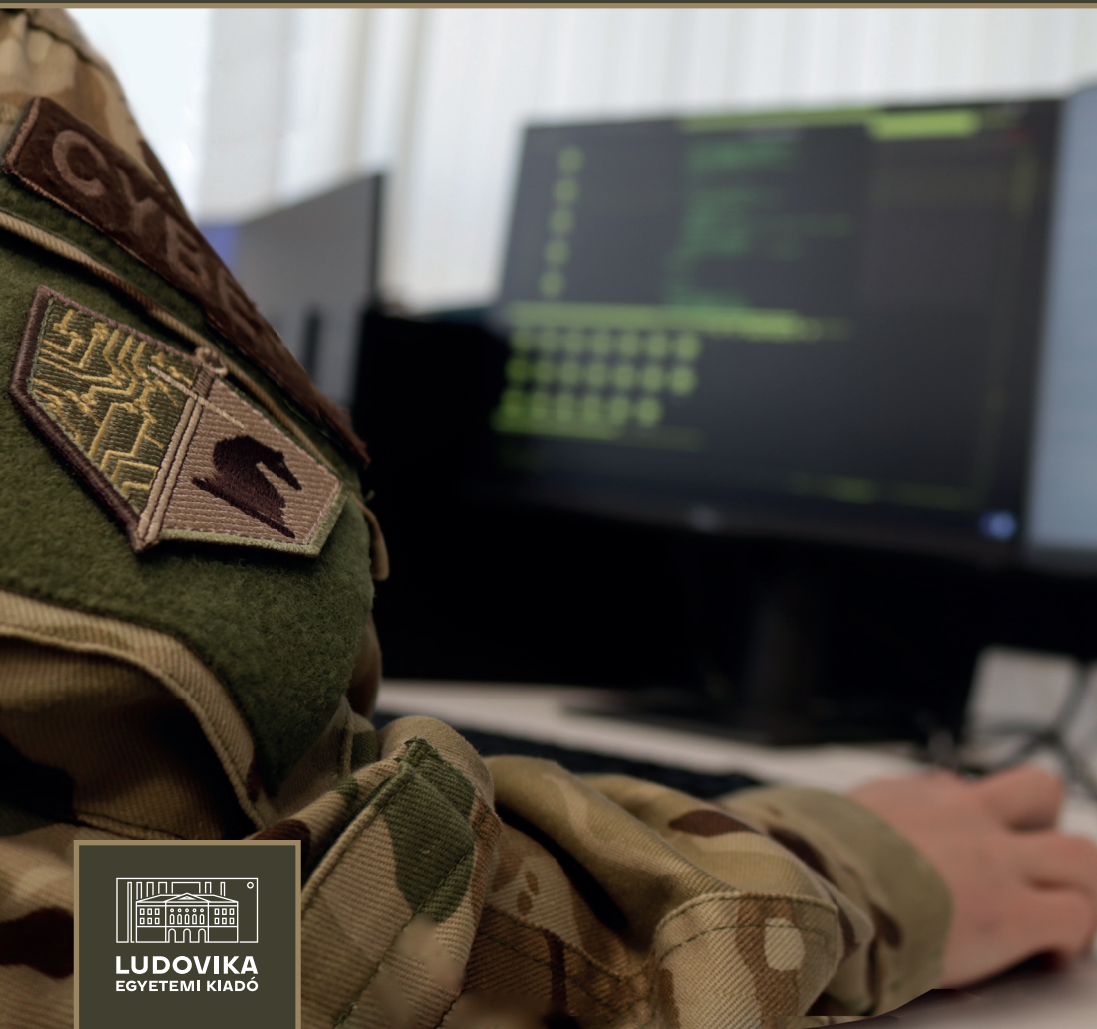
Taktikák és stratégiák a kiberhadviselésben

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

DOI: https://doi.org/10.36250/01079_00

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

© A szerző, 2023
© A kiadó, 2023

Minden jog védve.

Tartalom

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.

https://doi.org/10.36250/01079_01

https://orcid.org/0000-0002-1469-8679

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).

A NATO V. cikkelyének alkalmazási problémái

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.

Ivano-Frankivszk régióban az otthonok mintegy fele néhány órán át áram nélkül maradt. Egy ukrán sajtóorgánum szerint az áramkimaradás oka egy „vírust" használó „hackertámadás" volt. Szakértők vizsgálatai megállapították, hogy az eset nem volt egyedi, Ukrajna más energiaipari vállalatait egyidejűleg több támadás is érte, amelyek során a romboló hatású, úgynevezett KillDisk kártevő programot használták, amely elméletileg képes a kritikus rendszerek leállítására is.[74] Az energiaszolgáltató cégeket ért támadás mögött az ukrán kormány vádja szerint orosz hackerek állhattak, azonban ezt nem bizonyították.[75]

2017-ben az úgynevezett NotPetya-kampány az ukrán alkotmány ünnepe előtti munkanap utolsó óráiban kezdődött el. Bár a fertőzést több országból is jelentették, a legtöbb esetet Ukrajnában azonosították. A kártékony kód egy adóbevallási program frissítési mechanizmusán keresztül fertőzött, és végül több ezer ukrán vállalatot elért. Az áldozatok között számos kritikus infrastruktúra is megtalálható volt, mint például a kijevi Boriszpil repülőtér, több energetikai cég, de jelentős számú civil létesítmény is érintett volt. A káros kódot egyértelműen pusztító céllal hozták létre.[76] Az eset a Kézikönyv szerint értékelve egyértelműen kibertámadásnak minősül, hiszen a kritikus infrastruktúrák koordinált támadásával, például az egészségügyi rendszer vagy a rendvédelmi szervek elektronikus infrastruktúráinak esetleges kiesése, elérhetetlensége esetén megalapozottan várható személyek sérülése vagy halála.[77] A Kézikönyv szerint támadásnak minősül az ilyen kiberfegyverek használata még akkor is, ha az infrastruktúrában közvetlen kárt nem okoznak, csak közvetve fejtik ki hatásukat azok elérhetetlenségének biztosításával.[78]

Ez az eset az attribúció szempontjából kivétel, mivel 2018 februárjában hét ország (USA, Nagy-Britannia, Dánia, Litvánia, Észtország, Kanada és Ausztrália) közösen ítélte el Oroszországot a NotPetya-támadás miatt.

[74] Robert Lipovsky – Anton Cherepanov: BlackEnergy Trojan Strikes Again: Attacks Ukrainian Electric Power Industry. *WeLiveSecurity,* 2016. január 4.

[75] Al-Agha Cintia Asoum: Az ukrán kibertámadás okai – a jövő háborúja? *Biztonságpolitika.hu,* 2016. április 3.

[76] Krasznay (2020): i. m. 30–33.

[77] 2020. szeptemberben zsarolóvírus-támadásnak esett áldozatul a Düsseldorfi Egyetemi Kórház, amelynek közvetlen folyományaként az orvosok nem tudtak időben kezelni egy sürgős ellátásra szoruló nőt, akit a mentők így kénytelenek voltak másik városba szállítani. A beteg az átszállítás közben életét vesztette, ezzel hivatalosan ő lett a zsarolóvírus-támadások első halálos áldozata. Koi Tamás: Megvan a zsarolóvírusok első hivatalos halálos áldozata. *Hwsw,* 2020. szeptember 18.

[78] Krasznay (2020): i. m. 33.

2018-ban az ukrán állam tájékoztatása szerint feltehetően a Kreml által támogatott támadók olyan kritikus infrastruktúrát céloztak meg, amely az ivóvíz tisztításáért felelős. Szerencsére, az akár emberek életébe kerülő katasztrófát sikerült az ukrán szerveknek elhárítaniuk.[79]

A fenti incidenseket elemezve egyértelműen megállapítható, hogy e műveleteket fegyveres támadásnak lehet minősíteni, és ezek akár az önvédelem jogos gyakorlását is megalapozhatnák.

Az Egyesült Államok elleni SolarWinds-támadás

2020. december közepén derült fény az Egyesült Államok történetének eddigi legsúlyosabb kibertámadására, amelynek során a SolarWinds cég által forgalmazott, Orion nevű rendszerfelügyeleti és biztonsági program meghackelt frissítésén közel húszezer fontos állami hivatal – közöttük az USA hadügyminisztériuma, pénzügyminisztériuma és az USA atomfegyvereinek kezeléséért felelős kormányzati hivatal – rendszerébe juthattak be a támadók.[80]

A vizsgálatok megindulásával párhuzamosan elindultak a támadó kilétére vonatkozó találgatások a sajtóban, amelyek az orosz titkosszolgálat, az SVR korábbi csoportjait nevezték meg elkövetőként. Kiberbiztonsági szakértők már sokkal árnyaltabban fogalmaztak kezdettől fogva, mivel a támadó azonosítása és kilétének bizonyítása egy ilyen támadás esetén akár hónapokba is telhet. Az ügy kivizsgálására a Nemzetbiztonsági Tanács által életre hívott Kiber Koordinációs Egyesített Munkacsoport 2021. január 5-én nyilatkozatot adott ki az addigi eredményekről; kijelentették, hogy az akció hátterében egy feltételezhetően orosz eredetű állami hackercsoport (APT – *advanced persistent*

[79] Alexander J. Martin: Russian Hackers Targeted Ukraine's Water Supply, Security Service Claims. *Sky.com,* 2018. július 11.

[80] CISA: *Active Exploitation of SolarWinds Software* (2020. december 13.); Ravie Lakshmanan: US Agencies and FireEye Were Hacked Using SolarWinds Software Backdoor. *The Hacker News,* 2020. december 13.

threat) állhat.[81] A nyilatkozat külön kitér arra is, hogy a támadást kifejezetten hírszerző műveletként értékelik.

Ez utóbbi kijelentésnek azért is van jelentős súlya, mivel a támadás napvilágra kerülésétől kezdve több olyan politikai nyilatkozat is született, amely kifejezetten háborús cselekedetnek nyilvánította a SolarWinds-akciót, amellyel szemben Amerikának válaszcsapást kell mérnie az elkövetőkre.[82] Hiszen, amennyiben fegyveres támadásnak nyilvánul az incidens, úgy az Egyesült Államokat is megilletheti az önvédelem jogának gyakorlása, így akár fegyveres válaszcsapást is indíthat az elkövetőkkel szemben.

