadnak, azokra nincsen valós befolyásuk.[9] Hozzájárul ehhez a kibertérnek a gátlásokat háttérbe szorító jellege, valamint az is, hogy egyes csoportokon belül eltérő aktivitású, eltérő célú és eltérő végletekben gondolkodó szereplők vesznek részt. Ezekből adódóan a kibertérben létrejövő kapcsolati hálózatokban az egyén radikalizálódása rendkívül felgyorsul.

Az egyén radikalizálódása a csoporton belüli aktivitás fokozódása mellett a csoporton túlra ható (kiber)tevékenységekben figyelhető meg, így például közösségi oldalakon történő toborzás, az elveiknek, nézeteiknek megfelelő hírek terjesztése, saját nézeteik igazolása, akár – még nem hagyományos értelemben vett – agresszív módon is. A kontrollt vesztett egyén a legtöbb esetben ezzel az agresszióval még jogi normát nem sért. A kiberagresszió fogalma viszont rendkívül szemléletes – „*A cyberagresszió úgy értelmezhető, mint minden olyan, az egyén negatív érzelmeiből fakadó, cybertérben megnyilvánuló manifesztáció, ami magára a cselekvőre vagy másra nézve negatív hatású, vagy valamely normát sért, de még nem tartalmazza a fenyegetést és a kényszerítést, hanem azok megelőző, bevezető szakasza*”[10] –, hiszen kifejezésre juttatja, hogy az egyén itt lépi át a Rubicont, vagyis teszi meg az első olyan lépéseket, amelyek a későbbi, már akár bűncselekményi tényállást megvalósító cselekményhez vezethetnek. Sajnálatos módon a kibertér gátlásmódosító hatása okán az elkövetők legtöbbször – bár hagyományos térben legtöbbjük ilyent nem tenne – nem is

[8] Gondoljunk bele, a közösségi hálón mennyi olyan „kihívással” (ilyenek voltak többek között a dezodor-, a koronavírus-, a koponyatörő-, a kiki-, vagy a tüzes-kihívás) találkoztunk az elmúlt években, amely a digitális közösséghez tartozó egyének legtöbbjét sokkolta, azonban mégis óriási számú követőre talált. Lásd bővebben: Blog.generalielorelatok.hu: Coronavirus challenge..., 2020.
[9] Christakis – Fowler, 2010, 38-41.
[10] Kiss, 2020, 28.

érzékeli, hogy rendkívüli mértékben átlépte az emberek között kialakult kommunikáció hétköznapi normáit.[11] A radikalizálódása a hálózathoz kapcsolódó szereplőknek eltérő fokozatot ölt, pontosan abból adódóan, hogy eltérő magatartási mintákat vesznek át a szereplők a csoport többi tagjától. Így minél nagyobb méretű egy hálózat, annál kevésbé homogén a magatartási minták átvétele. A csoport attitűdje, a radikalizmusának szintje tehát nem az egyén felől határozható meg, mivel „a kapcsolati hálóknak makrószintű tulajdonságai vannak. A makroszintű tulajdonságok olyan, az egészre jellemző új vonások, amelyek a részek közötti kölcsönhatásokra és köztük fennálló kapcsolatokra vezethetők vissza."[12]

Nemcsak a kibertér gyakorol hatást a hagyományos térre, hanem az is viszonthatást gyakorol rá. A technológia ugyanis alapvetően társadalmi konstrukció, amely révén a hagyományos tér folyamatai nem szeparálhatók a kibertér folyamataitól; azok szorosan összefonódnak egymással.[13] Mivel az egyik hatást gyakorol a másikra, így alaptézisként fogható meg, hogy a hagyományos tér társadalmi feszültségei – legyenek azok politikai, vallási, ideológiai, kriminológiai jellegűek – ebben a globális belső kibertérben szintén megjelennek. Eme feszültségek ezekben a személyre szabott globális közösségekben azonban – ahol az egyén sérelme, érdeke, világlátása hatványozott számban és mértékben tudja formálni a hálózat többi tagjának értékrendjét, éntudatát – fokozott intenzitással jelennek meg. „Az online térben keletkező új normák átvándorolhatnak a való életbe. Ami tehát a virtuális világban történik, az hatással van a valóságos világra, és viszont... A technológia és az eszközök változásával a cyberkörnyezet is változik, és ez visszahat az emberi viselkedésre... Minél több a változás, annál több új helyzet áll elő, és csak még nagyobb lesz a zűrzavar."[14] Felismerték e tézist az állami és nemállami szereplők is, így céljaik eléréséhez, amennyiben szükségesnek vélik, a növekvő társadalmi feszültséget is kifejezésre juttatják, és a saját eszközeit, a globalizálódó technológiát és kultúrát fordítják szembe a hálózati világhoz csatlakozó ellenséges állammal vagy államokkal.[15]

Az egyének és csoportjaik cselekménye, vagyis „szinte minden, amit online teszünk, digitális kipárolgást, digitális port és digitális lenyomatot hoz létre".[16] Ezek pedig egy hibrid támadást megelőző feltérképezés során a támadó fél jegyzetébe kerülnek, amely törésvonalakat, ha érdemesnek látják, aktiválják és végletekig fokozzák. Ennek eszközei többek között a kiválasztott csoportba való beépülés, a propaganda és a dezinformálás.

[11] Tettük hivatkozási alapja az internet szabadsága és a véleménynyilvánítás szabadsága, annak valós tartalmát és korlátait természetesen nem ismerve. Lásd bővebben: Koltay, 2019, 107-128.
[12] Christakis – Fowler, 2010, 42.
[13] Escobar, 1994, 211-231.
[14] Aiken, 2020, 18., 25.
[15] Lásd bővebben: Bartkó, 2019; Dornfeld, 2019, 46-63.; Mezei, 2019, 125-147.; Tóth, 2016, 26-42.
[16] Aiken, 2020, 20.

