Nyáry Gábor

Akindzsik a kibertérben

Virtuális háború kontra digitális felforgatás

A szemünk előtt, a közvetlen szomszédságunkban véres háború dúl, és ez óhatatlanul vonzza a tekintetünket. De ne legyenek kétségeink: veszélyes konfliktusok terepe a földgolyó jó része. Az életünket felismerhetetlenségig megváltoztatja, jó értelemben is, veszélyekkel is a digitalizációnak nevezett drámai átalakulás. Nemcsak a technológia változik, de a minket körülvevő világ is. Tektonikus geopolitikai átrendeződés zajlik körülöttünk. A többpólusú világban az érdekérvényesítés és a szabályoknélküliség a jellemző, amihez jól illeszkedik a kiberhadszínterek átláthatatlan, képlékeny közege. Ami vitathatatlan: szakadatlanul „dörögnek" már a fegyverek ebben az új kiberdimenzióban. Ami viszont még kérdés: ez vajon „kiberháború", vagy valami más lesz?[1] Szakértők sorra tárják fel a probléma jelentésrétegeit, és a megértéshez talán közelebb segít minket a kiber-nemzetbiztonsági kutatásokban ma már egyáltalán nem ismeretlen analógiás gondolkodás.[2] Egy számunkra ismerősen csengő metaforát hívunk ehhez segítségül.

A sarkaiból kifordult világ – bevezető helyett

Hajlamosak vagyunk még mindig úgy fogalmazni, hogy „információs társadalomban" élünk. Pedig az igazság az, hogy a világunk egyre inkább elmozdul egy „digitális társadalom" felé. A kapcsolat persze szerves, hiszen ez utóbbi az információ központi szerepe köré szerveződő közösségből nő ki azáltal, hogy lassan minden tevékenységünk digitális eszközökön alapszik, és az interneten nyugvó, decentralizált hálózatok szervezik életünk működését. Az anyagi javak termelése és fogyasztása, a gazdaság szintén a digitalizáció rohamos terjedésével kap új dimenziót. Sommás megfogalmazással úgy jellemezhető ez a folyamat, mint amelyben az adatok és a hálózatok körbefonják, átitatják a termelési folyamatokat,

[1] Vö. Amit Sharma: Cyber Wars: A Paradigm Shift from Means to Ends. *Strategic Analysis,* 34. (2010), 1. 67–73.

[2] A témában máig megkerülhetetlen a kiberháborúhoz kapcsolódó mítoszképzés mechanizmusait feltáró tanulmány. Vö. Erik Gatzke: The Myth of Cyberwar. *International Security,* 38. (2013), 2. 41–73.

https://doi.org/10.36250/01164_19

a kormányzati és személyes fogyasztást, a határokon átívelő kereskedelmi forgalmat és természetesen a gazdaságot mozgató pénzügyeket is.

A dolgoknak azonban rendszerint megvan a maguk árnyoldala is. A korszerű technológiák mindent átszövő használata megsokszorozza a jólétünket, kényelmünket – de ugyanakkor hallatlanul kiszolgáltatottá is teszi a modern társadalmakat. Ahogy bővül a világban felhalmozódó adattömeg, ahogy terjeszkedik, bővül a digitális gazdaság – egyre növekszik a kiberbiztonsági kockázatok abszolút és relatív mértéke is. A sérülékenység az ár, amelyet a digitalizáció elképesztő lehetőségeiért fizetnünk kell. A kibertér, életünknek ez az új dimenziója nem csupán a tisztességes vagy békés szándékú szereplőknek ad otthont. Jól képzett, a technológia réseit könyörtelenül kihasználó kiberbűnözők igyekeznek csapdába csalni, megtéveszteni, kifosztani egyént, vállalatot, államot. De ami még nyugtalanítóbb: az online terek feltáruló világa újfajta harcosok küzdelmének a terepe is. A digitális világban, állítják sokan, már ma is dúl a „háborús szint alatti", csendes hadakozás. Vagy már „háború"?

Módszertani megközelítések és lehetőségek

A viszonylag hosszú ideje zajló szakmai vitákban való eligazodást egy sajátos módszertani eszköz (valójában inkább látásmód), az analógiákon nyugvó leírás és érvelés segítheti. A történettudomány természetesen régóta használja ezt a kézenfekvő lehetőséget, de ma már a politológia számos részterületének művelői is szívesen nyúlnak ehhez az „eszközhöz".

Clausewitz a kibertérben

A szomszédban valóságos háborúban csapnak össze az ellentétek, de ugyanakkor a hírek és dezinformációk körül kavargó információs hadviselés is igazi csatatereket idéz. Nem is beszélve a kiberhadszínterekről. A 19. század elejének nagy teoretikusa, a porosz Clausewitz munkássága óta mindent tudni vélünk a háborúról, ám napjaink eseményei mintha fejük tetejére fordítanák ezeket az öröknek gondolt igazságokat is. Szakemberek, a nemzetközi kapcsolatok, a kiberbiztonság kutatói vitatkoznak olyan alapvető kérdéseken, hogy a digitális tereket is elborító támadások, akciók háborúnak tekinthetők-e? Vajon egyáltalán használhatók még ezek a fogalmaink? Ha igen, akkor hogyan?

Analógiás gondolkodás a kiber-nemzetbiztonsági kutatásban

Az analógiás gondolkodás (történeti összehasonlítás) nem ismeretlen a nemzetközi kapcsolatok kutatásában.[3] Természetesen maga a politika is szívesen nyúl ehhez a támponthoz, és a nemzetbiztonság számos döntését támogatták meg az elmúlt fél évszázadban ilyen elemzési segédeszközzel. Klasszikus példa erre az amerikai Vietnám-politika formálása, amelynél erősen támaszkodtak a korábbi koreai konfliktus számos tanulságára. Az ügy egyben a veszélyekre is figyelmeztet: a helytelenül megválasztott analógiák könnyen vezethetik gondolkodási tévútra az elemzőket. A nemzetközi kapcsolatok területének történetianalógia-slágere mostanában kétségtelenül az úgynevezett Thuküdidész-csapda koncepciója, ami pedig arra mutat rá: a plasztikus történelmihelyzet-hasonlatok sem mindig képesek áttekinthetőbbé, egyértelműbbé tenni az elemzendő mai helyzeteket.

