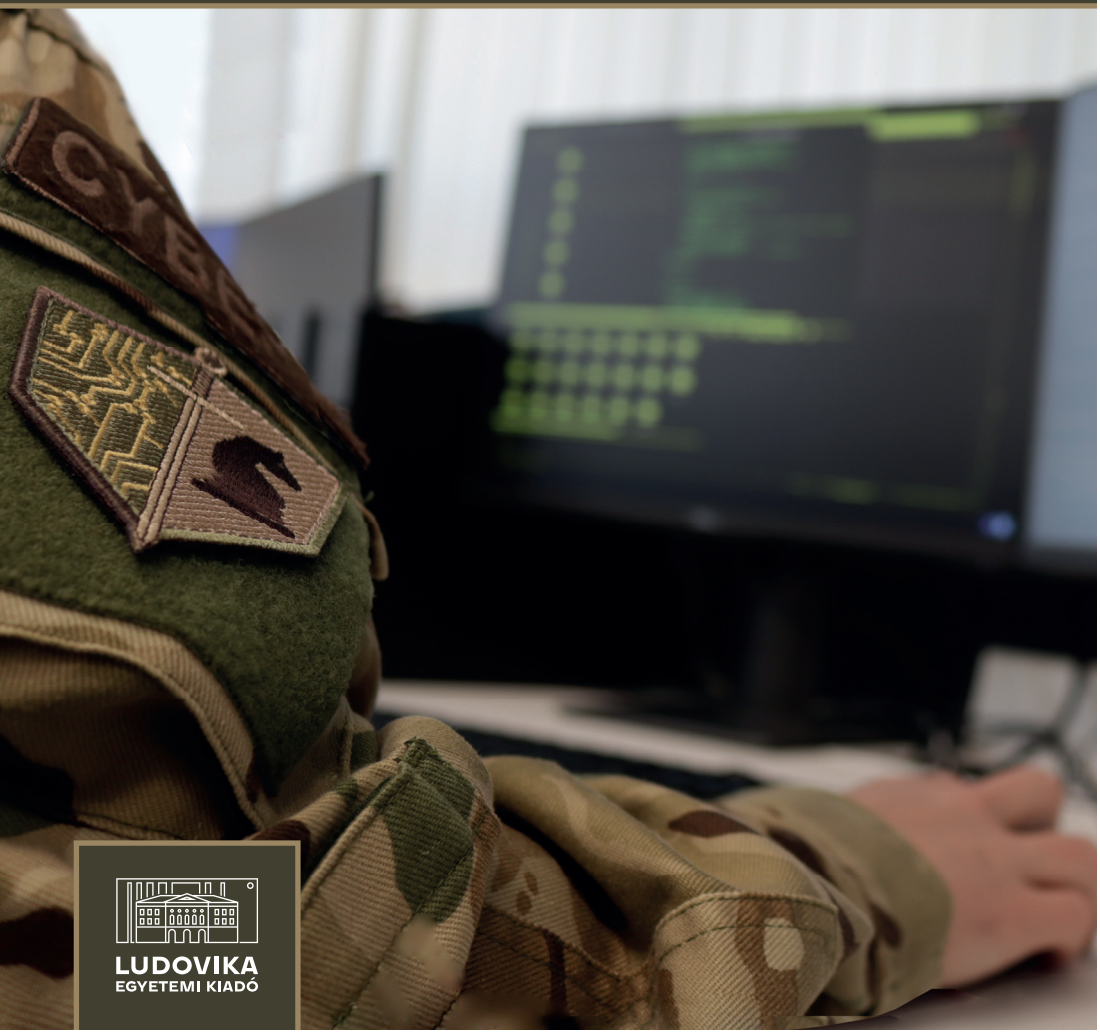
Taktikák és stratégiák a kiberhadviselésben

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 7

A kiberhadviselés fogalma, nemzetközi jogi háttere, történeti áttekintése *(Legárd Ildikó)* 11

A kibertéri műveletek fejlődése: a számítógép-hálózati műveletektől a kibertéri befolyásolásig *(Haig Zsolt)* 41

Elrettentés a kibertérben: elérhető cél vagy ábránd? *(Nyáry Gábor)* 61

Hírszerzés a kibertérben *(Deák Veronika)* 87

A proxycsoportok alkalmazásának taktikája: a hacktivisták *(Krasznay Csaba)* 115

Magánbiztonsági vállalatok szerepe az állami műveletekben *(Koller Marco)* 133

Nyomásgyakorlás a kritikus információs infrastruktúrák támadásán keresztül – A Digital Pearl Harbortól a digitális ökoszisztéma teljes támadásáig *(Kovács László)* 151

Az ellátási láncok támadása, azaz mi történik, ha már a nyomtatott áramkör sem megbízható? *(Koczka Ferenc)* 169

A katonai információs rendszerek elleni műveletek – az informatikai megsemmisítés a valós szőnyegbombázástól a precíziós *malware*-ig *(Üveges András József)* 199

Nemzeti kiberhadviselési stratégiák, végrehajtó szervezetek *(Dévai Dóra)* 221

Szövetségi stratégiák – Az EU–NATO-együttműködés *(Molnár Anna)* 237

Lehetőségek a magyar kiberműveleti képességek fejlesztésére *(Ambrus Éva)* 259

Következtetések a következő évtizedre *(Molnár Dóra)* 279

Vákát

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.

