Kelemen Roland

A cyberfare state alapgondolata – Az egyén és kapcsolatai átalakulásának hatása az állam működésére és biztonságára[1]

A tanulmány a cyberfare state állammodell alapgondolatára építve mutatja be a kibertér hatását az egyénre és azok kapcsolódásaira, vagyis a társadalmi hálózatokra. Ennek során a dolgozat kimutatja, hogy a társadalmi totalitás ezen szegmenseinek alapjellemzőiben jelentős kvalitatív és kvantitatív változások mentek végbe az elmúlt évtizedekben, amelyek alakították azok dinamikáját, formálhatóságát és összességében az állam biztonságára gyakorolt hatásukat is. Ennek megfelelően az államoknak reagálniuk kellett a jelenségre, amelyre a jogállamhoz való viszonyuk alapján eltérő válaszokat adtak. A smart total control cyberfare state államai a kibertér vívmányait is felhasználva elmozdultak az orwelli állam irányába, míg a demokratikus berendezkedésű államok esetében az egyének (felhasználók) képességeinek erősítése, tudásuk gyarapítása az egyetlen járható út. A tanulmány második felében az erre irányuló lépéseket tekinti át a szerző.

Bevezetés

A 21. század első évtizedeiben az államok, azok intézményrendszere és a hátterüket jelentő társadalmak jelentős átalakuláson estek át. Ennek az átalakulásnak a motorja a kibertér és az ahhoz kapcsolódó technológiák voltak. E technológiák behatoltak nemcsak az emberek életének minden szegmensébe, de egyre inkább formálták a társadalmi totalitás egyes részeit is, így az államok működését sem hagyták érintetlenül, ideértve annak szinte minden területét. A technológiai átalakulás soha nem látott sebességre kapcsolt, aminek eredményeként megdőlni látszik Moore törvénye.[2] Ezen

[1] Ezen állammodell alapstruktúrájának a kidolgozása a szerző saját munkájának az eredménye, amit az alábbi tanulmányban adott közre: Kelemen Roland: Cyberfare state – Egy hibrid állammodell 21. századi születése. *Military and Intelligence CyberSecurity Research Paper,* 2. (2022), 1. 1–32.

[2] Az innovációnak a gyorsaságát mutatja, hogy Moore törvénye, amely szerint az integrált áramkörök összetettsége körülbelül 18 havonta megduplázódik, napjainkban egyre inkább megdőlni látszik, hiszen ez a tendencia gyorsulóban van. Lásd Gordon E. Moore: Cramming More Components onto Integrated Circuits. *Electronics,* 38. (1965), 8. 114–117. E jelenség motorja korunk egyik nóvuma, konvergáló technológiája a tárgyak internete (IoT – Internet of Things), amely az információtudomány fejlődésével, a szenzorok használatának fokozódó térnyerésével (ami magával hozza az árak rapid csökkenését) egyre inkább a mindennapi életünk részévé válik mind az otthonokban, mind pedig a közszférában. Lásd Németh Richárd: Kibertámadások gazdasági vonatkozásai a vállalati szférában.

https://doi.org/10.36250/01164_04

átalakulás legalább ilyen mélyen érinti az emberek hétköznapjait vagy a társadalmi alrendszereket. Emellett pedig jelentős biztonsági kihívások elé állítja az államokat, amelyek alkotmányos szabályaik, történeti és politikai hagyományaik mentén eltérő válaszokat adnak ezekre a kihívásokra.

Míg a cyberfare state egyik altípusa, a smart total control cyberfare state felfogásában és biztonsági megoldásaiban az egyének és az egyének kapcsolatai, vagyis a társadalmi hálózatok felett a lehető legteljesebb felügyeletet igyekeznek kialakítani (lásd például a kínai Aranypajzs rendszert vagy a társadalmi kreditrendszert, a „halal" internetprotokollt)[3], addig a nyugati demokratikus államok esetében szükségszerűen a jogállami paradigmák tiszteletben tartása mellett kell a kibertérből és a hozzá kapcsolódó technológiákból eredő pozitív hatások melletti biztonsági kockázatokat kezelni.

Jelen tanulmányban röviden azt kívánom áttekinteni, hogy a kibertér és a hozzá kapcsolódó eszközök milyen hatást gyakoroltak az egyénekre és kapcsolataikra, és ezen hatások milyen irányú változást eredményeztek az államok biztonsági környezetében. Ezen áttekintést követően pedig kitérek arra, hogy a nyugati, demokratikus államok szövetségi (NATO), illetve európai uniós szinten milyen válaszokat adtak erre a problémára.

A kibertér hatása az egyénre és a társadalmi hálózatokra

Az elmúlt pár évtizedben ugrásszerű változás következett be a társadalmi totalitás egészében, amely nem hagyta változatlanul az egyes részkomplexumokat, így a társadalmi struktúrát és a társadalmi hálózatokat sem. Alvin Toffler elmélete szerint az emberi történelem három hullámra osztható. Az első hullámban a gazdasági termelés alapja a földművelés, ahol a társadalmi struktúra és a leginkább jellegadó társadalmi hálózatok egybeestek. A második hullámot az ipari társadalom korának tekinti. Ezen időszakban felerősödött az egyén társadalmi szerepe, a társadalmi hálózataik hatóereje már nem feltétlenül függött a társadalmi struktúrában betöltött helyüktől. Végül a harmadik hullám az információ kora, vagyis az információs társadalom térnyerése.[4] Fontos elméleti alapja volt annak a felismerése, hogy az információ, a tudás a társadalmi struktúrában betöltött szerepet, viszonyokat alapjaiban határozza meg.[5] Ugyanis az információ már önálló értékké vált, annak

In Dernóczy-Polyák Adrienn (szerk.): *Kutatási jelentés 1.* Győr, Universitas-Győr Nonprofit Kft., 2019. 307–325.

