dr. Dornfeld László – Keleti Arthur – Barsy Miklós – Kilin Józsefné – Berki Gábor – dr. Pintér István

Műhelymunkák

A virtuális tér geopolitikája

Tanulmánykötet

2016/1. szám

Geopolitikai Tanács Közhasznú Alapítvány – Budapest, 2016
w w w . c g e o p o l . h u

Szerkesztette: Pintér István

A kötetben publikált tanulmányok
a szerzők önálló véleményét tartalmazzák,
így az abban foglaltak nem tekinthetők
a Geopolitikai Tanács hivatalos álláspontjának.

Idézés: Szerző neve (2016) A cikk címe. In: PINTÉR, István: A virtuális tér geopolitikája. Geopolitikai Tanács Műhelytanulmányok, 2016/1. p. oldalszám.HU ISSN 1788-7895. ISBN 978-963-9816-34-3.

Citation: Name of the author (2016) Name of the article. In: PINTER, Istvan: Geopolitics of the Virtual Space. Council on Geopolitics Working Papers, 2016/1. pp.
HU ISSN 1788-7895. ISBN 978-963-9816-34-3.

Tartalom

Bevezető helyett

Frédérick Douzet*

Geopolitika a kibertér megértéséhez**

Fordította: Monti Norbert

Nyelvi lektor: Vincze Katalin

* Az Université de Paris VIII Geopolitikai Francia Intézetének professzora, a Castex kiberstratégiai elnöke (IHEDN partneri társulás, az Airbus Group támogatásával)

** A cikk a Hérodote, 2014. év 152-153. számában jelent meg.

Bevezető

A Hérodote havilap már 1997-ben színt vallott az „Internet politizálja a világot" című cikkével, amelyben bejelentette: „az Internet a konfliktusok késleltetése helyett, inkább megsokszorozza és komplikálja azokat" (Douzet, 1997). Az optimista véleményekkel szemben, amelyek a földrajzi határok megszűnését jósolták, havilapunk már akkor rámutatott azon geopolitikai kihívásokra, amelyeket a megállíthatatlan információ és kommunikációs rendszerek elterjedése okoz világszerte.

> *Az internet már önmagában is több geopolitikai konfliktus forrása. A különböző érdekeltségű nemzetek mindenféle dominálási stratégiát vetnek be, hogy ellenőrizhessék a hálózatok tartalmát, működését és gazdasági növekedését. A nemzetbiztonság számára stratégiailag fontos (…) és a hatalmi harcok során rendkívül erős eszköz a csoportok, kisebbségek, politikai, vallási és gazdasági erők kezében, helyi vagy akár világszinten.*

Edward Snowden nyilvánosságra hozott titkos dokumentumai az Egyesült Államok Nemzetbiztonsági Ügynökségének (NBÜ) teljes körű megfigyeléséről, minden kétséget kizáróan mutatják, hogy a földrajzi tényezők továbbra is lényegesek, és a geopolitika még mindig segít a modern világ konfliktusainak megértésében. A stratégiai és nemzetközi tanulmányok (CSIS)[1] kutatója, James A. Lewis is így érvel. Bemutatja, hogy a titkos dokumentumokról szóló információk hatása országonként változó, de globálisan, a számítógépes forradalom ellenére, pillanatnyilag az USA stratégiai érdekei és céljai továbbra is változatlanok maradnak. Az a térképészeti kutatás, melyet Louis Pertnaud[2] végzett, feltárja a politikai határok jelentőségét, még akkor is, ha a technológia átszeli azokat. Az 1990-es évek elején a tér és idő határait nem ismerő kommunikáció robbanásszerű növekedése a demokratikus eszmék és értékek terjesztését és ezzel együtt a demokratizálódás, illetve béketerem-

1 Stratégiai és Nemzetközi Tanulmányok Kutatóközpontja, amelynek a székhelye Washington DC-ben található, három egymást követő évben A Global Go To Think Tank Index az első agytrösztként tarja számon a „Nemzet védelem és biztonság" kérdésében, a University of Pennsylvany éves beszámolója az Egyesült Államok agytrösztjeiről.

2 Az Université de Paris VIII Geopolitikai Intézetének Master hallgatója.

tés reményét ígérte. A hálózatok összekapcsolódásából megszületett kibertér a „globális falu" eszmei képét vetítette fel, amelyet már Marshall McLuhan harminc évvel ezelőtt megálmodott (McLuhan, 1964). A kommunikációs hálózatok bővítése mindig is egy jobb világ utópiáját vetítette elénk (Musso, 2003; Mattelart, 2009); de az internet nemcsak ígéretet, de kihívást hozott magával.

Az internet exponenciális növekedése forradalmasította életmódunkat, felforgatta a gazdaságot, megsokszorozta a kommunikációs eszközeink számát és újabb látóhatárokat tárt elénk, amelyeket csak most kezdünk igazán felfedezni. Ám ugyanakkor területi feszültségeket keltett és megnövelte a konfliktusok számát, hiszen mindenki azért küzd, hogy ellenőrizhesse és szabályozhassa az internetet. Az új fenyegetésekből új feszültségek kristályozódtak ki. Ezek a kiberbűnözéshez vagy az informatikai hálózatok felhasználásához kötődnek, és a már meglévő politikai konfliktusok, katonai összeütközések, gazdasági nézeteltérések, hírszerzés, diplomáciai és kulturális befolyás keretein belül játszódnak le. A Big Data (hatalmas mennyiségű adat) és az Open Data (nyilvános adatok tárháza) megjelenésével egyre több vita alakul ki a magánélet tiszteletben tartásának, a szólásszabadság és egyéb személyi szabadságjogok kérdésében. A Snowden-ügy mindezeket egyszerre érinti, mivel a virtuális térben e tényezők összefonódnak.

Sokáig az internet kérdése a kulturális és technológiai szakértők kis csoportjának a kezében volt. Azonban, a dilemmák berobbantak a közszférába, mivel az internet gyors fejlődésével (közel 3 milliárd felhasználó világszerte) a mindennapi életünk szerves részévé vált, így sok technikai döntés vált politikai és stratégiai döntéssé is. A kibertérben mozgó sok szereplő (egyének, csoportok, start-up vállalkozások) gyors reagálásukkal és elképesztő kreativitásukkal kivették részüket – és a profitot – a hálózat növekedéséből, ha akarjuk, ha nem.

A kormányok, a katonai haderők, a vállalkozások és a polgárok egyre inkább meg akarják érteni a felmerülő kérdéseket, hogy megvédjék érdekeiket. Koherens stratégiát kívánnak kiépíteni, hogy új lehetőségeket ragadhassanak meg a kockázati tényezők kezelésével egy időben. Ez különösen igaz az államok esetében, amelyek mindent átható hatalma szembesül a virtuális tér többi szereplőjével, a bűnözőkkel, a hackerekkel, aktivistákkal, a nagy

magánvállalatokkal, a másként gondolkodókkal, a nem állami szférához tartozó szereplőkkel vagy éppen más államokkal. Ezen erőhatalmi összeütközések nem a klasszikus geopolitikai térben zajlanak, de mégis szükségünk van a geopolitikára az elemzésükhöz.