Vákát

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.

Kiberhadviselés a NATO-ban

Az államok ellen irányuló kibertámadások egyértelművé tették, hogy a NATO-nak is reagálnia kell a kihívásokra, és a kiberbiztonsággal, kiberműveletekkel kapcsolatos intézkedéseket kell bevezetnie. Az észtországi és grúz események hatására 2008-ban új Kibervédelmi Irányelvet fogadtak el, amely elsősorban a nemzeti eljárások összehangolására irányult,[34] illetve megalakult a NATO Kooperatív Kibervédelmi Kiválósági Központ (*NATO Cooperative Cyber Defence Centre of Excellence* – NATO CCD COE) Tallinnban, amely oktatási és kutatási központként funkcionál.

A NATO a 2014-es walesi csúcs zárónyilatkozatában kijelentette, hogy

> „[…] a nemzetközi jog – beleértve a nemzetközi humanitárius jogot és az ENSZ Alapokmányát – a kibertérben is érvényesül. A számítógépes támadások elérhetik azt a küszöbértéket, amely veszélyeztetheti a nemzeti és az euro-atlanti jólétet, biztonságot és stabilitást. Ezek hatása ugyanolyan káros lehet a modern társadalmak számára, mint a hagyományos támadások. Ezért megerősítjük, hogy a számítógépes védelem része a NATO alapvető kollektív védelmi feladatának."[35]

2016-ban, a varsói csúcstalálkozón az állam- és kormányfők a kiberteret hivatalosan is műveleti dimenziónak deklarálták, ezzel a kibertér hadviselési dimenzióvá vált, ahol a NATO-nak olyan hatékonyan kell megvédenie magát, mint a levegőben, a szárazföldön és a tengeren.[36] A kibervédelmet a NATO kollektív feladatai közé sorolták, az operatív hadviselést pedig kiterjesztették a kibertérre is, ezzel biztosítva, hogy egy, a NATO tagállama elleni koordinált kibertámadást a szövetség egésze elleni támadásnak tekintsenek.[37]

Több mint harminc globális techvállalat (többek között a Facebook, az F-Secure, a Github, a HP, a LinkedIn, a Microsoft, a Nokia, az Oracle, a Symantec, a TrendMicro) a biztonságos kibertér nemzetközi szintű garantálása érdekében 2018-ban aláírta a Microsoft kezdeményezésére létrehozott úgynevezett kibervé-

[34] NATO: *Bucharest Summit Declaration.* (2008. április 3.). 47. pont.

[35] NATO: *Wales Summit Declaration Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales* (2014. szeptember 5). 72. pont; Kelemen Roland – Németh Richárd: A kibertér alanyai és sebezhetősége. *Szakmai Szemle,* 2019. 103.

[36] Kovács (2018b): i. m. 272.

[37] NATO: *Warsaw Summit Communiqué. Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Warsaw* (2016. július 8–9.); Kovács (2018b): i. m. 273.

delmi technikai egyezményt *(Cybersecurity Tech Accord),* ismertebb elnevezéssel a digitális genfi egyezményt *(Digital Geneva Convention).* Ezt később a francia kormány is támogatásáról biztosította, és *Paris Call for Trust and Security in Cyberspace* címen kérte fel a releváns szereplőket a csatlakozásra. A kezdeményezéshez magyarországi vállalatok is csatlakoztak, azonban a legjelentősebb kiberműveleti erőkkel rendelkező országok, mint az USA, Oroszország, Kína vagy Irán, még nem írták alá a dokumentumot. Az egyezmény célja, hogy olyan globális szabályokat rögzítsenek a kibertámadásokra vonatkozóan az állampolgárok védelme érdekében, mint amelyeket a II. világháború után az 1949-ben létrejött genfi egyezmény biztosít a konvencionális háborúk esetében.[38]

A növekvő fenyegetést a NATO főtitkára, Jens Stoltenberg is megerősítette 2019-ben:

> „Csak egy kattintás szükséges a világszerte elterjedő számítógépes vírus elküldéséhez, de globális erőfeszítésekre van szükség ahhoz, hogy megakadályozzuk a pusztítást, és a NATO ebből kiveszi a részét. Pár perc alatt egyetlen kibertámadás dollármilliárdos értékű kárt okozhat gazdaságunkban, leállíthatja a globális vállalatokat, megbéníthatja kritikus infrastruktúránkat, alááshatja demokráciánkat és megbéníthatja katonai képességeinket. Láttuk, hogy ennek nagy része már megtörtént. És a valóság az, hogy a kibertámadások fenyegetést jelentenek, amelyekkel az elkövetkező évtizedekben küzdenünk kell.
>
> A szövetségünk biztonságát veszélyeztető számítógépes fenyegetések egyre gyakoribbak, összetettebbek és pusztítóbbak. Ezek az alacsony szintű próbálkozásoktól a technológiailag kifinomult támadásokig változnak. Állami és nem állami szereplőktől származnak, otthonról és a világ túlsó feléről. A rosszindulatú szereplők bármit megtámadhatnak automatizáltan és hálózatba kapcsolva, beleértve a zsebünkben lévő mobiltelefonokat vagy a kritikus rendszereinket és infrastruktúránkat vezérlő számítógépeket. A támadások mindannyiunkat érinthetik."[39]