Kevéssé közismert, de a kiber-nemzetbiztonság különösen fontos koncepcionális segédeszközként nyúlt már eddig is az analógiák, történeti múltban gyökerező hasonlatok eszközrendszeréhez. Elég, ha a szakterület leghíresebb metaforájára, a „Cyber Pearl Harbor" kifejezésre gondolunk, amellyel Leon Panetta akkori amerikai hadügyminiszter vetítette előre 2012-ben a kiberháború mindent elpusztító rémképét.[4] Számunkra különösen fontos (egyben jól mutatja az analógiás történeti gondolkodásban rejlő lokálisprobléma-specifikáló erőt), hogy hazai kutatók is egy szellemes történeti metaforával (a „Digitális Mohács"-koncepció megalkotásával) a magyar közönségnek plasztikus módon vázolták fel a kibertér fenyegetéseinek perspektíváit.[5]

Az analógiás gondolkodás, amely szinte ösztönösen használt fogalomértelmező eszközünk, különösen alkalmas arra, hogy innovatív megoldásokkal segítsen át nehéz problématerületeken. A kibertérben való hadviselés egyszerűnek látszó, de valójában roppantul megosztó értelmezési feladatában mi is egy ilyen történeti

[3] Specifikusan a kiberbiztonsággal kapcsolatos alkalmazhatóságot vizsgálja Reasoning by Analogy in Cyberspace. Deadly Balloons and Avoiding Digital Doom. *CFR's Blogs,* 2017. december 18. Alapmunka továbbá David Sulek – Ned Moran: What Analogies Can Tell Us About the Future of Cybersecurity. In Christian Czosseck – Kenneth Geers (szerk.): *The Virtual Battlefield. Perspectives on Cyber Warfare.* Amsterdam, IOS Press, 2009.

[4] A koncepció gyökereit, majd pályaívét kitűnően összegzi Sean Lawson – Michael Middleton: Cyber Pearl Harbor: Analogy, Fear, and the Framing of Cyber Security Threats in the United States, 1991–2016. *First Monday,* 24. (2019), 3–4. 1–24.

[5] Vö. Kovács László – Krasznay Csaba: Digitális Mohács 2.0: kibertámadások és kibervédelem a szakértők szerint. *Nemzet és Biztonság,* 10. (2017), 1. 3–16.

analógiát hívunk segítségül. A választott analógia bár időben szokatlanul távoli, de kulturális kontextusában nagyon is megfogható, és így a tisztánlátásunkat előmozdító eszköz lehet a jövőben.

Modernitás és a háború új arca

A technológia, amely persze maga is egy társadalmi igény terméke, nyilvánvaló és jól ismert módon képes alakítani az emberi közösségek intézményeit és folyamatait. Talán sehol sem olyan jól dokumentált és széles körben ismert ez a visszahatás, mint a pusztítás eszköztárának és eljárásainak alakulásában. Ez az időtlen kapcsolódás mégis az ipari-tudományos forradalomtól kezdve hozott igazi változásokat. A most zajló IKT-alapú átalakulásnak, és ennek részeként az emberi fegyveres küzdelmek konceptuális transzformációjának is jó okkal kereshetjük az előképét a 19–20. század fordulójának eseményeiben.

Emlék a múltból: a stratégiai pusztítás gondolata gyökeret ver

1940. november 14-én este, a hitleri Németország 3. Légi hadseregének 515 nehézbombázója a magasba emelkedett. A gépek a Londontól északnyugatra elterülő Coventry városa felé vették az irányt. Lényegében ellenállás nélkül közelítették meg a mit sem sejtő települést, és pusztító bombazáport zúdítottak a páratlan műemlékekkel is rendelkező, fontos ipari központra. A terv, ma már tudjuk, nem az ipari övezetek elérése volt: a 3000 gyújtóbombával a sűrűn lakott polgári negyedeket vették célba.[6] A város történelmi negyedei romba dőltek, a halálos áldozatok száma százakra rúgott. A II. világháború elején, az Anglia elleni német légi háború nyitó időszakában történt az eset, amely fordulópontot jelentett a légi hadviselés akkor még újnak számító gyakorlatában.

Tömegipar és a totális háború

A megelőző, 1914 és 1918 között zajló nagy háború időszakában életre hívott repülőcsapatok sokáig csak a megfigyelő, felderítő szerepet mondhatták magukénak. A két világháború közötti időszakban aztán, párhuzamosan a repülőtechnika gyors fejlődésével a világ katonai teoretikusai kutatni, vitatni kezdték a születőben levő új fegyvernem lehetséges alkalmazásait. Talán meglepő, de egy itáliai tábornok, Giulio

[6] A légi offenzíva átfogó összegzését hozza Tami Davis Biddle: *Rhetoric and Reality in Air Warfare.* Princeton, Princeton University Press, 2002.

Douhet képzeletében fogant meg először a gondolat, hogy a repülő szerkezetek, erős robbanóanyagokat szállítva, az arcvonalak fölötti egyszerű csetepatéknál sokkal drámaibb módon is befolyásolhatnák a hadviselés menetét. Az olasz generális *Az égbolt meghódítása* című meghatározó könyvében a stratégiai bombatámadások elméletét fektette le. Azt vallotta: az új hadszíntér, a levegőég eme új fegyverei, a repülőgépek egymagukban képesek lehetnek eldönteni a jövőben a háborúk kimenetelét. Nem azt állította, hogy az új fegyverek, a távolból felemelkedve és megközelítve a célt, képesek teljesen romba dönteni annak infrastruktúráját. Douhet a tömegbombázások morális eszközként való alkalmazásában hitt: azt állította, hogy a polgári célpontok, mai szavunkkal a kritikus infrastruktúrák elleni tömeges támadások képesek lehetnek arra, hogy megtörjék az ellenség harci kedvét, lelkierejét. Az olasz katonai gondolkodó a totális háború elvét rajzolta fel, ahol mindenki, az egész társadalom harcoló fél, egyben ellenség.[7]

