

Analogikus gondolkodás a kibertérről

jelige: WAY 258

lezárás dátuma: 2014. november 14.

Tartalomjegyzék

Rövidítések jegyzéke	3
Bevezetés	5
Cyber-Hype és digitális apokalipszis	9
<i>Miért nem folyik kiberháború?</i>	<i>10</i>
Katonai analógiák – a kiberhatalom természete	15
<i>Tengeri hatalom vs. Kiberhatalom</i>	<i>15</i>
<i>Légi hatalom vs. Kiberhatalom</i>	<i>16</i>
<i>Szárazföldi hatalom vs. Kiberhatalom.....</i>	<i>16</i>
<i>Nukleáris hatalom vs. Kiberhatalom</i>	<i>17</i>
<i>Új hidegháború a kibertérben?</i>	<i>19</i>
A kibertér mint globális közjószág	20
<i>Mit tegyünk a kalózok ellen?</i>	<i>21</i>
Mit tanít az élővilág?	23
<i>A vírus-analógia</i>	<i>23</i>
<i>A kibertér mint ökoszisztéma</i>	<i>24</i>
A kibertér mint társadalmi tér.....	26
Befejezés	29
Felhasznált irodalom.....	31

Rövidítések jegyzéke

ACTA	Anti-Counterfeiting Trade Agreement Hamisítás elleni kereskedelmi megállapodás
APTs	Advanced Persistent Threats Fejlett állandó fenyegetések
CIA+R	Confidentiality, Integrity, Availability + Resilience Bizalmasság, Sértetlenség, Rendelkezésre Állás + Rugalmasság
CNO	Computer Network Operations Számítógép-hálózati hadviselés
CNA	Computer Network Attack Számítógép-hálózati támadás
CND	Computer Network Defence Számítógép-hálózati védelem
CNE	Computer Network Exploitation Számítógép-hálózati felderítés
DoS Attack	Denial of Service Attack Túlterheléses támadás
DDoS Attack	Distributed Denial of Service Attack Elosztott túlterheléses támadás
ISP	Internet Service Provider Internetszolgáltató
PIPA	PROTECT IP Act Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act A gazdasági kreativitást és szellemi tulajdont fenyegető valós online fenyegetések megelőzéséről szóló törvény

SCADA

Supervisory Control and Data Aquisition

Felügyeleti, vezérlő- és adatgyűjtő rendszer

SOPA

Stop Online Piracy Act

Online kalózkodás elleni törvény

Bevezetés

Az analógiák jelentésátvitelen alapuló nyelvi eszközök. Lényegük, hogy két egyedi helyzetet elsősorban intuitív módon összekapcsolva rávilágítanak a köztük lévő hasonlóságokra. Az analógiák olyan gondolatmankók, melyek megkönnyítik a minket érő információk kognitív elrendezését, leegyszerűsítés révén gyorsítják az információfeldolgozást. Ebből a szempontból egyrészt meglehetősen hasznosak, ugyanakkor jelentős kockázatokat is rejtnek magukban. Két szituáció megfeleltetése egymásnak sosem lehet tökéletes, a leegyszerűsítés következtében elkerülhetetlen az információvesztés, sőt, előfordul, hogy két analógnak tekintett esetet alaposabban megvizsgálva kiderül, hogy azok csupán a felszínen hasonlítanak egymáshoz, lényegüket tekintve eltérők (Marton, 2013:39-42). A Gadamer és Wittgenstein gondolataiból kinőtt „nyelvi fordulat” nyomán és a posztmodern filozófiának a társadalomtudományok területére történő betörésével az analógiák mellett érdemes szólni a metaforák természetéről is. A fogalmi metaforák¹ az analógiák egy speciális, különlegesen erős fajtájának tekinthetők, melyek a kognitivisták nyelvészeti képviselői szerint tükrözik az ember megismerési és gondolkodási folyamatait. E felfogás szerint a kommunikáció során használt metaforák határozzák meg, hogy egy jelenségről hogyan gondolkodunk (Bańcerowski, 1999).

Analógiák és metaforák a döntéshozatali folyamatok során gyakran komoly politikaformáló erővel bírnak, sokszor találkozunk velük akadémiai vitákban, sőt, a mindennapi gondolkodásunkat is átszövik, így alaposabb vizsgálatuk önmagában is hasznos. Minél jobban ismerjük az általunk használt analógiákat, annál kevésbé valószínű, hogy a téves következtetés hibájába esünk. A kibertér, mely immár több évtizedes múltra tekint vissza, ha nem is teljesen új, de meglehetősen kevésbé ismert és értett jelenségnek számít, politikai, társadalmi és technológiai szempontból egyaránt. Ennek oka részben a technológiai fejlődés sebességében és az ebből fakadó hatásokban, részben pedig a megfelelően képzett – a technikai, társadalomtudományi és politikai oldalt egyaránt ismerő – szakértők hiányában keresendő. Mint minden új és ismeretlen jelenségnél, a kibertérrel kapcsolatban is adódik, hogy analógiák és metaforák segítségével fogjunk hozzá a megismeréshez. A témát övező diskurzus ennek megfelelően bővelkedik ezekben. A dolgozat célja, hogy bemutassa a kibertérrel kapcsolatos leggyakoribb analógiákat és metaforákat, valamint külön-külön

¹ Az irodalmi metaforákkal szemben kognitív módon értelmezett, a mindennapokat átszövő, az emberi gondolkodást jelentősen befolyásoló fogalmi metaforák („conceptual metaphors”) elméletét George Lakoff dolgozta ki.

értékelje ezek erősségeit és gyengéit. Az elemzés azt kívánja megvilágítani, hogy az analógiák hogyan járultak hozzá a kiberbiztonsági kérdések egy részének buzáni értelemben vett túlbiztonságiasításához. Amellett is állást foglalunk, hogy a kiberbiztonság katonai dimenzióját teljes joggal uraló katonai terminológiának a teljes diskurzusra történő áttérjedése káros következményekkel jár a társadalmi és politikai dimenzióban, de olykor még magában a katonában is. A dolgozat egyúttal a nem állami szereplők kiberbiztonsági diskurzuson keresztül való vizsgálatának fontosságára és a jelenleginél jóval erősebb társadalmi megközelítés szükségességére is fel kívánja hívni a figyelmet.

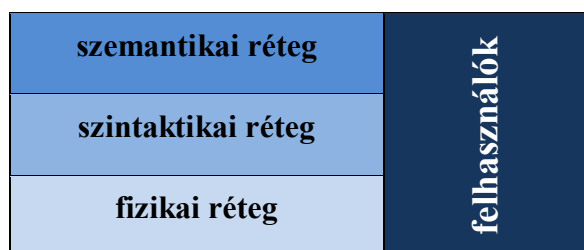
A különböző nyelvi eszközök hiányos ismerete és inkonzisztens használata okozója és folyamatos fenntartója a kibertérről való gondolkodást uraló definíciós káosznak és a rengeteg fogalomzavarnak. Az alábbi oldalakon az analógiák befolyásoló erejét hangsúlyozva igyekszünk támpontot adni a definíciós dzsungelben való eligazodáshoz.² Ezt nemcsak azért kívánjuk megtenni, hogy a leggyakoribb hasonlatokat összegyűjtjük, hanem azért is, hogy minden esetben hangsúlyozzuk, hogy mit NE értsünk bele az adott analógiába.

Az elemzés Martin Libicki kibertér-definíciójának kibővített változatára épít. Libicki a kibertér az egymásra épülő fizikai, szintaktikai és szemantikai rétegek rendszereként definiálta (Libicki, 2009:12-13). A fizikai réteg a fizikai térben létező infrastruktúrát, számítógépeket, áramköröket, vezetékeket, vezeték nélküli jeladókat stb. foglalja magában. A kibertér fizikai infrastruktúra nélkül nem létezhet. A szintaktikai réteg azokat az utasításokat (programokat, protokollokat, stb.) jelenti, amelyek alapján a gépek egymással és a felhasználóval kommunikálnak. A szemantikai réteg alatt magát a kibertérben tárolt, továbbított, és előállított információt értjük. Libicki definícióját szükségesnek látjuk bővíteni egy negyedik réteggel, a felhasználók rétegével. Ez a réteg nem az előző háromra épül rá, hanem átfogja azokat. A felhasználó képes a kibertér mind a négy rétegével interakcióba lépni. A szakirodalom nagy része a fizikai, szintaktikai és szemantikai rétegekkel folytatott interakciókra koncentrál. A fizikai kapacitások elégtelensége, a szintaktikai sebezhetőség, vagy a kibertérben tárolt információ megbízhatóságának kérdése egyértelműen biztonsági kérdésnek tekinthető, melyeket jellemzően ártó szándékú felhasználók fenyegetnek.³ A felhasználók egymás közötti interakciója ugyanakkor legalább annyira fontos eleme a kibertérnek, mint az előzőek, ha nem éppen az a legfontosabb. Jelentőségéhez mérten azonban

² Folyamatban van egy kibertérrel kapcsolatos definíciós adatbázis felépítése az Open Technology Institute keretei között. Az adatbázis elérhető a <http://cyberdefinitions.newamerica.org/> oldalon.

³ Számítógépes hálózatok természetesen támadhatók kinetikus módon is, fenyegetésükhöz nem szükséges a kibertér felhasználójának lenni.

meglehetősen kevés figyelmet kap ez az aspektus. A felhasználói réteg beillesztése a kibertér definíciójába messzemenő következményekkel jár. Először is, a definíció bővítése segíti a kiberbiztonság, információbiztonság és hálózatbiztonság fogalmi elkülönítését. Másrészt, a felhasználók kategóriáját felbontva a kiberbiztonsági elemzés fókuszába beemelhetővé válnak az egyének, csoportok, különböző nem állami szereplők, és államok, illetve ezek egymás közti interakciója. A tág definíció segítségével lehetővé válik egy sor, elsősorban társadalomtudományi kérdés megfelelő vizsgálata az Anonymustól kezdve az al-Kaida szervezeti struktúrájának átalakulásán vagy az Iszlám Állam rekrutációs és propagandamódszerein át a több százmillió Facebook-felhasználó által teremtett új típusú szociális tér természetéig. A definíció kiszélesítése elősegítheti, hogy a kiberbiztonsági kérdésekre a hadtudomány és a stratégiai tanulmányok művelői mellett a nemzetközi tanulmányok, a szociológia, a politikatudomány és más társadalomtudományok képviselőinek figyelme is ráirányuljon (Liff, 2013). Mindennek következtében a nemzetközi rendszer alapvető, hatalomeloszlásra vonatkozó kérdései is könnyebben vizsgálhatóvá válnak. Nem mellékesen azért, mert a hatalom diffúziója szorosan kapcsolódik a globális számítógépes hálózatok létrejöttéhez (Nye, 2010).



