Taktikák és stratégiák a kiberhadviselésben

Szerkesztette
Krasznay Csaba

LUDOVIKA
EGYETEMI KIADÓ

Taktikák és stratégiák a kiberhadviselésben

Taktikák és stratégiák a kiberhadviselésben

Szerkesztette
Krasznay Csaba

LUDOVIKA EGYETEMI KIADÓ
Budapest, 2023

A mű TKP2020-NKA-09 számú projekt a Nemzeti Kutatási Fejlesztési és Innovációs Alapból biztosított támogatással, a Tématerületi Kiválósági Program 2020 pályázati program finanszírozásában valósult meg.

Szerzők:
Haig Zsolt, HHK Elektronikai Hadviselés Tanszék
Kovács László, HHK Elektronikai Hadviselés Tanszék
Molnár Anna, HHK Nemzetközi Biztonsági Tanulmányok Tanszék
Krasznay Csaba, EJKK Kiberbiztonsági Kutatóintézet
Molnár Dóra, HHK Nemzetközi Biztonsági Tanulmányok Tanszék
Nyáry Gábor, EJKK Kiberbiztonsági Kutatóintézet
Ambrus Éva, NKE Katonai Műszaki Doktori Iskola
Deák Veronika, NKE Katonai Műszaki Doktori Iskola
Dévai Dóra, NKE Katonai Műszaki Doktori Iskola
Koczka Ferenc, NKE Katonai Műszaki Doktori Iskola
Koller Marco, NKE Hadtudományi Doktori Iskola
Legárd Ildikó, NKE Közigazgatástudományi Doktori Iskola
Üveges András József, NKE Katonai Műszaki Doktori Iskola

Lektor:
Póser Valéria

Kiadja a Nemzeti Közszolgálati Egyetem
Ludovika Egyetemi Kiadó
A kiadásért felel: Deli Gergely rektor

Székhely: 1083 Budapest, Ludovika tér 2.
Kapcsolat: kiadvanyok@uni-nke.hu

Felelős szerkesztő: Varga Zoltán
Olvasószerkesztő: Bujdosó Hajnalka
Korrektor: Csinta Áron
Tördelőszerkesztő: Stubnya Tibor

Borítófotó: Harctéri Kamera Csoport

ISBN 978-963-531-799-8 (nyomtatott)
ISBN 978-963-531-800-1 (elektronikus PDF) | ISBN 978-963-531-801-8 (ePub)

Tartalom

Előszó

Kibertámadás. Egyre többször hallani a kifejezést a médiában, de kevesen tudják, mit is jelent tulajdonképpen. Az incidensek mögött ugyanis több különböző motivációt találhatunk. A legtöbb esetben anyagi haszonszerzés hajtja az elkövetőket, amivel leggyakrabban találkozunk tehát, az a kiberbűnözés. Megítélése egyértelműen a kiberbűnözésről szóló budapesti egyezmény körébe tartozik, és alapvetően nincsen vita arról az államok között, hogy üldözendő cselekmény, bár az akarat nyugatról keletre, a képesség pedig északról délre csökken ezen bűncselekményág megfékezésére.

Szintén gyakran lehet hallani információszerzési célzattal véghez vitt támadásokról, az úgynevezett kiberkémkedésről. Amennyiben ezt állami szereplő hajtja végre, a cselekmény nemzetközi jogi megítélése szürke zónába tartozik, de gyakran kötődik valamilyen katonai szervezethez. Ritkán, de találkozhatunk hacktivista-, illetve kiberterrorista-cselekedetekkel is, amikor a csoport célja valamilyen politikai ideológia terjesztése, esetleg ennek az ideológiának a támogatására valamilyen kiberfizikai rendszeren keresztül pusztítás végrehajtása. Ezeket a nemzeti jog kezeli, az eddig ismert esetekben ugyanis államoktól független csoportosulások, például az Anonymous csoport, vagy államokhoz nem egyértelműen, inkább patrióta alapon kapcsolódó csoportok tevékenységét lehetett megfigyelni.

