13. fejezet

Következtetések a következő évtizedre

Molnár Dóra

Bevezetés

Az elmúlt évszázadban az emberi civilizáció drasztikusan megváltozott, és ezek a változások visszatükröződnek a hadviselésben alkalmazott stratégiákban és taktikákban is. A hadviselés jellemzője, hogy mindig is ember által irányított tevékenység volt, és ez a jövőben is így lesz. Még ha robotok is fogják uralni a harcteret, a humán tényező mindig fontos szerepet fog játszani a döntéshozatal és az irányítás folyamatában. A hadviselés ugyanakkor soha nem lesz kiszámítható, ezért a jövőbeli fejlemények előrejelzésére tett minden kísérlet valószínűleg csak korlátozott sikerrel járhat. Inkább kérdéseink vannak, semmint biztos válaszaink. Olyan kérdések, mint: a kibernetikai műveletek vajon elérik-e, elérhetik-e kitűzött céljaikat? Vagy: milyen kockázatokkal jár az eszkaláció? Vagy: milyen körülmények között vezethetnek az egyre gyakoribb és kifinomultabb kibertevékenységek akaratlan eszkalációhoz és katonai erő alkalmazásához?

Az utóbbi évtizedekben azt láthattuk, hogy a nagyhatalmi verseny egyre inkább magában foglalja a rivális államok közötti kibertevékenységeket is abban a kibertérben, amelyben a háború törvényei tisztázatlanok. Olyannyira, hogy egyenesen naivitásnak tűnik azt gondolni, hogy a nemzetközi közösség belátható időn belül széles körű konszenzusra jut a kiberhadviselés szabályait illetően, vagy azzal kapcsolatban, hogy a jelenlegi, a nemzetközi humanitárius jogra vonatkozó normák alkalmazhatók-e, és ha igen, hogyan, a kibertérre. S adódik a költőinek tűnő kérdés: egyáltalán érdekelt-e bármelyik fél a kiberhadviselés szabályozásában? Nem véletlenül fogalmazott úgy Barack Obama, az Egyesült Államok 44. elnöke 2015-ben, hogy a kibertér jelenleg egyfajta vadnyugat.[1]

A kibertér nemcsak felforgatta a politikai határokat, hanem megrendítette az államok számára keretet adó vesztfáliai rendszer gyökereit is. A földrajzi

[1] The White House: *Remarks by the President at the Cybersecurity and Consumer Protection Summit.* Stanford (CA), Stanford University, 2015. február 13.

https://doi.org/10.36250/01079_13

https://orcid.org/0000-0002-1476-5253

határok hiánya és a látszólagos átláthatatlanság a hadviselés ezen ötödik területén lehetővé tette, hogy a rosszindulatú nem állami szereplők sokasága biztonsági fenyegetésként legyen jelen. Ebben a térben a hírszerzés és az adatlopás láthatatlan, az információs kampányokat nem mindig lehet azonosítani, és gyakran a szabotázs sem különböztethető meg a balesetektől. A kibertérben kialakuló új konfliktusok sohasem fognak hasonlítani a múltbéli vagy a jelenlegi konfliktusokra. Olyan időket élünk, amikor azt sem tudjuk, hogy mikor kezdődik, és mikor végződik egy kibertámadás, béke van-e, vagy virtuális háború zajlik…

Ilyen viszonyok között vállalkozik ez a fejezet arra, hogy prognózisba bocsátkozzon a jövő kiberháborúját illetően. Ehhez először a nemzetállamok lépéseinek mögöttes mozgatórugóit kell megérteni, ugyanis ezek lényegében olyan prizmák, amelyeken keresztül láthatjuk, hogyan hajtják végre jövőbeni lépéseiket. Ez a gondolkodásmód az egyes állami politikákban és stratégiákban tükröződik. A kiberháborúkat meghatározó másik alapvető kérdés az új technológiák köre, amelyeket előbb-utóbb háborús céllal is használni fognak. Általánosságban elmondható, hogy a jelenlegi stratégiák túlzottan a technológiai kérdésekre és a nemzeti ellenállóképesség megteremtésére összpontosulnak, a normatív magatartás kialakulását elősegítő értékteremtés rovására. Tekintettel a nemzetek előtt álló kiberbiztonsági kihívások nagyságrendjére, a kibertér geopolitikai jövőjének mérséklésére irányuló nemzetközi konszenzus hiányára és arra, hogy az értékek érvényesítésének összehangolt törekvése hiányzik a kiberbiztonsági stratégiákból, sokat kell még tenni ahhoz, hogy a kibertérben békés viszonyok uralkodjanak. Az eddigi kibertér a politikai háborúskodás és a kényszerdiplomácia területe volt, és ha az államok nem változtatnak jelenlegi gyakorlatukon, akkor könnyen tényleges csatározások színterévé válhat.

A kibertér mint kiindulási pont és a kiberkonfliktusok

A jövő kiberbiztonságával kapcsolatban, még ha számos nyitott kérdés is akad, egy kérdést biztosan meg tudunk válaszolni: a kiberakciók és interakciók színterét, amely nem más, mint a kibertér.[2] A kibertér legfőbb jellemzőit ezért

[2] E közös tér elnevezése azonban nem egységes. Vannak államok, ahol több okból kifolyólag inkább az információs tér vagy digitális tér kifejezést használják, ilyen például Németország is. Erről részletesebben lásd Molnár Dóra: Kiberbiztonság Németországban. Pillanatkép a német digitális térről. *Nemzet és Biztonság,* 11. (2018), 1. 142–156.

érdemes közelebbről is megvizsgálni, ugyanis az ebben a speciális közegben zajló folyamatokat ezek az alapvető tulajdonságok nagymértékben determinálják. A kibertér számos jellemzője közül az alábbi öt az, amely a jövő kiberkonfliktusaival szoros összefüggésben állhat:[3]

1. A kibertér egyrészt – némiképp meglepő módon – egyben fizikai tér is. Ennek oka részben az, hogy az információ, amely keresztülhalad a kibertéren, a fizikai infrastruktúrában gyökerezik, amely létrehozza, majd tárolja az adatokat; részben pedig az, hogy a fizikai infrastruktúra (amelynek egyébiránt a kibertér létrejötte is köszönhető) általában a fizikai államhatárokon belül található. Amellett azonban, hogy a kibertér fizikai tér, egyben logikus térnek is nevezzük, mert az áthaladó információ egyeztetett útválasztási protokollokon megy keresztül. E kettőség az oka annak, hogy a történelemben ez idáig vagy széles körű, de időben korlátozott kibertámadásokat láthattunk, vagy elhúzódó, de kisebb hatást elérő támadásokat, és olyan támadás még nem volt (talán a SolarWinds-esetet leszámítva), amely huzamosabb időn át képes volt jelentős hatást elérni. A fizikai és logikai attribútumok ezen egyedi szintézise két fontos megállapításhoz vezethet. Egyrészt valamely fizikai tér tényleges részvétele nélkül nehezen képzelhető el egy, pusztán a kibertérben zajló nagyobb összecsapás, másrészt pedig támadó műveletek esetén azt jelenti, hogy azok bár gyorsan átlépik a határokat, azonban az elért hatások sokkal nagyobb valószínűséggel lesznek visszafordíthatók, mint más típusú katonai támadások esetén.
2. A kibertér domináns szereplője a magánszektor, amely nemcsak birtokolja, üzemelteti és irányítja a hálózatokat, hanem nagymértékben függ is az alapul szolgáló hálózatoktól és információtól. Ráadásul ez a kitettség a jövőben csak fokozódni fog. Kérdéseket vet fel, hogy kiberháború esetén milyen szerepet játszhat a hagyományos háborúk megvívásának főszereplője, az állam, és az állami szerepvállalás hogyan egyeztethető össze a magánszektor tevékenységével és érdekeivel, ezen műveletek koordinációja miként valósítható meg.
3. A kibertér további jellemzője, hogy taktikai szinten gyorsan reagál, de működését tekintve mégis lassú. Ennek oka, hogy bár az egyedi

[3] *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy.* Washington (DC), National Research Council, The National Academies Press, 2010. 78.

kiberakciókat gyorsan véghez lehet vinni, azonban valamennyi támadás tervezési ciklusa egy adott katonai hatás elérése érdekében ennél jóval hosszabb, és a kívánt hatás elérése sem azonnal következik be.

4. A kibertérben a támadás amolyan *primus inter pares* lehet a védelemmel összevetve. Ennek hátterében az áll, hogy gyakran nehéz különbséget tenni támadó és védekező jellegű lépés között, és egy alapvetően védelmi jellegű hozzáállás is támadónak tűnhet a szemben álló fél nézőpontjából. (Erről a kérdéskörről, valamint a védelem szerepéről a fejezet alább részletesen szól.)
5. A kibertér markáns jellemzője, hogy tele van bizonytalansággal. Ez következik a célok és a dinamika elégtelen ismeretéből, a lépcsőzetes hatások bizonytalanságából, valamint abból, hogy egy rendkívül összetett és gyorsan változó közegről van szó, ahol a változás irányát igen nehéz megjósolni. Ez a jellemző a jövő kiberháborújával kapcsolatos feltételezéseket nagymértékben determinálja.