**A kibertér felépítése Libicki definíciójának
kibővítésével**

A definíció kiszélesítésének azonban megvannak a kockázatai is. A felhasználóknak a kibertér részeként való kezelése magában hordja a „kiber” és a „valós” tér összemosásának a veszélyét. Noha a dolgozat mellett érvel, hogy a kettő nem különíthető el élesen, sőt, a kibertérben történő események (beleértve a felhasználók kognitív folyamatait és annak eredményeit) legalább annyira valósak, mint bármi a fizikai világban, azt mindenképp szükséges leszögezni, hogy a kibertér semmiképpen sem tekinthető hagyományos értelemben vett térnek. A definíció kitágítása azzal a módszertani következménnyel járhat, hogy kénytelenek leszünk minden olyan biztonsági kérdést kiberbiztonsági kérdésként kezelni, aminek távolról vagy közelről valamilyen kapcsolata van a számítógépes hálózatokhoz. Ez felszínre hozza a kérdést, hogy a „kiber” előtag milyen hozzáadott értéket képvisel a vitában,

egyúttal potenciálisan azzal is fenyeget, hogy a kiberbiztonsági kutatás fókuszát veszti. A tág definíció veszélyeinek szem előtt tartása mellett mégis arra az álláspontra helyezkedünk, hogy a kibertérrel összefüggő jelenségeket társadalmi kontextusban kell vizsgálni, elvégre a hacktivizmustól a (kiber)háborúig a társadalmi valóságban gyökerező jelenségekről, társadalmi cselekvésről van szó.

A dolgozat nem kíván pontot tenni a definíciós viták végére, csupán arra próbál rávilágítani, hogy ezek a nézeteltérések nem pusztán politikai megfontolásokat tükröznek, hanem mélyebben, az adott társadalom kultúrájában, nyelvhasználatában gyökereznek.

Cyber-Hype és digitális apokalipszis

„Cyberwar is Coming!” – hirdeti Arquilla és Ronfeldt sok tekintetben meghatározó tanulmányának címe 1993-ból (Arquilla, Ronfeldt, 1993). „Könnyedén egy kibertámadás lehet a következő Pearl Harbor”⁴ – ezek a szavak Leon Panetta, akkori CIA igazgató szájából hangzottak el 2011 februárjában az amerikai Kongresszus előtt. 2012 végén a fiatalabb Bush elnöksége alatt a nemzeti hírszerzés igazgatójaként (Director of National Intelligence) tevékenykedő Mike McConnell arra figyelmeztetett, hogy az Egyesült Államok nem várhat a World Trade Center összeomlásának kibertérben lezajló megfelelőjére⁵ (Rid, 2013a). 2011-ben a Department of Homeland Security újságírókat utaztatott az Idahói Nemzeti Laboratóriumba, hogy bemutassák egy négy évvel korábbi titkos kísérlet felvételeit, amely során számítógépes támadások révén rongáltak meg egy generátort, valamint hogy élőben is szimuláljanak egy vegyipari komplexum elleni kibertámadást (Singer, Friedman, 2014). A The Economist 2010. júliusi számának borítóját egy nagyváros feletti gombafelhő és a vaskos cím – „Cyberwar” díszítette. Magyarországon 2010-ben jelent meg a hazai kiberbiztonsági szakirodalom sarokkövének számító Digitális Mohács tanulmány (Kovács, Krasznay, 2010). Az ezekhez hasonló példákat még hosszan sorolhatnánk. A közös bennük, hogy – akár tartalmuktól függetlenül is – olyan analógiákra építenek, amelyek a kibertér biztonságiasításának irányába hatnak. Ez a törekvés a kibertérből érkező objektív fenyegetések mértékét tekintve érthető és helyénvaló, vagy legalábbis az volt. A kiberbiztonsági szakértőknek a terület felemelkedésével párhuzamosan azzal a szomorú ténnyel kellett szembenézniük, hogy sem az átlagpolgár, sem a politikai döntéshozó nem érti a kibertér működését, hatásait. A „kiber” sokáig az informatikusok, technikai szakértők világának számított (sok tekintetben még ma is annak számít), olyan területnek, amit a digitális bevándorlók és a digitális analfabéták nemzedéke (gondoljunk a vezető politikusok átlagéletkorára akár Magyarországon, akár máshol) nagyon nehezen ért meg. Ilyen kontextusban a szakma természetes módon fordult érzelmekre ható, túlzó analógiákhoz. A biztonságiasítás egyre több beszédaktuson keresztül, egyre komolyabb egzisztenciális fenyegetést lefestve, és egyre több forrást, különleges jogkört és új szervezeteket igényelve zajlott le és zajlik ma is. A folyamat mára oda vezetett, hogy kijelenthetjük, sok tekintetben átestünk a ló túlsó oldalára.

⁴ „the next Pearl Harbor could very well be a cyberattack” (fordítás a szerzőtől)

⁵ „[the US could not] wait for the cyber equivalent of the collapse of the World Trade Centers.” (fordítás a szerzőtől)

A Pearl Harbor, 9/11, és Mohács analógiák azt a feltételezést hordozzák magukban, hogy az ország területét jelentős mértékű erő fenyegeti, amellyel szemben katonai képességek felsorakoztatása szükséges. Nem is kellett hozzá sok idő, hogy a kibertérrel kapcsolatos diskurzuson eluralkodjon a katonai nyelvezet. A kiberháború, kibertámadás, kibervédelem olyan fogalmakká váltak, amelyeket egy kiberbiztonsági elemzés ritkán nélkülöz. A katonai fogalmak használata úgy is a militarizálás irányába befolyásolja a politikusok és az állampolgárok gondolkodását, hogy a katonaság ténylegesen ennél jóval szofisztikáltabb szakzsargonnal dolgozik. Rid szavait használva, a kibertér militarizálása valóban nem történt meg, a kibertérről folytatott diskurzus militarizálása azonban régen befejeződött (Rid, 2013a).

Miért nem folyik kiberháború?

Clausewitz meghatározása szerint a háború erőszak alkalmazása annak érdekében, hogy ellenfelünket saját akartunk teljesítésére kényszerítsük. Ezt kiegészítve a háború instrumentális jellegére vonatkozó megállapításokkal, a clausewitzi definíció három elemét különíthetjük el: az erőszakot, a háború politikai természetét, és magát az instrumentalitást. Ennek a definíciónak a mai napig egyetlen kibertérben elkövetett cselekmény sem felel meg. A „legerőszakosabb” kibertámadást az Urengoj-Szurgut-Cseljabinszk gázvezeték 1982-es felrobbanása jelenti.⁶ A történet szerint a Szibériát átszelő gázvezeték működtetéséhez szükséges vezérlőrendszert (SCADA-rendszert) a Szovjetunió önmaga nem volt képes előállítani, külső piacokon kellett beszerezni azt. A CIA az alkalmat megragadva az oroszok által Kanadától megvásárolt szoftverbe károkozásra képes kódot juttatott, mely a rendszer beüzemelését követően a vezeték egyik oldalát lezárva, a másik oldalán a nyomást megnövelve nagy erejű robbanást idézett elő. (Clarke, Knake, 2010:93-94). A robbanás megtörténte azonban kérdéses, halálos áldozatairól pedig nincsenek megbízható információk.⁷ Az orosz példánál ismertebb esetnek számítanak 2007-ből az észti események és az Izrael Szíria elleni légicsapását kísérő kiberműveletek, 2008-ból az orosz-grúz háború alatt tapasztalt kibertérbeli összecsapások, 2009-ből az Egyesült Államokat és Dél-Koreát érő támadások, 2010-ből pedig a STUXNET vírus alkalmazása Irán ellen. Ezeket az eseteket egyaránt szokás kiberháború címkével illetni, ugyanakkor az erőszak hiánya miatt egyikük sem felel meg a háború definíciójának.

⁶ A történet hitelességével kapcsolatban vannak kétségek.

⁷ Egyes értesülések több mint 70 halálos áldozatról szólnak.

Thomas Rid a kibertámadások kategorizálására a következő modellt javasolja (Rid, 2012). A kibertámadások széles spektrumának egyik végén a politikai dimenziót nélkülöző bűncselekmények helyezkednek el.⁸ Ezek többsége haszonszerzési céllal történik, az adathalászat révén ellopott hitelkártya-adatoktól a célzottan megvalósított ipari kémkedésig. A spektrum másik végén a háború fenti definíciójának megfelelő, emberéletek kioltásával, nagymértékű fizikai pusztítással járó politikai céllal elkövetett erőszakos cselekmények találhatók. Ezek joggal hívhatók kiberháborúnak. A kettő közötti szürke zónába olyan cselekmények esnek, melyeket politikai bűncselekményként kategorizálhatunk. A felforgatás, kémkedés és szabotázs cselekményét különíthetjük el, melyeket az egyes államok jogrendje jellemzően büntetőjogi kategóriákként ismer el, ugyanakkor államellenes jellegük és az elkövetésükben más államok gyakori közvetlen vagy közvetett érintettsége kiemeli őket a köztörvényesnek tekinthető bűncselekmények közül. A sokszor kiberháborúként aposztrofált cselekmények közül az Észtország elleni elosztott túlterheléses támadás (DDoS) és a grúz-orosz háborút kísérő műveletek a felforgatás, az orosz gázvezeték és a natanzi nukleáris létesítmény elleni támadások a szabotázs kategóriájába esnek. Kétség kívül súlyos cselekményekről van szó, ugyanakkor azt is látni kell, hogy sem ilyen jellegű esetek miatt, sem pedig kémkedés miatt nem szoktak az államok háborút indítani. Izrael 2007-ben az Operation Orchard művelet keretében számítógépes eszközökkel vakította meg a szíriai légvédelmet, ezzel lehetővé téve, hogy vadászgépei biztonságosan berepüljenek Szíria légterébe és lebombázzanak egy épülő nukleáris létesítményt. A CNA művelet egyértelműen kritikus módon járult hozzá a fizikai pusztítás kivitelezéséhez és emberéletek kioltásához, természetét tekintve politikai és instrumentális volt, tehát meggyőző érvek szólnak amellett, hogy kiberháborúként aposztrofáljuk. Ugyanakkor az akciót egy nagyobb katonai művelet integráns részének kell tekintenünk, és kijelenthetjük, hogy önmagában nem minősült volna háborús cselekménynek.⁹

Az tehát, hogy mit tekintünk a kibertérben elkövetett háborús cselekménynek, az alkalmazott erőszak mértékétől függ. Ez visszavisz minket ahhoz a Hannah Arendt által feszegetett kérdéshez, hogy mit értünk erőszak alatt, hogy különböztetjük meg az erőtől, a hatalomtól,

⁸ A kategória a különböző bűncselekmények súlyossága és az elkövetés módjának szofisztikáltsága szerint tovább bontható, de analízisünk szempontjából ezt nem célszerű megtennünk.