Végül idetartoznak az egyértelműen katonai műveletek, azaz a nyilvánosság számára is ismert kiberhadviselés, amely egyre gyakrabban része, támogatója a hagyományos, kinetikus műveleteknek. Összességében viszont azt lehet érzékelni, hogy az államok katonai műveleteik során akár leplezetten, akár nyíltan, de mind a négy motivációt előszeretettel használják fel. Könyvünk célja éppen ezért az, hogy áttekintsük a kiberhadviselés ismert történetét, és a nyilvánosság számára is megismerhető, mérvadó források segítségével, kritikus elemzéssel bemutassuk az olvasónak az államok által használt kiberműveleti eszköztárat.

Ez már csak azért is fontos terület, mert a legtöbb kibertámadás nem éri el azt a szintet, hogy állam elleni támadásnak nevezhessük – habár az a határ sem egyértelmű, ahonnan már az egész államot érintő tevékenységről beszélhetünk. Általánosságban a tulajdon megsemmisülése vagy az ember sérülése lehet az a kulcsmomentum, amely a fizikai világban kinetikus vagy a kibertérben informatikai jellegű erő alkalmazását válthatja ki egy viszontválaszban. De ez még mindig nem háború a szó jogi értelmében. Michael Schmitt

és Liis Vihul, a téma két elismert kutatója éppen ezért felhívja a figyelmet arra, hogy a „háború", így a „kiberháború" fogalma is meghaladott a nemzetközi jog fogalmi keretei között, mert a 20. század közepétől a „fegyveres konfliktus" szóhasználat terjedt el a négy genfi egyezménnyel párhuzamosan. A humanitárius jog szempontjából ugyanis nem számít, hogy a hadviselő felek betartották-e a hadüzenet formai követelményeit, vagy sem. A katonai jellegű kibertámadások megítélése abban az esetben egyértelmű, amikor egy hagyományos fegyveres konfliktus kísérőjeként jelennek meg, ahogy történt az 2008-ban, a grúz–orosz konfliktusban vagy a szíriai polgárháborúban. Ezekben az esetekben minden hadviselő félnek be kell tartania a humanitárius jog szabályait. A kiberháborút tehát szerencsésebb „kibertérben történő fegyveres konfliktusnak" nevezni, így megkülönböztetve azt a békeidőben végrehajtott kibertéri műveletektől a nemzetközi jog szempontjából. Márpedig napjainkban éppen ezt a szabályozatlan, „se nem béke, se nem háború" állapotot érzékelhetjük, ami sokkal kevésbé korlátozza az államokat, mint ha a „hagyományos háború" forgatókönyve szerint kellene eljárniuk.

A kibertéri műveletek nemzetközi jogi szempontjait vizsgáló *Tallinni kézikönyv* javaslatot tesz a „kibertámadás" meghatározására, amely merőben eltér a mérnöki *terminus technicusból* levezethető fogalomtól. A Kézikönyv 92. szabálya ekképpen fogalmaz: „Egy kibertámadás olyan kiberművelet, legyen az akár támadó, akár védelmi jellegű, mely alapján személyek sérülése vagy halála, illetve objektumok megrongálódása vagy megsemmisülése megalapozottan várható." Ezen forrás 103. szabálya szerint a kiberhadviselés eszközei a kiberfegyverek és a hozzájuk tartozó kiberrendszerek, módszerei pedig azok a kibertaktikák, technikák és eljárások, amelyekkel az ellenséges tevékenységet végrehajtják. A könyv szerzői azt a célt tűzték ki maguk elé, hogy ezt a témát járják körbe a lehető legalaposabban. Jelenleg ugyanis nincs magyar nyelven elérhető, az offenzív katonai kibertéri műveletek taktikáit és stratégiai szándékait elemző mű. Hasonló munkák idegen nyelven sem gyakoriak, tekintettel a téma érzékenységére és a nyilvánosságra hozott információk mennyiségére, valamint megbízhatóságára. A szerzők mégis úgy gondolják, hogy a kibertéri műveletek közel 30 éves története tartogat már annyi esetet és az ezeket alátámasztó hiteles beszámolót, hogy be lehet mutatni a terület fejlődését, és rá lehet mutatni az egyes taktikai és stratégiai elemek erősségeire, esetleges hibáira, el lehet tehát végezni a kritikai elemzést.