A Fehér Ház 2021. április 15-én kiadott állásfoglalása alapján egyértelműen orosz kormányzati körökhöz köthető az Egyesült Államokat ért eddigi egyik legsúlyosabb kibertámadás, amelyet az orosz hírszerzés, azaz az SVR hajtott végre.[83] A bejelentést kísérve a pénzügyminisztérium azonnali szankciókkal sújtott öt orosz technológiai céget, amely a minisztérium szerint az SVR-t, illetve általában véve az orosz kémtevékenységet támogathatta.[84]

Az ügy legfontosabb tanulsága, hogy bár jelen esetben az attribúcióra, tehát az elkövető azonosítására, bizonyítására és diplomáciai megnevezésére is sor került, ez önmagában kevés volt az V. cikkely életbe léptetéséhez, mivel az Egyesült Államok egyértelműen nem kibertámadásként és háborús cselekedetként, hanem hírszerzési akcióként nevesítette az esetet. Természetesen a határvonal rendkívül keskeny, „mindkét tevékenységet ugyanazon a hálózaton és eszközökkel végzik, és a választóvonalat csupán néhány billentyű leütésével át lehet lépni".[85]

[81] „This work indicates that an Advanced Persistent Threat (APT) actor, likely Russian in origin, is responsible for most or all of the recently discovered, ongoing cyber compromises of both government and non-governmental networks." In Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA). 2021. január 5.

[82] Nyáry Gábor: Háború és béke a kibertérben (2. rész). *Ludovika.hu,* 2021. január 19.

[83] Reuters – Christopher Bing: White House Blames Russian Spy Agency SVR for SolarWinds Hack: Statement. *Reuters,* 2021. április 15.

[84] U.S. Treasury: Treasury Sanctions Russia with Sweeping New Sanctions Authority (2021. április 15.).

[85] Nyáry (2021): i. m.

Következtetések – Van-e háború a kibertérben?

Napjainkra a technikai fejlődés jelentősen átalakította a katonai értelemben vett fenyegetések rendszerét, a háborúról alkotott fogalmainkat. Az államok egymás közti viszonyaiban és konfliktusaiban már nem a hagyományos hadszíntereken folytatott klasszikus, szimmetrikus hadviselés dominál, hanem a hadszíntér virtuális dimenzióiban megnyilvánuló hibrid és kiberhadviselés a jellemző. A kibertér speciális műveleti területet biztosít a katonai tevékenységek számára, amely a kiber-információszerzés és a kibervédelem területe mellett olyan kibertámadások kivitelezését is lehetővé teszi, amelyek hatalmas pusztítást képesek okozni klasszikus katonai fellépés és fegyverek nélkül is.

Egy biztos, a kibertérben végrehajtott támadások már nem írhatók le a háború klasszikus fogalmát megalkotó, a háború mibenlétét elemző, a fegyveres erőt és az ütközeteket középpontba állító Carl von Clausewitz gondolataival.[86] „A nem fegyverrel elkövetett, halálos áldozatot közvetlenül nem követelő, de hatalmas anyagi károkat és káoszt előidézni képes újfajta, aszimmetrikus kihívások miatt bővült a háború és a támadás fogalmainak jelentése. A károkozás mértékétől függően egy nem fegyveres támadás – megítélését tekintve – akár egy fegyveres támadással is egyenértékű lehet." A kiberhadviselés anyagi kár okozásában és a közrend megzavarásában potenciálját tekintve egyre kevésbé marad el a hagyományos fegyverektől.[87]

Ugyanakkor a napjainkban sokszor elhangzó „kiberháború" és „kibertámadás" kifejezéshez sem a nemzetközi jogban, sem a NATO terminológiájában nem párosul hivatalos definíció, ráadásul a négy genfi egyezménnyel párhuzamosan inkább a „fegyveres konfliktus", illetve az ENSZ Alapokmányában használt „fegyveres támadás" szóhasználat terjedt el leginkább. Bár a Kézikönyv meghatározza a kibertámadás fogalmát (92. szabály), ám az az államokat nem kötelezi, azonban fontos elvi és gyakorlati iránymutatásként szolgál e cselekmények megítélésében.

Jelenleg még egyetlen kibertámadás esetén sem került sor annak háborús cselekményként történő azonosítására, és így a támadással egyenértékű válaszlépés foganatosítására. A fejezetben bemutatott példák is bizonyítják, hogy ritkán lehet olyan kibertámadásokkal találkozni, mint például az Észtország elleni

[86] Tóth I. János: Clausewitz a háború lényegéről. *Létünk,* (2014), 3. 30.

[87] 1656/2012. (XII. 20.) Korm. határozat Magyarország Nemzeti Katonai stratégiájának elfogadásáról. 52. pont.

támadás vagy a NotPetya-kampány, amelyek kritikus infrastruktúrák vagy akár azok egyes elemeinek támadásán keresztül kifejezetten egy adott ország működését igyekeznek ellehetetleníteni. Tehát ebben az értelemben, bár számos, a Kézikönyvben meghatározott fogalmat kimerítő kibertámadás történt az elmúlt években, némelyik eset a fegyveres támadás szintjét is elérhette, azonban a kibertérben ez idáig a kibertámadásokhoz mérhető, akár fegyveres ellentámadás nem volt bizonyítható. Az Észak-atlanti Szerződés V. cikkelye alkalmazásának hiánya elsősorban az attribúció nehézségeire vezethető vissza, hiszen a támadó kilétének bizonyítása ütközik a legnagyobb nehézségbe a kibertámadások esetében. Ismert ellenség híján azonban katonai akcióval nem lehet visszatámadni.

Összefoglalva tehát klasszikus értelemben nem beszélhetünk arról, hogy háború folyna a kibertérben, azonban az elmúlt néhány év eseményeit áttekintve egyértelmű, hogy a jövő konfliktusait a hálózatokon fogják megvívni, ami szükségessé teszi a kiberháború és a kiberhadviselés fogalmának nemzetközi szintű meghatározását és szabályozását. A kibertér adta lehetőségek egy új típusú háború korszakát indították el, ahol a „kibertéri nagyhatalmak", mint az USA, Oroszország, Kína, Irán, Izrael vagy Észak-Korea, az anonimitás és a láthatatlanság felhőjébe burkolózva egyre erőteljesebben fejlesztik kiberképességeiket, amelyek erejét időnként megvillanni látjuk egy-egy kibertámadásban, de valódi hatásukat ma még talán meg sem tudjuk becsülni.

Irodalomjegyzék

1656/2012. (XII. 20.) Korm. határozat Magyarország Nemzeti Katonai stratégiájának elfogadásáról

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

A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény

Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény

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. Online: https://nmhh.hu/dokumentum/219724/Alkonyi_Aurel_Informacios_kontroll.pdf

Asoum, Al-Agha Cintia: Az ukrán kibertámadás okai – a jövő háborúja? *Biztonságpolitika.hu*, 2016. április 3. Online: https://biztonsagpolitika.hu/egyeb/az-ukran-kibertamadas-okai-a-jovo-haboruja

Az Észak-Atlanti Szerződés. 1949. április 4. Online: www.nato.int/cps/ic/natohq/official_texts_17120.htm?selectedLocale=hu

Berki Gábor: A kibertéri konfliktusok változásai. *Hadmérnök,* 8. (2013), 1. 173–185. Online: http://hadmernok.hu/2013_1_berkig.pdf

Berki Gábor: Kiberháborúk, kiberkonfliktusok. In Pintér István (szerk.): *Műhelymunkák. A virtuális tér geopolitikája.* Budapest, Geopolitikai Tanács Közhasznú Alapítvány, 2016. 245–284. Online: http://real.mtak.hu/id/eprint/80322

CISA: *Active Exploitation of SolarWinds Software* (2020. december 13.). Online: https://us-cert.cisa.gov/ncas/current-activity/2020/12/13/active-exploitation-solarwinds-software.

Clarke, Richard A. – Robert K. Knake: *Cyber war: The Next Threat to National Security and What to do about it*. New York, Harper & Collins, 2010. 13–18.

Douzet, Frédérick: Geopolitika a kibertér megértéséhez. (Ford. Monti Norbert.) In Pintér István (szerk.): *Műhelymunkák. A virtuális tér geopolitikája.* Budapest, Geopolitikai Tanács Közhasznú Alapítvány, 2016. 19–42. Online: https://mek.oszk.hu/16100/16182/16182.pdf

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.). Online: https://eur-lex.europa.eu/legal-content/hu/TXT/?uri=CELEX%3A52021DC0118

Európai Bizottság: *Európa digitális évtizede: a 2030-ra kitűzött célok* (2021. március 9.). Online: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_hu

Fekete Csanád – Sipos Zoltán: A kibertér megjelenése az orosz katonai műveletekben a 2008-as orosz–grúz háború tükrében. *Honvédségi Szemle,* 145. (2017), 1. 59–71. Online: http://publicatio.bibl.u-szeged.hu/14808/1/Honved_neveles_Honvedsegi_Szemle.pdf

Gémesi Csaba: A kibertér és szereplői. *Hadmérnök,* 13. (2018), 3. 403–415. Online: http://hadmernok.hu/183_30_gemes.pdf

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

Gibson, William: *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.

Haig Zsolt: *Információs műveletek a kibertérben*. Budapest, Dialóg Campus, 2008.