Az ismertetett sorok kiválóan körvonalazzák az új típusú, negyedik generációs hadviselést és az annak részeként azonosítható kiberháborút, amely a hagyományos hadviseléstől eltérő jellemzőkkel bír. Az államok és információs rendszereik közötti virtuális háború ugyan a virtuális dimenzióban zajlik, mégis az a társadalmi, kulturális, gazdasági és politikai élet szinte minden területén megjelenik. Elveszti jelentőségét a harctér és a hátország közti megkülönböztetés, nem katonai tárgyi területek (például gazdaság, nem hadviselő felek) is érintetté válnak az összecsapásokban, megszűnik a katona és a polgár, az állam és a társadalom,

[38] Microsoft: *A Digital Geneva Convention to Protect Cyberspace* (2018. január).

[39] NATO: *NATO will Defend itself. Article by NATO Secretary General Jens Stoltenberg Published in Prospect's New Cyber Resilience Supplement* (2019. augusztus 27.).

a front és a haza közti különbség. Az ellenségesség még intenzívebbé válik, a támadásokat sok esetben több fronton egyszerre, a legváratlanabb pillanatban követik el. A támadók már nemcsak egy másik állam fegyveres egységeit támadják, hanem az állami szerveket, a társadalmat, illetve magát az egyént is.[40] Az aszimmetrikusként is jellemzett hadviselésben elmosódik a béke és a háború közti határvonal, a harctér nehezen felismerhető, ahol a nagyhatalmakon túl nem állami szereplők is szerephez jutnak. A háború „nem klasszikus jogviszonyként" jön létre, nincs hadüzenet vagy ultimátum.[41]

A kiberhadviselés nemzetközi jogi megítélése

A kiberhadviselés hagyományos formáktól eltérő jellemzői már előrevetítik a kibertámadások esetén felmerülő nemzetközi jogi szabályok alkalmazhatóságának problémáját, ugyanis a kibertevékenységek olyan sajátosságokkal bírnak, amelyek nem teszik egyértelművé a nemzetközi jog alkalmazását. A hagyományos fegyveres konfliktusokra már több évtizede létező, az egész világra kiterjedő, nagyon szigorú nemzetközi hadi jogi szabályozás létezik, azonban a kiberhadviselésre nem találunk egy az egyben alkalmazható nemzetközi jogi szabályokat.[42] Ennek legfőbb oka, hogy a hadi jogi tárgyú, katonai célpontok és bevethető fegyverek korlátozását előíró hágai egyezmények (1899, 1907), valamint a szintén nemzetközi humanitárius jogi előírásokat magukban foglaló genfi egyezmények és azok kiegészítő jegyzőkönyvei elfogadásakor (1949 és 1977) még a kiberhadviselés nem volt tényező. Az ismertetett hadi jogi nemzetközi szabályok kibertámadásokra történő alkalmazása több ponton is nehézségekbe ütközik.

Az egész nemzetközi jogrend, mind az erő alkalmazását szabályozó joganyag *(ius ad bellum),* mind pedig a nemzetközi humanitárius jog *(ius in bello)* nehezen választható el az államterülettől és a fölötte szuverenitást gyakorló államoktól. A kibertérben azonban a fizikai csatatérhez hasonló határok, frontok nehezen értelmezhetők. Ráadásul a virtuális csatatér nem tisztán katonai jellegű, mivel az adatforgalom jelentős része polgári használatú hálózaton zajlik, így azt sem

[40] Legárd Ildikó: A barát és ellenség megkülönböztetése a kibertérben. *Jog – Állam – Politika,* 12. (2020), 3. 125–140.

[41] Kelemen Roland: A kibertérből érkező fenyegetések jelentősége a hibrid konfliktusokban és azok várható fejlődése. *Honvédségi Szemle,* 148. (2020), 4. 69.