A kiadvány illeszkedik a Nemzeti Közszolgálati Egyetem oktatási és kutatási portfóliójához és intézményközi megállapodásaihoz, így elsősorban tankönyvként

hasznosítható a kiberbiztonsági mesterképzésben, és jegyzetként felhasználható a katonai képzéseken. Kiegészíti a témában korábban megjelent monográfiákat, s kapcsolódik a Honvédelmi Minisztérium és a Nemzeti Közszolgálati Egyetem által megkötött, kiberbiztonsági kutatásokat elősegítő együttműködési megállapodáshoz, illetve támogatja a Magyar Honvédség Parancsnoksága Kibervédelmi Szemlélője által végzett tevékenységet. Nem érinti azonban az orosz–ukrán háborút, amely a kézirat 2021-es lezárása után tört ki.

A szerzők a téma elismert magyarországi szakértői. Prof. dr. Kovács László a Magyar Honvédség Parancsnokságának korábbi kiberszemlélőjeként elsődleges felelőse volt a magyar haderő kiberképességei fejlesztésének. Prof. dr. Molnár Anna az európai védelempolitika szakértője. Prof. dr. Haig Zsolt az NKE Katonai Műszaki Doktori Iskolájában a védelmi elektronika, informatika és kommunikáció kutatási terület vezetője, a kiberhadviseléssel foglalkozó kutatások úttörője Magyarországon. Dr. Krasznay Csaba az NKE Kiberbiztonsági Kutatóintézetének vezetőjeként, a témában legkomolyabbnak számító CyCon konferencia előadójaként több mint egy évtizede foglalkozik a kiberhadviselés kérdésével. Dr. Molnár Dóra az európai kiberbiztonsági stratégiák kutatója. Dr. Nyáry Gábor a kiberdiplomácia, a nemzetközi kiberkapcsolatok szakértője. Rajtuk kívül az NKE három doktori iskolájának kiberbiztonsági témákkal foglalkozó doktoranduszai (Ambrus Éva, Dévai Dóra, Koczka Ferenc, Koller Marco, Legárd Ildikó, Üveges András) vettek részt a könyv megírásában, amely alapvető forrása lehet azon hallgatóknak, akik akár a katonai, akár a nemzetközi kapcsolatok területén végzik tanulmányaikat, és a szakértőknek, akik a honvédelmi vagy külügyi ágazatokban szándékoznak megismerni a kibertéri műveletek valóságát.

Budapest, 2023. június 15.

1. fejezet

A kiberhadviselés fogalma, nemzetközi jogi háttere, történeti áttekintése

Legárd Ildikó

A kibertér néhány évtizeddel ezelőtt még futurisztikusnak számító fogalma mára a mindennapjaink meghatározó részét képző, megkerülhetetlen tényezővé vált. A bolygót behálózó online világ és az életünket megkönnyítő infokommunikációs eszközök, technológiák és szolgáltatások érzékelhető valósággá váltak, amelyek amellett, hogy megkönnyítik az életünket, számos súlyos biztonsági kockázatot is rejtenek magukban.

A robbanásszerű digitális fejlődés, az információs hálózatok szélsebes terjedése a hadviselést is alapjaiban változtatta meg. Az államok a globális, határok feletti, folyamatos fejlődésben lévő kibertérben rejlő potenciális lehetőségeket hamar felismerték, ami a kibertér fokozódó militarizálódásához vezetett, így a kiber- és hibrid hadviselési formák mind dominánsabbá váltak az államok egymás közti viszonyaiban. Amerikai kiberbiztonsági szakértők vélekedése szerint a 21. század konfliktusai – állami és nem állami szereplők között egyaránt – elsősorban a kibertérben fognak lezajlani, pontosabban már évek óta zajlanak.[1]

A kibertér fogalma

A kibertér *(cyberspace)* kifejezést először William Gibson amerikai–kanadai sci-fi-író használta a számítógép-alapú hálózatok és az ember interaktív virtuális kapcsolatrendszerének leírására, az 1982-ben megjelent *Burning Chrome*[2]

[1] Richard A. Clarke – Robert K. Knake: *Cyber war: The Next Threat to National Security and What to do about it*. New York, Harper & Collins, 2010. 12.

