HADMÉRNÖK
VÉDELEMINFORMATIKA

16. évfolyam (2021) 2. szám 187–204.
DOI: 10.32567/hm.2021.2.13

Kovács László[1]

Offenzív kiberműveletek 1.: Az offenzív kiberműveletek természete

Offensive Cyber Operations Part One: The Nature of Offensive Cyber Operations

A cikk címében szereplő offenzív kiberműveletekhez szükséges képességek kialakításáról számos országban hatalmas szakmai vita alakult ki az elmúlt időszakban. Ugyanakkor az offenzív kiberműveletek alkalmazásának körülményei és azok következményeinek számbavétele ugyanolyan fontosak, mint maguk a műveletek. Ennek megfelelően jelen írás címe önmagában is sok kérdést felvet. Szükséges-e az offenzív kiberképességek kialakítása? Ez egyenlő-e a kibertámadó képességek kialakításával? Ezek a képességek milyen feltételek mentén alkalmazhatók akkor, ha egy kibertámadás mögött állami szerepvállalás áll? Része lehet-e a modern fegyveres küzdelemnek a kibertérben való támadás? Ezeket a kérdéseket igyekszik jelen írás számba venni két részben. A tanulmány első része az offenzív képességek általános hátterét járja körül, míg a második rész a képességek kialakításának feltételeit, szervezeti hátterét és az alkalmazás módjait, valamint annak feltételeit vizsgálja.

Kulcsszavak: **kiber, képesség, támadás, hadviselés**

There has been a huge debate in many countries about developing offensive cyber capabilities. However, not only the offensive cyber capabilities but also the consequences of their use are really serious questions. Accordingly, this paper's title also raises many questions. Is it necessary to build and maintain offensive cyber capabilities? Is this equivalent to building cyberattack capabilities? Under what conditions can these capabilities be applied in case of state support or involvement behind a cyberattack? Can an attack in cyberspace be part of the modern warfare? These issues are being considered in this two-part paper. The first part of the study

[1] Magyar Honvédség Parancsnoksága, kibervédelmi haderőnemi szemlélő; Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Elektronikai Hadviselés Tanszék, egyetemi tanár, e-mail: kovacs.laszlo@uni-nke.hu

examines the general background of offensive cyber capabilities, while the second part examines the conditions for developing skills, their organisational background and the ways and conditions of using them.

Keywords: **cyber, ability, attack, warfare**

1. Bevezetés

A kibertér, ez a közel 40 éve folyamatosan alakuló és átalakuló virtuális tér fokozatosan a mindennapjaink szerves és elengedhetetlen részévé vált. Bár a kibertér nem egy új dimenzió, annak újszerűsége mégis naponta újra és újra látványosan jelentkezik, hiszen minden nap tanúi lehetünk olyan technikai újdonságoknak, amelyek rendkívül gyorsan szolgáltatásokká, ráadásul emberek millió által elfogadott, közkedvelt és minden nap használt elengedhetetlen szolgáltatásokká válnak.

A kibertér meghatározása, azaz ennek a részben megfoghatatlan térnek a körülírása sok definíciót szült az elmúlt években. A tudományos kutatások teoretikus vitái mellett azonban ezeknek a terminológiai vitáknak, valamint az azokat övező – sokszor kisebb-nagyobb bizonytalanságokkal is járó – útkeresésnek gyakorlati haszna is volt és van napjainkban is. Az egyik gyakorlati haszon akkor érhető tetten, amikor a kibertér biztonságát vizsgáljuk. Ez a biztonságról való gondolkodás nem nélkülözheti a kibertámadó képességek kialakítása és alkalmazása területének elemzését sem, hiszen az hamar világossá vált, hogy a kibertéri védelem hatékonyságához a szemben álló féllel vagy a potenciális támadóval szembeni offenzív fellépés sok esetben nemcsak hatékonyságnövelő eszköz, hanem az egyetlen védelmi megoldás lehet. Ennek megfelelően szükséges a kibertérnek és az abban szerepet játszó eszközöknek, rendszereknek a meghatározása is, hiszen a kibertámadások hatásai csak akkor mérhetők fel, ha tisztában vagyunk a kibertér mibenlétével.

Ugyanakkor az offenzív kiberműveleti képesség az egyik olyan terület, amely során vizsgálatainknak már nemcsak a szükségszerű védelmet kell elemeznie, hanem annak az azon jóval túlmutató, a szemben álló fél információs rendszereit, szolgáltatásait és akár állampolgárait is közvetlenül érintő kérdéseire is ki kell terjednie. Ennek megfelelően egy-egy végrehajtott kibertámadás potenciális – közvetlen és közvetett – következményeit, és nem utolsósorban a támadások hatásait is fel kell mérni. Ennek oka a kibertér meghatározásában is szereplő hálózatok összekapcsoltsága. Ezek a hálózatok az összekapcsoltságuk révén egymásra is hatással vannak.

A kibertámadások hatásainak tervezése során figyelembe kell venni, hogy a hálózatok összekapcsoltsága miatt az általunk végzett támadások a saját rendszereinkre is hatással lehetnek, azaz a saját támadásunk a saját rendszereinkben is okozhatnak károkat nem megfelelő tervezés és végrehajtás miatt.

A következmények előrejelzése ugyanakkor nem lehetséges a kibertér meghatározása és kapcsolódási pontjainak számbavétele nélkül, amelyen keresztül az említett támadóakciók megvalósulnak. Azonban ez teljeskörűen és mindenre kiterjedően pont a kibertér nagysága és komplexitása miatt nemcsak hogy nagyon nehéz, de már-már lehetetlen vállalkozás is. Ebből következően egy adott kibertámadás során fellépő következmények nem mindig mérhetők fel mindenre kiterjedően és teljeskörűen. Erre

talán az egyik legjobb példa a Stuxnet féregvírus, amely az iráni atomlétesítmények elleni támadásként híresült el 2010-ben. A nagy port felvert támadás elkövetésével sokan az Egyesült Államokat és Izraelt vádolták meg. A kibertérből kilépő és fizikai károkat is okozó rosszindulatú szoftverrel elkövetett támadás után évekkel később annak egyes elemei a kibertér kiismerhetetlen, vagy legalábbis nehezen kiismerhető bugyraiban tűntek fel ismét.[2]

Az offenzív kiberképességek kialakítása és alkalmazása során, éppen a fentiek miatt, az egyik nagy problémakör a hatásvizsgálat. Mivel a kibertér nem tisztán polgári vagy nem tisztán katonai tér, egy-egy rendszer elleni, az azok működését befolyásoló akciók számos más, esetenként nem is abban a dimenzióban működő rendszerre lehetnek hatással. Ezek felmérése a rendszerek összetettsége és komplexitása miatt szintén nehéz és bonyolult feladat. Mindezeken túl a kibertér megvalósításában és kialakításában nemcsak állami szereplők, hanem kis- és közepes vállalkozások, ipari szereplők, de még maguk az állampolgárok, azaz a felhasználók is részt vesznek. Ezért egy rendszer elleni kibertámadás nemcsak az adott rendszert létrehozó, az azt működtető, hanem az azzal kapcsolatban lévő többi rendszerre és alrendszerre is kihatással lehet. A hatásvizsgálat ráadásul ma már nemcsak a kész és működő rendszerek esetében szükséges, hanem már a gyártás, vagy akár a kutatás-fejlesztés időszakára is ki kell, hogy terjedjen, mert ezekben az időszakokban elkövetett támadás sokszor majd csak jóval később – az adott eszköz, rendszer, vagy szolgáltatás használata során – fejti ki igazi hatását.