[42] Kovács (2018b): i. m. 272.

könnyű sok esetben megítélni, mi minősül jogszerűen támadható katonai célpontnak, és ki minősül „jogszerű harcosnak”.[43] Éppen ezért a NATO kérésére a NATO CCD COE szakemberei, nemzetközi hírű jogászok és kutatók megvizsgálták a hagyományos hadviselés területén alkalmazott nemzetközi jogi és nemzetközi hadi jogi szabályok kiberhadviselés területén történő alkalmazhatóságát, aminek eredményeként megjelent a *Tallinni kézikönyv (Tallinn Manual)* első, 2013-as változata,[44] és 2017-ben megjelent a 2.0-ás.[45]

Tallinni kézikönyv

A *Tallinni kézikönyv* ugyan „nemzetközi jogi értelemben nem kötelezi az államokat – ám a szokásjogi erejű normák alkalmazásától nem térhetnek el”.[46]

A 2013-as első kiadás a *Tallinni kézikönyv a nemzetközi jog alkalmazhatóságáról a kiberhadviselésben (Tallinn Manual in the International Law Applicable to Cyber Warfare)* címet viseli. A Kézikönyv két nagy részben, 7 fejezetben, 95 szabály megfogalmazásával tárgyalja részletesen a *Nemzetközi kiberbiztonsági jog (International Cyber Security Law)* és a *Kiber-hadijog (The Law of Cyber Armed Conflict)* szabályait.

2017-ben jelent meg a 2013-as kiadás aktualizált és jelentősen bővített változata *A nemzetközi jog kiberműveletekben való alkalmazhatósága (Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations)* címmel, amely négy részre osztva 154 szabályt elemez. Az új Kézikönyv – a korábbi verzióval ellentétben – már jelentős terjedelemben foglalkozik a kibertér nem erőszakos, elsősorban a békeidőben megjelenő műveleteinek leírásával is.

A mű *első része* a nemzetközi jog általános szabályait és azok kibertérben történő alkalmazhatóságát mutatja be, külön kiemelve azokat a kibertevékenységeket (például kémkedés békeidőben), amelyeket önmagában nem szabályoz egyetlen nemzetközi jogszabály sem. Többek között elemzi a szuverenitás, a kellő gon-

[43] Lattmann Tamás: Nemzetközi jogi szabályozás célzott kibertámadások esetén. In Deák Veronika (szerk.): *Célzott kibertámadások. Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára*. Budapest, Nemzeti Közszolgálati Egyetem, 2018. 43–44.

[44] Michael N. Schmitt (szerk.): *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press, 2013. 304.

[45] Michael N. Schmitt (szerk.): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge, Cambridge University Press, 2017. 638.

[46] Lattmann (2018): i. m. 45.

dosság, a joghatóság és az attribúció kérdését, az állam általi ellenintézkedések körét. A *második rész* a nemzetközi jog olyan sajátos jogintézményeivel foglalkozik, mint amelyeket a nemzetközi emberi jogi törvények szabályoznak, de külön kitér a diplomáciai és a konzuli jogra, a hagyományos hadszínterekre, valamint a telekommunikációra vonatkozó joganyag és a kibertér kapcsolatára. A *harmadik rész* a nemzetközi béke és biztonság kiberműveletekkel kapcsolatos szabályait veszi sorra. Ennek keretében olyan fontos területek jelennek meg, mint a békés rendezés, az erőszak alkalmazásának tilalma és a kollektív biztonság, valamint az ENSZ Biztonsági Tanácsának szerepe. Végül a *negyedik rész* foglalkozik az úgynevezett „kiber-hadijoggal", itt határozták meg a központi szerepet betöltő kibertámadás fogalmát. Olyan fontos területeket fejt ki, mint hogy a kibertéri konfliktusok során – hasonlóan a hagyományos hadviseléshez –, el kell kerülni a civil áldozatokat, tehát például tilos a civil célpontok, kórházak, egyházi személyek és objektumaik, illetve számítógépes rendszereik, a gyerekek és újságírók elleni támadás. A Kézikönyv külön kitér a civilek részvételére a számítógépes támadásokban, a hadviselés eszközeinek és módszereinek meghatározására, és kiemeli, hogy nem szabad felesleges sérülést és szenvedést okozni a szemben álló félnek. A könyvben szabályozzák továbbá a kulturális és a természeti javak védelmét, a humanitárius segítségnyújtást, a megszállt területekkel kapcsolatos kérdéseket és a semleges kiberinfrastruktúra védelmét is.

A NATO Kooperatív Kibervédelmi Kiválósági Központja ötéves projekt keretében felülvizsgálja a *Tallinni kézikönyv* 2017-es változatát, ami magában foglalja a korábbi fejezetek teljes frissítését a kiberműveletekre és az azokra adott állami válaszokra tekintettel. A *Tallinn Manual 3.0* kidolgozásába a nemzetközi jog szakértőit és tudósok széles körét vonják be, illetve lehetőséget biztosítanak az államok számára, hogy javaslataikkal segítsék az új verzió előkészítését. A felülvizsgálat legfőbb célja a nemzetközi jog létező szabályainak objektív leképzése a kibertér kontextusában.[47] A továbbiakban használt „Kézikönyv" elnevezés a *Tallinni kézikönyv* 2017-ben megjelent, második kiadására utal.

[47] NATO CCDCOE: *CCDCOE to Host the Tallinn Manual 3.0 Process* (2021. május).