II. DEZINFORMÁLÁS ÉS TÖMEGPSZICHÓZIS ALAKÍTÁSA A HIBRID KONFLIKTUS SORÁN

A kibertéri dezinformálás első megnyilvánulásai voltak, hogy terrorista csoportok kiberképességeket használtak támadási képességeik bővítése, hatékonyságuk növelése érdekében. A Hamasz a 2010-es évek elején dezinformációs és a tömeghangulatot befolyásoló eszközöket alkalmazott izraeli és nem izraeli e-mail címekre és telefonokra küldött álhíreket tartalmazó e-mailekkel és szöveges üzenetekkel, valamint propagandatartalmakkal. Az Iszlám állam már tovább fokozta ezt a tevékenységet; kifinomult és meglehetősen agresszív marketingkampányt folytattak, és magas szintre fejlesztették a kibertérben megjelenő pszichológiai hadviselést. Pakisztáni terroristák 2008-ban pedig arra is rávilágítottak, hogy valós idejű információgyűjtésre és koordinálásra is alkalmas a social media figyelése és az okostelefonon történő kommunikáció.[17]

Az állami szereplők felismerték az ilyen akciókban rejlő potenciált. „Ott, ahol az információs tér a hír- és véleménycsere piaca gyanánt minden felhasználó előtt nyitva áll, az állam pedig alig cenzúrázza, bárki terjeszthet szándékosan és stratégiai céllal kifinomult üzeneteket és folytathat felforgató tevékenységet, hogy az ellenfelet lélektanilag befolyásolja és egy bizonyos magatartásra késztesse."[18] Eltérően a korábbi koroktól, ehhez nem kell már repülőgép, az ellenség vonalai mögé bejuttatott ember, amely (aki) a röpiratokat, újsághíreket közzéteszi, hiszen az átpolitizált közösségi felületeken a támadó által kiválasztott, célhoz illeszkedő csoport tagjaihoz eljuttatott információk, hírmorzsák, fake news kiváltják a kívánt hatást. Ezt segíti az azonnali visszacsatolás lehetősége, vagyis, aki ismeri a támadás narratíváját, az látja, hogy az aktivált információk a szükséges hatást elérték-e, mégpedig valós időben. Így lehetősége nyílik arra, hogy nyomban tudja módosítani a stratégiát, illetve a következő, már jól előkészített tartalmat is elérhetővé tegye. A kiválasztott csoport vagy csoportok tagjai pedig az online platformok sajátosságai okán individualizált hírcsokrokhoz jutnak, vagyis az érdeklődési körhöz kötődő információk jelennek meg javarészt a felületeiken, így jószerével folyamatosan az előre jól lehatárolt támadási célokat szolgáló híranyaghoz jutnak az adott felhasználók. Ezen hírek egyre szélsőségesebb állításokat fogalmaznak meg. „A lényeg, hogy ellehetetlenítsék a tényeket, a nyilvános diskurzusba vetett bizalmat, a politikai helyzet szabad és ésszerű értékelését, valamint a konszenzusteremtést. Ezek helyére lépnek az alternatív tények, az érzelmi befolyásolás és a provokáció, hogy kételyt, bizalmatlanságot szítsanak és megosszák a társadalmat."[19]

Napjainkban ennek legkiválóbb terepei a social media platformok. Mivel a szólásszabadság és a médiaszabadság a demokrácia alapjai, így a social media felületén kialakult hálózatokat, csoportokat külső szereplők felhasználják

[17] Bachmann – Gunneriusson, 2015, 82-83.
[18] Hofstetter, 2020, 93.
[19] Hofstetter, 2020, 85.

támadásaik során. E felületek jelentős nyilvánossága lehetőséget teremt a rágalmazó, zaklató, doxing[20] vagy dezinformációs műveletek végrehajtására. Ennek során a jogi szabályozás kiskapuit, vagy még inkább a szabadságjogokat használják ki és forgatják vissza a megtámadott állammal szemben, aláásva ezzel az állami intézményekbe vetett bizalmat, polarizálva a társadalmat, felerősítve a meglévő törésvonalakat, vagy újakat generálva. Jól illusztrálja a folyamatot a franciaországi sárgamellényes tüntetésekkel kapcsolatos orosz fellépés. Már a mozgalom megszületésében és növekedésében is jelentős szerepe volt a Facebook-csoportnak, amit a magas üzemanyagárak és a rendkívül megemelkedett megélhetési költségek indikáltak. Problémát okozott az is, hogy a hagyományos média kezdetekben alig vette észre a szerveződést, mivel az egyes tagok a Facebook-csoporton belüli hírekre, üzenetekre, videókra támaszkodtak, az újságírók viszont inkább a Twitterre, ezért meglepte őket a helyzet súlyossága. Az Avaaz az eseményekkel kapcsolatban 2019 áprilisáig 105 millió álhírt számolt össze, ezek a politikai döntéshozókkal, a rendőrségi brutalitással, az ellenőrizhetetlen bevándorlással, a rasszizmussal és az idegengyűlölettel foglalkoztak. Oroszország hamis híreket terjesztett német, spanyol, holland, lengyel, svéd és olasz nyelven. Az RT orosz állami hírcsatorna néhány riportere részt vett a tüntetéseken, és úgy ábrázolta a helyzetet, mintha Párizs háborús övezet volna. A dezinformációs kampányból nem maradhatott ki a hagyományos média munkatársainak lejáratása sem, őket korruptnak, megbízhatatlannak, a kormánnyal mindenben összejátszónak mutatták be.[21] A 2016-os amerikai elnökválasztás is hasonló tapasztalatokat szült. Ekkor az orosz beavatkozás lényeges eleme volt, hogy a választások előtt a social media platformokon keresztül megfelelő hírcsomagokhoz juttassák a kiválasztott társadalmi csoportokat, ezzel megpróbálva befolyásolni a választások lehetséges kimenetelét.[22] Az események egyértelmű tanulsága volt, hogy a szembenálló nagyhatalmak kihasználják a social media által kínált lehetőségeket, és kis létszámú internetes közösségeket is képesek a mainstream média fölé emelni, ezáltal e platformok termékeny talajt biztosítanak az összehangolt és ellenséges propagandának és dezinformálásnak.