⁹ Ez felveti a kérdést, hogy nemzetközi jogi szempontból gyakorolható-e elhárító önvédelem egy ilyen jellegű kibertámadás észlelésekor, de még a vadászgépek megjelenése előtt. A preemptív önvédelem gyakorlása hagyományos esetekben is mindig rendkívül vitatott kérdés, ezt a kiberfegyverek megjelenése tovább komplikálja. Értékelésünk szerint egy ilyen jellegű kibertámadás indikatív körülmény, és mindenképpen erősíti az önvédelem gyakorlásának jogosságát, noha önmagában nem alapozza meg azt.

agressziótól és más hasonló fogalmaktól¹⁰ (Arendt, 1973:87; idézi Stone, 2013). A dolgot tovább bonyolítja – ha már a clausewitzi definícióval dolgozunk – hogy a porosz hadtudós által használt „Gewalt” egyaránt fordítható erőként, erőszakként, hatalomként és kontrollként. Clausewitz ugyan egyértelművé teszi, hogy a „fizikai erőt” érti alatta, ugyanakkor a definíció tisztánlátást ez még nem teszi könnyűvé. Mint ahogy az sem, hogy a „szabotázs” és a „háborús cselekmény” nem kölcsönösen kizáró fogalmak, egy adott művelet könnyedén beleeshet egyszerre mindkét kategóriába (Stone, 2013). Meggyőző érvek szólnak amellett, hogy a STUXNET esetében is erről van szó. A kibertéren keresztül kétség kívül jelentős pusztítás okozható, emberéletek olthatók ki. Nagyon is lehetséges a kibertéren keresztül háborút vívni. Ugyanakkor a kibertérben végrehajtott erőszak a „hagyományos” erőszakhoz képest csakis közvetett lehet, annál az egyszerű oknál fogva, hogy egy számítógépes vírus önmagában soha nem lesz képes embert ölni (Rid, 2013b). Végso soron, amit biztosan kijelenthetünk, az pusztán annyi, hogy a kibertér határozottan ellenáll az egyértelmű kategorizálás kísérleteinek. Ez a tény azonban semmiképpen sem indokolja a háborús analógiák folyamatos használatát, hiszen láttuk, hogy a legtöbb kibertérben elkövetett cselekmény nem, vagy csak vitatható módon tekinthető háborús cselekménynek.

Érdemes egy rövid pillantást vetnünk arra is, hogy a kibertérben zajló folyamatok milyen hatással lehetnek a hagyományos háborúk kitörésére. Liff négy hipotézisét vizsgálva mi is arra a következtetésre jutunk, hogy a kiberfegyverek megjelenése nem, vagy csak kis mértékben növeli a hagyományos háborúk kitörésének esélyét (Liff, 2012). Liff első hipotézise szerint a hagyományos fegyveres konfliktusok kitörésének valószínűsége a kiberfegyverek aszimmetrikus jellege miatt növekedhet. A kibertéren keresztül más fegyverekhez képest viszonylag olcsón okozható pusztítás, ráadásul minél fejlettebb technológiailag egy társadalom, működése minél inkább függ az internettől, annál sebezhetőbbé válik. Ez az aszimmetria az államok közti katonai hatalom eloszlását egyenlőbbé teszi, és háborúk kirombantására sarkallhat olyan államokat, amelyek jelentős erőfölénnyel szemben ezt nem tennék meg. A feltételezés helyességét ugyanakkor erősen megkérdőjelezi, hogy a kiberfegyverek korántsem olcsók,¹¹ az eszkalációs dominanciát a hagyományos fegyverek terén előnyt élvező államok képesek fenntartani (azaz képesek kibertámadásra hagyományos fegyverekkel válaszolni), valamint, hogy háborúk pusztán a

¹⁰ Az angol nyelv még változatosabb ebből a szempontból, a „power”, „strenght”, „force”, „authority”, „violence” és „agression” fogalmak részben átfedik egymást, az egyértelmű distinkció közöttük szinte lehetetlen.

¹¹ A STUXNET sikeréhez többek között például rendkívüli mértékű hírszerzési munkára és a vírus fizikai tesztelésére volt szükség a natanzi urándúsító centrifugák pontos másán.

kibertéren keresztül nem nyerhetők meg. A második hipotézis szerint a kibertéren keresztül elkövetett támadások tagadhatósága, a betudhatóság problémája védettséget biztosít a támadó számára, ezért növeli annak az esélyét, hogy az anonimitás miatt a megtorlás elkerülésében reménykedő szereplők támadást indítsanak. A probléma ezzel kapcsolatban akkor jelentkezik, ha ezekre a tevékenységekre háborúként próbálunk tekinteni. Egy háborúban ugyanis akaratunknak az ellenfélre való kényszerítése érdekében elengedhetetlen, hogy ellenfelünk tisztában legyen azzal, hogy kik vagyunk és mi az akaratunk. Liff harmadik hipotézise a támadás és védelem egyensúlyának előbbi javára való felborulása miatt jósolja a hagyományos háborúk kitörésének gyakoribbá válását. Ezzel kapcsolatban ugyanakkor kérdéses, hogy ellenséges államok a kibertérből érkező potenciális fenyegetés miatt próbálják meg hagyományos fegyverekkel döntésre vinni a dolgot. Ez a megállapítás Liff negyedik hipotézisében is visszaköszön, ami szerint a kibertérben rendkívül nehezzé válik az elrettentés és ez a konfliktusok sűrűsödéséhez vezet. Az elrettentést részben pont az eskalációs dominancia képességét kísérő akarat hiteles demonstrálása teszi nehezzé. Ez visszavezethető a betudhatósági problémára, illetve arra, hogy nehéz társadalmi támogatást találni egy olyan háború megvívásához, ahol az ellenfél kilétében sem lehetünk biztosak. Az elrettentést a nem állami szereplők jelenléte még nehezebbé teszi. Liff konklúziója, hogy az államközi háborúk kitörésének esélye a kiberfegyverek megjelenésével nem növekszik radikálisan, ezeknek az eszközöknek a szerepe a tágabban vett politikai alkufolyamatokban jelentősebb.

A kibertér túlbiztonságiasításának oka, hogy szinte az összes releváns szereplő magára nézve hasznosnak tekinti a folyamatot, így annak fenntartásában érdekelt. A probléma a rövid és a hosszú távú célok ellentmondásából fakad. A „cyber-hype” fenntartása és gerjesztése az akadémiai szféra számára figyelmet, a média számára eladott példányokat, a politikusok számára új ellenségképet, az állami szervezetek számára költségvetési forrást, a kiberbiztonsági vállalatok számára pedig egy rendkívül gyorsan bővülő gazdasági szektort jelent.

A hosszú távú hatásai a folyamatnak azonban rendkívül károsak. A nyugati országok védelmi költségvetéseinek általános csökkenő tendenciája ellenére a kiberképességek fejlesztésére évről évre több pénz jut. A jelenséget kihasználva egyre elterjedtebbé vált, hogy egy program finanszírozásának fenntartása érdekében, a program elé a „kiber” előtagot illesztve és a kibertérrel való akármilyen távoli vagy nem létező kapcsolatot megtalálva újracsomagolják azt, így a politikai döntéshozó könnyebben meggyőzhetővé válik, torz erőforrás-allokációt eredményezve (Lee, Rid, 2014). Ez a torzítás nemcsak a költségvetési források tekintetében

jelenik meg, hanem az emberi erőforrások tekintetében is. A megnövekedett biztonsági igény a kibervédelemért felelős szervezeteket megnövekedett nyomás alá helyezi. Ez az eredménykényszer a növekvő források ellenére, de részben a torz elosztás következtében, a kibertérrel kapcsolatos tevékenység kiszervezéséhez vezet. A haderőknek, állami szervezeteknek nincs ideje arra, hogy saját, magasan képzett szakértői gárdát neveljenek ki, így különböző nem állami szereplőkhöz fordulnak. A katonai magánvállalatok alkalmazása háborúban erősen vitatott kérdésnek számít, míg a hackerek állami felbérése lassan normává növi ki magát. A túlbiztonságiasítás a teljesítmény szempontjából az outputra és nem az inputra helyezi a hangsúlyt, ami hosszútávon nehezíti megfelelő, állami alkalmazásban álló szakértők kinevelését (Thomas, 2014). A túlbiztonságiasítás a gazdasági szektorban is érezteti a hatását. A folyamatos és kivédhetetlennek vélt fenyegetések, „*a hacker mindig átjut a védelmen*”¹² mentalitás következtében a fogyasztók belenyugodtak, hogy a tűzfalak, vírusvédelmi programok és számítástechnikai eszközök gyártói nem tudnak 100%-os biztonságot garantálni, így el sem várják azt. A kiberbiztonsági cégek értékét ráadásul nem az objektív teljesítmény, hanem ez ezzel sok esetben igencsak laza kapcsolatban álló reputáció adja. Számos nagy értékű akvizíciónak lehettünk tanúi a közelmúltban, ahol a felvásárolt vállalat és a felvásárló egyaránt profitált a kiberbiztonsági kockázatokat övező felhajtásból.¹³ A hatalmas összegek és a percepció által hajtott folyamat felveti egy kiberbiztonsági buborék kialakulásának lehetőségét (Lee, Rid, 2014). Ez a jelenség ráadásul kiemelten érdekeltté teszi ezeket a cégeket olyan „incidensleíró” jelentések publikálásban, melyek független szereplők általi verifikációja szinte lehetetlen (Guitton, 2013). Ezek a jelentések kétségkívül sok hasznos információval szolgálhatnak, ráadásul az állami szervezeteknek sok esetben nincs meg a kapacitása ilyenek készítésére, mégis érdemes ezeket megfelelő forráskritikai fenntartásokkal kezelni. Végül azt is érdemes kiemelni, hogy a „hype” rombolja a felhasználók, sőt, az államok közti bizalmat. Az internet alapvetően bizalomra épülve született meg, és ma is számos funkció alapvető feltétele a bizalom. Ezt a bizalmat épp elég komoly mértékben fenyegetik az objektív módon jelenlévő veszélyek, nem szükséges felnagyítani azokat. A folyamatos kiberháború érzete kihat az államközi kapcsolatokra is, felesleges súrlódásokat eredményezve. Kína és az Egyesült Államok kapcsolatát egyre jobban terhelik a kibertér körüli ellentétek és vádaskodások, amik sok esetben társadalmi percepciókból és nem objektív tényekből fakadnak.