Az offenzív kiberképességek kialakításának és esetleges alkalmazásának kérdésköre a kibertér felértékelődése miatt ma már stratégiai szinten jelentkezik. Ezért szükséges azt is megvizsgálnunk, hogy egy adott ország nemzeti biztonsági stratégiája, illetve nemzeti kiberbiztonsági stratégiája hogyan rögzíti, vagy – annak hiányában – hogyan kellene, hogy rögzítse ezt a kérdéskört. Ez annál is inkább fontos, mert a kibertámadó képességek már puszta deklarálása is hozzájárulhat a napjainkban oly fontossá vált elrettentéshez. Kérdés persze, hogy a támadó képességek meglétének, vagy akár az arra való törekvésnek a megjelenítése eléri-e a kívánt hatást, azaz e képességek puszta megjelenítése a stratégiákban valóban elrettentő erővel rendelkezik-e.

További nagyon fontos kérdés maga a technika és technológia, amely a kibertámadó képességek egyik alapját fogja jelenteni. A kérdés az, hogy milyen technológiát kell kifejlesztenünk, amely hatékony eszköz lehet, ha a szemben álló fél védelmét meghaladó, azt annulálni képes – támadó – eszközökre van szükségünk. Ez a probléma felveti – hatásaiban, produktumaiban és költségeiben – a hatékony kutatás-fejlesztés kérdését is.

Addig, amíg néhány éve még sokszor tabunak számított a kibertámadó képességekről és a kibertámadásokról beszélni, addig ma egyre hangosabb a szakmai és a tudományos közélet is ezektől a kérdésektől, és ezen túlmenően számos ország többé-kevésbé nyíltan fejleszti is ezeket a képességeit.

A fentiekben megfogalmazottaknak megfelelően jelen írás az offenzív, benne a támadó kiberképességek szükségességét és azok esetleges hatásait kívánja megvizsgálni

[2] Kovács László: *A kibertér védelme.* Budapest, Dialóg Campus, 2018. 163.

úgy, hogy közben arra is igyekszik választ keresni, hogy az offenzív kiberképességek mennyiben jelentenek többet vagy mást, mint önmagában a kibertámadó képességek.

A tanulmányban összegzett vizsgálatok irodalomkutatásra építenek, esetenként az összehasonlító elemzés, majd szintézis módszerének alkalmazásával kiegészítve.

Az elvégzett vizsgálatokból levont következtetések a szerző sajátjai, azok nem feltétlenül esnek egybe, és nem tükrözik sem a Nemzeti Közszolgálati Egyetem, sem a Magyar Honvédség hivatalos álláspontját vagy véleményét.

2. Az offenzív kiberképességekről általában

Az offenzív kiberképességekkel kapcsolatos vizsgálataink sorában az elsőként megvizsgálni szükséges kérdés a következő: mit is jelent önmagában az offenzív kiberképesség? A válasz a tudományos dedukció módszerét alkalmazva meglehetősen egyszerű lenne, hiszen az offenzív kiberképességeket egyszerűen azonosíthatnánk a kibertámadások képességével. Kibertámadás alatt pedig általánosságban valamely infokommunikációs rendszerbe, nem engedélyezett módon megvalósuló, informatikai eszközök felhasználásával történő ártó szándékú behatolást értjük. Ennek megfelelően különbséget kell tennünk a kibertámadás és az etikus hacking között. Az etikus hacking alapvetően olyan, előre jól definiált, az esetek túlnyomó többségében szerződésben rögzített feltételek mellett megvalósított hálózati behatolást jelent, amely elsődleges célja a hálózaton, illetve az azt alkotó IKT-rendszerekben esetlegesen meglévő sérülékenységek felfedése, majd az azokra védelmi megoldások átadása a rendszert üzemeltetőnek.

Természetesen számos módszer létezik a kibertéri hatások kivitelezésére, amelyek lehetnek akár nem közvetlen kibertéri támadások, például a fizikai dimenzióban végrehajtott támadások a szemben álló fél számítógép-hálózatai hardverinfrastruktúrája ellen, vagy akár az elektromágneses spektrumban történő elektronikai zavarás a vezeték nélküli átviteli megoldások ellen, azok mégis negatívan befolyásolják a szemben álló fél információs rendszereinek működését.

Ugyanakkor a fentiek fényében azonnal felmerülhet a kérdés: akkor miért nem kibertámadásnak hívjuk egyszerűen az offenzív kiberképességeket, azaz a kibertámadások miért nem egyenlők az offenzív kibertevékenységekkel? A válasz – az egyszerűsítés módszerét alkalmazva – erre a kérdésre az, hogy a kibertámadások végrehajtásához számos egyéb kiegészítő tevékenységet kell végrehajtani, jellemzően a támadás vagy támadások kivitelezése előtt. Így az offenzív kiberképességek jóval többet jelentenek, és jóval többet foglalnak magukban, mint a kibertámadások végrehajtása.

A (kiber)támadást megelőzően információkat kell összegyűjteni – a lehető legszélesebb körből – a támadás célpontjára vagy célpontjaira vonatkozóan. Ez az információgyűjtés a célpont vagy célpontok (rendszerek) felépítését, az abban alkalmazott védelmi megoldásokat, technikai jellemzőiket, illetve az azt alkalmazó humán erőforrás összetételét, felkészültségét és nem utolsósorban reakcióidejét és képességét kell hogy megválaszolják. Ezt követően, de még mindig a támadást megelőzően annak eljárását kell megtervezni és kialakítani, mert az összetett védelmi rendszerek ellen

csak komplex, több egydimenziós és több támadási módszert akár egymással párhuzamosan alkalmazni képes megoldásokkal lehet hatékonyan fellépni.

Ugyanakkor a támadás eljárásának és módszereinek kiválasztása után azok közvetett, illetve közvetlen hatásainak vizsgálata is szükséges, amely feltételezi bizonyos fokú szimuláció elvégzését is. Ez az alkalmazni kívánt támadási metódus(ok), a célpont infrastruktúrájához hasonló környezetben való kipróbálását, tesztelését jelenti. Ennek során lehetőséget kell teremteni a kibertámadások következményeinek lehető legpontosabb meghatározására. Ez azonban még mindig csak egy nagybani becslést jelent a várható következmények meghatározására, hiszen egy – bár a célrendszerek felépítéséhez a lehető leginkább hasonlatos, de mégis – mesterséges környezetben, szimulált események láncolatán keresztül kívánjuk mindezt megtenni. Ez a leggondosabb eljárás esetén is csak közelítő értékeket ad a várható következményekről. Az esetleges járulékos veszteségek számbavétele azonban így nem minden esetben lehet reális és valódi. A várható járulékos veszteségek vagy károk pontos előrejelzésének hiányában azonban nem minden esetben vállalható sem a politikai, sem a katonai felelősség egy kibertámadásért. A következmények felmérésére talán az egyik legjobb példa a már korábban említett Stuxnet-támadás, hiszen az azt követő elemzések rámutattak, hogy annak hatékonysága egy alaposan ellenőrzött, a támadást megelőzően elvégzett tesztelést vagy teszteléseket is feltételezett.[3]

Így tehát fontos leszögezni, hogy az offenzív képességek jóval többet jelentenek, mint önmagukban a támadási képességek megléte.

A következő vizsgálni kívánt kérdés: miért szükséges kialakítani az offenzív[4] kiberképességeket? A kérdés abszolút jogos voltát támaszthatja alá sok ország, és így alapvetően Magyarország biztonságról a 21. században alkotott felfogása, hiszen hazánk és az európai országok a békés egymás mellett élés elkötelezettjei, és alapvetően védelmi jellegű biztonság- és védelempolitikai elvek jellemzik.