A Google, az Amazon, a Facebook és az Apple ellenőrzik a közösségi felületeket, így a politikai információkat is, a napi hírek kapuőrei, ami által a közbeszédet ők irányítják, ők döntenek a tartalmakról, vagyis arról, mi kerülhet ki nyilvánosan. „A szűrőbuborék-elmélet szerint az internetes kapuőrök a társadalmi kohézió gyengülését idézik elő azzal, hogy felhasználóiknak tetsző, az ő egyetértésükkel találkozó tartalmakat teszik leginkább láthatóvá."[23] Tehát a már amúgy is sajátos gondolkodás, elméletek, érdeklődés mentén polarizálódott közösségeket tovább erősíti a social media platform által összeállított hírfolyam, amellyel lényegében ezek a platformok már külső állam dezinformációs

[20] Személyről vagy szervezetről információk megszerzése és közzététele.
[21] Makela, 2019, 10-13.
[22] Rosenstedt, 2021, 5.
[23] Koltay, 2019b, 4.

tevékenysége nélkül is manipulálják az embereket. A felhozott ellenérv az, hogy lehetőség van az Interneten más típusú hírforrások felkutatására is, az átlag felhasználóra viszont ez nem jellemző, emellett pedig a keresőszolgáltatások szintén manipulálják a lehetséges találatok körét.[24]

A „... platformszolgáltatók működése sok tekintetben túllép a klasszikus állami jogi szabályozás joghatósági kérdésén. A szolgáltatások határok nélkülisége csak hozzájárul ahhoz, hogy a közösségi platformok a nemzetállami szuverenitás tanára épülő állami jogalkotási dokumentumokkal szemben bizonyos esetekben rezisztensek maradjanak. Egyúttal a közösségi platform szolgáltatói rendszerint maguk alkotnak szabályokat, amelyekkel lényegében meghatározzák a véleménynyilvánítás kereteit, a kimondhatóság határait, és ezen mechanizmusokhoz illeszkedő, normasértés esetén alkalmazható eljárásokat is bevezetnek."[25] Ezen eljárások során a szolgáltatók a jogellenes vagy csak valótlan tartalmakért viselt felelősséget áthárítják a felhasználóra, amely egy hibrid szcenárió esetében nagy valószínűség szerint nem is létező személy, így a felelősség valójában – a támadó állam nehezen bizonyítható nemzetközi közjogi felelősségén túl – erodálódik. A tartalmat algoritmusok segítségével kuratálják és személyre szabják, ez pedig segíti a szenzációhajhász közlések, a pletykák, a valótlanságok és a gyűlölet terjedését. Az algoritmusok azon túl, hogy üzleti érdekeket szolgálnak, valójában tervezőiknek a politikai elfogultságát és a kulturális értékeit tükrözik vissza, nem megfeledkezve arról, hogy maguk az algoritmusok is manipulálhatók. Jelentős probléma tehát, hogy a közzétett tartalmakat, véleményeket a szolgáltató saját érdeke, világnézete mentén szelektálja, így a magáncenzúrán[26] túl ezzel képes „... a társadalmi közvitát torzítani, tematizálni, akár politikai, akár gazdasági vagy más érdekből".[27] A social media platformok gyakorlata, üzleti modellje kedvez a fake news terjedésének, és adott esetben a trollok, provokátorok, gyalázkodók ellehetetlenítik a lokális párbeszédet, hiszen lényegében csak az üzemeltető által eltávolíthatók, kezelhetők.[28] Ezzel pedig közvetve, de kiszolgálja a támadó államot, a védekező állam eszköz nélkül marad.

III. AZ EURÓPAI UNIÓ FELLÉPÉSE A DEZINFORMÁCIÓS TEVÉKENYSÉGGEL SZEMBEN

Oroszország Ukrajna elleni tevékenységének hatására felismerte ezt az Európai Unió is, ezért 2015-ben felállították az East StratCom Task Force elnevezésű munkacsoportot, amelynek célja, hogy javítsa az Unió képességeit a külső

[24] Koltay, 2019b, 6.
[25] Klein, 2018, 233.
[26] Lásd ennek problémáját bővebben: Koltay, 2017, 129-140.; Koltay, 2018, 267-292.
[27] Klein, 2018, 235.
[28] Koltay, 2019, 10.

