

SLRG Working Paper – Nr. 2021/1.



SmartLaw Research Group

**Biztonság – Geopolitika – Digitalizáció,
avagy Amaël Cattaruzza „A digitális
adatok geopolitikája” című kötetének
főbb üzenetei**

Farkas Ádám

Jelen tanulmány¹ egy kibővített és különösen a biztonság és védelem kérdéseivel való összefüggésekre fókuszáló ismertetését kívánja adni Amaël Cattaruzza „A digitális adatok geopolitikája” című kötetének. A szerző célja nem csak ismertetni a könyvet, hanem rávilágítani azokra a biztonsági kapcsolódásokra a kötetből, amelyek további kutatásokat, illetve biztonságfejlesztési intézkedéseket igényelnek. A dolgozat tehát ismertetés és előrejelzés is a szakértők, kutatók, védelmi és biztonsági szervezetek, továbbá a politikai döntéshozók számára egyaránt.

Kulcsszavak: digitalizáció, kibertér, geopolitika, multipoláris világrend

*The present study seeks to provide an expanded review of Amaël Cattaruzza's book, *The Geopolitics of Digital Data*, with an extended focus on security and defense issues. The aim of the author is not only to describe the book, but also to highlight the security connections from the volume that require further research and security improvement measures. Thus, the paper is also a description and forecast for experts, researchers, defense and security organizations, as well as policy makers.*

Keywords: digitization, cyberspace, geopolitics, multipolar world order

„Az adatok tehát nem semlegesek és nem függetlenek az őket létrehozó társadalmi csoportoktól. Az adatoknak céljuk van, ami mögött a szereplők stratégiái és elgondolásai húzódnak meg.”²

2020 szeptemberében jelent Amaël Cattaruzza „A digitális adatok geopolitikája” című munkája Magyarországon, melyet a Pallas Athéné Books bocsátott a magyar olvasók rendelkezésére. Ezzel egy újszerű, a földrajztudományt a geopolitika révén a digitalizációval összekapcsoló áttekintő mű vált megismerhetővé a hazai olvasókör számára. A kötet földrajztudós szerzője a Francia Geopolitikai Intézet szakértője³ és a témára irányuló kutatási program⁴ tagja, aki törekedett arra, hogy a szükséges szakzsargon használata mellett egy hiteles, mégis emészthető írásművel járja körül választott témáját.

„Az adatok tehát nem semlegesek és nem függetlenek az őket létrehozó társadalmi csoportoktól. Az adatoknak céljuk van, ami mögött a szereplők stratégiái és elgondolásai húzódnak meg.”

A kötet a maga százharminc oldalán egy számos aspektust érintő, komplex áttekintést adja a cím szerinti témakörnek. Mondandóját a szerző három nagy részbe és a következtetésekbe rendezte, a három részen belül összesen tizenhat altéma feldolgozásával. Témakörei mások mellett az adat jelentésétől annak társadalmi-technikai jellegétől és költötségeitől, az adat szociálpszichológiai vonatkozásain, majd az adatok regionalizációján, az adatáramlás geopolitikáján és az adatokért vívott harcon át egészen a tér és az adat viszonyáig, a harctér digitalizációjáig, továbbá a területi hatalom – hálózati hatalom értelmezési párokig terjed.

E feldolgozás során a szerző egyértelműen rámutat arra, hogy az információs térben zajló tevékenységek erősödése, illetve – egyéni, szakmai, társadalmi, gazdasági, politikai, tudományos, stb. – életünk digitalizálása

¹ Az Innovációs és Technológiai Minisztérium ÚNKP-20-4-II-NKE-11 kódszámú Új Nemzeti Kiválóság Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.

² Amaël CATTARUZZA: *A digitális adatok geopolitikája. Hatalom és konfliktusok a big data korában*. Budapest, Pallas Athéné Books, 2020., 13. o.

³ Lásd: https://www.geopolitique.net/fr/our_team/amael-cattaruzza/

⁴ Lásd: Geopolitics of the Datasphere (GEODE); <https://geode.science/en/home/>



az előnyök mellett teret enged a hatalmi, stratégiai törekvéseknek is. A szerző munkájában nem agítál, de számot vet a trendek alakulásával és azokkal a „csendes” folyamatokkal is, amelyek például az adattárak territorializálása révén jól tükrözi a globális hatalmi térben zajló versengés hatásait és függőségi-befolyásolási viszonyait a digitalizációra.

Persze a szerző már felütésében is önkritikus, hiszen a hagyományos értelmezési sémákra építve maga is tudja, hogy a digitális adatok geopolitikájáról írni kockázatos és kritikus kérdéseket felvető vállalkozás lehet. Ennek alapvető kérdéseit ezért már a bevezetőjében igyekszik kezelni a (1) digitális technológiák alkalmazásával létrehozott földrajz, a (2) digitális technológiák földrajza és a (3) digitális technológiák által létrehozott földrajz stációinak azonosításával, illetve mindezek geopolitikai kapcsolódásainak láttatása révén. Ezek kapcsán rögzíti, hogy „az új digitális környezet nem szigorúan véve technikai, hanem társadalmi, politikai, gazdasági stb. tételekkel bíró emberi alkotás. [...] Mindemellet

a hatalom kérdése központi eleme a földrajz és a digitális technológiák mindhárom kategória szerinti összekapcsolódásából eredő tudományos eredményeknek. Így jöttek létre e különböző tudományágakon átívelő geopolitikai elemzések.”⁵

A gondolat és kutatási irány újszerűségével, kritikus voltával tehát a szerző tisztában van, jelzi azonban, hogy ennek voltak már előzményei, melyek közül a kibertér geopolitikai megközelítése és a kibertér rétegeinek elmélete kap külön figyelmet, rögzítve, hogy: „A kibertér ilyen elméleti fogalom meghatározásának érdeme az, hogy lehetővé teszi az internet konkrét geopolitikai elemzését. Az egymásra rakódott rétegek mögött a kibertérben feltűnik a hatalom földrajzi megtestesülése.”⁶ Ha pedig az olvasó mindezt összekapcsolja a kibertér fogalma⁷, biztonsági vonatkozásai⁸ és nemzetközi jogi kihívásai⁹, vagy adott esetben a hibrid fenyegetések és a befolyásolási törekvések kiber-vonatkozásai¹⁰ kapcsán egyre szélesedő kutatási és szakiro-

⁵ Amaël CATTARUZZA i.m. 10. o.

⁶ Amaël CATTARUZZA i.m. 12. o.

⁷ A téma kapcsán példaként lásd: OTTIS R. – LORENTS P.: *Cyberspace: Definition and Implications*. In Proceedings of the 5th International Conference on Information Warfare and Security, Dayton, OH, US, 8-9 April. 2010., 267-270. o.; U. M. MBANASO – E. S. DANDAURA: *The Cyberspace: Redefining a New World*. In IOSR Journal of Computer Engineering, 2015/3., 17-24. o.; MUNK Sándor: *A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései*. In Hadtudomány 2018/1. szám, 113-131. o.; SZKÁLA Károly – MUNK Sándor: *A kibertér fogalma, értelmezése és fejlődése*. In Földrajzi Közlemények 2018/4. szám, 344-355. o.; KELEMEN Roland – NÉMETH Richárd: *Multidisciplinary Approach of the Concept and Characteristics of the Cyberspace*. In Glavanits Judit – Király Péter Bálint (szerk.): *Law 4.0 Challenges of the Digital Age*. Győr, Széchenyi István Egyetem Deák Ferenc Állam- és Jogtudományi Kar, Nemzetközi Köz- és Magánjogi Tanszék, 2019., 49-59. o.