Ugyanakkor, ha egy másik szemszögből vizsgáljuk ezt a kérdést, és azt vesszük górcső alá, hogy ezt a békés egymás mellett élést milyen veszélyek fenyegetik, akkor már nem teljesen egyértelműek a válaszok, amelyeket kapunk. Hazánk új, 2020 áprilisában megjelent nemzeti biztonsági stratégiája Magyarország biztonsági környezete elemzésekor rámutat, hogy ma már a hatalmi vetélkedés kiterjed a kibertér dominanciájáért is. A stratégia ugyanígy veszélyként értékeli a kiberbűnözést, az ártó szándékú kibertéri tevékenységeket, valamint a kibertéri kritikus adatok illegális megszerzését is.[5]

Napjainkban az európai országok túlnyomó többsége a kibertéri veszélyeket felismerte, az azok kezelésére tett intézkedéseik pedig sokrétűek. Ezekben az intézkedésekben sok országban belefoglaltatik a technikai válaszok egész sora, amelyek azonban már nem csak a passzív védelmi megoldásokat jelentik.

[3] Kovács László – Sipos Marianna: A Stuxnet és ami mögötte van: Tények és a cyberháború hajnala. *Hadmérnök,* 5. (2010), 4. 171.

[4] Jelen írás nem használja a védelem megfelelőjeként a defenzív kifejezést. Ennek oka elsősorban az, hogy a hazai terminológia ezen a területen most alakul ki, és jelenleg a támadó képességek általában az offenzív kifejezéssel azonosíthatók, még akkor is, ahogy jelen írás is kitér rá, ha az offenzív képességek nem azonosak a támadás képességének puszta meglétével, illetve annak alkalmazásával.

[5] A Kormány 1163/2020. (IV. 21.) Korm. határozata Magyarország Nemzeti Biztonsági Stratégiájáról. 48. pont.

A fentieket egy újabb megközelítésből vizsgálva ki kell jelentenünk, hogy a digitális korszak társadalmai olyan alapvető kihívásokkal küzdenek, amelyek korábban nem, vagy csak részben álltak fent.[6] Ezek közül a kihívások közül az egyik legmarkánsabb az információs infrastruktúráktól való függőség. Ezek az infrastruktúrák azonban ma még mind fizikai, mind informatikai értelemben rendkívül sérülékenyek. Ez persze látszólag egyfajta paradoxon, hiszen ezek a sérülékenységek okozzák egyben az ezek kihasználására irányuló rosszindulatú tevékenységek jelentette fenyegetettséget is. Ugyanakkor ez csak látszólag ellentmondás, hiszen a sérülékenységeknek technikai és technológiai, valamint gazdasági okai vannak. A gazdasági okok között szerepelhet az is, hogy a lehető leggyorsabban kell a piacra dobni egy-egy szoftver- vagy hardverterméket. Ez az időkényszer azonban sok esetben a biztonságos tervezést, fejlesztést és gyártást a háttérbe szorítja. Pedig mindezek már saját szakmai terminológiát is kaptak az elmúlt években *biztonságtudatos fejlesztés (security by design)* néven.[7]

Ezek a ma még meglévő sérülékenységek természetszerűleg vonzzák a támadás lehetőségét, így teremtve meg a biztonsági kihívást napjainkban.

Mindezek alapján megjelenik egy újabb kérdés vizsgálatunk tárgyaként: lehetséges-e azokat az értékeket és érdekeket, amelyeket a fenti „békés egymás mellett élés" elv megfogalmaz az infokommunikációs rendszerektől függő digitális társadalomban csak védelmi jellegű tevékenységekkel fenntartani a jelenleg releváns veszélyek és kihívások mellett? A kérdés mögött az a tény rejtőzik, amely szerint egy bekövetkezett kibertámadás időbeni lefolyása – leszámítva néhány hosszú ideig tartó támadási metódust[8] – rendkívül gyors. Ezek bekövetkezése esetén már – jó esetben is – csak a következmények felszámolása, valamint az eredeti helyzet – esetenként csak részlegesen megvalósítható – helyreállítása történhet meg. A részleges helyreállítás szerepeltetésének itt az oka az, hogy a támadás következményeinek a feltárása több ok miatt is rendkívüli nehézségekbe ütközhet. Ilyen ok az például, hogy a támadás olyan szofisztikált, hogy annak minden eleme nem, vagy csak részlegesen deríthető fel, illetve a megtámadottnak nincs arra adata vagy bizonyítéka, hogy milyen információkat is érintett az adott támadás.

Az ezekre a kérdésekre adható válaszokat szintetizálva azt tudjuk megállapítani, hogy a kibertámadó képességek alkalmazásának célja elsősorban az, hogy minél távolabb tartsuk a potenciális ellenérdekelt felet a saját rendszereinktől. Lekössük kiberkapacitásait a védekezéssel, ne legyen sem lehetősége, sem esélye a saját rendszereink felderítésére és támadására.

A kibertérben zajló műveleteknek, benne a kibertámadásoknak általában proaktív megközelítésre kell épülniük.[9] Ennek egyik legfontosabb oka az, hogy ezzel a proaktivitással lehet a kezdeményezést fenntartani a kibertérben. Amennyiben a kibertérműveleteink csak a védelemre épülnek – az ebben megjelenő bizonyos szintű reaktív tevékenységeink esetén is – nagy eséllyel a szemben álló fél kezdeményezőképességeinek a dominanciája valósul meg. A hagyományos műveleti dimenziók esetében

[6] Kovács (2018): i. m. 119.
[7] Kovács (2018): i. m. 13.
[8] Az APT *(Advanced Persistent Threat),* azaz fejlett, folyamatosan fennálló veszélyek a gyakorlatban támadási folyamatot jelentenek, amelynek során nagyon fejlett támadó célú eszközöket alkalmaznak.
[9] NATO: *Allied Joint Doctrine for Cyberspace Operations, AJP 3.20.* NATO Standardization Office, 2019. 17.

már megszokott mozgás és cselekvés szabadsága a kibertérben is rendkívül fontos. Amennyiben a kibertéri tevékenységeink csak a védelemre koncentrálnak, akkor a saját mozgás- és cselekvési szabadságunkat korlátozzuk a kibertérben. Még a jól megszervezett és látszólag jól is működő kibertéri védelmi tevékenységünk esetén is fennáll annak a veszélye, hogy a szemben álló fél kiberműveleteinek olyan hatásai lesznek, amelyek jövőbeni támadásokat készítenek elő, azokat információgyűjtésre használják, illetőleg megosztják a saját kiberműveleti erőink reagálóképességeit. Ez pedig nyilvánvalóan a saját mozgás- és cselekvési szabadságunk korlátozásához vezet.

Amennyiben a kibertámadások céljait tekintve védelmi jellegűek, akkor azok a szemben álló fél információs rendszereit megcélozva, onnan potenciálisan a mi rendszereink ellen irányuló támadást akadályozhatnak meg. Azaz a támadás célja ebben az esetben egyértelműen védelmi jelleget ölt.