Az új gépezetek és a majdani harcaiknak teret adó „levegőég" persze még újdonságnak számítottak. Valahogy úgy, mint napjainkban a kibertér és benne a különféle támadó szoftverek, a sokat emlegetett kiberfegyverek. Nem voltak még a gyakorlat által kitaposott ösvények, és az elméleti vitákban különböző elképzelések csaptak össze arról, hogyan lenne a legcélszerűbb felhasználni ezeket a modern innovációkat. A kiforratlan alkalmazás, a koncepciók sokfélesége jellemezte az 1939-ben kirobbant második nagy világégés első időszakát. A technológiai kételyek mellett elsősorban morális szempontok korlátozták az új lehetőségek ilyen példátlan pusztítást hozó alkalmazását, amelyet Douhet tábornok javasolt elméletében. A kezdetben szintén a kizárólag katonai jellegű pontcélok bombázására koncentráló brit légügyi vezetők az első háborús hónapok szorongatottságában a polgári célpontok, német városok tömeges pusztítását vetették fel, ám a példátlan lépés sokakat elriasztott ettől a fordulattól. A háború utáni időkben merült fel az elmélet: valójában a brit vezetés különböző hírszerzési forrásokból előre értesült a Coventry elleni közelgő német támadásról, mégsem hozott intézkedéseket a polgári lakosság megóvására. A feltételezés az: egy ilyen tömeges katasztrófával akarták megalapozni a közvéleményben az általuk tervezett stratégiaváltást. A történészi vita máig sem zárult le, egy dolog azonban biztos: Coventry drámája fordulópontot hozott a brit bombázóparancsnokság háborús stratégiájában.[8] Három és fél évvel később Németország települései romhalmazzá váltak.

[7] Az 1930-as évek nagy stratégiai közvitáit tekinti át, bemutatva és értékelve a korszak legjelentősebb újítója, Douhet munkásságát Thomas Hippler: *Bombing the People. Guido Douhet and the Foundations of Air Power Strategy, 1884–1939.* Cambridge, Cambridge University Press, 2013.

[8] Richard Overy: *The Bombers and the Bombed. Allied Air War over Europe, 1940–1945.* New York, Viking, 2015.

Háború a kibertérben – vagy valami más?

Napjaink szakértői és döntéshozói is a konfliktusok jellegét kutatják, a technológia hátán érkező új lehetőségek hadi alkalmazhatóságát latolgatják. Az egyik tábor az összecsapásokat forradalmasító eszköznek látja a kiberarzenált, akár a II. világháborúban városokat eltörlő bombázó ármádiákat. Mások a korlátokra figyelmeztetnek, és tagadják a digitális Armageddon rémképét.

A digitalizáció Douhet tábornokai – a héják

A nagy bombázó offenzívákról felvillantott iménti kép, és ezen belül is bizonyára a pesszimistább perspektíva ötlött a kiber-nemzetbiztonság szakembereinek jó része eszébe, amikor 2022 februárjában megindultak az orosz csapatok Ukrajna ellen. Pontosabban: a hosszú ideje prognosztizált, ám mindeddig elmaradt elsöprő kibervégítélet kapcsán. A szakma lényegében az orosz invázió megkezdődése óta azt kérdezgeti: hol marad a mindent elsöprő – és a tankoszlopokat, repülőgépeket megelőző, sőt azokat feleslegessé tevő – digitális csapás?[9] A mindent eldöntő, új hadialkalmazás, azaz a „kiberháború"? A kiberbiztonsági szakma, a katonai vezetések és a politikusok évek óta mondják, hogy a geopolitikai szembenállás legújabb terepe, a kibertér uralására koncentráló Oroszország pusztító csapással avatja majd fel a 21. század új kiberharcmodorát, amint összeütközésbe kerül a Nyugattal. A feltételezés természetesen nem volt alaptalan, hiszen az elmúlt években, de inkább évtizedben jó néhány olyan incidensre került sor a kibervilágban, amelyeket az orosz állam intézményeihez kapcsol a biztonsági szakma. Az Ukrajnával kirobbant véres és elhúzódó konfliktusuk pedig 2014 óta az orosz állami hackerszervezetek egyfajta kísérleti terepévé, laboratóriumává tette a szomszédos országot. Az eddigi időszak egyik legveszélyesebb és globális szinten is roppant károkat okozó kibertámadása és a középpontjában álló hírhedt NotPetya kiberkártevő is az ukrajnai polgári infrastruktúrák elleni orosz hackertámadással indult útjára 2017-ben. Szakmai körökben tehát meglehetősen erősen elterjedt az a feltételezés, hogy egy eljövendő fegyveres összetűzésnek is fontos kísérője (talán eldöntője) lesz a számítógépes infrastruktúra, elektronikus igazgatási és kereskedelmi rendszerek elleni koncentrált támadás. Azóta, hogy két amerikai tudós, a RAND kutatói közreadták mérföldkőnek számító tanulmányukat, a hadviselés gyökeres átalakulását hirdető digitális stratégiai evangelisták száma egyre növekedett a világban. John Arquilla és David Ronfeld 1993-ban publikált könyve már a címével meghatározta a közgondolkodást:

[9] Vö. Ukrainian President Speaks Amid Russian Invasion; Troop, Military Vehicles Enter Ukraine from Belarus; Ukraine Hit by Wave of Cyberattacks as Invasion Begins. Aired 4:30-5a ET. *CNN.com – Transcripts,* 2022. február 24.

Cyberwar Is Coming (A kiberháború eljövetele), hirdette a gyorsan népszerűvé vált munka, amely mély nyomokat hagyott a 21. század stratégiai gondolkodásmódján.[10]

Elemzők és ellenzők – a realista galambok

A „kibertér Douhet-jeivel", a kiberháború elkerülhetetlenségét hirdetőkkel szemben mindig is jelen volt és hallatta szavát egy másik szakmai elképzelés is.[11] A kibertérben folyó katonai műveletek lehetséges szerepének túlértékelése ellen felszólaló brit képviselő, a honvédelmi bizottságot vezető Tobias Ellwood velősen így fogalmazta meg ezt a „kiberszkeptikus" álláspontot: „kiberfegyverekkel senki nem foglalhat el egy országot. Tankkal viszont igen." A kibertér háborús lehetőségeinek korlátozott voltát aztán remekbe szabott tanulmányában járta körbe Thomas Rid, a digitális hadviselés egyik legjobb szakértője.[12] Munkájának a címe (amely később könyv formájában is megjelent) világosan tükrözi álláspontját: *Cyberwar Will Not Take Place.* A mű meggyőző érveléssel állítja: „A kiberháború nem fog beköszönteni!" Elemzését a háború klasszikus értelmezésétől indítva Rid leszögezi: a kibermműveletek nem képesek olyan értelemben kárt okozni, embert ölni, mint a hagyományos fegyverek. A kibertér akcióinak természetesen van hatása: diszruptív, zaklató, „nyirbáló" jellege tagadhatatlan, ám ez messze nem azonos a klasszikus értelemben vett „háború" eszközeinek és eljárásainak pusztító jellegével. A koncepció ilyen jellegű újragondolói közül külön is érdemes kiemelni két kutató munkásságát: Lennart Maschmeyer és Nadiya Kostyuk elgondolkodtató és gazdag tényanyagra építő tanulmányaikban bizonyítják a kiberhadviselés szubverzív jellegét.[13] Háborús „fegyvernek" nem alkalmas – de zaklatni, nyugtalanítani, zavart kelteni, felderíteni kiválóan felhasználható.[14] Nem véletlen tehát, vallja a szakemberek egy meglehetősen népes (és érvelését meggyőző empirikus kutatási anyaggal is megtámogató) csoportja, hogy a fegyveres harc kirobbanását nem kísérte egy „mindent elsöprő", az ellenfelet szinte puskalövés nélkül térdre kényszerítő „kiberháború": a rettegett kiber-Armageddon nem következett be. A kiber-nemzetbiztonság, konfliktuskutatás kiemelkedő szakembere, az amerikai Brandon Valeriano talán a legfontosabb