⁸ A téma kapcsán lásd: A. ERTAN – K. FLOYD – P. PERNIK – T. STEVENS (eds.): *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*. Tallinn, CCD CoE, 2020.; Alexander KLIMBURG (eds.): *National Cyber Security Framework Manual*. Tallinn, CCD CoE, 2012.; KELEMEN Roland: *A kibertérből érkező fenyegetések jelentősége a hibrid konfliktusokban és azok várható fejlődése*. In Honvédségi Szemle 2020/4. szám, 65-81. o.; KELEMEN Roland – NÉMETH Richárd: *Vulnerabilities of the Cyberspace Due to Its Social Nature*. In Rastislav Funta (szerk.): *Počítačové právo, UI, ochrana údajov a naj-*

väčšie technologické trendy. 2019, 51-66. o.; KELEMEN Roland – NÉMETH Richárd: *A kibertér alanyai és sebezhetősége*. In Szakmai Szemle, 2019/3. szám, 95-118. o.

⁹ Példaként lásd: Michael N. SCHMITT (eds.): *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge, Cambridge University Press, 2013.; Michael N. SCHMITT (eds.): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge, Cambridge University Press, 2017.; Katharina ZIOLKOWSKI: *Confidence Building Measures for Cyberspace – Legal Implications*. Tallinn, CCD CoE, 2013.; KELEMEN Roland – FARKAS Ádám: *To the Margin of the Theory of a New Type of Warfare: Examining Certain Aspects of Cyber Warfare*. In Szabó Marcel – Gyeney Laura – Lános Petra Lea (szerk.): *Hungarian Yearbook of International Law and European Law* (2019). Den Haag, Eleven International Publishing, 2020., 203-226. o.; KELEMEN Roland – SIMON László: *A kibertérben megjelenő fenyegetések és kihívások kezelésének egyes nemzetközi jogi problémái*. In Farkas Ádám – Végh Károly (szerk.): *Új típusú hadviselés a 21. század második évtizedében és azon túl. Intézményi és jogi kihívások*. Budapest, Zrínyi Kiadó, 2020., 150-170. o.

¹⁰ Példaként lásd: GIANNOPOULOS G. – SMITH H. – THEOCHARIDOU M. (eds.): *The Landscape of Hybrid Threats. A Conceptual Model Public Version*. Luxembourg, Publications Office of the European Union, 2021.; Josef SCHROEFL: *Cyber power is changing the concept of war*. Helsinki, Hybrid CoE Strategic Analysis 21., 2020.; KELEMEN Roland: *A kibertérből érkező fenyegetések jelentősége a hibrid konfliktusokban és azok várható*



dalmi eredményekkel, akkor a szerző vállalkozása már nem hogy megkérdőjelezhető újdonságként, hanem szükséges hiánypótlásként is értelmezhető.

Érdeemes tehát egy ilyen mű főbb üzeneteit a megszokott leírás és értékelés kereteit néhol feszegetve, tágabb kontextusban szemlélve vizsgálni és tudatosítani. A digitalizáció különféle hatásainak, így geopolitikai vonatkozásainak elkerülése ugyanis lehetetlen opció a jövőnkötet illetően, vagyis a jelenséget meg kell ismerni, értelmezni kell és konstruktív reagálással kell megközelíteni, amihez a szóban forgó kötet úgy vélem, értékes gondolatokkal járulhat hozzá.

ELSŐ RÉSZ: MIT IS NEVEZÜNK „ADATNAK”?

A szerző e rész elején rögzíti, hogy a digitalizáció révén az adatok soha nem látott mennyiségi növekedése mellett azt is látni kell, hogy

- a nem digitális adatok mennyisége lényegében eltörlődik a digitális adatoké mellett,
- a rendkívüli mennyiségű adat hatékony rendszerezése és feldolgozása már önálló diszciplínát igényel,
- az adatfeldolgozás folyamata is digitális megoldásokat tesz szükségessé,

amiből arra a megállapításra jut, hogy az „emberi megértés határait meghaladó mennyiségű megfelelő adat kiválasztása tehát szorosan az azt feldolgozó algoritmusoktól függ.”¹¹ Ezt a ténymegállapítást az olvasó már előjáróban összekötheti azzal a kérdésfeltevéssel, hogy vajon ezen algoritmusok mekkora sérülékenységet jelentenek magára az adatfeldolgozás folyamatára, illetve esetlegesen az adatok

vagy azok kiválasztásának manipulálása révén a tudatunk alakulására.¹²

E viszonylag direkt kritikai kérdést elkerülve a szerző a probléma felfejtését az adat történelmi jelentősége felől közelíti meg. Ezzel egyrészt egyértelműsíti, hogy a történelem során időszakosan visszatérő volt az „adatrobbanás” jelentősége csak más-más mértékben, ahogy az is, hogy az adatok hasznosítását hatékonyabbá tevő vívmányok minden időben segítették a hatalmi szereplők pozícióinak erősítését Mezopotámia agyagtábláitól, a Han Birodalom népszámlálási jegyzékein át egészen a könyvnyomtatásig.

A történelmi alapvetés után persze a szerző azt is leszögezi, hogy a digitalizációval megvalósuló áttörés úgy fest korszakos, a korábbiakat léptékekkel meghaladó ugrást eredményez és nem csak az adatok mennyisége és az élet minden szegmensére való kiterjedése, hanem a tudományos gondolkodásra és ez által az elemzés módszereire gyakorolt hatása miatt is. E körben rögzíti, hogy a big data újszerűsége messze többet takar, mint az adatok mennyiségét, mivel abba beleértendő az adatok sebessége, változatossága, teljeskörűsége, felbontása, kapcsolatba rendezhetősége és skálázhatósága is.¹³ E sokrétűség az, ami miatt a szerző a big data jelentőségét, különösen annak flexibilitását és új kapcsolatokba rendezhetőségét hangsúlyozza, jelezve, hogy ez olyan információszerzési és prognosztikus lehetőségeket nyit meg, amelyek messze meghaladják a technikai és tudományos érdeklődés körét, mivel valós társadalmi vonatkozásokkal bírnak. E társadalmi kapcsolódás jelentőségére Michel Foucault nyomdokaiban járva egy korábbi tudományos fejlődés következményeinek megvilágításával hívja fel a figyelmet, miszerint: „A gazdaságtudományok tehát a hatalom tudományává, a

fejlődése. In Honvédségi Szemle 2020/4. szám, 65-81. o.; HÓDOS László: *A hibrid konfliktusok felvelési szakasz, avagy a fenyegetés észlelésének, megelőzésének és kezelésének nemzetbiztonsági aspektusai*. In Honvédségi Szemle 2020/4. szám, 49-64. o.

¹¹ Amaël CATTARUZZA i.m. 17. o.

¹² E tekintetben a Cambridge Analytica kérdéskörén és a Facebook mögött álló portfólió felosztására irányuló folyamaton túl érdemes lehet e körben az álhírek és a dezinformáció kérdésköreinek hatásaira is kitékinteni.

E körben lásd például: KREKÓ Péter: *Tömegparanoia. Az összeesküvés-elméletek és álhírek szociálpszichológiája*. Budapest, Atheneum Kiadó, 2018.; KREKÓ Péter: *Tömegparanoia 2.0. Összeesküvés-elméletek, álhírek, dezinformáció*. Budapest, Atheneum Kiadó, 2021.; Lee MCINTYRE: *Post-Truth*. Cambridge, MIT Press, 2018.; Ignas KALPOKAS: *A Political Theory of Post-Truth*. Cham, Palgrave Pivot 2019.