A változás irányának előrejelzése nemcsak a kibertér jellemzőire vonatkozóan jelent kihívást, hanem a kibertérbeli viszonyok jövőbeli alakulását illetően is. Abban egyetértés mutatkozik, hogy a kibertér ma ellenséges környezet. Jól tükrözik ezt nemcsak a nemzetállamok kiberképességei, hanem az is, hogy a legtöbb vállalat és kormány rendelkezik biztonsági műveleti központokkal (*Security Operation Center:* SOC). Bár nem valószínű, hogy a kibertér ellenséges mivoltában a következő tíz évben változás állna be, azt mégsem zárhatjuk ki. Ez esetben 2030-ra egy hálózatvédelmi és hálózatirányítási mesterségesintelligencia-algoritmus olyannyira csökkentené a kiberkockázatokat, hogy kitörne a kiberbéke. Jelen állás szerint mégis az a forgatókönyv tűnik valószínűbbnek, hogy 2030-ra a világ már megvívta vagy éppen vívja az első kiberháborút: egy olyan hipersebességű háborút, amely kiterjedt nemzetállami támadásokat tartalmaz egymás kritikus infrastruktúrája ellen, beleértve a távközlést, a csővezetékeket, a pénzügyi rendszereket, valamint az elektromos áramtermelő és átviteli hálózatokat. Ha abból indulunk ki, hogy az ember veleszületett jellemzője a versengés és a túlélésért folytatott küzdelem, akkor elkerülhetetlennek látszik ez utóbbi szcenário bekövetkezte.

De ne szaladjunk ennyire előre, ugyanis a háború mindig a legmagasabb intenzitású konfliktus, amelyet általában egyéb, alacsonyabb intenzitású tevékenységek előznek meg! Ezek között a kibertérben több olyat is nevesíthetünk, amelyben a katonai elem domináns szerepet játszhat, és amellyel a jövőben reá-

lisan számolni kell.[4] A *kiberellenes tevékenységek (counter cyber)* az integrált védekező és támadó műveletek olyan átfogó kategóriája, amelyek célja a kívánt mértékű kiberfölény elérése és megtartása. A *tiltó műveletek (cyber interdiction)* az ellenség katonai kibernetikájának elterelésére, megzavarására, késleltetésére vagy megsemmisítésére irányuló akciókat jelentik, még mielőtt azokat a képességeket hatékonyan felhasználhatnák a baráti erők ellen vagy más módon céljaik eléréséhez. A *közeli kibertámogatás (close cyber support)* az olyan ellenséges célpontok elleni tényleges fellépést jelenti, amelyek a baráti erők közvetlen közelében találhatók, és veszélyeztetik az integrált kibermissziók sikerességét. Az eddigi művelettípusok inkább a védelmi műveletek körébe sorolhatók, szemben a továbbiakkal, amelyek már egyértelműen támadó szemléletűek. A *harcoló erők általi kiberfelderítés (cyber reconnaissance in force)* egy olyan katonai (és nem hírszerzési) támadó kiberműveletet jelent, amelynek célja az ellenség erejének felderítése vagy tesztelése vagy egyéb információk megszerzése. Az *ellenséges kibervédelem elnyomása (supression of enemy cyber defences)* olyan tevékenység, amely semlegesíti, megsemmisíti vagy ideiglenesen rontja az ellenséges kibervédelmet romboló és/vagy zavaró eszközök segítségével. S végül a *stratégiai kiberművelet (strategic cyber mission)* egy vagy több kiválasztott ellenséges kibercélpont ellen intézett széles körű támadás, amelynek célja a fokozatos pusztítás, valamint az ellenség háborúmegvívási képességének és akaratának megtörése. Ezek a műveletek tehát azok, amelyekkel a jövőben minden bizonnyal fogunk találkozni, egyes típusok esetében minden bizonnyal nagy számban.

A bevezető gondolatok zárásaként érdemes kitérni a kibertérben zajló műveletek funkcióira, amelyek közül az Egyesült Államok katonai doktrínája hármat nevesít: a támadó és a védekező kiberműveleteket, valamint a Védelmi Minisztérium információs hálózati műveleteit.[5] A doktrína értelmében a támadó kiberműveletek *(offensive cyber operations)* „célja az erő kivetítése erő alkalmazásával a kibertérben vagy azon keresztül”.[6] (A 2019-ben felállított Solarium Kibertér

[4] A részletes definíciókat lásd *Joint Publication 1-02 (JP 1-02): Dictionary of Military and Associated Terms*. Washington (DC), Department of Defense, 2019. október.

[5] *FM 3-38 Cyber Electromagnetic Activities*. Department of the Army HQ, 2014. február.

[6] *US Military Doctrine.*

Bizottság[7] is megismétli ezt a definíciót a 2020. március 11-i jelentésében.)[8] A szárazföldi erők ilyen támadó kiberműveleteket a katonai műveletek teljes spektrumában végeznek az ellenség, valamint az ellenséges tevékenységek és kapcsolódó képességek ellen a kibertérben és a kibertéren keresztül, azzal a céllal, hogy a parancsnok szándékát és céljait támogassák. Érdekes álláspontot képvisel ezzel szemben az Ausztrál Stratégiai Politikai Intézet, amely a támadó kiberműveletek és a támadó kiberképességek fogalmát szinonimaként használja.[9] A jövő zenéje még, hogy azon országok, amelyek támadó kiberképességekkel rendelkeznek, ténylegesen hogyan fogják e képességeiket a műveletek során is offenzív céllal használni, az azonban szinte bizonyos, hogy a két fogalom más jelentéssel bír. Ami a képességeket illeti, jelenleg 23 ország bizonyítottan is rendelkezik támadó kiberképességekkel, míg további 30 ország valószínűsíthetően.[10] (Magyarország is ez utóbbi körbe tartozik.)

Támadó kiberműveletek – kiberháború?

Leegyszerűsítve azt mondhatnánk, hogy minden kiberháború támadó kiberművelet, de nem minden támadó kiberművelet kiberháború. A kiberháborúnak ugyanis vannak olyan ismérvei, amelyeknek más támadó kiberművelet nem felelnek meg. Érdemes tehát megvizsgálni az egyes kategóriák közötti különbségeket, mert a jövőben ezekkel a fogalmakkal várhatóan sokkal gyakrabban fogunk találkozni, mint manapság.

Az egyes műveletek elhatárolásához a brit Nemzeti Kiberbiztonsági Központ egykori igazgatója, Ciaran Martin által felvázolt tipológiából indulunk ki, amely egy ötfokozatú skálán helyezi el a kiberműveleteket. A skála egyes elemeinek kezdőbetűi után ezt HACKS-struktúrának is nevezhetjük.[11] A HACKS-modell

[7] A Bizottságot (*Cyberspace Solarium Commission:* CSC) az Egyesült Államok Kongresszusa állította fel 2019-ben azzal a céllal, hogy konszenzust alakítson ki a jelentős következményekkel járó számítógépes támadásokkal kapcsolatban: hogyan lehet és kell megvédeni az Egyesült Államokat a kibertérben?

[8] *US Solarium Cyberspace Commission Report.* 2020. március. 36–144.

[9] Tom Uren – Bart Hogeveen – Fergus Hanson: *Defining Offensive Cyber Capabilities*. Australien Strategic Policy Institute, 2018. július 4.

[10] Digwatch: *UN GGE and OEWG*. 2021.

[11] Martin Ciaran: *Cyber-Weapons Are Called Viruses for a Reason: Statecraft and Security in the Digital Age.* London, King's College, 2020. november.

azért lehet különösen hasznos, mert egyrészt kiemeli az adott támadás súlyosságának spektrumát, másrészt pedig lefed valamennyi jövőbeni támadó kiberműveletet. Ahogyan haladunk a skálán felfelé, úgy találkozunk egyre kevesebb ténylegesen is megvalósult művelettel. A struktúra legalsó szintjén a hekkelés *(hacking)* található, ez nem más, mint konkrét nemzetvédelmi célok elérése érdekében folytatott számítógépes művelet, amely révén a beavatkozó hozzáférést szerez az ellenfél elektronikus eszközeihez. A második szint az ellenséges infrastruktúra megsemmisítése *(adverserial infrastructure destruction),* amely az ellenséges digitális infrastruktúra célzott megsemmisítését jelenti.[12] Széles körben ismert eset és jó példa erre az amerikai kiberparancsnokság, a Cyber Command 2018-as művelete az Internetes Kutatási Ügynökség szentpétervári trollgyárának infrastruktúrája ellen. A harmadik szintet az ellenhatás-műveletek *(counter-influencing)* alkotják, amelyek lényegében a támadó kiberműveletek elrettentéscélú alkalmazását foglalják magukban. Más szóval utóbbiakat nevezhetjük digitális zaklatásnak is, ennek jellemzője, hogy általában fedett műveletek képezik, passzívak (legalábbis kezdetben), és nem semmisítenek meg vagy rombolnak infrastruktúrát. A negyedik szint a *„kinetikus" támadás,* olyan offenzív kibernetikai művelet, amely jelentős kárt és fennakadást okoz az adott ország infrastruktúrájában (például megzavarja a város áramellátását, vagy kikapcsolja a televíziós hálózatot). Tehát itt már nemcsak az adott fenyegetés megszakítása a cél, hanem azon túl, mintegy válaszként, a tényleges károkozás. Bár kinetikus támadásra még kevés példát találunk, de a jövőben ezen esetek száma bizonyosan szaporodni fog. A példák közt említhetőek az orosz támadások: 2014-ben Oroszország hat órára lekapcsolta Kijev egyes részeinek áramellátását, majd egy évvel később a TV5 Monde francia televíziócsatorna működését bénította meg 11 órára. Végül az ötödik és egyben a legmagasabb szintet a rendszer egészére kiterjedő, katonai és polgári célpontok elleni *kibertámadások* jelentik fegyveres konfliktus során *(systems wide).* Ehhez hasonló, stratégiai szintű támadásra 2016-ban már majdnem sor került, amikor az amerikai Kiberparancsnokság Nitro Zeus néven széles körű támadást tervezett Irán ellen, ám az végül idő előtt kitudódott.[13] A kérdés tehát nem az, hogy sor fog-e kerülni ilyen kibertámadásra, hanem az, hogy mikor.