[10] John Arquilla – David Ronfeldt: Cyberwar is coming! *Comparative Strategy,* 12. (1993), 2. 141–165.

[11] Különösen érdekes, mivel a gyakorló kiberbiztonsági felsővezető szemszögéből láttatja és értékeli az eseményeket, Ciaran Martin: Cyber Realism in a Time of War. *Lawfare Blog,* 2022. március 2.

[12] Thomas Rid: *Cyberwar Will Not Take Place.* Oxford, Oxford University Press, 2013.

[13] Átfogó és sok szempontból úttörő munka Lennart Maschmeyer: *Slow Burn. Subversion and Escalation in Cyber Conflict and Covert Action.* Toronto, University of Toronto, 2020.

[14] Különösen meggyőzően érvel az ilyen műveletek „nem-háborús" klasszifikációja mellett Nadiya Kostyuk – Yuri M. Zhukov: Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events? *Journal of Conflict Resolution,* 63. (2017), 2. 1–44.

összegzését adta a témának kollégájával, Ryan Maness-szel közösen írt munkájában.[15] A könyv, igazodva a szerző évtizedes kutatási területéhez, az elsők között dolgozza fel empirikus adatokra támaszkodva a kibertér változatos akcióit és támadásait, és a kemény tényekre alapozva utasítja el az új hadügyi forradalmat vizionáló „kiber-Douhetek" szenzacionalistának tekintett álláspontját. A már említett Nadiya Kostyuk szintén több évtized kiberakcióinak empirikus adatait vizsgálva kereste a bizonyítékot arra, hogy az ilyen műveletek a „valódi" (kinetikus) katonai akciót helyettesítőek voltak-e (tehát ténylegesen „kiberháborúnak" tekinthető eseménysorok), vagy inkább a fizikai támadásokkal összehangolt, azokat kiegészítő lépések. Kostyuk megállapítása meglepő: sem az egyik, sem a másik alkalmazást nem támasztják alá a tényleges adatok. Inkább jellemző az, hogy a kiberakciókra és a kinetikus fegyveres mozdulatokra egymástól függetlenül került sor.[16] A kiberműveletek tehát, állítja a kutató, jellemzően nem a „háború" állami eszköztárának részét képezik.[17]

Eszközök, emberek és integrációk. A hadviselés új paradigmái a kibertérben

Noha a csúcstechnológiájú hagyományos (vagy nukleáris) fegyverzetek árához képest a támadó kiberkapacitások csupán szerény ráfordításokat igényelnek, tévedés volna alábecsülni ennek mértékét. A komoly kibertámadások összetett csapatokat, magas szakértelmű közreműködőket, fejlett eszközöket igényelnek – és mindezt hosszú időn át. A kiberfegyverek háborús alkalmazhatóságát ráadásul számtalan körülmény korlátozza.

Időzíthetőség, kontrollálhatóság, integrálhatóság

Ahogy azt feljebb láttuk, a szakértők egy része határozottan állítja, hogy a rosszindulatú számítógépes programok tényleges háborúra kevéssé alkalmasak. Súlyosan nehezíti a tényleges hadi alkalmazhatóságukat az időzítés kérdése. Bár mindegyik eset egyedi, a szakemberek szerint átlagosan két-három évig is eltarthat egy komoly kibertámadás előkészítése és végrehajtása. Ennek összehangolása (a szokásos gyakorlat szerint adott időpontokban induló és végrehajtandó) hagyományos katonai hadmozdulatokkal gyakorlatilag lehetetlen. A tetemes időigény és a pontos időzítés

[15] Brandon Valeriano – Ryan C. Maness: *Cyber War versus Cyber Realities. Cyber Conflict in the International System.* Oxford, Oxford University Press, 2015.

[16] Vö. Nadiya Kostyuk – Erik Gartzke: Why Cyber Dogs Have Yet to Bark Loudly in Russia's Invasion of Ukraine. *Texas National Security Review,* 5. (2022), 3. 113–126.

[17] Vö. még Lennart Maschmeyer: A New and Better Quiet Option? Strategies of Subversion and Cyber Conflict. *Journal of Strategic Studies,* 2022. július 27.

korlátai már eleve kétségessé tennék ezeknek az eszközöknek a háborús eszközként való alkalmazását.[18]

Hasonlóan komoly problémát jelent a hadi alkalmazás szempontjából az a körülmény, hogy nagyon nehéz előre pontosan meghatározni az akcióval kiváltott hatásokat. Amíg például egy rakétacsapás által előidézett kár viszonylag pontosan felbecsülhető, addig ez a kiberfegyverek alkalmazásakor több szempontból is problémás lehet. Ehhez kapcsolódik az egyik legsúlyosabb alkalmazási nehézség: a rendkívül tökéletlen kontrollálhatóság. Ez annyit jelent, hogy az okozott kár sok esetben nem szűkíthető egyetlen kiválasztott célpontra. A globális konnektivitás révén az ilyen informatikai károkozók könnyen „kiszabadulhatnak", majd a világhálón tovaterjedve ellenőrizhetetlen pusztítást végezhetnek – akár az akciót indító állam rendszereit is megfertőzve. A korábban említett NotPetya támadás éppen ezzel az utóhatásával okozta a legnagyobb riadalmat szakmai körökben. A nehéz kontrollálhatóság az Ukrajna elleni invázióhoz kapcsolódó kiberműveletekben ismét előbukkant. A fegyveres támadás megindulásával egy időben az ukrajnai internetes kommunikáció egy részét biztosító Viasat műholdas rendszere, a KA-SAT ellen (vélhetően oroszok által) bevetett számítógépes kártevő is gyorsan „elszabadult". A rosszindulatú program azután sokfelé okozott károkat.