szereplők által előállított dezinformáció előrejelzése, felderítése és a reagálás területén. 2018-ban cselekvési tervet fogadtak el a félretájékoztatással szemben. Ez osztott tagállami és uniós intézményi fellépésről rendelkezett. A koordinált válasz négy pilléren nyugszik: (1) az uniós intézmények képességeinek javítása a félretájékoztatás eseteinek észlelése, elemzése és leleplezése területén; (2) a félretájékoztatással kapcsolatos koordinált és együttes válaszlépések megerősítése; (3) a magánszektor mozgósítása a félretájékoztatás elleni küzdelem érdekében; (4) tudatosság növelése és a társadalom rezilienciájának javítása. Azt az elvárást állította fel, hogy meg kell erősíteni azokat az uniós szerveket, amelyek a területen feladattal bírhatnak, emellett létre kell hozni egy riasztási rendszert, amely valós időben képes jelezni a dezinformációs tevékenységet, és a tagállamoknak ki kell jelölnie kapcsolattartó pontot. A magánszektor mozgósítása alatt a dokumentum a platformok szerepének hangsúlyozását és felelősségük kiemelését értette, mivel ezek nem kezelték megfelelően az érintett problémakört. A társadalmi ellenállóképesség növelése érdekében előirányozták a független tényellenőrzőkből álló csoportok létrehozását, akiknek feladata a dezinformálás feltárása és a közvélemény tájékoztatása.[29] Ennek érdekében elfogadtak egy önszabályozó gyakorlati kódexet, amelynek aláírói többek között vállalták, hogy elősegítik a megbízható tartalmak láthatóságát, mégpedig a félrevezető tartalmak csökkentése révén, valamint fokozzák a hamis fiókokkal szembeni fellépést, továbbá növelik a hirdetések és szponzorált tartalmak átláthatóságát.[30] Magyarországon 2021 tavaszán indult el a tényellenőrzők programja, a Facebook erre a feladatra az APF hírügynökséget vonta be.[31] Az ilyen csoportok hatékonysága mindamellett megkérdőjelezhető. Abból kiindulva, hogy a hibrid konfliktusok rendkívül összetettek, nemcsak a dezinformálásból álló cselekményeket ölelik fel, hanem számos soft, medium és hard eszköz és módszer is a tárházukban van, így példának okáért a gazdasági és pénzügyi műveletek, a kiberműveletek, valamint a bűnszervezetek, terrorista csoportok tevékenységének ösztönzése, finanszírozása, támogatása.[32] Ezeket a komplex – mondhatni totális – kihívásokat a fegyveres védelem ágazatai (honvédelem, rendészet, nemzetbiztonsági tevékenység) külön-külön sem tudják megfelelően kezelni. Szükségszerű az ilyen totális biztonsági kihívásokra[33] az ágazatok összehangolt, koordinált, információmegosztáson alapuló fellépése.[34] Ez értelem-

[29] Az Európai Bizottság és az Unió Külügyi és Biztonságpolitikai Főképviselőjének közös közleménye – Cselekvési terv a félretájékoztatással szemben, Brüsszel, 2018.12.15., Join(2018)36. Final.

[30] Klein, 2018, 246.

[31] A külső és főként független tényellenőr szavatolhatja, hogy egyetlen tagállam, állam se tudja a véleménynyilvánítás szabadságának korlátozására felhasználni a dezinformáció elleni fellépés eszközparkját. Utóbbi veszélyeit lásd bővebben: Gosztonyi, 2021, 91-101.

[32] Lásd: Rácz, 2014.

[33] Farkas, 2018.

[34] Farkas Ádám Magyarországon ezt 2015 óta szorgalmazza, és ennek kibontakozása tapasztalható a Védelmi és biztonsági tevékenységek összehangolásáról szóló 2021. évi XCIII. törvény elfogadásával, de ahogy arra Farkas is felhívta a figyelmet, ez a folyamat jóval szélesebb körű újraszabályozást, újraszervezést és mindezek előtt szemléletváltást igényel. Lásd: Farkas, 2015, 2-29.; Farkas, 2018b; Farkas, 2019.

szerűen becsatornázza a nemzetbiztonsági ágensek által megszerzett adatokat, amelyek mentén átfogóbb döntést tud hozni a megtámadott állam, míg a civil, polgári tényellenőrök ezen információk hiányában hozzák meg döntéseiket, javaslataikat, egy magánvállalat számára, amely továbbra sem ismeri az adott társadalmi valóságot és/vagy politikailag, ideológiailag elfogult. Az is kérdéses, hogy a magánszektor által kiválasztott, felkért tényellenőrök mennyiben függetlenek, vagy tudják magukat függetleníteni a magánvállalati célok, attitűd alól.

A cselekvési tervnek megfelelően 2019-ben létrehozták a Rapid Alert System-et. Ennek célja megkönnyíteni az információcserét és összehangolni a tagállami és uniós intézmények fellépését a dezinformációval szemben. Ennek érdekében 27 tagállami kapcsolattartó pontból álló hálózatot hoztak létre; feladatuk a koordinálás és a legjobb gyakorlatok megosztása. A megosztott hatáskörök miatt nehézkes a problémamegoldás, továbbra is fennmaradt a tagállami eszközpark.[35] A Covid–19[36] által okozott pandémiás helyzet ismét előtérbe helyezte a kérdéskört, mivel generált egy ún. infodémiát.[37] Az infodémia kapcsán az Unió számára is világossá vált, hogy különbséget kell tenni hamis vagy félrevezető tartalmak különböző formái között, így a jogellenes és a káros, de nem jogellenes tartalmak között. Utóbbiak esetében a dezinformálás akkor áll fent, ha megtévesztés, közérdeknek való károkozás vagy gazdasági károkozás szándékával tették közzé. Az ebből adódó dezinformációs tevékenység leküzdésének alapjául a korábbi cselekvési terv, a gyakorlati kódex és a gyors reagálású csoport gyakorlata szolgál. Ez nem több azonban, mint célirányos cáfolatok, mítoszrombolás és médiatudatossági kezdeményezések.[38] A fellépés tényleges eszközparkja tehát továbbra is a platformszolgáltatónál maradt. Annak ellenére, hogy a tartalmak fentebbi osztályozása, vagyis annak eldöntése, hogy a káros tartalom dezinformálás céljából került-e megosztásra, kizárólag tagállami hatáskörben valósulhat meg.