¹³ Ld.: Amaël CATTARUZZA a i.m. 23. o.



statisztikák pedig a lakosság irányítására és ellenőrzésére szolgáló eszközzé lépnek elő.”¹⁴

Ebben a képletben pedig az emberek zöme önként, az előnyök kiaknázása érdekében válik komponensé a szerző szerint, aki Dominique Cardonra hivatkozva jelzi, hogy a társadalom új típusú számszerűsítése egyéni igényeken alapul. „A youtuber mostantól fogva ellenőrizheti videója nézőszámát, az étterem-tulajdonos számszerűsítheti oldalának népszerűségét, az író valós időben követheti eladási példányszámát az Amazonon, és így tovább. A közösségi médiában pedig mindannyian saját magunk ítélnéjük meg jóhírlükét és befolyásunkat.”¹⁵ Ennek a folyamatnak persze a globalizáció és a fogyasztói társadalom számtalan hatására visszavezethető pszichológiai alapjai vannak, melyek mind a jelen áttekintés, mind pedig az alapul szolgáló kötet keretein túlnyúlnak. Azt azonban a szerző érzékletesen rögzíti, hogy az egyén digitális visszatükrözésére – átrajzolására? (a szerző) –, illetve érdekeinek előmozdítására irányuló vágy lényegében az egyik motorja a digitalizáció szakadatlan felívelésének, amivel azonban nem csak egy új kibontakozási terep, hanem egy új piac, sőt egy új hatalmi tér nyílt meg. Ezt egyik oldalról a magán kézzel lévő adatsokaság visszaélészerű használatának példájára mutatva a Cambridge Analytica-üggyel szemlélteti, másik oldalról pedig annak megvilágításával, hogy az „okoseszközök fejlődésével immár az egyéni és kollektív viselkedésről gyűjtött, sokszor az érintettek tudta nélkül (vagy beleegyezésüket nem világos formában kérve) rögzített adatok képezik olyan statisztikai előrejelzések alapját, amelyek jelentős befolyást gyakorolnak a gazdasági és politikai döntéshozók választásaira.”¹⁶

E gondolatiságon – az adat és a technológia viszonyának áttekintésével is – tovább haladva a szerző a technikai alapú megközelítéstől a társadalmi felé mozdul el és elsőként az adat szociálpszichológiájára világít

rá. E körben érdekes okfejtéssel vázolja fel, hogy miért érdemesebb az adatok keletkezésének hierarchikus megközelítése helyett egy dialektikába hajló megoldás felé fordulni, figyelemmel arra, hogy az adatok kezelésére irányuló fő kérdések – milyen adatot, milyen célból, milyen módszerrel, stb. – döntéseken, a döntések pedig egy a döntéshozó környezetéből és közegéből adódó erőter hatásain alapulnak. Innen nézve jut arra a megállapításra a szerző, hogy „Az adatokat végső soron a különböző társadalmi, gazdasági, politikai, kulturális, technikai dimenziók átfedései hozzák létre, amely dimenziókban hatnak az őket kialakító társadalmak különféle jellegzetességei (gondolkodásmód, ismereti formák, gazdasági és politikai rendszer, jogrendszer, technikai fejlettségi szint, intézményrendszer, kollektív képzelet, stb.). [...] A társadalmi és a technikai vetület e mély összefonódásán keresztül láthatjuk, hogy az adat nem semleges számjegy vagy a valóság egyszerű visszatükröződése, amely arra vár, hogy rögzítsék. Az adatok egy társadalmi-térbeli kontextusba illeszkedő és geopolitikai dimenzióra vonatkozó társadalmi igényt elégítenek ki.”¹⁷

Ezzel azt is mondhatnánk, hogy a szerző kinyitotta Pandora szelencéjét. Egyik oldalról ugyanis egyértelmű az adatok jelentősége miatt az a megközelítés, hogy a digitalizáció korában a technológia fejlődése fajsúlyossá teszi mind a kutatás-fejlesztésben, mind a tágabb értelemben vett tudományos, illetve piaci és állami – e körben mások mellett katonai, rendészeti, nemzetbiztonsági, járványügyi, stb. – elemző gondolkodásban az alkalmazott és a természettudományos megközelítést és a technológiai képességfejlesztések előtérbe helyezését, ami egy új globális versenyt indukál. Másik oldalról azonban óvatosan, de ráirányítja arra is a figyelmet, hogy pontosan az olyan kritikus területeken, ahol az adatok használatával vég-

Paradoxonnak tűnő módon tehát látni kell, hogy a digitalizáció robbanásában mind a jóléti, mind pedig a visszaélészerű kiaknázás terén legalább annyira szükséges a kritikus hatás eléréshez a humán, mint az alkalmazott tudományok fejlesztése és gyakorlatba való átültetése.

¹⁴ Amaël CATTARUZZA i.m. 26. o.

¹⁵ Amaël CATTARUZZA i.m. 26. o.

¹⁶ Amaël CATTARUZZA i.m. 28. o.

¹⁷ Amaël CATTARUZZA i.m. 42. o.



zett cselekmények hatékonyságát az határozza meg, hogy azok az emberekre és azok viszonyaira milyen hatást gyakorolnak, ismét kimagaslóvá válik a humántudományok szerepe és az e körbe tartozó piaci és állami képességek fejlesztése is. Paradoxonnak tűnő módon tehát látni kell, hogy a digitalizáció robbanásában mind a jóléti, mind pedig a visszaélészerű kiaknázás terén legalább annyira szükséges a kritikus hatás eléréshez a humán, mint az alkalmazott tudományok fejlesztése és gyakorlatba való átültetése.

Nem meglepő talán, hogy ezen okfejtéstől a szerző az adatok mögötti döntéshozatali és ideológiai mező felé mozdul el. Az okfejtés ezen részének tételgondolata a következő: „Megjelenik tehát az adat »életciklusa«, amely a különböző, egyszerre egymást követő és egyidejűleg zajló állomásokon halad át: előállítás, átvitel, tárolás, feldolgozás. [...] Minden egyes fázis egy geopolitikai és stratégiai kontextusra irányítja a figyelmet, és az adatteremtési és –felhasználási folyamat alatt végig választásokra kényszeríti a döntéshozókat.”¹⁸ Az adat és a digitalizáció témakörének ilyen megközelítésű vizsgálata megfelelő alapot ad a geopolitikára való áttéréshez, emellett rendkívül érdekes áttekintést alapoz meg adatok életciklusának döntéshozatali mátrixa és geopolitikai vetülete kapcsán, melyben az egyes fázisok kapcsán a kedvező lehetőségeket, a kockázatokat-sérülékenységeket, illetve a stratégiai és geopolitikai vetületeket is jól áttekinthető módon láttatja¹⁹ a szerző.