Az ENSZ Alapokmánya deklarálja a fegyveres erőszak tilalmát, amely alól csupán két kivétel létezik: a fegyveres erő Biztonsági Tanács felhatalmazásán alapuló alkalmazása, valamint az egyéni és kollektív önvédelem jogának (51. cikk) gyakorlása.[48] Az 1. cikk bevezeti a „támadó cselekmény" fogalmát, azonban az Alapokmány vagy más nemzetközi jogszabály e fogalmat nem határozza meg. Az Észak-Atlanti Szerződés V. cikkelye a következőképp hivatkozik az Alapokmányra:

> „A Felek megegyeznek abban, hogy az egyikük vagy többjük ellen, Európában vagy Észak-Amerikában intézett fegyveres támadást valamennyiük ellen irányuló támadásnak tekintenek; és ennélfogva megegyeznek abban, hogy ha ilyen támadás bekövetkezik, mindegyikük az Egyesült Nemzetek Alapokmányának 51. cikke által elismert egyéni vagy kollektív védelem jogát gyakorolva, támogatni fogja az ekként megtámadott Felet vagy Feleket azzal, hogy egyénileg és a többi Felekkel egyetértésben, azonnal megteszi azokat az intézkedéseket – ideértve a fegyveres erő alkalmazását is –, amelyeket a békének és biztonságnak az észak-atlanti térségben való helyreállítása és fenntartása érdekében szükségesnek tart. Minden ilyen fegyveres támadást és ennek következtében foganatosított mindennemű intézkedést azonnal a Biztonsági Tanács tudomására kell hozni. Ezek az intézkedések véget érnek, ha a Biztonsági Tanács meghozta a nemzetközi béke és biztonság helyreállítására és fenntartására szükséges rendszabályokat."[49]

E cikkely kibertámadásokra történő alkalmazhatósága szempontjából több, alapvető kérdés tisztázása is szükséges: hogyan értelmezhető a támadás és a fegyveres támadás fogalma a kibertérben; egy kibertámadás mikor minősül állam elleni támadásnak; hogyan biztosítható a támadó azonosítása, az attribúció?

A fegyveres támadás fogalmának értelmezése a kibertérben

A kibertér felől számos, különböző motivációjú cselekmény valósulhat meg,[50] azonban ezeket élesen el kell választanunk a nemzetközi jog szerinti, a hadviselés körébe tartozó esetektől. Nemzetközi szabályozás hiányában a Kézikönyv

[48] ENSZ Alapokmány 39. cikk (Magyarországon kihirdette az Egyesült Nemzetek Alapokmánya törvénybe iktatásáról szóló 1956. évi I. törvény).

[49] NATO: *Az Észak-Atlanti Szerződés.* V. cikkely. 1949. április 4.

[50] Jól elkülöníthetők a kibertér felől érkező fenyegetések következő típusai: a kiberbűnözés, a hacktivizmus, a kiberterrorizmus, a kiberkémkedés és a kiberhadviselés. Krasznay Csaba: A polgárok védelme egy kiberkonfliktusban. *Hadmérnök,* 7. (2012), 4. 143–144.

92. szabálya tesz javaslatot a kibertámadás fogalmának meghatározására: „Egy kibertámadás olyan műveletet jelent, legyen az akár támadó, akár védelmi jellegű, mely alapján személyek sérülése vagy halála, illetve objektumok megrongálódása vagy megsemmisülése megalapozottan várható."[51] Természetesen a kibertámadás ténye önmagában nem feltétlenül elegendő, hogy a megtámadott államot önvédelmi helyzetbe hozza, a támadás intenzitása határozza meg annak minősítését. A Kézikönyv szerint, amennyiben a támadás nagyszámú ember életét veszélyezteti vagy oltja ki, illetve az infrastruktúrában jelentős kárt okoz, fegyveres támadásnak tekinthető. A Kézikönyv meghatározásából következik, hogy a kiberműveletek körébe tartozó információszerzés és a kibervédelem nem minősíthető fegyveres támadásnak.[52]

A Kézikönyv 92. szabálya segíthet annak megállapításában is, hogy az adott támadás eléri-e az állam elleni támadás szintjét, ugyanis az egész államot érintő tevékenység kérdéséről sem találunk szabályozást a nemzetközi jogban. Általánosságban elmondható, hogy a tulajdon megsemmisülése vagy az ember sérülése kiválthatja az erő alkalmazását a megtámadott állam válaszában.[53]

Ilyen kibertámadás érte például 2010 nyarán az iráni Natanzban található erőműben urándúsításra használt gázcentrifugákat. A kifejezetten ipari folyamatirányító rendszerek ellen kifejlesztett Stuxnet nevű féreg célja az volt, hogy a centrifugákat észrevétlenül tönkretegye, és ezzel megzavarja a dúsítási folyamatot. A Stuxnet volt az első olyan szoftver, amely képes volt tömegesen támadni ipari létesítmények vezérlőszoftvereinek működését. Ez volt az első alkalom, hogy egy rosszindulatú program közvetlen módon, valódi fizikai kárt okozott egy kritikus infrastruktúrának számító létesítményben, mivel a natanzi erőműben a gázcentrifugák túlpörgetésével legalább 1000 centrifuga vált használhatatlanná, és az akcióval sikerült az iráni atomprogramot több évvel visszavetni.[54] A vírus származásáról és az elkövetők kilétéről nincsenek pontos adatok, de a szakemberek jelentős része izraeli és amerikai fejlesztőket gyanít a támadás mögött a rosszindulatú kód visszafejtése közben talált nyomok alapján, azonban Oroszország részvételével kapcsolatos feltételezések is napvilágot láttak.[55]

[51] Schmitt (2017): i. m. 415.; Krasznay Csaba: Nemzetközi kapcsolatok a kibertérben. In Bódi Antal et al.: *Az Ibtv. gyakorlata*. Budapest, Nemzeti Közszolgálati Egyetem, 2020. 20.