Haig Zsolt – Kovács László: Fenyegetések a cybertérből. In *Nemzet és Biztonság,* 1. (2008), 5. 61–70. Online: www.nemzetesbiztonsag.hu/cikkek/haig_zsolt__kovacs_laszlo-fenyegetesek_a_cyberterb__l.pdf

Haig Zsolt – Kovács László – Ványa László: Az elektronikai hadviselés, a SIGINT és a cyberhadviselés kapcsolata. *Felderítő Szemle,* 10. (2011), 1–2. 183–209. Online: http://hdl.handle.net/20.500.12944/2003

Haig Zsolt – Várhegyi István: A cybertér és a cyberhadviselés értelmezése. *Hadtudomány,* 18. (2008), elektronikus szám. 1–12. Online: http://hdl.handle.net/20.500.12944/2202

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. Online: www.icj-cij.org/public/files/case-related/70/070-19860627-JUD-01-00-EN.pdf

Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms (2010. november 8.). Online: https://irp.fas.org/doddir/dod/jp1_02.pdf

Joint Statement by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of the Director of National Intelligence (ODNI), and the National Security Agency (NSA) (2021). Online: www.cisa.gov/news/2021/01/05/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure

Kajtár Gábor: A terrorizmus elleni önvédelem a XXI. században. *Kül-Világ,* 8. (2011), 1–2. 2–25. Online: http://epa.oszk.hu/00000/00039/00024/pdf/EPA00039_kulvilag_2011_01-02_kajtar.pdf

Kajtár Gábor: Az erőszak tilalma. In Jakab András et al. (szerk.): *Internetes Jogtudományi Enciklopédia.* Budapest, ORAC Kiadó – Társadalomtudományi Kutatóközpont Jogtudományi Intézete. A szócikk lezárva: 2018. március 16. Online: https://ijoten.hu/szocikk/az-eroszak-tilalma

Kelemen Roland: A kibertérből érkező fenyegetések jelentősége a hibrid konfliktusokban és azok várható fejlődése. *Honvédségi Szemle,* 148. (2020), 4. 65–81. Online: http://dx.doi.org/10.35926/HSZ.2020.4.5

Kelemen Roland – Németh Richárd: A kibertér alanyai és sebezhetősége. *Szakmai Szemle,* 2019. 95–118. Online: www.academia.edu/44681770/A_kibertér_alanyai_és_sebezhetősége

Kelemen Roland – Pataki Márta: A kibertámadások nemzetközi jogi értékelése. *Katonai Jogi és Hadijogi Szemle,* 3. (2015), 1. 53–90. Online: http://epa.oszk.hu/02500/02511/00004/pdf/EPA02511_katonai_jogi_szemle_2015_01_053-090.pdf

Koi Tamás: Megvan a zsarolóvírusok első hivatalos halálos áldozata. *Hwsw,* 2020. szeptember 18. Online: www.hwsw.hu/hirek/62298/zsarolovirus-ransomware-tamadas-hacker-korhaz-dusseldorf.html

Kovács László: Információs hadviselés kínai módra. *Nemzet és Biztonság,* 2. (2009), 7. 35–44. Online: www.nemzetesbiztonsag.hu/cikkek/kovacs_laszlo-informacios_hadviseles_kinai_modra.pdf

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

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

Kovács László: A kiberbiztonság és a kiberműveletek megjelenése Magyarország új Nemzeti Biztonsági Stratégiájában. *Honvédségi Szemle,* 148. (2020), 5. 3–18. Online: http://dx.doi.org/10.35926/HSZ.2020.5.1

Kovács László – Illési Zsolt: Cyberhadviselés. *Hadtudomány,* 21. (2011), 1–2. 29–41. Online: www.mhtt.eu/hadtudomany/2011/1/HT-2011_1-2_5.pdf

Kovács László – Sipos Marianna: A Stuxnet és ami mögötte van: tények és a cyberháború hajnala. *Hadmérnök,* 3. (2010), 4. 163–172. Online: http://hadmernok.hu/2010_4_kovacs_sipos.pdf

Közös közlemény az Európai Parlamentnek és a Tanácsnak – A hibrid fenyegetésekkel szembeni fellépés közös kerete, európai uniós válasz. Bevezetés. 2016. április 6. Online: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52016JC0018&from=HU

Kralovánszky Kristóf: A kibertér fejlődése. *Hadmérnök,* 14. (2019), 4. 197–212. Online: http://dx.doi.org/10.32567/hm.2019.4.13

Krasznay Csaba: A polgárok védelme egy kiberkonfliktusban. *Hadmérnök,* 7. (2012), 4. 142–151. Online: http://hadmernok.hu/2012_4_krasznay.pdf

Krasznay Csaba: Nemzetközi kapcsolatok a kibertérben. In Deák Veronika (szerk.): *Az Ibtv. gyakorlata. Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára, 2020.* Budapest, Nemzeti Közszolgálati Egyetem, 2020. 6–36.

Lakshmanan, Ravie: US Agencies and FireEye Were Hacked Using SolarWinds Software Backdoor. *The Hacker News,* 2020. december 13. Online: https://thehackernews.com/2020/12/us-agencies-and-fireeye-were-hacked.html

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. 39–52.

Legárd Ildikó: A barát és ellenség megkülönböztetése a kibertérben. *Jog – Állam – Politika,* 12. (2020), 3. 125–140. Online: https://jap.sze.hu/images/lapsz%C3%A1mok/2020/3/JAP_2020_03_legard-ildiko.pdf

Lipovsky, Robert – Anton Cherepanov: BlackEnergy Trojan Strikes Again: Attacks Ukrainian Electric Power Industry. *WeLiveSecurity,* 2016. január 4. Online: www.welivesecurity.com/2016/01/04/blackenergy-trojan-strikes-again-attacks-ukrainian-electric-power-industry/

Martin, Alexander J.: Russian Hackers Targeted Ukraine's Water Supply, Security Service Claims. *Sky.com,* 2018. július 11. Online: https://news.sky.com/story/russian-hackers-targeted-ukraines-water-supply-security-service-claims-11432826

Microsoft: *A Digital Geneva Convention to Protect Cyberspace* (2018. január). Online: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RW67QH

NATO: *Bucharest Summit Declaration* (2008. április 3.). Online: www.nato.int/cps/en/natolive/official_texts_8443.htm

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.). Online: www.nato.int/cps/ic/natohq/official_texts_112964.htm

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.). Online: www.nato.int/cps/en/natohq/official_texts_133169.htm

NATO: *NATO will Defend itself. Article by NATO Secretary General Jens Stoltenberg Published in Prospect's New Cyber Resilience Supplement* (2019. augusztus 27.). Online: www.nato.int/cps/en/natohq/news_168435.htm?selectedLocale=en

NATO CCDCOE: *CCDCOE to Host the Tallinn Manual 3.0 Process* (2021. május). Online: https://ccdcoe.org/news/2020/ccdcoe-to-host-the-tallinn-manual-3-0-process/

Nyáry Gábor: Az adatok geopolitikája: az Internet mitikus szabadságától a digitális szuverenitás felé. *Ludovika.hu,* 2020. december 7. Online: www.ludovika.hu/blogok/cyberblog/2020/12/07/az-adatok-geopolitikaja-az-internet-mitikus-szabadsagatol-a-digitalis-szuverenitas-fele/

Nyáry Gábor: Háború és béke a kibertérben (2. rész). *Ludovika.hu,* 2021. január 19. Online: www.ludovika.hu/blogok/cyberblog/2021/01/19/haboru-es-beke-a-kiberterben-2-resz/

O'Neill, Patrick Howell: The Cyberattack that Changed the World. *The Daily Dot,* 2016. május 20. Online: www.dailydot.com/debug/web-war-cyberattack-russia-estonia/

Reuters – Christopher Bing: White House Blames Russian Spy Agency SVR for SolarWinds Hack: Statement. *Reuters,* 2021. április 15. Online: www.reuters.com/business/white-house-blames-russian-spy-agency-svr-solarwinds-hack-statement-2021-04-15/

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

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

Toonders, Joris: Data is the New Oil of the Digital Economy. *Wired,* 2014. július. Online: www.wired.com/insights/2014/07/data-new-oil-digital-economy/

Tóth I. János: Clausewitz a háború lényegéről. *Létünk,* (2014), 3. 25–41. Online: http://epa.oszk.hu/00900/00997/00031/pdf/EPA00997_Letunk-2014_3_025-041.pdf

Tölgyesi Beatrix: Az orosz „szuverén internet" törvényről. *Nemzet és Biztonság,* 13. (2020), 2. 113–132. Online: www.nemzetesbiztonsag.hu/cikkek/822-cikk_szoveg-13437-1-10-20201106.pdf

U.S. Treasury: *Treasury Sanctions Russia with Sweeping New Sanctions Authority* (2021. április 15.). Online: https://home.treasury.gov/news/press-releases/jy0127

Yannakogeorgos, Panayotis A. : Was Russia Behind Stuxnet? *The Diplomat,* 2011. december 10. Online: https://thediplomat.com/2011/12/was-russia-behind-stuxnet/

2. fejezet

A kibertéri műveletek fejlődése: a számítógép-hálózati műveletektől a kibertéri befolyásolásig

Haig Zsolt

A kibertéri technológiák fejlődése

Az elmúlt években az infokommunikációs technológiák rohamos fejlődése a korábbi számítógép-hálózati struktúrákon túlmutató, alapvető szemléletváltást idézett elő a hálózatok kialakításában, felépítésében, kapcsolati formáikban, valamint működési környezetük, azaz a kibertér értelmezésében. A paradigmaváltást a hagyományos számítógép-hálózatok mellett elsősorban a vezeték nélküli hálózati technológia egyre erősödő dominanciája jellemzi, ideértve például a vezeték nélküli szenzorhálózatok, az 5G mobilkommunikáció, a gép-gép (*machine to machine* – M2M) kommunikáció és a dolgok internete (*Internet of Things* – IoT) egyre szélesebb körű alkalmazását. Ezek mellett a mesterséges intelligencia, a virtuális/kiterjesztett valóság, a mélytanuló rendszerek, a gépi látás és más hasonló forradalmi technológiák is jelentősen átalakítják a kibertéri tevékenységek jellegét.

Az újfajta vezeték nélküli technológiáknak köszönhetően megfigyelhető, hogy az IoT terjedése következtében egyre több fizikai eszköz, hétköznapi használati tárgy is az internetre csatlakozik. Így az internetre kapcsolódó hálózatos eszközök száma folyamatosan növekszik, amelyek között a vezeték nélküli kommunikációt használók száma egyértelmű dominanciát mutat. A Statista felmérése és prognosztizációja szerint 2018 végén világszerte 22 milliárd IoT-eszköz volt használatban, ami 2025-re várhatóan 30,6 milliárdra, 2030-ra pedig 50 milliárdra nő.[1]

Zheng és Carter elemzése szerint az IoT terjedését alapvetően az olcsó, kis méretű, de nagy teljesítményű szenzorok és aktuátorok megjelenése; a vezeték

[1] Statista: *Number of Internet of Things (IoT) Connected Devices Worldwide in 2018, 2025 and 2030.* (2021. január).

https://doi.org/10.36250/01079_02

https://orcid.org/0000-0002-0326-9086

nélküli kommunikációs technológia bővülése; az adattárolási és feldolgozási kapacitás növekedése; valamint az újszerű szoftveralkalmazások, a jelfeldolgozás és a mesterséges intelligencián alapuló gépi tanulás fejlődése generálja.[2] Az IoT ma már megjelenik az emberek mindennapi életében, az okosotthonokban és az okosvárosokban, valamint a társadalmi működést biztosító infrastruktúrákban, mint például az egészségügy, az energiaellátás, az ipari vállalatok, a közlekedés, a közbiztonság és a honvédelem.