2020 decemberében az Európai Bizottság előterjesztette az Európai Demokráciára vonatkozó cselekvési tervet. Ennek negyedik pontja szól a dezinformáció elleni küzdelemről. Szorosabb együttműködés kialakítása mellett érvel a magánszektorral, a civil társadalommal, a tudományos élettel és az Unió nemzetközi partnereivel, azonban még mindig csak a hibrid konfliktus jobb megértése érdekében. Vagyis továbbra is csak ígéretként fogalmazták meg az eljárásrend

[35] Makela, 2019, 15.

[36] A Covid–19 által okozott helyzet sajtóra gyakorolt hatását lásd: Cendic – Gosztonyi, 2020, 14-29.

[37] A fogalmat a WHO vezette be és a következőképpen határozta meg: „az infodémia egy problémával kapcsolatos túlzott információáradat, amely megnehezíti a megoldás azonosítását. Magában foglalja az egészségügyi szükséghelyzet során terjedő félretájékoztatást, dezinformációt és pletykákat. Az infodémia hátráltathatja a hatékony népegészségügyi válaszintézkedéseket, továbbá zavart és bizonytalanságot kelthet az emberek körében." Lásd: WHO: Coronavirus disease 2019 (COVID-19) Situation Report - 45.

[38] Az Európai Bizottságnak és az Unió külügyi és biztonságpolitikai főképviselőjének közös közleménye: A Covid19-cel kapcsolatos dezinformáció kezelése – lássuk a valós tényeket, Brüsszel, 2020.6.10. Join(2020)8. Final.

hatálybaléptetését, a közös módszertani keret kidolgozását. A platformok esetében az általuk használt algoritmusok átláthatatlanságát, a hírekkel kapcsolatos – fentebb ismertetett – gyakorlatát kritizálta, amely problémákat a dokumentum szerint furcsamód csak a gyakorlati kódex értékelése során azonosították. A Bizottság véleménye szerint a dezinformálás elleni hatékony fellépés záloga a platformszolgáltatók erőteljesebb és világosabb kötelezettségvállalása, valamint a megfelelő felügyeleti mechanizmuson alapuló megközelítés kialakítása. A Bizottság álláspontja abban nem változott, hogy a dezinformálás elleni küzdelem egyik legfontosabb terepe a polgárok médiatudatos nevelése.[39]

A cselekvési tervnek megfelelően a Bizottság előterjesztette a digitális szolgáltatások egységes piacáról szóló rendeletjavaslatát. A rendelet célja az Alapjogi Chartában biztosított jogokat tiszteletben tartó, de biztonságos, kiszámítható és megbízható online környezet kialakítása. A javaslat meghatározza a jogellenes tartalom fogalmát: „bármely olyan információ, amely önmagában vagy egy tevékenységre való hivatkozással, beleértve a termékek értékesítését vagy a szolgálatások nyújtását, nem felel meg az uniós jognak vagy valamely tagállam jogának, függetlenül az adott jog pontos tárgyától vagy jellegétől”.[40] E jogellenes tartalmakra tekintettel engedi meg a rendeletjavaslat a tagállami igazságügyi vagy közigazgatási szerv határozatán nyugvó tartalom elleni fellépést, továbbá bármely személy vagy szervezet jogellenes tartalom bejelentésére irányuló tartalomfelülvizsgálati mechanizmus megindítását. Emellett a rendelet továbbra is lehetővé teszi a tartalommoderálást a platformok részéről. Egyértelműen előrelépés, hogy a platformok felelősségének megállapítását is lehetővé teszi a javaslat a jogellenes tartalmakért. A tartalommoderálással kapcsolatban pedig előírja, hogy évenként egyszer erről köteles jelentést tenni, amelynek része az önálló tartalommoderálás okai és alapja, s az ezekkel kapcsolatos belső panaszkezeléssel kapcsolatos információk megosztása és értékelése. Utóbbiból következik, hogy a platformoknak a korábbitól eltérően átlátható belső panaszkezelési rendszert kell működtetni, aminek része az eltávolítás, hozzáférhetetlenné tétel, a szolgáltatás felfüggesztésével vagy megszűntetésével kapcsolatos döntések felülvizsgálata és indokolása. Ezek már önmagukban olyan előrelépések, melyek a hibrid fenyegetések dezinformációs műveleteinek hatékonyságát csökkenthetik. Ilyennek tekinthető a rendelet 20. cikke is, aminek értelmében az online platformok felfüggeszthetik a szolgáltatás nyújtását olyan személynek, aki gyakran oszt meg nyilvánvalóan jogellenes tartalmat. Ezt szolgálja még az online hirdetések átláthatósága is, hiszen visszakövethetőbbé teszi az egyes félrevezető tartalmakat. Az online óriásplatformokkal szembeni plusz elvárás a kockázatértékelés, amely kiterjed olyan tartalmak megjelenhetőségére, amik

[39] Az Európai Bizottságnak közleménye az Európai Demokráciára vonatkozó cselekvési tervről. Brüsszel, 2020.12.3. COM(2020) 790 Final.

