https://doi.org/10.56233/SZABADPIAC.2022.2.3

Nyáry Gábor:

KÖD ÉS FÉNYSUGÁR. A KIBERHADVISELÉS DILEMMÁI A GEOPOLITIKAI KONFLIKTUSOK ÚJ „SZÜRKE ZÓNÁJÁBAN"

Bevezetés

A szemünk előtt, a közvetlen szomszédságunkban véres háború dúl, és ez óhatatlanul vonzza a tekintetünket. De ne legyenek kétségeink: veszélyes konfliktusok terepe (megint) szinte az egész Földgolyó. Az életünket szinte felismerhetetlenségig megváltoztatja, jó értelemben veszélyekkel együtt is a digitalizációnak nevezett drámai átalakulás. Nem csak a technológia változik, de a minket körülvevő világ is. A szovjet-amerikai nagyhatalmi szembenálláson alapuló, kétosztatú világrendet – a Szovjetunió bukását követően – felváltotta az Egyesült Államok hegemóniája. Ez az „egypólusú" berendezkedés azonban Amerika külső és belső gyengülése, illetve erős riválisok felemelkedése következtében lebomló félben van. Napjaink realitása immár a többpólusú világrend: az USA mellett Kína, Oroszország, de India, Irán és mások is részesei a hatalmi egyensúlynak. A hidegháború éles szembenállást jelentett, de világosak és kölcsönösen elfogadottak voltak a szabályok. Ma az egyéni érdekérvényesítés és a szabályok nélküliség a jellemző, ami jól illeszkedik a kiberhadszínterek átláthatatlan, képlékeny dimenzióihoz. Valóságos, „hagyományos" háborúban csapnak össze az ellentétek, de ugyanakkor az információ, a dezinformáció körül kavargó információs hadviselés is igazi csatatereket idéz, és a kibervilág is igazi hadszíntérnek tűnik sokak szemében. A XIX. század elejének nagy teoretikusa, a porosz Clausewitz munkássága óta mindent tudni vélünk a háborúról, ám napjaink eseményei mintha fejük tetejére fordítanák ezeket az öröknek gondolt igazságokat is. Szakemberek, a nemzetközi kapcsolatok, a kiberbiztonság kutatói vitatkoznak olyan alapvető kérdéseken, hogy a digitális tereket is elborító támadások, akciók háborúnak tekinthetők-e (Sharma, 2010)? Vajon, egyáltalán használhatók még ezek a fogalmaink? Ha igen, akkor hogyan?

Emlék a múltból: a stratégiai pusztítás gondolata gyökeret ver

1940. november 14-én este, a hitleri Németország 3. Légi hadseregének 515 nehézbombázója a magasba emelkedett. A gépek a Londontól észak-nyugatra elterülő Coventry városa felé vették az irányt. Lényegében ellenállás nélkül közelítették meg a mit sem sejtő települést, és pusztító bombazáport zúdítottak a páratlan műemlékekkel is rendelkező, fontos ipari központra. A terv, ma már tudjuk, nem az ipari övezetek elérése volt: a 33.000 gyújtóbombával a sűrűn lakott polgári negyedeket vették célba. A város történelmi negyedei romba dőltek, a halálos áldozatok száma több százra rúgott. A II. világháború elején, az Anglia elleni német légi háború nyitó időszakában történt az eset, amely fordulópontot jelentett a légi hadviselés akkor még újnak számító gyakorlatában (Overy, 2015).

Tömegipar és a totális háború

A megelőző, 1914 és 1918 között zajló nagy háború időszakában életre hívott repülőcsapatok sokáig csak a megfigyelő, felderítő szerepet mondhatták magukénak. A két világháború közötti időszakban aztán, párhuzamosan a repülőtechnika gyors fejlődésével, a világ katonai teoretikusai, kezdetben persze csak elméleti alapvetésekben, kutatni, vitatni kezdték a születőben levő új fegyvernem lehetséges alkalmazásait. Talán meglepő, de egy itáliai tábornok, Giulio Douhet képzeletében fogant meg először a gondolat, hogy a repülő szerkezetek, erős robbanóanyagokat szállítva, az arcvonalak fölötti egyszerű csetepatéknál sokkal drámaibb módon is befolyásolhatnák a hadviselés menetét (Hippler, 2013). Az olasz generális, az Égbolt meghódítása című meghatározó könyvében a stratégiai bombatámadások elméletét fektette le. Azt vallotta: az új hadszíntér, a levegőég eme új fegyverei, a repülőgépek egymagukban képesek lehetnek eldönteni a jövőben a háborúk kimenetelét. Nem azt állította, hogy az új fegyverek, a távolból felemelkedve és megközelítve a célt, képesek teljesen romba dönteni annak infrastruktúráját. Douhet a tömegbombázások morális eszközként való alkalmazásában hitt: azt állította, hogy a polgári célpontok, mai megfogalmazással, a kritikus infrastruktúrák elleni tömeges támadások képesek lehetnek arra, hogy megtörjék az ellenség harci kedvét, lelki erejét. Az olasz katonai gondolkodó a totális háború elvét rajzolta fel, ahol mindenki, az egész társadalom harcoló fél, egyben ellenség.