Az IoT-technológia egyik kritikus eleme az adatkommunikáció, különösen a vezeték nélküli megoldások. A szenzor/aktuátor oldalán alapvetően kis hatótávolságú és alacsony energiaigényű kommunikációt használnak, mint például ZigBee, WiFi, BLE *(Bluetooth low energy).* A felhőalapú adatfeldolgozás oldalán azonban többnyire nagyobb hatótávolságú kommunikációra van szükség, amelyet cellás mobilrendszerekkel vagy nagy hatótávolságú, de alacsony fogyasztású eszközökkel valósítanak meg, mint például a Lo-RaWan *(Long Range Radio Wide Area Network)* vagy az NB-IoT *(Narrow Band IoT).*

Az 5G megjelenése és elterjedése az IoT széles körű felhasználásnak egyik fő hajtóereje. Ez az új mobiltechnológia a korábbi rendszerekhez (3G, 4G) képest többek között nagyobb adatátviteli sebességet (elméleti csúcs: 20 Gbit/s; felhasználói: 100+ Mbit/s), rendkívül alacsony késleltetést (1 ms), valamint a 4G-nél nagyobb kapacitást és kapcsolatsűrűséget (10^6 eszköz/km^2) biztosít.[3] Ezek a minőségi jellemzők alapvető fontosságúak az IoT nagymértékű elterjedéséhez, különösen az önvezető járművek és az okosközlekedés számára. Az előrejelzések szerint 2024-re az 5G mobilelőfizetések száma világszerte mintegy 1,9 milliárdra növekedik.[4]

A vezeték nélküli hálózatos tendencia a katonai rendszerekben is megfigyelhető: a polgári technológiák fokozatos megjelenését tapasztalhatjuk a katonai hálózatokban is. A NATO például megkezdte az IoT katonai alkalmazhatóságának kutatását,[5] és az eredmények azt igazolják, hogy az IoT katonai célú felhasználásának, az IoMT *(Internet of Military Things)* vagy IoBT *(Internet*

[2] Denise E. Zheng – William A. Carter: *Leveraging the Internet of Things for a More Efficient and Effective Military.* Center for Strategic & International Studies. Rowman & Littlefield, 2015. szeptember 1–2.

[3] ITU RM 2083: *Recommendation ITU RM 2083-0 (09/2015) Framework and Overall Objectives of the Future Development of IMT for 2020 and Beyond.* 2015.

[4] Statista: *Forecast Number of Mobile 5G Subscriptions Worldwide by Region from 2019 to 2026* (2021. január).

[5] NATO STO: *Military Applications of Internet of Things.* 2016.

of Battlefield Things) -megoldásokon belül számos területe lehet, amelyek közé tartoznak például az automatizált felderítő és vezetési, irányítási rendszerek, a logisztika, a tűzvezetés, az egészségiállapot-monitorozás és egyéb alkalmazások.

A mai hálózatos technológiák és az internethez való hozzáférés egyik alapvető kérdése a mobilitás, ami miatt a hálózatok tipikus kommunikációs módszere egyre inkább az elektromágneses spektrumot használó vezeték nélküli kapcsolatokra helyeződik. E tartomány használata kibővíti a potenciális támadási lehetőségeket, például a rádiófelderítés és a rádiózavarás vagy a GPS-zavarás és a *spoofing* révén, ami még tovább növeli a hálózatba kapcsolt rendszerek sebezhetőségét.

A kibertéri hálózatos technológiákban a másik igen jelentős tendencia, hogy a közösségi média terjedésével intenzíven növekszik a kibertér kognitív információs és interakciós célú használata. Ma az emberek információs tevékenységeiket nagyrészt az interneten, különösen a közösségi médiában végzik. Ennek eredményeként mint felhasználók a kibertér szereplőjévé válnak, és ezen keresztül célzott információkkal minden eddiginél könnyebben elérhetők, ezáltal befolyásolhatók, vagy akár manipulálhatók. Mindez azt is jelenti, hogy a kibertér komplexitása miatt a fenyegetések is összetettebbekké, a támadási felületek pedig egyre változatosabbakká és kiterjedtebbekké válnak.

A kibertér értelmezése

A kibertéri műveletek és különösen az e műveletekben alkalmazható szerteágazó információs tevékenységek megértéséhez mindenekelőtt szükséges a kibertér értelmezése. Ahogy az első fejezetben is olvasható, a kibertérnek számos értelmezése lehetséges. Jelen fejezetben egy újabb, elsősorban katonai megközelítésű értelmezéssel gazdagítjuk a korábbi definíciókat. A *Tallinn Manual* meghatározása szerint a kibertér „a számítógépes hálózati adattárolásra, módosításra és cserére szolgáló, fizikai és nem fizikai összetevőkből kialakított környezet”.[6] A definíció fontos megállapítása, hogy a kibertér nemcsak virtuális, azaz nem fizikai összetevőkből, hanem fizikai komponensekből is áll.

[6] Michael N. Schmitt (szerk.): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge, Cambridge University Press, 2017. 564.

Ugyanakkor az előzőekben bemutatott vezeték nélküli hálózatos technológiák radikális elterjedése a kibertér újszerű, kiterjesztett megközelítését eredményezte. Ez azt jelenti, hogy a kibertér értelmezésében a fizikailag és matematikailag is jól definiálható elektromágneses spektrum új elemként jelenik meg, amit számos meghatározás is alátámaszt. Egyik ezek közül Sanjeev Relia definíciója, amely szerint:

> „A kibertér az az ember alkotta digitális közeg, amelyet az elektromágneses spektrumban az elektronikai eszközök felhasználásával az emberek közötti adat- és információgyűjtésre, tárolásra és továbbításra használnak, és amely szervezeti, kulturális, nemzeti vagy politikai határok nélkül azonnali, határtalan, globális kapcsolatokat tesz lehetővé."[7]

Idesorolandó Daniel Kuehl meghatározása is, aki azt állítja, hogy

> „a kibertér az információs környezetben egy olyan globális tartomány, amelynek egyedi és megkülönböztető jellegzetessége, hogy az egymással összefüggő és hálózatba kapcsolt infokommunikációs rendszerekben az információ létrehozását, tárolását, módosítását, cseréjét és felhasználását végző elektronikai és elektromágneses spektrumot használó eszközök működnek".[8]

A hadtudomány az elsők között ismerte fel a kibertér átfogó és kibővített értelmezését, és azt a katonai műveleti környezet és az információs környezet egyik fontos területének tekinti. A nagyhatalmak és a NATO is nagy hangsúlyt fektet arra, hogy a kiberteret és az abban zajló műveleteket meghatározza. A NATO AJP-3.20 összhaderőnemi kibertéri műveleti doktrínája szerint a kibertér „minden olyan összekapcsolt kommunikációs, informatikai és egyéb elektronikai rendszerekből, hálózatokból és az azokban kezelt adatokból álló globális tartomány, beleértve az önálló vagy független rendszereket is, amelyek adatokat dolgoznak fel, tárolnak vagy továbbítanak".[9]

A hivatkozott kibertéri definíciókat elemezve az alábbi következtetéseket vonhatjuk le: a kibertér mesterségesen létrehozott tartomány, amely például a közösségi médiának köszönhetően újfajta személyközi kapcsolatokat,

[7] Sanjeev Relia: *Cyber Warfare: Its Implications on National Security.* New Delhi, Vij Books India Pvt Ltd., 2015. 22–23.

[8] Daniel Kuehl: From Cyberspace to Cyberpower: Defining the Problem. In Franklin D. Kramer – Stuart H. Starr – Larry K. Wentz (szerk.): *Cyberpower and National Security.* University of Nebraska Press, 2009. 27.

[9] AJP-3.20: *Allied Joint Doctrine For Cyberspace Operations. Edition A Version 1.* NATO Standardization Office, 2020. január 4.

kapcsolati hálókat biztosít az emberek számára. Ki kell azonban emelnünk azt a tényt, hogy a kibertér mint újfajta kapcsolati tér nem kizárólag az emberek számára áll rendelkezésre.

Ke Xu és szerzőtársai rávilágítanak a kibertér azon természetére, amelyet az emberek, a számítógépek és az intelligens eszközök összekapcsolódása jellemez. Ez az összekapcsolódás megfigyelhető az IoT-nak és a meglévő hálózati rendszereknek az integrációjában, beleértve az internetet, a felhőalapú számítástechnikát, a cellás mobilhálózatokat, valamint a közösségi és ipari hálózatokat. Rámutatnak, hogy a heterogén hálózatos technológiák integrációja a kibertéri hálózati innováció fő mozgatórugójává vált.[10]

A bemutatott definíciók elemzése és szintézise alapján megfogalmazható a kibertér újszerű, átfogó definíciója.

> „A kibertér egy az ember által mesterségesen létrehozott olyan dinamikusan változó tartomány, amelyben az információ gyűjtését, tárolását, feldolgozását, továbbítását és felhasználását végző, egymással hálózatba kapcsolt, és az elektromágneses spektrumot is felhasználó infokommunikációs eszközök és rendszerek működnek, lehetővé téve ezzel az emberek és a különféle eszközök közötti folyamatos és globális kapcsolatot."[11]

Ez a meghatározás rámutat, hogy a kibertér ma már nemcsak az interperszonális kapcsolatok, hanem az ember-gép és az M2M-kapcsolatok színterévé is vált. Ezenkívül lehetőséget ad a kibertéri műveleteknek az eddiginél szélesebb körű értelmezésére, amely a hálózatok és komponenseik elleni tipikus logikai szoftveres fenyegetéseken és védelmen túl az elektromágneses spektrumban és a kognitív térben alkalmazható technikákat és módszereket is magában foglalja (bővebben lásd később).

A fenti meghatározás alátámasztja a kibertér struktúrájának újszerű megközelítését is. A kibertérrel foglalkozó különféle szakirodalmi munkák és katonai doktrínák a kiberteret háromrétegű struktúrában ábrázolják, amely rétegek szorosan illeszkednek az információs környezet dimenzióihoz. E rétegek: a fizikai réteg, a logikai réteg és a kiberszemélyiség-réteg *(1. ábra)*.[12]

[10] Ke Xu – Yi Qu – Kun Yang: A Tutorial on Internet of Things: From a Heterogeneous Network Integration Perspective. *IEEE Network,* 30. (2016), 2. 102–108.

[11] Haig Zsolt: *Információs műveletek a kibertérben.* Budapest, Dialóg Campus, 2018. 226.

[12] AJP-3.20 (2020): i. m. 3; JP 3-12: *Cyberspace Operations.* 2018. június 8. I-3.