[2] Magyarul lásd William Gibson: Izzó króm. In William Gibson et al.: *Izzó króm. William Gibson és mások művei.* Ford. Bárday Tamás et al. Kaposvár, Valhalla Páholy, 1997. 205–232.

című novellájában, majd a *Neuromancer*[3] című regényében. A kibertér fogalma az elmúlt évtizedekben folyamatos változás alatt állt, tartalma a fejlődés ütemével párhozamosan bővül, ezért egységes meghatározással nem, csak egyedi megfogalmazásokkal találkozhatunk. Az Egyesült Államok Védelmi Minisztériuma által kiadott szótár *(Dictionary of Military and Associated Terms)* szerint a kibertér „az információs környezet egy globális tartománya, amely tartalmazza az informatikai infrastruktúrák, a bennük tárolt adatok egymással összefüggő hálózatát, beleértve az internetet, a távközlési hálózatokat, a számítógéprendszereket, valamint a beágyazott feldolgozó és vezérlő elemeket".[4] Hazánkban a fogalmat a 2013-as *Nemzeti Kiberbiztonsági Stratégia* határozza meg: „[a] kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti."[5] A későbbi fejezetekben még számos más értelmezéssel lehet találkozni, ami jól mutatja, hogy szakterülettől függően mennyire tág a lehetséges definíciók köre.

A kiberteret a 90-es évek mozgalmai leginkább a vadnyugathoz hasonlították, ahol nemhogy nem törekedtek a szabályok kialakítására, hanem az amerikai demokrácia bölcsőjéhez hasonlítva az internet szuverenitását, szabadságát hirdették, amelyben a nemzetközi szabályozást a lehető legkisebb mértékűre kell szorítani. „Az internet szabadságát hirdető, napjainkban is fennálló elmélet[6] szerint az internet nyitott felépítését, erősen decentralizált, központ nélküli működését éppen a szabad információcsere és szólásszabadság jegyében lett létrehozva annak érdekében, hogy az információ szabadon tudjon áramlani, bármilyen akadály ellenére is."[7] Tehát a kibertér egyfajta „digitális közlegelő", amely mindenkié, vagy éppen senkié, mint a nyílt óceánok vagy a világűr.

A kérdéskörrel kapcsolatos másik, az előbbivel ellentétes koncepció a „kibertér szuverenitása". A kibertér lehetőségeit felismerve a nemzetállamok egyre határozottabban igyekeznek érvényre juttatni saját hatalmukat a „kibertér rá eső

[3] William Gibson: *Neurománc*. Ford. Ajkay Örkény. Budapest, Valhalla Páholy, 1992.

[4] Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms (2010. november 8.); Berki Gábor: A kibertéri konfliktusok változásai. *Hadmérnök,* 8. (2013), 1. 173–185.

[5] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról.

[6] Alix Desforges francia geopolitikus elmélete, amely szerint az internet szabadsága az 1960-as évek kulturális forradalmából eredeztethető.

[7] Gémesi Csaba: A kibertér és szereplői. *Hadmérnök,* 13. (2018), 3. 407.

részében", éppen úgy, mint a fizikai határok által meghatározott földrajzi térben.[8] A francia védelmi minisztérium korábbi tisztviselője, Stéphane Dossé szerint: „Úgy tűnhetett, hogy az államoknak fel kellett húzniuk a zászlót a kibertérben, amelyet elfoglalnak és ahol szuverenitásukat gyakorolják, hogy a szűzföldeket gyarmatosítsák, és felkészüljenek egy esetleges támadásra."[9] E területen Kína és Oroszország igyekezett az elmúlt években a legmesszemenőbben kiterjeszteni szárazföldi határait a kibertérre is, és technológiai, illetve szabályozási eszközökkel biztosítani szuverenitása legteljesebb gyakorlását.

Kína vonta elsőként az internetet állami felügyelet alá. Számára komoly problémát és sok kellemetlenséget okozott az egyre növekvő számú, interneten jelen lévő kínai felhasználó, aki államilag nem ellenőrzött és nem támogatott tartalmakat érhetett el a világhálón keresztül, ezért 2003-ban elindította a közbiztonsági minisztérium által fenntartott, Aranypajzs névre keresztelt hardver- és szoftverrendszert, amely képes a webes cenzúra teljes körű biztosítására. Az elterjedtebb nevén Kínai Nagy Tűzfalként ismert rendszer számos kifinomult informatikai technikát alkalmaz az internetes tartalmak cenzúrájához, mint például az IP-cím blokkolása vagy a DNS-szűrés és -átirányítás. Mindemellett Kína, amennyiben politikai érdekei úgy kívánják, sokkal keményebb eszközök alkalmazására is képes. 2009-ben az Urumcsiben (Hszincsiang tartomány fővárosa) történt ujgur zavargások során például korlátozták az internet-hozzáférést, valamint lekapcsolták a nemzetközi telefonvonalakat is.[10]