A geopolitika meghódítja a kiberteret

Felvetődik a kérdés, miképp tudjuk megérteni a kibertérben zajló konfliktusokat a geopolitika segítségével. A geopolitika tanulmányozza és különböző szinteken elemzi a hatalmi versengést és befolyást egy-egy területen. Foglalkozik a területen jelenlévő konfliktus dinamikájával, az ellentmondások bemutatásával, a szereplők stratégiájával, amely a terület ellenőrzéséhez, megszerzéséhez és érdekeik megvédéséhez szükséges az adott földrajzi térségben. Vagyis a földrajzi terület van figyelmének központjában, amely a kibertér esetében nyilvánvalóan problémát okoz. A kibertér egy új területi forma lenne? És, ha ez igaz, melyek lennének a földrajzi határai? Melyek a felségterület határai?

Mit értünk kibertér alatt? Nem létezik egységes és tárgyilagos meghatározás, de több definíciót is találhatunk, amelyek többé-kevésbé pontosak, és tükrözik a szereplők aggodalmait, illetve érdekeit. Az oroszok, ugyanúgy, mint a kínaiak, kevésbé használják a kibertér fogalmát – amely egy külön terület gondolatát ébresztené fel – így inkább internetről beszélnek. Ily módon az információbiztonság és a viták megoldása az állam kompetenciájává válik. A könnyebb megértés érdekében, létezik egy minimális meghatározás: A kibertér egyszer's mind az Internet[3] és az a tér, amit létrehoz: egy immateriális tér, amelyben földrajzi területtől független változások történnek, minden nemzet polgárai között, pillanatok alatt, a távolságot teljesen megszüntetve.

Az internet technikai definíciója általánosan elismert (lásd a szószedetet a kiadvány végén): a világ informatikai hálózata több, mint 40000, ugyanazt

3 Pontosabban a digitalizált adatok automatizált kezelése a számítógépes hálózatok világhálózatán, a Nemzeti Hálózat- és Információbiztonsági Ügynöksége eszerint, 2011. Az információs és kommunikációs rendszerek nemcsak az internetre korlátozódnak, de az internet hozta létre mindazt, amit ma kibertérnek tartunk.

a nyelvezetet használó, autonóm hálózatok kapcsolata. Viszont az általa létrehozott tér meghatározása nehezebb, mert ellentmondásos nyilatkozatokból, a tudományos-fantasztikus irodalomból, az aktivizmusból, a politika és a marketing területéről származó képekből táplálkozik. A *Felhő* csak még bonyolítja a szemantikai ködbe burkolózó kiberteret.

Réteges szerkezet

Ahhoz, hogy jobban megértsük a kiberteret meg kell említenünk annak réteges szerkezetét. A virtuális teret, oly „rétestésztának" tekinthetjük, melynek különböző rétegei között kölcsönhatás van. A szereplők 3, 4, 5 vagy akár 7 rétegre is szétbonthatják ezt. Ennek a struktúrának minden szintjén a szereplők közötti hatalmi versengést találjuk, gyakran technikai kérdésekkel kapcsolatban, amelyek mégis rendkívül geopolitikaiak, ahogy ezt látni is fogjuk. Az egyszerűség kedvéért négy réteget fogunk bemutatni. Az első a fizikai réteg. Az internet infrastruktúráját főleg tengeralatti és szárazföldi kábelek összessége alkotják, melyek az internet gerincét (backbone), illetve a távközlési rendszerek és számítógépek jelentik: egy sor földrajzi és politikai korlát alá vetett, földrajzi területre telepített hardverről van szó, amelyet megépíthetnek, átalakíthatnak vagy tönkretehetnek, rákapcsolhatnak vagy lekapcsolhatnak a hálózatról. Jérémy Robine és Kavé Salamtian cikke megmutatja ennek az infrastruktúrának a fontosságát és stratégiai jellemzőit. Az infrastruktúra, mivel geolokalizálható, könnyebb felmérni térképészetileg, mint kibergeográfiailag. Kevin Limonier térképekre alapozva elemzi az orosz infrastruktúra stratégiai jellegzetességeit és azon ábrázolásokat, amelyek azokat alátámasztják. A fizikai infrastruktúrát a nyitottság és az információáramlás nevében hozták létre integrált biztonság nélkül. Az internet alapítóatyáinak egyike, Louis Pouzin szerint az Internet biztonságossá tételéhez az alapoktól kellene elkezdeni az újraépítését[4].

A második réteget alkotja a logisztikai infrastruktúra. Ide tartoznak mindazon szolgáltatások, amelyek lehetővé teszik az adatátvitelt a hálózat egyik

4 N. Madelaine, «Louis Pouzin: "L'Internet doit être refait de fond en comble"». *Les Échos,* n°21442 du 24 mai 2013, p. 23

pontjáról a másikba, vagyis az információáramlást, hálózati adatcsomagokra bontva, a feladótól a címzettig. A logisztikai felépítés alapvetően a harmonizáción, egy közös nyelvezeten alapszik, amely lehetővé teszi, hogy minden számítógép kommunikálhasson egymás közözött: ez az Internet Protocoll (TCP/IP). Ezek a szolgáltatások az „útválasztók", azaz a hálózati forgalomirányításhoz szükségesek, hogy az adatcsomagok áramolhassanak a hálózatok között. Ezen kívül van az Azonosító (a hálózati azonosító vagy felhasználói név) és a Hálózati cím (amely átalakítja a címeket jelölő számsorozatokat olvasható szavakká a felhasználó számára). Más tényezőket is lehet geolokalizálni néhány technikai beállítással (domain nevek, IP címek…). Bertrand de La Chapelle interjú során beszél a hálózati címek körül folyó vitákról. Az Egyesült Államok továbbra is erős szimbolikus hatalmat gyakorol a hálózati címek felett a Kereskedelmi Minisztériumon keresztül. Dominique Lacroix pedig bemutatja a domain nevek megszerzésének gazdasági és politikai kihívását.

A harmadik réteg az alkalmazásokból áll, ezek felhasználóbarát informatikai programok, amelyek lehetővé teszik, hogy bárki használhassa az internetet anélkül, hogy ismerné a számítógépes programozást (Web, email, közösségi oldalak, kereső motorok). A Snowden-ügy világosan megmutatta néhány nagyvállalat (Google, Facebook, Amazon…) alkalmazásainak világszintű sikerét. Ezek azok a nagyvállalatok, amelyekre a felhasználók szívesen rábízzák személyes adataikat, és amelyeket a marketing, illetve az ország információszolgáltatói ügyesen kiaknáznak. Mindezt Stéphane Frénot és Stéphane Grumbach a gazdaság új fekete aranyának tartják. Az adatok nem tűnnek el így a felhőkben (Cloud), de a magán- és közszereplők kezelés alatt álló szerverekben tárolják őket.

