A közösségimédia-platformok és a hibrid konfliktusok kapcsolata

FARKAS ÁDÁM* – KELEMEN ROLAND**

1. Bevezetés

A hibrid konfliktusok képében bizonyos szempontból egy régi ismerős tekint vissza ránk, egy valóban újszerű formában.[1] 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. 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 művelteket 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 viszonyulás, 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 Ludendorf totális háborújában megjelent.

Így szemlélve tehát, ha a hibrid fenyegetéseket a katonai és a nem katonai tényezők és célok kombinált alkalmazásaként fogjuk fel, nem mondhatjuk, hogy a jelenség magja újszerű lenne. Feltehető a kérdés, hogy mi eredményezte mégis a régi ismerős forradalmi átalakulását, amelynek révén mára a hadviselés új generációjáról, sőt a biztonsági környezet gyökeres változásáról beszélünk. A válasz világos: újszerűsége a „korábban is alkalmazott nem katonai tényezők tárházának robbanásszerű gyarapodásából és ezáltal kialakulni látszó stratégiai dominanciája-

* Tudományos munkatárs, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar.

** Adjunktus, Széchenyi István Állam- és Jogtudományi Kar; tudományos munkatárs, Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar.

[1] Lásd Williamson Murray – Peter R. Mansoor: *Hybrid Warfare: Fighting Complex Opponents from the Ancient World to the Present.* Cambridge, Cambridge University Press, 2012; Ofer Fridman – Vitaly Kabernik – James C. Pearce (szerk.): *Hybrid Conflicts and Information Warfare. New Labels, Old Politics.* Boulder-London, Lynne Rienner, 2019.

ból, illetve ezek hatóerejének a társadalom- és technológiafejlődés miatti megerősödéséből következik".[2] A mögöttes technológia- és társadalomfejlődés origóját pedig a digitalizáció és annak – különösen, de nem kizárólag társadalmi – térnyerése jelenti. Ez ugyanis alapjaiban szabta újra az állam működését és a társadalmi, gazdasági folyamatokat az egyéni szintű interakciók széles körétől a napi szokásokon át a csoportos és társadalmi szintű viszonyulásokig. Ezzel pedig a stratégiai – és ezek között hadászati – célokra is használható nem katonai tényezők szerepe páratlan mértékben megnőtt. Míg tehát a történelem korábbi szakaszaiban ezek a tényezők korlátozott szereppel bírtak, hiszen kiaknázásukhoz fizikai jelenlétre volt szükség, addig ma a digitalizáció által részben feloldott fizikai kötöttségek miatt sokkal nagyobb szerepe van a nem katonai tényezőknek, mint korábban valaha.

A jelen tanulmány célja ennek a változásnak különösen a közösségimédia-platformokra vetített áttekintése, de oly módon, hogy a megértést szolgáló példák és a transzatlanti térség jogállamai előtt álló elvi kihívások mellett elsőként arra is rávilágítson, milyen jellemzőkkel írható le az a biztonsági környezet és abban a hibrid narratíva, amelyben a digitális tér e markáns új szelete ilyen rendkívüli szerepre tett szert a biztonság viszonylatában is.

2. A biztonsági környezet hibriditásának alapvonalai

A hibriditás védelmi és biztonsági vonatkozásai kapcsán jellemzően három fogalom keveredik gondolkodásunkban: a hibrid hadviselés, a hibrid konfliktus, valamint a hibrid fenyegetés. Ezek szoros összefüggésben állnak egymással, de nem tehető közéjük egyenlőségjel. Keveredésük azonban tévútra viheti mindazokat, akik a katonai-stratégiai értelmezésnél tágabb kontextusban kívánják megérteni ezeket a jelenségeket, márpedig a jelenleg zajló orosz–ukrán háború ellenére korunk biztonsági környezetét ez a kérdéskör a hagyományos katonai konfliktusok terepénél jóval nagyobb mértékben szövi át.

E három kategória tehát a tág értelemben vett biztonsági környezet hibriditásának tagolásaként is felfogható, amelyek egymáshoz viszonyított megértése azért is fontos, mert rá tud világítani arra, hogy egy hibrid szcenárió szerinti beavatkozásra készülő állami vagy nem állami szereplő milyen módokon, mikor és mennyire elhúzódó módon építheti fel a megcélzott állam vagy közösség ellen megvalósítandó tevékenységeinek láncolatát. Fontos e tekintetben arra külön is felhívni a figyelmet, hogy az államok közti rivalizálásban, sőt a nem állami szereplők államhatalommal szembeni fellépéseiben is hagyományosan nagy szereppel bír a társadalom, amely az állam hatalmának legitimációs és egyben élő alapját adja. A digitalizáció és különösen annak az egyénitől a társadalmi szintig terjedő hatásai ugyanis könnyebben elérhetővé teszik ezt a hagyományosan fontos társadalmi dimenziót, amivel sokrétű lehetőséghalmazt nyitnak meg mindhárom hibrid narratíva előtt. A hibrid hadviselés – hibrid konfliktus – hibrid fenyegetés reláció ugyanis ebben a sorrendben a szűkebbtől a tágabb kategória felé halad, amit ezért érdemes ehelyütt kibontani.

[2] Farkas Ádám – Resperger István: 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 –intézményi és jogi kihívások.* Budapest, Zrínyi, 2019, 132.

A *hibrid hadviselés* egyértelműen katonai értelemben vett, főbb elemeiben katonai gondolkodásmód szerint és eszközrendszer segítségével megvalósított fellépést jelent. Ha nemzetközi jogi értelemben nem is, tartalmi értelemben ez egy háborúmegvívási formulaként is felfogható.[3] Bár az amerikai szóhasználat miatt kedvelt a „hadviselés" kifejezés jelzős szerkezettel való megjelenítése számos új típusú kihívás kapcsán – például információs hadviselés, kiber hadviselés, pszichológiai hadviselés –, fontos rögzíteni, hogy a hadviseléshez tartalmilag szükséges legalább egy olyan fél, amely haderőként, a hadviselés szabályaihoz igazodva lép fel a szembenállásban. Ebben az értelmezésben a hibriditás nagyrészt azt jelenti, hogy a katonai szembenállás megvívása nem tisztán és nem kizárólag katonai eszközök és tényezők alkalmazásával valósul meg.