[3] Gosztonyi Gergely: A kínai internetcenzúra modellje. *Pro Futuro,* 12. (2022a), 1. 1–9; Gosztonyi Gergely: Special Models of Internet and Content Regulation in China and Russia. *ELTE Law Journal,* 9. (2021), 2. 87–99.

[4] Alvin Toffler: *A harmadik hullám (információs társadalom A-tól Z-ig).* Budapest, Typotex, 2001.

[5] Fritz Machlup: *The Production and Distribution of Knowledge in the United States.* Princeton University Press, 1962; Z. Karvalics László: „A tudás termelése és elosztása az Egyesült Államokban":

megszerzése és birtoklása tett valakit, illetve valakiket tényleges hatalmi tényezővé. Ezen folyamatban a technológiai robbanás mellett óriási szerepe volt a globalizáció kiteljesedésének. E körben „[a] globalizációt akként gondolhatjuk el, mint a jelenkori társadalmi élet világméretű összekapcsoltságának szélesedő, mélyülő és gyorsuló valóságát, annak kulturális, kriminális, pénzügyi, spirituális, és számos egyéb aspektusával".[6] Ehhez viszont elengedhetetlen attribútummá vált a kibertér, tudniillik a kibertér kiépülésének köszönhetően váltak ténylegesen globálissá az emberi interakciók, a gazdaság és a kultúra. Fontos felismerés, hogy a technológia önmagában nem határozza meg a történelmi fejlődést és a társadalmi változásokat, viszont a technológia felhasználásának vagy fel nem használásának a módja megmutatja egy társadalom alkalmazkodási képességét.[7] Mint a bevezetőben erre utaltam, a smart total controll cyberfare state államai e technológia révén elmozdultak egy orwelli világ irányába, ahol az egyének és kapcsolataik felett az állam és a technológiai partnerei fúzióban fellépve a védelem, a biztonság, a status quo megőrzése érdekében a lehető legteljesebb kontroll kialakítása irányába haladnak. A nyugati társadalmak mindeközben megpróbálják a technológia pozitív, jóléti funkcióit hangsúlyozni és továbbra is erős gátak között tartani az állami információéhséget.[8] Így egyre nagyobb teret nyertek az államoktól elkülönült szereplők. „Korunkra a nemzetállamok riválisaivá nőtték ki magukat többek között a tőke-, a termelési, a kommunikációs, bűnözői hálózatok, a nemzetközi intézmények, a szupranacionális katonai gépezetek, a nem kormányzati szervezetek, a nemzetek feletti vallások, sőt, még a különböző társadalmi mozgalmak is."[9] A tudás- (és információ-) intenzív társadalomban tehát az állam másodlagos szereplővé kezd válni a transznacionális tényezők mellett (tekintsünk e körben a közösségimédia-platformok tevékenységére irányuló állami szabályozás kialakításának eredendő lehetetlenségére). Furcsa kettőssége ennek társadalmi oldalról, hogy az állam információhoz jutását korlátozzák, és hangosan tiltakoznak egy-egy hírszerzési kiszivárgás esetében (lásd Wikileaks, Snowden-ügy), de eközben a többség hallgatásba burkolózik azzal kapcsolatban, hogy „[a]z információ […] kifürkészése és az adatok felhasználók hozzájárulásával, de az átadott adatkör mélységére és súlyára kiterjedő átfogó ismeret hiányában történő rendelkezésre bocsátása a legnagyobb tech-cégek részére milyen visszaélési lehetőséget

Fritz Machlup újraértékelése az információs társadalom elmélettörténetében. *Információs Társadalom,* 9. (2009), 2. 20–34.

6 Pongrácz Alex: A hálózat csapdájában? Globalizáció és totalitás. In Farkas Ádám (szerk.): *Védelmi alkotmányosság az új típusú biztonsági kihívások erőterében.* Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2018. 43.

7 Manuel Castells: *The Information age. Economy, Society, and Culture.* I. kötet. *The Rise of the Network Society.* 2. kiadás. Oxford, Blackwell Publishing, 2010. 7.

8 Pongrácz Alex: Variációk hibrid állammodell-építésre. *Military and Intelligence Cybersecurity Research Paper,* 2. (2022), 3. 3–8.

9 Pongrácz Alex: A globalizáció toposzai. In Kecskés Gábor (szerk.): *Doktori Műhelytanulmányok 2014.* Győr, Széchenyi István Egyetem Állam- és Jogtudományi Doktori Iskola, 2014. 158.

biztosít akár […] az Amazon, a Facebook és a Google"[10] számára. Ezzel a társadalmi struktúra – amely korábban maximum nemzetállami értelmezést jelentett – annak az igénynek megfelelve, vagy azt felhasználva, kiszolgálva, hogy az állam hatalmi tényezőként másodvonalba kerüljön, valamint annak köszönhetően, hogy életünk minden területe lényegében összekapcsolódott, és a szerveződés világméretűvé vált, így már sokkal inkább értelmezhető transznacionális vagy globális közegben, semmint államon belül. Ez a társadalmi struktúrát megkettőzi, és a nemzeti társadalmi struktúra mellett kialakult egy transznacionális vagy globális társadalmi struktúra is. Az egyének társadalmi hálózatainak is e kettős struktúra irányába kell igazodniuk, ami már eredendően konfliktusok forrása, és a nemzeti társadalmakon belüli törésvonalakat eredményez.

A fentieken túl a kibertér és a hozzá kapcsolódó technológiák önmagukban jelentős hatást gyakoroltak, ugyanis átalakították az emberek hétköznapjait, a szolgáltatóközpontú gondolkodás átvette az uralmat a korábbi tradicionális működés felett. Az IoT vagy IoD[11] rendszerek már szükségszerűen módosították az emberek egymás közötti és az ember-gép közötti, sőt a gép-gép közötti interakciókat is. Minden adat, minden eszköz és minden személy valós időben elérhetővé vált a világ bármely pontján, ami átalakította a társadalmi hálózatok dinamikáját is. Mivel egy-egy nagyobb társadalmi hálózat sohasem alszik, vagyis a kapcsolatok egy része mindig aktív magatartást tanúsít, mindig képes arra, hogy a célnak megfelelő reakciót adjon egy-egy felmerülő jelenségre, hírre, információra, és akár ennek megfelelően „riassza" a hálózat többi tagját.