[12] Ez lényegében egybeesik az amerikai „kitartó elkötelezettség" *(persistent engagement)* fogalmával.

[13] Matthias Schulze: Cyber in War: Assessing the Strategic, Tactical, and Operational Utility of Military Cyber Operations. *12th International Conference on Cyber Conflicts.* Tallinn, NATO CCDCOE Publications, 2020.

A *kiberháborúval* mindenképpen részletesen is foglalkozni kell, mert a jövő háborúinak az egyik, ha nem is kizárólagos színtere a kibertér lesz. Ugyanakkor már a kiberháború fogalmának használatakor kérdésekbe ütközünk, mert annak tényleges tartalmát illetően a mai napig nincs egyetértés a nemzetközi közösségben. Az alapvető kérdés, hogy a hagyományos háborúfogalom használható-e a kiberháború esetében. A dilemma létjogosultságát már az is jól jelzi, hogy míg a hagyományos háborúkat nemzetállamok vívták egymás ellen, addig a kibertérben számos olyan nem állami szereplő tett szert jelentős hatalomra, amely képes lehet a jövő háborújának megvívására. Ehhez kapcsolódó további kérdéskör az attribúció, azaz hogy az adott háborús cselekedet végrehajtását kinek lehet tulajdonítani. Eddig ugyanis a hagyományos háborúk során nem jelentett akadályt a háborúban részt vevő felek beazonosítása és nevesítése. A kibertérben azonban ez a kérdés is más értelmet nyer, és könnyen előfordulhat, hogy a jövő kiberháborúiban (de nem is csak a háborúkban, hanem alsóbb szintű támadó kiberműveletek esetében is) adott támadó cselekmények mögött pontosan meg nem határozható entitások állnak majd.

Sokan – köztük Colin Gray is – amellett érvelnek, hogy a kibertámadások különböznek a hagyományos háborútól, mert nem felelnek meg a háború clausewitzi definíciójának, amely szerint a háború erőszakos, eszközszerű és politikai erőhasználat.[14] Ezen vélemények hátterében az áll, hogy sok stratéga a kibernetikai képességeket pusztán eszközként, és nem új háborús eszközként kezeli. Ehhez azért az is hozzátartozik, hogy Gray a kiberteret nem tekinti a taktikai alkalmazás és a stratégia szempontjából nagymértékben különbözőnek az eddigi működési területektől.[15]

Ugyanakkor, ha a háború három szükségszerű elemének tartalmára tekintünk, ezeknek mai korhoz adaptált tartalma megfelelhet a kibertérbeli háborúk ismérveinek is. Valóban helytelen lenne azt állítani, hogy Clausewitz elképzeléseit nem kell a jelenlegi biztonsági légkörnek megfelelően módosítani, hiszen korszakalkotó hadtudományi műve megjelenése (1832) óta igen sok minden megváltozott – különösen a kiberfegyverek megjelenése, amely aláásta nemcsak a maximális erőhasználatra vonatkozó kívánalmat, hanem egyúttal előtérbe helyezte Szun-ce minimális erőre és megtévesztésre vonatkozó gondolatait is.

[14] Carl von Clausewitz szerint a háború a politika folytatása más eszközökkel. Lásd Carl von Clausewitz: *A háborúról.* I. kötet. Budapest, Zrínyi, 1961. 56.

[15] Colin S. Gray: *Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling?* Strategic Studies Institute, 2013. április 1.

Szun-ce ugyanis azt tartja a legügyesebb megoldásnak, ha harc nélkül sikerül legyőzni az ellenfelet – amely a kibertérben könnyen megtörténhet, hiszen hagyományos fegyveres erő alkalmazására nem is kerül sor, és a célok eléréséhez elég lehet minimális erőkifejtés. Ez a korlátozott erőhasználat rögtön elvezet bennünket az első fogalmi elemhez, az erőszakos erőhasználathoz. Maga Clausewitz, bár egyértelművé teszi, hogy az erő a háború sarkalatos pontja, soha nem számszerűsíti, hogy mekkora erő szükséges ahhoz, hogy adott cselekmény háborús cselekedetnek minősüljön. Clausewitz pusztán kijelenti, hogy maximális erő kívánatos a fölény eléréséhez (amelyhez érdemes rögtön hozzáfűzni azt, hogy ez a kibertérben nem alkalmazható, mert a fölény megszerzése valójában minimális erővel is elérhető). Önmagában az erőhasználat korlátozott mivolta tehát nem jelenti azt, hogy a háború ezen fogalmi eleme csorbát szenvedne a kiberháború esetében. Az „erőszak" és az „erő" kifejezés nem összemosandó. Bár az utóbbinál kiberháború esetén korlátozottan, az előbbi vonatkozásában az elért eredményből következtethetünk annak mértékére. Egy kiberháború ugyanis hatalmas károkat tud okozni, amelyeket nem feltétlenül emberéletekben lehet számszerűsíteni. A nyilvánvaló, fizikai vagyont érintő kár mellett itt gondolni kell a támadásoknak az emberek pszichés jóllétére gyakorolt hatására és így az okozott pszichés sérülésekre is.[16] A másik két fogalmi elem, tehát az erőhasználat eszközszerű jellege és politikai motivációja különösebb magyarázatot nem igényel, hiszen ezek kiberháború esetében is adottak.

Jelen pillanatban azonban még nehéz elképzelni egy olyan háborút, amely kizárólag a kibertérben zajlik, nincs fizikai kapcsolata az egyéb terekkel, és azokra (vagy a gazdaságra) nem gyakorol közvetlen hatást. A jelenleg egyre általánosabban elterjedt, a háborús szintet még el nem érő támadó kiberműveletek jelentősége abban áll, hogy a hagyományos hadviselési eszközök és módszerek hatékonyságát képesek megerősíteni, valamint a katonai kommunikációt észszerűsítik, stratégiai előnyt biztosítva ezáltal az államoknak. Ezért az ezen műveletekkel való foglalkozás legalább annyira fontos lesz a jövőben, mint a kiberháború kérdésköre.

A háborúknak három alapvető típusuk van az alkalmazott erők és eszközök alapján: a hagyományos, a nukleáris és a kiberháború.[17] E három típusnak hétféle kombinációja képzelhető el elméletben: egyetlen eszközfajtával megvívva a háborút (három eset), kétféle eszköztípust alkalmazva (három eset), és ha mindhármat

[16] Harriet Charlotte Turner: Cyber War Forthcoming: "It Is Not a Matter of If, It Is a Matter of When". *E-International Relation,* 2020. július 8.

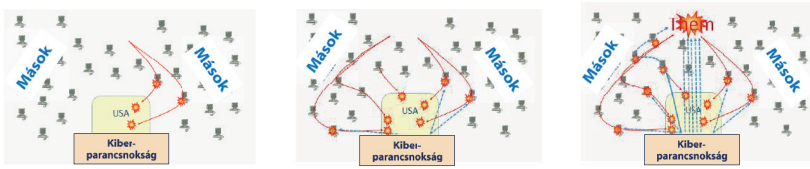
[17] *Proceedings of a Workshop…* (2010): i. m. 110.

egyszerre alkalmazzák. Ezek közül a kiberháború négy esetben juthat szerephez: ha más eszközök igénybevétele nélkül, pusztán kiberfegyverekkel vívják, ha párban áll vagy a hagyományos háborúval, vagy a nukleáris háborúval, vagy ha mindhárom típusú eszközt bevetik ugyanazon konfliktus során. Ezen kombinációk közül nem valószínű azok bekövetkezte, amelyekben a nukleáris erő jutna szerephez, és szintén nem várható, hogy kizárólag a kibertérben kibereszközökkel vívott háborúra kerülne sor. Ezért a legvalószínűbb, hogy a jövőben a hagyományos háborúknak lesz kibervetülete is. Az is kérdéses, hogy mely térben veszi kezdetét a konfliktus. Valószínűbb, hogy a kiberincidensek fognak elérni egy olyan háborús szintet, amely ellenségeskedést a felek hagyományos erők bevetésével a fizikai térben is folytatni fogják. Ugyanakkor nem kizárt a fordított sorrend sem: azaz a hagyományos háborúnak idővel lesz egy széles körű kibersíkja, kiegészítve a szárazföldi, légi vagy vízi műveleteket, és hozzájárulva azok sikeréhez – olyannyira, hogy akár egyes hagyományos elemeket kiberelemekre cserélhetnek le azok kisebb költségigénye és potenciálisan nagyobb hatékonysága okán.