1. ábra: A kibertér struktúrája

Forrás: a szerző szerkesztése az AJP-3.20 (2020): i. m. 3. és a USNA: *Aspects and Pillars of Cyber Security* (é. n.) alapján

A fizikai réteg az adatok és információk kibertérbeni gyűjtését, tárolását, feldolgozását és továbbítását végző eszközökből áll. Idetartoznak a hálózati infrastruktúrák, számítógépek, szerverek, *routerek, hubok, switchek,* vezetékes és vezeték nélküli kommunikációs eszközök, valamint az adattároláshoz, az adatfeldolgozáshoz és az adatátvitelhez elengedhetetlen egyéb berendezések.[13] A fentieken kívül e rétegbe tartoznak a kiberfizikai eszközök, valamint a fizikailag definiálható elektromágneses spektrum is, azon belül is különösen a rádiófrekvenciás tartomány.

A logikai réteg a hálózatok virtuális tere, amely a kibertér fizikailag nem megfogható elemeit tartalmazza. E réteg adatokból és kódokból áll, mint például

[13] AJP-3.20 (2020): i. m. 3.

az operációs rendszerek, a protokollok, a szoftveralkalmazások, a *firmware,* valamint egyéb szoftverek és adatkomponensek.

A kiberszemélyiség-réteg a szervezetek és az egyének virtuális reprezentációiból áll. Idetartoznak az e-mail-címek, a felhasználói azonosítók, a közösségimédia-fiókok, az avatarok, az álnevek, az egyéni IP- és MAC-címek stb.[14] E rétegen keresztül lehet közvetlenül elérni a felhasználókat.

A kibertér e rétegeinek azonosítása lehetőséget ad arra, hogy az információs műveletekkel összefüggésben, a kibertéri műveletek keretében értelmezzük a három rétegben folytatható információs tevékenységeket.

Az információs műveletek rövid áttekintése

Ahhoz, hogy az információs műveletekkel összefüggésben értelmezzük a kibertéri műveleteket, célszerű röviden áttekinteni az információs műveletek lényegét és információs képességeit. Az információs műveletek működési területe az információs környezet, amelyben fizikai, információs és kognitív dimenziók értelmezhetők. A kibertér e környezet egyre fontosabb és jelentősebb részét képezi, és mint ahogy az előzőekben láttuk, az információs környezet mindhárom dimenzióját érinti.

Az információs műveletek kifejezés olyan katonai műveleti képességet jelent, amelynek általános célja a katonai műveletek támogatása az információs környezetben. Ezt az általános célt a műveletek jellegétől, környezetétől és célközönségétől függően információs fölény kialakításával és/vagy befolyásoló hatások előidézésével érheti el. A hagyományos katonai műveletekben az információs fölény alapvetően technikai kérdés, amelyet a szemben álló fél információs képességeinek gyengítésével és a saját képességek védelmével lehet elérni. A 4. generációs műveletekben azonban az információs műveleteket gyakran nem ellenséges erők ellen hajtják végre, hanem a célközönséget semleges, civil szereplők képezik. E műveletekben a cél nem a képességek gyengítése, hanem a civil szereplők meggyőzése vagy befolyásolása. Ezt a befolyásoláson alapuló adaptív információs fölény révén lehet elérni.[15]

[14] AJP-3.20 (2020): i. m. 3–4.

[15] Joint Doctrine Note 2/13: Information Superiority. Swindon, Ministry of Defence, 2013. 1–4.

> „Az információs műveletek az információs környezetben érvényesülő információs képességek integrált, összehangolt és koordinált alkalmazására irányuló tevékenységek összessége, amelyek a műveletek célkitűzéseinek elérése érdekében, kognitív képességekkel közvetlenül, ill. technikai képességekkel közvetetten hatásokat gyakorolnak a műveletekben résztvevő célközönség szándékára, helyzetértelmezésére és képességeire."[16]

A meghatározás alapján az információs műveletek lényege és erősokszorozó jellege a különféle információs képességek integrációjában és a műveleti céloknak megfelelő összehangolásában rejlik. Ezek az információs képességek attól függően, hogy milyen dimenziókra hatnak, két nagy csoportba sorolhatók: technikai képességek és kognitív képességek.

A technikai képességek az információkezelési folyamatokra összpontosítanak, nevezetesen az információgyűjtésre, -tárolásra, -feldolgozásra és -továbbításra, és közvetetten gyakorolnak hatásokat a célközönségre. Ezzel szemben a kognitív képességek különböző információközvetítő eszközök és módszerek használatával az információ tartalmára fókuszálnak, és közvetlenül az emberek tudati tevékenységét célozzák meg előre megtervezett üzenetekkel.

A fentiek alapján az információs műveletek technikai és kognitív képességei közé a következőket sorolhatjuk:

- technikai képességek:
  - elektronikai hadviselés (*electronic warfare* – EW);
  - számítógép-hálózati műveletek (*computer network operations* – CNO);
  - információs célpontok fizikai megsemmisítése;
  - műveleti biztonság technikai képességei;
  - megtévesztés technikai képességei;
- kognitív képességek:
  - pszichológiai műveletek (*psychological operations* – PSYOPS);
  - civil-katonai együttműködés;
  - a műveletbiztonság kognitív képességei;
  - a megtévesztés kognitív képességei.[17]

A célközönségnek megfelelő technikai és kognitív képességek szinkronizált és integrált alkalmazása biztosítja az információs műveletek céljainak elérését, és ezáltal a katonai műveletek sikeres támogatását.

[16] Haig (2018): i. m. 210.
[17] Haig (2018): i. m. 215.

Kibertéri műveletek

A kibertéri műveletek értelmezéséhez az információs műveletekkel analóg módon célszerű megvizsgálni, hogy e műveletekben a fölény kialakítható-e, és ha igen, akkor mely információs tevékenységek és milyen módon alkalmazhatók ennek érdekében. Az alábbi alfejezetekben e kérdéseket tekintjük át.

Kibertéri fölény és kibertéri befolyásoló hatások

A kibertér jelentőségének felismerésével párhuzamosan a katonai doktrínákban is megjelent a kibertéri fölény értelmezése. Az amerikai hadsereg 2017-ben kiadott FM 3-12 doktrínája az alábbiak szerint definiálja a kibertéri fölényt: „a kibertéri fölény egy katonai erő kibertéri dominanciájának azon foka, amely lehetővé teszi számára, ill. a kapcsolódó földi, légi, tengeri és űrbéli erők számára, hogy adott időben és helyen biztonságos és megbízható műveleteket folytasson anélkül, hogy az ellenség vagy a szemben álló fél akadályozná abban."[18] A kibertéri műveletek számos analógiát mutatnak az információs műveletekkel, amelyek közül az egyik a fölény kialakítására való törekvés. A kibertéri fölény az információs fölénynek az a része, amely a hálózatba kapcsolt infokommunikációs rendszerek felhasználásával érhető el, és ennek eredményeként a saját képességek jelentősen megnőnek.

A 4. generációs hibrid műveletekben, ahol gyakran nincs ellenség, vagy nem azonosítható egyértelműen, a hagyományos információs fölényhez hasonlóan a fentieknek megfelelően nem lehet kialakítani a kibertéri fölényt. Ebben az esetben ugyanis a kibertámadások és a kibertéri negatív befolyásoló tevékenységek nem alkalmazhatóak a civil szereplőkkel szemben. A cél ehelyett a pozitív befolyásolással kialakított adaptív kibertéri fölény megteremtése.

A kibertéri műveletek értelmezése

A kibertéri műveletek kialakulása katonai megközelítésben az információs műveletekhez kötődik, azon belül a számítógép-hálózatok harctéri megjelenésével

[18] FM 3-12: *Cyberspace and Electronic Warfare Operations.* Washington DC, Headquarters Department of the Army, 2017. április 1–3.

közel egy időben a CNO-hoz vezethető vissza. Habár az USA szárazföldi haderejének 1996-os első információsműveletek-doktrínája[19] még nem tartalmazta ezt a fajta képességet, két évvel később az összhaderőnemi információs műveletek doktrínája[20] már beemelte a számítógép-hálózati támadást (*computer network attack* – CNA) és az informatikai biztonságot *(computer security)* az információs műveletek elemei közé. A CNO komplex képességként pedig elsőként az amerikai összhaderőnemi információs műveletek 2006-os doktrínájában jelent meg mint az információs műveletek alapvető képessége.[21]

A kibertéri műveletek fogalma tehát a CNO-ból fejlődött ki, de a korábban bemutatott kibertéri technológia fejlődése és a kibertér komplex értelmezése következtében ma már annak nem csak egyedüli képességét jelenti. A NATO kibertériműveletek-doktrínája általánosságban fogalmazza meg a kibertéri műveleteket, amelynek értelmében e műveletek „a kibertérben vagy azon keresztül végzett tevékenységek, amelyeknek célja a saját erők cselekvési szabadságának megőrzése a kibertérben és/vagy a parancsnokok céljainak elérését szolgáló hatások előidézése".[22] A doktrína a támadó és védelmi célú kibertéri műveleteket különbözteti meg.

A kibertéri műveleteknek az információs műveletekkel való szoros kapcsolódása, illetve a kibertér kibővített értelmezése lehetőséget ad arra, hogy a fenti doktrína meghatározásához képest konkrétabban definiáljuk a kibertéri műveleteket. Ezekre figyelemmel, a kibertéri műveletek alatt a kibertérben érvényesülő információs képességek integrált, összehangolt és koordinált alkalmazására irányuló tevékenységek összességét értjük, amelyek a műveleti célok érdekében, a kibertéri hálózatos infokommunikációs rendszereket felhasználva hatásokat gyakorolnak a műveletekben részt vevő célközönség szándékára, helyzetértelmezésére és képességeire. Fontos hangsúlyozni, hogy mint ahogy az információs műveletekkel, úgy a kibertéri műveletekkel is minden esetben az emberre, a felhasználóra, vagyis a célközönségre kívánunk hatást gyakorolni. Ezt a kibertérben a hálózatos infokommunikációs technológiát felhasználva, kognitív információs képességekkel közvetlenül, illetve technikai információs képességekkel közvetetten érhetjük el.[23]

[19] FM 100-6: *Information Operations.* Washington DC, Headquarters Department of the Army, 1996. augusztus.

[20] JP 3-13: *Joint Doctrine for Information Operations* (1998. okóber 8.).

[21] JP 3-13: *Joint Doctrine for Information Operations* (2006. február 13.). II-4.

[22] AJP-3.20 (2020): i. m. 4.

[23] Haig (2018): i. m. 237.