A szembenállás azonban jól azonosítható és földrajzilag is behatárolható, e kereten belül pedig jelentős részben a katonai gondolkodás stratégiai-hadműveleti-harcászati dimenzióiban bevett sémákra épít. Szigorúan értelmezve az orosz–ukrán szembenállást, álláspontunk szerint a hibrid hadviselésről onnantól célszerű beszélni, ahonnan a felek nyíltan katonai eszközökkel és a hadviselésre jellemző szerveződéssel, katonai műveleti keretek között léptek fel egymás ellen. Kiemelendő persze, hogy a hibrid hadviselésben a katonai megközelítés és működés dominanciája mellett érvényesül a nem katonai tényezők kiaknázása, vagyis azok mögött sok esetben – magas eszkalációnál többségében – a katonai műveleti célok támogatása azonosítható.

E körben beszélhetünk a katonai tevékenységet segítő nem katonai kibertéri cselekményekről, diplomáciai és gazdasági lépésekről, valamint rendkívül jellemző módon olyan információs és kommunikációs törekvésekről, amelyek célja a szemben álló fél erőinek, nemzetközi és nemzeti támogatottságának destabilizálása. Ez utóbbi körben pedig a digitális térnek kimagasló szerepe van az emblematikus személyes történetek propagálásától kezdve a veszteségszámok eltérő kommunikációján át a szembenálló felek egymás ellen vívott, de lényegében a globális társadalmi tér digitális szférájának egészére kiterjeszthető dezinformációs műveleteiig. A digitális tér fizikai kötöttségektől függetlenedő hatóképessége pedig azért is fontos, mert a jelenleg zajló háború kapcsán is jól látható, hogy a katonai-stratégiai célokat támogató lépések egyik fél részéről sem korlátozódnak a műveleti terület lakosságára, hanem kiterjednek a konfliktusra reagáló valamennyi állam digitális közösségeire is, amennyiben azokban reagálási hajlandóság mutatkozik.

A *hibrid konfliktus* az értelmezés következő – tágabb – osztályozási szintje lehet a gondolatrendszerünkben. E körben is jellemző a katonai stratégiai célok fajsúlyos megjelenése, azok előmozdítása vagy elérése, de az időbeli és a funkcionális horizont jelentősen kiszélesedik. Ebben az értelmezésben is egyértelműen azonosítható egy konkrét szembenállási helyzet. Ez a belbiztonsági krízis szintjén túllépő, esetileg vagy földrajzilag lehatároltan a fegyveres konfliktusra jellemző vonásokkal is párosul. Ebben a megjelenési formában azonban a katonai dimenzió helyett vagy mellett a különféle nem katonai tényezők szimultán alkalmazásának van kimagasló jelentősége. E körben például olyan nem nemzetközi fegyveres konfliktusos jelleg is azonosítható, amelyben csak fenntartásokkal bizonyítható egy szembenálló fél katonai jelenléte, mivel inkább szakadár, illetve polgárháborús jelleget ölt a konfliktus, mint háborúsat.

---

[3] Bettina Renz – Hanna Smith: *Russia and Hybrid Warfare – Going beyond the Label.* Helsinki, Aleksanteri Institute, 2016, https://bit.ly/3xmN793; Kateryna Zarembo – Segiy Solodkyy: *The Evolution of Russian Hybrid Warfare: The Case of Ukraine.* Washington, Center for Europan Policy Analysis, 2021, https://bit.ly/3aZMXwU.

A hibrid konfliktus vonatkozásában a külső beavatkozás tekintetében a megcélzott államon belül szított fegyveres szembenállással közel azonos értékű súlyt kaphatnak a nem katonai tényezők. E tekintetben a gazdasági és a diplomáciai nyomásgyakorlástól a nemzetközi jogi fellépésen át a titkosszolgálati eszközökkel megvalósuló destabilizációs, dezinformációs és befolyásolási műveletekig terjedő paletta rendkívül széles.[4] Ebben a perspektívában a kibertér alkalmazása már a katonai dimenzión messze túlmutató jelentőséggel bír, elsősorban a döntéshozatal és a társadalmi támogatottság aláásása kapcsán. A hibrid konfliktus tehát felfogható egy köztes állapotként is,[5] amikor jelen lehet már egyfajta katonai jellegű szembenállás vagy annak a perspektivikus lehetősége – akár szövetségi szinten is –, de a nyílt, háborús vonásokkal bíró konfliktus helyett még a nem katonai szférákban zajló beavatkozások súlya tekinthető meghatározónak.

Úgy is mondhatjuk, hogy a hibrid konfliktusban már egyértelmű a direkt és közvetlen szembenállás, de annak megvívásában még nem a katonai erő dominál, hanem a nem katonai tényezők széles körű és stratégiailag szervezett alkalmazása a szembenálló fél stabilitásának aláaknázása, potenciális – a katonai narratívára is kiterjedő – cselekvési lehetőségeinek korlátozása érdekében. A hibrid konfliktus tehát felfogható a hibrid hadviselés előkészítéseként is, de nem jelenti azt, hogy a konfliktusból szükségképpen háborús vagy nyílt katonai szembenállás következne. A hibrid konfliktusnak tehát a hibrid hadviselésbe való átlépés lehetséges, de eshetőleges következménye, ami egyfelől a katonai dimenzión túlmutató beavatkozásokat alapoz meg, másfelől azonban a szembeálló fél korlátozásán belül az esetleges katonai műveletek előkészítését szolgáló beavatkozásokkal is operál.