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

A digitalizáció Douhet tábornokai – a héjják

Ez az egyik, bizonyára a pesszimistább perspektíva, ami az év elején Ukrajnában kibontakozó véres háború kapcsán a kibertérben zajló akciókhoz és hadműveletekhez kapcsolódva az eszébe ötlik az embernek. Pontosabban: az egyelőre szinte még nem vagy csak alig zajló akciók és hadműveletek kapcsán. A szakemberek egy része lényegében az orosz invázió kezdete óta azt kérdezgeti: hol marad a mindent elsöprő – és a tankoszlopokat, repülőgépeket megelőző – digitális csapás? A mindent eldöntő, új hadialkalmazás, azaz a „kiberháború"? A kiberbiztonsági szakma, a katonai vezetők és a politikusok évek óta mondják, hogy a geopolitikai szembenállás legújabb terepe, a kibertér uralására koncentráló Oroszország pusztító csapással avatja majd fel a 21. század új, kiberharcmodorát, amint összeütközésbe kerül a Nyugattal (Gartzke, 2013). A feltételezés természetesen nem volt alaptalan, hiszen az elmúlt években, de inkább évtizedben jó néhány olyan incidensre került sor a kibervilágban, amelyet az orosz állam intézményeihez kapcsol a biztonsági szakma. Az Ukrajnával kirobbant véres és 2014 óta elhúzódó konfliktus a szomszédos ország, az orosz állami hackerszervezetek egyfajta kísérleti terepévé, laboratóriumává vált. Az eddigi időszak egyik legveszélyesebb, és globális szinten is roppant károkat okozó kibertámadása, valamint a középpontjában álló, hírhedt NotPetya kiberkártevő is az ukrajnai polgári infrastruktúrák elleni orosz hackertámadással indult útjára 2017-ben.

Baljós előjáték, az ukrán energiahálózat elleni támadások 2015-ben

Előzmények, figyelmeztető jelek, esetek természetesen már korábban is előfordultak. A legnevezetesebb akciósorozat 2007-ben Észtországot bénította meg néhány napra. A helyi orosz kisebbség politikai képviseletei és az észt kormányzat közötti (egy szimbolikus kérdésben kirobbant) éles ellentétek pillanatokon belül kibertámadások sorát indították el. Napokra kiesett az észt közigazgatás elektronikus rendszere, de a bankok, napilapok, műsorszolgáltatók webhelyei is elérhetetlenné váltak a koncentrált, túlterheléses támadások nyomán. Számos közintézmény, közszolgáltató szervezet a kisebb horderejű ún. elcsúfító (defacement) támadásokkal volt kénytelen szembesülni. Az első – határokon átnyúló – kibertámadásként emlegetett esemény (amely mögött oroszországi szervezeteket és magányos támadókat sejtettek) egyfajta ébresztőként szolgált a NATO, és általában a nyugati világ kiberbiztonságért felelős döntéshozói számára.

Néhány évvel később, az Ukrajna oroszbarát vezetését leváltó Majdan-forradalom, majd az annak nyomán kibontakozó nyílt, fegyveres küzdelmek szinte az első perctől kezdve kiterjedtek a kibertérre is. A Krím-félsziget orosz annektálása, majd a Donbasz vidékén meginduló fegyveres harcok új korszakot nyitottak a kiberhadviselésben is. A legfigyelemreméltóbb akciósorozat a 2015. év végén vette kezdetét. Vélhetően orosz hackerek – több hullámban – támadást intéztek Ukrajna energiahálózata (az azt üzemeltető intézmények) informatikai rendszerei ellen. Igaz, „csupán" néhány órára (vagy napra), de csaknem negyedmillió fogyasztó maradt energia nélkül, ami riasztó perspektívát festett a kiberfegyverekben rejlő stratégiai potenciálokról.

2017: a NotPetya művelet és a kiberakciók új dimenziója

2017. június 27-én, a közelgő hosszú hétvége előtt, eseménytelen munkanapra készültek az ukrán vállalatok, minisztériumok dolgozói. A másnapi, Alkotmánynapi ünnep családi programjait tervezgető alkalmazottak meglepve tapasztalták, hogy munkahelyi számítógépeiken, bekapcsolás után, csak egy fenyegető felirat jelenik meg a monitoron: „Az ön gépét zároltuk. 300 bitcoin befizetése ellenében biztosítjuk a feloldó kódot." Az országban fontos állami intézmények, minisztériumok, bankok, elektromos társaságok számítógépes rendszerei váltak működésképtelenné. A 21. század egy társadalma előtt hirtelen felrémlett: milyen az, amikor a mindent behálózó számítógépes rendszerek nem használhatók semmire. Az akcióban egy korábban már több helyen felbukkant, „Petya" kódnevű ún. zsarolóvírus aktivizálódott ismét. Vagy legalábbis így tűnt. Érdekes egyébként, hogy a rosszindulatú szoftveres kód itt is, a Windows operációs rendszerek sérülékenységeit kihasználva jutott be a megtámadott gépekbe, hálózatokba. Hamarosan tapasztalni lehetett azt is, hogy a kiberkártevő valójában nem elégszik meg az adatok zárolásával (hogy aztán azokat az elektronikus „pénzben", bitcoinban megszabott váltságdíj kifizetése után megint hozzáférhetővé tegyék). Ez a változat, amit éppen ezért „NotPetyának" kezdtek hívni a védelmi szakemberek, nem pénzszerzési szándékkal készült: egyre nyilvánvalóbbá vált, hogy a cél az adatok végleges törlése, a számítógépes rendszerek használhatatlanná tétele volt. A kiberkártevő azonban hamarosan elszabadult, és egyfajta globális járványban fertőzött meg számítógépes rendszereket szerte a világban. Úgy mondják: ez volt minden eddigi idők legpusztítóbb kibertámadása.