Eredményesség

A Viasat rendszerei elleni támadás még egy fontos körülményre felhívta a figyelmet. A kiberakcióval megtámadott modemek jelentős része (egyszerű, a cég központjából hálózaton át végzett szoftveres javítással) ismét működőképessé volt tehető, és a szolgáltatás alig néhány órányi kiesés után zavartalanul folytatódott. Az érintett vevődobozok egy számottevő része javíthatatlan károkat szenvedett; azonban ezek kicserélése is csupán néhány napot vett igénybe. Tehát: a hosszas előkészítéssel indított és hatását tekintve nehezen fókuszálható kibernetikus támadás viszonylag olcsón és gyorsan javítható károkat okozott csupán.[19] A tényleges katonai alkalmazhatóság kritériumainak érvényesülését ugyanakkor jól példázza a 2022 őszén indított és az ukrán energetikai rendszer pusztítását, lassítását, rombolását célzó hagyományos támadássorozat. Két nap előkészítés és néhány tucat cirkálórakéta ráfordítása elégséges volt ahhoz, hogy Oroszország hosszú időre működésképtelenné tegye becslések szerint az ukrán energetikai hálózat 30%-át.

[18] Vö. Max Smeets: A Matter of Time: On the Transitory Nature of Cyberweapons. *Journal of Strategic Studies,* 41. (2018), 1–2. 6–32.

[19] Számtalan szerző emeli ki, hogy a kibertérben zajló műveletek stratégiai eredményessége (eredménytelensége) alapvető (mérhető) támpontot adhat az ilyen akciók jellegének megítélésében, a „háború", vagy valami más dilemmájának tisztázásában. Vö. Richard J. Harknett – Max Smeets: Cyber Campaigns and Strategic Outcomes. *Journal of Strategic Studies,* 45. (2022), 4. 1–34.

Adott célpontok elleni, időzített és legfeljebb kisebb mértékű nemkívánatos következményekkel járó támadásokra tehát összehasonlíthatatlanul alkalmasabbnak látszanak a hagyományos fegyverzetek.

Dilemmák és trilemmák

A kiberharc megvívásához kapcsolódó alapvető paraméterek közötti sajátos összefüggés bemutatására a téma egyik legismertebb kutatója, a zürichi Lennart Maschmeyer szellemes sémát szerkesztett.[20] Tézise szerint egy akció stratégiai hasznosságának feltétele az, hogy mérhetően hozzájáruljon az állami célok eléréséhez (vagy az erőegyensúly megváltozásához). Maschmeyer az intenzitást, a végrehajtás gyorsaságát és a kontrollálhatóságot tekinti olyan változóknak, amelyek a kiberművelet operatív eredményessége szempontjából kulcsfontosságúak. Felállítja azt a tételt, hogy egyszerre e három változóból legfeljebb kettő maximalizálható. A végrehajtás gyorsaságát és az akció hatásosságát növelve arányosan csökken annak kontrollálhatósága. Ez annyit jelent, hogy az operatív szempontból használható sebességgel és megfelelő intenzitással végrehajtott kibertámadás nagy eséllyel csúszhat ki az akciót végrehajtó ellenőrzése alól. A nemkívánatos következmények pedig nemcsak csökkentik az akció stratégiai értékét, de egyenesen önveszélyessé is tehetik a műveletet. Egy másik kombinációt figyelembe véve, a végrehajtás sebességét maximalizálva, ám ugyanakkor az ellenőrizhetőség kívánalmát is szem előtt tartva a támadó jó eséllyel lesz kénytelen értékelhető szint alá csökkenteni az akció intenzitását (azaz csupán csekély, vagy semmilyen stratégiai hatást nem lesz képes kiváltani a művelet). Ha pedig a hatásosságot és az ellenőrzés alatt tartást maximalizálná a végrehajtó (elméletileg e két paraméter teljesülése szolgálná a leginkább a stratégiailag számottevő eredményességet), úgy az a kivitelezés gyorsaságát csökkentené a használhatóság határa alá.

Célok

A szubverzív elméleten túl más elképzelések is születtek a kiberhadviselés mibenlétére vonatkozóan. Érdekes Benson fogalomrendje: ő a nemzetközi kapcsolatok értelmezési keretrendszerében próbál választ adni a kiberműveletek jellegére vonatkozó kérdésre.[21] A külpolitika-elmélet legközpontibb fogalmával, az erőegyensúly

[20] Lennart Maschmeyer: The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations. *Journal of International Security,* 46. (2021), 2. 51–90.

[21] Egyben a kiberhadviselés és a nemzetközi kapcsolatok szélesebb kontextusát is bemutatja. David Benson: Not Cyberwar, but Cyberbalance. *Aether. A Journal of Strategic Airpower and Spacepower,* 1. (2022), 2. 81–96.

kérdésével kapcsolja össze a kiberfegyverekkel folytatott műveleteket. Feltételezése az, hogy a kibertérben folyó műveletek célja valójában nem a másik fél megsemmisítése. Sokkal inkább az (adott térségben, adott időben fennálló) erőegyensúly megváltoztatása, eltolása az egyik (vagy több) fél képességeinek megnyirbálása, meggyengítése által. Az elmélet erőssége az, hogy a nemzetközi kapcsolatok rendszerét a maga összetettségében látja és értelmezi, amely szereplők egész sorának bonyolult kapcsolatain alapuló egyensúly formájában működik. Az ilyen koncepció különösen a multipolárissá váló világrenden belüli értelmezésekhez jelenthet hatékony keretet. Benson érvelése az, hogy számos kibertámadás valójában a nemzetközi struktúra egyensúlyrendjének megváltoztatására irányul; célja az egyik (vagy több fél) „hátrányosabb helyzetbe hozása" *(handicapping).*