Végül a negyedik réteg a társadalmi információ és interakció rétege, amit néha kognitív vagy szemantikai rétegnek is neveznek. Itt játszódik felhasználók eszmecseréje valós időben szerte a világon, és ezt lehet a legnehezebben geopolitikai szempontból megérteni és ábrázolni. Ez azonban a legkevésbé sem irreleváns, amikor meg kell határoznunk mely országok a legbarátiabbak a Facebook közösségi oldallal kapcsolatban, milyen nyelven lehet elérni a Föld bizonyos régióinak az információit, honnan indulnak ki a közösségi oldalakon folyó lázadások vagy félrevezetési kampányok egy kormánnyal vagy intézménnyel szemben.

A kibertér lenne egyszerre mindez: emberek, adatok és számítógépek hálózata – és egyre inkább elterjedő mobil eszközök hálózata (telefonok, tabletek és hamarosan hűtőszekrények, karkötők, sportcipők…); információs tér, területhez nem kötött információcsere, amelyet nehéz megérteni. Fizikai területre épített materiális infrastruktúrából áll, ide értve a világűrben megtalálható műholdakat is. A felhasználó és céljai szerint tehát a kibertér jelenthet egy fizikai infrastruktúrát vagy teljesen más fogalmat.

A geopolitika egy létfontosságú eszközt nyújt a kibertér megértéséhez: az ábrázolásokat. Ezen ábrák konstrukciók, gondolkodásmódok, a geopolitikában szereplő eszmék együttesének többé-kevésbé logikus és koherens halmaza. Az objektív tényekre alapozza a megfigyeléseit, megőrizvén mélyen szubjektív jellegét. Az ábrák nem semlegesek: befolyásolhatják a szereplők stratégiáit, hogy meggyőzzék, felbujtsák, lelkesítsék, mobilizálják a további szereplőket (akik lehetnek a választópolgárok, az aktivisták, a befektetők, a haderők vagy az internet felhasználók…).

Gyarmatosítás a kibertérben

A kibertér nem egy földrajzi értelembe vett terület, azaz „térség, amelyen egy emberi csoport él, és amelyet kollektív tulajdonának tekint" (Lacoste, 2003), vagy az államok szempontjából ítélve „határokkal körbezárt térség, amelyen az állam kifejti a jogkörét" (Lacoste, 2003). Olyan térnek tekinthetjük, amelyben az emberek érintkeznek, de még földrajzi területnek is feltűntethető, mint ahogy Alix Desforges a virtuális teret ábrázolta a cikkében.

A kibertér fogalma paradox módon két teljesen ellentétes okból született meg. Először a sci-fi író, William Gibson (1984) írt az elektronikusan generált, „végtelen kuszaság" háromdimenziós teréről, amelybe a szereplők számítógéphez csatlakozva lépnek be. Mentálisan megjeleníti az egész emberiség informatikai rendszereinek szívében elraktározott információit és adatait, amelyet az internet felhasználók generációja fog birtokolni.

Ez a megjelenítés lázba hozta az internet úttörőinek képzeletét. 1990-ben meg is alkották az Electronic Frontier Foundation-t (EFF), jóval azelőtt, hogy az internet a nagy közönség színe elé került volna. Az alapítvány neve a „ha-

tárvidékre" és vadnyugatra hivatkozik, amely Frederick Jackson Turner történész elmélete szerint az amerikai demokrácia bölcsője. John Perry Barlow, alapító tag, 1996-ban még a virtuális tér függetlenségi nyilatkozatát is megfogalmazza, amelyben kijelenti, hogy a kibertérnek saját szuverenitása van, illetve, hogy az „intellektualitás civilizációjában" a világ kormányainak törvényei nem alkalmazhatóak. Alix Desforges szerint az 1960-as évek kulturális forradalma inspirálta a hálózat felépítését a nyitottság, az önirányítás, a szabad információcsere és szólásszabadság jegyében. Erősen decentralizált, központ nélküli, hogy az információ szabadon tudjon áramlani, bármilyen akadály ellenére is. Olyan világ ez, ahol minden, ami az emberi elmétől származik „újratermelhető és terjeszthető anélkül, hogy pénzbe kerülne". A szabadság szele folyamatosan lelkesíti a hacktivistákat, hogy harcoljanak minden olyan próbálkozással szemben, ami a szabad információáramlást gátolná az interneten.

Egy ideig elhanyagolták a koncepciót, de a virtuális tér újból előkerül a 2000-es évektől kiindulva. Az államok vitáikban úgy állítják be, mint olyan terület, amelyet meg kell hódítani, ellenőrizni, felügyelet alatt tartani és birtokolni. Terület, amelynek tiszteletben kell tartani a határait, a szuverenitását és törvényeit. Legfőképpen azonban a nemzetbiztonság elleni fenyegetésként és a nemzeti érdekek célpontjaként látták.

A 2007-ben Észtország ellen indított támadások sokként érték a kormányokat, köztük Franciaországot is. A kormányok felismerték, hogy mennyire le vannak maradva az ilyen fenyegetések kivédésében A tallini szovjet hősi emlékmű eltávolítása nagy port kavart fel. A kormányoldalak, a nemzetbiztonsági szervek, de a bankok és más közszolgáltatásokat is ért a masszív szolgáltatásmegtagadással járó támadás (DDoS) zajlott le. Több tízezer zombi számítógép hálózata, vagyis botnetek árasztották el egyszerre az ország hálózatait, amíg teljesen le nem bénították őket (fekete képernyő). Ezek a botnetek vírussal megfertőzött gépek, amelyeket sokszor a felhasználók tudta nélkül irányítanak. A támadással napokon át megfosztották a lakosokat az online közszolgáltatásoktól. Az orosz kormány tagadott minden felelősséget, még ha a technikai és politikai nyomok Oroszország felé mutattak is. Az azt követő évben a Grúziát ért kibertámadás ugyancsak megmutatta, hogy egy ilyen jellegű csapás milyen módon is tudja segíteni a konvencionális erőket

egy fegyveres konfliktus során. Azóta több ország, köztük Franciaország is, megerősítette kapacitását és próbálta ellenőrizni, illetve növelni hatalmát a kibertérben.

Stéphan Dossénál, a francia védelmi minisztérium köztisztviselőjénél tisztábban nem is fogalmazhatnánk: „Úgy tűnhetett, hogy az államoknak fel kellett húzniuk a zászlót a kibertérben, amit elfoglalnak, és ahol szuverenitásukat gyakorolják, hogy a szűzföldeket gyarmatosítsák és felkészüljenek egy esetleges támadásra" (Dossé, 2010). A 2013-as biztonsági fehér könyv tisztán kijelenti, hogy a kibertér stratégiai prioritás és a kiberfegyverek az arzenál részét képezik.