[52] Schmitt (2017): i. m. 341. 71. szabály 8. pont.

[53] Krasznay (2020) i. m. 18–19.

[54] Kovács László – Sipos Marianna: A Stuxnet és ami mögötte van: tények és a cyberháború hajnala. *Hadmérnök,* 3. (2010), 4. 163–172.

[55] Panayotis A. Yannakogeorgos: Was Russia Behind Stuxnet? *The Diplomat,* 2011. december 10.

A Stuxnet esete is bizonyítja, hogy a kibertéri események hátterében álló támadók kilétének meghatározása és bizonyítása nem egyszerű feladat.

Az attribúció

A kibertér az anonimitás terepe, ahol gyakran rejtve marad a támadó. Azonban a kibertámadásra adandó válaszlépés előtt mindenképpen bizonyítani kell nemcsak a kibertámadás tényét, hanem az elkövető kilétét is. Az attribúció, azaz az elkövető megnevezése nélkülözhetetlen ahhoz, hogy egy támadást a kiberhadviselés körében értelmezzünk, és hogy ennek során egy államot azonosítsunk támadó félként.

Az attribúciónak két összetevője van: a technikai és a diplomáciai, azaz politikai attribúció. A technikai azonosítás során technikai eszközökkel, több forrásból származó információkkal, *forensic* eljárásokkal igyekeznek bizonyítani minden kétséget kizáróan az elkövető kilétét. Amennyiben ez sikeresnek bizonyult, politikai és/vagy diplomáciai eszközökkel nevezik meg a támadót.[56]

A NATO V. cikkelye szerinti önvédelmi jog gyakorlásához azonban mindenképpen a támadó állami voltát szükséges bizonyítani, amely egyértelmű lehet abban az esetben, ha valamely állam reguláris csapata (például kiberhadtest) követi el a támadást, és nehezebb ennek megítélése, amennyiben magánszemélyek vagy azok csoportjai jelennek meg elkövetőként. Az államnak való betudhatóságra nincsenek nemzetközi jogi szabályok, így annak eseteire az ENSZ Közgyűlési 3314. (XXIX.) számú határozatából, illetve a Nemzetközi Bíróság ítélkezési gyakorlatából következtethetünk. Az előbbi 3. cikk *g)* pontja kimondja, hogy agressziónak minősül az, ha egy állam fegyveres csoportokat küld egy másik állam ellen, vagy ebben komoly része van.[57] Magánszemélyek és -csoportok cselekedetei kizárólag akkor tudhatók be az államnak, ha azok az állam utasítása, irányítása vagy ellenőrzése alatt tevékenykedtek.[58] Az ellenőrzés tekin-

[56] Kovács László: A kiberbiztonság és a kiberműveletek megjelenése Magyarország új Nemzeti Biztonsági Stratégiájában. *Honvédségi Szemle,* 148. (2020), 5. 9–10.

[57] Az ENSZ Közgyűlési 3314. (XXIX.) számú határozata, 3. cikk *g)* pont; Kajtár Gábor: „Az erőszak tilalma". In Jakab András – Fekete Balázs (szerk.): *Internetes Jogtudományi Enciklopédia.* Nemzetközi jog rovat, rovatszerkesztő: Sulyok Gábor. 2018.

[58] Kelemen Roland – Pataki Márta: A kibertámadások nemzetközi jogi értékelése. *Katonai Jogi és Hadijogi Szemle,* 3. (2015), 1. 69.; részletesebben lásd Schmitt (2017): i. m. 94–100. 17. szabály.

tetében a Nemzetközi Bíróság Nicaragua-ügyben hozott ítélete az irányadó, amely szerint az ellenőrzésnek ténylegesnek kell lennie.[59]

A Kézikönyv a részt vevő magánszemélyek esetében megkülönbözteti a támadásban aktívan szerepet vállaló, szándékos magatartást tanúsítók körét, illetve a gondatlan, passzív elkövetőket. A 97. szabály alapján a polgári személyek elvesztik védettségüket a támadásban való közvetlen részvétel esetén, tehát jogszerűen támadhatóvá válnak informatikai és egyéb jogszerű módszerekkel, amennyiben fennáll a jogos önvédelem gyakorlásának a joga.[60] Passzív támadó lehet azonban az a gyanútlan végfelhasználó is, akinek az informatikai infrastruktúráját tudtán kívül, például *botnet* részeként használják. A velük szembeni lehetséges intézkedéseket a Kézikönyv nem említi, ami arra utal, hogy velük szemben nem gyakorolható az önvédelem joga. Természetesen nemcsak magánszemélyek, hanem semleges államok is lehetnek tudtukon kívül részesei kibertámadásnak. A 2007-es Észtország elleni támadások során a világ számos országából, például Magyarországról is érkeztek olyan hálózati forgalmak, amelyek összességében hozzájárultak az észt infrastruktúra teljes megbénításához.[61]