A kibertéri műveletek effajta értelmezése a NATO és az USA korábban hivatkozott kiberműveleti doktrínáinak a továbbgondolása, amelynek alapját az adja, hogy az információs műveletekhez hasonlóan az adott műveleti térben, vagyis a kibertérben értelmezhető információs képességek integrációja és a műveleti céloknak megfelelő összehangolása a korábbi szűken vett értelmezéshez képest nagyobb lehetőségeket és műveleti hatékonyságot biztosít.

A kibertéri műveletek információs képességei

A kibertér kiterjesztett értelmezését figyelembe véve az információs műveletek szinte mindegyik korábban felsorolt technikai és kognitív információs képessége alkalmazható a kibertéri műveletekben támadó, védelmi, valamint befolyásolási céllal.

Támadásra és védelemre a kibertér fizikai és logikai rétegében alapvetően a különféle technikai képességekkel számolhatunk, amelyek közül a legjellemzőbb és legelterjedtebb a logikai rétegben megvalósuló klasszikus CNO, amelynek keretében hálózati felderítő-, támadó- és védelmi tevékenységek alkalmazhatók. Emellett a fizikai rétegben a vezeték nélküli technológiáknak köszönhetően egyre fokozottabban számolhatunk a hálózatos rendszerek és a hálózati kommunikáció elektronikai alapú felderítésével, azon belül is elsősorban a rádiófrekvenciás tartományban a rádióelektronikai felderítéssel (*signal intelligence* – SIGINT), valamint ezek elektromágneses spektrumban való támadásával (például zavarásával) és védelmével, vagyis az EW-vel. E technikai képességeken belül a teljesség igénye nélkül az alábbi támadó- és védelmi tevékenységek alkalmazhatók:

- a számítógép-hálózatokhoz való hozzáférés és azok felderítése, kihasználása (CNO);
- az adatbázisokhoz való hozzáférés, azok módosítása és megsemmisítése (CNO);
- kártékony programokkal *(malicious software – malware)* a hálózat és elemei működésének korlátozása (CNO);
- túlterheléses támadásokkal (*distributed denial of service* – DDoS) a szolgáltatásokhoz való hozzáférés akadályozása (CNO);
- a hálózati kommunikáció felfedése és lehallgatása (SIGINT);
- az adatgyűjtő szenzorok és hálózati kommunikációs eszközök és rendszerek elektronikai zavarása (EW);

– a hálózatos rendszerekben alkalmazott navigációs rendszerek elleni elektronikai támadások különböző formái, például elektronikai zavarás, hamisítás (EW); valamint
– védelem a másik fél hasonló tevékenységei ellen (CNO, EW).

A kibertér és az elektromágneses spektrum közötti konvergencia a vezeték nélküli hálózatos technológiáknak köszönhetően egyre markánsabbá válik. A teljes konvergencia azonban még nem valósult meg, de például az amerikai hadsereg 2017-ben kiadott szakmai doktrínája[24] már kellően alátámasztja az elektromágneses spektrumban zajló EW és a kibertéri műveletek közötti egyre szorosabb kapcsolatot, különösen azért, mert az elektromágneses spektrumban alkalmazható technikák kibővítik a hálózatok elleni fenyegetések lehetőségét.

Az EW sok tekintetben hasonlít a CNO-hoz. Mindkettő fő feladata az infokommunikációs rendszerek felderítése, támadása és védelme, de míg az előbbi ezeket az elektromágneses spektrumban, fizikai hatások előidézésével éri el, addig az utóbbi mindezeket logikai módszerekkel, például *malware*-ekkel végzi. Az EW a kibertérben a hálózati eszközök és a hálózati kommunikáció elektronikai megfigyelésében (SIGINT, elektronikai támogatás), elektronikai támadásában (elektronikai zavarás, megtévesztés és megsemmisítés), valamint a saját rendszerek elektronikai védelmében nyilvánul meg. Egy további szoros kapcsolódási pont, hogy a vezeték nélküli hálózatokba a különféle *malware*-ek a rádiófrekvenciás tartományt felhasználva juttathatók be. Ez sajátos és újszerű elektronikai támadási technikának tekinthető, amely a rádiófrekvenciás zavarás helyett a fizikai és logikai módszereket ötvözi. Ez különösen nagy fontosságot kap a szoftvervezérelt rádiórendszerekkel (*software defined radio* – SDR) megvalósított hálózati kommunikáció esetében.

A hálózatos technológia jelentősen kiterjeszti a kognitív hatásokat előidéző képességek lehetőségeit, alkalmazási módjait is a kibertérben. Az internet és azon belül a közösségi média új lehetőségeket nyitott a kognitív befolyásolás terén, amit egyre nagyobb mértékben használnak ki az egyes szereplők. Ez azt jelenti, hogy az internetes médiafelületeket és a közösségi szolgáltatásokat kognitív hatások előidézésére használják.

Kibertéri befolyásolásra, illetve megtévesztésre és manipulációra a kibertér kiberszemélyiség-rétegében a kognitív képességek közül elsősorban a PSYOPS és a megtévesztés alkalmazható. Az előbbi körébe tartozhatnak az internetes

[24] FM 3-12 (2017): i. m.

hírportálokon és a közösségi médián keresztül terjesztett valós üzenetek és hírek, amelyek képesek befolyásolni a kiválasztott célcsoportot vagy célszemélyeket, illetve a közvéleményt. Az utóbbi körébe pedig az álhírekkel megvalósított félretájékoztatás, félrevezetés és manipuláció sorolható.

A kibertér befolyásolási célból való felhasználásának egyik legnagyobb előnye, hogy az üzenetek rövid idő alatt széles tömegekhez juthatnak el, aminek köszönhetően az információ terjedési sebessége és célcsoportja megsokszorozódik. Mindezeken túl a véleményvezérek közösségi oldalakon keresztüli megcélzásával a befolyásuk alatt lévők jóval könnyebben elérhetők, és az üzenetek is hatékonyabban célt érnek és érvényesülnek. A teljesség igénye nélkül a kibertéri műveletek legjellemzőbb információs képességeit, célpontjait, valamint eszközeit és módszereit az *1. táblázat* foglalja össze.

1. táblázat: A kibertéri műveletek legjellemzőbb információs képességei

Kibertéri műveleti képesség	**Célpontok**	**Eszközök és módszerek**
Számítógép-hálózati műveletek	Hálózat, szoftverek, operációs rendszerek, adatbázisok, hardverelemek, kiberfizikai eszközök	Számítógép-hálózati felderítés, támadás, védelem, például *malware,* DDoS, adatbázistörlés, -módosítás, APT-támadás stb.
Elektronikai felderítés	Hálózati elektronikai eszközök, vezeték nélküli kommunikáció	SIGINT, műszeres felderítés, nyílt forrású felderítés
Elektronikai hadviselés	Hálózati elektronikai eszközök, szenzorok, vezeték nélküli kommunikáció, navigáció, kiberfizikai eszközök	Elektronikai felderítés, elektronikai zavarás, elektronikai megtévesztés, elektronikai megsemmisítés, elektronikai védelem
Pszichológiai műveletek	Emberek, közösségi csoportok	Befolyásolás internetes hírportálokon, közösségi médián, e-mail-en keresztül, *social engineering*
Megtévesztés	Hálózat, szenzorok, adatbázisok, kommunikáció, emberek, közösségi csoportok	Elektronikai megtévesztés, imitálás, dezinformáció, *spoofing, social engineering,* álhírek stb.

Forrás: Haig (2018): i. m. 240.

A politika, a gazdaság és az egész társadalom működésének hálózatos infokommunikációs technológiától való függősége ahhoz vezetett, hogy mára a kibertérből érkező fenyegetések egyre gyakoribbakká váltak. Szinte naponta hallani újabb és újabb kibertámadásokról, amelyek akár technikai, akár kognitív tevékenységek formájában valósulnak meg. Többnyire a technikai oldalhoz sorolható például a katona-politikai hatású és a NATO kibertéri gondolkodását is megváltoztató 2007-es Észtország elleni DDoS-támadássorozat,[25] vagy például a 2021. májusi jelentős gazdasági károkat és üzemanyaghiányt okozó zsarolóvírus-támadás az észak-amerikai Colonial Pipeline olajvezetékhálózat ellen.[26] A legismertebb kognitív kibertámadásokhoz pedig többek között a 2016-os amerikai elnökválasztási kampány befolyásolása sorolható, amelyben többek között szerepet játszott a Cambridge Analytica és a Facebook felhasználói adatbotránya,[27] illetve a szentpétervári székhelyű Internetkutató Ügynökség (Internet Research Agency – IRA)[28] nevű „trollgyár" is.

Bár e néhány kiragadott példa esetében is megfigyelhető volt, hogy többféle információs tevékenységet is alkalmaztak a támadók, azoknak a kibertéri műveletekre jellemző összehangolt és integrált alkalmazása leginkább az orosz–ukrán konfliktusban figyelhető meg. E konfliktusban ugyanis egyértelműen felismerhető a hibrid hadviselés keretében alkalmazott kibertéri műveletek korábban bemutatott komplexitása, amelyet a 2. táblázat is szemléltet. A válságot megelőzően mind orosz, mind ukrán hackercsoportok több száz DDoS- és *defacement* támadást intéztek állami szervek weboldalai ellen. A válság kirobbanását követően az ukrán mobiltávközlési hálózatot és a vezetési és irányítási rendszereket korlátozták egyrészt a szolgáltató létesítményének elfoglalását követően odatelepített blokkolókkal, valamint az EW rendszerekben alkalmazott különféle zavaró berendezésekkel.[29] 2015 decemberében az ukrán áramellátásban volt

[25] Kovács László: *A kibertér védelme.* Budapest, Dialóg Campus, 2018. 145.

[26] Renee Dudley – Daniel Golden: The Colonial Pipeline Ransomware Hackers Had a Secret Weapon: Self-promoting Cybersecurity Firms. *MIT Technology Review,* 2021. május 24.

[27] Kovács László – Krasznay Csaba: „Mert övék a hatalom": Az internet politikát (is) befolyásoló hatása a 2016-os amerikai elnökválasztás során. *SVKK Elemzések,* (2017), 9.

[28] Jason Parham: Facebook and the Price of Tech Utopia. *Wired.com,* 2018. április 10.