Mindezekhez mérten a *hibrid fenyegetés* a legtágabb kategóriaként ragadható meg.[6] Itt a nyílt katonai fellépés távlatos lehetőségként vagy a többi cselekménnyel szembeni reakciók mérséklésére szolgáló elrettentésként jelenik „csak" meg. A katonai erő a fellépés hátterében, a geopolitikai versengésbe ágyazottan van jelen. A fenyegetési palettán lényegében a nem katonai tényezők alkalmazása dominál, de a katonai stratégiai gondolkodásból merített szisztematikusság és a nagyhatalmi pozícióerősítés érdekében, vagyis olyan céloktól vezérelve, amelyek a történelem korábbi szakaszaiban hagyományosan katonai erővel voltak biztosíthatók, ma azonban ezek direkt alkalmazása nélkül is előmozdíthatók. Ennek fontossága abban rejlik, hogy a nyílt katonai fellépés egyértelműen korlátozó-romboló reakciót vált ki az agresszor nemzetközi kapcsolataira és gazdasági pozícióira nézve, míg az ezt elkerülő hibrid narratíva kiválthat szankciókat, de teljes körű politikai-gazdasági ellentevékenységet nem tud megalapozni.

A hibrid fenyegetésben kulcspozíciót töltenek be a titkosszolgálati eszközök és módszerek, a társadalmi tényezők, a különféle – a beavatkozóhoz közvetlenül nem köthető – nem állami szereplők, valamint a politikai és gazdasági térben megvalósuló cselekmények. Ez persze azt is feltételezi, hogy a hibrid fenyegetések eszközként való alkalmazása többéves vagy akár évtizedes felépítési és alkalmazási ciklusba ágyazottan valósítható meg. A digitális tér jelentősége ebben a

---

4 Frans-Paul van der Putten et al. (szerk.): *Hybrid Conflict: The Roles of Russia, North Korea and China.* Hága, Clingendael Institute, 2018.

5 Mariusz Balaban – Pawel Mielniczek: *Hybrid Conflict Modeling,* https://bit.ly/3tx5hUi.

6 Eugenio Cucumano – Marian Corbe (szerk.): *A Civil-Military Response to Hybrid Threats.* Cham, Palgrave Macmillan, 2018.

szférában az információs és a pszichológiai műveletekbe ágyazottan a legnagyobb,[7] hiszen kiváló terepet biztosít a humán tényezőre épülő destabilizációs és befolyásolási műveleteknek az egyénitől a társadalmi szintig. Lényegét tekintve úgy is fogalmazhatnánk, hogy a hibrid fenyegetéseknek döntően, de nem kizárólag a digitális térre épített cselekményei adják a bevezetőben említett régi ismerős valóban új megjelenési formájának esszenciáját. Ez a legtágabb kategória végső soron valamely hatalmi szereplő szisztematikus, térben rendkívül tág, akár globális keretben is megvalósuló, rövid, közép- és hosszú távú stratégiai célok elérésére egyaránt alkalmas, nem katonai eszközökre építő, de a katonai erő bevonásának lehetőségével, illetve a katonai és a titkosszolgálati erők nem hagyományos feladatkörben történő alkalmazásával párosuló fellépések összességeként fogható fel.[8]

Ha ezt elvonatkoztatjuk a konkrét szereplők cselekvési sémáitól, akkor lényegében a biztonsági környezet hibriditásával is azonosítható az az újszerűség, hogy az infokommunikációs robbanás miatt az állami és a nem állami szereplők tervezési, szervezési és beavatkozási lehetőségei páratlan mértékű növekedésen estek át. Az persze, hogy a különféle hatalmi szereplők háborús fellépés keretein kívül, nem katonai eszközök felhasználásával avatkoztak be egyes államok és társadalmak működésébe akár későbbi katonai fellépésük előkészítése, akár a háborús szándéktól független érdekek érvényesítése érdekében, nem új a történelemben. Az sem újszerű, hogy a hatalmi szembenállás korábbi eszközrendszere és jellege jelentősen átalakult a technológiai fejlődés nyomán, hiszen a 20. századi totális háború – igaz, a hadviselésen belül, de – hasonlóan korszakos változást hozott magával.

A 21. század biztonsági környezetében az az igazi újdonság, hogy a valóban globális kapitalista gazdasági rendszer és annak szürke és fekete tartománya, valamint a glóbusz egészét behálózó és az emberek korábban nem látott tömegeit elérő, valós idejű infokommunikáció révén olyan változások sora megy végbe a mindennapi életet érintően, amelyek miatt az állami és nem állami szereplők érdekérvényesítő lépéseiben alapvető érdek a beavatkozásokat a katonai konfrontáció szintje alatt tartani. Olyan célok és olyan mérvű beavatkozások valósulnak meg jelenleg is, amelyek korábban nagyrészt katonai erővel voltak elérhetők, de a szembenálló fél pozícióinak gyengítése, a nemzetközi béke és biztonság rendszerének kikerülése érdekében alapvető cél, hogy ne nyílt katonai szembenállás útján történjen a hatalmi fellépés. Úgy is fogalmazhatnánk – korábbi kutatásainkra és a skandináv térség államainak kiújuló totális védelmi felfogására figyelemmel –, hogy a hibrid fenyegetések szisztematikus alkalmazása vált a fő fellépési irányná, ha úgy tetszik, totális biztonsági kihívási környezetet teremtve ezzel.[9] Ez persze – ahogy az

---

[7] Lásd William E. Leigher: Cyber Conflict in a Hybrid Threat Environment: Death by a Thousand Cuts. Helsinki,Hybrid CoE 2021; Daniel P. Bagge: *Unmasking Maskirovka: Russia's Cyber Influence Operations.* New York, Defense, 2019.

[8] Georgios Giannopoulos – Hanna Smith – Marianthi Theocharidou: *The Landscape of Hybrid Threats: A Conceptual Model. Public Version.* Luxembourg, European Union, 2021.

[9] A téma kapcsán lásd Farkas Ádám: *A totalitás kora?* Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2016; NATO SHAPE: Exercise Trident Juncture 18: Total Defence Concept, https://bit.ly/2Rpj4Xq; Ieva Bērzina: Total Defence as a Comprehensive Approach to National Security. In Nora Vanaga – Toms Rostoks (szerk.): *Deterring Russia in Europe. Defence Strategies for Neighbouring States.* London, Routledge, 2019, 71–89.; James Kennet Wither: Back to the Future? Nordic Total Defence Concepts. 20 *Defence Studies* (2020) 61–81.; Swedish Defence Commission Secretariat: *Resilience. The Total Defence Concept and the Development of Civil Defence 2021–*

orosz–ukrán háború is mutatja – nem zárja ki a nyílt katonai szembenállás lehetőségét, de azt is formálja működésében.

Ennek a hibrid fenyegetési mátrixnak és az ebben rejlő – feltehetően – történelmi léptékű újdonságnak a fő hozadéka a nem katonai vagy hagyományosan nem védelmi és biztonsági tényezők szerepének felértékelődése és védelmi-biztonsági rendszerbe kapcsolásának megkerülhetetlenségén túl az, hogy lényegében folyamatossá teszi az államok védelmi és biztonsági, illetve társadalmi és információközvetítő rendszereire is nehezedő nyomást. Ez a módszer ugyanis a társadalmi közegbe ágyazva tudja leginkább kifejteni hatását, méghozzá akkor, ha az egy szerves és hosszú idejű beágyazódás eredményeként jön létre. Ebből is következik, hogy a hibrid fenyegetések keretében használt eszközök és módszerek sok esetben magasan konspiráltak a valódi célokkal való összefüggés tekintetében, továbbá az információs csatornák, gócpontok vagy véleményformáló entitások hitelességének kialakítása és megóvása érdekében.

Ez a fajta „köztünk élő" ellentevékenység pedig csak a különféle biztonsági események átfogó megközelítés mentén történő folyamatos elemzésével, az érintett állami szervek és társadalmi szerveződések kooperációjával, valamint a biztonságtudatosság erősítésével azonosíthatók és mérsékelhetők. Ez a védelmi és a biztonsági rendszerek jelentős reformját és az állami-társadalmi ellenállóképesség fokozását teszi elsődleges feladattá a biztonság hatékony garantálása érdekében a hibriditás korában. Fontos azonban kiemelni, hogy a hibrid fenyegetések elleni fellépés vonatkozásában kiemelt figyelmet kell szentelni a tradicionális európai értékek megóvásának és lehető legteljesebb fenntartásának, hiszen az eltúlzott reakciók állami-társadalmi torzulást idézhetnek elő, ami nem kívánt módon épp az ellenérdekelt tevékenységek céljainak elérését segítheti elő. A megfelelő megoldás megtalálásában tehát az aktuális helyzetekre adott válaszok mellett kiemelt szerepe van az elemzésnek, az értékelésnek, mindezek mellett a tudományos vizsgálódásnak és a problémakör tudományterületeken átívelő megvitatásának is. Egy rendszerszerű és jól strukturált, széles eszköztárra építő fenyegetéssel szemben ugyanis a gyors, pillanatnyi és adott jelenségekre korlátozódó válaszok csak szépségtapaszt, nem pedig megoldást jelentenek.

Természetesen a hibrid fenyegetések körében a jól kiaknázható eszközrendszer és a komplex biztonság szinte minden szektorára kiterjedő fellépési lehetőség az, ami a hibriditás újdonságát adja, a hibrid fenyegetések mellett a hibrid konfliktusok és a hibrid hadviselés terén is jelentős hatást fejt ki. Az a technológiai robbanás ugyanis, amely a társadalmi-gazdasági-politikai-biztonsági környezetet gyökeresen átalakította, jelentős fejlesztéseket indukált a védelmi és a biztonsági eszköz- és módszerrendszer tekintetében is. Ebből adódóan azonban az infokommunikációs forradalom előnyeinek kiaknázása a konfliktusok és a hadviselés tekintetében új, potenciális sérülékenységeket is magával hozott. Nem véletlen, hogy ezekben a vonatkozásokban a *warfare* kifejezés divatos használatán túl lényegében valóban új fegyvernemek jelentek meg a technológiai újításokkal.

A kiber hadviselés és a kibertér műveleti területté nyilvánítása ennek a fejlődési folyamatnak a legkézenfekvőbb példája, hiszen a digitalizáció a hagyományos kommunikációs csatornákon messze túllépve a harceszközök és a harci járművek működését és irányítását is áthatja, ame-

2025, https://bit.ly/3MS17wZ; *Support and Cooperation. A Description of the Total Defence in Norway.* Oslo, Norwegian Ministry of Defence – Norwegian Ministry of Justice and Public Security, 2018.

lyek korrumpálása vagy bénítása ezáltal a szemben álló fél kiemelt céljaként jelenik meg. Hasonlóan fontos a kiber domain lehetőségeinek kiaknázása a hibrid konfliktusok átmeneti vagy ingoványos terepén is, hiszen az egyszerre mozdíthatja elő a nem katonai eszközökkel elérendő stratégiai célok teljesülését és készítheti elő a katonai beavatkozást. Érdemes tehát ennek a vonatkozásnak a további elemeit mélyebben is kielemezni, és mind a hibrid fenyegetések, mind a hibrid konfliktusok, mind pedig a hibrid hadviselés újdonságai kapcsán belátni azt, hogy minden egyes új jelenség végül visszatükröződik a digitális térben, méghozzá azzal a céllal, hogy információs úton befolyásolja a feleket.

Erre kézenfekvő példa az elmúlt időszakból az az internetes információs hullám, amely mind az örmény–azeri, mind az orosz–ukrán harccselekmények tekintetében szabályos kampányként zajlott le a dróntechnológia hagyományos páncélos hadviseléssel szembeni sikerei kapcsán. Ez ugyanis az adott konfliktusok tekintetében demoralizációs hatást célzó információs művelet, a konkrét konfliktusok keretein kívül pedig a technológiai fejlődés hadviselésre gyakorolt hatásaival kapcsolatos információs csomag, amely már a világ minden táján relevanciával bírhat a konkrét fegyveres cselekményekhez való érzelmi és tudati kapcsolódás nélkül is. Érdemes azonban ezt a fajta, az információs térben való megjelenést konkrét példákon keresztül is továbbgondolni.

3. A közösségi média mint a modern kori információs műveletek egyik kiemelt színtere

A közösségi média és a mai értelemben vett – digitális alapú – információs műveletek azonos forrásra vezethetők vissza: az információs forradalomra és az annak hátterét adó robbanásszerű technológiai fejlődésre. Ebből adódóan nem meglepő, hogy az idő előrehaladtával a két különböző időpontban és eltérő szándékkal kialakult intézmény útjai keresztezték egymást. A két fogalom és közös keresztmetszetük ugyanis megtestesíti a digitális társadalomhoz, a digitalizálódó államhoz kapcsolódó technológia hasznosíthatóságának, felhasználhatóságának Janus-arcúságát. Az egyik oldalról a közösségi média korábban soha nem látott módon – és részleteiben még meg nem ismert pszichológiai hatásokat kiváltva – egyszerűsíti le az emberek közötti kapcsolatteremtést, kapcsolatmegosztást, a hálózatok alakítását, a kommunikációt, azonban a másik oldalról a felhasználói adatok integritása jelentős problémát jelent,[10] emellett az információhoz jutás befolyásolhatósága, az információ valós tartalma és a fiatalkorú felhasználókat ért abúzushatások is kérdéseket vetnek fel.[11]

---

[10] Mind a platformüzemeltetők, mind a külső szereplők által. Lásd Péter Bányász: Social Engineering and Social Media. *Nemzetbiztonsági Szemle,* 2018/5., 59–77.; Bányász Péter: *Közösségi média és közszolgálat.* Budapest, NKE Közigazgatási Továbbképzési Intézet, 2020.

[11] A probléma akut, hiszen óriási lelki terhet jelent a gyermekek számára, hogy az online térben, annak eszközei és sajátos jellemzői révén jelentősen felerősödött a korábbi hagyományos térben ismert abúzus hatása. Nem véletlen, hogy Magyarország is saját digitális gyermekvédelmi stratégiával rendelkezik. Lásd bővebben Mary Aiken: *Cybercsapda. Hogyan változtatja meg az online tér az emberi viselkedést?* Budapest, Harmat – Új Ember, 2020; Sorbán Kinga: A bosszúpornó és *deepfake* pornográfia büntetőjogi fenyegetettségének szükségességéről. *Belügyi Szemle,* 2020/10., 81–104.; Kiss Tibor – Pari Katalin – Prazsák Gergő: *Cyberdeviancia.* Budapest, Dialóg Campus,

Ezek mind-mind jelentős társadalmi feszültségeket generálnak, sőt sok esetben nemzetbiztonsági kockázatokat rejthetnek magukban. A fenti hatásokat minden állam felismerte: kihasználják annak előnyeit (információs műveletek, vagyis többek között a közösségi média negatív impulzusainak felerősítése[12]), és detektálták annak társadalmi, nemzetbiztonsági kockázatait (társadalmi, illetve jogi sérülékenység). E kockázatok kizárását egyes államok drasztikus lépésekkel, állampolgáraik lehető legteljesebb, totális megfigyelésével, korlátozásával akarják kikapcsolni.[13] Azonban az euroatlanti régió államainak jogállami keretei és szellemi értékei ezt nem tehetik lehetővé, így ezen államoknak egy ettől alapjaiban eltérő megoldást kell kialakítaniuk e problémák orvoslása, kezelése érdekében. Mindehhez viszont elsődlegesen a probléma széles körű feltárása, mélységi megismerése szükségeltetik.

A kibertéri dezinformálás első megnyilvánulásai azok voltak, amikor a terroristacsoportok kiberképességeket használtak támadási lehetőségeik 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 fokozta ezt a tevékenységet; kifinomult és meglehetősen agresszív marketingkampányt folytatott, és magas szintre fejlesztette a kibertérben megjelenő pszichológiai hadviselést. Pakisztáni terroristák 2008-ban pedig arra is rávilágítottak, hogy valós idejű információgyűjtésre és koordinálásra is alkalmas a közösségi média figyelése és az okostelefonon történő kommunikáció.[14]

A fenti történésekkel párhuzamosan 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 azt, bárki terjeszthet szándékosan és stratégiai céllal kifinomult üzeneteket, és folytathat felforgató tevékenységet, hogy az ellenfelet lélektanilag befolyásolja és egy bizonyos magatartásra késztesse".[15] Tehát a jogállamok, amelyek biztosítják a közösségimédia-platformokon is a lehető legteljesebb körben a véleménynyilvánítás szabadságát, önmaguk egyik legalapvetőbb krédója által válhatnak támadhatóvá, hiszen eltérően a korábbi koroktól, a tömegek félretájékoztatásához már nincs szükség repülőgépre, hogy az ellenség vonalai mögé röpiratokat, megtévesztő tartalmú újsághíreket juttathassanak, ugyanis az átpolitizált közösségi felületeken a támadó által kiválasztott, célhoz illeszkedő csoport tagjaihoz eljuttatott információk, hírmorzsák és a *fake news* kiváltják a kívánt hatást.

2019; Mezei Kitti: Az online gyermekpornográfia és a büntetőjog. *Ügyészek Lapja,* 2021/4., 19–30.; Magyarország Digitális Gyermekvédelmi Stratégiája, https://bit.ly/3xioHgQ.

12 Bányász Péter: A közösségi média mint az információs hadszíntér speciális tartománya. *Hadmérnök,* 2017/II. különszám, 108–121.

13 Például Kína a társadalmi pontrendszerrel és az Aranypajzs, vagyis a kínai nagy tűzfal révén kívánja megvalósítani, de ebbe a körbe sorolható Szingapúr okosváros projektjeibe burkolt megfigyelési rendszere, az iráni „halal" internetprojekt, az orosz internet kialakítása is. Ezeket lásd Gergely Gosztonyi: Special Models of Internet and Content Regulation on China and Russia. ELTE Law Journal, 2021/2., 87–99.; Vincent Mosco: Okosvárosok a digitális világban. Budapest, Pallas Athéné, 2019; Kelemen Roland: Cyberfare state – egy hibrid állammodell 21. századi születése. *Military and Intelligence CyberSecurity Research Paper,* 2022/1., 1–32.

14 Sascha-Dominik Bachmann – Hakan Gunneriusson: Hybrid Wars: The 21st Century's New Threats to Global Peace and Security. 1 *South African Journal of Military Studies* (2015) 82–83.

15 Yvonne Hofstetter: *Láthatatlan háború, avagy miképpen fenyegeti a digitalizáció a világ biztonságát és stabilitását.* Budapest, Corvina, 2020, 93.

Ezt segíti az azonnali visszacsatolás lehetősége, vagyis aki ismeri a támadás narratíváját, az látja, mégpedig valós időben, hogy az aktivált információk elérték-e a kívánt hatást. Így lehetősége nyílik arra, hogy nyomban módosítsa a stratégiát, és a következő, már jól előkészített tartalmat is elérhetővé tegye. A kiválasztott csoport(ok) tagjai pedig az online platformok sajátosságai okán individualizált hírcsokrokhoz jutnak, vagyis javarészt az érdeklődési körükhöz kötődő információk jelennek meg a felületeiken, így az adott felhasználók jószerével folyamatosan az előre jól lehatárolt támadási célokat szolgáló híranyaghoz jutnak hozzá. Ezek a hírek egyre szélsőségesebb állításokat fogalmaznak meg. A „lényeg, hogy ellehetetlenítsék a tényeket, a nyilvános diskurzusba vetett bizalmat, a politikai helyzet szabad és észszerű értékelését, valamint a konszenzusteremtést. Ezek helyére lépnek az alternatív tények, az érzelmi befolyásolás és a provokáció, hogy kételyt, bizalmatlanságot szítsanak, és megosszák a társadalmat."[16]

Ennek a jelenségnek a legkiválóbb terepét a közösségimédia-platformok adják. Mivel a szólás- és a médiaszabadság a demokrácia alapja, a külső szereplők felhasználják a közösségi média felületén kialakult hálózatokat, csoportokat a támadásaik során. E felületek jelentős nyilvánossága lehetőséget teremt a rágalmazó, zaklató, *doxing*[17] 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 egy Facebook-csoportnak, amelyet a magas üzemanyagárak és a rendkívül megemelkedett megélhetési költségek indukáltak. Problémát okozott az is, hogy a hagyományos média kezdetben 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.[18] Az Avaaz az eseményekkel kapcsolatban 2018 novembere és 2019 márciusa között a Facebookon megjelent száz legnézettebb álhírt vizsgálta meg,[19] ezek a politikai rendszerellenességgel (28%), a rendőrségi brutalitással (27%), a mozgalom nem valós, koholt támogatottságával (19%), az állami cenzúrával (14%), az ellenőrizhetetlen bevándorlással, a rasszizmussal és az idegengyűlölettel (10%), valamint egyéb, nem kategorizált kérdésekkel (2%) foglalkoztak.[20]

Oroszország aktívan közreműködött a hamis hírek terjesztésében, így német, spanyol, holland, lengyel, svéd és olasz nyelven adta közre ezeket a hírcsomagokat. 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] Megdöbbentő módon a vizsgált száz valótlan hírt több

16 Uo., 85.

17 Személyről vagy szervezetről információk megszerzése és közzététele.

18 Jarmo Makela: Countering Disinformation: News Media and Legal Resilience. 1 *Hybrid CoE Paper* (2019) 10–13.

19 Többek között a politikai dezinformáció ellen is küzdő civil szervezet, https://bit.ly/2P7uIKj.

20 Yellow Vests Flooded by Fake News: Over 100M Views of Disinformation on Facebook. *Avaaz Report* 15/03/2019, https://politi.co/3NOxYEq, 5–6.

21 Makela i. m. (18. lj.) 10–13.

mint négymillióan osztották meg, és ezeket több mint százöt millió ember tekintette meg. A teljes képhez hozzátartozik, hogy az öt legnagyobb francia hírszolgáltató (köztük a *Monde,* a *Figaro* vagy a France24) YouTube-csatornája összesen kicsit több mint 24 millió embert ért el a vizsgált eseményhez kapcsolódó tartalmakkal, míg a dezinformációs kampány központi orgánuma, az RT France, több mint 30 milliós forgalmat generált ebben az időszakban. [22]

Ezek az adatok önmagukban alátámasztanák egy-egy ilyen hibrid dezinformációs kampány hatásosságát, azonban ha még hozzáveszük az egyes tartalmak terjedési sebességét és az azokra adott szolgáltatói reakciót, akkor még élesebben kirajzolódik a probléma nagysága. Az egyik megosztott tartalom vérző fejű civileket ábrázol, akik a poszt állítása szerint a rendőri brutalitás áldozataivá váltak. Ezt a posztot 2018. november 20-án tették közzé, rövid idő alatt 136 ezren osztották meg és több mint 3,5 millióan nézték meg. Valójában kiderült, hogy a képek több különböző országban és teljesen eltérő időpontokban készültek (például Spanyolországban 2012-ben és 2017-ben), az összeállítás célja pedig a fellépő rendőrök brutalitásának ábrázolása és a tüntetők, továbbá a francia és a szolidaritást érző más államok társadalmainak radikalizálása volt.

A Facebook azonban nem távolította el a bejegyzést, érdemben pedig csak 2019 márciusában jelezte egyes mainstream orgánumok cikkeivel – amelyek a megtévesztettek számára nyilván nem hiteles orgánumok – a tartalmak valótlanságát és az állítások célját. Az ilyen dezinformációs kampányok határokat átívelő jellegét igazolja, hogy e szcenárió részeként már Hollandiában is elterjedt a nézet, hogy a rendőrök – hasonlóan a francia kollégáikhoz – mindenkivel szemben erőszakot alkalmaznak, akik szolidaritást vállaltak a sárgamellényes tüntetőkkel. Ezt fokozó *fake news* volt az a hír, amelyik egy, amúgy jogellenes magatartás megvalósító – a videón gyermekét babakocsiban toló – nővel szembeni rendőri fellépést ábrázolt. A videó szerint a rendőrök minden különösebb indok nélkül alkalmaztak kényszerítő eszközöket a nővel szemben, csak azért, mert a tüntetés jelképének számító sárga mellényben volt. Az eredeti videónak a tüntetőkhöz semmi köze nem volt, sőt a babakocsiban is, mint később kiderült, egy műbaba feküdt. Azonban a platform lassú szűrési és címkézési gyakorlata okán a videót gyorsan lefordították francia, angol és olasz nyelvre, és csak az angol verziót 31 ezer ember osztotta meg és 1,3 millió nézte meg.[23]

A 2016-os amerikai elnökválasztás is hasonló tapasztalatokat szült. Ekkor az orosz beavatkozás lényeges eleme volt, hogy a választások előtt a közösségimédia-platformokon keresztül megfelelő hírcsomagokhoz juttassák a kiválasztott társadalmi csoportokat, ezzel megpróbálva befolyásolni a választások lehetséges kimenetelét.[24] Az Avaaz csapata ezt vetítette elő a 2020-as amerikai elnökválasztásnál is, mivel 2019-ben 158 millió megtekintést értek el az Avaaz által megfigyelt politikai tartalmú, a közelgő elnökválasztást érintő valótlan közlemények. Ez a szám önmagában is horribilis, de ha hozzátesszük, hogy a 2018-as félidős választásokra 153 millió választó regisztrált, akkor egyenesen arra a következtetésre kell jutni, hogy minden egyes választót legalább egy valótlan hír elért. A szám nagyságát jól mutatja, hogy 2019-ben a két nagy párt Facebook-oldalát mindösszesen közel 60 millióan tekintették meg.[25]

---

22 Uo., 21.

23 Uo., 7–20.

24 Lina Rosenstedt: Improving Cooperation with Social Media Companies to Counter Electoral Interference. 5 *Hybrid Coe Paper* (2021) 5.

25 US 2020: Another Facebook Disinformation Election? US Flooded with Over 158M Views of Political Fake News ahead of the 2020 Elections. *Avaaz Report* 5/11/2019, https://bit.ly/3xmOpAV, 4–6.

Az elmúlt évek gyakorlata tehát azt mutatja, hogy a közösségimédia-platformok nem tudtak hatékonyan fellépni az olyan valótlan tartalmakkal szemben, amelyek társadalmi kockázata jelentős mértékű volt. Érdemes röviden megnézni a platformok ilyen típusú információkkal szembeni szűrési és címkézési gyakorlatát. A Google, az Amazon, a Facebook és az Apple ellenőrzi a közösségi felületeket, így a politikai információkat is; a napi hírek kapuőrei, így ők irányítják a közbeszédet, ők döntenek a tartalmakról, vagyis arról, hogy mi kerülhet nyilvánosságra. „[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."[26] Tehát a már amúgy is sajátos gondolkodás, elméletek, érdeklődés mentén polarizálódott közösségeket tovább erősíti a közösségimédia-platform által összeállított hírfolyam, amellyel lényegében ezek a platformok már külső állam dezinformációs tevékenysége nélkül is manipulálják az embereket. A felhozott ellenérv az, hogy lehetőség van az interneten más típusú hírforrások felkutatására is, az átlagfelhasználóra viszont ez nem jellemző, emellett pedig a keresőszolgáltatások szintén manipulálják a lehetséges találatok körét.[27]

> 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.[28]

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 a tervezőik politikai elfogultságát és 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[29] túl ezzel képes a „társadalmi közvitát torzítani, tematizálni, akár politikai, akár gazdasági vagy más érdekből".[30]

---

[26] Koltay András: A *social media* platformok jogi státusa a szólásszabadság nézőpontjából. *In Media Res,* 2019/1., 4.

[27] Uo., 6.

[28] Klein Tamás: Harmadik rész: Cyberjog, I. fejezet: Az online nyilvánosság alkotmányjogi vonatkozásai. In Klein Tamás – Tóth András (szerk.): *Technológia jog – robotjog – cyberjog.* Budapest, Wolters Kluwer, 2018, 233.

[29] Lásd ennek problémáját bővebben Koltay András: Az internetes kapuőrök és az emberi jogok európai egyezményének 10. cikke. A sajtószabadság új alanyai. *Állam és Jogtudomány,* 2017/különszám, 129–140.; Koltay András: Az újmédia kapuőreinek hatása a médiaszabályozásra. In Koltay András (szerk.): *Tíz tanulmány a szólásszabadságról.* Budapest, Wolters Kluwer, 2018, 267–292.

[30] Klein i. m. (28. lj.) 235.

Ezeket a következtetéseket erősíti egy másik Avaaz-jelentés, amely a 2020-as amerikai elnökválasztás után készült. Ennek első fejezete azt az egyértelműnek ható alcímet kapta, hogy „Miként hagyta cserben a Facebook az amerikai választókat". A választások után Sheryl Sandberg, a Meta ügyvezető igazgatója azt mondta, hogy a Facebook óriási erőfeszítéseket tett a dezinformáció ellen, mégpedig sikerrel. Eredményként azonosíthatták, hogy – véleményük szerint – nem volt orosz beavatkozás ebben az időszakban a platform határozott fellépése miatt. Az Avaaz azonban rámutatott arra, hogy a vizsgált száz legnézettebb *fake* poszt így is 162 milliós nézettséget ért el, emellett hangsúlyozta, hogy ez a száz poszt nem az összes közül a száz, hanem a Facebook tényellenőrei által azonosított *fake news* közül a száz legnézettebb. A jelentés rátért arra is, hogy amíg a platformok kizárólag önértékelést végeznek, továbbá a kutatók és a hatóságok számára csak azok az információk lesznek elérhetők, amelyeket kiadnak, addig a dezinformáció valós mértékéről még becsléseket is nehéz adni.[31]

Európa esetében ez még fokozottabb veszélyt jelent, amit a Covid–19 által okozott pandémia időszakának gyakorlata is jól visszaigazolt, ugyanis a közösségimédia-platformokon világméretű ún. infodémiát generáltak.[32] 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, a dezinformációt és a pletykákat. Az infodémia hátráltathatja a hatékony népegészségügyi válaszintézkedéseket, továbbá zavart és bizonytalanságot kelthet az emberek körében." Az infodémia kezelése azonban teljesen eltérő volt az Egyesült Államokban és az Európai Unióban.[33]

A Facebook félretájékoztatás elleni kampányának megközelítése, hogy Amerika az első, amiből az következik, hogy a hatékonysága ott a legjelentősebb, ami – mint fentebb láttuk – ott is erősen szubjektív és relatív. Ehhez képest a tényellenőrök a főbb európai, nem angol nyelvű *fake* tartalmak 56%-ára nem reagálnak, ami angol nyelvű *fake* tartalmak esetében csak 26%-os eredménytelenséget mutat. Ez az olasz nyelv esetében 69%, míg a spanyolnál csupán 33%, ami mellett el tudjuk képzelni, hogy a kisebb közép- és kelet-európai nyelvek, mint a magyar, a szlovák, a cseh vagy a horvát stb. esetében milyen hatékonysággal dolgozik a rendszer. Emellett a *fake* címke elhelyezése is jóval lassabban történik meg. Az amúgy sem gyors, az angol nyelvű tartalmak esetében tapasztalható 24 nap alatti *fake* címke kihelyezés a (nem angol) nagyobb európai nyelvek esetében csak 30 nap alatt történik meg. Ez az arány 2021-re kissé javult (55%-ra az első kategória, a címkézés pedig 28 napra), azonban a platform továbbra sem ismeri fel a klónozott tartalmat vagy a hamis állításokból készített egyes variánsokat, amelynek egyes változatait korábban már hamisként jelöltek meg.

A megfigyelt *fake news* esetében 51 eltérő változat 800 ezer interakciót ért el, és ezek 63%-áról hiányzott a Facebook figyelmeztető felirata. Az elkészített jelentés a fentiek mellett hang-

31 Facebook from Election to Insurrection: How Facebook Failed Voters and Nearly Set Democracy Aflame, *Avaaz Report* 18/3/2021, https://bit.ly/3OudQaL.

32 Lásd WHO: *Coronavirus disease 2019 (COVID-19). Situation Report,* https://bit.ly/3xNQXtk, 45.

33 Egy másik vizsgálat hasonló képet mutatott Dél-Amerika és kifejezetten Brazília esetében, azonban nincs képünk Afrikáról és Ázsiáról. Lásd Is Fake News Making Us Sick? How Misinformation may be Reducing Vaccination Rates in Brazil. *Avaaz Report*.

súlyozta, hogy a Facebook a vizsgált egy évben nem tartotta be az ígéretét, hogy a lehető legteljesebb mértékben azonosítja a pandémiához köthető hamis híreket és fellép e tartalmak ellen, így az önszabályozás nem járható út. Megerősítette a 2020-as amerikai elnökválasztások kapcsán már feltártakat: a platformszolgáltatók nem működnek együtt sem az államokkal, sem a kutatókkal, nem teszik átláthatóvá szűrési rendszereiket, nem adnak megfelelő képet dezinformációellenes gyakorlatukról.[34] Ennek pedig egyértelmű következménye, hogy a közösségimédia-platformokon az információs műveleteket végző államok és nem állami szereplők továbbra is sikeresen tevékenykedhetnek céljaik elérése érdekében, tovább szaporítva az e terület másik arcát jelentő biztonsági kockázatok garmadáját.

4. Összegzés

A hibriditás mint korunk biztonsági környezetének szövevényes és szerteágazó jellemzője egyértelműen rávilágít arra, hogy a hatalmi-katonai alapgondolkodású geopolitikai viszonyrendszerekben is rendkívüli mértékben felértékelődik a nem katonai tényezők szerepe, ezeken belül pedig a digitális tér és különösen a közösségimédia-platformok és más, tömeges információközvetítést lehetővé tevő csatornák jelentősége. Ez a hatás- és arányváltozás mind a hibrid hadviselés dominánsan katonai, mind a hibrid konfliktusok részint katonai, mind pedig a hibrid fenyegetések döntően nem katonai érvényesülési tartományában jelen van és komoly hatást gyakorol. Ebből adódóan a jelenséghez az államok és társadalmak rendszereinek alkalmazkodniuk kell, ha saját érdekeiket és stabilitásukat megfelelő szinten kívánják tartani. Ennek az alkalmazkodásnak pedig a hosszú történelmi fejlődésből következő értékek megóvásával együtt, de a kártékony cselekmények hatékony mérséklését szolgáló módon kell megvalósulnia, amihez a hibriditás elemzése és megértése mellett az új platformok és lehetőségek elemzése is kulcskérdés.

E körben megállapítható, hogy a közösségimédia-platformok gyakorlata és 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.[35] Ezzel pedig jó esetben akaratlanul és közvetve, de egy hibrid narratíva esetén kiszolgálják a támadó államot, a védekező állam pedig eszköz nélkül marad. A fentebb ismertetett események egyértelmű tanulsága volt, hogy a szembenálló nagyhatalmak élnek a közösségi média által kínált lehetőségekkel, 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, emellett pedig a platformszolgálatók nem tudnak és sok esetben a saját üzleti érdekeik miatt nem is akarnak aktívan fellépni ezekkel a tartalmakkal szemben, mert jelentős számú megtekintést és megosztást generálnak.

---

[34] Left Behind: How Facebook is Neglecting Europe's Infodemic. *Avaaz Report,* 20/4/2021, https://bit.ly/3mJEgsY.
[35] Koltay i. m. (26. lj.) 10.