¹² Stanley Baldwinnek a stratégiai bombázással kapcsolatban elhíresült mondata alapján, mely így hangzott „The bomber will always get through”

¹³ Ilyen volt például a Sourcelfire felvásárlás a Cisco által 2,7 milliárd dollárért, a Mandiant felvásárlása a FireEye által 1 milliárd dollárért vagy a Cyvera felvásárlása a Palo Alto Networks által 200 millió dollárért.

Katonai analógiák – a kiberhatalom természete

Ebben a fejezetben négy, rendszeresen visszatérő analógiát vizsgálunk meg. Ezek az analógiák a kiberhatalom (*cyber power*) jellegének értelmezését igyekeznek segíteni a hadtudományi irodalomból átvett jelenségekkel való összehasonlítás útján. A tengeri, légi, szárazföldi és nukleáris hatalommal összevetve a következtetésünk, hogy az összehasonlításokból vonhatók le értékes tanulságok a kibertér természetére vonatkozóan, de teljes mértékben egyik összehasonlítás sem állja meg a helyét, sőt, sok esetben a különbségek több mindent elárulnak, mint a hasonlóságok. Egyúttal annak a veszélyére is szeretnénk emlékeztetni, hogy a kibertér pusztán katonai szemlélete elvonja a figyelmet a politikai és társadalmi vonatkozásokról.

Tengeri hatalom vs. Kiberhatalom

A tengeri hatalom lényegét a tengereken és óceánokon megvívott csaták megnyerésének, a tengeri fojtópontok és hajózási útvonalak ellenőrzésének és a szárazföldre történő erőketvitítésnek a képességeként foglalhatjuk össze. Alfred Thayer Mahan az 19. század végén a tengeri hatalom koncepcióját olyan új találmányok fényében fogalmazta meg, mint a gőzhajó, a hajópáncél és a nagy hatótávolságú hajóágyú. A tengerek és a kibertér közti hasonlóságot sokan kiemelték már, hatalmas, szinte végtelen és kontrollálhatatlan területként lefestve mindkettőt. A görög eredetű „kiber” szó jelentése is a hajózás, navigálás cselekményét jelenti, azaz olyan mozgásra utal, melyet az irányok tekintetében nagy szabadságot élvezve tehetünk meg. A fojtópontként szolgáló tengeri szorosok és hajózási útvonalak párjaként tekinthetünk a nagy internetszolgáltatók infrastruktúráira, a gerinchálózatokra, a nagysebességű adatforgalmat lebonyolítani képes üvegszál optikai kábelekre és ezek csatlakozási pontjaira.

A hasonlóság azonban ennél tovább nemigen terjed. A kibertér egy teljes mértékben ember alkotta tér. Minden eleme a fizikai infrastruktúrától a felhasználókig valamely állam szuverén fennhatósága alá esik. A kibertér ráadásul változékony, folyamatosan bővül, egyes részei egy kapcsoló átállításával leválaszthatók (Betz, 2012). A kibertér és a tengerek közti legnagyobb különbséget pedig a hatalomgyakorlás belépési költségei (*entry cost*) jelentik. A tengeri platformok jellemzően a legdrágább eszközök egy haderő eszköztárában, míg a kibertérben való megjelenéshez elegendő egy számítógép és egy internetkapcsolat. Ennek következtében a kiber- és a tengeri környezet szereplői számukban és differenciáltságukban jelentősen

eltérnek. Noha az egyes államok kiberképességei közt jelentős eltérések vannak, egyetlen állam sem képes a kibertérre olyan értelemben dominálni, mint a tengereket (Nye, 2010).

Légi hatalom vs. Kiberhatalom

A légi hatalom egyik legnagyobb stratégiai előnyének és egyben legnagyobb veszélyének az ellenséges vonalak mögé való könnyű bejutás lehetőségét tartják. A légi hatalom teoretikusai kiemelik a légierő azon képességét, hogy nagyon rövid időn belül harcérrintkezésbe bocsátkozzon az ellenséggel, akár stratégiai célpontok támadása révén, és ezt a harcérrintkezést szükség esetén gyorsan képes legyen megszakítani is. Ami igaz a légierőre e téren, az hatványozottan igaz a kiberhadviselésre. A szó szerint fénysebességgel végrehajtott, akár a polgári infrastruktúrát célzó támadások lehetősége kétség kívül vonzó hasonlóságot jelent. Fentebb utaltunk Stanley Baldwin szavaira és a „hacker” és „bomber” szavak felcserélhetőségére.

A precíziós fegyverek megjelenésével a légi hatalom az öbölháború óta jelentős vonzerőre tett szert. A légierőről a közvélemény és a politikusok hajlamosak azt feltételezni, hogy lehetséges általa a saját erők veszélyeztetése nélkül és a civil áldozatok elkerülése mellett konfliktusokat eldönteni (Cohen, 1994). Ez a feltételezés gyakran a kibertérrel kapcsolatban is megfogalmazódik. A hasonlóság azonban sokkal kevésbé meggyőző, mint az elsőre tűnik. A tengeri hatalomhoz hasonlóan a légi hatalom megszerzése is igen költséges vállalkozás, a szereplőkre vonatkozó megállapításaink ebben az esetben is érvényesek. A légtér ráadásul homogén térnek tekinthető, ami a kibertérrel nehezen mondható el. A légi hatalommal kapcsolatos analógia inkább csak negatív irányból állja a meg helyét. Mindkét esetben olyan, új technológiák által meghódított térről van szó, melynek uralásától olyan stratégiai előnyöket várnak egyesek, amik egész egyszerűen nem realizálhatók. A levegőnél nehezebb repülőgépek elterjedése a kibertér expanziójához hasonlóan a túlbiztonságiasítás jelenségét és sok esetben alaptalan félelmeket hozott magával.

Szárazföldi hatalom vs. Kiberhatalom

A tengeri és légi hatalomhoz képest több hasonlóságot találhatunk a szárazföldi hatalommal (*land power*) való összevetés során. Ezek a hasonlóságok kiváltképp három dimenzióban jelennek meg: a jelenlévő szereplők számában, az alacsony belépési költségben, valamint a rejtőzködés lehetőségében (Nye, 2010). A tengeri és légi hadszíntérhez képest a szárazföldön és a kibertérben a dominancia megszerzése jóval nehezebb. A kibertérben kidomborodik a

hadviselés aszimmetrikus jellege. Minél inkább dominálni akarja valaki a kiberteret és minél inkább ki akarja használni a benne rejlő lehetőségeket, annál inkább függővé válik tőle és annál több támadási felületet teremt. A hálózatközpontú hadviselést folytató haderők olyan nem állami szereplők tömegével találják szemben magukat, akik habár fölényt nem tudnak kivívni maguk számára, képesek lehetnek hosszútávon felkelés jellegű magatartással kifárasztani egy államot. A kibertérben ráadásul rendkívüli módon összemosódik az állami és civil szereplők köre, olyan kérdéseket felvetve, hogy tehet-e ellenlépéseket egy állam egy másik állam állampolgárai ellen, például olyan esetben, mikor azok akár tudtukon kívül (pl. egy botnet részeként) részt vesznek az adott állam elleni támadásban. Legalább ekkora problémát jelent a civilek tudatos bekapcsolódása a háborús konfliktusokba. A kibertér a felderíthetetlenség és sebezhetetlenség illúzióját kínálva hazafias érzelmű állampolgárok tömegeit ösztönzi arra, hogy ezeket az érzelmeiket gyakorlatba átfordítva részt vegyenek államközi konfliktusokban. Ezek a szereplők ugyanakkor a saját államuk hivatalos szervei által is nehezen kontrollálhatók, adott esetben egy válság szükségtelen eskalációját okozhatják, a hadműveletekben való részvételük pedig felveti a hadijog szerinti támadhatóságukat (Lattmann, 2014). Ezek a személyek a kombattánsok és nem-kombattánsok közé szorulva könnyen egy jogi szürke zónában találhatják magukat, ahol egyfelől katonai célpontnak minősülhetnek, másfelől nem lesznek jogosultak a kombattáns státusszal járó védelemre, mivel annak ilyen drasztikus kiterjesztése ellentétben áll a harcokban ténylegesen érintett katonák lehető legnagyobb fokú védelmének kívánalmával. Állami szemszögből nézve, a kibertérben végzett tevékenységek során kiemelt módon figyelemmel kell lenni a lehetséges társadalmi, politikai és gazdasági hatásokra és meg kell sokszorozni a nem szándékolt következmények kiszűrésére tett erőfeszítéseket, ezek bekövetkeztének valószínűsége ugyanis rendkívül magas.

Nukleáris hatalom vs. Kiberhatalom

A kibertérben végrehajtott támadások ellen rendkívül nehéz védekezni. Egyrészt a támadások olyan sebességgel zajlanak le, amellyel nem automatizált reakció nem veheti fel a versenyt, másrészt a támadások sokszor korábban nem ismert sebezhetőséget kihasználva, úgynevezett „nulladik napi támadásként”¹⁴ jelentkeznek, harmadrészt pedig a kibertér annyira átszövi a mindennapjainkat, hogy rajta keresztül egyetlen támadással lehetséges milliók életét

¹⁴ A szárazföldi hadviseléssel való párhuzamba állítást gyengíti ez a megállapítás: a kibertérben az alapos felderítőmunkának köszönhetően a támadó sokszor jobban ismeri a megtámadott rendszert, annak gyengeségeit, mint a rendszer tulajdonosa maga.

befolyásolni. A védekezés és támadás egyensúlyának radikális felborulása adja a nukleáris fegyverekkel való összehasonlítás alapját.