[29] Sergey Sukhankin: Russian Electronic Warfare in Ukraine: Between Real and Imaginable. *Eurasia Daily Monitor,* 71. (2017), 14.

szolgáltatáskiesés, amelyet egy APT-támadás keretében a BlackEnergy nevű trójaival idéztek elő.[30]

2. táblázat: Az orosz–ukrán konfliktus kibertéri műveletek célpontjai, képességei és hatásai

Célpontok	Ukrán és orosz intézmények, hálózatok, csatlakoztatott eszközök, ipari vezérlőrendszerek, média, lakosság és semleges érintettek
Eszközök és módszerek	DDoS, weboldal defacement, *malware*-ek (BlackEnergy, Snake, Operation Armageddon, X-Agent, CrashOverride, NotPetya, BadRabbit, VPNFilter, Python/Telebot), elektronikai lehallgatás, zavarás, hagyományos elektronikus és online média, közösségi oldalak, Internetkutató Ügynökség, propaganda- és álhírkampányok
Hatások, eredmények	Szolgáltatáshoz való hozzáférés akadályozása, adatlopás, kommunikáció akadályozása, ukrán erőművek elleni támadás miatt több órás áramkimaradás, sérült számítógépek, eszközök és rendszerek, célközönség befolyásolása, manipulálása, félrevezetése
Időtartam	2013 novemberétől napjainkig

Forrás: Haig (2018): i. m. 240.

E technikai kiberképességek mellett a kognitív képességek is jelentős szerepet kaptak az orosz érdekek érvényesítésében. A hagyományos média *(Sputnik, Russia Today)* mellett az online médiát és a közösségi hálót is nagy hatékonysággal használták a célzott üzenetek továbbítására. Egy vizsgálat például igazolta, hogy 2014-től kezdve a Twitteren ugrásszerűen megnőtt az Ukrajnával foglalkozó tweetek száma. Ezeket a befolyásoló, manipuláló üzeneteket és gyakran álhíreket döntően a már említett szentpétervári „trollgyár" állította elő. Kiemelendő például, hogy 2014. július 18-án, a malajziai repülőgép lezuhanásának napján több mint 44 000, a következő napon pedig több mint 25 000 üzenetet tettek közzé. Ezekben a tweetekben 297 fiók terjesztett olyan információkat, amelyek szerint Ukrajna volt a felelős a maláj gép lelövéséért.[31]

A néhány kiragadott példa és a konfliktus kibertéri műveleteit összefoglaló *2. táblázat* is jól szemlélteti e műveletek komplexitását, és azt, hogy mind

[30] Marie Baezner – Patrice Robin: *Cyber and Information Warfare in the Ukrainian Conflict, Version 2.* Center for Security Studies (CSS), ETH Zürich, 2018. október 10.

[31] Oleksandr Nadelnyuk: How Russian "Troll Factory" Tried to Effect on Ukraine's Agenda. Analysis of 755 000 tweets. *VoxUkraine,* é. n.

a reguláris és irreguláris erők, mind a civil hackercsoportok által folytatott műveletek egyre gyakrabban járulnak hozzá katonai és politikai célok eléréséhez.

Következtetések

Mára a hálózatok kialakítása, a hálózati elemek és azok struktúrája, valamint a hálózati kommunikáció megvalósítása a hagyományos számítógép-hálózatokhoz képest jelentős átalakuláson ment keresztül. A felhőtechnológia, az IoT- és az M2M-kapcsolatoknak köszönhetően a kiberfizikai érzékelőkkel és aktuátorokkal rendelkező hálózatokban megvalósul a teljes összekapcsolódás, ahogyan azt például az okosotthon- és az okosváros-koncepciók is alátámasztják.

A közösségi hálózatok térnyerésének és fokozódó szerepének eredményeképpen pedig az emberek is egyre inkább a hálózatok részesévé válnak. Mindez rávilágít a kibertér azon természetére, ahol az emberek, a számítógépek és az intelligens eszközök egymással összekapcsolódnak. A kibertér mára az interperszonális kapcsolatok mellett az ember-gép és a gép-gép kapcsolatok színterévé vált.

Az egyének közösségi hálózaton való könnyebb elérhetőségének következtében, valamint a vezeték nélküli technológia természetéből adódóan az újfajta hálózatok a jól ismert szoftveres támadások mellett számos korábban nem jellemző sebezhetőséggel, fenyegetéssel is szembesülnek, mint például az érzékelők által gyűjtött adatok módosítása, a vezeték nélküli adatkommunikáció lehallgatása és/vagy elektronikai zavarása, illetve az emberek kognitív befolyásolása, manipulálása.

A kibertérben zajló katonai műveletek szempontjából az új technológiák és az újfajta sebezhetőségek szükségessé tették a kibertérnek és struktúrájának újraértelmezését. Ennek megfelelően a tisztán logikai felfogás mellett a fizikai tér, beleértve az elektromágneses spektrumot is, valamint a kognitív tartomány is fontos részét képezi a kibertérnek. A kibertér háromrétegű (fizikai, logikai és kiberszemélyiség-réteg) struktúrája lehetőséget ad a kibertéri műveletek komplexebb értelmezésére, amely nem korlátozódik kizárólag a CNO-ra. E komplex értelmezés lényege, hogy a kibertéri műveletek keretében az információs műveletekhez hasonlóan, olyan egymással összehangolt technikai és kognitív információs képességeket lehet alkalmazni, amelyek egymás hatásait kihasználva a kibertérben érvényesülnek. Ez pedig a korábbi értelmezéshez képest nagyobb lehetőségeket és műveleti hatékonyságot biztosít az alkalmazók számára.

Ezek a kibertéri információs képességek az alábbiak lehetnek:

- a logikai rétegben alkalmazott logikai (szoftveralapú) információs képességek, mint például *malware*-ek, DDoS-támadások, APT-támadások, tűzfalak, vírusirtók stb.;
- a fizikai rétegben és benne az elektromágneses spektrumban folytatott elektronikai felderítés (különösen a SIGINT), elektronikai zavarás, megtévesztés és megsemmisítés, valamint a fizikai és elektronikai védelem módszerei stb.;
- a kiberszemélyiség-rétegben, azaz a kognitív tartományban valós és hiteles vagy félrevezető információkon alapuló kognitív képességek, mint a PSYOPS, a megtévesztés, az álhírek stb.

A kibertéri műveletek hatékonysága tehát nagymértékben függ a kibertér mindhárom rétegében zajló információs tevékenységek összehangoltságától. A tapasztalatok pedig azt is mutatják, hogy a kibertér által biztosított hálózati technológiáknak köszönhetően nemcsak a katonai műveletekben, hanem a politikai és gazdasági konfliktushelyzetekben is a kibertéri műveletekbe integrált és egymással összehangolt információs tevékenységek nagyobb eredményességgel alkalmazhatók.

Irodalomjegyzék

AJP-3.20: *Allied Joint Doctrine For Cyberspace Operations. Edition A Version 1.* NATO Standardization Office, 2020. január 4.

Baezner, Marie – Patrice Robin: *Cyber and Information Warfare in the Ukrainian Conflict, Version 2.* Center for Security Studies (CSS), ETH Zürich, 2018. október. Online: www.researchgate.net/publication/322364443_Cyber_and_Information_warfare_in_the_Ukrainian_conflict

Dudley, Renee – Daniel Golden: The Colonial Pipeline Ransomware Hackers Had a Secret Weapon: Self-promoting Cybersecurity Firms. *MIT Technology Review*, 2021. május 24. Online: www.technologyreview.com/2021/05/24/1025195/colonial-pipeline-ransomware-bitdefender/

FM 100-6: *Information Operations.* Washington DC, Headquarters Department of the Army, 1996. április

FM 3-12: *Cyberspace and Electronic Warfare Operations.* Washington DC, Headquarters Department of the Army, 2017. április 1–3. Online: https://irp.fas.org/doddir/army/fm3-12.pdf

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

ITU RM 2083: *Recommendation ITU RM 2083-0 (09/2015) Framework and Overall Objectives of the Future Development of IMT for 2020 and Beyond.* 2015. Online: www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-I!!PDF-E.pdf

Joint Doctrine Note 2/13: Information Superiority. Swindon, Ministry of Defence, 2013. Online: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/819814/archive_doctrine_uk_info_superiority_jdn_2_13.pdf

JP 3-12: *Cyberspace Operations.* 2018. június 8.

JP 3-13: *Joint Doctrine for Information Operations* (2006. február 13.).

JP 3-13: *Joint Doctrine for Information Operations* (1998. október 8.).

Kovács László – Krasznay Csaba: „Mert övék a hatalom": Az internet politikát (is) befolyásoló hatása a 2016-osamerikai elnökválasztás során. *SVKK Elemzések,* (2017), 9. Online: https://bit.ly/3Ox1FKi

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

Kuehl, Daniel: From Cyberspace to Cyberpower: Defining the Problem. In Franklin D. Kramer – Stuart H. Starr – Larry K. Wentz (szerk.): *Cyberpower and National Security.* University of Nebraska Press, 2009. 24–42.

Nadelnyuk, Oleksandr: How Russian "Troll Factory" Tried to Effect on Ukraine's Agenda. Analysis of 755 000 tweets. *VoxUkraine,* é. n. Online: https://voxukraine.org/longreads/twitter-database/index-en.html

NATO STO: *Military Applications of Internet of Things.* 2016. Online: www.sto.nato.int/Lists/test1/activitydetails.aspx?ID=16536

Parham, Jason: Facebook and the Price of Tech Utopia. *Wired.com,* 2018. április 10. Online: www.wired.com/story/facebook-price-of-tech-utopia

Relia, Sanjeev: *Cyber Warfare: Its Implications on National Security.* New Delhi, Vij Books India Pvt Ltd., 2015.

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

Statista: *Forecast Number of Mobile 5G Subscriptions Worldwide by Region from 2019 to 2026* (2021. január). Online: www.statista.com/statistics/760275/5g-mobile-subscriptions-worldwide/

Statista: *Number of Internet of Things (IoT) Connected Devices Worldwide in 2018, 2025 and 2030* (2021. január). Online: www.statista.com/statistics/802690/worldwide-connected-devices-by-access-technology/

Sukhankin, Sergey: Russian Electronic Warfare in Ukraine: Between Real and Imaginable. *Eurasia Daily Monitor,* 71. (2017), 14. Online: https://jamestown.org/program/russian-electronic-warfare-ukraine-real-imaginable/

USNA: *Aspects and Pillars of Cyber Security* (é. n.). Online: www.usna.edu/CyberDept/sy110/calendar.php?type=class&event=2

Xu, Ke – Yi Qu – Kun Yang: A Tutorial on Internet of Things: From a Heterogeneous Network Integration Perspective. *IEEE Network,* 30. (2016), 2. 102–108. Online: https://doi.org/10.1109/MNET.2016.7437031

Zheng, Denise E. – William A. Carter: *Leveraging the Internet of Things for a More Efficient and Effective Military.* Center for Strategic & International Studies. Rowman & Littlefield, 2015. szeptember. Online: https://cdn.mashreghnews.ir/files/fa/news/1395/2/29/1638212_510.pdf

Vákát

3. fejezet

Elrettentés a kibertérben: elérhető cél vagy ábránd?