A védelmi célú kibertámadások sorában megkülönböztethetünk megelőző és preventív támadásokat.[10] Mindkettő védelmi célú kibertámadási fajta fő célja az, hogy a potenciális szemben álló felet, azaz a saját rendszereinket támadni szándékozó kiberkapacitásait lekössük, illetve annak vezetési rendszerét lelassítsuk vagy ellehetetlenítsük, valamint hogy lehetőség szerint a legnagyobb mértékben megfosszuk kibertámadó kapacitásaitól. A megelőző kibertámadás és a preventív kibertámadások között nem azok célja tesz különbséget, hiszen az mindkét esetben azonos, azaz a korábban felvázolt hatás elérése a cél. A különbség abban lelhető fel, hogy a két támadás eltérő információmennyiségre épül. A megelőző kibertámadás megindítása szélesebb körű és általánosabb információkat feltételez, míg a preventív kibertámadások a szemben álló félről szóló sokkal konkrétabb és szűkebb, pontos rendszerekre és eljárási módokra vonatkozó információkra épül.

Létezik egy másik megközelítés is, amely szerint, amennyiben tudjuk, hogy a szemben álló félnek vannak kiberfegyverei és rendelkezik azzal a tudással, képességgel, nem utolsósorban információval a mi sérülékenységeinkről, amelyeken keresztül a támadásait végre tudja hajtani ezekkel a kiberfegyverekkel, de mi mégsem alkalmazzuk az offenzív és benne a kibertámadó képességeinket az ellenérdekelt fél rendszereivel vagy fegyvereivel szemben, akkor szintén a szemben álló fél kibertéri mozgás- és cselekvési szabadságához járulunk hozzá.

Természetszerűleg a kibertámadások volumenét – állami támogatást feltételezve – az elkövetők igyekeznek a lehető legtovább a háborús küszöb alatt tartani. Nyilvánvalóan itt az egyik legfontosabb kérdés a nemzetközi joggal való esetleges szembekerülés.

Ezzel azonban már el is érkeztünk a hibrid műveletekhez, amelyek során a kiberműveletek kiemelt szerepet kapnak. Jelen írás nem tekinti céljának a hibrid műveletek elemzését, de azt szükséges leszögezni, hogy a háborús küszöb[11] alatt tartott konfliktus számos olyan hibrid, azaz a hagyományos katonai műveletek és nem katonai művelet jól megtervezett együttes sorozatát takarja, amelyek során az egyik legfontosabb

[10] Max Smeets – Herbert S. Lin: Offensive cyber capabilities: To what ends? In T. Minárik – R. Jakschis – L. Lindström (szerk.): *2018 10th International Conference on Cyber Conflict CyCon X: Maximising Effects.* Tallinn, NATO CCD-COE Publications, 2018. 60.

[11] A háborús küszöb alatti konfliktus: a nyílt fegyveres összecsapásnak elkerülése, amely során a nyílt konfrontációt kerülni igyekszik a hibrid tevékenységeket végző fél.

csatorna a kibertér.[12] Ennek megfelelően a hibrid műveletek során nem csak tisztán kiberműveletek kibertéri célpontok ellen történő alkalmazásáról beszélünk, hanem számos olyan egyéb műveletről, amelyek a kiberteret közvetítő közegként használják. Ilyen műveletek többek között a közösségi médiumokon keresztüli befolyásolás vagy propagandatevékenység.

Ugyanakkor a nem védelmi célú kibertámadások elsődleges célja a szemben álló fél információs rendszereinek és információs folyamatainak részleges vagy teljes, időszakos vagy végleges pusztítása, azok lefogása. A közvetett cél ebben az esetben nem más, mint a szembeálló fél döntési ciklusának akadályozása. Ez a fajta kibertámadás és az azt lehetővé tevő offenzív kiberképességek alapvetően már a kiberhadviselést vetítik előre, valamint feltételezik a kinetikus műveletek előkészítését vagy azok meglétét, hiszen a szemben álló fél döntési ciklusának kibertámadásokkal történő akadályozása a kinetikus műveletek mozgási és cselekvési szabadságához fog hozzájárulni. Ennek megfelelően a nem védelmi célú kibertámadásokat nemcsak a szemben álló fél kibertámadásai végrehajtásának akadályozására használják, hanem a saját szárazföldi, légi vagy különleges műveleti erőink fizikai dimenziókban végzett tevékenységeit támogatják, illetve azok hatékonysága növelésének érdekében hajtják végre.

3. Az offenzív kiberképességek összetevői

A fentiekben megfogalmazottaknak megfelelően tehát az offenzív kiberképességek jóval többet jelentenek, mint pusztán a kibertámadási képességek megléte.

Az offenzív kiberképességeket a következő nagy képességterületekre tudjuk felosztani: 1. információszerző és feldolgozó képesség, amelybe beletartozik a célkiválasztás, célazonosítás és célkövetés,[13] valamint a szimulációs képesség; 2. a kibertámadási képesség, azaz a kiber- és egyéb – például a fizikai vagy kognitív dimenzióban megjelenő – hatások kiváltásának képessége; 3. a hatások értékelésének képessége.

3.1. Az információszerző, célkiválasztó, célazonosító és célkövetési, valamint szimulációs képesség

A kibertámadást megelőzően az egyik legtöbb időt és a legaprólékosabb munkát a felderítés, illetve az adatgyűjtés igényli. Ezeknek a tevékenységeknek az összességére megfelelő képességeket kell kialakítani. Ez látszólag a hagyományos hírszerzési és elemzési feladatok eljárásrendjével biztosítható. Ez azonban csak részben igaz, mert a hagyományos hírszerzési feladatoknál szélesebb és jóval gyorsabban változó eljárásrendet és sok esetben adatkommunikációs csatornákat kell kialakítani. Ilyen eljárásrend lehet például a közösségi oldalakon megjelenő információk folyamatos

[12] Kiss Álmos Péter: A hibrid hadviselés természetrajza. *Honvédségi Szemle,* 147. (2019), 4. 17.

[13] A célkövetés itt alapvetően az információszerző és -elemző eszközök alkalmazása miatt szerepel, ugyanis a célok azonosítása ugyanazokat vagy hasonló eszközöket és eljárásokat igényli, mint a célkövetés.

megfigyelésével (monitorozásával), illetve gyűjtésével megbízott alias (kiberszemélyiség), aki a jelenlétével és a tevékenységével az adott közösségi platform rendszeres résztvevője.

A kibertérben megvalósítani kívánt műveletek információs (felderítő) támogatása igényli azt, hogy az összes elérhető, a művelet és a potenciális célpont szempontjából releváns, nem utolsósorban hiteles információt összegyűjtsenek. Ez lehet általános információgyűjtés és célzott felderítés eredményeként létrejövő információk együttese. A célzott felderítés a potenciális célpont (rendszer) felépítéséről, sérülékenységeiről, technikai és humán összetevőiről való adatok gyűjtését, majd azokból információk előállítását jelenti.

Ebben a tevékenységben nemcsak a célzott, hanem a széles körű adatgyűjtés, majd az azokra épített adatbányászat is kiemelkedő fontosságú. Ez az információgyűjtési és -elemzési képesség magában kell, hogy foglalja azoknak a potenciális támadási lehetőségeknek az azonosítását, amelyeken keresztül az adott kiberművelet (kibertámadás) hatékonyan végrehajthatóvá válhat. Meg kell jegyezni, hogy számos APT-támadás is felderítő és adatszerző kezdeti céllal történik, de az APT-k életciklusa a támadás, azaz a műveleti hatás kiterjesztését is tartalmazza.[14]

Nyilvánvalóan az információszerző és -feldolgozó képesség feltételezi a nemzetbiztonsági szolgálatok kiberhírszerzéssel foglalkozó szervezeti elemeivel fenntartott folyamatos és kétirányú kapcsolatot, de ugyanígy jelenti a nyílt forrásokból rendelkezésre álló információk gyűjtését, amelybe ma már a közösségi platformok segítségével folytatott információgyűjtő képesség is beletartozik. Természetesen a nyílt forrású információgyűjtésnek is vannak jogszabályi feltételei, illetve az azok által leírt attribútumai, amelyek meghatározzák ezt a fajta információgyűjtési tevékenységet.