Felmerülhet a kérdés, hogy milyen mögöttes motivációk mentén mehet végbe a jövő kiberháborúja.[18] Mindenekelőtt stratégiai megfontolások állhatnak az ilyen műveletek mögött, ami egyfajta nyomásgyakorlást jelent a másik fél akaratára és képességeire gyakorolt hatás elérése céljából. Műveleti oldalról közelítve a motiváció az ellenségeskedésben részt vevő ellenséges erők hagyományos, fizikai eszközeire hatást gyakorolni. Ezek mellett cél lehet az elrettentés, azaz egy másik állam azon szándékának letörése, hogy (kiber)támadást hajtson végre, valamint az aktív védelem is, amely olyan technikát jelent, amely korlátozza mások képességét kibertámadások végrehajtására, vagy segít a korábbi kibertámadásokat jellemezni és elkövetőit felderíteni. Végül speciális motivációkkal is találkozhatunk (a speciális műveletek analógiájára), amelyek bizonyos, időben és helyileg korlátozott hatások elérésére irányulnak, javarészt a fizikai küzdelem keretein kívül és általában titokban.

A kiberháborúk tényleges lefolyását illetően két, egymást részben fedő, részben kiegészítő megközelítés képzelhető el.[19] Haditechnikai oldalról közelítve: egy adott országot kibertámadás ér, amelyet a védekező fél ellentámadással megállít, és tovább védekezik az újabb esetleges támadásokkal szemben, visszaverve végül a támadást. Ezt a folyamatot szemlélteti az *1. ábra*.

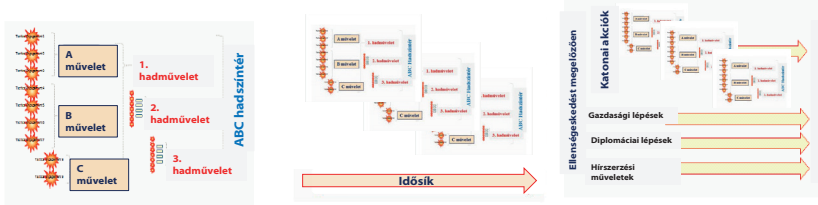
[18] Martin Libicki: Pulling Punches in Cyberspace. In *Proceedings of a Workshop…* (2010): i. m. 135.
[19] *Proceedings of a Workshop…* (2010): i. m. 96.



1. A támadás kezdete | 2. Védekezés, ellentámadás | 3. A támadás visszaverése

1. ábra: A kibertámadás haditechnikai vetülete
Forrás: Proceedings of a Workshop... (2010): i. m. 96.

A hagyományos hadviselés taktikai oldaláról nézve valószínűsíthető, hogy egy nagyszabású háború a kibertérben ugyanezt a sémát követné számos gyors, összekapcsolt (egymást követő vagy párhuzamos) támadással, amelyek mind részei egy nagyobb hadműveletnek – s akár nemcsak több hadszíntéren zajló műveletnek, hanem párhuzamosan gazdasági, diplomáciai és/vagy hírszerzési műveleteknek is.[20] Ezeknek a műveleteknek a vezetési-irányítási rendszere is nagyban eltér a hagyományos háborúkban alkalmazott megoldásoktól, köszönhetően annak, hogy virtuális cellákban kell gondolkodni. S míg a hagyományos műveletek esetén, ahol szükséges a fizikai jelenlét, egyszerre csak egy cellában tud ténylegesen ott lenni a harcoló katona, addig a kiberkatona egy időben több virtuális cellában is fogadni tudja az utasításokat.[21]



Egymást követő támadások | Párhuzamos támadások | Egyéb műveletek

2. ábra: A kibertámadás taktikai megoldása
Forrás: Proceedings of a Workshop... (2010): i. m. 97.

[20] *Proceedings of a Workshop...* (2010): i. m. 97.
[21] Norman R. Howes – Michael Mezzino – John Sarkesain: *On Cyber Warfare Command and Control Systems*. (H. n.), International Command and Control Institute, 2004.

A kiberháborúkkal kapcsolatosan azok befejezését illetően megállapíthatjuk, hogy az is nagyban eltér a hagyományos háborúkétól. Míg a fizikai háborúkban a békeszerződéseket gyakran követi egy- vagy többoldalú leszerelés, a leszerelés fogalma a kibertérben értelmezhetetlen, mivel a kiberháború sokkal inkább a sérülékenységekről szól, semmint a fegyverekről.[22]

Stratégiai gondolkodás a kiberháborúról

A kiberháború jövőjét meghatározó egyik alapvető tényező a nemzetállami gondolkodásmódban keresendő, amely az egyes állami stratégiákban ölt testet. A kibertér stratégiai szempontból jelenleg széttöredezett. Egyrészt Kína rohamos fejlődése és előretörése, másrészt számos más állam aktív – és egyre gyakrabban támadó jellegű – jelenléte miatt továbbra sem egyértelmű az Egyesült Államok dominanciája. Tekintettel arra, hogy a jövő háborújának jellemzőit nagymértékben fogja determinálni a stratégiai gondolkodás, röviden mindenképpen ki kell térni elsősorban az Egyesült Államok kibertérre vonatkozó stratégiai elképzeléseire, de nem mellőzhető a Kína és Oroszország egyre erőteljesebb lépései mögött megbújó gondolkodásmód ismertetése sem.

Az Egyesült Államok hosszú időn át a kiberháború hatásalapú megközelítésének híve volt.[23] Ennek értelmében nem az volt a fontos, hogy a hatás miként jön létre (kinetikus vagy kibernetikus síkon), hanem a cél, tehát hogy a kívánt hatást minden áron elérjék.[24] Ezen megközelítés ernyőjét az elrettentés koncepciója jelenti, amelyet az Egyesült Államok 2011 óta stratégiai szinten deklaráltan követ. Ezt a koncepciót először a kibertér nemzetközi stratégiájában *(Internations Strategy for Cyberspace)* rögzítették 2011-ben, majd 2015-ben a Védelmi Minisztérium is megerősítette azt. Az amerikai megközelítés szerint az elrettentés nem más, mint „a fellépés megakadályozása az elfogadhatatlan ellenintézkedések hiteles fenyegetésének puszta létezésével”.[25] Tehát az amerikai kibererő lényege, hogy az ellenfelek féljenek cselekedni Amerika ellen,

[22] Martin C. Libicki: *Cyberdeterrence and Cyberwar.* Santa Monica (CA), Rand Corporation, 2009. 135.

[23] Aaron Wright: The Future of Cyber Conflict. *The Cove,* 2020. augusztus 5.

[24] Jó példa erre a Stuxnet-támadás, amelyet katonai szempontból úgy terveztek meg, hogy járulékos károk nélkül érje el a kívánt hatást.

[25] *Joint Operations, 17 January 2017 Incorporating Change 1, 22 October 2018*. Joint Publications 3.0, 212.

tartva a megtorlástól. Az elrettentés alapját az erős védelem jelenti – szemben a hidegháború megtorlásalapú elrettentéskoncepciójával.

Az új évezredben az Egyesült Államok kiberpolitikája terrorcselekmények és kémkedési események árnyékában formálódott, aminek az lett a következménye, hogy a terület nagyban militarizálódott, és a Pentagon irányítása alá került.[26] Ezért normává vált a konkrét fenyegetések leküzdésére és a konkrét katonai műveletek támogatására irányuló politika. A jövőben e téren elképzelhető némi változás a magánszektor egyre dominánsabb jelenléte okán, azonban a katonai dominancia meg fog maradni – mert meg kell hogy maradjon a kibertér fokozatos militarizálódása miatt.

Az jelenleg nem kérdés, hogy technológiai szempontból az Egyesült Államok továbbra is a fejlesztés élvonalában áll hatalmas költségvetésének és a világ vezető magánszektorának köszönhetően, stratégiai szempontból azonban már nem olyan egyértelmű az amerikai dominancia. Az évtizedeken át alkalmazott hatásalapú megközelítést ugyanis az ellenfelek már kiismerték, és hatékonyan visszafordították az Egyesült Államok ellen 2013-tól kezdve – ahogyan az történt például a 2016-os elnökválasztásba történt orosz beavatkozás esetében. A 2018-ig eltelt öt évben az Egyesült Államok nem hajtott végre támadó kiberműveletet – ami nem azt jelenti, hogy a kibertérben Washington tétlenkedett volna, hanem azt, hogy ebben az időszakban ritkán vagy soha nem használta a kiberműveleteket nyílt válaszként vagy hatalmának rugalmasabbá tételére.[27] De felismerte, hogy lépnie kell, proaktívnak kell lennie.