Az előkészületek globális dimenziója: a SolarWinds hírszerzési akció

Bombaként robbant a hír 2020. december közepe táján, hogy ismeretlen hackerek behatoltak az amerikai kormányzat több szervezetének informatikai rendszereibe. Az incidens kiterjedtsége, és az elkövetés ravaszul átgondolt technikája is kezdettől komoly állami szereplőt sejtetett a háttérben. A támadók a texasi SolarWinds cég által forgalmazott, Orion nevű hálózatfelügyeleti szoftver frissítéseibe férkőztek be, és ezen keresztül hónapokon át tudtak hozzáférni mindazon kormányzati és nagyvállalati szereplők informatikai rendszereihez, amelyek ezt a rendszertámogató szoftvert használták. Mások mellett az USA Hadügyminisztériuma, Pénzügyminisztériuma sőt, az atomfegyverek kezeléséért felelős kormányzati hivatal is. De világszerte összesen mintegy 300 000 (!) ügyfél szerepel a listán, potenciális áldozatként.

Az amerikai kormányzat álláspontja az, hogy az elképesztően kiterjedt, hosszú időn át tartó hacker akció mögött az orosz külföldi hírszerző szervezet, az SzVR kiberkatonái álltak. Ennek megfelelően, válaszcsapásként az USA szankciókkal sújtott több érintettnek tartott orosz személyt és szervezetet. Ahogy az ilyen ügyekben már szinte törvényszerű, az „attribúciót", tehát az elkövető azonosítását megalapozó bizonyítékokat nem tárták a közvélemény elé az amerikai hatóságok. Egy dolog azonban bizonyosnak látszik: a SolarWinds néven elhíresült eset valójában kiberkémkedési ügy. Célja a hírszerzés, nem pedig a közvetlen károkozás volt.

A jelmezes főpróba: a Colonial Pipelines megbénítása 2021 nyarán

2021 tavasza. Bekövetkezett. Nem a világvége, de annak valamiféle intő jele. Az Egyesült Államok energiahálózatának egy fontos szegmense, a Colonial kőolajvezeték időlegesen működésképtelenné vált. A cég számítógépeit ugyanis – mint később kiderült zsarolóvírusos – hackertámadás érte. A Colonial kőolajvezeték klasszikus értelemben vett „kritikus infrastruktúra": napi 2,5 millió hordó olajat képes továbbítani a kutaktól a Keleti part fő elosztó csomópontjáig. Szerepe tehát igen jelentős az országrész energiaellátásában.

Az akció, amelynek elkövetőiként veterán, képzett számítógépes bűnözői csoportokat véltek a szakemberek, sok szempontból mérföldkőnek számít. A zsarolóvírusos támadások hullámként borítják most el az online világot. Jellemző célpontjai a társadalmak működését biztosító infrastruktúrák: energia hálózatok, egészségügyi rendszerek, pénzintézetek. A rohamos terjedés magyarázata: egyszerű, szinte bombabiztos „üzletet" kínál a bűnözői csoportoknak – akik mögött egyes feltételezések szerint (hallgatólagosan) állami szervezetek is állhatnak. A megtámadott cégek többnyire fizetnek: így történt ez a Colonial vállalat esetében is, amely 5 millió dollár váltságdíjat szurkolt le. Amerika szakértői között tartja magát a feltételezés: a támadók működését segítette az is, hogy Oroszország (ahonnan a bűnözők akciója kiindult) nem lép fel az ilyen törvénysértők ellen.

Az elmúlt másfél évtized eseményei, kiberincidensei nyomán szakmai körökben meglehetősen erősen elterjedt az a feltételezés, hogy egy eljövendő fegyveres összetűzésnek is fontos kísérője (előkészítője, de talán eldöntője is) lesz a számítógépes infrastruktúra, internetes hálózatok, elektronikus igazgatási és kereskedelmi rendszerek elleni koncentrált támadás (Kostyuk, Zhukov, 2022). Azóta, hogy két amerikai tudós, a híres RAND kutatói közreadták mérföldkőnek számító tanulmányukat, a hadviselés gyökeres átalakulását hirdető digitális stratégiai evangélisták száma egyre növekedett a világban. John Arquilla és David Ronfeld 1993-ban publikált könyve már a címével meghatározta a közgondolkodást. „Cyberwar is coming"(Kiberháború közeleg) hirdette a gyorsan népszerűvé vált munka, ami mély nyomokat hagyott a 21. század stratégiai (és informatikai) szakmájának gondolkodásmódján (Arquilla, Ronfeldt, 1993). Végül pedig: a kibereszközök háborús fegyverként való alkalmazhatósága egy, a közel-keleti erőviszonyokat megbolygató eset nyomán szinte kötelező „hittétellé" vált, szakértői körökben.

Kivétel erősíti a szabályt? A hírhedt Stuxnet-támadás Irán ellen

2010-ben, egy júniusi délutánon az iráni Natanz városka egyik különleges üzemében az ügyeletes főmérnök kétségbeesetten riasztotta a karbantartókat. Amíg a szerelőkre várt, döbbenten nézte a zártláncú ipari tévén, ahogy a B6-os centrifuga a megnövekedett vibrációtól darabokra szakad, egymás után roncsolva szét a sorba kötött gépeket. 2009 nyara óta egymást érték a hasonló balesetek, látszólag minden magyarázat nélkül, és a károk most már veszélybe sodorták az Iráni Iszlám Köztársaság egyik legfontosabb ipari programját. A natanzi üzem dúsított urániumot állított elő, ami a hagyományos atomerőművek „üzemanyaga". És az atombombáké!