Az információszerzés és -értékelés képessége önmagában azonban nem elegendő a kibertámadások hatékony végrehajtásához. Emellett szükséges még a célpontok azonosítása, priorizálása és elosztása is.

A célpont-azonosításhoz, csakúgy, mint a műveletтervezéshez szükséges egy teljes és valós kiberhelyzetkép kialakítása. A kiberhelyzetkép alapját az információszerző és -elemző tevékenység adja, így biztosítva lehetőséget a saját, a semleges, illetve a szemben álló fél erőforrásainak feltérképezésére. A kiberhelyzetkép birtokában van lehetőség a célok azonosítására, azok kijelölésére és priorizálására. Ezekben a tevékenységekben az egyik legfontosabb feladat – alapozva az információszerzés által rendelkezésre álló adatok és információk, valamint az így kialakított előzetes kiberhelyzetkép összességére – a szemben álló fél hálózatai technikai kialakításának (például topológiájának, védelmi hardvereinek és szoftvereinek), valamint védelmi mechanizmusainak a meghatározása.

Ezt követően, a kiberművelet céljainak ismeretében történhet meg a kibertér kulcsterületeinek, illetve a műveletek fő irányainak meghatározása. Ezek a célok attól függően változhatnak, hogy önálló kiberművelet végrehajtása a cél, vagy egy más domainben történő művelet kibertéri támogatásáról beszélünk.

Ezek ismeretében van lehetőség a felhasználható humán és technikai erőforrások kijelölésére, az erők elosztására, valamint ekkor kerülhet sor a kiberműveletek

[14] Kovács (2018): i. m. 154.

hatásainak vizsgálatára. Az erők elosztása magában kell, hogy foglalja az olyan nem, vagy nem csak kinetikus képességeket jelentő erőket is, mint például az elektronikai hadviselés erőinek és eszközeinek a feladat-végrehajtásához szükséges mértékben történő elosztása.

Ugyanakkor már az információszerzés időszakában felmerül egy nagyon komoly kérdés: a kiberhírszerés (információszerzés) volumene nem aggregál-e önmagában kibertámadást a másik, azaz az ellenérdekelt fél oldaláról? A kiberfelderítés, annak céljától függetlenül elérheti azt a küszöbszintet, amikor az ellenérdekelt fél azt a támadások előkészítéseként értékelheti, amely magával hozhatja a szemben álló fél kibertámadásainak megindítását.

Mindezekre már a szimulációs képességek alkalmazása során fény derülhet, megfelelően beállított, akár tapasztalati úton megszerzett indikátorok vagy küszöbértékek alkalmazásával. A szimuláció során ezen kívül a tervezett kibertámadások időrendiségének, a kinetikus és más nem kinetikus műveleteknek a végrehajthatóságát, azok megfelelő szinkronizációjának az ellenőrzését, valamint a tervezhető járulékos hatásokat is be kell mutatni. A szimuláció során lehetőség van a tervezett kibertámadások módjainak és eszközeinek a finomhangolására, valamint – az előbbiek figyelembevételével – azok hatásainak előzetes felmérésére.

3.2. A kibertámadás képessége[15]

A fentiekben megfogalmazott információszerző, célazonosító, célkiválasztó képességek és azok hatékony alkalmazása a kibertámadások előfeltételei. A megszerzett információkra alapozva, azok elemzése és értékelése után lehet a fizikai dimenzió(k)-ban folytatott műveletek részeként vagy önállóan a kibertámadást vagy kibertámadások sorozatát végrehajtani. Jelen írás nem kíván állást foglalni abban a teoretikus vitában, amely szerint nincs külön felderítés, illetve információszerzés a különböző műveleti terekben. Katonaszakmai körökben sokszor elhangzó vélemény, hogy egy felderítés létezik. Ezt támasztja alá a felderítés alapelveinek egyik legfontosabbika, amely szerint a felderítésnek centralizáltnak kell lennie, mert csak így biztosítható a felderítő erők és eszközök hatékony elosztása. Ugyanakkor a kibertér speciális jellege miatt ez még sok vitát fog generálni a jövőben, hiszen a kibertérben folytatott szisztematikus információgyűjtés már a felderítési ciklus bizonyos elemeinek újraértelmezését is igényelheti.[16]

A korábban megfogalmazottak szerint a kibertámadás olyan eljárás, amely erőt használ a szemben álló fél kiberterében (vagy azt felhasználva) azzal a céllal, hogy megváltoztassa a szemben álló fél kiberterének elérését, illetve az abban alkalmazott infokommunikációs rendszerek és/vagy entitások működését.

A kibertámadások felépítését alapvetően azok célja határozza meg, de még a különböző céllal végrehajtott kibertámadások esetében is fellelhetők azonos és viszonylag

[15] Jelen írásban nem cél annak vizsgálata, hogy milyen konkrét cél vagy célok ellen, illetve milyen jogi háttérrel és/vagy felhatalmazással történik a kibertámadó képességek alkalmazása.

[16] Haig Zsolt et alii: *Elektronikai hadviselés.* Budapest, Nemzeti Közszolgálati Egyetem, 2014. 26.

jól tipizálható támadási fázisok. Ebből következően önmagában a kibertámadások életciklusa látszólag nem sokban különbözik egymástól akkor, ha polgári rendszerek, illetve, ha katonai rendszerek ellen mint célpontok ellen alkalmazott támadásokról beszélünk. Bár nagyon sok eljárás és mód létezik a kibertámadások kivitelezésére, azok életciklusának elemei a korábbi megállapításunk szerint jól tipizálhatók. Ez olyannyira igaz, hogy a kibertámadások életciklusára néhány éve már egy szakmai kifejezést is alkotott a Lockheed Martin amerikai hadiipari cég, akik *Cyber Kill Chain*nek nevezték el a korai információszerzéstől a beavatkozásig tartó folyamatot. A cég ezt a folyamatot hét tipikus fázisra osztotta, amelyben a felderítés, előkészítés, bejuttatás, kiterjesztés, telepítés, vezérlés és a támadó eredeti céljának megfelelő tevékenység végzése mint fázisok különíthetők el.[17]

A szemben álló fél kiberműveleteibe offenzív módon történő beavatkozás, a fentiekben megfogalmazottak szerinti proaktivitást figyelembe véve azt is jelenti, hogy a támadások előtt elemeznünk kell és pontosan meg kell határoznunk a kibertámadás végrehajtásának minden egyes cikluselemét.

Katonai területre vonatkoztatva, azaz katonai célpontok elleni kibertámadások alkalmazása során nyilvánvalóan a szemben álló fél vezetési rendszereinek, illetve az azokban alkalmazott információs rendszereinek gyenge vagy sérülékeny pontjainak támadása lehet a leghatékonyabb.

Az offenzív kibertérműveletekkel elérni kívánt kiberhatás kiváltása során, a felfedezett sebezhetőségek alapos feldolgozása után lehetőség nyílik a célrendszert működésében befolyásolni a rendelkezésre álló támadóképességek és erőforrások típusai alapján. Ezek az erőforrások kiberfegyvereknek is nevezhetők, hiszen céljaikban a hagyományos – kinetikus elven működő – fegyverekhez hasonlóak. Ezek a célok nem mások, mint a célpont(o)k pusztítása, lefogása, működésük időleges vagy teljes akadályozása, azok hatásainak csökkentése, vagy a hatásuk kiváltásának megakadályozása.