Kibertér: Az államok ellentámadása

Kevés állam látta előre, hogy milyen stratégiai tétje lesz az információs és kommunikációs rendszerek gyors növekedésének és interkonnekciójának. Stratégiai szinten csak Oroszország, Kína, illetve az Egyesült Államok reagáltak hamar. Oroszország és Kína történelmükből fakadóan is ismerik az információ fontosságát, míg az Egyesült Államok a technológiai fejlődés élvonalán jár. Az innováció kezdetileg az okosan reagáló egyének és kis vállalkozó csoportok kezében volt. Ők tudták a legjobban kihasználni az új, és alig szabályozott médiumok adta lehetőségeket. Nekik köszönhetjük azokat a kiváló eredményeket, amelyek radikálisan megváltoztatták életvitelünket (szórakozás, kollektív finanszírozás, aktivizmus, marketing…), és így eddig elképzelhetetlen lehetőségeket tártak fel. Ám ugyanígy hackerek, bűnözők és bérencek is gyorsan, hatékonyan ki tudták használni ezeket az eszközöket. Az utóbbiak tevékenysége idézte elő a politikai hatalom és intézmények jelenlegi reakcióját. Bruce Schneier információbiztonsági szakértő kiválóan rátapint arra, hogy a kibertér konfliktusai a disztributív hatalom (aktivisták, disszidensek, hackerek és bűnözők), illetve a hatalom hagyományos birtokosai (kormányok, nagyvállalatok, intézmények) között alakultak ki[5]. Megmutatja, hogy kezdetben a rendszer hozzáférhetősége és decentralizációja a kis szereplőknek kedvezett – ideértve a rosszindulatú szereplőket is. Látszólag

5 „The battle for power on the Internet: Bruce Schneier TEDxCambridge 2013" a TEDxTalks által publikált videó 2013.09.25. –letöltve 2013.02.16 (www.youtube.com)

legyőzhetetlenné tette őket az a hatékonyság és koordinációs kapacitás, amit a rendszer nyújtott. Azonban a hagyományos szereplők a stratégiai téthez mérhető nagy eltökéltséggel állnak bosszút.

A biztonság nevében

Szuverenitásuk megvédésének érdekében az államok teljes erőbedobással térnek vissza a kibertérbe. A kibertámadások megállításának nehézségei kihathatnak a nemzetbiztonsági és a területvédelmi kapacitásaikra. Leginkább a létfontosságú infrastruktúra védelmét hangsúlyozzák, hiszen azoknak bármilyen jellegű megzavarása vagy szabotálása a civil lakosságot is veszélyeztetheti. Ez a fenyegetés szítja a legbaljósabb diskurzusokat is. Azon vitáznak a szakértők, hogy egy kibertámadás milliók halálát és államok bukását is okozhatja, még ha ez egy kis valószínűségű és be nem bizonyított, de ki nem zárható lehetőség. Olivier Kempf rámutat arra, hogy a terrorizmus és a kibertér közötti kapcsolat nem is olyan egyértelmű, mint ahogy azt feltételeznénk a domináns véleményekből. Rodrigo Nieto Gomez elemezte a kiberterrorista amerikai ábrázolásának konstrukcióját és szerepét a biztonságpolitikában. Ez az ábrázolás általában kriminalizálja a hackereket és ösztönzi a titoktartást ott, ahol az innovációnak pedig hatalmas ereje lenne. Ezzel elrejtik, hogy valójában mit is jelenthetne a terrorizmus a kibertérben.

A terroristatetteken kívül kritikus fontosságú az információ kézben tartása. Az információ gyűjtése, elemzése, manipulálása stratégiai előnyt jelent az ellenséggel szemben és megingathatja bizalmát saját információjának megbízhatóságában. A kibertámadások megzavarhatják az ellenség kommunikációját, és hatással lehetnek műveleteire, hiszen a koordináció egyre jobban alapszik a hálózatokon. A klasszikus elrettentő és biztonsági stratégiák nehézségekbe ütköznek, mert bonyolult kideríteni a támadások mögött állók kilétét és a támadások miértjét. Ugyanígy megnehezíti a klasszikus stratégiák bevetését az, hogy a technológia olcsó és könnyen elérhető, ezzel felerősítve a kis szereplőket a nagyhatalmakkal szemben. Azok az országok, amelyek leginkább függnek a hálózatoktól ugyanígy a legsebezhetőbbek a támadásokkal szemben. Ám az is valószínűbb, hogy fejlesztik hálózataik

védelmét, offenzív kapacitásukat, illetve kihasználják a hálózatok adta lehetőségeket, hogy növeljék erejüket és hatékonyságukat.

Az ideológiai harc a közösségi oldalakon is folytatódik. A demokráciában a kormányok nem hagyhatják figyelmen kívül az ellenzéket és a közvéleményt. Viszont, még a nagyhatalmak sincsenek felkészülve azokra az online „csomagokra", amelyet a dzihadisták tesznek elérhetővé, hogy gyorsan radikalizáljanak egyéneket, és egyénre szabott terrorista praktikákat ajánljanak.

Másrészt a belbiztonság és közrend megtartását kihívás elé állítja az a szervezett vagy szervezetlen bűnözés, amely a hálón található. Ez lehet illegális behatolás, adatlopás és megsemmisítés, illetve bármilyen bűnözői tevékenység a hálókon (bankrablás, csalás, személyazonossággal való visszaélés stb.). Az azonosítást nehezíti a bizonyítékok volatilitása. Gyors közbenjárás hiányában a bűnjelek eltűnhetnek a képernyőkről. A távtevékenység pedig tovább bonyolítja a nyomozást, a gyanúsított letartóztatását és bíróság elé állítását. A bűnözés könnyedén áthidalhatja a határokat a hálózatokon keresztül, ami nem igaz a rendfenntartókra. Ha a bűnöző és az áldozat egy országban találhatók, a hatóságok gyorsan tudnak cselekedni. Viszont amikor a bűnöző, az áldozat, és/vagy a hálózat különböző országokban találhatók, nemzetközi együttműködésre van szükség mind a rendfenntartók, a rendőrség és a bíróságok részéről, amelyek sokszor túl lassúak ahhoz, hogy hatékonyan lépjenek közbe. Igazságszolgáltatási határok szelik fel a kiberteret, és a rendőrség csak hivatalos engedéllyel léphet be, még ha csak a bűnözőt kívánja elfogni.

A kiberbiztonság dilemmái arra késztetik a kormányokat, hogy aktívan figyeljék a kibertér történéseit, ezzel kockáztatva, hogy az egyéni szabadságjogokat megsértik, ahogy azt a Snowden-ügy is felfedte. Az önkényuralmi rendszerek számára a kibertér megfigyelése és ellenőrzése létfontosságú a rendszer megőrzésének érdekében, mert a legnagyobb fenyegetés számukra belülről jön. A nagymennyiségű információmozgás gyengítheti az önkényuralmi rendszereket, ám ez az információ ugyanígy nagy szerepet játszik a disszidensek és más fekete bárányok felismerésében. Fréderick Douzet Kínáról szóló cikkében bemutatja, hogy eddig a rezsim kreatívan tudta venni az új kihívásokat.