A hagyományosan bányászott uránércet előbb tisztítják és koncentrálják, majd különleges eljárással dúsítják a maghasadásra alkalmas, U235-ös izotóp tartalmát. Erre hangsebességgel forgó centrifugákat használnak, amelyeket sorokba – úgynevezett kaszkádokba – kötnek, és a betáplált urán tartalmú gáz, a hosszú folyamat végére, eléri a kívánt izotóp koncentrációt. Az egész eljárást folyamatvezérlő számítógépek irányítják; a Siemens cég által gyártott célgépeken a vállalat különleges vezérlőszoftvere fut, ami arról gondoskodik, hogy a centrifugák forgása mindig egyenletes maradjon. Az iráni szakemberek nem is sejtették: a zárt rendszerként működő, biztonságosnak hitt számítógépes hálózatot különleges digitális kártevő, egy nagyon agyafúrt féregvírus fertőzte meg, amit vélhetően egy közönséges pendrive-on juttattak be a vezérlőbe.

A később Stuxnet-nek keresztelt rosszindulatú kód egy Windows-os biztonsági résen át bejutott a rendszerbe, majd vizsgálódásba kezdett: ha a megtámadott gépen nem talált különleges Siemens ipari vezérlő programot futni – akkor leállította magát. A Siemens rendszervezérlőit azonban megfertőzte és hamis parancsok kiadására kényszerítette, ami állandó sebességváltoztatásra késztette a centrifugákat. Ezek a vibráció hatására hamarosan tönkrementek. Ez volt a világtörténelem első olyan kiberakciója, ahol a támadások közvetlen fizikai károkat okoztak, tehát nem csak az érintett szoftverek, vagy számítógépek sérültek.

2012-ben aztán a New York Times szellőztette meg: a Stuxnet vírust felépítő és Iránra szabadító akció – az Olimpiai Játékok hadművelet – mögött az Egyesült Államok kiberhírszerző ügynöksége, a NSA állt, szoros együttműködésben az izraeli társintézménnyel. Az érintett titkosszolgálatok hivatalosan sohasem erősítették meg ezeket az állításokat. A kibertérben zajló furcsa hadviselés egyik legjellemzőbb jegye éppen ez: csendben, a háttérben zajlanak az akciók. Ha kipattan egy-egy ügy, akkor sem vállalja senki a felelősséget.

Sokan úgy tartják: ezzel az akcióval kezdődött el a kibertér igazi hadszíntérré változtatása: a távolról indított, hálózatokon eljuttatott, informatikai „kártevők", rosszindulatú szoftverek immár fizikai pusztításra is képesek éppen úgy, mint az igazi fegyverek. Legalábbis ez volt a közkeletű vélekedés. Csakhogy hasonló akcióra (bár erről némi vita akad a hozzáértők között) azóta sem került sor a világban.

Károkozók és kiberkatonák: a kibertér különös ökoszisztémája

Célpontok, eszközök, ahogy azt feljebb láttuk, sokfélék a kibertérben. Sokfélék az elkövetők is. A szakértők egyértelműen különválasztják a bűnözők ténykedéseit: ők károkat okoznak ugyan, de nem háborút viselnek. Sokszor azonban elmosódik a határvonal, és szervezett bűnözői csoportok együttműködnek titkosszolgálatokkal, katonai erőkkel (Harknett, Smeets, 2022). Abban is egyöntetű a szakmai vélekedés, hogy az állami szereplők, a „hivatalos" hackercsoportok (tehát a titkosszolgálatok vagy katonai szervezetek tagjai) sem mindig hadviselő felek: a kémkedés például egyértelműen nem számít háborús cselekménynek a kibertérben sem. Ez fontos szempont, hiszen „harci cselekménynek" minősülő kiberakcióra, elvben, akár hagyományos fegyverekkel is lehet ellencsapást mérni.

A tényleges kiberkatonák tartozhatnak országuk valamelyik hírszerző szervezetéhez, de lehetnek egyenruhás katonák is. Fontos az is: általában külön szervezetek, csoportok foglalkoznak a kibervédelemmel, és megint mások feladata az offenzív, támadó kiberakciók

szervezése és kivitelezése. Tulajdonképpen az utóbbiak a kibertér igazi háborús figurái. Ott találjuk őket valamennyi nagyhatalom szolgálatában. Sőt, a közepes és kis országokéban is. Egy néhány évvel ezelőtti kutatás azt mutatta ki, hogy a világ több mint 60 országa tart fenn támadó kiberháborús „képességeket", képzett hackereket, speciális számítógépes eszközöket és főleg megfelelő támadó szoftvereket.

Izrael

Izrael ezen a téren igazi nagyhatalom. Úgy tartják, hogy a közel-keleti ország rendelkezik az egyik legnagyobb kiberhadviselési katonai alakulattal (a híres-hírhedt 8200 sz. egység képében), és a legfejlettebb támadó eljárások, kiberkártevők, kémszoftverek is az izraeli találékonyságot dicsérik. Az ország kétségtelen tekintélye néhány nagy horderejű, ismertté vált akciónak köszönhető elsősorban. Ugyanakkor Izrael kiberhadviselési erejének hírét alátámasztja az a tény is, hogy az informatikai, adattudományi, mesterséges intelligencia kutatások és képzések – az 1970-es évek vége óta – megkülönböztetett figyelmet kapnak az ország polgári és katonai iskolázási rendszerében.