Ez a párhuzam azonban sok szempontból sántít. A kibertéren keresztül közvetett módon okozható erőszak mértéke össze sem hasonlítható egy atomháború pusztító erejével. A kiberfegyverek a tömegpusztító fegyverekkel (weapons of mass destruction) szemben inkább a tömeges rendbontás (weapons of mass disruption) eszközei. A nukleáris fegyverek rendkívül drága eszközök, kifejlesztésük nagyon sok időt és energiát igényel, jelenleg mindössze kilenc állam rendelkezik velük. Felügyeletük és a bevetésükről való rendelkezés a legszigorúbb állami kontrollt kívánja meg. A kibertérben ezzel szemben sokkal könnyebb szereplővé válni. A nukleáris fegyverek megjelenése a nagyhatalmak közti háború valószínűségét radikálisan lecsökkentette. Ahogy fentebb bemutattuk, a kiberfegyverek proliferációja az államközi konfliktusok gyakoriságára és jellegére nem gyakorol jelentős hatást. Bernard Brodie, a nukleáris stratégia kiemelkedő alakja 1946-os művének a „*The Absolute Weapon: Atomic Power and World Order*” címet adta. Az atombomba katonai bevetethetőségének hasznosságára Hiroshima és Nagaszaki kivételével szerencsére nem áll rendelkezésünkre empirikus adat, ennek ellenére a fegyver a hidegháború évtizedeinek politikai, katonapolitikai és társadalmi szempontból is meghatározó eleme volt. Ekkora hatást a kiberfegyverektől aligha várhatunk. Gyakran felmerül, hogy a nukleáris fegyverek használatát és terjedését korlátozó nemzetközi rezsim mintájára a kiberfegyverek esetében is szerződések megkötésével kéne garantálni a biztonságot. Habár születtek biztonság- és bizalomerősítő intézkedések multilaterális¹⁵ és bilaterális¹⁶ keretben is, és ezek ugyan pozitív eredménynek tekinthetők, a kibertérben a fegyverzetkorlátozás szinte lehetetlen vállalkozás. Nemcsak a számos definíciós probléma miatt, de a verifikáció lehetetlensége, a kettős felhasználású termékek problematikája miatt is, nem beszélve a politikai akadályokról. A robbanófejek száma és a ballisztikus rakéták hatótávolsága könnyebben mérhető, mint a botnetek mérete és egy kódsor veszélyessége.

¹⁵ Ilyen volt például 2013 decemberében az EBESZ Állandó Tanácsa által elfogadott dokumentum:
OSCE Confidence-Building Measures (CBMs) to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies

¹⁶ Erre példa az Oroszország és az Egyesült Államok közti párbeszéd az információs és kommunikációs technológiák biztonságáról.

Új hidegháború a kibertérben?

A hidegháborús összehasonlítás már nem katonai, hanem inkább politikai természetű. Brent Scowcroft¹⁷ 2011-ben a hidegháború és a kiberbiztonság „kísérteties hasonlóságáról” beszélt egy előadásában. A benyomásaival Scowcroft nem volt egyedül. David Ignatius amerikai újságíró a Pentagon hivatalnokaival folytatott interjúk után jelentetett meg cikket „Cold War feel on cybersecurity” címmel (Schachtman, Singer, 2011). A gazdasági szereplők közül a McAfee elnökhelyettese, Dmitri Alperovich szintén a hidegháború visszatérését látta megvalósulni a kibertérben (O’Connell, 2012). A hidegháborús analógia a tényleges katonai összecsapás nélküli, de politikai súrlódásokkal a végletekig terhelt helyzetre kíván rávilágítani, melyet ideológiai és technológiai verseny kísér. A hidegháború esetében két szuperhatalomról, egyértelmű pólusokról, hozzájuk szerződésekkal formálisan is kapcsolódó szövetségesekről, a két tábor fizikailag is szétválasztó vasfüggönyről és a harmadik világról, mint csatatérről beszélhetünk. A kibertér ezzel szemben nem néhány kormány, hanem többmilliárd felhasználó interakciója köré épül, akiknek a tevékenysége javarészt néhány ezer nagy internetszolgáltató (ISP) által működtetett infrastruktúrán, bizalomra épülve folyik, globálisan egyre nagyobb összefonódást eredményezve. (Schachtman, Singer, 2011). A hidegháború a hatalom nemzetközi koncentrációjának korszaka, ezzel szemben a kibertér a hatalom disztribúciójának jelképe. A hidegháborús hasonlat egy elemét azért érdemes kiemelnünk. Az amerikai döntéshozókon és a társadalmon az 1950-es évek második felétől a két szuperhatalom nukleáris képessége közötti vélt különbségek (missile gap) miatt eluralkodó hisztéria egészen hasonlatos a kibertérből érkező fenyegetések jelenlegi eltúlzásához. Mindkét esetben az objektív veszélyek felnagyítása figyelhető meg, több olyan szereplő által, akiknek az érdeke ezt kívánta meg.

¹⁷ Brent Scowcroft Gerald Ford és George H.W. Bush elnök alatt szolgált nemzetbiztonsági tanácsadóként.

A kibertér mint globális közjószág

Nem ritka az a vélekedés, amely a kibertér liberális és erősen normatív alapállásból a nemzetközi közjószágok sorába helyezi. A nemzetközi közjószágok olyan erőforrásokat jelentenek, melyek kiaknázása az emberiség egészének az érdekében kellene, hogy történjen. Hasznukból egyetlen szereplőt sem lehet kizárni, felhasználásukat pedig jellemzően kötelező erejű nemzetközi szerződésben megerősített normák szabályozzák. Ilyen nemzetközi közjózágnak tekinthetők mindenekelőtt a tengerek és óceánok. A tengerek szabadságának gondolata már Grotius idején megfogalmazódott és később számos alkalommal megerősítésre került, főként abból a megfontolásból, hogy a tengeri hajózás a kereskedelem és az emberek közti kapcsolattartás, a prosperitás megteremtésének az eszköze. Nemzetközi közjózágnak tekinthetjük az állami szuverenitás alatt nem álló tengerfenék erőforrásait, továbbá (többé vagy kevésbé elfogadott módon) az Antarktisz, a Naprendszerben található égitesteket, de felfogható közjózággént a biológiai sokféleség, a stabil nemzetközi pénzügyi rendszer, de akár a nemzetközi béke is. A közjószágok közös vonása, hogy kiaknázásuk érdekében minden szereplő egyformán érdekelt az együttműködés kialakításában és fenntartásában. A kibertér a tengerekhez hasonlóan – sőt azoknál jóval nagyobb mértékben – a gazdasági tevékenység és az emberek közti kapcsolattartás színtere, a globalizáció jelképe. Azonban nem szabad megfeledkeznünk arról, hogy a tengerekkel és a közjószágok többségével ellentétben a kibertér ember alkotta, végső soron emberek által birtokolt, fenntartott és fejlesztett közeg. A kibertér szereplői közt éles verseny folyik, legyenek azok államok, szolgáltatók, társadalmi mozgalmak, jóhiszemű felhasználók vagy a lehetőséget váró hackerek. Még nemzeti vagy regionális szinten sem beszélhetünk teljes együttműködésről. Az internetszolgáltatók által birtokolt infrastruktúrák a kommunikációs protokollokon keresztül fizetség, közös előnyök, vagy az állam kényszerítő erejének hatására – és nem az együttműködés kedvéért – kapcsolódnak össze. A kibertérben hemzsegek a rosszindulatú szereplők, a társadalmak sok kérdésben megosztottak,¹⁸ ráadásul az államok közti egyetértésről sem beszélhetünk (Demchak, 2012). A kibertérrel kapcsolatos kooperációt nemzeti szinten, sőt, pusztán az állami szervek között is meglehetősen nehéz megteremteni, nemzetközi szinten ez még nagyobb kihívás. Együttműködésre azonban szükség van, méghozzá olyanra, amely a számos érdekelt felet magában foglalja.

¹⁸ Például a szellemi tulajdon, a szólásszabadság mértéke vagy a személyiségi jogok védelme tekintetében.

Mit tegyünk a kalózkodás ellen?

A kalóztevékenység fogalma napjainkra annyira szerves részét képezi a kiberterről való gondolkodásunknak, hogy gyakran bele sem gondolunk a metafora eredetébe. A 16. század elejétől kezdve az Újvilág meghódításával egyre több hajó vágott neki az Atlanti-óceán átszelésének. Ahogy nőtt a tengerek gazdasági szerepe, úgy nőtt az ezt kihasználni vágyók száma. Az Amerika felfedezésétől a 19. század közepéig tevékenykedő kalózkodó kiváltképp hasznos párhuzamot szolgáltatnak, nemcsak egy káros jelenség leírása, hanem annak kezelése szempontjából is. Az összehasonlítás kimondottan a kalózkodás egy szegmensében találó: az államilag támogatott kalózkodás esetében. Az arannyal és ezüsttel megrakott hajók kifosztása és az értékes gazdasági titkok vagy szellemi tulajdon elektronikus úton történő ellopása közt a párhuzamot egyszerű észrevenni. A kalózkodótól és kibertérbeli megfelelőiktől nem idegen a kereskedelmi csatornák lezárása (a hajózási útvonalak veszélyeztetése vagy a blokádként felfogható DDoS támadás), de a gazdasági infrastruktúra vagy a katonai eszközök közvetlen támadása sem. A kalózkodó nyomás alá kerülve könnyedén zászlót cserélhetett vagy eltűnhettek a végtelen tengeren, a kibertérben a hackerek számára ugyanígy adott a lehetőség. Sir Francis Drake vagy Jean Fleury a brit és a francia korona szolgálatában álltak, de nem az ellenőrzése alatt. Az újkor kalózkodójának¹⁹ magatartása nem sokban különbözik az állami megbízásokra könnyen kapható „hazafias hackerek” vagy a nem teljesen legális munkákra szóló kormányzati szerződésekre vágyó cégek magatartásától. A kalózkodó katonai célokra való alkalmazása alapvető normának számított, gondoljunk a Nagy Armada pusztulására, vagy 1812-es brit-amerikai háborúban az utóbbiak oldalán résztvevő több mint 500 hajóra, ami annak fényében, hogy a hivatalos amerikai haditengerészet mindössze 23 hajóval rendelkezett, meglehetősen figyelemre méltó (Singer, Friedman, 2014). Nem egészen fél évszázaddal később az amerikai polgárháború során, 1862-ben Lincoln elnök mégis nemcsak visszautasította kalózkodó felbélését, de immorálisnak bélyegezte a Konföderáció vezetőit, amiért ők nem tettek ugyanígy. A kalózkodó-analógia hasznossága ezen ötven év eseményeinek megértésében rejlik. Ezalatt az idő alatt a kalózkodás támogatásában korábban érdekelt nemzetek felismerték, hogy már nem szolgálja gazdasági érdekeiket a jelenség. A britek felszámolták a kalózkodószármány elosztására szolgáló feketepiacot, a kalózkodóknak menedéket nyújtó kikötőket, mint Port Royal vagy Jamaica erővel kényszerítették együttműködésre, míg a kereskedelmi útvonalakat egyre több hadihajó kezdte védelmezni. Mindemellett erre az