Ugyanakkor a kibertámadások hatékonyságának maximalizálása érdekében azokat mind egymással, mind a kinetikus műveletek végrehajtásával szinkronizálni kell. Ez a szinkronizáció egyfajta koordinációt is jelent, amely hatalmas kihívás elé állítja az eltérő műveleti terekben, és ahogy korábban utaltunk rá, akár földrajzilag eltérő helyeken műveleteket folytatókat. Ugyanakkor ez a koordináció elengedhetetlen, hiszen a kiberműveletek – benne a kibertámadásokkal – időben sok esetben megelőzik a kinetikus műveleteket (például a szemben álló fél vezetési rendszereinek lefogása céljából), amely kibertámadásokat ezért fedetten és/vagy álcázottan kell végrehajtani. A térben, időben és eljárásaikban koordinált műveletek egymás hatásait erősítik.

Az offenzív kiberműveletek tehát, függetlenül attól, hogy önállóan vagy más műveleti térben végrehajtott műveletek részeként hajtják végre, a kinetikus műveletek hatékonyságát növelik. A kibertámadások nemcsak a kibertérben, hanem a fizikai térben és a kognitív dimenzióban is kifejtik hatásukat.

[17] Lockheed Martin: *The Cyber Kill Chain.* 2021.

3.3. A hatások értékelésének képessége

A hatáskiváltás értékelésének képessége magában foglalja a művelet sikerességének értékelését. Amennyiben szükséges, akkor a célpontáthelyezés, a célhelyesbítés vagy a hatáskiváltó erőforrások cseréjére, illetve azok megváltoztatására is ki kell terjednie.

A hatások értékelése nemcsak a kibertérben kell, hogy megtörténjen, hanem az érintett többi műveleti – fizikai és/vagy kognitív – térben is. A hatások értékelése, a járulékos (közvetett) hatásokra és esetleges veszteségekre kiterjedően kell, hogy megvalósuljon.

4. Offenzív kiberképességek stratégiai megfontolásai és az attribúció

A kibertámadó képességek a stratégiai elrettentés célját is szolgálhatják. Ugyanakkor szintén kérdésként merül fel az, hogy a kibertámadó képességek csak abban az esetben szolgálják-e az elrettentést, ha maguk a képességek nyilvánosságot kapnak. Ez rögtön azt a problémát is magával hozza, amely a valós képességek nyilvánosságra hozásában, majd azok bizonyításában jelentkezik. A stratégiai kibertámadó képességek ugyanis csak abban az esetben jelentenek stratégiai elrettentést is, ha azok hitelesek. Ugyanakkor ez egy valódi paradoxon lehet, hiszen ezeket a képességeket egyik ország sem szívesen hozza nyilvánosságra – maximum utal ezekre –, mert azok részletes technikai adatai, illetve a képességek mibenléte (az eljárásmódok, a már alkalmazott eszközök és azok hatásai, vagy az azokból levont részletes következtetések) a szemben álló fél részére a védekezéshez szükséges alapvető információkat jelentené.

A nyilvánosságra hozott kibertámadó képességek egyik példáját Németország esetében láthatjuk. Németország a NATO számára felajánlotta mind kibervédelmi, mind kibertámadó képességeit.[18] Ugyanakkor fontos hangsúlyozni, hogy a NATO az offenzív kiberképességekre mint a tagállamok által önként felajánlott és alkalmazott képességekre tekint. Erre a SCEPVA *(Sovereign Cyber Effects Provided Voluntarily by Allies),* azaz nem szó szerinti fordításban a „Szövetségesek Önkéntes Hozzájárulásán Alapuló Kiberhatásai" kifejezést is megalkotta.[19] Ezt jelen tanulmány 2. részében külön is elemezzük.

Ugyanakkor mégis szükséges lehet az offenzív képességek valamilyen szintű bemutatása a már említett elrettentés céljából. Erre talán jó megoldás annak stratégiai szintű dokumentumokban való megjelenítése.

Amennyiben a stratégiai elrettentés kérdését és annak közelmúltban játszott szerepét vizsgáljuk, akkor azt megállapíthatjuk, hogy az elrettentés a hidegháborúban alapvetően a nukleáris elrettentő erőre épült.[20] A hidegháború végével az elrettentés intézménye azonban nem tűnt el teljesen, sőt a 21. század hajnalán a kérdés ismét előkerült.

[18] Pierluigi Paganini: Germany makes its cyber capabilities available for NATO alliance. *Security Affairs,* 2019.
[19] AJP-3.20 (2019): i. m.
[20] Kovács László: *Kiberbiztonság és -stratégia.* Budapest, Dialóg Campus, 2018. 28.

Az elrettentés ma a NATO stratégiájában nagyon hangsúlyos szerepet kap.[21] Bár ma már nem elsősorban a nukleáris, hanem a hagyományos, konvencionális fegyverekre alapozott elrettentésről beszélhetünk, de az elrettentés maga újra a biztonság- és védelempolitika egyik fontos elemének tekinthető a legmagasabb szinten. A NATO 2018-as brüsszeli csúcsértekezletén született döntés ezt tovább erősíti, hiszen az elrettentés a NATO Európa keleti felén való jelenlétével még nagyobb hangsúlyt kap. Ezt a csúcsértekezlet zárónyilatkozata a következőképpen tartalmazta: „Továbbra is reagálunk a megromlott biztonsági környezetre az elrettentés és a védelmi politikánk fokozásával, ideértve a Szövetség keleti részén való megjelenését is."[22] A zárónyilatkozat arra is kitér, hogy a Szövetség elrettentési és védelmi politikája minden műveleti térre, így a kibertérre is vonatkozik.[23]

A kibertérre vonatkoztatva az elrettentés mint védelmi elv nem működik, legalábbis sokáig számos ország ezen a véleményen volt. Ez azonban a biztonságpolitikában a fentiekben megfogalmazott – alapvetően a hagyományos fegyverekre épített – elrettentés politikájának újbóli bevezetésével párhuzamosan megváltozott.[24] Így ma sok ország a stratégiai dokumentumaiban rögzíti is a kibertéri elrettentést. Az elrettentés az Egyesült Államok Védelmi Minisztériuma egyik korábbi, 2015-ös kiberstratégiájában így jelenik meg: „A fokozódó fenyegetés, amellyel szembe nézünk, szükségessé teszi, hogy Védelmi Minisztérium hozzájáruljon egy átfogó kiberelrettentési stratégia kidolgozásához és végrehajtásához, annak érdekében, hogy megakadályozza a legfontosabb állami és nem állami szereplőket amerikai érdekek elleni kibertámadások elkövetésében."[25]

Így tesz hazánk is, hiszen a 2020 tavaszán megjelent új nemzeti biztonsági stratégiában az elrettentés fogalmi körében is értelmezhető kijelentést tesz: „Magyarország a fizikai biztonságot veszélyeztető vagy jelentős anyagi károk okozására képes kiberképességeket fegyvernek, alkalmazásukat fegyveres agressziónak tekinti, amelyre a fizikai térben megvalósuló válaszadás is lehetséges."[26]