[40] Az Európai Bizottság javaslat Az Európai Parlament és a Tanács rendelete a digitális szolgáltatások egységes piacáról (digitális szolgáltatásokról szóló jogszabály) és a 2000/31/EK irányelv módosításáról, Brüsszel, 2020.12.15., 2020/0361(COD), 49. o., 2. cikk, g).

a társadalmi párbeszédre negatív hatással vannak. Ezen esetekben a kockázatcsökkentési intézkedésekkel megtörténhet többek között tartalommoderálás vagy szolgáltatás korlátozása.[41]

A javaslat rendelkezik arról, hogy ki kell dolgozni egy uniós válságkezelési protokollt, amely lehetővé teszi a hatékony, átlátható fellépés lehetőségét közbiztonságot vagy közegészségügyet veszélyeztető helyzetekben. A protokoll kidolgozóinak feladata lesz annak meghatározása, hogy mi minősül rendkívüli körülménynek, valamint mely szerveknek biztosít hatáskört és milyen hatáskört, továbbá a válságkezelési protokoll bevezetésének eljárását. Itt azonban érdekes összeütközés lehet az uniós és tagállami hatáskörök között, hiszen a közbiztonság, belbiztonság alapvetően tagállami hatáskör. Kérdéses az is, hogy a válsághelyzet azonosítható-e a belső jogrendi különleges jogrenddel, annak egy digitális verziója, mondhatni egy kibertéri különleges jogrendje. Ezen esetekben nehezen elfogadható, hogy egy tagállam hibrid támadás esetében, ahelyett, hogy önállóan intézkedjen és kérje a platformszolgáltatótól, hogy korlátozzon bizonyos tartalmakat, helyette az uniós válsághelyzeti protokoll hatályba léptetését kivárva, az óriásplatform-szolgáltatók kapcsolattartási pontján keresztül próbálja érdekeit érvényesíteni. E megoldással tehát lényegében az óriásszolgáltatók egyetlen kapcsolattartási ponton keresztül kommunikálnak a tagállamokkal.[42] Kérdéses, hogy egy tagállamot érintő politikai jellegű különleges jogrend[43] esetében, amilyet alapvetően egy hibrid szcenárió elő kíván idézni, az uniós mechanizmus beindítható-e késleltető politikai csatározások nélkül, illetve a kapcsolattartási ponton keresztül elérhető órásplatform szolgáltató ilyen esetekben kötelezhető-e a fellépésre? További problémát jelent, hogy a rendelet a jogellenes tartalmakkal foglalkozik. Azonban egy hamis információ, ahogy fentebb a demokrácia cselekvési terv esetében az Unió is megjegyezte, nem feltétlen jogsértő. Vagyis a nem jogsértő hamis információk elleni fellépés lehetőségét az óriásplatform-szolgáltató kockázatelemző tevékenységi körében szabályozza csak a rendelettervezet, így tagállami közbenjárásra ilyen tartalom moderálása maximum az eszkaláció magasabb fokát – bár jelenleg nem tudjuk mennyire magas e fok – jelentő válságkezelési protokoll aktiválása után lesz lehetséges. Mivel ez egy uniós intézmény lesz, ebből adódóan nem, vagy csak részlegesen tud illeszkedni az egyes tagállamok társadalmi valóságához, nem feltétlen tudja kezelni azokat a töréspontokat, amelyeket egy hibrid konfliktus esetében kezelnie kell a megtámadott államnak.

[41] DSA 6-28. cikk.
[42] DSA 37-38. cikk.
[43] Lásd: Kelemen, 2018, 59-86.

IV. ÖSSZEGZÉS

A kibertér sajátosságai, így például a ténylegesen globális interakciók, az anonimitás látszata, a tematizált hálózatok létrehozásának a lehetősége felgyorsította az egyének szindikalizálódási képességét és a radikalizálódás lehetőségét. A hibrid konfliktus reneszánszát jelentő 2000-es években a terrorista csoportok aktívan használták ennek lehetőségét, majd ezt felismerve az állami szereplők, valamint az Iszlám Állam már rendkívül jól összehangolt marketing- és pszichológiai műveleteket hajtottak végre.

Oroszország hibrid akciói óraműpontossággal megtervezett dezinformációs műveleteket foglaltak magukba, amelyek révén mesterien használták ki a támadott állam társadalmi törésvonalait. E szcenáriók közül a legismertebb és legszélsőségesebb eredményt hozó az Ukrajnát ért támadás volt. Azonban hamar világossá vált, hogy a hibrid eszközpark egyes módszerei – így a dezinformálás – alacsonyabb intenzitású és más célú támadásokban is alkalmazhatók. Ez volt megfigyelhető a 2016-os amerikai elnökválasztás során, vagy a francia sárgamellényes tüntetések esetében is. A dezinformációs kampányok sikerességét fokozták a social media platformokon kiépült, sokszor átláthatatlan kapcsolati rendszerek, hálózatok, valamint maguknak a platformoknak a tartalommoderálási tevékenysége, a hírfolyamok összeállításának a gyakorlata, vagyis a szűrőbuborékok közösségre kártékony hatása. E platformok a legtöbb esetben az állam feletti magáncenzorként, szabályozóként léptek fel felületeiken, amely elősegítette a támadó állam céljainak érvényesülését.

Az Európai Unió 2015 után lépett fel a dezinformálás ellen, azonban tényleges intézkedések alig történtek.[44] A cselekvési tervek nem jelentettek módosulást a platformszolgáltatók mindennapos gyakorlatában. A Covid–19 pandémia viszont ismét világossá tette, hogy égető szükség van a fellépésre. A 2020-as demokrácia cselekvési terv és a közzétett rendeletjavaslat már előrelépést jelent, mivel a platformszolgáltatókat is részlegesen felelőssé teszi a jogellenes tartalmakért, a bejelentési mechanizmust és a tartalommoderálást, valamint az azzal szembeni panaszt átláthatóvá kívánja tenni. Mindemellett azonban a hamis, de nem jogellenes tartalmakkal szembeni fellépés lehetősége továbbra is korlátozott, pedig egy hibrid konfliktus alapját inkább ezek jelentik. Az óriásplatformok kockázatelemző tevékenysége során ezeket moderálhatják, de csak ha úgy értékelik, hogy a társadalmi párbeszédet torzítják. Lényegében továbbra is a szolgáltató diszkrecionális döntése ez. A kidolgozandó válságkezelési protokoll a közbiztonságot vagy közegészségügyet veszélyeztető válságok esetében