MÁSODIK RÉSZ: AZ ADATOK TERRITORIALIZÁCIÓJA FELÉ

A második részt a szerző annak rögzítésével kezdi, hogy a címadó kifejezés, az adatok territorializációja – területiesítése – paradox kifejezésnek tűnhet a világháló korában. Ezt mind a kibertér fogalma körüli gondolatok, mind pedig a kötet korábbi okfejtései az interneten gyarapodó adatmennyiségről alá is

támasztanak. E paradoxon azonban látszólagos, de kiváló eszköz arra, hogy a digitális adatokat összekapcsolja a geopolitikával, a hatalmi gondolkodással és ennek cselekményekben való megtestesülésével. A szélsőséges ideológiák elleni digitális térben való fellépés, a 2007-es Észtország elleni kibertámadás, majd azután a Grúzia, az Ukrajna elleni támadások, a Stuxnet, a Flame, a WannaCry, a NotPetya, a PRISM és az XKeyscore mint legismertebb tünetek ugyanis rávilágítottak arra, hogy a digitalizációnak vannak árnyoldalai, sőt nagyon komoly hatalmi vonatkozásai is. „Nem meglepő tehát, hogy az államok vagy a magánszféra egyes szereplői elkezdtek birtokba venni a kibertérrel és az adatokat. Az utóbbi években ráadásul valódi digitális területek jelentek meg. Így az érdekelt felek különböző geopolitikai következményeket észlelhetnek, akár az általuk gyakorolt politikai vagy jogi ellenőrzés, akár az abból általuk mérített erőforrások, akár az általuk kivetített értékek és szimbólumok vagy a rájuk áthárított azonosítási folyamatok terén. Végső soron e különböző – helyi, nemzeti, regionális – szinteken végbemenő territorializációs dinamika versengési és hatalmi viszonyok kialakulását vonja maga után a kibertérben, számos játékost mozgásba hozva.”²⁰ – írja a szerző. De mit is érthet ez alatt részleteiben?

A territorializáció első komponenseként az adatközpontok és a felhőszolgáltatás témakörét ragadja meg. Egyértelművé teszi, hogy ez a módszer a hatékonyság és praktikuság – bárholonnan online elérhető, nem kell saját adathordozó, stb. – elvei mentén lényegében adatközpontosítást jelent, melyben „az adatközpontok nemcsak a meglévő adatokat aknázzák ki, hanem azokból folyamatosan újakat is generálnak.”²¹ Emellett azonban arra is felhívja a figyelmet, hogy ez a centralizáció a globális piac révén céges köntösben teszi lehetővé adott hatalmi szereplőknek a fizikai területükön kívüli adatokhoz való hozzáférést és ez által a fizikai területükön kívüli hatásgyakorlást is. Nem véletlen, hogy éles szembenállások – például Ukrajna – esetén a felek betiltják a szemben álló(nak vélt) fél webszolgáltatóinak működését a saját területükön, mivel

¹⁸ Amaël CATTARUZZA i.m. 46. o.

¹⁹ Ld.: Amaël CATTARUZZA i.m. 47. o. 1. táblázata.

²⁰ Amaël CATTARUZZA i.m. 52-53. o.

²¹ Amaël CATTARUZZA i.m. 56. o.



ezzel az üzletszerű – de nem minden esetben államtól független²² – adatkinyerést próbálják akadályozni.

Az hogy ezek után a szerző az adatközpontokra mint a hatalmat raktáron biztosító entitásokra utal, nem meglepő, főleg, mert ezzel köti át – a Snowden-ügyre hivatkozva – azt a trendet, amely a regionális adatközpontok létesítésére irányul és a kétezres évek eleje óta egyre erősödik. A szuverenitásvédő regionális adatközpontokra példaként hoz francia és orosz törekvést is. Ezzel egyértelműsíti, hogy a világhatalmi versengésben a digitális szuverenitás megerősítése majd megóvása is egy kulcs tényező lesz.

E megközelítés révén az adattárolásról az adatáramlás geopolitikai vonatkozásai felé halad tovább a gondolat. E körben egyrészt a mélytengeri, illetve gerinc jelentőségű szárazföldi adatkábelek fontosságára, az ezek által generált sebezhetőségekre hívja fel a figyelmet Algéria 2015-ös „digitális sötét-ségbe” borulását felidézve. Rámutat azonban arra is, hogy ezek a nagyteljesítményű vezetékek nem csak „támadásra” és „elsötétítésre”, hanem megcsapolásra, azaz megfigyelésre is lehetőséget teremthetnek a megfelelő feltételek fennállta esetén. Ez utóbbi kapcsán az Amerikán áthaladó gerinc-jelentőségű vezetékek Upstream és Tempora kémprogramokkal való megcsapolását idézi fel, hogy aztán rögzíti: élénkül világszerte a törekvés arra, hogy a globális digitális adatközlésben az USA döntő túlsúlya mérséklésre kerüljön. E körben arra is felhívja a figyelmet, hogy a GAFAM²³ kábelpiaci szerepe nem segítette az amerikaiakkal szembeni bizalom kérdésén.

Mindezek felvezetésével a szerző lényegében pontot tesz a territorializáció paradoxonának kérdésére, mikor úgy fogalmaz: „Az utóbbi években Európához hasonlóan a világ több részén is megsokasodtak a regionális routingot és az adatok elhelyezését (data localisation vagy adatlokalisálás) érintő hasonló viták és intézkedések. Természetes az

olyan országok, mint Kína vagy Irán már régés-rég beemelték a nemzeti routingra vonatkozó lépéseket a digitális védőpajzsot érintő, átfogó intézkedéseik közé, amelyeknek az a célja, hogy elszigeteljék őket a külvilágtól (ezeket »kínai nagy tűzfal« és iráni »halal internet« néven szokás emlegetni). Mára ez a hozzáállás számos más államban is elterjedt, például Malajziában, Ausztráliában, Dél-Koreában vagy éppen Brazíliában.”²⁴ Az, hogy a listában vannak a transzatlanti térség szempontjából szövetséges szereplők is, sokat sejtető a jövőre nézve.

Az előző megállapítást és sejtetést aztán a szerző még egyértelműbbé teszi, mikor a személyre szabott tartalmak és szolgáltatások büvköre ellenére mutat rá arra, hogy hiába a fogyasztói társadalomra szabott alkalmazások sora, a leválást állami és piaci kooperációban végrehajtó szereplők tekintetében igenis csökken a digitális kitettség a külső hatalmak felé. Ezzel pedig egyértelművé és elválaszthatatlanná teszi a geopolitika és a digitális tér viszonyát, hiszen úgy fogalmaz: „Az adattárolás tükrében nagyon világosan látjuk tehát kirajzolódni a nemzetközi szintér erőviszonyait. E megállapításoknak mérsékelniük kell bizonyos elemzések hevét, amelyek a digitális technológiának köszönhetően a határok végét és egy posztvesztfáliai világ eljövetelét hirdetik. A jó öreg nemzetállami geopolitika még a kibertér valamennyi rétekében él és virul, és a szuverenitás, a befolyásolás vagy a hatlom még mindig aktuális kérdései napjainkban különböző módon, de át vannak ültetve ebbe az új környezetbe. Ez egyébként elsőre gyakran a jogon keresztül valósul meg, amely teljes egészében részt vesz az adatok territorializációjának folyamatában.”²⁵

Az adatok területiesítésének és ez által geopolitikai törekvésekhez kötésének folyamatában a tovább gondolkodás irányát egyértelműen a jog adja. E körben a szerző a hangsúlyt inkább arra fekteti, hogy a felhasználói

²² A szerző által említett ukrán-orosz reláció túl érdekes kitekinteni a kínai gazdasági és geopolitikai érdekek összekapcsolódásának kérdéseire is. Vö.: Bruno MACÃES: *Eurázsia hajnala. Az új világrend nyomában*. Bu-

dapest, Pallas Athéné Books, 2018.; Ling CHEN: *A globalizáció manipulálása. A bürokraták befolyása Kína üzleti világára*. Budapest, Pallas Athéné Books, 2019.