Az önvédelmi jog gyakorlása

Amennyiben a megtámadott állam részéről az eset összes körülményére tekintettel fennáll az önvédelem gyakorlásának joga, annak eszközeit és alkalmazásuk mértékét a nemzetközi szokásjog által megkövetelt és a Nemzetközi Bíróság által több ízben is megállapított[62] szükségesség és arányosság figyelembevételével határozhatja meg. A *szükségesség* azt jelenti, hogy a fegyveres támadás elhárítására nincs más mód, azonban „a megtámadott állam kizárólag a támadás elhárítása és visszaverése érdekében gyakorolhat önvédelmet. Vagyis a fegyveres erőszak alkalmazása nem lehet megtorló, büntető, vagy jövőbeli esetleges újabb támadásokat általánosan megelőző jellegű." Az *arányosság* követelmény értelmében az „önvédelem gyakorlása során az alkalmazott erőszak mértékének

[59] ICJ: Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua versus United States of America), Judgement of 27 June 1986, I.C.J. Reports 1986.
[60] Schmitt (2017): i. m. 428–432. 97. szabály.
[61] Krasznay (2020): i. m. 17–18.
[62] Például az idézett Nicaragua-ügyben hozott ítélet.

mindig a fegyveres támadással arányosnak kell lennie".[63] A felsoroltakat kiegészíti az *azonnaliság* kritériuma, azaz az önvédelmi jog gyakorlására akkor kerül sor, amikor a megtámadott fél erre az elhárításra képes.[64]

Az önvédelmi jog gyakorlása megítélésének nehézségét mutatja, hogy az eddigi kibertámadásokkal szemben a támadásokhoz mérhető ellentámadás még ezidáig nem volt bizonyítható, ami természetesen nem zárja ki, hogy a megtámadott fél védekező műveleteket ne hajtott volna végre.[65] Védekező művelet részeként végrehajtott fizikai ellencsapásra került sor 2019-ben Izrael részéről, amelynek során megtámadta és megsemmisítette a Hamász[66] egyik kiberműveleti központját, ahonnan véleménye szerint Izrael ellen kibertámadásokat hajtottak végre, ezzel megállítva a folyamatban lévő támadásokat.[67]

Konkrét esetek nemzetközi megítélése

A szakirodalom nem fogalmaz egyértelműen arról, hogy volt-e már egyáltalán a kiberhadviselés körébe tartozó, nyilvánosságra került olyan művelet, amely elérte a háborús szintet. Amit láttunk és sejtünk, azok leginkább felderítési, információszerzési célú műveletek voltak, illetve a hibrid hadviselés[68] körébe tartoztak. Az alábbiakban bemutatok néhány olyan esetet, amelyet klasszikusan a szakirodalom az első, állam elleni kibertámadások körében nevesít, illetve a közelmúlt eseményei közül a SolarWinds példáját, amely politikai nyilatkozatok sorához és a sajtó orgánumai általi nagy találgatásokhoz vezetett a tekintetben, hogy a támadás háborús cselekedet volt-e, vagy sem.

A kérdésnek azért van kiemelkedő jelentősége, mert ha a cselekmény a Kézikönyv 92. szabálya szerinti kibertámadásnak minősül, azaz háborús cselekedet,

[63] Kajtár Gábor: A terrorizmus elleni önvédelem a XXI. században. *Kül-Világ – a nemzetközi kapcsolatok folyóirata,* 8. (2011), 1–2. 14–15.

[64] Lattmann (2018): i. m. 42.

[65] Kralovánszky Kristóf: A kibertér fejlődése. *Hadmérnök,* 14. (2019), 4. 199–200.

[66] Hamász: Iszlám Ellenállási Mozgalom.

[67] Kralovánszky (2019): i. m. 200.

[68] A hibrid hadviselés „megragadja azoknak a kényszerítő és felforgató tevékenységeknek, valamint hagyományos és nem hagyományos módszereknek (például katonai, diplomáciai, gazdasági, technológiai) az egyvelegét, amelyeket állami vagy nem állami szereplők összehangolt módon használhatnak fel bizonyos célok elérése érdekében úgy, hogy eközben a hivatalosan deklarált hadviselés szintje alatt maradnak". Közös közlemény az Európai Parlamentnek és a Tanácsnak – A hibrid fenyegetésekkel szembeni fellépés közös kerete, európai uniós válasz. Bevezetés. 2016. április 6.

akkor a megtámadott fél akár fegyveres támadással is válaszolhat a jogszerű önvédelem keretében.