USA

Az Egyesült Államokról szinte soha nem hallunk a kibertér hadviselőiről szóló híradásokban. Ez azonban inkább a gondos álcázásnak tudható be, mert valójában Amerika az egyik legsokoldalúbb, legmagasabb technológiai színvonalú, legnagyobb csapásmérő erővel rendelkező kiberhaderő fenntartója. Természetes is: a világ vezető katonai nagyhatalma a legújabb technológiai küzdőtéren is az elsőségre tör. Az USA kiberhacosainak egy része a haderők kötelékében szolgál. Ugyanakkor a polgári titkosszolgálatok is hatalmas, fejlett technológiájú kiberkapacitásokkal rendelkeznek, a Nemzetbiztonsági Ügynökség, az NSA kifejezetten erre specializálódott.

Oroszország

Oroszország a kibertér mumusa, legalábbis a hírekben. Ebben nyilván jókora adag túlzás is van, ugyanakkor az ország bizonyosan számítástechnikai vezető hatalom, amelyik, kiberképességeit stratégiai szemlélettel veti be, hogy külpolitikai, nemzetbiztonsági céljainak a kibertérben is érvényt szerezzen. Az elmúlt évtizedek több, jelentős kiberakciója is orosz állami hackercsoportok műveként robbant be a köztudatba. A regionális katonai parancsnokságok önálló kiberhadviselési alakulatokkal rendelkeznek, és a vezérkar is külön egységeket tart fenn. Természetesen a hírszerző ügynökségek, a katonai felderítésért felelő GRU és a polgári SzVR is számottevő hackercsoportok felett rendelkezik. Noha az Ukrajna elleni akcióik megmutatták Oroszország károkozó képességeit, valódi meglepetést a kiberhírszerző műveleteik okoztak (a már említett SolarWinds hadművelettel).

Kína

Kína sok területen most robban be az élbolyba, és a kiberhadviselés is ilyen. Hackeralakulatainak fókusza – közvélekedés szerint – a hírszerzés: elsősorban gazdasági, hadiipari jellegű információk megszerzésére specializálódva. Egyes hírek szerint a kínai

hadsereg 100 ezer fős hacker seregtesttel rendelkezik, az ipari titkok megszerzésére. Noha ez túlzásnak tűnik, az a hivatalos dokumentumokból is kitetszik, hogy a Kínai Népköztársaság hadereje a kibertérben való eredményes hadviselést elsődleges célként kezeli. Kína a globális hatalom elsőségére jelentkezett be, és tisztában van azzal, hogy a modern korban a hatalom jókora része a kibertérben tanyázik.

Észak-Korea

A kicsik között kitűnik kiberhadviselési erejével, illetve támadó aktivitásával Észak-Korea. Szakmai vélemények szerint az ország elsősorban a pénzügyi-üzleti hírszerzés területén erős a kibertérben. Ugyanakkor az elmúlt évben több, kifejezetten támadó akció (például a WannaCry kódnevű, globális zsarolóvírusos támadás) mögött is az észak-koreai hackereket gyanították a szakértők. Feltételezések szerint tekintélyes, 6 000 főnyi kiberhadsereg áll az ország kormányának szolgálatában. Erejük titkát abban is sejtik, hogy Észak-Korea katonai költségvetésének egyedülállóan nagy hányadát fordítja a kiberhadviselés fejlesztésére.

Nagy-Britannia, Irán és még sokan mások

Az élbolyban ott találjuk még Nagy-Britanniát, amely az egyik legnagyobb múltú kiberhatalom a világon. Jelentős védelmi kapacitásai mellé – az utóbbi fél évtizedben – folyamatosan építette ki támadó kiberhadviselési erőit is. Az eredetileg 500 fősre tervezett alakulat ma, a hírek szerint az egyik legjobb a világon. A feltörekvő közepes kiberhatalmak között találjuk Iránt, de a kis országok között is akad figyelemre méltó, mint például a kiberhadviselés nemzetközi szabályrendszerének kidolgozásában élenjáró Észtország.

Elemzők és ellenzők – a realista galambok

A „kibertér Douhet-jeivel", a kiberháború elkerülhetetlenségét hirdetőkkel szemben mindig is jelen volt és hallatta szavát egy másik szakmai elképzelés is (Maschmeyer, 2020). A kibertérben folyó katonai műveletek lehetséges szerepének túlértékelése ellen felszólaló brit képviselő, a honvédelmi bizottságot vezető Tobias Ellwood, velősen így fogalmazta meg ezt a „kiberszkeptikus" álláspontot: „kiberfegyverekkel senki nem foglalhat el egy országot. Tankkal viszont igen" (Cyber realism, 2022). A kibertér háborús lehetőségeinek korlátozott voltát aztán remekbe szabott tanulmányában járta körbe Tomas Rid (akkoriban a neves brit King's College, ma pedig az amerikai Johns Hopkins Egyetem tudósa), a digitális hadviselés egyik legjobb szakértője. Munkájának címe (amely egy évvel később koncepcionálisan még jobban kiérlelve, könyv formájában is megjelent) világosan tükrözi álláspontját: „Cyberwar Will Not Take Place" (Rid, 2013). A korabeli „kibertranszformációs" hangulatot erősen lehűtő dolgozat meggyőző érveléssel állítja: „A kiberháború nem fog beköszönteni!" Elemzését a háború klasszikus értelmezésétől indítva Rid leszögezi: a kiberműveletek nem képesek olyan értelemben kárt okozni, embert ölni, mint a hagyományos fegyverek. A kibertér akcióinak természetesen van hatása (és ennek megfelelően jelentősége, értelme is): diszruptív, zaklató, „nyírbáló" jellege tagadhatatlan, ám ez messze nem azonos a klasszikus értelemben vett „háború" eszközeinek és eljárásainak pusztító jellegével. A koncepció ilyen jellegű újragondolói közül külön is érdemes kiemelni két kutató munkásságát. Lennart Maschmeyer

és Nadia Kostyuk elgondolkodtató és gazdag tényanyagra építő tanulmányaikban bizonyítják a kiberhadviselés szubverzív jellegét (Kostyuk, Gartzke, 2022; Maschmeyer, 2022). Háborús „fegyvernek" nem alkalmas – de zaklatni, nyugtalanítani, zavart kelteni, felderíteni kiválóan felhasználható. Nem véletlen tehát, vallja a szakemberek egy meglehetősen népes (és érvelésüket meggyőző, empirikus kutatási anyaggal is megtámogató) csoportja, hogy a fegyveres harc kirobbanását nem kísérte egy „mindent elsöprő", az ellenfelet szinte puskalövés nélkül térdre kényszerítő „kiberháború": a rettegett kiber-armaggedon nem következett be (Ukraine cyber, 2022).