Ezt az irányváltást jelezte 2018-ban a Trump-adminisztráció új nemzeti kiberstratégiája is.[28] A stratégiai irányváltás lényege, hogy az Egyesült Államok a pusztán taktikai hatások elérésétől az agresszívabb információs műveleti megközelítés felé kíván fordulni, azonban az, hogy ezt milyen lépések megtételével fogja megtenni, még erősen kérdéses.[29] Az elmozdulás első jele volt az egy hónappal később, 2018 októberében a Védelmi Minisztérium által kiadott kiberstratégia,[30] amely már új fogalomként az „előretolt védelem” *(defense forward)* koncepciót használja. Ennek lényege, hogy a Pentagon a külföldi hálózatokon

[26] Wright (2020): i. m.

[27] Marc Pomerleau: Two Years In, How Has a New Strategy Changed Cyber Operations? *C4ISRNet,* 2019a. november 11.

[28] Lásd *National Cyber Strategy of the United States of America*. 2018. szeptember.

[29] Kate Fazzini: Trump’s New Strategy Means the U.S. Could Get More Aggressive With Russia and China Over Hacking. *CNBC,* 2018. szeptember 21.

[30] *Department of Defense Cyber Strategy 2018*. (Summary.)

folyamatosan „munkálkodik" a támadások megelőzése érdekében, még mielőtt azok megtörténnének – tehát az ellenfél hálózataihoz és infrastruktúrájához hozzáférést biztosít, hogy lássa, mit is tervez.[31] Ez már ingoványos talaj a támadó műveletek felé, amit maga a stratégia is deklarál azáltal, hogy kimondja: a közös erők támadó kiberképességeket és innovatív koncepciókat fognak alkalmazni, amelyek lehetővé teszik a kibertérműveletek felhasználását a konfliktusok teljes spektrumában. Ezen is továbblépve a Kongresszus 2018 végén lehetővé tette a Kiberparancsnokságnak, hogy az Egyesült Államok hálózatain kívül, valamint a bejelentett harci zónákon (mint Szíria vagy Afganisztán) kívül is működhessen. Ez már egyértelműen „felhívás keringőre". Annak módját pedig, ahogyan a stratégiában lefektetett célokat az Egyesült Államok el kívánja érni, a „kitartó elkötelezettség" *(persistent engagament)* koncepció tartalmazza, amelynek lényege, hogy az ellenfél tevékenységét állandó nyomás alatt kell tartani, bárhol is működjön. Paul Nakasone, a Kiberparancsnokság négycsillagos parancsnoka találó hasonlatával élve: ahogyan a légierő sem tétlenkedik, a gépek nem állnak a hangárokban, hanem minden nap repülnek, információt hoznak, és ha kell, erőt demonstrálnak – ugyanez a koncepció a kibertérben is.[32] A „kitartás" a Kiberparancsnokság filozófiája szerint három részből tevődik össze: kitartó elkötelezettség, kitartó jelenlét és kitartó innováció. Ezáltal olyan új módszereket lehet és kell kifejleszteni, amelyek segítségével az ellenfelet megzavarják vagy pluszköltségek kiadására kényszerítik, elérve ezáltal azt a végcélt, hogy kétszer is meggondolja, támadni kíván-e.[33] Ez a koncepció azonban, ha (a hanyatló hatalomként épp globális jelentőségét visszanyerni igyekvő) Oroszország esetében működött is, nem biztos, hogy működni fog a felemelkedő Kínával szemben. Ahhoz, hogy a koncepció eredményesen megvalósuljon a jövőben, négy feltételnek meg kell felelnie. Ezek: a siker ütemterve (az amerikai agilitásnak költségnövelő hatása lesz, és visszatereli az ellenfelet a globális normákhoz); speciális kritériumrendszer arra az esetre, ha a koncepció működésképtelennek bizonyul; a politika fojtószelepszerepe (az amerikai elnök külföldi partnerrel való találkozása esetén a diplomácia előtérbe kerülése az ilyen műveletek lelassítása mellett); valamint

[31] Mark Pomerleau: Here's How Cyber Command's 'Defense Forward' Strategy Protects the Nation in Cyberspace. *C4ISRNet,* 2018. november 19.

[32] Ken Dilanian: Under Trump, U.S. Military Ramps up Cyber Offensive Against Other Countries. *NBCNews,* 2019. június 23.

[33] Mark Pomerleau: Cyber Command Changed Its Approach. Is the Difference Noticable? *C4ISRNet,* 2019b. augusztus 20.

az időbeli korlát (a felhatalmazások konkrét ideig szóljanak, hogy ezt követően a politikai döntéshozók áttekinthessék az elért eredményeket).[34]

A jövő kérdése, hogy ez az új stratégiai megközelítés mennyire lesz hatékony az egyre növekvő számú kibertámadással szemben. 2000 és 2016 között a rivális államok 272 dokumentált kiberműveletet hajtottak végre egymás ellen, három fő taktika mentén: a megzavarás, a kémkedés és a degradáció előnyös helyzet elérése érdekében.[35] Ezek közül mindössze 11 eredményeként sikerült olyan tartós végállapotot elérni, amely hatására a célállam viselkedése megváltozott.[36] Ez tehát nem egyértelmű siker. Kérdés továbbá, hogy megelőző jellegű támadó kiberháború esetében működésbe lép-e az úgynevezett biztonsági dilemma. Azaz egy támadó jellegű lépés más államokban félelmet kelt-e, és túlreagálást, vagy esetleg konfliktusspirált indukál. Nem kizárt ugyanis, hogy még a korlátozott célú, előretolt védelemként definiált kibernetikai támadó cselekmények is adott helyzetben félreértelmezhetők, és akaratlan eszkalációhoz vezethetnek.[37] Ez a jövőre nézve igen problémás, ugyanis az államok számára egyre nagyobb nehézséget okoz különbséget tenni a kémkedés és a nagyobb károkat okozó degradációs műveletek között. Amit az Egyesült Államok előretolt védelemnek nevez, azt Kína és Oroszország könnyen megelőző csapásnak tekintheti, ezért a következő lépés nem lesz más részükről, mint felkészülés a további támadó műveletekre. Ez az új stratégia „örök kiberháborúhoz" vezethet.[38] Ahhoz, hogy ez ne következzen be, az Egyesült Államoknak egy, az aktív védelem köré szervezett globális hálózatot kell kiépítenie, ahol a hírszerzési információkat megosztják egymással a résztvevők, és elérik azt, hogy jelentős mértékben csökkennek az ellenfelek kiberműveleteiből származó várható előnyök.

A formálódó újabb hidegháború másik, nevezzük keleti oldalának régi-új szereplője az *Orosz Föderáció,* ahol a kiberkérdések tárgyalása egészen más talajon áll. Az ország a kiber- és a kiberháború kifejezést sem alkalmazza, helyette az információs hadviselés *(informacionnoje protyivoborsztvo)* szóösszetételt használja a kiberhatások megvitatásakor. Ahogyan az Egyesült Államok

[34] Jason Healey: The Implications of Persistent (And Permanent) Engagement in Cyberspace. *Journal of Cybersecurity,* 5. (2019), 1. 1–15.

[35] Brandon Valeriano – Benjamin Jensen: The Myth of the Cyber Offense: The Case for restraint. *CATO Policy Analysis,* 2019. január 15.

[36] Ezek többsége Kína és Oroszország által az Egyesült Államok ellen irányuló, éveken át tartó kémkedés letörése volt.

[37] Valeriano–Jensen (2019): i. m.

[38] Jason Healey: Triggering the New Forever War, in Cyberspace. *The Cipher Brief,* 2018. április 1.

kiberpolitikáját a terrorizmus befolyásolta, úgy nyomták rá Oroszország ezirányú politikájára bélyegüket a Szovjetunó összeomlásából fakadó gazdasági és területi viták. Ez – instabil geopolitikai helyzettel párosulva – kettős következménnyel járt: erőteljes, proaktív összpontosítás a támadásra, valamint a kiberszuverenitásba vetett hit a szabad, nyitott információs tér helyett.[39] Ennek az orosz megközelítésnek két pillére van: az információs-technológiai és az információs-pszichológiai. Míg az előbbit a támadások jellemzik (a befolyásolási műveletektől kezdve a rosszindulatú programok ellenséges hálózatok elleni telepítéséig),[40] addig az utóbbit a botnetek és a közösségi médiában hamis felhasználói fiókok használatával lehet körülírni.[41] Ez utóbbi sikere különösen szembeötlő (volt a 2016-os amerikai elnökválasztáson is), és minden bizonnyal az információs hadviselés továbbra is kiemelkedően fontos eleme marad az orosz stratégiának – még inkább a támadó műveletekre összpontosítva.[42]

S végül: *Kína*. Az ország, amelyet már ma is a leghírhedtebb kiberháborús résztvevőnek tartanak, amely mindig arra törekszik, hogy másokkal is érzékeltesse hatalmát és befolyását.[43] Kína pártolja a kiberhatalom átfogó fogalmának használatát, amely magában foglalja egy ország cselekvésre és befolyásolásra vonatkozó képességét a kibertérben, és olyan elemekből tevődik össze, mint az IT és az IT-ipari képességek, az internetes piac és diplomáciaképességei, az internetes kultúra hatása, a katonai kibererő és a kiberstratégia-alkotásban való nemzeti érdek.[44] Oroszországhoz hasonlóan Kína is az információs műveletek kifejezést használja, és úgy véli, hogy az internetes szuverenitás nem különbözik a területi szuverenitástól. Kína végeláthatatlan háborút vív, amelyben nincs különbség békeidejű és háborús kiberműveletek között.[45] Ezen elképzeléseket a Népi Felszabadító Hadseregnél minden bizonnyal létező korlátlan hadviselés

[39] The Sinicization of Russia's Cyber Soverignty Model. *Council on Foreign Relations,* 2020. április 1.

[40] Sergei A. Medvedev: *Offense-Defense Theory Analysis of Russian Cyber Capabilities.* Calhoun Institutional Archive of the Naval Postgraduate School, 2015. március.

[41] Scott Shane: The Fake Americans Russia Created to Influence the Elections. *The New York Times,* 2017. szeptember 7.

[42] Michael Connell – Sarah Vogler: Russia's Approach to Cyber Warfare. *CNA,* 2017. március.

[43] Sachin Kumar Sahu et al.: A Review: Outrageous Cyber Warfare. *IEEE,* 2016.

[44] Li Zhang: A Chinese Perspective on Cyber War. *International Review of the Red Cross,* 94. (2012), 886.

[45] Elsa B. Kania: Cyber Deterrence in Times of Cyber Anarchy – Evaluating the Divergences in U.S. And Chinese Strategic Thinking. *International Conference on Cyber Conflict.* Washington DC., 2016. október 21–23.

doktrínája összegzi. A kifejezést először Csiao Liang és Vang Hsziang-szuj tábornok használta, kifejtve, hogy a hadviselés már nem szigorúan katonai művelet, és a harctérnek már nincsenek határai.[46] A stratégiai fordulópont dokumentáltan 2013 volt, amikor a kínai katonai doktrínában a kínai hadsereg holisztikus szempontból első alkalommal foglalkozott nyilvánosan a kiberháborúval, valamint a kiberteret a „gazdasági és társadalmi fejlődés új pilléreként és a nemzetbiztonság új területeként" határozta meg.[47] Az új offenzív kiberdoktrínát példázzák azok az esetek, amelyekben Kína a riválisaitól technológiai és szellemi tulajdont lop el katonai felhasználás céljából – mint ahogy történt az *Aurora* művelet esetében is, amikor kínaiak számos top 100 Fortune-vállalatot hekkeltek meg (úgymint a Google, a Yahoo vagy az Adobe). Egyébiránt egyedülálló a kínai doktrínában az, ahogyan az államhatalom teljes körű gyakorlásának részeként a Kínai Kommunista Párt céljainak elérése érdekében a kiberteret használja. S bár Kínával kapcsolatosan számos kérdést homály fed, afelől senkinek sem lehet kétsége, hogy Peking számára prioritás az amerikaihoz hasonló, de azt minden tekintetben felülmúló taktikai kibernetikai képesség fejlesztése. Mindezek alapján két következtetést bizonyosan le lehet vonni. Egyrészt Kína a kiberképességeit nem légüres térben fejlesztette, hanem más államok (és elsősorban az Egyesült Államok és Oroszország) változó kiberhadviselési megközelítésére és gyakorlatára válaszképp. Másrészt pedig a kínai kormány kibernetikus háborúval kapcsolatos nézetei összhangban állnak katonai stratégiájával, amelyet a biztonsági környezet változása, a hazai környezetváltozás és a külföldi hadseregek tevékenységének megfelelően időről időre módosítanak. E stratégia központi tétele az aktív védelem elve, amely alapján a kiberháborúban az elsődleges cél a védelmi képességek fokozása a túlélés és az ellensúlyozás érdekében egy támadó kibercsapás után. Kína szerint ugyanis „a legjobb védekezés a támadás" elve a kibertérben nem alkalmazható, mivel az első kibertámadás után a megcélzott fél pontos ellentámadással válaszolhat, amennyiben erős védelemmel rendelkezik. Ez esetben pedig a támadó lesz az, aki érzékeny veszteségeket szenved, ha nem rendelkezik kellőképp jó védelmi képességekkel.[48] Ennek az elméletnek a gyakorlati igazolása még a jövőre vár. Az azonban bizonyos, hogy a mai napig

[46] Jason Fritz: How China Will Use Cyber-Warfare to Leapfrog Military Competitiveness. *Culture Mandala,* 8. (2008), 1. 28–80.

[47] Lyu Jinghua: *What are China's Cyber Capabilities and Intentions?* Carnegie Endowment for International Peace, 2019. április 1.

[48] Jinghua (2019): i. m.

nincs megcáfolhatatlan bizonyíték arra vonatkozóan, hogy Kína a kibertérben támadó és megsemmisítő szándékkal lépett volna fel.

A jövő technológiái

A kiberháború jövőjét meghatározó tényezők másik csoportját az újabb és újabb eszközök kifejlesztése jelenti – ezek a jövő technológiái. A fejlődés olyan rohamos, hogy bármi konkrétumot igen nehéz lenne megjósolni, azonban az már most látszik, hogy mely technológiák azok, amelyek a jövőben meghatározóak lesznek. Ezek közül a terjedelmi korlátok okán kettőt emelek ki: a kvantumtechnológiát és a mesterséges intelligenciát.

Mi sem mutatja jobban a *kvantumtechnológia* fontosságát, mint az, hogy Hszi Csin-ping kínai elnök 2017-ben a kvantumkommunikációt és a számítástechnikát mint kiemelt „megaprojektet" nevesítette, hangsúlyozva a kvantumtechnológiák fontosságát a nemzetbiztonság szempontjából is.[49] A kvantumversenybe Kína és az Egyesült Államok is sokat fektet már most, mert pontosan tudják, hogy aki előnyre tesz szert, az büntetlenül képes lesz más államok adatbázisában bármit megtenni.[50] Sok nemzet már most olyan adatokat halmoz fel, amelyeket ma még ugyan nem tudnak visszafejteni, de kvantumszámítással megtehetnék, és a jövőben meg is fogják tenni. Emellett a kvantumszámítás alkalmazásai a kiberháborúban is korlátlanok. A 2030–2040-es évekre tehető, hogy a qubitszám (a számítógépes bitek kvantumegyenértéke) és a koherenciaidő (az az idő, amely alatt egy egység képes információt tárolni) is jelentősen meg fog nőni, olyan mértékben, hogy akár 10 másodperc alatt képesek lesznek feltörni a titkosításokat.[51] Az előrejelzések szerint a nagyszabású kvantumszámítógépek a laboratóriumokon kívül is elérhetővé válnak, ami nemcsak a kutatás számára teremt hatalmas új lehetőségeket, hanem új veszélyeket és kihívásokat is tartogat az államok számára.

[49] Elsa B. Kania – John K. Costello: Quantum Technologies, U.S.–China Strategic Competition, and Future Dynamics of Cyber Stability. *International Conference on Cyber Conflict.* Washington (DC), 2017.

[50] Matthew S. Williams: Life in 2050: A Glimpse at Warfare in the Future. *Interesting Engineering,* 2021. április 25.

[51] Jaime Sevilla – C. Jess Riedel: Forecasting Timelines of Quantum Computing. *ArXiv,* 2020. december 9.

A másik technológiai újítás, a *mesterséges intelligencia* (*artificial intelligence:* AI) számos új lehetőséget kínál a hatékonyság és az eredményesség növelésére mind a virtuális, mind a kinetikus csatatéren. Az első, aki új referenciaértékeket ér el az AI-ben, akkora erőre és előnyre tesz szert, amely lehetővé teszi számára több adat elemzését, jelentős stratégiai és taktikai előnyöket biztosítva a döntéshozatali folyamatokban. A hadműveletekben katonai előny elérése érdekében kétféleképp használható fel a mesterséges intelligencia. Vagy az aktuális katonai doktrínákba és koncepciókba épül be azzal a céllal, hogy a meglévő képességeket fokozza, vagy az emberi környezet cselekvési sebességét és hatékonyságát javítsa – ez az evolúciós út. Vagy – önállóan vagy más feltörekvő technológiákkal együtt – új doktrínák kifejlesztéséhez vezet, amelyek szembemennek a mai csatatér meglévő fizikai és jogi határaival – ez a forradalmi perspektíva.[52] Az egyes államok bármelyik utat is választják, a megszerzett előny igen jelentős lesz, és megindul a fejlődés az információs hadviseléstől az intelligens hadviselés felé. Ez a folyamat a nagyhatalmak esetében már most is zajlik, és 2030-ra látványos eredmények is várhatók.

Cyber Pearl Harbor vagy Cyber 9/11?