Janicsárok kontra akindzsik: lehetséges magyarázó analógiák

Mint láttuk, a kibertér hadviselését vizsgáló kutatók egy része kétségbe vonja az ilyen akciók „háború" jellegét. Sőt, elemzéseikben feltételezik, hogy az ilyen eszközcsoport nem is alkalmas hagyományos háborúk megvívására, de még közvetlen támogatására sem. Nagyon is alkalmas eszköznek látszik azonban a zaklató, felforgató tevékenységek céljára. Ezen kutatási érvrendszer összegzésére, értelmezési keretbe helyezésére alkalmasnak gondoljuk a történeti analógiákat segítségül hívó munkamódszert.[22] A közelmúltban – a jellegzetes amerikai, atlanti környezet tapasztalataihoz igazodva – különösen érdekes alapvetés született: a kiváló oxfordi kutató, Florian Egloff a 18–19. századi atlanti vizek kalózkodásának jellemzőivel vetette össze (világította meg) a kibertérben folyó műveletek irreguláris jelenségtartalmát.[23]

Mi egy, a saját történeti-kulturális környezetünkhöz jobban illeszkedő (ezért számunkra plasztikusabb) történeti analógiát felhasználva, a 16–17. századi magyarországi határvidéki életforma, a végvári harcok ikonikus katonaalakját hívjuk segítségül[24] az oszmán török hadszervezet egyik pillére, a könnyű fegyverzetű, sokszor fegyelmezetlen könnyűlovas, az akindzsi személyében, aki mintegy ellentéte a képzett, fegyelmezett, reguláris janicsárnak.[25] A janicsár a háborúk központi

[22] A hódoltság kori magyarországi hadtörténet egyik klasszikusa Hegyi Klára, aki számos munkában dolgozta fel a problémakört. Például Hegyi Klára: *The Ottoman Military Organization in Hungary. Fortresses, Fortress Garrisons, and Finances.* Belin, Klaus Schwartz Verlag, 2018.

[23] Vö. Florian J. Egloff: *Cybersecurity in the Age of Privateering.* Oxford, Oxford University Press, 2015.

[24] A téma bőséges szakirodalmában máig alapmunka Caroline Finkel: *The Administration of Warfare: the Ottoman Military Campaigns in Hungary, 1593–1606.* Wien, VWGÖ, 1988.

[25] Ágoston Gábor: *The Last Muslim Conquest. The Ottoman Empire and Its Wars in Europe.* Princeton, Princeton University Press, 2021.

alakja; a „száguldó és égető" akindzsi viszont a hosszú „se nem béke, se nem háború" időszakok, a szürkezóna harcosa.

16–17. századi geopolitikai élet-halál harc és az oszmán hadművészet

A történelmünkben jól ismert 150 évnyi időszak, a hódoltság, a végvári harcok kora tulajdonképpen egy generációkon átívelő „határvidéki világot" teremtett meg a korabeli Magyar Királyság jókora részén.[26] Háború (a kor fogalmai és a mi kategóriáink szerint) csupán rövid időszakokra lángolt fel; a hosszú századok idejének zömében „béke" uralkodott itt, vagy pontosabban: „nem háború". A 100–130 erősségből álló török peremvonallal ugyanennyi magyar vár nézett szembe. Az őrség védelméből gyakran csaptak ki a könnyűlovas akindzsik. Feladatuk hármas volt: állandó felderítéssel segítették a saját oldalukat (hírszerző funkció); időről időre összecsaptak az ellenség kisebb alakulataival (erőlekötő és figyelemelterelő funkció), végül pedig folyamatosan nyugtalanították, zaklatták az ellenfél civiljeit (lélektani hadviselési funkció). Az irreguláris harcmodor mesterei voltak. Nem a háború eszközei voltak (többnyire a szürke „nem háborús" időkben portyáztak), nem az ellenfél legyőzése, hanem annak meggyengítése, elbizonytalanítása volt a küldetésük.

Irregulárisok a kibertérben: a „szürkezóna" hadműveletei

Visszakanyarodva a jelenbe: az Ukrajnában zajló konfliktus egyfajta iskolapéldája annak az újfajta harcmodornak, amely az utóbbi években sokfelé jellemzi a geopolitikai szembenállások új világát.[27] Olyan komplex konfliktusrendszereknek vagyunk tanúi, ahol eszközök és alkalmazási módok sokasága keveredik. Hagyományos háború jellegű fegyveres harc; propagandára és dezinformációra építő információs hadviselés; a másik fél informatikai rendszereinek megzavarását, blokkolását célzó kiberakciók; pénzügyi-kereskedelmi korlátozások és szankciók. Sokfajta és különböző intenzitású eszközt és eljárást vetnek be a szemben álló felek, akár egy időben is.[28] Ez a hibrid háború, amelyet a hagyományos fegyveres harc fogalmaival sokszor értelmezni is nehéz. A nyugati szakirodalom az úgynevezett „szürkezónás" *(grey*

[26] Vö. Ágoston Gábor – Bruce Masters (szerk.): *Encyclopedia of the Ottoman Empire.* New York, Facts on File, 2009. A kitűnő általános összefoglaló a társadalmi-politikai kontextus mellett a hadszervezésre is jó forrás.

[27] Sacha-Dominik Bachmann – Hakan Gunneriusson: Hybrid Wars: the 21st-century's New Threats to Global Peace and Security. *Scientia Militaria, South African Journal of Military Studies,* 43. (2015), 1. 77–98. Egyben jó bemutatása a hibrid háború és az úgynevezett szürkezónás műveletek összefüggésének.

[28] A hibrid hadviselésen belüli kiberkomponensek kapcsolódási pontjai mellett az utóbbiak „hadjáratformáló" szerepét emeli ki Florian J. Egloff – Lennart Maschmeyer: Shaping Not Signaling:

zone) hadviselésről is beszél: arról a posztmodern világunkra jellemző se nem háború, se nem béke állapotról, ahol az ellenfél elbizonytalanítását, meggyengítését, szándékainak és lehetőségeinek kifürkészését célzó akciók vannak túlsúlyban. Erre a célra pedig (az információs hadviseléssel kombinálva) különösen alkalmasnak látszanak a kiberfegyverek. Annál az egyszerű oknál fogva, hogy a digitalizáció által szinte átitatott társadalmaink biztonsága és magabiztossága épül ma már éppen azokra a technológiákra, amelyeket könnyűszerrel vehetnek célba ezek a (halált, fizikai pusztulást nem, de fennakadást, zűrzavart, bizonytalanságot, félelmet okozó) újszerű fegyverek. Tehát a társadalmakat megbénító, térdre kényszerítő, távolról vezérelt „kiberháború" koncepciója talán túlzó rémkép.[29] De a kiberfegyverek veszélyessége nagyon is valóságos.