[44] Többek között fontos, hogy célként jelölték meg a társadalmi ellenállóképesség fokozását, amely irányába azonban konkrét lépések nem történtek. Kiemelendő, hogy ennek egyik módja lehetne a kutatási programok összehangolása a köz- és a magánszféra, valamint az egyetemek között, valamint a biztonságtudatos felhasználók képzése, amely nem merülhet ki a hagyományos informatikai mérnöki képzésekben, hanem már a középiskolákban és az egyetemek más szakjain is meg kell, hogy jelenjen. Lásd: Szépvölgyi, 2021, 135-142.

teszi lehetővé a korlátozásokat. Ez már az eszkaláció magasabb fokát jelenti, és erősen kérdéses, miként egyeztethető össze ez a tagállamok védelmi hatáskörével, mennyire lesznek kiszolgáltatva az egyes tagállamok az uniós döntéshozatali mechanizmusnak egy külső, hibrid kihívás során.

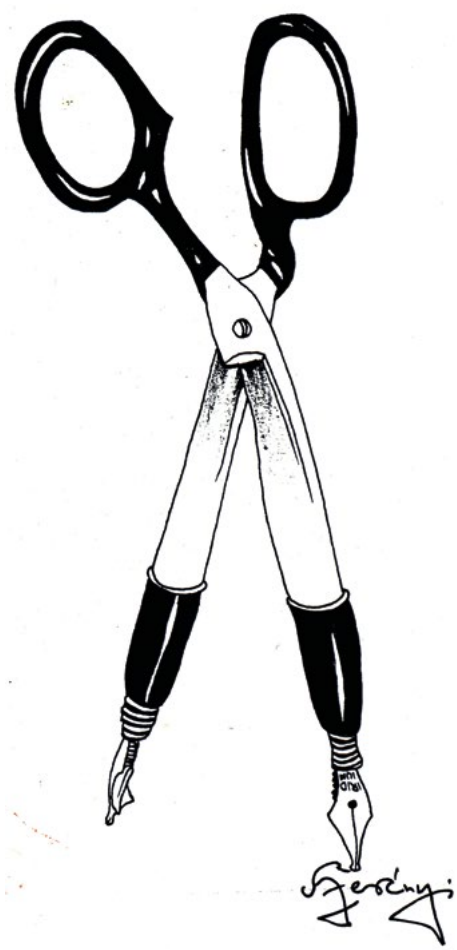
FORRÁSJEGYZÉK

- Aiken, Mary (2020): *Cybercsapda – Hogyan változtatja meg az online tér az emberi viselkedést?* Harmat Kiadó, Budapest.
- Bachmann, Sascha-Dominik – Gunneriusson, Hakan (2015): Hybrid wars: The 21st Century's new threats to Global Peace and Security. In: *South African Journal of Military Studies.* 2015/1. sz.
- Bartkó Róbert (2019): *Az irreguláris migráció elleni küzdelem eszközei a hazai büntetőjogban*. Gondolat Kiadó, Budapest.
- Blog.generalielorelatok.hu: Coronavirus challenge és a legveszélyesebb netes kihívások, 2020. (Elérhető: https://blog.generalielorelatok.hu/biztonsag/coronavirus-challenge-es-veszelyes-internetes-kihivasok/. Letöltés ideje: 2021.05.31.).
- Cendic, Kristina – Gosztonyi, Gergely (2020): Freedom of Expression in times of Covid-19: chilling effect in Hungary and Serbia. In: *Journal of Liberty and International Affairs, Institute for Research and European Studies – Bitola.* 2020/6. sz.
- Christakis, Nicholas A. – Fowler, James H. (2010): *Kapcsolatok hálójában. Mire képesek a közösségi hálózatok, és hogyan alakítják sorsunkat?* Typotex, Budapest.
- Dornfeld László (2019): Kiberterrorizmus – a jövő terrorizmusa? In: Mezei Kitti (szerk.): *A bűnügyi tudományok és az informatika*. Pécsi Tudományegyetem Állam- és Jogtudományi Kar, MTA Társadalomtudományi Kutatóközpont, Budapest–Pécs.
- Escobar, Arturo (1994): Welcome to Cyberia – Notes on the Anthropology of Cyberculture. In: *Current Anthropology.* 1994/3. sz.
- Farkas Ádám (2015): Szemléletváltást védelmi aspektusban!: Gondolatok a fegyveres erő hazai polgári kontroll-rendszeréről és annak korábbi modelljéről, különös tekintettel a fegyveres erő rendeltetésére és a felette kialakított alkotmányos szabályozási és hatalom-megosztási sémára, valamint a különleges jogrendi szabályozásra. In: *Pázmány Law Working Papers.* 2015/18. sz.
- Farkas Ádám – Resperger István (2020): Az úgynevezett „hibrid hadviselés" kihívásainak kezelése és a nemzetközi jog mai korlátai. In: Farkas Ádám – Végh Károly (szerk.): *Új típusú hadviselés a 21. század második évtizedében és azon túl.* Zrínyi Kiadó, Budapest.
- Farkas Ádám (2018): *A totalitás kora? A 21. század biztonsági környezetének és kihívásainak totalitása és a totális védelem gondolatkísérlete.* Magyar Katonai Jogi és Hadijogi Társaság, Budapest.
- Farkas Ádám (2018b): *Az állam fegyveres védelmének alapvonalai és Kiegyezést követő polgári evolúciója.* Széchenyi István Egyetem Állam- és Jogtudományi Doktori Iskola, Győr.
- Farkas Ádám (2019): *Az állam fegyveres védelmének alapvonalai.* Katonai Nemzetbiztonsági Szolgálat, Budapest.
- Gosztonyi Gergely (2021): Az internet-hozzáférés korlátozásának gyakorlata az Emberi Jogok Európai Bírósága előtt. In: *In Medias Res.* 2021/1. sz.
- Hoffman, Frank G. (2007): *Conflict in the 21st Century: The Rise of Hybrid Wars.* Potomac Institute for Policy Studies, Arlington.