A szuverenitás kihívásai

Bertrand de La Chapelle, az Internet et Juridiction (Internet és Igazságszolgáltatás) projekt alapítója egy interjúban említette meg, hogy a szuverenitás gyakorlása mennyivel bonyolultabbá vált az államok számára, mivel a joghatásköri korlátok kibogozhatatlanok a kibertérben. A kibertérben a tevékenységek túlmennek a határokon, és az állam már nem tudja érvényesíteni a törvényeit és jogszabályait. Ez akár saját területén, saját polgáraival is megtörténhet, ha éppen egy külföldi vállalkozás nyújtja a szolgáltatást. A jogkör a kibertérben gyakran a hatalmi versengések terméke, semmint konszenzuális. A visszatérő konfliktusok egyike a szólásszabadságot érinti. Franciaországban hozott szigorítások például elképzelhetetlenek az Egyesült Államok jogi keretein belül. 2012-ben antiszemita kommenteket posztoltak franciául egy, a Twitter-en indított, élményítő viccversenyen a (zsargonban hashtagként mondott) #UnBonJuif („Egy jó zsidó"). Ez hosszú huzavonához vezetett a francia igazságszolgáltatás és az amerikai cég között. Csak tíz hónapos per után fogadta el a Twitter, hogy kiadja azokat az adatokat, amelyek lehetővé tették a posztolók beazonosítását. Az internet nagyvállalatai – a híres GAFA (Google, Amazon, Facebook, Apple) oly mértékű gazdasági befolyást szereztek, amellyel hatalmi játszmába szállhatnak. Nem könnyen vetik alá magukat egy olyan állam igazságszolgáltatásának, amely az általuk tárolt tartalom eltávolítását vagy a felhasználóik adatainak kiszolgáltatását írja elő. Ez az önkényuralmi rendszerek esetében a felhasználók védelmének szempontjából előnyös lehet, de ezzel egy nyereséges piac elvesztését kockáztatja a vállalat.

Végül az államok gazdasági és pénzügyi szuverenitása kemény kihívások elé néz. A hálózatok jelentősen meggyorsították az árucikkek és a pénzügy forgalmát, amely megkönnyíti az adócsalást és a nemzetközi pénzügyi válságok elterjedését. Dominique Lacroix cikke többek között bemutatja, hogy az új domain nevekre jelentkező nagyvállalatok adóparadicsoma hol koncentrálódik. A Yahoo! tevékenységének átszervezése Európában Írországban történt (ahol a társasági adó 12,5%-os[6]), ami a vállalat különböző adóköteles

6 Összehasonlításképpen a kivetett társasági adó azon vállalatok esetében, amelyeknek a tőkéje kevesebb, mint 75%-ban magánszemélyek kezében van, 33,1% az összes nyereséget illetően. (impots.gouv.fr)

európai telephelyeinek áthelyezéséhez vezet. A hálózatok növelik az ipari kémkedés, a szellemi és ipari tulajdon vagy az üzleti titok ellopásának kockázatát és nagyságát. Danilo D'Elia elemzi ezeket a kockázatokat és megmutatja, hogy a geopolitikai konfliktusok milyen potenciált rejtenek. Túlmegy a nemzetek gazdasági és pénzügyi erején, olyan mértékben, hogy a magán szektor érdekei összekapcsolódnak a nemzeti érdekekkel és a vállalatok kiberbiztonsága nemzeti érdekké is válhat. Magától értetődik, hogy a kiberbiztonság piaca ugyanannyira érzékeny, mint amennyire virágzó, ami arra ösztönzi a kormányokat, hogy részt vegyenek benne.

Új fenyegetések?

Sok fenyegetés nem jelent újdonságot, de sokkal gyorsabban, erősebben, eddig nem tapasztalt mértékben terjednek a kibertérben. Legyen szó kínai hackerekről, akik nagymennyiségű információt lopnak el cégektől (a Mandiant beszámoló szerint), a 1,7 millió fájlról, amit Snowden adott le, a hihetetlen nagyságrendű adatról, amit az NBÜ gyűjtött össze vagy az Aramco 300000 számítógépéről, amiket egy csapásra szabotáltak 2012-ben; a következmények gyorsabbak, erősebbek és nagyobbak, mint amit eddig tapasztaltunk.

Néhány kihívás viszont a kibertér sajátja: beazonosítani és bebizonyítani a támadás forrását, előrelátni, megakadályozni, vagy megállítani a támadást; a szuverenitás és igazságszolgáltatás szövevényessége; a technológia gyors evolúciója és a hálózatok permanens rekonfigurációja, amelyeknek gyors és folyamatos adaptációra van szükségük; a kísérleti kiberfegyverek kifejlesztése; ezen fegyverek tesztelésének nehézségei; hatásainak kétségessége, hiszen sok függ az ellenfél kapacitásától; és végül a tény, hogy a legjobb támadások azok, amiket nem veszünk észre… Sokak szerint a kibertér új területe (vagy környezete) a hadászatnak, a szárazföld, tenger, víz és űr mellett. Ám a többivel ellentétben ez nem egy természetes környezet – minden, ami a kibertérben történik mesterséges – és így átíveli a többi közeget.

A stratégiának, amit az államok fejlesztettek ki, hogy megvédjék szuverenitásukat és maximalizálják hatalmukat a kibertérben, geopolitikai következményei vannak. Komoly kérdéseket vetnek fel, új fenyegetéseket kreálnak.

Miért tanulmányozzuk a kibertér geopolitikáját?

A kiberkonfliktusok technikai szálainak van mivel elbátortalanítani a polgárokat, illetve az emberi- és társadalomtudományok kutatóit. Nem véletlen-e vajon, hogy e kérdések hosszú ideig a szakértők kis csoportjának a kezében maradtak? Miért foglalkozunk velük mindezek ellenére? Mert ebben a világban szeretnénk élni. Mert az információs és kommunikációs rendszerek állandó jelleggel jelen vannak a mindennapi életünkben, és az ezzel kapcsolatban meghozott döntések érinteni fogják az életünk minden aspektusát. Mert számos hatalom anélkül fejlődött ki, hogy az ellenzékkel megvitatták volna a fékek és ellensúlyok rendszerét.

Egy fordulóponton vagyunk és sokan közülünk, beleértve választott képviselőinket, felfedezik azokat az eszközöket, programokat és politikát, melyeket a nagyvállalatok, a kormányok vagy a bűnözők fejlesztettek ki azért, hogy megvédjék az érdekeiket és maximalizálják a teljesítményüket, profitjukat a kibertérben. A régi stratégiai paradigmák és nemzetközi játékszabályok nem érvényesek, az újak még megírásra várnak. A technológiai fejlődés gyorsasága meghaladja egy új jogi keret kidolgozásnak vagy a törvények adaptációjának gyorsaságát. A partnerek közötti titoktartás kultúrája, a bizalomhiány lelassítják az erőfeszítéseket. Válaszút előtt állunk. Mindez kihatással lesz a jövőnkre. Három terület különösen megérdemli a figyelmünket.