Proliferáció – a digitális tér „atomfegyverei" helyett a kiberterek „piszkos bombája"?

Ha egyszer majd sikerül az ukrajnai háború fegyveres részét lezárni, az még nem feltétlenül jelenti majd, hogy a szellemet vissza lehet tuszkolni a palackba. Az akciók és a fegyverzetek „társadalmasításával" újabb veszélyforrás is rászabadulhat a társadalmakra: a kiberfegyverzetek proliferációja, elterjedése. A háború sajátos kísérőjelenségeként egy „párhuzamos" kiberhadjárat is kibontakozott a hadműveletek első hetétől kezdve: nehezen beazonosítható magánosok (régóta ismert hackercsoportok, kiberaktivisták, illetve vélhetően egyéni „kiber-revolverhősök") egész serege kapcsolódott be az online terekben folyó küzdelmekbe. A különféle szervezett és magános hacktivisták mellé felzárkóztak az ukrán állam által szervezett „IT-hadsereg" emberei is. A számok természetesen ellenőrizhetetlenek, ám az ukrán források több százezres kiber-közreműködői „seregről" beszélnek. Az általuk bejelentett akciók jó részét sem erősítette meg senki. Ugyanakkor ezek a kiberszabadcsapatok ténylegesen ellenőrizhető támadásokat is szép számmal hajtanak végre. Ezek egy része különösebb szakértelmet, szofisztikáltságot (illetve erőforrásokat) nem igénylő, túlterheléses támadás (DDoS), vagy főleg a kezdeti időkben egyszerű webhelyelcsúfítás *(defacing)* volt. Viszonylag hamar megjelentek az adatszivárogtatásos akciók, majd az adattörlések is, a szakemberek véleménye szerint azonban ezek a megmozdulások általában semmiféle komoly fennakadást, kárt vagy sérülést nem okoznak a megtámadott félnek, ez az első napokban döntően az orosz állami és gazdasági szervezetek köréből kikerülő intézményeket jelentette. Időközben aztán a kibertér eme betyárcsapatai

Understanding Cyber Operations as a Means of Espionage, Attack, and Destabilisation. *International Studies Review,* 23. (2021), 3. 997–998.

[29] A megállapítás mellett a gyakorló kibervédelmi szakma jeles képviselői is kiálltak, méghozzá az Ukrajna elleni orosz invázió időszakában rögzített esetekre alapozva. Vö. William Turton: Mandiant Executive Cautions against Russia-Cyberattack Panic. *Bloomberg,* 2022. február 15.

között megjelentek az Oroszországot támogató és az ukrán állami és gazdasági szervezeteket támadó „alakulatok" is. Az ő esetükben is többnyire igaz: ténykedésük inkább csak felszínes zaklatásnak tekinthető.[30]

Fegyverek helyett normák: a kibertér deeszkalálásának kísérletei és esélyei

A kibertérben zajló, egyre intenzívebb, egyre nagyobb károkat okozó akciók magas szintre emelték az ilyen incidensek nemzetbiztonsági kockázatát. Ezért aztán erősödnek a törekvések – nemzetállami szinten és a nemzetközi közösségben is – a kibertérben való működés, a támadó kiberakciók szabályozására.

A kibertér, a látszat ellenére, nem valamiféle „technológiai Vadnyugat". Léteznek normák, jól kigondolt, világos szabályok az itt zajló konfliktusokra, a követendő vagy tiltott magatartásokra. A nyugati szövetség tagjai például közös szabályrendszert dolgoztak ki a kiberháborús helyzetek szabályozására. A Tallini kézikönyvekhez hasonló normarendszereken dolgozik az országok jóval szélesebb körét átfogó ENSZ is.[31] Az összes ilyen jogi eszköz gyenge pontja viszont az, hogy ezek nem kényszerítő erővel bíró megállapodások.

A digitális terekben elmérgesedő helyzet ugyanakkor valamiféle megegyezés kényszerét is magában hordozza. A geopolitikai rivalizálás szemben álló pólusai ebben a tekintetben is más koncepciót vallanak magukénak. Amíg az oroszok és a kínaiak a támadó szoftverek szabályozására fókuszálnának, az amerikaiak konzekvensen elutasítják az ilyesfajta „kiberfegyverzet-korlátozási megállapodás" gondolatát. Mint mondják, az eredendően kettős rendeltetésű kibereszközök világában ez lehetetlen feladat lenne. Noha van ebben egy adag igazság, nem indokolatlan annak a feltételezése sem, hogy az USA nem szívesen korlátozná magát ezen a kulcsfontosságú harcmezőn. Az amerikai megközelítés, ennek megfelelően, nem a kibertér fegyverzeteinek, hanem inkább a támadható célpontoknak a körét szeretné szabályozni, korlátozni.

Az ezen a téren Biden és Putyin tárgyalásai nyomán 2021-ben megindult lassú egyezkedés a konfrontatív attitűd felülkerekedése, majd az ukrajnai konfliktus elmérgesedése miatt megtorpant. A kedvezőtlen kilátások ellenére bizakodásra késztetnek viszont a háború eddigi eseményei: az, hogy semelyik fél sem vállalkozott arra, hogy pusztító támadást indítson a másik kritikus infrastruktúrái ellen.

[30] A kiberfegyverek illegális terjedésével kapcsolatban a nemzetközi rendőri vezetők már megkongatták a vészharangot. Vö. Ryan Browne: Military-Made Cyberweapons Could Soon Become Available on the Dark Web, Interpol Warns. *CNBC,* 2022. május 23.

[31] A kiberdiplomáciai törekvések számunkra érdekes európai dimenzióját összegzi Molnár Dóra: *Törékeny nagyhatalmiság: a kiberbiztonság. Az európai kibertér brit, német és francia szegmensei.* Budapest, Nemzeti Közszolgálati Egyetem, 2018.

Egyszerűen megfogalmazva: ahogy a fizikai hadszíntéren is óvakodnak attól, hogy háborús oknak tekinthető gesztusokat tegyenek, a kibertérben sem ragadtatják el magukat ilyen végzetes lépésre. A kibertér talán mégsem a háború közege.

Felhasznált irodalom

Ágoston, Gábor: *The Last Muslim Conquest. The Ottoman Empire and Its Wars in Europe.* Princeton, Princeton University Press, 2021.