¹⁹ Az angol nyelv megnevezésben is különbséget tesz a kizárólag saját szakállára dolgozó kalózkodó (pirate) és a szolgálatait az államnak fizetség fejében felajánló hajósok (privateer) között.

időszakra tehető a parti tenger feletti szuverenitás kialakulása és a hajózással kapcsolatos nemzetközi jogi normák megszilárdulása. A tengeri kalózkodás visszaszorítása egybeesett azzal, hogy az államok joghatóságot követeltek maguknak a tengerek felett. A szuverenitás kiterjesztésének azonban feltételévé vált a biztonság garantálása. A kialakuló normák és szokásjogi szabályok mellett a kalózkodást elítélő 1856-os párizsi deklarációval kötelező érvényű írásos szerződést is sikerült teremteni, melyet 42 állam (a nemzetközi rendszer szereplőinek nagy része) elfogadott (Shachtman, Singer, 2011). Az akkori jelenségeknek megtaláljuk a modern megfelelőit. Az interneten fellelhető fertőzött tartalom mindössze 50 internetszolgáltatóhoz köthető, a spameken keresztül hirdetett hamis gyógyszerek 95%-áért ugyanazon a három bankon keresztül fizethetünk világszerte és egy alkalommal egyetlen szerver leállításával a globálisan kiküldött levélszemét mennyisége egyik napról a másikra 70%-al csökkent (Singer, Friedman, 2014). Az ezen szereplők elleni fellépés csak szándék kérdése. A nemzetközi normákat tekintve hidegháborús logikájú fegyverzetkorlátozási egyezmények helyett sokkal kifizetődőbb a kibertérben való általános viselkedés és felelősségre vonás szabályainak megteremtésén dolgozni. Az ártó szándékkal fellépő nem állami szereplők már azoknak az államoknak a gazdaságát is kezdik megkárosítani, amelyek eddig elnézőbbek voltak velük szemben. A politikai akarat az államok részéről megtalálható. A kalózkodás elleni fellépés ráadásul a bizalmat is erősítené, ahogy erősítette az egyébként vetélkedő Egyesült Államok és Nagy-Britannia között a 19. században.

Mit tanít az élővilág?

A vírus-analógia

Mióta a kibertér biztonságos megteremtése felkerült az állami teendők listájára, az egyes államok számos eltérő (és eltérően sikeres) intézményi megoldással rukkoltak elő. A felállított (és jellemzően sokszor átalakított) struktúrák alapvető kérdése, hogy az egyes szervezetekhez – katonaság, titkosszolgálatok, polgári ügynökségek – milyen felelősségi területek és jogkörök, illetve milyen költségvetési források kerüljenek. Anélkül, hogy bármely állam intézményi megoldását értékelnénk, az alábbiakban a vírus-analógia segítségével egy szervezeti modell pozitívumait emeljük ki. Ez a modell az amerikai járványügyi központok (Centers for Disease Control and Prevention, CDC) modellje. A CDC története egy 7 fős munkacsoporttal és egy 10\$-os befektetéssel indult 1947-ben, amely mára egy 15,000 fős személyzetet foglalkoztató sikeres ügynökséggé nőtte ki magát. Tevékenysége felöleli az alap- és alkalmazott kutatást, az újonnan megjelenő fenyegetések előrejelzését, az információ megosztását minden olyan szereplő felé, akinek szüksége van rá, valamint adott esetben szükségkórházként is funkcionál. A CDC feladatai közé tartozik, hogy javaslatot tegyen a beavatkozásra, valamint koordinálja a megelőzési erőfeszítéseket. A vezetőit a kormányzat nevezi ki, de alkalmazottait egészen különböző szakterületekről válogatja. A CDC fizikailag az Egyesült Államok számos pontján jelen van (ezért a többes szám), ami nagyban megkönnyíti feladatainak ellátását. A szervezetnek ráadásul nemcsak a természetben előforduló vírusokkal, hanem ember alkotta fertőzésekkel, biológiai fegyverekkel kapcsolatban is van kompetenciája. Az Egyesült Államok közegészségügyi rendszerének központi eleme a felelősség megosztása. A CDC nem egyedüli szervként, hanem kórházakkal, kutatóközpontokkal, egyetemekkel, magáncégekkel, más kormányzati szervekkel és a WHO-val együttműködve, az együttműködés koordinátoraként végzi tevékenységét (Singer, Friedman, 2014).

A számítógépes vírusok és az emberi szervezetet fenyegető vírusok közt számos párhuzam állítható. Ahhoz, hogy egy társadalom egészségesnek mondhassa magát, szükséges, hogy tagjai tisztában legyenek az alapvető egészségügyi kockázatokkal, szükséges, hogy megfelelő oktatásban részesüljenek arról, hogy hogyan kerülhetik el ezeket. A fertőzés ellen a legjobb módszer a megelőzés, amelyet bizonyos esetekben szisztematikus módon (pl. a kötelező oltások beadásával gyermekkorban) nagy hatékonysággal végre lehet hajtani. A számítógépes

vírusok fertőzési, reprodukciós és evolúciós mechanizmusai meglehetősen hasonlóságot mutatnak a biológiai vírusokkal (Charney, 2010).

A CDC modelljének alkalmazása a kibertérben, illetve a kiberbiztonságnak közegészségügyi problémaként való keretezése számos előnnyel járna. Az államközi konfliktusok és militarizáció helyett az egyének, csoportok, gazdasági szereplők, államok és nemzetközi szervezetek közti együttműködés irányába tolná el a diskurzust. Az egyéni tudatosság, egyfajta „kiberhigiénia” megteremtése társadalmi szempontból is rendkívül fontos lenne. Az éttermekre, iskolákra, és közterekre (gondoljunk a dohányzás korlátozására) vonatkozó higiéniai és egészségügyi előírások az internethasználat esetében is követhető példát jelentenek. Az egészségügyi modell alkalmazása ráadásul a számítógépes hálózatokkal szembeni alapvető követelmények kialakítását is megkönnyíthetné. Ahogy a számítógépes hálózatok, úgy az emberi test is folyamatos támadásnak van kitéve. A támadások nagy részét immunrendszerünk első védelmi vonala könnyedén visszaveri, egy másik részét testünk külső segítség nélkül leküzdí, némely esetben szükség van külső beavatkozásra. Az emberi test és az immunrendszer működési sajátossága ugyanakkor az, hogy akármilyen támadás éri, testünk igyekszik a szervezet fő funkcióinak ellátását biztosítani. Számítógépes hálózatok esetében is az lenne a cél, hogy bármilyen biztonsági incidens ellenére a rendszer maga működőképes maradjon. A hálózatokkal szembeni elvárásokat a CIA modell segítségével szokták megfogalmazni. A betűszó a bizalmasság (confidentiality), az integritás (integrity), és az elérhetőség (availability) szavakat takarja. A közegészségügyi modell segítené azokat a törekvéseket, amelyek ennek rugalmassággal (resilience) való bővítését célozzák, elvégre a természet sem a leggyorsabbat, legerősebbet vagy legnagyobb jutalmazza, hanem a leggyorsabban alkalmazkodni képest (Betz, Stevens, 2013). Az állam szabályozó erejét mindeddig visszafogottan gyakorolta a kibertérben.

A kibertér mint ökoszisztéma

A vírusok és fertőzések mellett egy másik hasznos, természetben gyökerező analógiával találkozunk, ha a kibertér és a számítógépes hálózatokat az ökológia szemüvegén keresztül szemléljük. Egy vírus máshogy viselkedik szabadon a természetben és máshogy egy Petri-csészében; számítógépes párja is eltérő tulajdonságokat mutat egy zárt sandbox jellegű környezetben és „szabadon engedve” az internet vadonjában. Nem is kell olyan közeli felvételt készítenünk erről a *környezetről*, és mégis szembetűnő a kibertér lakóinak számos fajtája (Betz, Stevens, 2013). Vírusok, férgek, trójai vírusok, zombik, spyware, adware,

rootkit eszközök és billentyűleütés figyelők fenyegetik a kibertér felhasználóját, taktikájuk a tömeges adathalásztól a célzott „szigonyos halászatig”²⁰ és „watering-hole”²¹ támadásokig terjed. Az analógia azonban túlmutat a káros tartalmak viselkedésének vizsgálatán. Ahogy az ökológia középpontjában az ökoszisztémák rendszerszerű, átfogó szemlélete áll, úgy a kibertér ökoszisztémaként kezelve nekünk is figyelembe kell vennünk nemcsak annak káros, hanem hasznos elemeit is. Az ökoszisztéma jellemzője, hogy számos különböző szereplőt fog össze egy rendszeren belül, amely szereplők különböző okokból és célokkal lépnek interakcióra egymással. Ilyen szemléletet alkalmazva a kibertér részének kell tekintenünk az internetszolgáltatókat, a fejlődő infrastruktúrát, a hálózatok üzemeltetőit, a tartalom előállítóit, a programok és alkalmazások fejlesztőit és végfelhasználóit egyaránt. Az ökoszisztéma-analógia segít annak felismerésében, hogy ezek között a szereplők között – szinte kivétel nélkül minden szereplő között – valamilyen jellegű kapcsolat létezik. Ez a kapcsolat lehet pozitív vagy negatív előjelű, szimbiotikus vagy parazitikus, de akár semleges is.