Az Észtország elleni támadás (2007)

Az Észtország elleni támadás menetét és legfőbb jellemzőit *[a] kiberhadviselés fogalma* részben ismertettük, jelen sorok az esemény háborús megítélésének kérdését elemzik a Kézikönyv és a nemzetközi szabályozás tükrében.

Észtország esete bebizonyította, hogy a kibertámadás során bevetett eszközök és módszerek alkalmasak lehetnek arra, hogy fegyverként alkalmazzák őket, így felmerült a NATO V. cikkelyének életbe léptetése, azonban a felek nem éltek vele.[69] Ez is bizonyítja, hogy az észt infrastruktúra ellen elkövetett támadássorozat valóban a kiberhadviselés körébe tartozott, kimerítette a Kézikönyvben meghatározott fegyveres támadás kritériumait, azonban az V. cikkely életbe léptetéséhez egy fontos tényező hiányzott, mégpedig a támadó kilétének minden kétséget kizáró bizonyítása. Az ügy felderítésében kezdetben a NATO szakértői is részt vettek, és bár a támadás „digitális lábnyomai" oroszországi szerverekhez vezettek, a támadás jellegéből adódóan az elkövetők egyértelmű azonosítása sikertelennek bizonyult. A támadáshoz olyan botnethálózatot hoztak létre, amely az orosz gépeken kívül még 178 ország területén található zombigépeket is felhasznált. Természetesen az orosz kormányzat az ügyben mindenféle érintettséget tagadott.[70]

Az orosz–grúz háborút kísérő kibercselekmények (2008)

Az orosz–grúz, hagyományos hadszíntereken folyó háborút kísérő, korábban bemutatott kibertámadások nemzetközi jogi megítélése egyértelműbb, mivel az informatikai támadásokat egy fegyveres konfliktus során, azzal párhuzamosan követték el, amikor a hadviselő feleknek be kell tartania a humanitárius jog nemzetközi szabályait.[71]

[69] Krasznay (2020): i. m. 21.
[70] Haig–Kovács (2008): i. m. 67.
[71] Az 1949-ben elfogadott genfi egyezmények közös 2. cikke értelmében az egyezményekben szereplő előírásokat minden „fegyveres konfliktus" esetén alkalmazni kell.

Az interneten keresztül intézett támadásokat két lépcsőben hajtották végre. Elsőként, még a tényleges fizikai támadásokat megelőzően a grúz kormányzati weboldalakat blokkolták túlterheléses támadásokkal, majd tartalmukat kicserélték az ország külső megítélésének lerontása érdekében. A Grúz Nemzeti Bank oldalán például Miheil Szaakasvili elnök összevágott képeit helyezték el diktátorok társaságában. A második lépcsőben, a konvencionális támadásokkal párhuzamosan, elsősorban a lakosság dezinformálására törekedtek a támadók által létrehozott weboldalak segítségével, valamint kommunikációs hálózatok (például telefonszolgáltatások) és médiafelületek blokkolásával.[72]

Ha azonban eltekintenénk a háború hagyományos színtereken folyó aspektusaitól, a Grúzia elleni támadássorozatot aligha lehetne kibertámadásként értékelni, és önmagában nem alapozná meg az V. cikkely alkalmazását. Egyrészt hiányzik az attribúció ténye. Szakértők ugyan egyetértenek abban, hogy a kibertér felől érkező támadások szorosan kapcsolódtak a katonai lépésekhez, és a támadások egy fegyveres konfliktus kísérőjeként jelentek meg, mégis, az elkövetők személyét nem sikerült minden kétséget kizáróan bizonyítani. Másrészt Grúzia a támadás időszakában nem rendelkezett fejlett informatikai hálózattal, ezért nem is rázták meg a támadások annyira, mint például Észtországot, nem bénult meg a kormányzat, a közigazgatás vagy a bankrendszer. Így önmagában a kibertérből induló cselekmények nem merítik ki a Kézikönyvben megfogalmazott kibertámadás fogalmát, az önvédelmi jogot megalapozó fegyveres támadásnak pedig a legcsekélyebb mértékben sem lehet tekinteni.

> „Ebből is látható, hogy a kibertéren keresztül érkező támadások csak abban az esetben fejtik ki a kellő hatásukat, ha fejlett információs hálózattal rendelkezik a megtámadott fél. Grúzia esetében ez nem mondható el, így – fontosságuk ellenére – a kinetikus műveletekre nagyobb szerep hárult a háború során, mint a kibertéren keresztül folytatott tevékenységeknek."[73]

Ukrán kritikus infrastruktúrák elleni támadások

Ukrajnában az elmúlt években számos kiberműveletet hajtottak végre, jellemzően az ország kritikus infrastruktúrái ellen. 2015-ben az ukrajnai, 1,4 millió lakosú

[72] Fekete Csanád – Sipos Zoltán: A kibertér megjelenése az orosz katonai műveletekben a 2008-as orosz–grúz háború tükrében. *Honvédségi Szemle,* 145. (2017), 1. 67–68.
[73] Fekete–Sipos (2017): i. m. 68.