A háború új arca: a támadás és védekezés új paradigmái

Miközben az emberi konfliktusok sok mindent megőriztek évezredes hagyományaikból, a háború, a nyílt fegyveres harc a technológia fejlődésével párhuzamosan átalakul. A digitalizáció terjedése a nemzetek közötti erőszakos érdekérvényesítés új formáit teremtette meg. Új kifejezés is született: a „háborús szint alatti konfliktus". A kiberfergyverekkel felszerelkezett hackerseregek törekvése, hogy úgy szálljanak szembe az ellenséggel, hogy az a megtámadott fél „háborús ingerküszöbe" alatt maradjon. Ártson neki, de ne késztesse válaszcsapásra (Ukraine warns of massive cyberattacks, 2022). A szinte folyamatosan zajló, kisebb-nagyobb hackerakciók egyik fontos célja éppen ez: tapogatni, próbálni az ellenfél rendszereit; megismerni gyenge pontjait, illetve megtapasztalni, hogyan reagál a másik állam a támadásokra.

Tömegpusztító fegyverek fillérekért?

A kiberhadszíntér egyik fontos jellemzője: kiegyenlíti a játékteret kicsik és nagyok, szegények és gazdagok között. Az utóbbi fél évszázad töretlen technikai fejlődése jóvoltából a fegyverek beláthatatlanul hatásosak és drágák lettek. Az USA legmodernebb vadászgépe, az F-22 Raptor darabja 334 millió dollárba kerül: az 100 milliárd forint. De egy jóval régebbi F-16-osért is elkérnek 20 milliárd forintot. És ez csupán egy gép, hol van még egy teljes légierő! Az oroszok legmodernebb harckocsija, a T-14 1 milliárd forintba kerül. Az amerikai Abramsért már 1,8 milliárdot számítanak fel, míg a németek Leopard 2 páncélosa darabonként 2 milliárd forintba kerül. Könnyen belátható: korszerűen felfegyverzett, ütőképes hadseregről, a nagyhatalmakat, és még néhány regionális erőközpontot leszámítva, ma lényegében egyetlen ország sem álmodhat. A kiberháborúhoz viszont csupán számítógépek kellenek, meg szoftverek. A csillagászati árú hagyományos fegyverekhez képest ezek jóval szerényebb tételek, ami nem csupán a kis államok, de terrorszervezetek körében is egyre népszerűbbé teszi a kiberhadviselés koncepcióját. Érdemes azonban figyelembe venni azt is: a jelentős (nagy fontosságú, komplex, jól védett) számítógépes rendszerek elleni támadás eszköz- és ráfordításigénye nem jelentéktelen. Ez a kibertér kisbűnözői számára elérhetetlen gyümölcs; itt csak a jól felszerelt, kellő erőforrásokkal rendelkező állami hátterű csoportok vagy a szervezett bűnözés óriásai érhetnek el sikereket.

Az „attribúció" problémája, avagy a tettesnek nehéz a nyomára bukkanni

A kibertérben folyó műveleteknek van még egy sajátossága, ami vonzóvá teszi ezt a digitális hadszínteret, nagyok és kicsik számára egyaránt. Mint korábban már említettük: a csendben zajló kiberműveleteknél az elkövetők igyekeznek az ismeretlenségben maradni. Amikor napvilágra kerül egy-egy akció ténye, akkor sem vállalja senki a végrehajtás felelősségét. A kibertámadások elleni védekezés egyik legnagyobb problémája ez: nehéz, sokszor lehetetlen a támadó egyértelmű, bizonyítható azonosítása. Ahogy szaknyelven mondják: az attribúció. A felderítést nehezíti, hogy az elkövetők általában igyekeznek a nyomaikat eltüntetni. Nem ritka az a ravasz megoldás, amikor más államok hackercsoportjaihoz köthető, ismertté vált támadó szoftvert használnak egy harmadik ország ellen. Szakértők szerint különösen az orosz hackeralakulatok szeretik ezt a manővert. A korábban már említett NotPetya támadásnál is egy már korábban ismertté vált, másik szoftverrel próbálták így álcázni a kilétüket (Sherman, 2022).

Virtuális dimenzió – valóságos elrettentés: az igazán kemény dió

A hidegháború korszakában az atomnagyhatalmak egymást kölcsönösen sakkban tartó koncepciója az ún. elrettentés elve volt. Lényege: mindkét fél tudta, hogy nem érdemes megtámadnia a másikat, mert ezért a cselekedetért az olyan súlyos árat fizettetne vele, ami értelmetlenné tenné a „győzelmet". Brutálisan egyszerű elv – és működött! A kiberkorszak nagy tragédiája, hogy ez a hosszú időn át biztonságot garantáló hozzáállás a digitális eszközök, hálózatok birodalmában lényegében nem alkalmazható. Ahol egy támadás észrevétlen maradhat, vagy kiderülése esetén könnyen tagadható, ott nem lehet biztosan tudni azt sem: ki legyen a válaszcsapást kilátásba helyező fenyegetés címzettje. Amiből az következik: egy új, a megváltozott környezetben is működőképes koncepció kidolgozásáig a kibertér veszélyes közeg marad (Valeriano, Maness, 2015).