A kibertér fontos hatása, hogy az ahhoz való csatlakozás révén lehetővé válik, hogy befolyásolják az éntudatot, képessé téve egyes aktorokat annak módosítására, „átprogramozására". Mindez azért alakulhat így, mert a kibertér egyes szegmensei lényegében szándékosan úgy vannak tervezve, hogy az egyén sajátos világnézete, érdeklődési köre, tervei, céljai, függőségei mentén kapjon információt, érjen el felületeket, jusson hozzá kapcsolódó termékekhez. Lényegében a közösségimédia-platformok ezen felismerés mentén szervezik saját üzleti modelljüket.[12] Mindez úgy történik, hogy ez a speciális közeg 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 „[c]yberkörnyezetben csökken az ítélőképesség és nő az impulzivitás, némileg hasonlóan ahhoz, ahogyan az alkohol hat ránk. A cyberközeg sajátos jellemzői – a külső kontroll vagy felügyelet

[10] Farkas Ádám: *A védelem és biztonság-szavatolás szabályozásának alapkérdései Magyarországon.* Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2022. 41.

[11] Baranyi Péter et al.: Introducing the Concept of Internet of Digital Reality – Part I. *Acta Politechnica Hungarica,* 18. (2021b), 7. 225–240; Baranyi Péter et al.: Internet of Digital Reality: Infrastructural Background – Part II. *Acta Politechnica Hungarica,* 18. (2021a), 8. 91–104.

[12] Tökéletes példái ennek a szűrőbuborék-rendszerek és a kapuőrök tevékenysége. Lásd Koltay András: A social media platformok jogi státusa a szólásszabadság nézőpontjából. *In Media Res,* 8. (2019), 1. 1–56.

hiánya, a névtelenség, a távolság, a fizikai elkülönültség érzete – elősegítik a gátlások levetkőzését."[13]

Ez a kontrollvesztés önmagában növeli az ismeretlenek közötti szindikalizáció lehetőségét. Ez egy olyan robbanásszerű kvantitatív változást jelent, amely ennek köszönhetően kvalitatív jellemzőit is módosítja a társadalmi hálózatoknak. Ugyanis az új hálózatok méretüket tekintve minden korábbi társadalmi kapcsolati hálót meghaladnak, és számuk és méretük 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.[14] Az egyén mindent megtesz, hogy egy-egy közösség részese lehessen, míg mások hagyományos térbeli céljaik eléréséhez használják az általuk vagy mások által kialakított hálózatokat. Emellett viszont az alaptényezője változik meg a társadalmi hálózatnak, hiszen korábban a társadalmi hálózatok bizalmi oldalát a lokalitás, a kölcsönös ismertség adta, ebből adódóan voltak erősek a kisebb helyi hálózatok és gyengébbek a nagyobb, regionális vagy országos hálózatok; ez viszont átalakul, mivel ezeknél a hálózatoknál a hálózat erőssége már nem földrajzilag körülírható, sokkal inkább a benne megjelenő erősebb individuumok jelenléte vagy egy mindenek fölé helyezett cél primátusa jelenti az összetartó és bizalmi kapcsolatot. Erős vezető(k), tagok vagy egy vallásként tisztelt cél rendkívüli kötőerőt jelent ezekben a hálózatokban. Előbbiek maguk determinálják a hálózat makrotulajdonságait, utóbbi viszont a tagok kollektív tudata mentén alakulhat, mert egy magasztos cél lehet pozitív, de szélsőséges mentalitással társulva biztonsági kockázatot is jelenthet. Utóbbiak megfigyelhetők voltak a korábbi társadalmi hálózatok esetében is, azonban itt, ha emellé rendeljük a kvantitatív és technológiai jellemzőket is, valamint a társadalmi struktúra egy részének a társadalmi totalitáson kívülre kerülését, ami lehetővé teszi az egyes cselekmények relativizálását, mivel lehet olyan cél, amit a belső társadalmi struktúra ellenérzéssel fogad, míg a külső akár támogat is vagy fordítva (erre alkalmas példa lehet a migrációval kapcsolatos állásfoglalások, Black Lives Matter mozgalomra és utóhatásaira adott eltérő válaszok), így a hatalmi viszonyban lévők részéről érzékelhetően jelentősebb potenciállal/kockázattal bíró hálózatok rajzolódnak ki, amit a lentebb ismertetett tulajdonságok tovább erősítenek.

Tovább vizsgálva a formáló körülményeket, meg kell állapítani, hogy a kibertér növeli a kialakított hálózatok testreszabottságát is, mivel a kialakult közösségek tagjai közötti interakciók a kibertérnek köszönhetően már országhatárokat, sőt

[13] Mary Aiken: *Cybercsapda. Hogyan változtatja meg az online tér az emberi viselkedést?* Ford. Török Csaba. Budapest, Harmat Kiadó, 2020. 35.

[14] Pintér Róbert: Úton az információs társadalom megismerése felé. In Pintér Róbert: *Az információs társadalom. Az elmélettől a politikai gyakorlatig.* Budapest, Gondolat – Új Mandátum, 2007. 25.

kontinenseket is átlépnek. A hasonlóan gondolkodó egyének határok nélkül tudnak kommunikálni, egymással információkat megosztani, csoportokat létrehozni, hálózatokat szervezni. Ami tovább erősíti a határokon átnyúló társadalmi struktúráknak a hatalmi pozícióját, hiszen lehetőséget ad, hogy akár információs műveletek mentén alakíthassák egy-egy társadalmi hálózat szemléletét.