A kibertérben megvalósuló elrettentés, illetve annak stratégiai dokumentumokban való megjelenítése több részből áll. Egyrészt a fentiekben megfogalmazott reális képességeken kell, hogy alapuljon, azaz olyan erős és robusztus, megbízható védelmet kell kiépítenünk, hogy annak áttörése csak aránytalanul nagy energiabefektetéssel legyen megvalósítható a szemben álló fél vagy a potenciális szemben álló fél részéről. Másrészről egy, a szemben álló fél részéről elkövetett esetleges kibertámadással szembeni – ahogy a magyar nemzeti biztonsági stratégiában is megjelenik – akár a fizikai térben megvalósuló választ vagy válaszokat kell kilátásba helyezni. Az elrettentés egy harmadik összetevője az attribúció lehet. Bár nem minden ország él ezzel, ez nem jelent mást, mint az adott kibertámadás elkövetőjének nyilvános megnevezését. Ez azonban nem jelenthet puszta gyanúsítást, hanem konkrét tényeken és bizonyítékokon kell

[21] NATO: *Deterrence and Defence.* 2021.
[22] NATO: *Brussels Summit Declaration.* Brussels, 2018.
[23] NATO (2018): i. m.
[24] Kovács László: A kiberbiztonság és a kiberműveletek megjelenése Magyarország új nemzeti biztonsági stratégiájában. *Honvédségi Szemle,* (2020), 5. 9.
[25] US Department of Defense: *The Department of Defense Cybersecurity Strategy.* 2015. 10.
[26] 1163/2020. (IV. 21.) Korm. határozat 101. pont.

alapulnia, hiszen egy adott esetben ez a megnevezés nemzetközi feszültségekhez vezethet, főleg abban az esetben, ha az adott kibertámadást állami támogatással követték el, és az attribúció során az adott – a támadást közvetlenül vagy közvetett módon támogató – országot meg is nevezzük. A hazai nemzeti biztonsági stratégia is megemlíti azonban azt, hogy az attribúcióhoz szükséges technikai bizonyítás nagyon nehéz és nem is minden esetben lehetséges: „A kiberműveletek sokszor nehezen bizonyítható attribúciójára, az elkövető azonosítására, megnevezésére való tekintettel a válaszlépések különösen körültekintő, eseti elbírálást igényelnek az érintett kormányzati szervezek bevonásával."[27]

Azt azonban kijelenthetjük, hogy az elrettentés, akár az attribúcióval közösen valóban működhet a kibertérben, ehhez azonban a technikai megoldásoktól – beleértve az offenzív képességek kialakítását is – kezdve számos elemet stratégiai szinten kell megjeleníteni. Ezek közösen valóban hozzájárulhatnak egyfajta elrettentésként ahhoz, hogy a szemben álló fél elálljon a kibertérben tervezett rosszindulatú, ártó szándékú tevékenységétől.

A kibertéri elrettentés azonban önmagában kevés eredménnyel jár akkor, ha nemzeti biztonsági stratégiájának szintjén nincsenek meg mellette a megfogalmazott egyéb elrettentési megoldások, mint például az offenzív kiberképességek.

5. Úton a kiberhadviselés felé

A kibertérben végzett műveletek, benne nemcsak a védelmi célú, hanem az offenzív kiberműveletek felértékelődése napjainkban nem kétséges.

A kiberképességek fejlődésével azonban a hadviselés is változik. A kibertéri tevékenységek ma két alapvető részre oszthatók. Az első kategóriába az önálló kiberműveletek tartoznak, amelyek zömmel békeidőben történnek, és amelyek során a konfliktus háborús küszöb alatt tartása a cél. Ezek a kiberműveletek a hibrid műveletek pilléreiként is felfoghatók, azok részeként és/vagy azokkal párhuzamosan folynak. A másik kategóriába azok a kiberműveletek tartoznak, amelyek egy fegyveres konfliktus során a kinetikus műveletek, tehát a hagyományos műveleti terekben folytatott katonai műveletekkel párhuzamosan, azok hatásainak növelése érdekében folynak.

Katonai területen ezek a műveletek nemcsak stratégiai szinten, hanem hadműveleti és harcászati szinten is jelentkeznek. Ezeket a kiberműveleteket integrálni kell a szárazföldi erők és a légierő megfelelő szintű műveleteibe. Az így megjelenő komplex – több dimenzióban egyszerre jelentkező – műveletek célja a szemben álló fél vezetési rendszerének megbontása, működésének akadályozása és lassítása. Az azonos időben, de több dimenzióban végrehajtott műveleteket ma egyre többször multitérműveleteknek nevezzük. Ennek lényeges eleme az, hogy egy időben több olyan művelet is zajlik, amelyek bár egymást támogatják, segítik, mégis más dimenziókban (például szárazföld, levegő, elektromágneses spektrum, kibertér) történik azok végrehajtása. Az Amerikai Egyesült Államok hadseregének doktrinális központja, a US Tradoc már 2018-ban megjelentetett olyan tanulmányt, amely a multitér-hadviselés utódjának

[27] 1163/2020. (IV. 21.) Korm. határozat 101. pont.

tekinthető multitérműveleteket elemezte. Az ebben megfogalmazott legfontosabb problémára – azaz a miért is kell multitérműveletekről beszélni? – a dokumentum a választ az USA versenytársainak – elsősorban Kína és Oroszország – rendkívül gyorsan fejlődő technikai és műveleti képességeiben adta meg. Ezek a képességek lehetővé teszik – a tanulmány megfogalmazása szerinti versenytárs országoknak –, hogy érdekeiket egyszerre több dimenzióban végrehajtott műveletekkel, azokat összehangolva, egymást támogatva, hajtsák végre és így érjék el a céljaikat.[28] Ezek a célok a korábban említett vezetés megbontásán túl akár békeidőben az államigazgatás működésének megbontását, vagy akár gazdasági válság előidézését is jelenthetik. Az ezeknek az akcióknak köszönhetően bekövetkező instabilitás természetszerűleg gyengíti az adott célországot, másrészről pedig megkönnyíti a további destabilizációs műveletek végrehajtását.

Ugyanakkor nagy valószínűséggel már a közeljövőben eljutunk arra a pontra, amely során már nem választható élesen szét e két kategória és az azokban folytatott kiberműveletek. Eljutunk a valódi kiberhadviselésig, amely során már nem csak állami támogatású csoportok, hanem államok vívnak egymással küzdelmet a kibertérben. Ennek célja nem lesz más, mint a kibertérben is kivívni azt a fölényt, amely a teljes győzelem kivívásának és nem utolsósorban e győzelem fenntartásának egyik alapfeltétele lesz. E pont lesz az, amikor már nem lesz élesen szétválasztható az említett két kiberműveleti kategória határa.

A kibertéri fölény megtartása azonban összetett feladat, amely nemcsak a szemben álló fél képességeinek, lehetőségeinek és céljainak ismeretét feltételezi, hanem egy olyan komplex tevékenységet is takar, amelyben a fizikai tér, a kibertér és az információs tér kihívásai egyszerre kezelhetők.[29]

A fentieket összefoglalva ma még talán kissé futurisztikusnak, sőt analógiáját tekintve kissé tudománytalannak tűnhet Douhet légifölény-elméletével[30] párhuzamot vonni a kibertéri fölény fontosságát illetően. Azonban a fentiekben megfogalmazottak alapján kijelenthető, hogy aki a jövőben a fegyveres vagy más konfliktusokban a győzelmet meg kívánja szerezni, azt meg kívánja tartani, annak – a hagyományos fizikai műveleti terekhez hasonlóan – a kiberteret is uralnia kell. A kibertéri fölény alapvető módon fog hozzájárulni a győzelemhez.

A kibertéri fölény kivívásához pedig az egyik igen fontos összetevő az offenzív kiberképességek megléte.