Egy ilyen ökoszisztémán belül a hatalom eloszlása inkább diffúz, mintsem koncentrált. A rendszer egésze szempontjából kritikus, hogy a rendszer szereplői egyéni szinten is védve legyenek (DHS, 2011). A rendszer „egészsége” attól függ, hogy a kulcselemei és a populáció, amelyet átfog, mennyire képesek rugalmasan reagálni a környezet változásaira. A rendszer egy kritikus eleme elleni támadás az egész rendszert fenyegetheti. Ez alatt a kijelentés alatt egyaránt érthetünk konkrét támadást, ami például egy kiemelkedő forgalmat bonyolító internet-szolgáltató ellen irányul, vagy kevésbé konkrét eseményt, amely például a rendszer alapjául szolgáló bizalmat rengeti meg. Az ökoszisztéma fejlődése a szereplőinek tevékenységéből ered. A szereplők igen nagy száma rendkívül megnehezíti, azonban nem teszi lehetetlenné a fejlődési irány belülről történő befolyásolását. Ennek a befolyásolásnak a fent hivatkozott DHS dokumentum szerint az eszköze nem a közvetlen vezetés és irányítás (a katonai terminológia szerinti C2 rendszer), hanem sokkal inkább az összpontosítás és konvergencia („focus” és „convergence”) kell, hogy legyen. A pozitív és negatív ösztönzők, a közös viselkedési kultúra kialakítása a kibertérben sokkal hatékonyabb lehet, mint a közvetlen kényszerítés.

²⁰ Az ún. spear phishing olyan támadás, mely során a támadó egy általában alapos felderítés után kiválasztott személytől (pl. egy minisztérium vagy egy vállalat dolgozója) próbál meg információkat szerezni vagy rajta keresztül bejutni egy nagyobb hálózatba.

²¹ A watering-hole támadások során a támadó egy ártalmatlannak tűnő és bizonyos csoportok által gyakran látogatott honlap felülete mögé helyez el káros tartalmat, mely a honlapot meglátogatók számítógépét automatikusan megpróbálja megfertőzni.

A kibertér mint társadalmi tér

A kibertér természetére vonatkozó egyik legalapvetőbb metafora magának a jelenségnek az elnevezéséből fakad. Annak ellenére, hogy a kiberterről nehezen tudunk bármit is mondani anélkül, hogy térnek neveznénk, ritkán gondolunk bele abba, hogy miért is hívjuk így és milyen térről is van szó. A tér-metafora igazság szerint a kibertér elnevezés megjelenése után töltődött fel tartalommal, a névválasztást így intuíciónak, vagy valószínűleg inkább a kognitív lingvisztika azon jelenségének kell betudunk, amely szerint természetszerűleg használunk tér- és idő-metaforákat nyelvünkben és gondolkodásunkban (Cohen, 2007:230). A tér-analógia feltárása a jogtudomány területéről indulva jutott el a társadalomtudományok szélesebb asztalára. A társadalomelmélet a konstruált (mesterséges) terek három alapvető fajtáját különíti el. A vágyainkból táplálkozó utópiát (és ennek ellenpontját, a disztópiát), a létező terek mintájára konstruált izotópiát, valamint a heterotópiát. Utóbbi koncepcióját Michel Foucault francia filozófusnak köszönhetjük. Foucault megfogalmazásában a heterotopia olyan tér, mely az utópiához hasonlóan minden más térrel kapcsolatban áll, azonban valós hellyel is rendelkezik. Heterotópiában a viselkedés hétköznapi szabályai különböző módokon felfüggesztésre kerülnek, teret adva olyan viselkedési mintáknak – „kísérletezésnek” – amilyen mintákkal a hagyományos térben nem találkozunk. Foucault példaként többek között a bordélyházat, a gyarmatokat, a színházat és a kertet említi. A bordélyházban a hétköznapi gátlások levetkőzése, a gyarmatokon egy új társadalmi rend kialakítása, színházban a tér és idő összesűrítése válik lehetővé, a kert pedig kísérlet a természet egy idealizált miniatűrjének létrehozására (Cohen, 2007:214).

A kibertér heterotópiaként való felfogása több szempontból is hasznos. Az analógia révén rögtön nyilvánvalóvá válik, hogy a kibertér nem utópia. A kibertér nem olyan tér, amilyennek vágyaink szerint lennie kellene. A nyugati társadalmak szeretik abba az illúzióba ringatni magukat, hogy a kibertér a szabadság birodalma, ahol az emberi jogok és demokratikus elvek maradéktalanul érvényesülnek, ahol a kormányzás struktúrája lapos, és ahol mindenki egyenlő jogokkal és egyenlő hatalommal bír. De ennek ellentéte sem igaz a kibertérre. Nem a hagyományos tér pusztá kiterjesztéséről van szó, a mindennapi normák nem ültethetők át egy az egyben, és erre sok esetben igény sincsen. Gondoljunk a mozifilmek előtti rövid figyelemfelhívó bejátszásokra, melyek az illegális letöltést hivatottak visszaszorítani: a kisfilmek a „Nem lopnál autót, nem lopnál táskát. Miért lopnál filmet?” analógiára építenek. Ez az analógia ugyanakkor téves, ha elfogadjuk a kibertér heterotóp természetét, és azt, hogy

a kibertérben más normák, vagy legalábbis más módon érvényesülő normák uralkodnak. Ebben az esetben ugyanis egy film illegális letöltése normatív módon tökéletesen megfér az autólópás elutasításának gondolatával. A torrent oldalak letöltési statisztikái és a kalózpártok társadalmi támogatottsága egyaránt ezt a nézetet látszik megerősíteni.

Az utóbbi években egyre inkább tanúi lehettünk az utópikus gondolkodás visszaszorulásának. John Perry Barlow, akit az internet egyik alapító atyjának és az utópikus gondolkodás megtestesítőjének tekinthetünk 1996-ban a meglehetősen hangzatos „*Declaration of the Independence of Cyberspace*” címet adta manifestójának, melyben a kormányzati modellek internetre való alkalmazhatatlansága mellett érvelt. Barlow nézeteit később mérsékelte. Hasonlóképp, William Gibson sci-fi író, akinek a művein keresztül a kibertér elnevezés elterjedt, maga is bevallotta az utóbbi években, hogy a kifejezés nem volt több egy értelmet nélkülöző divatos frázisnál (Betz, Stevens, 2013).

Mi is akkor a gyakorlati következménye a kibertér heterotóp jellegének? A kibertér megértéséhez akkor kerülünk közelebb, ha azt a fizikai és társadalmi valóságban gyökerező, ahhoz számos ponton szorosan kapcsolódó, de annak mégsem integráns részét képező jelenséggént fogjuk fel, amely intenzív módon visszahat a fizikai és társadalmi valóságra és formálja azt. Nézzünk néhány példát az izotópiától való elkülönítésre. Mikor a vásárlás folyamata bekerült a kibertérbe, sokan azt feltételezték, hogy lényegében pontosan olyan lesz, mint besétálni egy boltba, csak gyorsabb és kényelmesebb, nagyobb termékválaszték és olcsóbb árak mellett. A webshopok polcáról válogatunk, fizetünk, majd az áru valamilyen úton-módon megérkezik hozzánk. A valóságban ezzel szemben az internetes vásárlás – vállalati szempontból az interneten keresztüli beszerzés – minőségileg új gazdasági folyamatokat indukált, például az „éppen időben” elvre épülő termelési rendszer kialakulását vagy a kriptovaluták megjelenését. Másik, biztonságpolitikai szempontból érdekesebb példa lehet az al-Kaida szervezeti struktúrájának átalakulása vagy az a mód, ahogy az Iszlám Állam rekrutációs tevékenységét végzi.

Nem szabad ugyanakkor abba a hibába esnünk, hogy a kibertér egyszer és mindenkorra heterotóp térnek bélyegezzük. A kibertér és a róla való gondolkodás az elmúlt években dinamikus változáson ment keresztül. Az internet korai éveiben egészen közel állt az utópiához. Az internet elődjének tekinthető ARPANET hat amerikai egyetem számítógépes hálózatát kötötte össze a tudományos tevékenység előmozdítása és az információ szabad áramlása érdekében, egy olyan közegben ahol felhasználók kivétel nélkül és maximálisan

megbíztak egymásban. Az internet a bővüléssel párhuzamosan egyre inkább mozdult el heterotóp irányba, ma pedig már annak a jelei is látszanak, hogy ez az elmozdulás tovább folytatódhat. Az államok egyre inkább próbálják szuverenitásukat kiterjeszteni a kibertérre, egyre erőteljesebben próbálják a hagyományos normákat átültetni, egyelőre változó sikerrel. Gondoljunk az elbukott SOPA és PIPA kezdeményezésekre az Egyesült Államokban, az ACTA-ra nemzetközi szinten, vagy a NATO Kibervédelmi Kiválósági Központja által összeállított Tallinn Manual megállapítására, mely szerint a nemzetközi jog szabályai a kibertérben is irányadók. Az említett elbukott szabályozási kezdeményezések egyáltalán nem jelentik azt, hogy az internet nem állna valamilyen mértékű állami kontroll alatt. Olyan tartalmak ellen, mint például a gyermekpornográfia, az államok és a társadalmak tagjai egyértelműen és nagyon keményen állást foglaltak. Az internet szabályozásának jelensége még szembetűnőbb a „nagy tűzfalat” építő Kínában, az internet korlátozásának gondolatával az ukrán válság kapcsán eljáró Oroszországban, és az ezt ténylegesen meglépő Törökországban vagy az arab tavasz által érintett államokban. Ezekben az államokban az a közös, hogy eleve hiányzik az a nyugati demokratikus kultúra, ami a kibertér utópikus szemléletét vagy legalábbis az utópikus szemlélet szólásszabadsággal és az információ szabad áramlásával való összekapcsolását megalapozta volna. Egy kínai állampolgár valószínűleg teljesen mást gondol a „tökéletes” internetről, mint egy nyugati. Ennek a kibertérrel kapcsolatos nemzetközi diskurzus szempontjából kulcsfontosságú jelentőséget kell tulajdonítanunk. A jelenlegi trendek azt mutatják, hogy a hagyományos normák és a kibertér normái utóbbi expanziójával folyamatosan közelednek egymáshoz. Tekintve, hogy a fiatalabb generációk életét egyre komolyabb – akár a fizikai valóságét meghaladó – mértékben határozza meg az internet, elképzelhető, hogy néhány generáción belül a kibertérben születő és fejlődő normák felváltják a jelenleg hagyományosnak tekintett normákat. Ez akár ahhoz az extrém szituációhoz is vezethet, hogy filmek után autót lopni sem lesz normatívan elítélendő, például a dizájnt internetről letöltve, az autó alkatrészeit pedig 3D-nyomtató segítségével kinyomtattva.