- Hofstetter, Yvonne (2020): *Láthatatlan háború, avagy miképpen fenyegeti a digitalizáció a világ biztonságát és stabilitását.* Corvina, Budapest.
- Kelemen Roland (2018): A kivételes hatalom szabályozásának elméleti rendszere, honvédelmi kapcsolódásai és megvalósulása a dualizmus kori Magyarország. In: Farkas Ádám (szerk.): *A honvédelem jogának elméleti, történeti és kortárs kérdései.* Dialóg Campus Kiadó, Nordex Kft, Budapest.
- Kilinskas, Kestutis (2016): Hybrid Warfare: an Orienting or Misleading Concept in Analysing Russia's Military Actions in Ukraine? In: *Lithuanian Annual Strategic Review.* 2016/1. sz.
- Kiss Tibor (2020): *Agresszió a cybertérben.* Nemzeti Közszolgálati Egyetem, Budapest.
- Klein Tamás (2018): Harmadik rész: Cyberjog I. fejezet: Az online nyilvánosság alkotmányjogi vonatkozásai. In: Klein Tamás – Tóth András (szerk.): *Technológia jog – Robotjog – Cyberjog.* Wolters Kluwer, Budapest.
- Koltay András (2017): Az internetes kapuőrök és az emberi jogok európai egyezményének 10. cikke – A sajtószabadság új alanyai. In: *Állam- és Jogtudomány.* 2017/Különszám.
- Koltay András (2018): Az újmédia kapuőreinek hatása a médiaszabályozásra. In: Koltay András (szerk.): *Tíz tanulmány a szólásszabadságról.* Wolters Kluwer, Budapest.
- Koltay András (2019a): Az internet szabályozása és a szólásszabadság alapkérdései. In: *A bírói hatalom gyakorlásáról szóló 1869. évi IV. törvénycikk megalkotásának 150. évfordulójára.* Kúria – HVG-Orac, Budapest.
- Koltay András (2019b): A social media platformok jogi státusa a szólásszabadság nézőpontjából. In: *In Media Res.* 2019/1. sz.
- Makela, Jarmo (2019): Countering Disinformation: News Media and Legal Resilience. In: *Hybrid CoE Paper.* 2019/1. sz.
- Mezei Kitti (2019): A szervezett bűnözés az interneten. In: Mezei Kitti (szerk.): *A bűnügyi tudományok és az informatika*. Pécsi Tudományegyetem Állam- és Jogtudományi Kar, MTA Társadalomtudományi Kutatóközpont, Budapest–Pécs.
- Németh Richárd (2019): Kibertámadások gazdasági vonatkozásai a vállalati szférában. In: Dernóczy-Polyák Adrienn (szerk.): *Kutatási jelentés 1.* Universitas-Győr Nonprofit Kft., Győr.
- Németh Richárd (2020): Kiberfenyegetettség nagyvállalati környezetben. In: *Magyar Bűnüldöző.* 2020/2. sz.
- Pintér Róbert (2007): Úton az információs társadalom megismerése felé. In: Pintér Róbert: *Az információs társadalom – Az elmélettől a politikai gyakorlatig*. Gondolat – Új Mandátum, Budapest.
- Pongrácz Alex (2018): A hálózat csapdájában? Globalizáció és totalitás. In: Farkas Ádám (szerk.): *Védelmi alkotmányosság az új típusú biztonsági kihívások erőterében*. Magyar Katonai Jogi és Hadijogi Társaság, Budapest.
- Rácz András (2014): Oroszország hibrid háborúja Ukrajnában. In: *Külügyi és Külgazdasági Intézet Tanulmányok.* 2014/1. sz.
- Rosenstedt, Lina (2021): Improving Cooperation with Social Media Companies to Counter Electoral Interference, In: *Hybrid Coe Paper.* 2021/5. sz.
- Szépvölgyi Enikő (2021): Kiberbiztonság – mindannyiunk felelőssége. In: *Katonai Jogi és Hadijogi Szemle.* 2021/1. sz.
- Tóth Zoltán Balázs (2016): Az Iszlám Állam online térhódítása. In: *Nemzetbiztonsági Szemle.* 2016/4. sz.
- WHO: Coronavirus disease 2019 (COVID-19) Situation Report - 45. (Elérhető: https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200305-sitrep-45-covid-19.pdf?sfvrsn=ed2ba78b_4. Letöltés ideje: 2021.05.31.).

EGYÉB FORRÁSOK

- Az Európai Bizottság és az Unió Külügyi és Biztonságpolitikai Főképviselőjének közös közleménye – Cselekvési terv a félretájékoztatással szemben, Brüsszel, 2018.12.15., Join(2018)36. Final.
- Az Európai Bizottságnak és az Unió Külügyi és biztonságpolitikai főképviselőjének közös közleménye. A Covid19-cel kapcsolatos dezinformáció kezelése – lássuk a valós tényeket, Brüsszel, 2020.6.10. Join (2020)8. Final.
- Az Európai Bizottságnak közleménye az Európai Demokráciára vonatkozó cselekvési tervről. Brüsszel, 2020.12.3. COM(2020) 790 Final.
- Az Európai Bizottság javaslat Az Európai Parlament és a Tanács rendelete a digitális szolgáltatások egységes piacáról (digitális szolgáltatásokról szóló jogszabály) és a 2000/31/EK irányelv módosításáról, Brüsszel, 2020.12.15., 2020/0361(COD), 49. o., 2. cikk, g).



Szerényi Gábor, Twin pens

Szerényi Gábor, Enterieur