Oroszország már a 2000-es évek elejétől olyan jogszabályokat fogadott el, amelyek az internetforgalom fokozatos szigorítására, felügyeletére és cenzúrázására irányulnak. A folyamat csúcspontja a 2019-ben elfogadott törvénymódosítás,[11] amelyet a nyugati országok csak „szuverén internet" törvényként emlegetnek. A rendelkezések olyan internetfelügyeleti rendszert hoznak létre, amely még a kínainál is szélesebb körű jogosítványt ad az államnak az internet szabályozására, illetve lehetővé teszi rendkívüli helyzet esetén az országos hálózat leválasztását a globálisról, és így a teljes átállást az úgynevezett Runetre.

[8] Nyáry Gábor: Az adatok geopolitikája: az Internet mitikus szabadságától a digitális szuverenitás felé. *Ludovika.hu,* 2020. december 7.

[9] Idézi Frédérick Douzet: Geopolitika a kibertér megértéséhez. (Ford. Monti Norbert.) In Pintér István (szerk.): *Műhelymunkák. A virtuális tér geopolitikája.* Tanulmánykötet. Budapest, Geopolitikai Tanács Közhasznú Alapítvány, 2016. 22–23.

[10] Kovács László: Információs hadviselés kínai módra. *Nemzet és Biztonság,* 2. (2009), 7. 35–44.

[11] A „szuverén internet" törvény valójában a távközlésről szóló 2003. évi szövetségi törvény módosítása.

Ez utóbbi az internet oroszországi, illetve a nagyrészt a szovjet utódállamokban használt, orosz nyelvű szegmense. A „rendkívüli helyzet"-ről azonban a törvény nem határoz meg részleteket, csak annyiban, hogy az orosz internetet fenyegető veszélyek típusait és a foganatosítandó intézkedéseket az Oroszországi Föderáció Kormánya hagyja jóvá.[12]

Az Európai Unió is a kibertér szabályozottsága és a digitális függetlenség mellett érvel. A Bizottság 2021. március 9-én bemutatta jövőképét az Európai Unió digitális átalakulására 2030-ig, amelyben kiemeli, hogy „[az] EU elő fogja mozdítani emberközpontú digitális menetrendjét a globális színtéren, és törekedni fog arra, hogy világszerte a szabályok és keretfeltételek igazodjanak vagy közelítsenek az uniós normákhoz és szabványokhoz".[13]

Magyarország szabályozási koncepciója szintén a kibertér szuverenitására épül. A Nemzeti Kiberbiztonsági Stratégia a következőképpen határozza meg Magyarország kiberterét: „a globális kibertér elektronikus információs rendszereinek azon része, amelyek Magyarországon találhatóak, valamint a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy Magyarországra irányulnak, illetve amelyekben Magyarország érintett."[14]

A kibertér katonai értelmezése, a kiberhadviselés

Katonai értelemben a kibertér a hadviselésnek a korábbi, fizikai térben megjelenő (szárazföldi, légi, tengeri és kozmikus) hadszínterekkel egyenértékű, önálló hadszínterévé vált.[15]

[12] Tölgyesi Beatrix: Az orosz „szuverén internet" törvényről. *Nemzet és Biztonság,* 13. (2020), 2. 113–132.; valamint Alkonyi Aurél Zalán: *Információs kontroll és állami felügyelet a modern Oroszország tömegkommunikációs felületein*. Nemzeti Közszolgálati Egyetem Államtudományi és Nemzetközi Tanulmányok Kar Intézményi Tudományos Diákköri Konferencia 2020. évi tavaszi/őszi forduló.

[13] Európai Bizottság: *A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának. Digitális iránytű 2030-ig: a digitális évtized megvalósításának európai módja* (2021. március 9.); Európai Bizottság: *Európa digitális évtizede: a 2030-ra kitűzött célok* (2021. március 9.).

[14] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról.

[15] Kovács László – Illési Zsolt: Cyberhadviselés. *Hadtudomány,* 21. (2011), 1–2. 30.