Ágoston, Gábor – Bruce Masters (szerk.): *Encyclopedia of the Ottoman Empire.* New York, Facts on File, 2009.

Arquilla, John – David Ronfeldt: Cyberwar Is Coming! *Comparative Strategy,* 12. (1993), 2. 141–165.

Bachmann, Sacha-Dominik – Hakan Gunneriusson: Hybrid Wars: The 21st-century's New Threats to Global Peace and Security. *Scientia Militaria, South African Journal of Military Studies,* 43. (2015), 1. 77–98. Online: http://dx.doi.org/10.2139/ssrn.2506063

Benson, David: Not Cyberwar, but Cyberbalance. *Aether. A Journal of Strategic Airpower and Spacepower,* 1. (2022), 2. 81–96.

Biddle, Tami Davis: *Rhetoric and Reality in Air Warfare.* Princeton, Princeton University Press, 2002.

Browne, Ryan: Military-made Cyberweapons Could Soon Become Available on the Dark Web, Interpol Warns. *CNBC,* 2022. május 23. Online: www.cnbc.com/2022/05/23/military-cyber-weapons-could-become-available-on-dark-web-interpol.html

Egloff, Florian J.: *Cybersecurity and the Age of Privateering.* Oxford, University of Oxford, 2015.

Egloff, Florian J. – Lennart Maschmeyer: Shaping Not Signaling: Understanding Cyber Operations as a Means of Espionage, Attack, and Destabilisation. *International Studies Review,* 23. (2021), 3. 997–998. Online: https://doi.org/10.1093/isr/viaa086

Finkel, Caroline: *The Administration of Warfare: the Ottoman Military Campaigns in Hungary, 1593–1606.* Wien, VWGÖ, 1988.

Gartzke, Erik: The Myth of Cyberwar. *International Security,* 38. (2013), 2. 41–73.

Harknett, Richard J. – Max Smeets: Cyber Campaigns and Strategic Outcomes. *Journal of Strategic Studies,* 45. (2022), 4. 1–34. Online: https://doi.org/10.1080/01402390.2020.1732354

Hegyi, Klára: *The Ottoman Military Organization in Hungary. Fortresses, Fortress Garrisons and Finances.* Berlin, Klaus Schwarz Verlag, 2018.

Hippler, Thomas: *Bombing the People. Guido Douhet and the Foundations of Air Power Strategy, 1884–1939.* Cambridge, Cambridge University Press, 2013.

Kostyuk, Nadiya – Erik Gartzke: Why Cyber Dogs Have Yet to Bark Loudly in Russia's Invasion of Ukraine. *Texas National Security Review,* 5. (2022), 3. 113–126. Online: http://dx.doi.org/10.26153/tsw/42073

Kostyuk, Nadiya – Yuri M. Zhukov: Invisible Digital Front: Can Cyber Attacks Shape Battlefield Events? *Journal of Conflict Resolution,* 63. (2017), 2. 1–44. Online: https://doi.org/10.1177/0022002717737

Kovács László – Krasznay Csaba: Digitális Mohács 2.0: kibertámadások és kibervédelem a szakértők szerint. *Nemzet és Biztonság,* 10. (2017), 1. 3–16.

Lawson, Sean – Michael Middleton: Cyber Pearl Harbor: Analogy, Fear, and the Framing of Cyber Security Threats in the United States, 1991–2016. *First Monday,* 24. (2019), 3–4. 1–24.

Martin, Ciaran: Cyber Realism in a Time of War. *Lawfare Blog,* 2022. március 2. Online: www.lawfareblog.com/cyber-realism-time-war

Maschmeyer, Lennart: *Slow Burn. Subversion and Escalation in Cyber Conflict and Covert Action.* Toronto, University of Toronto, 2020.

Maschmeyer, Lennart: The Subversive Trilemma: Why Cyber Operations Fall Short of Expectations. *Journal of International Security,* 46. (2021), 2. 51–90. Online: https://doi.org/10.1162/isec_a_00418

Maschmeyer, Lenart: A New and Better Quiet Option? Strategies of Subversion and Cyber Conflict. *Journal of Strategic Studies,* 2022. július 27. Online: https://doi.org/10.1080/01402390.2022.2104253

Molnár Dóra: *Törékeny nagyhatalmiság: a kiberbiztonság. Az európai kibertér brit, német és francia szegmensei.* Budapest, Nemzeti Közszolgálati Egyetem, 2018.

Overy, Richard: *The Bombers and the Bombed. Allied Air War over Europe, 1940–1945.* New York, Viking, 2015.

Reasoning by Analogy in Cyberspace. Deadly Balloons and Avoiding Digital Doom. *CFR's Blogs,* 2017. december 18. Online: www.cfr.org/blog/reasoning-analogy-cyberspace-deadly-balloons-and-avoiding-digital-doom

Rid, Thomas: *Cyber War Will Not Take Place.* Oxford, Oxford University Press, 2013.

Sharma, Amit: Cyber Wars: A Paradigm Shift from Means to Ends. *Strategic Analysis,* 34. (2010), 1. 67–73. Online: https://doi.org/10.1080/09700160903354450

Smeets, Max: A Matter of Time: On the Transitory Nature of Cyberweapons. *Journal of Strategic Studies,* 41. (2018), 1–2. 6–32. Online: https://doi.org/10.1080/01402390.2017.1288107

Sulek, David – Ned Moran: What Analogies Can Tell Us About the Future of Cybersecurity. In Christian Czosseck – Kenneth Geers (szerk.): *The Virtual Battlefield. Perspectives on Cyber Warfare.* Amsterdam, IOS Press, 2009.

Turton, William: Mandiant Executive Cautions Against Russia-Cyberattack Panic. *Bloomberg,* 2022. február 15. Online: www.bloomberg.com/news/articles/2022-02-15/mandiant-executive-warns-of-cyber-panic-we-need-to-get-a-grip

Ukrainian President Speaks Amid Russian Invasion; Troop, Military Vehicles Enter Ukraine from Belarus; Ukraine Hit by Wave of Cyberattacks as Invasion Begins. Aired 4:30-5a ET. *CNN.com – Transcripts,* 2022. február 24. Online: https://transcripts.cnn.com/show/cnr/date/2022 -02-24/segment/22

Valeriano, Brandon – Ryan C. Maness: *Cyber War versus Cyber Realities. Cyber Conflict in the International System.* Oxford, Oxford University Press, 2015.