A kiberfegyverek hátulütői: erőforrás igény, nehéz időzíthetőség, nehéz kontrolálhatóság

Ahogy azt feljebb láttuk, szakértők egy része határozottan állítja, hogy a kiberfegyverek (rosszindulatú számítógépes programok) tényleges háborúra kevéssé alkalmasak. Valójában súlyosan nehezíti a tényleges hadi alkalmazhatóságukat az időzítés kérdése (Smeets, 2018). Bár mindegyik eset egyedi, a szakemberek szerint átlagosan 2-3 évig is eltarthat egy komoly kibertámadás előkészítése és végrehajtása. Ennek összehangolása (a szokásos gyakorlat szerint adott időpontokban induló és végrehajtandó) hagyományos katonai hadmozdulatokkal gyakorlatilag lehetetlen. A tetemes időigény és a pontos időzítés korlátai már eleve kétségessé tennék ezeknek az eszközöknek a háborús eszközként való alkalmazását. Továbbá természetesen a ráfordított idő és munka megfelelően képzett, megfelelő informatikai felszereléssel ellátott csapatok összehangolt ténykedését feltételezi; a magányos működvelő képtelen ilyen akciók kivitelezésére.

Hasonlóan komoly problémát jelent a hadi alkalmazás szempontjából az a körülmény, hogy nagyon nehéz előre pontosan meghatározni az akcióval kiváltott hatásokat. Amíg például egy rakétacsapás által előidézett kár viszonylag pontosan felbecsülhető, addig ez a

kiberfegyverek alkalmazásakor több szempontból is problémás lehet. Ehhez kapcsolódik az egyik legsúlyosabb alkalmazási nehézség: a rendkívül tökéletlen kontrollálhatóság. Magyarul ez annyit jelent, hogy (a számítógépes rendszerek összekapcsoltsága, hálózatossága következtében) az okozott kár sok esetben nem szűkíthető egyetlen kiválasztott célpontra. A globális konnektivitás révén az ilyen informatikai károkozók könnyen „kiszabadulhatnak", majd a világhálón tovaterjedve ellenőrizhetetlen pusztítást végezhetnek – akár az akciót indító állam rendszereit is megfertőzve. A korábban említett, talán legsúlyosabb ilyen károkozó akció, a NotPetya támadás éppen ezzel az utóhatásával okozta a legnagyobb riadalmat szakmai körökben. Tartja magát a feltételezés, hogy ez az eset minden támadó kiberképességeket fejlesztő állam döntéshozóit egyfajta megfontoltságra intette az ilyen fegyverek alkalmazását illetően. A nehéz kontrolállhatóság az Ukrajna elleni invázióhoz kapcsolódó kiberműveletekben ismét előbukkant. A fegyveres támadás megindulásával egy időben, az ukrajnai internetes kommunikáció egy részét biztosító Viasat műholdas rendszer ellen (vélhetően oroszok által) bevetett számítógépes kártevő is gyorsan „elszabadult". A rosszindulatú program sokfelé okozott károkat, beleértve a németországi szélerőmű rendszerek egy részét is (Mandiant, 2022).

Irregulárisok a kibertérben: a „szürke zóna" hadműveletei

Az Ukrajnában (is) szolgáltató Viasat társaság rendszerei elleni támadás még egy fontos körülményre hívta fel (ismételten) a figyelmet. A kiberakcióval megtámadott modemek jelentős része (egyszerű, a cég központjából hálózaton át végzett szoftveres javítással) ismét működőképessé tehető volt, és a szolgáltatás alig néhány órányi kiesés után zavartalanul folytatódott. Az érintett vevődobozok egy számottevő része javíthatatlan károkat szenvedett; azonban ezek kicserélése is csupán néhány napot vett igénybe (és a költségek sem voltak eget verőek). Egy szóval: a hosszas előkészítéssel indított, és hatását tekintve nehezen fókuszálható kibernetikus támadás viszonylag olcsón és gyorsan javítható károkat okozott csupán. A tényleges katonai alkalmazhatóság kritériumainak érvényesülését ugyanakkor jól példázza a 2022 őszén indított, és az ukrán energetikai rendszer pusztítását, lassítását, rombolását célzó hagyományos támadássorozat. Két nap előkészítés és néhány tucat cirkálórakéta ráfordítása elégséges volt ahhoz, hogy Oroszország hosszú időre (talán hónapokra) működésképtelenné tegye – becslések szerint – az ukrán energetikai hálózat 30%-át. Adott célpontok elleni, időzített és legfeljebb kisebb mértékű nem kívánatos következményekkel járó támadásokra tehát összehasonlíthatatlanul alkalmasabbnak látszanak a hagyományos fegyverzetek.