A kiberhadviselés fogalma

A kibertérhez hasonlóan a kiberhadviselés fogalmára sem találunk egységes meghatározást, annak tartalma a technika megállíthatatlan fejlődésével párhuzamosan gazdagodik. Ahhoz, hogy közelebb jussunk a kiberhadviselés mibenlétéhez és rendszertani meghatározásához, meg kell vizsgálni az információs hadviselés és műveletek fogalmát.

A 21. században az adat a világ új olaja,[16] és tényleges hatalmi tényezővé vált, így erőteljes információs fegyverkezést indított el a nemzetállamok részéről. Az *információs hadviselés* fogalma a 1980-as évek közepén jelent meg először, és már az 1991-es Öbölháborút is meghatározta. „Az azóta eltelt időszakban azt a tevékenységet, amelynek elsődleges célja az információs fölény és az információs uralom megszerzése, majd ennek vezetési, illetve hadműveleti fölénnyé váltása, információs hadviselés helyett – főleg a katonai terminológiában – információs műveleteknek nevezzük."[17] Az *információs műveletek* Haig Zsolt meghatározása szerint:

> „az információs környezetben érvényesülő információs képességek integrált, összehangolt és koordinált alkalmazására irányuló tevékenységek összessége, amelyek a műveletek célkitűzéseinek elérése érdekében, kognitív képességekkel közvetlenül, illetve technikai képességekkel közvetetten hatásokat gyakorolnak a műveletekben részt vevő célközönség szándékára, helyzetértelmezésére és képességeire."[18]

Tehát az információs műveletek

> „olyan összehangolt és koordinált tevékenységet takarnak, amelyek a műveleti biztonság, a katonai megtévesztés, a pszichológiai műveletek, az elektronikai hadviselés és a számítógép-hálózati műveletek különböző akcióival támogatják a harc sikeres megvívását."[19]

Az információs műveleteknek három, egymással összefüggő dimenziója van. A *fizikai dimenzióban* jelennek meg a különböző információs infrastruktúrák, infokommunikációs rendszerek elleni fizikai, pusztító, úgynevezett „kemény

[16] Joris Toonders: Data is the New Oil of the Digital Economy. *Wired,* 2014. július.
[17] Kovács–Illési (2011): i. m. 31.
[18] Haig Zsolt: *Információs műveletek a kibertérben*. Budapest, Dialóg Campus, 2018. 210.
[19] Kovács (2009): i. m. 35.

típusú" *(hard kill)* támadások. Az *információs dimenzióban* az úgynevezett „lágy típusú*" (soft kill)* támadások valósulnak meg, amelyek jellemzően információs folyamatok, adatszerzés, adatfeldolgozás, tárolás, kommunikáció, elektronikus úton való, korlátozó hatású támadások, valamint a saját információs folyamatainkra irányuló hasonló támadások megakadályozása. A *kognitív (tudati) dimenzióban* végrehajtott műveletek közvetlenül az emberi gondolkodást veszik célba valós, csúsztatott vagy hamis információkkal.[20] Napjaink hagyományos hadszíntereit az információs hadszíntér kapcsolja össze, amelyben egyre nagyobb szerepe és jelentősége van az említett, mindhárom dimenziót érintő kibertérnek.[21]

Az *információs műveletek három területre* oszthatók: a kinetikus energián alapuló, a kognitív[22] és a hálózati hadviselésre. Ez utóbbi az információs dimenzióban megvalósuló elektronikai és számítógép-hálózati hadviselést foglalja magában.[23] A kiberhadviselést ezen *hálózati műveleteken* belül értelmezzük úgy, hogy az párhuzamosan a hagyományos (szárazföldi, légi, tengeri és kozmikus) műveletekkel az információs és bizonyos értelemben a kognitív dimenzióban is megjelenik.[24] Eszerint meghatározhatjuk a *kiberhadviselés technikai megközelítésű fogalmát:* „[c]yberhadviselésnek nevezhetjük mindazon tevékenységeket, amelyekben a számítógép-hálózati hadviselés, a számítógép-hálózati műveletek, az elektronikai hadviselés, bizonyos esetekben a SIGINT,[25] valamint a cyberterrorizmus, illetve az ellene folyatott tevékenységek közösen jelennek meg."[26]

A *kiberhadviselés célja* a katonai műveletek információs környezetben történő támogatása, valamint az információs fölény kivívása és fenntartása, egyrészt a saját oldali elektronikus és hálózatalapú információszerző, -továbbító és -feldolgozó rendszerek védelmével, másrészt az ellenfél hasonló rendszerei

[20] Haig Zsolt – Várhegyi István: A cybertér és a cyberhadviselés értelmezése. *Hadtudomány,* 18. (2008), elektronikus szám. 2.; Haig (2018): i. m. 149–152., 211.

[21] Haig (2018): i. m. 211.

[22] Kinetikus energián alapuló hadviselés *(kinetic warfare),* amelyet a fizikai dimenzióban hajtanak végre, és az információs infrastruktúrák, infokommunikációs rendszerek elemeinek fizikai pusztítását, rongálását, tönkretételét jelenti. Kognitív hadviselés *(cognitive warfare),* amely alapvetően a tudati, értelmi dimenzióban érvényesül, és a katonai megtévesztést, műveleti biztonságot, illetve a pszichológiai műveleteket foglalja magába. Haig–Várhegyi (2008): i. m. 6.

[23] Haig–Várhegyi (2008): i. m. 6.

[24] Kovács–Illési (2011): i. m. 31.

[25] SIGINT: *Signals Intelligence,* azaz rádióelektronikai felderítés.

[26] Haig Zsolt – Kovács László – Ványa László: Az elektronikai hadviselés, a SIGINT és a cyberhadviselés kapcsolata. *Felderítő Szemle,* 10. (2011), 1–2. 183–209.

működésének megzavarásával, korlátozásával, vagy akár elektronikus úton történő megsemmisítésével.

A kiberhadviselés támadó és védelmi jellegű műveletekből áll. A *támadó műveletek* célja a szembenálló fél információs rendszereinek felfedése, befolyásolása, esetleg tönkretétele közvetlen (például rosszindulatú szoftverek, zavaró jelek, megtévesztő információk) vagy közvetett formában (az ellenfél rendszerének túlterhelése hamis adatokkal, megtévesztő hálózati tevékenység). A *védelmi műveletek* célja, hogy biztosítsák a hozzáférést a saját hálózatos információs rendszerekhez, és azok hatékony használatát, valamint minimálisra csökkentsék e rendszerek sebezhetőségét és a közöttük fellépő zavarokat. Maga a védelem is lehet támadó és védelmi jellegű. A támadó jellegű védelem során a saját rendszerek elleni támadás lehetőségének minimalizálása a cél, a támadó fél támadási lehetőségeinek szűkítésével, amihez a támadó műveletek eszközeit és módszereit használják fel (például az ellenség rádiózavaró eszközeinek elektronikai tönkretételével). A védelmi jellegű tevékenység a saját rendszerek sebezhetőségét csökkenti (például tűzfal, vírusirtók, hozzáférés-szabályozás, behatolásdetektálás, adaptív válaszlépések alkalmazása).[27]

A kibertér egyre növekvő szerepet tölt be a modern hadviselésben. A 2007-ben bekövetkező Észtország elleni összehangolt kibertámadást egyes szakírók már az első kiberháborúnak *(Web War I.)* nevezték.[28] A digitálisan rendkívül fejlett és az e-közigazgatást magas szinten megvalósító Észtországgal szemben egy tallinni, II. világháborús, szovjet hősi emlékmű eltávolítása után kezdődött zavargásokkal párhuzamosan indultak el az első internetes, elsősorban DDoS-támadások,[29] kiemelten az észt közigazgatás kommunikációs rendszerei és a különböző webes szolgáltatások ellen. A kibertámadások közel három hétig tartottak, és az észt parlament, kormányhivatalok, minisztériumok, illetve telefontársaságok, bankok és médiacégek szerverei, tehát elsősorban az ország kritikus infrastruktúrái[30] voltak a célpontok. Az Észtország adatforgalmát

[27] Haig–Várhegyi (2008): i. m. 7–9.

[28] Patrick Howell O'Neill: The Cyberattack that Changed the World. *The Daily Dot,* 2016. május 20.

[29] DDoS: Elosztott szolgáltatásmegtagadással járó támadás. Egy számítógép-hálózati szolgáltatás teljes vagy részleges megbénítása, helyes működési módjától való eltérítése ártó, támadó szándékkal, elosztottan, több forrásból. Haig Zsolt – Kovács László: Fenyegetések a cybertérből. *Nemzet és Biztonság,* 1. (2008), 5. 61–70.

[30] Hazánkban a kritikus infrastruktúrák védelmével kapcsolatos előírásokról a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény rendelkezik. Eszerint a létfontosságú rendszerelem „az 1. mellékletben meghatározott ágazatok

irányító kulcsfontosságú szerverek naponta többször omlottak össze, így végül a közigazgatás számítógép-hálózatát le kellett kapcsolni az internetről. Az elektronikus banki forgalom részint megszűnt, részint akadozott. Az akció mind Észtországot, mint a NATO-t felkészületlenül érte.[31]

A támadás rávilágított arra, hogy egy kibertérből érkező koncentrált támadás, amely a társadalom számára létfontosságú feladatokat ellátó rendszereket is érint, egy egész ország működésképtelenségét is maga után vonhatja, akár békeidőben is.

A 2008-as orosz–grúz háború során Oroszország a hagyományos hadszíntereken konvencionális csapásokat indított Grúzia ellen, amelyekkel egy időben kiberműveleteket is végrehajtott. A grúz kormány állítása szerint Oroszország az internetforgalmat ellenőrzése alá vonta, az ország kormányzati weboldalait – köztük az elnök saját weblapját is – megbénították, tartalmukat kicserélték, valamint az ország lejáratását célzó, dezinformációs kampányt indítottak kifejezetten e céllal létrehozott oldalakon.[32]

Az utóbbi évtizedben jelentős számú hasonló jellegű kibertámadás történt, ami megkérdőjelezhetetlenné tette az államok jelenlétét a kibertérben. Kialakult és nemzetközileg elfogadottá vált a kiberhadviselés mára már elengedhetetlen fogalmi összetevője: amennyiben egy kibertámadás vagy támadássorozat mögött egy ország vagy országcsoport (esetleg ezekkel egyenértékű politikai vagy gazdasági hatalom) áll, és a támadás egy másik ország vagy országcsoport létfontosságú rendszerei ellen irányul, a támadás céljától és motivációjától függetlenül kiberhadviselésről beszélünk.[33]

valamelyikébe tartozó szolgáltatás, eszköz, létesítmény vagy rendszer olyan rendszereleme, továbbá azok által nyújtott szolgáltatások, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához – így különösen az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához, az ország honvédelméhez – és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna."

31 Kovács László: *A kibertér védelme*. Budapest, Dialóg Campus, 2018b. 145–148.; Berki Gábor: Kiberháborúk, kiberkonfliktusok. In Pintér (2016): i. m. 265–266.

32 Berki (2016): i. m. 266–267.

33 Kovács László: *Kiberbiztonság és -stratégia*. Budapest, Dialóg Campus, 2018a. 23.; Kovács (2018b): i. m. 273.

Kibertámadás – egyre többször hallani, de kevesen tudják, mit is jelent valójában. A legtöbb esetben anyagi haszonszerzés hajtja az elkövetőket, amivel leggyakrabban találkozunk tehát, az a kiberbűnözés.

Gyakran hallani viszont az információszerzési célú támadásokról, a kiberkémkedésről is. Ha ezt állami szereplő hajtja végre, a cselekmény nemzetközi jogi megítélése szürke zónába tartozik, máskor valamilyen katonai szervezethez kötődik.

Ritkán, de ugyancsak találkozhatunk hacktivista és kiberterrorista cselekedetekkel, amikor a csoport célja valamilyen politikai ideológia terjesztése, esetleg ezen ideológiának a támogatására valamilyen kiberfizikai rendszeren keresztül pusztítás végrehajtása.

Végül idetartoznak a tisztán katonai műveletek, azaz a kiberhadviselés, amely egyre gyakrabban része, támogatója a hagyományos, kinetikus műveleteknek. Összességében viszont az államok katonai műveleteikhez mind a négy motivációt előszeretettel használják fel. Könyvünk célja, hogy a téma elismert magyar szakértőivel áttekintsük a kiberhadviselés ismert történetét, és a nyilvánosság számára is megismerhető, mérvadó források segítségével, kritikus elemzéssel bemutassuk az államok által használt kiberműveleti eszköztárat.

9 789635 317998