Béke és kollektív biztonság

Az első probléma a béke és a kollektív biztonság kérdése. Ennek a számnak több cikke is mutatja, hogy a fenyegetettség mennyire is dominálja a jelenlegi vitákat. Különösen az Egyesült Államok irányvonala az, amelyet a vita és eszközök eszkaládólása jellemez, amelynek egyik motorja a Kína elleni versengés. A kínai kormány törvényes úton vagy illegálisan, minden információt összegyűjt, legyen az informatikai, ipari, gazdasági, politikai vagy hadászati. Ennek a stratégiának célja, hogy információs erőfölényt szerezzen az Egyesült Államokkal szemben, amely riasztó aggodalmat kelt a tengerentúlon.

Az előző két év folyamán a média rengeteg titkot tárt fel, szakértők kijelentéseket tettek, kongresszustagok és még maga a Fehér Ház is feltárták a kiberfenyegetések kockázatait, amelyek a nemzet biztonságát és jólétét veszélyeztetik. Egyre többen vádolják nyíltan Kínát. A nemzeti hírszerzési szolgálat igazgatója, Jim Clapper egy szenátusi bizottság előtt bejelentette, hogy a kiberfenyegetés azon a ponton van, hogy veszélyesebbé válhat a nemzetbiztonság számára, mint a terrorizmus.

Az általános szövetségi megszorítások ellenére a kibervédelem költségvetése 800 millió dollárral nőtt 2013-ban. A Kiberhadviselési Parancsnokságnak[7] pedig megszabták, hogy effektíve 900 főről 4900 főre kell, hogy nőjön az elkövetkező években. A Snowden-ügy rámutatott, hogy milyen agresszív információgyűjtési politikát folytatott az Egyesült Államok, még ha ez a többi nemzettel való együttműködés és az eddigi bizalom kárára is megy. James Lewis a politikát relatívnak látja, hiszen a kínaiak és oroszok számára ez nem volt meglepetés, és emiatt nem is fogják kétségbe vonni a nemzetközi tárgyalásokat. Továbbra sem erős a bizalom és több köztisztviselő is hangoztatja, hogy „a kibertérben nincsenek barátok".

Sokak szerint az Egyesült Államok fogja kezdeményezni az első kiberháborús hadműveletet, egy kísérleti támadást, amely a kényszerítő diplomácia és a fegyveres támadás közötti harmadik utat képviseli. David Sanger feltárta a New York Times-nak, hogy a Stuxnet nevű, az izraeli titkosszolgálattal együtt kidolgozott vírus hogyan támadta meg a Natanz centrifugáit, hogy ezzel is lelassítsák Irán nukleáris programját.

Az elmúlt két év információi és a nemrég tett bejelentések arra utalnak, hogy a kiberfegyverkezési verseny elkezdődött. Több ország is prioritásává tette a kiberbiztonságuk és kiberkapacitásuk növelését és fejlesztését. Franciaország és az Egyesült Királyság kijelentették 2013-ban, hogy offenzív kapacitásaikat növelni fogják. 2011-ben az Egyesült Államok, illetve 2013-ban Franciaország azt nyilatkozta, hogy egy nagy volumenű kibertámadás akár háborús tettnek is minősülhet, és fenntartják a jogot, hogy visszavágjanak. Az oroszok bírálják a kibertér militarizálását, miközben ők maguk is fejlesztik saját kapacitásukat.

7 A kiberműveletek és a NSA katonai egysége

Martin Libicki, a RAND vállalat kutatója és a kibertérbeli elrettentés úttörője cikkében arról írt, hogy a konfliktusok milyen szinten eszkalálódhatnak, ha a kibertámadásokra konvencionális módon válaszolunk. Véleménye szerint a károk kisebbek maradnak, ha a kibertérben zajlanak le, ami emiatt nyílván kevésbé elrettentő is. Oriane Barat-Ginies, nemzetközi jogi doktor ellenben a Tallinni Kézikönyvet író szakértők érveit hozza fel. Ez a kézikönyv különböző jogi javaslatok gyűjteménye, ami azt fejti ki, hogy a nemzetközi jog hogyan használható fel a kibertérben. E gyűjtemény szerint a jogszerű védekezés és konvencionális fegyverek használata kibertámadás esetén megengedett, hiszen az utóbbi fegyveres agressziónak minősül.

Az eszkalálódás kockázatát komolyan kell vennünk. Ahogy ezt a két cikk is mutatja, nincs semmilyen garancia arra, hogy egy, a kibertérben elkezdett konfliktus a kibertérben fog maradni. Nem ismerjük eléggé a kiberfegyverek járulékos veszteségét sem. Az amerikai köztisztviselők pedig bejelentették, hogy akár pontos csapásokat is indíthatnak a kibertérben, ami elég aggasztó.

Ebben a kontextusban a hidegháborúval való összevetések megsokszorozódnak. A *Foreign Policy*ban David Rothkopf még a *hűvös* háború ötletét is felveti, ami egy kicsit langyosabb és szerteágazóbb, mint a hidegháború: „A *hűvös* háború célja az, hogy folyamatosan tudjunk csapásokat mérni anélkül, hogy élesben folyna háború. Mindezzel kevésbé kívánatossá, sőt szükségtelenné teszi a forró háborút" [Rothkopf, 2013].

Vissza kell-e állítani a hidegháborús (vagy *hűvös* háborús) szövetségeket? Szabad-e továbbra is a nemzetközi kapcsolatok pesszimista jövőképében gondolkodnunk és nulla-összegű játéknak tekintenünk azt? Vagy ez egy lehetőség arra, hogy a kollektív biztonság keretein belül gondolkozzunk, ezzel belevonva a folyamatba olyan országokat, mint Kína és Oroszország? Eme két ország hajlandó együttműködni a nemzetközi szabályozások létrehozásában, még ha nagy nézőpontbeli különbségek is vannak, ahogy azt James Lewis is megemlítette. Martin Libicki cikke rámutatott, hogy stratégiai megfontolásokra lesz szükség ahhoz, hogy az eszkalálódást megelőzzük. A vita még távol áll a megoldástól.

A másik kérdés az, hogy a kollektív biztonság érdekében mégis milyen keretrendszert építünk ki. A közös európai biztonság- és védelmi politika létrehozása már nehéz volt, és a kibervédelemi politika meghatározása még

nehezebb. A kapacitások megosztása a szuverenitás elhagyásának tűnhet, mert a technológia az az érzékeny pont, amely egy állam erősségeit és gyengeségeit tárhatja fel. Jean-Loup Samaan és Vincent Joubert bemutatták, hogy az Európai Unió és a NATO ezeket a kérdéseket stratégiai prioritásaikba ágyazták és kezdeményező lépéseket tettek. De a szerepek és kompetenciák felosztása továbbra is tisztázatlan maradt, és jelenleg úgy tűnik, a két intézmény között alig van koordináció, és a szuverenitás béklyóin nehéz felülkerekedni. Ráadásul a szövetségesek között nagy kapacitásbeli különbségek vannak. Leginkább a fejlett technológiával rendelkező országok tulajdonítanak nagy fontosságot a nemzeti szuverenitásnak és ápolják kétoldalú kapcsolataikat ezen a területen, főleg az Egyesült Államokkal.

A transzatlanti vitát tovább bonyolítják a gazdasági kérdések. A Snowden-ügy fényt vetett arra, hogy az európai országok adataik kezelésében menynyire függnek a nagy amerikai vállalatoktól. Ezek az adatok így nyílván az Egyesült Államok kormányának is a fennhatósága alá kerülnek. Ugyanezt a függést vehetjük észre az eszközök esetében, amelynek fő alternatívája a szintén problematikus kínai eszközök. Sokan az európaiak naivitására tapintottak rá, akik azóta megkérdőjelezik szuverenitásuk megőrzésének lehetőségét a nyitott piacokon. Lehet-e az európai kiberbiztonságot fejleszteni függetlenül a kibervédelemtől? Mit tehet Európa a rendeleteken, technikai szabványokon és iparpolitikán keresztül a kiberbiztonság javítása érdekében? Milyen alternatíva létezik a kínai és amerikai felszerelésekre és eszközökre? A belföldi piacok túl korlátozottnak tűnnek ahhoz, hogy valóban versenyképesek maradjanak. Akkor hogyan tudjuk az államok közötti bizalmat növelni, közös politikai és ipari megoldásokat találni?

Ezek sürgető kérdések, mert a biztonsági fenyegetésen kívül, a digitális adatok halmaza nő és még nőni fog. Hogyan védjük meg őket? És kitől?

A demokrácia és az egyéni szabadságjogok

Egyre több személyes adat lesz elérhető az interneten, többé-kevésbé nyíltan. Az OPEN DATA-val (nyílt adatok) közadatok, az adminisztráció adatai elérhetők lesznek, új információs eszközöket és olyan átláthatóságot nyújtva,

amely a demokrácia működését javíthatná. Remélhetjük, hogy különösen Franciaország, ahol a publikus adatok kommunikációja még messze sem tökéletes, előnyben részesíti majd a nyitottság ezen mozgalmát. Azonban, a személyes adatok kriminális vagy véletlen jellegű közzététele felveti a nagyvállalatok és a kormányok belépésének a kérdését.

Ha van legalább egy dolog, amelyben mindenki egyetért Edward Snowden esetén az az, hogy elindított egy vitát, amelyre különben nem lett volna alkalom. Az informátorok, akik előzőleg megpróbálták felhívni a figyelmet az NBÜ tevékenységére, nem kaptak nagy visszhangot. Szükség volt egy világszintű eseményre azért, hogy a nagyközönség rádöbbenjen és politikai kérdéssé tegye ezt az ügyet. A 2001. szeptember 11-i terrortámadások már nem elegendőek a vita elleplezésére. A kérdés az lett, hogy hogyan lehet kibékíteni a demokráciát és a megfigyelést.

A demokratikus ellenőrzés folyamata ebben a témában a polgárok nagytöbbsége között ismeretlen – sőt még a képviselők esetében is – és láthatólag az Egyesült Államokban, a nagyon behatárolt procedúrák ellenére is (legalábbis papíron) diszfunkcionálisak. Ádáz jogi viták folynak arról, hogy a kormány túllépte a saját jogkörét és eltaposса az állampolgárok civil jogait. Még ha úgy tűnik, a beletörődés magával sodorta a francia reakciókat, a német közvélemény felbolydult. A Stasi emléke nem is olyan távoli… A titkokat gyakran követeli a hírszerzés azért, hogy megőrizzék a nyomozások hatékonyságát, azonban jelenlegi társadalmunkban egyre nehezebb megőrizni ezeket az információkat, még a kormány számára is. Snowdennek valószínűleg még sok versenytársa lesz.

A biztosítékok, a fékek és ellensúlyok (ki, mikor, hol és hogyan?), a megfigyelések kiértékelései (amit közpénzből fizetünk) nemcsak arra jók, hogy egyéni szabadságjogainkat és a demokrácia eszméit megőrizzük, hanem a megfigyelés törvényességét is megszabjuk.

A tét nagy horderejű. Az egészségügyi kartonunk, a politikai véleményünk, az iskolai eredményeink, a szexuális orientációnk, vásárlásaink, utazásaink, barátaink, barátaink barátai, a barátaink barátainak a barátai… Az összes információ és még több más nyomozás, egyeztetés tárgyát képezhetik, és egy ijesztően pontos profil kialakítása válik lehetővé. Sok információ ma már

elérhető és gyakran önszántukból adják ki a közösségi oldalak és blogok felhasználói.

A biztosítékok kérdése felvetődik a nagyvállalatok esetében is, amelyek nincsenek alávetve a demokratikus ellenőrzésnek, csak a törvényeknek és a kormányukkal való erőltetett együttműködésnek. Érdemes még megemlíteni, hogy az adatok kiaknázásából származó előnyök, amelyek elemzik az ízléseinket, memorizálják a választásainkat és testreszabott szolgáltatásokat javasolnak számunkra, sokszor a szabadságjogaink megsértésének kompromisszumával jár.

Ezek a viták hatalmas gazdasági problémákat tárnak fel. Stéphane Grumbach és Stéphane Frénot, az INRIA kutatóinak cikke megmutatja, hogy az adatok összegyűjtésének, keresztezésének, elemzésének és kiaknázásának képessége társadalmaink gazdasági motorjává vált. A nyílt-adatok piacán tagadhatatlan stratégiai előnyt jelent az amerikai vállalatoknak az online szolgáltatásokban elért dominanciájuk, amelyhez hozzákapcsolódik az adatfeldolgozás szakértelme, a technológiai know-how. Másrészt a szuverenitás kérdései és a Snowden-ügy tovább komplikálhatja a kereskedelmi megállapodásokról folyó tárgyalásokat. Ezeket mégsem fogjuk lényegesen megkérdőjelezni. A döntés az európaiak kezében van, akik – ellentétben néhány feltörekvő piaccal –, nem lettek internetes bajnokok.

Ezen kívül még felvetődik, hogy az európai tagállamok képesek-e politikai és gazdasági befolyást kovácsolni az internet óriásaival szemben. A személyes adatok védelmének reformja lehetővé tenné a mozaikszerű európai nemzeti törvénykezés harmonizálását, elősegítené a vállalatok mobilitását Európában, illetve megerősítené az állampolgárok jogainak védelmét. A törvény a személyes adatokat gyűjtő cégeket kötelezné, hogy azokat csak a felhasználók beleegyezésével gyűjtsék; megengedné a lehetőséget, hogy az adatokat törölni lehessen; illetve létrehozna egy ügynökséget, amely a pereket kezelné. A Snowden-ügy dacára a törvényjavaslat 2015-ben el lett napolva, amiért az amerikai nagyvállalatok különösen masszív lobbiját és a tagállamok komoly nézeteltéréseit okolhatjuk. A lehetőség széles tárháza áll előttünk…

Az internet jövője

Végezetül a nemzeti stratégiák is hozzájárulnak az internet kialakításához, amelyek szintén fontos kihívások. Dilma Rousseff, Brazília államfője a maszszív ellenőrzésről szóló információk feltárását követően (mobiltelefonját ideértve) kifejezte azon kívánságát, hogy leváljon a túlságosan amerikaissá vált (USA centrikus) internetről és egy, 2014 áprilisában tartandó csúcstalálkozó megrendezését javasolta az internet szabályozásáról Brazíliában. Bertrand de La Chapelle interjújában megemlíti ezt is mint kihívást. Ebert Mannes és Tim Maurer bemutatják, hogy a feltörekvő országok, ahol a netfelhasználók száma rohamosan növekszik, rosszul élik meg az amerikai fölényt, amely az internet architektúrájában, irányításában, a felszerelésekben, a szolgáltatásokban, a tartalomban és az adatok kezelésében lévő dominanciát takarja. Ezért saját befolyásukat növelő stratégiát fejlesztenek ki. A BRICS körülbelül húsz afrikai országgal van partneri kapcsolatban, és egy 32000 km hosszú tengeralatti kábel projektet indítottak el, amely összekötné Oroszországot, Kínát, Indiát, Dél-Afrikát, Brazíliát (BRICS) és az Egyesült Államokat. Ugyanakkor a BRICS-országok nem képeznek egy homogén csoportot és nem ugyanazokkal a demokratikus hagyományokkal rendelkeznek, mint ahogy Hannes Ebert és Tim Maurer cikke is mutatja.

Számos demokratikus állam aggódik az „internet balkanizációja" miatt. A hálózat fizikai és politikai szétaprózódása, kezdeti sikerének, szabad és nyílt szellemének elvesztését jelentené. Kína, Oroszország, Irán, Szaúd-Arábia, Észak-Korea stratégiákat alakítottak ki a hálózatuk ellenőrzésére, a fizikai infrastruktúrától a tartalom forgalmáig. Kevin Limonier cikke nagyon jól bemutatja az Oroszország által készített ábrákat és stratégiákat, amelyekkel megvédi a szuverén internet koncepcióját. A Telekommunikáció Nemzetközi Szövetségének berkeiben ezen országok az állami ellenőrzésű internet fejlesztését javasolják. Bertrand de La Chapelle szerint a nemzetközi tárgyalások rendszeresen két kritikus ponton akadnak el: a nyugati államok előrébb teszik az emberi szabadságjogok tiszteletét (szólásszabadság, információhoz jutás, a magánélet tiszteletben tartása), illetve a nem állami szereplők bevonását egy többszereplős kormányzási modellbe, míg Kína, Oroszország és más államok számára e kérdések kizárólag az államok szuverenitását illetik.

Az összekapcsolt gazdasági és politikai érdekeknek elég erősnek kell maradniuk, hogy az eddigi közös alapstruktúra ne legyen kérdéses.

Az NBÜ programjáról szóló titkos információk, az olyan feltörekvő demokratikus országok felemelkedése, mint Brazília és India, és az Icann erőfeszítései, hogy figyelembe vegyék a regionális követeléseket, már mozgatják a szálakat. Tét az internet jövője. Hogyan lehet helyet csinálni minden nemzet számára és kialakítani egy elegendően biztonságos környezetet, mindezzel megtartva a hálózatok szabad és nyitott mivoltát?

Zárószó

A kibertér egy időben vált a szereplők közötti hatalmi versengés kérdésévé, az összeütközés színterévé és a geopolitikai konfliktusok kegyetlen fegyverévé. A kibertérért és a kibertérben folyó harcok nem különíthetők el a klasszikus geopolitikai hatalmi versengéstől. Ezek ellenben egy új módja és dimenziója a geopolitikának, amely minden szinten és több skálán van jelen.

A kibertér geopolitikai kihívásai diszkréten keveredtek a politikai, gazdasági, szociális és kulturális meggondolásokkal. A többlépcsős és transzdiszciplináris jellege megnyitja az informatika, sőt még a matematika előtt is, és ezzel lehetővé teszi a geopolitika kérdéseinek elemzését egész komplexitásukban.

A viták technikai dimenziója kétségtelenül különös erőfeszítést igényel az olvasó számára. De megéri a fáradtságot. Mivel nemcsak a kibertér hatalmi és biztonsági kérdéseiről van szó, hanem azon értékekről is, amelyeket mint demokratikus nemzet megvédünk. Olyan értékek, amelyek szeretnénk, ha irányítanák az általunk épített világot.

Felhasznált irodalom

CATTARUZZA A. et DOUZET F. (2013), « Le cyberespace au cœur de tensions géopolitiques internationales», DSI, hors-série n°32.

DESFORGES A. (2013), « Les frontières du cyberspace», in DOUZET F. et GlBLIN B. (dir.), Des frontières indépassables?, Armand Colin. Paris.

DOSSÉ S. (2010), «Vers une stratégie de milieu pour préparer les conflits dans le cyberes¬pace? », DSI, n°59. mai.

DOUZET F. (1997), « Internet géopolitise le monde », Hérodote, n° 86/87. p. 222-233.

–, (2007), «Les frontières chinoises de l'Internet», Hérodote, n° 125, p. 127-142.

L'Internet Corporation for Assigned Nantes and Numbers (Icann) est l'organisation qui coordonne le système d'addresses Internet et de noms de domaine (<www.icann.org>).

–, (2013), «Chine. États-Unis: la course aux cyberarmes a commencé». Sécurité globale, n°23.

–, (2013), «Chine: cyberstratégie, l'art de la guerre revisité». Diploweb, 12 septembre (<www.diploweb.com>)

GIBSON W. (1984), Neuromancer, Ace, New Jersey.

KE\1 PF O. (2012), Introduction à la cyberestratégie, Economica, Paris.

LACOSTE Y. (dir.) (1993), Dictionnaire de géopolitique, Flammarion, Paris.

LACOSTE Y. (2003), De la géopolitique aux paysages, dictionnaire de la géographie, Armand Colin, Paris.

MATTELART A. (2009), Histoire de l'utopie planétaire. De la cité prophétique à la société globale, La Découverte, Paris.

MCLUHAN M. (1964), Understanding Media. The Extensions of a Man, McGraw-Hill. New York.

MUSSO P. (2003), Critique des réseaux, PUF, Paris.

ROTHKOPF D. (2013), «The cool war», Foreign Policy, 20 février.

SANGER D. (2013), « In cyberspace, new cold war», New York Times, 24 février.

VlRlLlO P. (1997), « Un monde surexposé », Le Monde diplomatique, août.