A kibertér heterotóp szemlélete definíciós választásunkat is alátámasztja. Az internet szociális fórummá, a 21. század agorájává nőtte ki magát. A kibertér rendkívüli hatású eszmék szülőhazájává és közvetítőjévé, társadalmi struktúrák átalakítójává, új típusú identitások megteremtőjévé vált csoportok és egyének szintjén egyaránt. Kibertér és társadalom nem választható el egymástól.

Befejezés

James Der Derian 2013-ban megjelent tanulmányában a háború átalakulásáról ír. A globális információs hálózatok létrejöttével olyan korszakba érkeztünk, ahol helyi incidensek nemzetközi válságokká nőhetik ki magukat, ahol a háború képei egyre gyorsabban váltogatják egymást az előttünk lévő képernyőn és ahol az erőszak globálissá vált. A globális média egyedülálló jelentőséggel bír az erőszak szervezésében, megvalósításában, igazolásában és ábrázolásában (Der Derian, 2013). Ennek a globális médiának központi eleme a kibertér. Der Derian arra próbálja meg felhívni a figyelmet, hogy a globális hálózatok átalakítják a háborút. Nem pusztán a megvívására használt eszközök és a háborút passzívan figyelő globális közönség megjelenésének tekintetében. Az erőszak társadalomformáló ereje megnőtt, és nem csupán azok számára, akik az erőszak közvetlen elkövetői vagy elszenvedői, hanem azok számára is, akik számára a szemük előtti képernyőn jelenik meg. De nemcsak az erőszak bír ilyen hatással. A globális hálózatok képesek *minden* társadalmi folyamat felnagyítására, erejének megsokszorozására, irányának megváltoztatására, és ugyanezek ellenkezőjére is. Paul Virilio *Az információs bomba* című könyvében információ és interaktivitás kapcsolatát az energia és radioaktivitás kapcsolatához hasonlítja (Virilio, 2000, idézi Der Derian, 2013). Az analógia rendkívül találó. A kibertér felhasználói közti interaktivitás megállíthatatlanul fokozódik. A folyamatot következményei egyértelműen stratégiai kérdéssé teszik, de teljes megértéséhez a stratégiai tanulmányok tudományos eszköztára kevés. Ahogy önmagában kevés a hadtudomány, a nemzetközi tanulmányok, a politológia, a szociológia, a pszichológia, a médiatudomány, az antropológia, a statisztika vagy éppen a lingvisztika eszköztára is. A sikert ezek együttes, interdiszciplináris alkalmazása sem garantálja. Komoly érvek szólnak amellett, hogy a társadalomtudományoknak a kvantumfizika és a káoszelmélet alapvető eredményeit magukévá kéne tenniük. Előbbi a közvetlen tapasztalaton alapuló világképen túllépve és a determinisztikus megállapítások helyébe a valószínűségen alapuló előrejelzést helyezve középpontjának a bizonytalanságot tekinti. Utóbbi alapvetően determinisztikus, sok összetevőből álló, nem lineáris rendszerek leírását kísérli meg, illetve ezek esetében fogalmaz meg korlátokat az előrejelzésre nézve.

Dolgozatomban amellett érveltem, hogy a „kiberbiztonság” nem kezelhető pusztán katonai kérdésként. A kibertér definíciójába indokolt beleértенünk a felhasználókat. A kibertér tudományos vizsgálatának középpontjában a társadalomnak kell állnia, a társadalmi aspektusok vizsgálatát azonban nehezíti, hogy a kiberbiztonsági szakirodalmat túlnyomórészt

katonai nyelvezet, katonai analógiák uralják. A fenti oldalakon kínált néhány alternatíva reményeim szerint hozzájárul a kibertér teljesebb megértéséhez. Mindazonáltal szeretnénk megismételni kezdeti állításunkat, miszerint analógiák útján semmilyen jelenség megismerése nem lehet teljes. Az analógiák és metaforák tudatos használata pusztán segédeszköz. A kibertér természetének legnagyobb veszélyt rejtő aspektusa, hogy drasztikusan megnöveli a stratégiai szempontból fontos *ismeretlenek* és a *megismerhetetlenek* számát.

Felhasznált irodalom

- Arendt, Hannah (1973): *Crisis of the Republic*, Harmondsworth, UK: Penguin
- Arquilla, John – Ronfeldt, David (1993): Cyberwar is Coming!, *Comparative Strategy*, 12:2, pp. 141-165.
- Bañcerowski Janusz (1999): A kognitív nyelvészet alapelvei, *Magyar Nyelvőr*, 123. évf. 1. szám
- Betz, David (2012): Cyberpower in Strategic Affairs: Neither Unthinkable nor Blessed, *Journal of Strategic Studies*, 35:5, pp. 689-711.
- Betz, David J. – Stevens, Tim (2013): Analogical reasoning and cyber security, *Security Dialogue*, 44:2, pp. 147-164.
- Brantly, Aaron F. (2014): Cyber Actions by State Actors: Motivation and Utility, *International Journal of Intelligence and Counterintelligence*, 27:3, pp. 465-484.
- Charney, Scott (2010): Collective Defense: Applying Public Health Models to the Internet
- Clarke, Richard – Knake, Robert K. (2010): *Cyber War: The Next Threat to National Security and What to Do About It*, New York, NY: Harper Collins
- Cohen, Eliot A. (1994): The Mistique of U.S. Air Power, *Foreign Affairs*, 73:1
- Cohen, J. E. (2007): Cyberspace As/And Space, *Columbia Law Review*, 107:1, pp. 210-256.
- Demchak, Chris C (2012): Resilience and Cyberspace: Recognizing the Challenges of a Global Socio-Cyber Infrastructure (GSCI), *Journal of Comparative Policy Analysis: Research and Practice*, 14:3, pp. 254-269.
- Der Derian, James (2013): From War 2.0 to quantum war: the superpositionality of global violence, *Australian Journal of International Affairs*, 67:5, pp. 570-585.
- DHS (2011): Enabling Distributed Security in Cyberspace: Building a Healthy and Resilient Cyber Ecosystem with Automated Collective Action, Department of Homeland Security White Paper, <http://www.dhs.gov/xlibrary/assets/nppd-cyber-ecosystem-white-paper-03-23-2011.pdf> (letöltés: 2014.11.11.)
- Guillon, Clement (2013): Cyber insecurity as a national threat: overreaction from Germany, France and the UK?, *European Security*, 22:1, pp. 21-35.
- Junio, Timothy J. (2013): How Probable is Cyber War? Bringing IR Theory Back In to the Cyber Conflict Debate, *Journal of Strategic Studies*, 36:1, 125-133.

- Kovács László – Krasznay Csaba (2010): Digitális Mohács. Egy kibertámadási forgatókönyv Magyarország ellen, *Nemzet és Biztonság*, 2010/1.
- Lattmann Tamás (2014): Az informatikai hadviselés nemzetközi jogi aspektusai. Előadás az ELTE NT SzHÉK és a Biztonságpolitikai Szakkollégium szervezésében, 2014. szeptember 30.
- Lee, Robert M. – Rid, Thomas (2014): OMG Cyber!, *The RUSI Journal*, 159:5, pp. 4-12.
- Lewis, James A. (2014): National Perceptions of Cyber Threats, *Strategic Analysis*, 38:4, pp.566-576.
- Libicki, Martin C. (2009): Cyberdeterrence and Cyberwar, Santa Monica, CA: RAND Corporation
- Libicki, Martin C. (2012): Don't Buy the Cyberhype: How to Prevent Cyberwars From Becoming Real Ones, *Foreign Affairs*, 2013. augusztus 14.
<http://www.foreignaffairs.com/articles/139819/martin-c-libicki/dont-buy-the-cyberhype> (letöltés: 2014.11.08.)
- Liff, Adam P. (2012): Cyberwar: A New 'Absolute Weapon'? The Proliferation of Cyberwarfare Capabilities and Interstate War, *Journal of Strategic Studies*, 35:3, pp. 401-428.
- Liff, Adam P. (2013): The Proliferation of Cyberwarfare Capabilities and Interstate War, Redux: Liff Responds to Junio, *Journal of Strategic Studies*, 36:1, pp. 134-138.
- Marton Péter (2013): A külpolitika elemzése: fogalmak és módszerek a külpolitika forrásainak feltárására, Budapest: Antall József Tudásközpont
- Nye, Joseph S., Jr. (2010): Cyber Power, Belfer Center for Science and International Affairs, 2010. május, <http://belfercenter.ksg.harvard.edu/files/cyber-power.pdf> (letöltés: 2014.11.08.)
- Nye, Joseph S., Jr. (2011): The Future of Power, New York, NY: Public Affairs
- O'Connell, M. E. (2012): Cyber Security without Cyber War, *Journal of Conflict & Security Law*, 17:2, pp. 187-209.
- Rid, Thomas (2012): Cyber War Will Not Take Place, *Journal of Strategic Studies*, 35:1, pp. 5-32
- Rid, Thomas (2013a): Cyberwar and Peace: Hacking Can Reduce Real-World Violence, *Foreign Affairs*, 92:6
- Rid, Thomas (2013b): More Attacks, Less Violence, *Journal of Strategic Studies*, 36:1, pp. 139-142.

- Rid, Thomas – McBurney, Peter (2012): Cyber Weapons, *The RUSI Journal*, 157:1, pp. 6-13.
- Shachtman, Noah – Singer P. W. (2011): The Wrong War: The Insistence on Applying Cold War Metaphors to Cybersecurity Is Misplaced and Counterproductive, *Government Executive*, 2011. augusztus 15.
- Singer, P. W. – Friedman, Allan (2014): Cybersecurity and Cyberwar: What Everyone Needs to Know, New York, NY: Oxford University Press
- Stone, John (2013): Cyber War Will Take Place, *Journal of Strategic Studies*, 36:1, pp. 101-108.
- Thomas, Timothy (2014): Creating Cyber Strategists: Escaping the 'DIME' Mnemonic, *Defence Studies*, 14:4, pp. 370-393.
- Virilio, Paul (2000): The Information Bomb. London: Verso