Az Ukrajnában zajló konfliktus azonban egyfajta iskolapéldájaként szerepel annak az újfajta harcmodornak, ami az utóbbi években sokfelé jellemzi a geopolitikai szembenállások új világát (Maschmeyer, 2021). Olyan komplex konfliktus-rendszereknek vagyunk tanúi, ahol eszközök, és alkalmazási módok sokasága keveredik (The Propaganda War, 2022). Hagyományos háború jellegű fegyveres harc; propagandára és dezinformációra építő információs hadviselés; a másik fél informatikai rendszereinek megzavarását, blokkolását célzó kiberakciók; pénzügyi-kereskedelmi korlátozások és szankciók. Sok fajta és különböző intenzitású eszközt és eljárást vetnek be a szemben álló felek, méghozzá nem feltétlenül lineárisan (hol az egyiket, hol a másikat), hanem akár egy időben is. Ez a hibrid háború,

amit a hagyományos fegyveres harc fogalmaival sokszor értelmezni is nehéz (Bachmann, Gunneriusson, 2015). A nyugati szakirodalom az ún. „szürke zónás" (grey zone) hadviselésről is beszél: arról a posztmodern világunkra jellemző sem nem háború, sem nem béke állapotról, ahol az ellenfél elbizonytalanítását, meggyengítését, szándékainak és lehetőségeinek kifürkészését célzó akciók vannak túlsúlyban (Military-made cyber weapons, 2022). Erre a célra pedig (különösen más eszközökkel, például az információs hadviselés fegyverzetével kombinálva) kifejezett alkalmasnak látszanak a kiberfegyverek. Annál az egyszerű oknál fogva, hogy a digitalizáció által szinte átitatott társadalmaink biztonsága és magabiztossága épül ma már éppen azokra a technológiákra, amelyeket könnyű szerrel vehetnek célba ezek a (halált, fizikai pusztulást nem, de fennakadást, zűrzavart, bizonytalanságot, félelmet okozó) újszerű fegyverek (Egloff, Maschmeyer, 2021). Tehát, a társadalmakat megbénító, térdre kényszerítő, távolról vezérelt „kiberháború" koncepciója talán túlzó rémkép, de a kiberfegyverek veszélyessége nagyon is valóságos.

Irodalom

Arquilla, J., Ronfeldt, D. (1993). Cyberwar is coming! *Comparative Strategy*, vol. 12, 2, 141-165.

Bachmann, S., Gunneriusson, H. (2015). Hybrid wars: the 21st-century's new threats to global peace and security. *Scientia Militaria South African Journal of Military Studies*, 43, 1, 77-98.

Ciarán, M. (2022).*Cyber Realism in a Time of War* https://www.bloomberg.com/news/articles/2022-02-15/mandiant-executive-warns-of-cyber-panic-we-need-to-get-a-grip?

Egloff, F. J., Maschmeyer, L. (2021). Shaping not signaling: understanding cyber operations as a means of espionage, attack, and destabilisation. *International Studies Review*, vol. 23, 1, 997-998.

Gartzke, E. (2013). The Myth of Cyberwar. *International Security*, vol. 38, 2, 41-73.

Harknett, R., Smeets, M. (2022). Cyber campaigns and strategic outcomes. *Journal of Strategic Studies*, vol. 45, 4, 1-34.

Hippler, T. (2013). *Bombing the People. Giukio Douhet and the Foundations od Air Power Strategy, 1884-1939*. Oxford, Oxford University.

Kostyuk, N., Gartzke, E. (2022). Why cyber dogs have yet to bark loudly in Russia's invasion of Ukraine. *Texas National Security Review*, vol. 5, 3, 113-126.

Kostyuk, N., Zhukov, Y. M. (2017). Invisible digital front: can cyber attacks shape battlefield events? *Journal of Conflict Resolution*, vol. 63, 2, 1-44.

Mandiant Executive Cautions against Russia-Cyberattack Panic (2022). https://www.bloomberg.com/news/articles/2022-02-15/mandiant-executive-warns-of-cyber-panic-we-need-to-get-a-grip?

Maschmeyer, L. (2022). A new and better quiet option? Strategies of subversion and cyber conflict. *Journal of Strategic Studies*, vol. 45, 4,1-25.

Maschmeyer, L. (2021). A tale of two cybers. How threat reporting by cybersecurity firms systematically underrepresents threats to civil society. *Journal of Information Technology and Politics*, vol. 18, 1, 1-20.

Maschmeyer, L. (2020). *Slow burn. Subversion and escalation in cyber conflict and covert action.* Toronto, University of Toronto.

Military-made cyberweapons could soon become available on the dark web, Interpol warns (2022). https://www.cnbc.com/2022/05/23/military-cyberweapons-could-become-available-on-dark-web-interpol.html

Overy, R. (2015). *The Bombers and the Bombed. Allied Air War over Europe, 1940-1945*. New York, Viking.

Rid, T. (2013). *Cyber war will not take place*. Oxford, Oxford University.

Sharma, A. (2010). Cyber wars: A paradigm shift from means to ends. *Strategic Analysis*, vol. 34, 1, 67-73.

Sherman, J. (2022). *Untangling the Russian Web: Spies, Proxies, and Spectrums of Russian Cyber Behaviour*. Washington, Atlantic Council.

Smeets, M. (2018). A matter of time: on the transitory nature of cyberweapons. *Journal of Strategic Studies*, vol. 41, 1-2, 6-32.

The Propaganda War has Eclypsed Cyberwar in Ukraibne (2022). https://www.technologyreview.com/2022/03/02/1046646/THE-PROPAGANDA-WAR-HAS-ECLIPSED-CYBERWAR-IN-UKRAINE/

Ukraine cyber (2022). https://transcripts.cnn.com/show/cnr/date/2022-02-24/segment/22

Ukraine warns of 'massive cyberattacks' coming from Russia on critical infrastructure sites (2022). https://www.cyberscoop.com/ukrainians-warn-of-massive-cyberattacks/

Valeriano, B., Maness, R. C. (2015). *Cyber war versus cyber realities. Cyber conflicts int he international system*. Oxford, Oxford University.