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. A hiperdiadikus terjedésnek köszönhetően egy szervezetben, így például egy munkahelyen, kollégiumi közösségben, egyetemen már horizontálissá válik az információáramlás, bonyolultabbak és nehezebben visszakövethetőek a hatások, viszonthatások. E horizontális terjedést helyezzük át a kibertérbe, ahol a hálózat tagjainak száma több ezerre, tízezerre, sőt akár millióra is emelkedhet. A minta terjedése így már nem egyszerűen hiperdiadikus, hanem szuper-hiperdiadikus. Itt egy-egy viselkedési minta átadásához, vírusszerű terjedéséhez nem kell az, hogy minden szereplő azt magáévá tegye, támogassa, elsajátítsa.[15] Az így kialakított hálózatoknak létrejönnek olyan tulajdonságai és funkciói, amelyek az egyéntől elszakadnak, azokra nincsen valós befolyása.[16] 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

[15] 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, amelyek a digitális közösséghez tartozó egyének legtöbbjét sokkolták, mégis óriási számú követőre találtak. Lásd bővebben: Coronavirus challenge és a legveszélyesebb netes kihívások. *Generali előrelátók blog,* 2020. április 24.

[16] Nicholas A. Christakis – James H. Fowler: *Kapcsolatok hálójában. Mire képesek a közösségi hálózatok, és hogyan alakítják sorsunkat?* Budapest, Typotex, 2010. 38–41.

szakasza”[17] –, 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 elkövető legtöbbször – bár hagyományos térben legtöbbjük ilyet nem tenne – nem is érzékeli, hogy rendkívüli mértékben átlépte az emberek között kialakult kommunikáció hétköznapi normáit.

A radikalizálódása a hálózathoz kapcsolódó szereplőknek eltérő fokozatot ölt, pontosan abból adódóan, hogy eltérő magatartási mintákat vesznek át a szereplők a csoport többi tagjától. Eltérő lesz az is, hogy miként viszonyul egy-egy tag a belső vagy külső társadalmi struktúrához, vagy azok mindegyikéhez. Ugyanis már a korábbi történeti közegben kialakult az az ereje az egyes társadalmi hálózatoknak, hogy a társadalmi struktúrában kevésbé jelentősek is hatni tudnak a kialakult társadalmi viszonyrendszerre. Így az a társadalmi hálózat, amely a belső társadalmi struktúrával szembehelyezkedik, de a külső társadalmi struktúrát támogatja, lehetőségként jelenik meg a külső tényezők számára – olyan lehetőségként, amely később támogatható, erősíthető társadalmi töréspontot eredményezhet. Emellett a mindkét struktúrát bíráló, támadó és tagadó hálózatok radikalizálhatóságában rejlik a legnagyobb potenciál, hiszen ezen csoportok kisebb ráfordítással is szélsőséges radikalizmusra hajlamosak.

A fentiek okán megállapítható, hogy ezen szuper-hiperdiadikus mintakövetésen alapuló nagy méretű hálózatok esetében a hálózat méretéből adódóan kevésbé jellemző a homogén magatartási minták átvétele. A csoport attitűdje, a radikalizmusának szintje tehát nem az egyén felől határozható meg, mivel „[a] kapcsolati hálóknak makroszintű tulajdonságai vannak. A makroszintű tulajdonságok olyan, az egészre jellemző új vonások, amelyek a részek közötti kölcsönhatásokra és köztük fennálló kapcsolatokra vezethetők vissza.”[18] Ez pedig adódik a kvantitatív jellemzőkön túl abból is, hogy az egyes tagok a korábban meghatározott célok mentén eltérően reagálnak a társadalmi struktúrákra. És míg korábban a jelentősebb társadalmi hálózatok vagy közvetlen kapcsolatban voltak a társadalmi struktúrával, vagy törekedtek arra, hogy abba beolvadjanak, addig az elmúlt évtizedekben ezen hálózatok egy része kimondottan alkalmas arra, hogy ezen struktúrák valamelyikét felszámolja.

Melyik társadalmi hálózat tud ilyen potenciált magában hordozni? Érdemes itt idézni a világhírű magyar hálózatkutató, Barabási Albert-László szavait: „Igen, tényleg van szólásszabadság a hálón. Azonban annak nagyobb a valószínűsége, hogy hangunk túl gyenge ahhoz, hogy meghallják. Azokat az oldalakat, amelyeknek csak kevés bejövő mutatója van, lehetetlen véletlen barangolással megtalálni. Ehelyett örökké a középpontokhoz vagyunk irányítva.”[19] Ezen következtetést erősíti egy

[17] Kiss Tibor: *Agresszió a cybertérben.* Budapest, Nemzeti Közszolgálati Egyetem, 2020. 28.
[18] Christakis–Fowler (2010): i. m. 42.
[19] Barabási Albert-László: *Behálózva – A hálózatok új tudománya.* Budapest, Libri Kiadó, 2020. 191.

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.[20] Jól mutatják e fenti gondolatok, hogy a kibertérben a társadalmi hálózatok soha nem látott mértékben formálhatók, és ezáltal szembeállíthatók a társadalmi struktúrával, amihez hozzájárul a közösségimédiaplatform-szolgáltatók üzleti gyakorlata, amit eszközként használnak a hibrid konfliktusok ellenérdekű felei is.

Az egyéni reziliencia kialakítására tett lépések – ez lehet a Nyugat válasza a problémára?!

A 21. században az átalakult társadalmi, gazdasági és biztonsági környezet megváltoztatta az állam működését és az államról való gondolkodást, megteremtve a technológia nóvumaira épülő, arra reagáló állammodellt, a cyberfare state-et. Ezen új állammodellnek – bár első pillantásra nem úgy tűnhet – a központi aktora az egyén, hiszen az a társadalmi, gazdasági és állami sérülékenység centrális figurájává vált a technológiai újításoknak köszönhetően. Jól illusztrálja ezt, hogy az informatikai szakemberek a leggyengébb láncszemként tekintenek a humán faktorra. Nem véletlenszerű, hogy a nem jogállami keretek között működő államok (smart total control cyberfare state) esetében mindent megtesznek annak érdekében, hogy az ezen aktor jelentette biztonsági kockázatokat a lehetőségekhez mérten redukálják, úgy, hogy az egyéni szabadságjogokat figyelmen kívül hagyó korlátozó, megfigyelő rendszereket építenek ki, mindezt jóléti megoldásoknak álcázva.

Ezzel szemben a jogállami keretek között működő államok esetében a társadalmi reziliencia kialakítása során még csak az utóbbi években indult meg annak felismerése, hogy az állami, önkormányzati és gazdasági szereplőkön túlmutató, ellenálló képességet növelő programokat, szabályozásokat kell kialakítani. Azonban ezek például a kínai, orosz vagy szingapúri rendszerekhez képest időbeli csúszásban vannak,

[20] *Facebook from Election to Insurrection: How Facebook Failed Voters and Nearly Set Democracy Aflame.* Avaaz Report, 2021. március 18.

és sok esetben még csupán bábállapotban léteznek. Már az is üdvözölendő, hogy a NATO és az Európai Unió néhol megcsúszva, de azonosította ezen fenyegetések körét, és elkezdett fejlődési programokat kidolgozni. Ezt tükrözi vissza a NATO modern technológiákkal kapcsolatos Emerging Disruptive Technology (EDT) rendszere, amelyhez kapcsolódó tanácsadó csoport 2020-as jelentésében hangsúlyozta ezen technológiák társadalmi hatásait, valamint azt, hogy szükségszerű ezen a területen az oktatás és képességfejlesztés. Utóbbiak azért elengedhetetlenek, mert ezek a technológiák rendkívül bonyolult rendszereket eredményeznek, ahol a döntéshozóknak (politikai, gazdasági), illetve az egyéneknek úgy kell eligazodniuk, hogy nem rendelkeznek átfogó ismeretekkel, amelyek viszont nélkülözhetetlenek volnának a NATO versenyképességéhez akár szervezeten belül, akár azon kívül is. Ami viszont nem jelent egyet azzal, hogy minden szereplőnek mélységi műszaki ismeretekkel kell rendelkeznie, vagyis a cél sokkal inkább a tudatosság, az alapismeretek szintjének növelése, azaz a technológiai műveltség magasabb szintre helyezése. A szervezeten belüli képesség növelésére kínálnak lehetőséget az egyes NATO képzési központok. Emellett elkerülhetetlennek vélik az együttműködés kialakítását a magánszektorral és a felsőoktatással is. Szintén kiemelik, hogy ezen együttműködések lehetőséget teremthetnek külsős ismeretterjesztő projekteknek, továbbá egyetemi képzések fejlesztésének, amelynek keretében a NATO mester- és doktori képzések esetében ösztöndíjprogramokat hozhatna létre, ezzel növelve társadalmi elfogadottságát is.[21] A NATO, bár a gazdasági és akadémiai szférára irányultan megkezdte az együttműködés kereteinek kialakítását (ilyen a DINA [Defence Innovation Accelerator for the North Atlantic] és az EDT-hez kötődő tudományos tanácsadó testület is), azonban az egyénekre irányuló programok a gyakorlatban még váratnak magukra, pedig a szakértők között egyre inkább világossá vált, hogy „[a]z emberek tömeges adatainak […] elemzésével és felhasználásával cselekvésünk, gondolkodásunk befolyásolható […] technikailag lehetővé vált az egyes társadalmak integritásának, az állami intézmények iránti bizalom kártékony befolyásolása is".[22]

Az Európai Unió[23] 2019-es globális kül- és biztonságpolitikai stratégiája e területen nem mutat újdonságot. Szintén hangsúlyozza az együttműködés szükségességét az egyes szférákkal, valamint a kiberbiztonság területén a NATO-val való kapcsolatok megerősítését.[24] Ilyen együttműködési projekt például a dezinformációs szcenáriók korai felismerésére és a reagálás javítására szolgáló 2015-ben felállított

[21] NATO Advisory Group on Emerging and Disruptive Technologies. Annual Report. Brüsszel, NATO Emerging Security Challenges Division, 2020. 10. 14–15.

[22] Molnár Ferenc: A reziliencia kérdése és a NATO. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok,* 1. (2021), 15. 6.

[23] Az Európai Unió stratégiai autonómiája az EDT területén sok tekintetben irreálisnak tűnik. Lásd Ester Sabatino – Alessandro Marrone: Emerging Disruptive Technologies: The Achilles' Heel for EU Strategic Autonomy? *IAI Istituto Affari Internazionali,* (2021), 31.

[24] The European Union's Global Strategy – Three years on, looking forward. 2019. 11–13. Az ezen dokumentum alapját jelentő korábbi stratégiát lásd Molnár Anna: Közös jövőkép, közös cselekvés:

East StratCom Task Force elnevezésű munkacsoport. 2018-ban cselekvési tervet fogadtak el a félretájékoztatással szemben. Ez osztott tagállami és uniós intézményi fellépésről rendelkezett. A koordinált válasz négy pilléren nyugszik, a negyedik pillér a tudatosság növelése és a társadalom rezilienciájának javítása. A társadalmi ellenálló képesség növelése érdekében előirányozták a független tényellenőrzőkből álló csoportok létrehozását, akiknek feladata a dezinformálás feltárása és a közvélemény tájékoztatása.[25] 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. A Bizottság álláspontja abban nem változott, hogy a dezinformálás elleni küzdelem egyik legfontosabb terepe a polgárok médiatudatos nevelése.[26]

Az unió üdvözölendő kísérletei közé tartozik a Bizottság által előterjesztett Digitális szolgáltatások egységes piacáról szóló rendeletjavaslat. A rendelet célja az Alapjogi Chartában biztosított jogokat tiszteletben tartó, de biztonságos, kiszámítható és megbízható online környezet kialakítása. „Mindez – a várakozások szerint – az emberi jogok, a jogegyenlőség, a jogbiztonság, a szabadság és a demokrácia, azaz összefoglalóan a jogállam megerősödéséhez vezet el majd, hiszen az egységes felelősségi szabályok, az átláthatóság és kiszámíthatóság az online környezetben visszaszorítja a fentebb tárgyalt hamis hírekkel és dezinformációval kapcsolatos problémákat."[27] A rendelet továbbra is engedi a tartalommoderálást a platformok részéről. Egyértelműen előrelépés, hogy a platformok felelősségének megállapítását is lehetővé teszi a javaslat a jogellenes tartalmakért. A tartalommoderálással kapcsolatban előírja, hogy évenként erről kötelesek jelentést tenni a szolgáltatók. A beszámoló részének kell lenniük az önálló tartalommoderálás okainak és az arra indokot adó (belső vagy külső) szabályozási alapoknak, s az ezekkel összefüggő belső panaszkezeléssel kapcsolatos információk megosztásának és értékelésének. Utóbbiból következik, hogy a platformoknak a korábbitól eltérően átlátható belső panaszkezelési rendszert kell működtetniük, aminek része az eltávolítás, a hozzáférhetetlenné tétel, a szolgáltatás felfüggesztésével vagy megszüntetésével kapcsolatos döntések felülvizsgálata és indokolása. Ezek már önmagukban olyan szabályok,

erősebb Európa. Az EU globális kül- és biztonságpolitikai stratégiája. *Nemzet és Biztonság*, 9. (2016), 2. 75–85.

[25] Európai Bizottság: *Közös Közlemény az Európai Parlamentnek, az Európai Tanácsnak, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának. Cselekvési terv a félretájékoztatással szemben.* JOIN(2018)36 végleges (2018. december 5.).

[26] Európai Bizottság: *A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának az Európai Demokráciára vonatkozó cselekvési tervről.* COM(2020)790 végleges (2020. december 3.).

[27] Gosztonyi Gergely: *Cenzúra Arisztotelésztől a Facebookig. A közösségi média tartalomszabályozási gyakorlatának komplexitása.* Budapest, Gondolat Kiadó, 2022b. 145.

amelyek előrelépést jelenthetnek az egyéni felhasználók védelme érdekében, és így segíthetnek a társadalmi reziliencia kialakításában, hiszen többek között a dezinformációs műveletek hatékonyságát csökkenthetik. Ilyennek tekinthető a rendelet 20. cikke is, amelynek 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, amelyek a társadalmi párbeszédre negatív hatással vannak. Ezen esetekben a kockázatcsökkentési intézkedés keretében történhet többek között tartalommoderálás vagy a szolgáltatás korlátozása.[28]

Összegzés

Az elmúlt évtizedekben a társadalmi hálózatok jelentős változásokon mentek át, amelyek jellemzőiket mind kvantitatív, mind kvalitatív oldalon átírták. A jelenkor társadalmi hálózatai méretüket tekintve soha nem látott kapcsolódási pontokat foglalnak magukba, mivel a kibertér lehetővé tette a földrajzilag nem kötött, lokális hálózatok meghaladását. Ez pedig elvezet oda, hogy a jelenkor társadalmi hálózatai tematizáltabbak, mint korábban, emellett sokkal inkább a közös cél, érdeklődés az alapja a bizalomnak, mintsem – mint korábban – a lokális ismertség. E hálózatoknak a szindikalizáló ereje jóval túlmutat a korábbi évszázadok hálózatain, és magába olvasztja a hasonlóan gondolkodó, hasonló témák iránt érdeklődő egyéneket, attól függetlenül, hogy ténylegesen mennyire egységes a világnézetük az adott témakörben. Az egyes magatartási minták már nem diadikus vagy hiperdiadikus módon terjednek a kapcsolati pontok között, hanem szuper-hiperdiadikus módon, amiből adódóan egy-egy magatartási séma nehezebben visszakövethető, átvétele nehezebben vagy egyáltalán nem megakasztható. Utóbbi jellemzők teszik, hogy ezen hálózatok a korábbi évszázadok hálózataihoz képest már nem definiálhatók a mikro-, vagyis az egyéni jellemzők oldaláról, hanem sokkal inkább makrotulajdonságok jellemzik őket.

Fontos tapasztalás, hogy a társadalmi struktúra és a társadalmi hálózatok kapcsolata átalakult. Míg a korábbi évszázadokban az volt a jellemző, hogy a társadalmi struktúrában jelentős szerepet betöltő társadalmi hálózatok voltak csak képesek befolyásolni a társadalmi struktúra viszonyait, esetleg biztonsági kockázatként megjelenni, addig leginkább a 19. század közepétől azt figyelhetjük meg, hogy a társadalmi struktúrában kevésbé jelentős társadalmi hálózatok is képesek

[28] Az Európai Parlament és a Tanács (EU) 2022/2065 rendelete (2022. október 19.) a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról (digitális szolgáltatásokról szóló rendelet). L 277/1 (2022. október 27.). 6–28. cikk.

hatni a társadalmi struktúrára, és sok esetben képesek voltak veszélyeztetni a nemzeti biztonságot is. Azonban a kibertér megjelenéséig ezen társadalmi hálózatok is mindig a társadalmi struktúrára reagáltak, vagy be kívántak olvadni, vagy módosítani kívánták azt. Ezzel szemben az utóbbi évtizedek átalakulása mára oda vezetett, hogy a társadalmi totalitáson kívüli társadalmi struktúrá(k) jött(ek) létre (például ilyenek lehetnek egyes franchise típusú terrorszervezetek, ideológiai alapú transznacionális szerveződések), így akár az egyes társadalmi hálózatok már nem is a társadalmi totalitás szerinti társadalmi struktúrájukhoz képest definiálják magukat, hanem egy társadalmi totalitáson túli társadalmi struktúrához képest, amely révén a társadalmakon belül további töréspontok keletkezhetnek.

E problémákra a cyberfare state modell két pólusa eltérő választ ad. Míg a nem vagy kevésbé demokratikus államok (például Kína, Oroszország, Szingapúr, India stb.) totális kontroll irányába mozdultak el az egyének vonatkozásában, addig a jogállami keretek között mozgó államalakulatok inkább az egyéni tudatosság erősítése mellett törtek lándzsát. E területeken az elmúlt években a felismerésen túl azonban összességében – az egyénre irányuló programok tekintetében – előrelépés nem történt, a független tényellenőrök rendszerének felállítása lényegi elmozdulást nem eredményezett, eredményezhetett az egyéneken nyugvó biztonsági kockázatok mátrixában. Még úgy sem, hogy „[a] NATO a kollektív védelem egyik kulcsfontosságú fejlesztési irányát látja a rezilienciában, ami azt is jelenti, hogy a szövetség szintjén hatékony ellenálló képesség nem korlátozódik a kormányzatok működésére, hanem azt rétegzettként értelmezi. Ez a rétegzettség a kellően informált, tudással felvértezett egyénektől és civil társadalomtól, a civil (állami, piaci) és katonai szervezeteken át, a teljes társadalmak ellenálló képességét jelenti."[29] Mindezzel szemben azt látjuk, hogy továbbra is holisztikus mind a NATO, mind az EU megközelítése. Annak ellenére van ez így, hogy minden fontosabb és a témát érintő stratégiai dokumentumban megállapítják a rendszerek összetettségét, bonyolultságát, ahol „az érintett emberek és csoportok képességbeli […] heterogenitása nem alakult át gyökeresen",[30] vagyis az egyének és az általuk létrehozott társadalmi hálózatok lényegében nincsenek felvértezve azzal a tudással, amelynek köszönhetően önmagukat meg tudják óvni az ártó tényezőktől. Nyilván ez nem jelenti azt, hogy a kibertér valamennyi ártalmával szemben kizárólag szövetségi, uniós és állami programoknak köszönhetően tud ellenállni az egyén, azonban a megfelelő és átfogó nevelési, oktatási és képzési programok, valamint a káros hatásokat jobban lekövető jogalkotás[31] hiányában

[29] Molnár (2021): i. m. 12.

[30] Farkas Ádám – Spitzer Jenő: Az információs korszak és az állami reziliencia egyes kérdései. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok,* 1. (2021), 18. 19.

[31] Jogalkotásban az egyént is érintő egyes területeken már találkozunk megoldásokkal, azonban az átfogó szemléletű megoldások hiányoznak itt is. Lásd bővebben Szépvölgyi Enikő: Az európai uniós reklámszabályozás és a kiskorúak védelme – a digitalizáció kihívásai. *Külgazdaság,* 66. (2022), 5–6. 109–122; Sorbán Kinga: A társadalmi tudatosság és az online közvetítő szolgáltatók szerepe az informatikai bűnözés elleni fellépésben. *Iustum Aequum Salutare,* 16. (2020b), 3. 179–192; Sorbán

nem lehet kialakítani a szükséges egyéni, társadalmi, nemzeti és szövetségi ellenálló képességet. A feladat összetett és „[…] ahhoz, hogy felnőjünk a cybertérben felmerülő új problémákhoz, arra lenne szükség, hogy a törvényeink és az oktatási rendszerünk ugyanolyan rohamos tempóban kövessék a változásokat, mint ahogyan a technológiákat fejlesztik és piacra dobják – ez pedig gyakorlatilag lehetetlen”.[32] Azonban a deklarációk szintjét már a nyugati demokratikus alapokon nyugvó államoknak is meg kell haladniuk, mivel az egyénre irányuló – jogállami kereteken nyugvó – tényleges cselekvés hiányában behozhatatlan stratégiai hátrányba kerülnek a másik pólust jelentő államokkal szemben.

Felhasznált irodalom

Aiken, Mary: *Cybercsapda. Hogyan változtatja meg az online tér az emberi viselkedést?* Ford. Török Csaba. Budapest, Harmat Kiadó, 2020.

Az Európai Parlament és a Tanács (EU) 2022/2065 rendelete (2022. október 19.) a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról (digitális szolgáltatásokról szóló rendelet). L 277/1 (2022. október 27.).

Barabási Albert-László: *Behálózva – A hálózatok új tudománya.* Budapest, Libri Kiadó, 2020.

Baranyi Péter – Csapó Ádám – Budai Tamás – Wersényi György: Internet of Digital Reality: Infrastructural Background – Part II. *Acta Politechnica Hungarica,* 18. (2021a), 8. 91–104. Online: http://acta.uni-obuda.hu/Wersenyi_Csapo_Budai_Baranyi_115.pdf

Baranyi Péter – Csapó Ádám – Budai Tamás – Wersényi György: Introducing the Concept of Internet of Digital Reality – Part I. *Acta Politechnica Hungarica,* 18. (2021b), 7. 225–240. Online: http://acta.uni-obuda.hu/Baranyi_Csapo_Budai_Wersenyi_114.pdf

Castells, Manuel: *The Information age. Economy, Society, and Culture.* I. kötet. *The Rise of the Network Society.* 2. kiadás. Oxford, Blackwell Publishing, 2010.

Christakis, Nicholas A. – James H. Fowler: *Kapcsolatok hálójában. Mire képesek a közösségi hálózatok, és hogyan alakítják sorsunkat?* Budapest, Typotex, 2010.

Coronavirus challenge és a legveszélyesebb netes kihívások. *Generali előrelátók blog,* 2020. április 24. Online: https://blog.generalielorelatok.hu/biztonsag/coronavirus-challenge-es-veszelyes-internetes-kihivasok/

Európai Bizottság: *A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának az Európai Demokráciára vonatkozó cselekvési tervről.* COM(2020)790 végleges (2020. december 3.)

Európai Bizottság: *Közös közlemény az Európai Parlamentnek, az Európai Tanácsnak, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának. Cselekvési terv a félretájékoztatással szemben.* JOIN(2018)36 végleges (2018. december 5.)

Kinga: A bosszúpornó és deepfake pornográfia büntetőjogi fenyegetettségének szükségességéről. *Belügyi Szemle,* 68. (2020a), 10. 8–104.

[32] Aiken (2020): i. m. 214.

Facebook: From Election to Insurrection. How Facebook Failed Voters and Nearly Set Democracy Aflame. Avaaz Report. 2021. március 18. Online: https://secure.avaaz.org/campaign/en/facebook_election_insurrection

Farkas Ádám: *A védelem és biztonság-szavatolás szabályozásának alapkérdései Magyarországon.* Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2022.

Farkas Ádám – Spitzer Jenő: Az információs korszak és az állami reziliencia egyes kérdései. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok,* 1. (2021), 18. Online: https://hhk.uni-nke.hu/document/hhk-uni-nke-hu/VBSZK%20M%C5%B1helytanulm%C3%A1nyok_2021_18_Farkas-Spitzer_Az%20inform%C3%A1ci%C3%B3s%20korszak%20%C3%A9s%20az%20%C3%A1llami%20rez%C3%ADliencia%20egyes%20k%C3%A9rd%C3%A9sei.pdf

Gosztonyi Gergely: Special Models of Internet and Content Regulation in China and Russia. *ELTE Law Journal,* 9. (2021), 2. 87–99. Online: https://doi.org/10.54148/ELTELJ.2021.2.87

Gosztonyi Gergely: A kínai internetcenzúra modellje. *Pro Futuro,* 12. (2022a), 1. 1–9. Online: https://doi.org/10.26521/profuturo/2022/1/11118

Gosztonyi Gergely: *Cenzúra Arisztotelésztől a Facebookig. A közösségi média tartalomszabályozási gyakorlatának komplexitása.* Budapest, Gondolat Kiadó, 2022b.

Kelemen Roland: Cyberfare state – Egy hibrid állammodell 21. századi születése. *Military and Intelligence CyberSecurity Research Paper,* 2. (2022), 1. 1–32.

Kiss Tibor: *Agresszió a cybertérben.* Budapest, Nemzeti Közszolgálati Egyetem, 2020.

Koltay András: A social media platformok jogi státusa a szólásszabadság nézőpontjából. *In Media Res,* 8. (2019), 1. 1–56.

Machlup, Fritz: *The Production and Distribution of Knowledge in the United States.* Princeton, Princeton University Press, 1962.

Molnár Anna: Közös jövőkép, közös cselekvés: erősebb Európa. Az EU globális kül- és biztonságpolitikai stratégiája. *Nemzet és Biztonság,* 9. (2016), 2. 75–85.

Molnár Ferenc: A reziliencia kérdése és a NATO. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok,* 1. (2021), 15. 1–13.

Moore, Gordon E.: Cramming More Components onto Integrated Circuits. *Electronics,* 38. (1965), 8. 114–117.

NATO Advisory Group on Emerging and Disruptive Technologies. Annual Report. Brüsszel, NATO Emerging Security Challenges Division, 2020. Online: www.nato.int/nato_static_fl2014/assets/pdf/2021/3/pdf/210303-EDT-adv-grp-annual-report-2020.pdf

Németh Richárd: Kibertámadások gazdasági vonatkozásai a vállalati szférában. In Dernóczy-Polyák Adrienn (szerk.): *Kutatási jelentés 1.* Győr, Universitas-Győr Nonprofit Kft., 2019. 307–325.

Pintér Róbert: Úton az információs társadalom megismerése felé. In Pintér Róbert: *Az információs társadalom. Az elmélettől a politikai gyakorlatig.* Budapest, Gondolat – Új Mandátum, 2007.

Pongrácz Alex: A globalizáció toposzai. In Kecskés Gábor (szerk.): *Doktori Műhelytanulmányok 2014.* Győr, Széchenyi István Egyetem Állam- és Jogtudományi Doktori Iskola, 2014. 157–168.

Pongrácz Alex: A hálózat csapdájában? Globalizáció és totalitás. In Farkas Ádám (szerk.): *Védelmi alkotmányosság az új típusú biztonsági kihívások erőterében.* Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2018. 43.

Pongrácz Alex: Variációk hibrid állammodell-építésre. *Military and Intelligence Cybersecurity Research Paper,* 2. (2022), 3. 3–8.

Sabatino, Ester – Alessandro Marrone: Emerging Disruptive Technologies: The Achilles' Heel for EU Strategic Autonomy? *IAI Istituto Affari Internazionali,* (2021), 31. Online: www.iai.it/sites/default/files/iaicom2131.pdf

Sorbán Kinga: A bosszúpornó és deepfake pornográfia büntetőjogi fenyegetettségének szükségességéről. *Belügyi Szemle,* 68. (2020a), 10. 81–104. Online: https://doi.org/10.38146/BSZ.2020.10.4

Sorbán Kinga: A társadalmi tudatosság és az online közvetítő szolgáltatók szerepe az informatikai bűnözés elleni fellépésben. *Iustum Aequum Salutare,* 16. (2020b), 3. 179–192.

Szépvölgyi Enikő: Az európai uniós reklámszabályozás és a kiskorúak védelme – a digitalizáció kihívásai. *Külgazdaság,* 66. (2022), 5–6. 109–122. Online: http://doi.org/10.47630/KULG.2022.66.5-6.109

The European Union's Global Strategy – Three Years on, Looking Forward. 2019. Online: www.eeas.europa.eu/sites/default/files/eu_global_strategy_2019.pdf

Toffler, Alvin: *A harmadik hullám (információs társadalom A-tól Z-ig).* Budapest, Typotex, 2001.

Z. Karvalics László: „A tudás termelése és elosztása az Egyesült Államokban": Fritz Machlup újraértékelése az információs társadalom elmélettörténetében. *Információs Társadalom,* 9. (2009), 2. 20–34.