A válasz röviden: talán egyik sem. Ezek az elnevezések nagy háborúk, ütközetek vagy támadások tipikus jellegzetességeiből indulnak ki, és a jövő kiberháborúját igyekeznek ezen analógiák mentén vizionálni, felvázolva különböző szcenáriókat.[53]

Egy Pearl Harbor-jellegű kibertámadás hasonlóan meglepetésszerű volna, mint ahogyan a japánok 1941-ben meglepték az amerikaiakat Pearl Harbor kikötőjénél. Egy ilyen támadás, ahol a szemben álló felek állami katonai alakulatok, taktikai értelemben meglepetés volna, azonban részét képezné egy nagy hadműveletnek, geopolitikai kontextusba ágyazva. Ebből kifolyólag egy ilyen kezdeti gyors, meglepetésszerű, masszív és stratégiai hatással bíró kibertámadást minden bizonnyal egy nagy, alapvetően hagyományos háború követne, amely vélhetően a kiberhadszíntéren is folytatódna. Talán nem véletlen, hogy a 2003-as amerikai kiberstratégia még éppen egy ilyen jellegű kiberháborúval számol,

[52] Joe Burton – Simona R. Soare: *Understanding the Strategic Implications of the Weaponization of Artificial Intelligence.* 11th International Conference on Cyber Conflict, Tallinn, 2019.

[53] Részletesebben lásd: *Proceedings of a Workshop…* (2010): i. m. 86–92.

amikor kimondja, hogy „amikor egy nemzet, terroristacsoport vagy más ellenfél az Egyesült Államokat a kibertéren keresztül megtámadja, az Egyesült Államok válaszának nem kell csak a büntetőeljárásokra korlátozódnia. Az Egyesült Államok fenntartja a jogot, hogy megfelelő módon reagáljon."[54] Sőt, még 2011-ben is a CIA volt főigazgatója, Leon Panetta úgy fogalmazott, hogy a következő Pearl Harbor egy kibertámadás lehet.[55] Bár ilyen támadás azóta sem következett be, s még ha be is következne a következő tíz évben, nem valószínű, hogy azt nagyszabású, hagyományos háború követné.

Ezzel szemben a Cyber 9/11 koncepció alapján egy nem állami szereplő (például terroristacsoport) követ el kibertámadást egy állam ellen. Ez esetben a szintén meglepetésszerű és masszív támadás célpontjai azonban nem katonai, hanem civil célpontok, és az elérni kívánt hatás sem stratégiai, hanem műveleti szintű. Egy ilyen támadás egyszeri alkalom volna, az nem lenne része nagyobb műveletnek. Hatását tekintve az várható, hogy – hasonlóképp a szeptember 11-i terrortámadáshoz – bár a támadásnak sok szempontból tragikus kimenetele lenne, gazdasági hatása messze elmaradna a várttól, és az Egyesült Államok relatíve könnyen átvészelné a nehéz időszakot (ahogyan tette azt 2001-ben is a támadást követő hetekben). A támadók nem fognak elrettenni a megtámadott fél támadó kiberképességei láttán, így az nem fogja őket visszatartani tettük elkövetésétől, azonban a fizikai erővel való elrettentés adott esetben hatásos lehet. A vázolt két szcenárió kapcsolódási pontja, hogy az elnevezést adó eseményekre az Egyesült Államok válasza elhúzódó katonai kampányhoz vezetett mind konvencionálisan, mind irreguláris módon, és erre lehetne számítani a kibertérben is.

Ez a két forgatókönyv a legismertebb, azonban számos más jellegű kiberháború is elképzelhető. Ezek között említhető a különleges műveletekhez nyújtott közvetlen támogatás, a hagyományos műveletek operatív támogatása (az úgynevezett „St. Mihiel" kiberművelet), a kizárólag a kibertérben zajló háború támadó és védekező erőkkel (amely a brit légi csata után a „Cyber Battle of Britain" becenevet kapná) vagy az úgynevezett Cyber Vietnam, az online gerillaháború. A jövő több-kevesebb eséllyel ezek bármelyikét elhozhatja.

[54] *The National Strategy to Secure Cyberspace*. 2003. február. 65.

[55] Jason Ryan: CIA Director Leon Panetta Warns of Possible Cyber-Pearl Harbor. *ABC News,* 2011. február 11.

Záró gondolatok

Az elmúlt évtizedben tanúi lehettünk annak a folyamatnak, ahogyan a „kiberbiztonsági dilemma" átformálta az államok stratégiáit a növekvő kibernetikai képességeikből kiindulva. Elég, ha az észt példára gondolunk: az országot ért váratlan és nagy erejű 2007-es kibertámadást követően óriási kibernetikai képességeket fejlesztett ki, és 2008-ban a NATO is tallinni székhellyel nyitotta meg Kibervédelmi Kiválósági Központját.[56] De említhetjük a 2010-ben felállított amerikai Kiberparancsnokságot vagy annak Információs Biztonsági Bázis elnevezésű kínai mását is.[57] A politikai döntéshozók számára azonban még mindig sok a nyitott kérdés. Ezek között említhetjük, hogy vajon a hagyományos nukleáris stratégai koncepciók (mint a megelőző csapás vagy a kölcsönösen garantált megsemmisítés) használhatók lehetnek-e a mai realitás közepette.[58] Problémás továbbá, hogy a kormányok hogyan képesek reagálni a kibertér kérdéseire, amikor ennek a területnek a legnagyobb része a magánszektorban gyökerezik. Az Egyesült Államokban például a kritikus infrastruktúra mintegy 85%-át a magánszektor birtokolja vagy üzemelteti, és nem közvetlenül a szövetségi ügynökségek.[59]

A jövő bármit hozhat, hiszen háborúk vannak, voltak és lesznek. Azonban nem mindegy, hogy a jövő háborúit kik, milyen eszközökkel, hol és hogyan fogják megvívni. A számok azonban magukért beszélnek: míg 2000-ben csak hét állam[60] rendelkezett saját kibererővel, addig 2018-ban már 61.[61] Nem kérdés az ötödik hadszíntér léte és növekvő dominanciája, militarizálódásának mértéke azonban igen. A támadó kiberképességeket aszimmetrikus jellegük miatt sok olyan országban felkarolták, ahol nem rendelkeznének kellő forrással ahhoz, hogy katonai vagy gazdasági szinten versenyezni tudjanak a világ leghatalmasabb nemzeteivel. S nem szabad elfelejteni azt sem, hogy a világ egyetlen államának sincs technikai képessége a kibertámadások megelőzésére, függetlenül

[56] *NATO's Cooperative Cyber Defence Centre of Excellence.*

[57] Russell Hsiao: China's Cyber Command? *The Jamestown Foundation,* 2010. július 22.

[58] Nitin Menon: The Potential Impact of Cyber Capabilities on Future Strategy. *E-International Relations,* 2021. május 5.

[59] *Critical Infrastructure Protection, Information Sharing and Cyber Security.* U.S.

[60] Ezek: az Egyesült Államok, Oroszország, Kína, Izrael, Észak-Korea, Görögország és Thaiföld.

[61] Jason Blessing: The Global Spread of Cyber Forces, 2000–2018. In *13th International Conference on Cyber Conflict: Going Viral Proceedings 2021.* NATO CCDCOE Publications, 2021. 249.

attól, hogy azok közvetlenül egy országot céloznak-e meg, vagy annak iparát.[62] A támadások egyre szélesebb körűek lesznek, és a már most nyilvánvaló hatásukkal is minden jövőbeni fegyveres konfliktus esetén számolni kell. Kulcsszerepe lehet (és van) a nemzetközi közösségnek, amelynek meg kell találnia a módot a holnap normáinak együttes létrehozására. Ez az út azonban – már most látjuk, hogy – nagyon hosszú, buktatókkal teli, és kérdéses, hogy egyáltalán végig lehet-e menni rajta. Ugyanis az olyan legalapvetőbb jogi kérdéseket illetően is, mint a (kiber)szuverenitás, Kelet és Nyugat álláspontja gyökeresen eltér egymástól. Ha az informatikai területet az elmúlt 30 évben „fiatalnak" és „növekvőnek" nevezték, talán most eljött az idő, hogy „felnőtté" váljon.

Irodalomjegyzék

Blessing, Jason: The Global Spread of Cyber Forces, 2000–2018. In *13th International Conference on Cyber Conflict: Going Viral Proceedings 2021.* NATO CCDCOE Publications, 2021. 233–256. Online: https://ccdcoe.org/library/publications/13th-international-conference-on-cyber-conflict-going-viral-proceedings-2021/

Burton, Joe – Simona R. Soare: *Understanding the Strategic Implications of the Weaponization of Artificial Intelligence.* 11th International Conference on Cyber Conflict, Tallinn, 2019. Online: https://ccdcoe.org/uploads/2019/06/Art_14_Understanding-the-Strategic-Implications.pdf

Ciaran, Martin: *Cyber-Weapons Are Called Viruses for a Reason: Statecraft and Security in the Digital Age.* London, King's College, 2020. november. Online: https://s26304.pcdn.co/wp-content/uploads/Cyber-weapons-are-called-viruses-for-a-reason-v2-1.pdf

Clausewitz, Carl von: *A háborúról. I. kötet.* Budapest, Zrínyi, 1961.

Connell, Michael – Sarah Vogler: Russia's Approach to Cyber Warfare. *CNA,* 2017. március. Online: www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf

Critical Infrastructure Protection, Information Sharing and Cyber Security. U.S. Chamber of Commerce. Online: www.uschamber.com/issue-brief/critical-infrastructure-protection-information-sharing-and-cyber-security

Department of Defense Cyber Strategy 2018. (Summary.) Online: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

[62] Ivan Kwiatkowski: The Future of Cyberconflicts. *SecureList,* 2020. december 18.

Digwatch: *UN GGE and OEWG*. 2021. Online: https://dig.watch/processes/un-gge

Dilanian, Ken: Under Trump, U.S. Military Ramps up Cyber Offensive Against Other Countries. *NBCNews,* 2019. június 23. Online: www.nbcnews.com/politics/national-security/under-trump-u-s-military-ramps-cyber-offensive-against-other-n1019281

Fazzini, Kate: Trump's New Strategy Means the U.S. Could Get More Aggressive With Russia and China Over Hacking. *CNBC,* 2018. szeptember 21. Online: www.cnbc.com/2018/09/21/trump-cybersecurity-policy-offensive-hacking-nsa-russia-china.html

FM 3-38 Cyber Electromagnetic Activities. Department of the Army HQ, 2014. február. Online: https://fas.org/irp/doddir/army/fm3-38.pdf

Fritz, Jason: How China Will Use Cyber-Warfare to Leapfrog Military Competitiveness. *Culture Mandala,* 8. (2008), 1. 28–80. Online: www.international-relations.com/CM8-1/Cyberwar.pdf

Gray, Colin S.: *Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling?* Strategic Studies Institute, 2013. április 1. Online: www.jstor.org/stable/resrep11496?seq=27#metadata_info_tab_contents

Healey, Jason: The Implications of Persistent (And Permanent) Engagement in Cyberspace. *Journal of Cybersecurity,* 5. (2019), 1. 1–15. Online: https://academic.oup.com/cybersecurity/article/5/1/tyz008/5554878

Healey, Jason: Triggering the New Forever War, in Cyberspace. *The Cipher Brief,* 2018. április 1. Online: www.thecipherbrief.com/triggering-new-forever-war-cyberspace

Howes, Norman R. – Michael Mezzino – John Sarkesain: *On Cyber Warfare Command and Control Systems*. (H. n.), International Command and Control Institute, 2004. Online: www.dodccrp.org/events/9th_ICCRTS/CD/papers/118.pdf

Hsiao, Russell: China's Cyber Command? *The Jamestown Foundation,* 2010. július 22. Online: https://jamestown.org/program/chinas-cyber-command/

Jinghua, Lyu: *What are China's Cyber Capabilities and Intentions?* Carnegie Endowment for International Peace, 2019. április 1. Online: https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pub-78734

Joint Operations, 17 January 2017 Incorporating Change 1, 22 October 2018. Joint Publications 3.0. Online: www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf

Joint Publication 1-02 (JP 1-02): Dictionary of Military and Associated Terms. Department of Defense. Washington, DC., 2019. október. Online: www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

Kania, Elsa B.: Cyber Deterrence in Times of Cyber Anarchy. Evaluating the Divergences in U.S. and Chinese Strategic Thinking. Washington (DC), International Conference on Cyber Conflict. 2016. október 21–23. Online: https://doi.org/10.1109/CYCONUS.2016.7836619

Kania, Elsa B. – John K. Costello: Quantum Technologies, U.S.–China Strategic Competition, and Future Dynamics of Cyber Stability. *International Conference on Cyber Conflict.* Washington (DC), 2017. Online: https://doi.ieeecomputersociety.org/10.1109/CYCONUS.2017.8167502

Kwiatkowski, Ivan: The future of cyberconflicts. *SecureList,* 2020. december 18. Online: https://securelist.com/the-future-of-cyberconflicts/99859/

Libicki, Martin C.: *Cyberdeterrence and Cyberwar.* Santa Monica (CA), Rand Corporation, 2009. Online: www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf

Libicki, Martin: Pulling Punches in Cyberspace. In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy.* Washington (DC), National Research Council, The National Academies Press, 2010. Online: www.nap.edu/download/12997

Medvedev, Sergei A.: *Offense-Defense Theory Analysis of Russian Cyber Capabilities.* Calhoun Institutional Archive of the Naval Postgraduate School, 2015. március. Online: https://core.ac.uk/download/pdf/36737355.pdf

Menon, Nitin: The Potential Impact of Cyber Capabilities on Future Strategy. *E-International Relations,* 2021. május 5. Online: www.e-ir.info/2021/05/05/the-potential-impact-of-cyber-capabilities-on-future-strategy/#_ftn2

Molnár Dóra: Kiberbiztonság Németországban. Pillanatkép a német digitális térről. *Nemzet és Biztonság,* 11. (2018), 1. 142–156. Online: www.nemzetesbiztonsag.hu/cikkek/neb_2018-01-09_molnar_dora_-_kiberbiztonsag_nemetorszagban-pillanatkep_a_nemet_digitalis_terrol.pdf

National Cyber Strategy of the United States of America. 2018. szeptember. Online: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

National Strategy to Secure Cyberspace. 2003. február. 6. Online: https://us-cert.cisa.gov/sites/default/files/publications/cyberspace_strategy.pdf

Pomerleau, Mark: Here's How Cyber Command's 'Defense Forward' Strategy Protects the Nation in Cyberspace. *C4ISRNet,* 2018. november 19. Online: www.fifthdomain.com/dod/2018/11/19/heres-how-cyber-commands-defend-forward-strategy-protects-the-nation-in-cyberspace/

Pomerleau, Mark: Cyber Command Changed Its Approach. Is the Difference Noticable? *C4ISRNet,* 2019b. augusztus 19. Online: www.fifthdomain.com/dod/cybercom/2019/08/20/cyber-command-changed-its-approach-is-the-difference-noticeable

Pomerleau, Mark: Two Years In, How Has a New Strategy Changed Cyber Operations? *C4ISRNet,* 2019a. november 11. Online: www.fifthdomain.com/dod/2019/11/11/two-years-in-how-has-a-new-strategy-changed-cyber-operations

Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy. Washington DC, National Research Council, The National Academies Press, 2010. Online: www.nap.edu/download/12997

Ryan, Jason: CIA Director Leon Panetta Warns of Possible Cyber-Pearl Harbor. *ABC News,* 2011. február 11. Online: https://abcnews.go.com/News/cia-director-leon-panetta-warns-cyber-pearl-harbor/story?id=12888905

Sahu, Sachin Kumar Kumar – Abhishek Anand – Aseem Sharma – Nidhi Nautiyal: A Review: Outrageous Cyber Warfare. *IEEE,* 2016. Online: https://doi.org/10.1109/ICICCS.2016.7542306

Sevilla, Jaime– Jess C. Riedel: Forecasting Timelines of Quantum Computing. *ArXiv,* 2020. december 9. Online: https://arxiv.org/pdf/2009.05045.pdf

Schulze, Matthias: Cyber in War: Assessing the Strategic, Tactical, and Operational Utility of Military Cyber Operations. *12th International Conference on Cyber Conflicts*. Tallinn, NATO CCDCOE Publications, 2020. Online: www.swp-berlin.org/fileadmin/contents/products/fachpublikationen/CyCon_2020_10_Schulze.pdf

Shane, Scott: The Fake Americans Russia Created to Influence the Elections. *The New York Times,* 2017. szeptember 7. Online: www.nytimes.com/2017/09/07/us/politics/russia-facebook-twitter-election.html

The Sinicization of Russia's Cyber Soverignty Model. *Council on Foreign Relations,* 2020. április 1. Online: www.cfr.org/blog/sinicization-russias-cyber-sovereignty-model

The White House: *Remarks by the President at the Cybersecurity and Consumer Protection Summit.* Stanford (CA), Stanford University, 2015. február 13. Online: https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit

Turner, Harriet Charlotte: Cyber War Forthcoming: "It Is Not a Matter of If, It Is a Matter of When". *E-International Relation,* 2020. július 8. Online: www.e-ir.info/2020/07/08/cyber-war-forthcoming-it-is-not-a-matter-of-if-it-is-a-matter-of-when

Uren, Tom – Bart Hogeveen – Fergus Hanson: *Defining Offensive Cyber Capabilities*. Australien Strategic Policy Institute, 2018. július 4. Online: www.aspi.org.au/report/defining-offensive-cyber-capabilities

US Solarium Cyberspace Commission Report. 2020. március. Online: https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view

Valeriano, Brandon – Benjamin Jensen: The Myth of the Cyber Offense: The Case for restraint. *CATO Policy Analysis,* 2019. január 15. Online: www.cato.org/policy-analysis/myth-cyber-offense-case-restraint

Williams, Matthew S.: Life in 2050: A Glimpse at Warfare in the Future. *Interesting Engineering,* 2021. április 25. Online: https://interestingengineering.com/warfare-in-2050-what-to-expect

Wright, Aaron: The Future of Cyber Conflict. *The Cove,* 2020. augusztus 16. Online: https://cove.army.gov.au/article/the-future-cyber-conflict

Zhang, Li: A Chinese Perspective on Cyber War. *International Review of the Red Cross,* 94. (2012), 886. Online: https://international-review.icrc.org/sites/default/files/irrc-886-zhang.pdf