6. Következtetések

A 21. században a biztonság abszolút módon több dimenzióban jelentkezik. Mégis, talán ma egy fejlett nyugati ország biztonsága a gazdasági biztonságán alapul. A gazdaság viszont ma már azoktól az infokommunikációs rendszerektől függ, amelyeket a kibertéri működéssel jellemezhetünk a legjobban. Ebből következően a kibertér

[28] TRADOC Pamphlet 525-3-1: *The U.S. Army in Multi-Domain Operations 2028.* 2018. 9.
[29] Haig Zsolt: *Információs műveletek a kibertérben.* Budapest, Dialóg Campus, 2018.
[30] Guilio Duehet: *The command of air.* Alabama, Air University Press Maxwell Air Force Base, 2019.

biztonsága közvetett módon – a gazdaságon keresztül – az adott ország teljes biztonságára hatással van. Így a kibertér biztonságának megteremtése stratégiai célból is alapvetően szükséges, hiszen a kiberhadviselés megjelenésével a gazdasági biztonság mellett a katonai biztonság is ismét kiemelt szerepet kap.

A kibertér biztonsága komplex tevékenységek sorozatából áll az oktatás, képzés, felkészítéstől kezdődően a magas szintű kibervédelmi kutatás-fejlesztésen át a kibervédelem technikai és technológiai megvalósításáig. Mégis van egy terület, amely az elmúlt időkben kezd csak nagyobb figyelmet kapni, ez pedig a kibertámadó képességek fejlesztése és azok a védelem érdekében történő felhasználása. Ugyanakkor, jelen írás összegzett következtetéseként kijelenthető, hogy a kibertámadások képessége csak egy részösszetevője az offenzív kiberképességeknek. A megalapozott kiberhelyzetkép, amely információszerző és -elemző tevékenységek egész sorát feltételezi, ugyanúgy része az offenzív képességeknek, mint a hatások értékelésének és a lehető legpontosabb előrejelzésnek a képessége.

Mindezeknek megfelelően a fenti elemzések egyik legfontosabb következtetése az, hogy az offenzív kiberképességek kialakítása komplex tevékenységek sorozatán keresztül jön létre, hiszen ez jóval túlmutat a kibertámadó képességek puszta meglétén, illetve azok alkalmazásán.

Ezeken kívül azonban stratégiai szintű – nem elsősorban a kibertérben meglévő – összetevők is szükségesek a kibertéri kihívások kezeléséhez, így az offenzív kiberképességek alkalmazásához. Ez pedig nem más, mint az adott ország biztonsági és védelmi stratégiai dokumentumaiban rögzített, majd jogszabályokban is megjelenő akarata és vállalásai ezen a területen. Ez jelenthet stratégiai elrettentést, de emellett jelentheti valódi és hatékony kiberműveleti alkalmazás lehetőségének a meghatározását is.

Persze számos kérdés felmerül a kiberműveletekkel, és így az offenzív kiberképességek birtokában meglévő kibertámadó műveletekkel kapcsolatban. Az egyik ilyen kérdés pont a fentebb megfogalmazott jogszabályi háttérrel kapcsolatos: alkalmazhatunk-e katonai kibertámadó műveleteket akkor, amikor a háború időszaka még nem deklarált? Hol kezdődik, és hol vannak a határai a nemzeti szuverenitásnak a kibertérben? Az ezekre a kérdésekre adható válaszok alapvetően befolyásolják azoknak az offenzív képességeknek az ellenoldali alkalmazását, amelyek még anélkül alkalmazhatók, hogy az szélesebb konfliktushoz vezetne. Ugyanakkor ez ahhoz a kérdéshez is elvezet, miszerint békeidőszakban, még háborús küszöb alatti tevékenység esetén alkalmazhatók-e a katonai kiberműveletek, benne a kibertéri információszerző és esetlegesen kibertámadó képességek?

A fentiek rögtön további problémafelvetést is indukálnak. Ezek közül az első az, hogy egy katonai kiberművelet nem vezet-e a szemben álló fél részéről olyan válaszhoz, amely kinetikus műveletek alkalmazása lesz?

Talán ezek a legfontosabb megoldandó kérdések, amelyek inkább jogi megfontolásokat és megoldásokat igényelnek nemzeti és nemzetközi szinten egyaránt, semmint a technikai képességek kialakítását. Ugyanis ez utóbbiak már megtörténtek. Azok alkalmazása csak idő kérdése.

Végül egy igen fontos következtetést kell levonni a fentiekben megfogalmazottak alapján. Ez pedig nem más, mint annak kijelentése, hogy aki a jövőben a fegyveres

vagy más konfliktusokban, például a hibrid műveletekben a győzelmet meg kívánja szerezni, azt meg kívánja tartani, annak – a hagyományos fizikai műveleti terekhez hasonlóan – a kiberteret is uralnia kell. Ebből következően megállapíthatjuk, hogy a kibertéri fölény alapvető módon fog hozzájárulni a győzelemhez.

Felhasznált irodalom

Duehet, Guilio: *The command of air.* Alabama, Air University Press Maxwell Air Force Base, 2019.

Haig Zsolt – Kovács László – Ványa László – Vass Sándor – Németh András (szerk.): *Elektronikai hadviselés.* Budapest, Nemzeti Közszolgálati Egyetem, 2014.

Haig Zsolt: *Információs műveletek a kibertérben.* Budapest, Dialóg Campus, 2018.

Kiss Álmos Péter: A hibrid hadviselés természetrajza. *Honvédségi Szemle,* 147. (2019), 4. 17–37. Online: https://honvedelem.hu/files/files/116701/hsz_2019_4_017_037_4557.pdf

Kovács László – Sipos Marianna: A Stuxnet és ami mögötte van: Tények és a cyberháború hajnala. *Hadmérnök,* 5. (2010), 4. 163–172.

Kovács László: *Kiberbiztonság és -stratégia.* Budapest, Dialóg Campus, 2018.

Kovács László: *A kibertér védelme.* Budapest, Dialóg Campus, 2018.

Kovács László: A kiberbiztonság és a kiberműveletek megjelenése Magyarország új nemzeti biztonsági stratégiájában. *Honvédségi Szemle,* (2020), 5. 3–18. Online: https://doi.org/10.35926/HSZ.2020.5.1

Lockheed Martin: *The Cyber Kill Chain*. 2021. Online: www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

NATO: *Allied Joint Doctrine for Cyberspace Operations, AJP 3.20.* NATO Standardization Office, 2019.

NATO: *Brussels Summit Declaration.* Brussels, 2018. Online: www.nato.int/cps/en/natohq/official_texts_156624.htm?selectedLocale=en

NATO: *Deterrence and Defence.* 2021. Online: www.nato.int/cps/en/natohq/topics_133127.htm

Paganini, Pierluigi: Germany makes its cyber capabilities available for NATO alliance. *Security Affairs,* 2019. Online: https://securityaffairs.co/wordpress/81125/cyber-warfare-2/germany-nato-alliance-warfare.html

Smeets, Max – Herbert S. Lin: Offensive cyber capabilities: To what ends? In T. Minárik – R. Jakschis – L. Lindström (szerk.): *2018 10th International Conference on Cyber Conflict CyCon X: Maximising Effects.* Tallinn, NATO CCDCOE Publications, 2018. 55–72. Online: https://doi.org/10.23919/CYCON.2018.8405010

TRADOC Pamphlet 525-3-1: *The U.S. Army in Multi-Domain Operations 2028.* 2018. Online: www.tradoc.army.mil/portals/14/documents/mdo/tp525-3-1_30nov2018.pdf

US Department of Defense: *The Department of Defense Cybersecurity Strategy*. 2015. Online: https://archive.defense.gov/home/features/2015/0415_cyber-strategy/final_2015_dod_cyber_strategy_for_web.pdf

Jogi forrás

1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról