EGY ÚJ DIMENZIÓ

TANULSÁGOK A LÉGIERŐ FEJLŐDÉSÉBŐL A KIBERTÉR SZÁMÁRA

AMBRUS ÉVA

A kibertér megjelenése és térnyerése az életünkben nem valami egyszeri esemény következménye, hanem lépésről lépésre vált nélkülözhetetlenné mindennapjainkban. Ahogy ez a fejlődés halad előre, felmerül a kérdés, hogy mikor s egyáltalán elérjük-e a technológiai szingularitást, vagyis azt a pontot az időben, amikor olyan szinten felgyorsul a technológiai–társadalmi fejlődés és változás, hogy azt értelmezni vagy előrejelezni nem lesz már lehetséges. Mielőtt ezt a pontot elérnénk, érdemes – a nemzetközi közösség törekszik is rá – néhány pontot tisztázni a kibertérben, például a nemzetközi jog hatályát, a mesterséges intelligencia (AI/MI) morális kérdéskörét vagy a kibertámadások attribúciós kérdéseit (az elkövetők azonosítása). Ennek megközelítéséhez érdemes a stratégiai gondolkodókat megvizsgálni, azonban még ezt követően is több kérdés marad nyitva, mint amik nyugvópontra kerülnének.

KETTŐS FELHASZNÁLÁS

A technológiai fejlődés összefonódik a katonai felhasználással – egymást előrevivő erők találkozása ez. A digitális korszak, a kibertér (*cyber space*), mint hadászati dimenzió, azonban korántsem olyan könnyen körülhatárolható terület, mint a szárazföldi, légi, tengeri vagy éppen az űr dimenziója a hadviselésben. Ennek egyik oka, hogy ezek dimenzióiban jól elkülöníthető a katonai és a civil felhasználás. Másfelől ezek a dimenziók mára sok esetben saját kiberképességekkel rendelkeznek. A hibridség ebben az esetben nemcsak abból fakad tehát, hogy a különböző dimenziók is megjelennek párhuzamosan a kibertérben, hanem hogy a civil és katonai kibertér sem jól elkülöníthető elemek. Hogy jobban megismerhetők legyenek azok a tulajdonságok, amelyek megkülönböztetik a kiberteret a többi hadszíntértől, érdemes összehasonlítani egy másik haderőnemmel, amelynek fejlődése a technológiai fejlődésen alapult: a légierőével, hiszen a légierő is támogató fegyvernemként jelent meg először a harctereken, majd idővel önállóvá vált.

A hadviselés történetében az új fegyverek és technológiák többsége fokozatosan jelent meg, több év telt el a bevezetésétől a széles körű elterjedéséig. A 20. század hajnaláig ezek a technológiai fejlesztések a szárazföldi vagy a tengeri hadszíntéren jelentek meg. Később az ember először a harmadik dimenzióba merészkedett, azaz a föld felszíne felé; ez egy valóban disruptív technológia megjelenése volt egy új dimenzióban, amely gyökeresen megváltoztatta a hadviselést, méghozzá rendkívül rövid idő alatt.

Ezzel szinte egy időben jelent meg az információ vezeték nélküli továbbításának technológiája. A vezeték nélküli hálózat korábban ismeretlen spektrumban működött, elsődleges feladata és hatása a hadműveletek tekintetében a kommunikáció javítása volt. Bár nagyon fontos előrelépés volt, nem volt ugyanolyan disruptív, mint a légerő megjelenése. Most, amikor belépünk a 21. századba,

a vezeték nélküli hálózat átterjedt a kibertérre – a bitek és bájtok területe több csatornán keresztül haladva békében és valószínűleg háborúban is befolyásolja életünk szinte minden területét. A kibertér fejlődésének sebessége lélegzetelállító, elegendő, ha arra gondolunk, hogy szinte naponta születnek néhány évvel ezelőtt még elképzelhetetlen új kibereszközök és technikák. A légierőhöz hasonlóan a kibertér is egy új, feltáratlan és disruptív dimenzióval egészíti ki a hadviselést. Ha elfogadjuk a kiberháború lehetőségét, sőt inkább valószínűségét, akkor azt is el kell ismernünk, hogy *terra incognitá*n járunk.

A legtöbb találmány, még azok is, amelyek valóban disruptívvá válnak, kezdetben arra szolgálnak, hogy jobban teljesítsenek egy feladatot; gyakran évtizedekbe telik, mire kiderül, hogy ezek a találmányok teljesen új hadműveleti koncepciókat tesznek lehetővé. Így volt ez a légierővel, de így van ez a kiber-

Harcigalamb – Brit katona postagalambot enged el az I. világháború nyugati frontján, az Amiens-i csaták valamelyikében *(Wikimedia Commons)*

világban is. Sejthető, hogy a kiberműveleteknek disruptív lehetőségei lesznek a háborúban, és hogy azok, akik élnek a kibertér adta lehetőségekkel, mérhetetlen előnyre tesznek szert ellenfeleikkel szemben.

Az információs korszak hadviselésre gyakorolt hatása az elmúlt két évtizedben kiemelt kérdés volt, mivel mind a politikai döntéshozók, mind a katonai vezetők, valamint a nemállami szereplők is foglalkoztak azzal, hogyan lehetne a legjobban kihasználni és megvédeni magukat a kibertér adta lehetőségektől, fenyegetésektől. A múltbeli fegyverekkel ellentétben a kiberháború folytatásához szükséges technológia nem korlátozódik a rendszer egyes szereplőire: a kritikus rendszerek (vagyis súlypontok) megtámadásának képessége megtalálható mind az állami, mind pedig a nemállami szereplőknél. Ennek okán elemezni szükséges ennek az új hadviselési módnak a módszereit és eszközrendszerét, valamint összetevőit és szereplőit. Az egyik legfontosabb kérdés, hogy mi minősül kiberháborúnak, kibertámadásnak, és vajon ugyanolyan súllyal esik-e latba az állami és a nemállami szereplők által elkövetett támadások esetben a retribúció?

> **a találmányok új hadműveleti koncepciókat eredményeznek**

EGY ÚJ STRATÉGIA SZÜKSÉGESSÉGE

A hagyományos (nagy)stratégiai gondolkodás vizsgálata vajon megoldásokkal szolgálhat-e ezekre a kérdésekre? Vajon a hadviselés korábbi megközelítései illeszkednek-e a kiberháború világához, vagy teljesen új stratégiai megközelítésekre van szükségünk? A hagyományos háborúhoz hasonlóan a kiberháború intenzitása különböző, hiszen vannak szereplők, amelyek bűnözői tevékenységet, míg mások hírszerzési tevékenységet folytatnak.

A klasszikus katonai stratégiai gondolkodók elméletei a kiberháborúra kivetítve is tartalmaznak olyan meglátásokat, amelyek alkalmazhatóak napjainkban is. Antoine-Henri Jomini stratégiai elképzeléseit a napóleoni korszak alakította, *A háború művészeté*nek középpontjában a korszak stratégiájának legfontosabb eleme állt – vagyis a „döntő csata" (*Entscheidungsschlacht*) keresése.[1] Jomini számára a győzelem receptje az elsöprő erő alkalmazása volt, a csatatér legmeghatározóbb, stratégiai pontján. A kiberháborúban ilyen lehet például egy szolgáltatásmegtagadással járó támadás az állam kritikus infrastruktúrái ellen, a lehető legnagyobb zavart okozva és korlátozva annak reagálóképességét. Az informatikai rendszerekkel összekapcsolt és információfüggő társadalmakat egy ilyen meghatározó ponton történő támadás megbéníthatja, ezért a „döntő csatát" civil célpontok ellen érdemes megvívni.

A 19. század első harmadában a katonai teoretikusok közül egy név emelkedik ki: Carl von Clausewitzé. Tekintettel *A háború*ról anyagmennyiségre, most a Clausewitz által javasolt stratégiai lehetőségek közül csak a súlypontot (*Schwerpunkt*) és a „háborús ködöt" emelném ki. Az előbbi ismert, az utóbbi azt a problémát jelöli, amikor az információk hiánya korlátozza a parancsnokok és politikusok hatékony cselekvőképességét – a kibertér adta lehetőségek márpedig hatványozottan megnövelhetik a „háborús köd" fokozásának képességét. A 2007-es Észtország elleni és a 2008-ban Grúziában elkövetett kibertámadások szemléltetik azt a képességet, amellyel fontos webhelyek megtámadásával próbálták növelni a „háborús ködöt" a kommunikáció megzavarása érdekében.[2] Ebből is látszik, hogy a fejlett technológiára támaszkodó, „nyitott társadalmaknál" a dezinformáció tovább bonyolítja a reagálási képességet.