²³ Google – Apple – Facebook – Amazon – Microsoft.

²⁴ Amaël CATTARUZZA i.m. 69. o.

²⁵ Amaël CATTARUZZA i.m. 73-74. o.



beleegyezésre, illetve a látszólag jogi szabályok által korlátozott adatátadásra épülő transzatlanti – Amerika-központú – szisztema gyenge pontjaira, kiskapuíra hívja fel a figyelmet. E tekintetben tételmondatként kezelhető az adatkezelő cégek kapcsán rögzített mondat, miszerint a szóban forgó „vállalatok bevételeinek nagy része pedig az internetfelhasználók által a weboldalaikon hagyott másodlagos adatokkal való kereskedésből származik.”²⁶ Ennek a piaci elvű, az adatok kereskedelmére épülő gyakorlatnak a hozadékként kezeli a szerző, hogy a GAFAM piaci dominanciája miatt lényegében az amerikai jog területen kívüli érvényesülését is lehetővé teszi. Ez az elsődlegesen az általános szerződési feltételekre épülő extraterritoriális hatás per sze lehetőséget teremtett az amerikai állam helyzetének javítására is, amit a Patriot Act és a FISA Amendments Act, illetve a 2018-as Cloud Act kapcsán konkrét jogi gyakorlathoz is kapcsolt a szerző. Innen aztán az EU puha kísérletein át odáig viszi gondolatait, hogy az adatok szabad áramlását korlátozó nemzetállami törvényalkotás trendjére, ez által pedig a jog, mint geopolitikai eszköz fontosságára hívja fel a figyelmet a digitalizáció kapcsán is.

A nemzetállami szerep és a jog, mint ezt erősítő eszköz számbavétele után nem meglepő, hogy a szerző kitér az internet kormányzásának kérdésére és e körben a (1) többszereplős és a (2) többoldalú modelleket veszi számba. A többszereplős alatt azt az amerikai modellt érti, ahol az állam mellett a nem államiszereplők beleszólása is jelentős. Ehhez mérten a 2012-es dubai nemzetközi távközlési világkonferencián felszínre került nézetkülönbségek apropóján vezeti fel a többoldalú kormányzási modellt, melynek lényege, hogy az internet kormányzása a kor-

mányközi szint – az ITU²⁷ mint ENSZ mellett működő szervezet – felé mozdulna el, amelyben azonban a túlsúlyt a kormányok képviselői adnák. Fontos azonban kiemelni, hogy a szerző is elkülöníti az internet kormányzását az interneten történő kormányzástól, mely utóbbi leginkább az egyes viszonyokba az internet révén történő beavatkozás lehetőségeit jelenti, s mint ilyen a nemzetállami szereplők mellett a különféle regionális tömörüléseknek, például az EU-nak vagy a Budapesti Konvenciót²⁸ kezdeményező Európa Tanácsnak is jelentős szerepet ad.

A geopolitikai szereplők közti bizalmatlanság, a kitettségek csökkentésére irányuló törekvések, valamint a több kormányzat között balanszírozó entitások szerepének számbavétele után adódik a konfliktusok ki-

bertérrel összefüggő megvalósulásának gondolata „A háborútól a kiberháborúig?” kérdéssel. E tekintetben azonban a szerző kerüli a szenzációhajhász megközelítést, ezért alapvetésként rögzíti, hogy az „angol »cyberwar« kifejezésből származó kiberháború szó a médiában elterjedt jelentése szerint a ki-

bertérben zajló minden olyan konfliktusos cselekményt jelöl, amelynek egy vagy több állam az előidézője vagy a célpontja. Gyors elterjedése ellenére a kifejezés tartalma tudományos és katonai berkekben mind a mai napig vita tárgya.”²⁹

Ebből a felütésből a szerző már biztonssággal tud tovább haladni – a kötet eddigi logikája szerint – a problémagócok azonosítása felé. Felvillantja ugyan az Észtorország, Grúzia és Ukrajna elleni műveleteket, de inkább arra helyezi a hangsúlyt, hogy a digitális tér milyen mértékben kitágította a nem állami szereplők mozgás- és hatásterét. E körben per sze vissza-visszatért az állam általi motiválás, fedett irányítás kérdésére, de közben olyan fajsúlyos és még eldöntésre váró kérdéseket

...az adatok szabad áramlását korlátozó nemzetállami törvényalkotás trendjére, ez által pedig a jog, mint geopolitikai eszköz fontosságára hívja fel a figyelmet a digitalizáció kapcsán is.

²⁶ Amaël CATTARUZZA i.m. 76. o.

²⁷ International Telecommunication Union – Nemzetközi Távközlési Egyesület.

²⁸ *Convention on Cybercrime*, Budapest, 23/11/2001. – Magyarországon kihirdette az Európa Tanács Budapesten,

2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről szóló 2004. évi LXXIX. törvény.

²⁹ Amaël CATTARUZZA i.m. 89. o.



azonosít, mint az, hogy pontosan mi is különböztet meg egy digitális térben megvalósuló háborús cselekményt egy közjogi bűncselekménytől egy olyan közegben, ahol az elkövető azonosítása és ez által egy adott államnak való betudás is rendkívül problémás.

Ezt a kérdéskört aztán csak fokozza a terrrorszervezetek digitális térben történő érvényesülésének problémakörével, illetve az olyan digitális térben ténykedő csoportok problémájával, melyeket hivatalosan meg nem erősített híresztelések egy-egy állam érdekeinek érvényesítéséhez kötnek. A téma kapcsán a szerző a sok nyitott kérdés mellett rávilágít arra, hogy az állami és nem állami szereplők is érdekelték abban, hogy valamilyen keretek közé szorítsák a digitális térben megvalósuló „kártételeket”, így nem meglepő a „digitális genfi egyezmény” szükségességének felvetése sem. Nem mulasztja el azonban arra sem felhívni a figyelmet, hogy miközben az államok egyik oldalról tisztább viszonyokat sürgetnek a digitális térben, aközben a másik oldalon saját offenzív – és nem kizárólag katonai – képességeiket fejlesztik geopolitikai érdekeik hatékony digitális érvényesítését segítőként.

A nyitott kérdések halmazával azonban a szerzőnek sikerül egyfajta kritikai csúcspontot elérnie a kötetben, hiszen a digitális tér és a geopolitika összekapcsoltságában vitán felül álló módon a legsúlyosabb problémakört a digitális „támadások” kérdésköre jelenti. Ez ugyanis egyfelől egyértelműsíti, hogy a digitalizáció a geopolitikai érdekek érvényesítésének is új és jelentős terepet biztosít, másfelől viszont átvezetést ad a harmadik rész kérdéséhez: jelesül, hogy a klasszikus geopolitika miként is tud érvényesülni a digitális térben.

HARMADIK RÉSZ: KIÁLLJAE A GEOPOLITIKA AZ ADATOK PRÓBÁJÁT?

A téma kibontása az előző rész zárásából és a korábban írtakból adja magát: mennyire tud alkalmazkodni a fizikai térhez kötöttségből –

a geográfiából – kinőtt geopolitika egy a fizikai tértől elkülönülő és annak törvényszerűségeit szinte szétfeszítő, áthidaló alternatív térhez? Mennyire tudnak a szuverenitásra mint területi főhatalom gyakorlására épülő államok versenyezni egy olyan tér kihívásaival, melynek sötét részén – a darkweben – sok tekintetben állami korlátozás nélkül is zajlik az adatok cseréje és törvénytelen cselekmények előkészítése, megvalósítása? Hogyan érintik a nemzeti identitást a digitális térben képződő és megerősödő csoportidentitások? A bizonytalanságot elkerülendő azonban előzetes választ meg is adja a szerző, mikor úgy fogalmaz: „A kód/tér fogalmán, a harctér digitalizálásán, az úgynevezett okos határon, az adatmegfigyelésen és a topológiai megközelítésen át a mindennapjainkban színre lépő adatrendszerekkel szemben egy mozgásban lévő, részletgazdag geopolitikai szintér rajzolódik ki.”³⁰

E narratívának megfelelően elsőként a kód/tér kérdését tekinti át a szerző és Lawrence Lessing 1999-es *Code and other Laws of Cyberspace* című munkájától indítva vezeti fel, hogy maguk a kiberteret felépítő kódok és algoritmusok is kulturálisan, politikailag determináltak már a létrejöttük közege és célja folytán. Innen aztán továbbhalad Rob Kitchin és Martin Dodge *Code/Space* című 2011-es munkája felé, melyben a szoftverek és a mindennapi élet kölcsönhatásait helyezték a középpontba, megállapítva, hogy a digitalizáció szintje életünk szempontjából eljutott az „everyware” állapotába, vagyis – tudatos elkerülés nélkül – lényegében az okos eszközökkel közvetítve a digitális tér mindenhol velünk van. E tekintetben felhívja a figyelmet arra, hogy az okos eszközökkel rendkívüli mennyiségű korábban szenzitívnek tekintett adatunkat önként adjuk közre a világhálón erre szakosított szereplőknek, s így lényegében „a kód és tér egymásba ágyazottsága (embeddedness) tehát egy kiterjesztett valóság, egy kusza adatokból áll területi másolat megjelenését idézi elő...”³¹ Ez a fajta másolat, vagy tükröződés azonban ránk vonatkozó, egyéni, csoportos és társadalmi szintű adatok sokaságából és folyamatos frissítéséből épül fel, ami geopolitikai szempontból kimagasló jelentőséggel bír, hiszen mindez „egy kettőződéshez

³⁰ Amaël CATTARUZZA i.m. 99. o.

³¹ Amaël CATTARUZZA i.m. 103. o.

vezet, az adatoknak egy területekhez, népekhez és világunk egészéhez társított új, láthatatlan rétegéhez, ami a kód közvetítésével lehetővé teszi a hozzáférést a szab szemmel láthatatlan információkhoz.”³² Ez a hozzáférési lehetőség pedig geopolitikai értelemben egy szinte kifogyhatatlan tárházat képez a befolyásolásra és az érdekek érvényesítésére, ezek által pedig a versengésre, de immár nem csak állami szereplők között.

A kód/tér illetően kapcsolatának leírásából adja magát a harctér digitalizációjának témája, melyben a szerző újra a nem állami szereplők lehetőségeire kanyarodik vissza és példaként a Laska-e-Taiba terrorcsoport 2008-as Mumbai támadásaira irányítja a figyelmet, melyek során a terroristák hatékonyságát nagyban fokozta, hogy a világhálón való időben – különösen közösségi hálókon és fórumokon – közzétett információk révén ismerték és tervezhették a rendfenntartó erők mozgását, érkezését, sőt profilozhatták túszaikat is. A digitális tér tehát egy ilyen értelemben „laikus” terrorcsoport „hírszerző” képességét klasszisokkal erősítette fel a korábbiakhoz képest, amiből a szerző is okkal vezeti le, hogy jelentős változások prognosztizálhatók a komolyabban szervezett entitások, különösen a hagyományos hatalmi aktorok képességeinek digitalizáció révén való fejlesztése terén a jövőben.

Erre a nyitott gondolatra aztán példákat is hoz az amerikaiak harctéri drónok felvételeire – a Google együttműködésével – épített arcfelismerő szoftver fejlesztésére irányuló projektjétől, a civil szoftverek katonák és titkosszolgák általi alkalmazása miatt keletkezett biztonsági rések és dekonspirációk esetein át a francia FELIN és Scorpion programokig. A különféle fejlesztésekben rejlő lehetőségeket a szerző ugyan nem vitatja, de biztonsági szempontból helyesen hívja fel a figyelmet arra, hogy a védelmi és biztonsági célú rendszerek és funkciók átfogó digitalizációja kapcsán van min elgondolkodni, hiszen az számos új kockázatnak nyit terepet. „A hálózatosítás, ami a tárgyak internetjének és az okos eszközöknek a hadsereg általi tömeges

használatával jár, tulajdonképpen már önmagában sebezhetővé teszi a hálózatot. Minél jobban bővül a hálózat, annál jobban megnyílik az egészét fenyegető potenciális támadások előtt.”³³ Erre persze a fejlesztői oldal a biztonsági protokollok, a hálózatra való csatlakozás korlátozása – egy fajta zárt célú alhálózat – gondolataival reagálhatnak, azonban a szerző által is hozott példák az emberi tényező nehezen kiküszöbölhető kockázatait akkor is validálják.

A harctér digitalizációja kapcsán a szerző végezetül számot vet a big data elemzésében rejlő további stratégiai lehetőségekkel, különösen a konfliktusok kialakulására irányuló trendek elemzésével, illetve az aszimmetrikus szituációkban a potenciális cselekmények modellezésével, melyek a műveleti hatékonyságot és ezzel a veszteségek megelőzését is segíthetik, nem kis hadiipari érdeklődésre és üzletkötési törekvésekre ösztökélve a lehetséges fejlesztőket. Erre példaként az amerikai COMPASS programot hozza, „amely aszimmetrikus konfliktusok esetében a játékelmélet, a modellezés és a szimuláció eszközeivel igyekszik megjósolni az ellenfél lépéseit. Kiterjedt adatlekérdezés után (videók, szövegek, képek, stb.) az algoritmusos feldolgozás segítségével a lehető legtöbb hipotézis számba vehető a kockázatok csökkentése és a legjobb forgatókönyvek megtalálása érdekében.”³⁴ E körben persze érdemes hozzátenni az optimista számvetéshez, hogy a szembenálló felek mindig reagáltak a technológiai túlsúly és fölény révén szerzett előnyökre és ez már-már védjegyévé vált az aszimmetrikus hadviselésnek, akár csak a birodalmak temetőjének nevezett Afganisztán és az ottani szereplők aszimmetriához szokott harcmodora.

A mindennapok terén persze a harctéri párhuzamtól visszább kell lépni és erre a valódi globalizáció és a közlekedés fejlődése, nem utolsó sorban pedig ennek a visszaélésekre is módot adó volta miatt az okos határ („smart borders”) lehetőséget is kínál a szerzőnek. A 9/11 utáni fokozott ellenőrzésre irányuló biztonságfokozási trendhez kötött gon-

³² Amaël CATTARUZZA i.m. 103. o.

³³ Amaël CATTARUZZA i.m. 109. o.

³⁴ Amaël CATTARUZZA i.m. 110. o.

dolat kapcsán a szerző az arany középutat keresi. Nem vitatja, hogy a világ jóval könnyebb bejárhatósága komoly kockázatokat is rejt és ezért fokozott ellenőrzést igényel, de a technika révén fokozható megfigyelési lehetőségek szabadságjogi aggályaira is rávilágít. A digitalizációnak a határok hatékonysága tekintetében nagyon komoly súlyt tulajdonít, hiszen úgy fogalmaz, hogy az „adatbázisok és kapcsolódásaik megsokasodásával a határnak ahhoz, hogy hatékony legyen, elméletileg nincs többé szüksége arra, hogy testet öltjön.”³⁵ Ehhez az elvi lehetőséghez aztán inkább a potenciális elvárásokat társítja, jelesül azt, hogy a határforgalom zökkenőmentes legyen, de a nem kívánatos tényezők kiszűrhetővé válnak. Ez a valóságban persze még messze áll az előbbi idézetben felvázolttól, de a szerző helyesen világít rá arra, hogy a SIS³⁶, az APIS³⁷ vagy épp a VIS³⁸ létrehozását a határfok fokozása motiválta. E körben pedig említés szintjén a szerző kitekint a biometrikus adatok rögzítésének kérdésére és aggályaira is, elismerve azonban, hogy az emberi test egyediségének adatosítása soha nem látott szintre emelheti a bizonyosságot az ellenőrzés terén.

Az okos határtól és az abban rejlő megfigyelési lehetőségektől aztán a kötet logikája az „adatmegfigyelés kora” felé viszi az olvasót, amely cím alatt azonban nagyjából a korábban már közöltek öleli össze és ülteti a védelmi és biztonsági feladatellátás stratégiai színtereire. Az okos eszközök sokasága és a dolgok internetje révén valós időben folyamatosan magunkról gyártott és átadott adatok biztonsági és ellenőrző jellegű felhasználásának gondolatát illetve a GEOINT³⁹ fejlődését felvetve a szerző az adatok alapján történő megfigyelés kihívásaira hívja fel a figyelmet. Itt sem vitatja, hogy a technológia fejlődését a rend és biztonság megóvása érdekében alkalmazni kell, hiszen az ezzel ellenérdekeltektől is használni fogják az innovációt, azonban a kötet talán ezen a ponton lép ki az egyensúlyi szerepből és engedni szabadjára a totális megfigyeléssel és az automatizált állami megfigyeléssel kapcsolatos aggodalmakat. E

körben is rávilágít a technikai, képességbeli és etikai korlátokra, de nagyobb teret enged az aggályoknak és feltételezésnek, mint a racionális kereteknek.

„A megfigyelés kora” címbe rejtett aggodalom persze a technológia robbanás-szerű fejlődéséből következő lehetőségek sokasága miatti bizonytalanságot is tükrözhet. Ezt az olvasói érzést a következtetéseket megelőző utolsó cím „A területi hatalomtól a hálózati hatalomig” is tükrözi, mivel az inkább csak egy levezető gondolatébresztés a megfigyelés bizonytalanságai után, mintsem egy önálló témarész kibontása. E körben a kibertérképek apropóján a szerző rögzíti, hogy „úgy gondoljunk a térre, mint olyan hálózatok sorára, amelyekben a távolság már nem releváns. Ebben a vonalak által összekötött pontok szimultán kapcsolatban vannak, tekintet nélkül arra, hogy fizikailag hány kilométer választja el őket egymástól. A terület elhalványul a hálózat mögött, a topográfia pedig a topológia mögött.”⁴⁰ Ez a témarész tehát nagyon sokat rejthetne magában, azonban a szerző itt már csak figyelemfelhívásra törekedett. Plasztikus példái mellett inkább éreztetni kívánta, hogy a digitalizáció révén a hatalomgyakorlásban a digitális hálózatba kapcsoltág vetekedni tud a területi kötődéssel, sőt lehet hogy idővel majd meg is előzi azt. Ezt azzal is igazolja, hogy a „közösségi hálózatok földrajza és geopolitikája kétségkívül a legbeszédesebb példái e relációs tereknek, amelyekben kapcsolatok szövődnek vagy szilárdulnak meg, erő- és befolyási viszonyok alakulnak és erősödnek meg egészen addig a pontig, hogy ma már egyetlen választást sem lehet megnyerni világos digitális stratégia nélkül.”⁴¹ Hova tovább mondjuk ki, ma már egyetlen választást sem lehet megtartani digitális befolyásolási törekvések nélkül.

³⁵ Amaël CATTARUZZA i.m.112. o.

³⁶ Schengen Information System

³⁷ Advanced Passenger Information System

³⁸ Visa Information System

³⁹ Geospatial Intelligence

⁴⁰ Amaël CATTARUZZA i.m. 121. o.

⁴¹ Amaël CATTARUZZA i.m. 123. o.



SZERZŐI ÉS OLVASÓI KÖVETKEZTETÉSEK

A szerző a következtetések között lényegében vállalkozása nagyságát és főbb eredményeit törekszik megérvelni. E körben úgy vélem az olvasó elégedett lehet, hiszen egy emészthető, jól strukturált, a reális példákat az elméleti megközelítéssel egyensúlyban tartó, s az elfoglalt álláspontok terén is középutas élménnyel gyarpodhatott.

Egyértelműen megerősíthető a kötet egésze alapján az az előzetes feltevés, hogy a digitalizációval járó változások fokozatosan a társadalmi mező egészére jelentősen kihatnak, s ebből adódóan aztán minden más szférára tovagyűrűznek hatásukban, ideértve a geopolitikát és annak eszköztárát is.

Ami talán a következtetések kapcsán érdekessége a kötetnek, hogy a kötet témájának fontosságát megérvelendő mintha a hálózati hatalom kérdését boncolgatná tovább. Ennek egyik eleme az a gondolat, miszerint: „Joseph Nye politológus már 2010-ben új írta le a kibertér, mint olyan területet, amely lehetővé teszi a hatalom generálását (Nye, 2010) mind a hard power (támadások, védelem és ellentámadás, vírusok és vírusirtók, digitális fegyverek és pajzsok használatával), mind a soft power (befolyásolási, információs és dezinformációs stratégia, kormányzási mód, stb.) vonatkozásában. Ezért megalkotta a cyber power fogalmát, és bemutatta, hogyan teremtett a kibertér új környezetet a szereplők közötti hatalommegosztásban. Ez pedig új hatalmat ad a nem állami szereplők kezébe, és mélyrehatóan alakítja az államokhoz fűződő viszonyukat.”⁴² Ez a gondolatkör ugyanis nem csak a geopolitikai viszonyokban jellemző hatalomgyakorlási és cselekvési formákra gyakorolt újító hatás miatt teszi fajsúlyossá a digitalizáció kérdését, hanem a nem állami szereplők térnyerésének

újabb alátámasztása révén nyitva hagy egy komoly kérdést a hálózati hatalomgyakorlás kapcsán is.

A Nye gondolataival felvezetett új helyzetet azonban a szerző maga is tovább fokozza és ezzel talán a kötet igazi mondanivalóját rejti sorai közé a geopolitika alakulása és azon belül a hatalom gyakorlása és színterei kapcsán. Ezt úgy fogalmazza meg, hogy az „utóbbi évtizedeket tehát a hatalomnak a digitális terület általi egyfajta újrafelosztása jellemezte. Ez az újrafelosztás ma részben ösz-

szeszavarja a szokásosan elfogadott geopolitikai kategóriákat és hierarchiakat a köz- és magánszféra szereplője, az állami és nem állami szereplő, az erős és gyenge szereplő között. Társadalmunk digitalizációja és a társadalmi interakciók robbanásszerű növekedése a kibertérben megmutatja és felgyorsítja a háború és béke, a katonai és civil világ, a hadszínterek és hétköznapi terek közötti, a modern korban létrejött különbségeket, valamint összes határ fokozatos eltűnését.”⁴³

E záró gondolatok – a szerző által szándékosan feltett majd nyitva hagyott kérdéseket megelőzve – ugyanis nem csak a kötet fontosságát és üzenetének helyességét támasztják alá, de egyben egy rendkívül

nagy kihívást támasztanak a szekértű, kutató olvasóközönség elé, hiszen e témakörök kapcsán további kutatások szükségesek, amelyek alapján aztán javaslatok kidolgozása és megoldások meghonosítása válhat lehetővé úgy, hogy a biztonsági kockázatok hatékony méréséklését épp úgy szolgálják mint a jogok túlzott korlátozásának elkerülhetőségét.

FELHASZNÁLT IRODALOM

- [1] A. ERTAN – K. FLOYD – P. PERNIK – T. STEVENS (eds.): *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*. Tallinn, CCD CoE, 2020.

⁴² Amaël CATTARUZZA i.m. 126. o.

⁴³ Amaël CATTARUZZA i.m. 126.o.

- [2] Alexander KLIMBURG (eds.): *National Cyber Security Framework Manual*. Tallinn, CCD CoE, 2012.
- [3] Amaël CATTARUZZA: *A digitális adatok geopolitikája. Hatalom és konfliktusok a big data korában*. Budapest, Pallas Athéné Books, 2020., 13. o.
- [4] Bruno MACÃES: *Eurázsia hajnala. Az új világrend nyomában*. Budapest, Pallas Athéné Books, 2018.
- [5] GIANNOPOULOS G. – SMITH H. – THEOCHARIDOU M. (eds.): *The Landscape of Hybrid Threats. A Conceptual Model Public Version*. Luxembourg, Publications Office of the European Union, 2021.; Josef SCHROEFL: *Cyber power is changign the concept of war*. Helsinki, Hybrid CoE Strategic Analysis 21., 2020.
- [6] HÓDOS László: *A hibrid konfliktusok felívelési szakasza, avagy a fenyegetés észlelésének, megelőzésének és kezelésének nemzetbiztonsági aspektusai*. In Honvédségi Szemle 2020/4. szám, 49-64. o.
- [7] Katharina ZIOLKOWSKI: *Confidence Building Measures for Cyberspace – Legal Implications*. Tallinn, CCD CoE, 2013.
- [8] KELEMEN Roland – FARKAS Ádám: *To the Margin of the Theory of a New Type of Warfare: Examining Certain Aspects of Cyber Warfare*. In Szabó Marcel – Gyeney Laura – Lános Petra Lea (szerk.): *Hungarian Yearbook of International Law and European Law* (2019). Den Haag, Eleven International Publishing, 2020., 203-226. o.
- [9] KELEMEN Roland – NÉMETH Richárd: *A kibertér alanyai és sebezhetősége*. In Szakmai Szemle, 2019/3. szám, 95-118. o.
- [10] KELEMEN Roland – NÉMETH Richárd: *Multidisciplinary Approach of the Concept and Characteristics of the Cyberspace*. In Glavanits Judit – Király Péter Bálint (szerk.): *Law 4.0 Challenges of the Digital Age*. Győr, Széchenyi István Egyetem Deák Ferenc Állam- és Jogtudományi Kar, Nemzetközi Köz- és Magánjogi Tanszék, 2019., 49-59. o.
- [11] KELEMEN Roland – NÉMETH Richárd: *Vulnerabilities of the Cyberspace Due to Its Social Nature*. In Rastislav Funta (szerk.): *Počítačové právo, UI, ochrana údajov a najväčšie technologické trendy*. 2019, 51-66. o.
- [12] KELEMEN Roland – SIMON László: *A kibertérben megjelenő fenyegetések és kihívások kezelésének egyes nemzetközi jogi problémái*. In Farkas Ádám – Végh Károly (szerk.): *Új típusú hadviselés a 21. század második évtizedében és azon túl. Intézményi és jogi kihívások*. Budapest, Zrínyi Kiadó, 2020., 150-170. o.
- [13] KELEMEN Roland: *A kibertérből érkező fenyegetések jelentősége a hibrid konfliktusokban és azok várható fejlődése*. In Honvédségi Szemle 2020/4. szám, 65-81. o.
- [14] KELEMEN Roland: *A kibertérből érkező fenyegetések jelentősége a hibrid konfliktusokban és azok várható fejlődése*. In Honvédségi Szemle 2020/4. szám, 65-81. o.
- [15] KREKÓ Péter: *Tömegparanoia 2.0. Összeesküvés-elméletek, álhírek, dezinformáció*. Budapest, Atheneum Kiadó, 2021.
- [16] KREKÓ Péter: *Tömegparanoia. Az összeesküvés-elméletek és álhírek szociálpszichológiája*. Budapest, Atheneum Kiadó, 2018.
- [17] Lee MCINTYRE: *Post-Truth*. Cambridge, MIT Press, 2018.; Ignas KALPOKAS: *A Political Theory of Post-Truth*. Cham, Palgrave Pivot 2019.
- [18] Ling CHEN: *A globalizáció manipulálása. A bürokraták befolyása Kína üzleti világára*. Budapest, Pallas Athéné Books, 2019.
- [19] Michael N. SCHMITT (eds.): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge, Cambridge University Press, 2017.
- [20] Michael N. SCHMITT (eds.): *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge, Cambridge University Press, 2013.
- [21] MUNK Sándor: *A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései*. In *Hadtudomány* 2018/1. szám, 113-131. o.



- [22] OTTIS R. – LORENTS P.: *Cyberspace: Definition and Implications*. In Proceedings of the 5th International Conference on Information Warfare and Security, Dayton, OH, US, 8-9 April. 2010., 267-270. o.
- [23] SZKÁLA Károly – MUNK Sándor: *A kibertér fogalma, értelmezése és fejlődése*. In Földrajzi Közlemények 2018/4. szám, 344-355. o.
- [24] U. M. MBANASO – E. S. DANDAURA: *The Cyberspace: Redefining a New World*. In IOSR Journal of Computer Engineering, 2015/3., 17-24. o.



IMPRESSZUM

Szerző(k):

Farkas Ádám PhD

Kézirat lezárásának ideje:

2021. március 5.

Szerkesztők:

Farkas Ádám PhD
Glavanits Judit PhD
Karácsony Gergely PhD
Keserű Barna Arnold PhD

Kelemen Roland
Király Péter Bálint
Németh Richárd
Spitzer Jenő

Kiadó:

Smart Law Research Group (Digitális Közösségek Fejlesztéséért Egyesület)

Kiadó képviselője:

Dr. Glavanits Judit

Kiadó székhelye:

9155 Lébény, Fő út 65.

Elérhetőségek:

<http://smartlawresearch.hu/slrgwp>

ISSN:

2732-3846

A borító a <https://wallpaperaccess.com/download/iot-3246253> címen elérhető ingyenes háttérkép felhasználásával 2021. február 15-én készült.

A sorozat egyes számaiban foglalt vélemények, állásfoglalások a szerzők saját véleményét tükrözik. Azok nem tekinthetők sem a kiadó, sem a szerzőt foglalkoztató intézmények hivatalos álláspontjának.

A sorozat célja a SmartLaw Research Group, illetve annak tagjai és esetleges külső együttműködők által végzett kutatások részeredményeinek közzététele a szakmai, tudományos megvitathatóság érdekében, illetve a későbbi publikációk előkészítésének támogatása érdekében.