A súlypont az egyik legtöbbet vitatott elképzelés, amely Clausewitztől származik. Clausewitz a súlypontokat „minden erő és mozgás központjának nevezte".[3] A súlypont fogalma legjobban összefüggésként írható le, amelynek

1 Antoine-Henri de Jomini: *The Art of War* [1838] Greenwood Press, Westport, 1971. (Magyarul lásd: Antoine-Henri de Jomini: *A hadviselés alapelveiről* (részletek) = *Szemelvények a XIX. század burzsoá katonai teoretikusainak és szakíróinak műveiből*. I. kötet. vál. Ölvedi Ignác, ZMKA, Bp. 1973. – *a Szerk.*)

2 William C. Ashmore: Cyber Attacks. *Baltic Security & Defence Review*, 2009/11.

3 Carl von Clausewitz: *A háborúról* [1832] ford. Szabó Júlia, Zrínyi, Bp. 2014. 595.

elvesztése pusztító hatással van az ellenség háborús képességére. Az Amerikai Egyesült Államok vezérkara „közös tervezési" doktrínája úgy értelmezi, hogy a súlypontok a morális vagy fizikai erő, azaz a cselekvési szabadság vagy akarat (erő)forrásai.[4] Fizikai súlypontok lehetnek szervezetek, a morális súlypontok pedig befolyásolják vagy egyenesen irányítják a fizikai súlypontokat. Morális súlypontok lehetnek közösségi vagy szövetségi érdekek, vezető személyiségek vagy maga a közvélemény. Ha a súlypont biztosítja az egységet, úgy annak megsemmisítése korlátozza a szereplőnek azon képességét, hogy hatékonyan fellépjen.

A kínai teoretikus, Szun-ce maximái is alkalmazhatóak a kiberháború értelmezésében.[5] Például az információra való összpontosítás korunk egyik kritikus eleme, ugyanúgy, ahogy az általa különösen előnyben részesített megtévesztés használata a kiberháborúban (ez a megtévesztési képesség ugyanis korlátozza az ellentámadás indításának képességét). Végül az az alapelv, hogy mindennek a megvédése egy rendszerben sebezhetőséget okoz, szintén megjelenik a kibertérben: nincs lehetőség minden rendszert, illetve a rendszerek minden elemét védeni, ezért aztán bizonyos elvek szerint kell rangsorolni és az erőforrásokat összpontosítani a kijelölt szereplőkre, elemekre.

A nagy stratégiai gondolkodók mellett érdemes kitekinteni a légierő stratégiáját meghatározó szereplőkre is, hiszen annak fejlődése nagyon is hasonlatos lehet a kiberműveletek fejlődése szempontjából. Ahogyan a légierő támogató jellege fokozatosan erősödött, úgy jelentek meg e dimenzióra jellemző sajátosságok, specifikus elképzelések, mint például a harcoló és nemharcoló közötti különbségtétel, a polgári morál támadása vagy a szereplők rendszerként való felfogása.

Guilio Douhet olasz tüzértiszt egyik alapgondolata az volt, hogy a légierő képes támadni az ellenség számára létfontosságú központokat.[6] Ez az elképzelés, amely a Clausewitz és Jomini által ajánlottakhoz hasonló jelentőségű volt, nemcsak a hadseregek számára fontos infrastruktúrák ellen irányult, hanem minden olyan létfontosságú iparágra, ami lehetővé tette az állam működését. Az egyik legkritikusabb feltételezés Douhet részéről tehát az volt, hogy nincs különbség a harcolók és a nem harcolók között. A kibertérben ennek az érvnek jelentős következményei vannak, miután általánosságban az információk döntő többsége polgári kommunikációs infrastruktúrákon keresztül áramlik. Az infokommunikációs technológia területén létrejött kölcsönös függőség szinte lehetetlenné teszi a polgári–civil és a kormányzati–katonai rendszerek, elemek szétválasztását. Ez által az összekapcsoltság által az információs társadalmakban a kiberműveletek spektruma egyaránt polgári és katonai irányú lesz.

Szun-ce a kiberháború értelmezésében is alkalmazható

Douhet másik kritikus javaslata a polgári morál szétzúzásának gondolata volt. Ennek 21. századi alkalmazásáról azt mondhatjuk, hogy egy információs rendszer elleni támadás feltehetően nem rontja azonnal a társadalmi morált, azonban ha ez kritikus elemet, főleg súlypontot érint, akkor jelentősen megzavarhatja a mindennapokat, és képes pánikot kelteni. Ilyenek lehetnek a kommunikációs rendszerek, a banki ügyintézés, a logisztikai szféra vagy az áramellátás. Az átmeneti zavart tovább fokozhatja, ha látszólag akadozik a válasz koordinálása, és miután az infokommunikációs szektor és a kibertér is megosztott, a válaszreakció ideje megnőhet, aláásva ezzel a társadalom bizalmát a politikai vezetés iránt.

John Warden ezredes kiemelkedő elképzelése volt az, hogy minden szereplőt rendszernek kell tekinteni. Ezen a nagyobb rendszeren belül öt alrendszer létezik megállapítása szerint: a vezetés, az erőforrások, az infrastruktúra, a lakosság és a tábori haderő.[7] Minden alrendszer középpontjában számos súlypont

4 Lásd bővebben: *Joint Planning – Joint publication, 5-0*. 2020. december 1.
5 Szun-ce: *A háború művészete*. ford. Tokaji Zsolt, Helikon, Bp. 2020.
6 Guilio Douhet: *The Command of the Air* [1942] ford. Dino Ferrari, Air Force History and Museums, Washington DC, 1998.
7 John A. Warden: Enemy as a System. *Airpower Journal*, 1995/tavasz

Távoli elérés – Amerikai drón bevetése Afganisztánban *(Brookings Institution)*

található, amelyek egyenként sebezhetők. Egy további elem, amely Warden állítása szerint fontos az ellenséges rendszer hatékony támadásában, a párhuzamos támadás használata. E rendszerszintű és párhuzamos támadás a kibertérben nagy fokú hatékonyságot jelent.

A mai katonai kiberműveleti erőfeszítések elsősorban a védelmi műveletekre és a műveleti támogatásra összpontosulnak, nem pedig a támadóképesség fejlesztésére. Az egyik fontos kérdés az attribúció, vagyis az egyes kibertámadások elkövetőinek kiléte. A kibertérben elkövetett támadások más megvilágításba kerülnek, ha azokat egy állami szervezet vagy ha egy nemállami szereplő hajtja végre. Fontos tisztázni a közös meghatározásokat, illetve összehangolt szabályokat és irányelveket alkotni. Ezek után lehetséges a taktika, a technikák és az eljárások egységesítése, tisztázva a szerepeket és a felelősséget a szereplők között. Miután egy-egy támadás – főleg a sérülékenység kihasználásán keresztül – gyorsan végbemehet, vagy gyors reagálást igényel, fontos elkerüli az időveszteséget. Emiatt is fontos a szerepkörök tisztázása. Miután azonban ez egy folyamatosan fejlődő terület, így a kihívások és fenyegetések is változnak, és ez a folyamatosan változó, bizonytalan tér hozzájárul a korábban említett „háború ködéhez".

Az, hogy a szereplők miként gondolkodnak a (kiber)háborúról, meghatározza, hogy hogyan reagálnak rá. Amennyiben elsősorban támogató haderőnemként tekintünk a kiberműveletekre, úgy annak defenzív oldala lesz fejlettebb. A katonai kiberműveletek számára kihívást jelent, hogy a kibertér

Tűztámogatás – A brit Royal Navy hadgyakorlata Cipruson, 2020. október 24. *(Wikimedia Commons)*

megosztott dimenzió, és szoros együttműködés szükséges a polgári hatóságokkal és a privát szférával. Ez azonban szintén elmossa a határokat a között, hogy mi számít támadásnak s mi nem, ki a támadó és ki asszisztált ehhez, akár önkéntelenül is. Egy „nem béke állapot" alakulhat ki, amely a (nyílt) konfliktus küszöbje alatt zajlik. Az elrettentés viszont egy másik lehetőséget is kínál, amely továbbra sem offenzív, de az adott állam rendelkezik a megtorlás képességével és hajlandóságával. Az elmúlt években ilyen stratégiai reorientációt hajtott végre többek között az Egyesült Államok, amikor a „kitartó elkötelezettség és előre védekezés" (*persistent engagement & defend forward*) elveit helyezte kiberstratégiájának középpontjába. Az elrettentés azt is jelenti, hogy egy államnak támadó képességgel kell rendelkeznie, amellyel kárt okozhat támadás esetén. Figyelembe véve az attribúciós problémát, az elrettentés képessége jelenleg igencsak korlátozott.

A HÁBORÚ ÚJ FORMÁJA

Mint láttuk, a klasszikus hadelméletek segítséget nyújthatnak a kibertér hadelméletének kidolgozásához, fejlesztéséhez. A súlypontok azonosítása, védelme és támadása a kibertérben ugyanolyan hatásos lehet, mint a többi hadszíntéren. Azonban jelenleg kevés gyakorlati tapasztalattal rendelkezünk az elméletekre vonatkozóan. Az aligha kétséges, hogy *a kibertér minden jövőbeni konfliktus alatt alkalmazható lesz a katonai műveletek során*. Azonban a kibertér új kihívásokat is teremt, mint amilyen az attribúció vagy a nagyfokú összekapcsoltság által sérülékennyé tett (katonai és civil) súlypontok; szükséges tehát áttekinteni és harmonizálni a fogalmakat, folyamatokat, hatásköröket, intézményeket. Tekintettel arra, hogy sok háborús képesség (például vezetés és irányítás, globális helymeghatározás) közvetlenül vagy közvetetten támaszkodik a kibertérre és arra a tényre, hogy a katonai szervezetek szerte a világon úgy vélik, hogy az információs hadviselés a háború új formája, a jövőbeni siker kulcsa a teljes spektrumú műveletek végrehajtásának képessége lesz a kibertérben. ■