Nyáry Gábor

Bevezetés

2021 forró nyara több szempontból is megrázta a világot. Az Egyesült Államok visszahúzódása Közép-Ázsiából, megtetézve Afganisztán villámgyors összeomlásával alapvetően új helyzetet teremtett a geopolitikában. A 21. századi konnektivitás, az új selyemút fő sodorvonalában található térség politikai, hatalmi viszonyainak alakulása természetszerű hatással van a globális erőtér sorsának alakulására. Ilyenformán ez az eseménysor közvetlenül kapcsolódik a multipolárisnak nevezett új világrend formálódásához. Van azonban a drámai átalakulásnak egy másik, közvetett kapcsolódási pontja is a geopolitikai struktúrák világához. A kelet-ázsiai térség regionális erőviszonyainak átalakulása mellett az afganisztáni összeomlásnak egy másik, messzire ható következménye is érzékelhető: ez az amerikai kredibilitás drámai megrendülése. Szövetséges és rivális egyaránt arról beszél: a mód, ahogyan az USA „lezárta" a két évtizedes afganisztáni térnyerését, alapjaiban kérdőjelezi meg az ország nagyhatalmi szerepvállalásának hitelességét.

Szokatlannak tűnhet, hogy egy meglehetősen specifikus téma – a kibertér elrettentési stratégiái és gyakorlatai – tudományos vizsgálata ilyen aktuálpolitikai felütéssel kezdődjön. Az ok prózai: ez a világesemény ékesszólóan mutatja az elrettentésproblematika legfontosabb összefüggését és meghatározó kulcsmozzanatát.[1]

Mindenekelőtt fontosnak tartjuk az elrettentés problémaköre vizsgálatánál a kontextus „becsületének" visszaállítását. Ez alapvető szempont a jelenség egyes részleteinek, illetve az elrettentési téma egészének megértéséhez. Világosan látnunk

[1] Plauzibilis feltételezésnek tekinthető ráadásul az is, hogy ez az eseménysor, éppen e két jellemzője (az átfogó geopolitikai erőviszonyok módosítása, illetve az amerikai kredibilitás megtépázása révén) számottevő hatással lehet a kiberelrettentés koncepciójának alakulására. Ez érintheti az egyes nagyhatalmak kiberelrettentési stratégiáinak alakulását, illetve a terület két vezető hatalma, az USA és Oroszország között nemrégiben megindult bilaterális tárgyalásokat.

https://doi.org/10.36250/01079_03

https://orcid.org/0000-0003-4327-9550

kell: az elrettentés a kibertérben – paradox módon – nem valamiféle „kibertéma". A „kibertér" nem önmagában létező, tehát önmagában vizsgálható terület. Egy átfogó, valamennyi „hadszínteret" *(domént)* és valamennyi „fegyverrendszert" felölelő biztonságpolitikai mező egyik – bár kétségtelenül növekvő fontosságú – szelete. Ennek megfelelően a kibertér nemzetbiztonsági célú használatára és kezelésére vonatkozó koncepciók is részei egy átfogó, a nemzetbiztonság valamennyi aspektusát érintő gondolkodásnak. Nem kivétel ez alól a kiberelrettentés témaköre: a vele kapcsolatos elméletek, stratégiák, operatív politikák és alkalmazási mechanikák tekintetében egyaránt. A nemzetbiztonsági, geopolitikai kontextus tehát meghatározó a kiberelrettentés vizsgálatánál.[2]

Az elrettentés kérdéseinek tanulmányozásánál feltűnő ugyanakkor az, hogy a nemzetközi szakmai közvélemény egy jókora része erősen technikai jellegű problémaként tekint erre az ügyre. A kiberelrettentés ennek megfelelően sokszor információtechnológiai vagy éppen játékelméleti szakproblémaként tűnik fel. Természetesen a kérdés sok (egyebek mellett erősen technikai jellegű) területet is érint. Legfontosabb jellemzője azonban a „nem technikai", tehát alapvetően humán jellege. Ha úgy tetszik: a kiberelrettentés vizsgálata sokkal inkább a pszichológusok, semmint a mérnökök terepe. A téma legkiválóbb kutatói nem mulasztják el hangsúlyozni: az elrettentés (a kibertérben éppen úgy, mint a többi hagyományos és új doménben) tulajdonképpen percepciós kérdés. Kulcsa az emberi mozzanat: az, hogy emberek (akik nemzeteket képviselnek ebben a játszmában) hogyan érzékelik a világot, annak veszélyeit, lehetőségeit és szükségességeit. Az elrettentés egyik legfontosabb eleme, tényezője nem véletlenül: a hitelesség, a hihetőség, tehát a kredibilitás. A holisztikus perspektíva és a lélektani elem egybefonódva szolgálja vagy gátolja az elrettentés mechanikáját. A valamelyik másik területen hitel nélküli vagy kredibilitását vesztett ellenfél a kibertér zugaiban is csak korlátozottan érvényesítheti elrettentési szándékát.[3]

[2] Ezt a holisztikus szemléletet szeretnénk hangsúlyozni a tanulmány más pontjain is: a terminológia kérdéseinek vizsgálatakor éppen úgy, mint az intervenciós eszközcsoportok bemutatásánál. Mindenhol aláhúzva, kidomborítva azt az álláspontot, amely szerint az „elrettentésként" ismert és használt koncepció valójában a nemzetek közötti stratégiai stabilitás témakörének egy szelete csupán. A gondolat jó összegzését adja a geopolitika egyik legjelesebb kutatója. Colin S. Gray: Geopolitics and Deterrence. *Comparative Strategy,* 31. (2012), 4. 295–321.

[3] John Stone: Conventional Deterrence and the Challenge of Credibility. *Contemporary Security Policy,* 33. (2012a), 12. 108–123.

Elrettentés vagy valami más? A fogalmi keretek használhatósága

Láthatjuk, már a téma exponálásának kezdetén kerülgetnünk kell bizonyos fogalmakat. Ideje, hogy egy kicsit elidőzzünk a terminológia problémájánál. Ebben az esetben ugyanis a szó köznapi értelmében is problematikus kérdéssel találjuk szembe magunkat. A tudományos kutatás, publikálás szokványos és indokolt eljárása, hogy a munka elején rögzítjük, definiáljuk a későbbiekben használni kívánt fogalmakat és kifejezéseket. A kiberelrettentés tanulmányozása azonban már itt, az első lépéseknél nagy akadályokat gördít elénk.[4] Olyannyira, hogy – a szokásos gyakorlattól eltérően – ebben a fejezetben nem kíséreljük meg átfogó keretrendszerként leírni, pontosan definiálni a témához kapcsolódó szavakat és fogalmakat. Itt tehát csupán arra szorítkozunk, hogy felvessük, bemutassuk a kiberelrettentés problémakörének elemzésekor felvetődő terminológiai problémákat. Úgy ítéljük meg, hogy az egyes fogalmak használatos (vagy általunk javasolt, használhatónak gondolt) elnevezéseit a későbbiekben, a fejezet egyes témaköreihez kapcsolódóan jobban, plasztikusabban, indokolhatóbban tudjuk majd magyarázni.

Az „elrettentés" fogalma ugyanis a maga nemében különös: egyszerre világos, plasztikus, nagy kifejező erőt mozgósító, ráadásul közérthető és közhasználatú kifejezés.[5] Másrészt viszont erősen félrevezető a szó használata. A helyzet röviden az (ahogyan arra a későbbiekben még részletesen kitérünk), hogy szinte az elrettentés koncepciójának megjelenésétől kezdve ez a kifejezés („elrettentés")[6] vált közkeletűvé, közhasználatúvá, és ez így is maradt napjainkig. Annak ellenére történt ez így, hogy időközben – a téma elméleti kérdéseinek alapos és kiterjedt tanulmányozása, valamint a sikerrel alkalmazott gyakorlatok meghonosodása nyomán – az eredeti koncepció jelentősen kibővült.[7] A koncepció, a fogalom szintjén ugyanis arról van szó, hogy (a nemzetközi térben egymással kapcsolódó, súrlódó) államok valamilyen módon megpróbálják elérni, biztosítani, hogy riválisaik, ellenségeik ne lépjenek fel ellenük támadó módon. Kezdetben ezt a fenyegetésen alapuló

[4] Emilio Iasiello: Is Cyber Deterrence an Illusory Course of Action? *Journal of Strategic Security,* 7. (2021), 1. 55–67.

[5] Michael J. Mazarr: *Understanding Deterrence*. Santa Monica, RAND, 2018; valamint Patrick M. Morgan: *Deterrence. A Conceptual Analysis*. London, Sage Publications, 1977. A kutatás jelenlegi állásáról ad összegzést Patrick M. Morgan: The State of Deterrence in International Politics Today. *Contemporary Security Policy,* 33. (2012), 12. 85–107.

[6] Angolul *deterrence*.

[7] Stephen L. Quackenbush: *Understanding General Deterrence Theory and Application*. New York, Palgrave Macmillan, 2011.

„elrettentés" kívánta szolgálni: ennek keretében azt tudatosították ellenfelükben, hogy az esetleges agresszív, támadó lépések válaszlépést, megtorlást fognak kiváltani.[8] Az idők folyamán azonban kialakult egy másik mechanizmus is, amelynek lényege, hogy az ellenfélben azt tudatosítják, hogy nem érdemes agresszíven, támadóan fellépni, mert az akció úgysem lesz sikeres (a megelőző lépéseinknek hála). Ezt az intézkedési pillért a szakma – talán a bevált elnevezéshez ragaszkodva – szintén „elrettentésnek" kezdte nevezni, és az elrettentés két módozataként említette a két különböző eszköz alkalmazását.[9] Valójában azonban nagyon eltérő intervenciós eszközökről van itt szó, ahol nemcsak a technika, hanem az egész mögöttes lélektani háttér is drámaian különböző. Ezt a megközelítést célszerűbb volna „eltántorításnak"[10] nevezni, hangsúlyozva, hogy itt nem a fenyegetés a meghatározó mozzanat a célok elérésére. A szakirodalom ezt a két módozatot említi többnyire az „elrettentés" szokványos megközelítésmódjaként. A hidegháború időszakában azonban kialakult még egy további koncepcionális lehetőség az ellenfél támadó fellépésének megelőzésére. E mögött igen fontos elméleti-tudományos felismerés áll, amely aztán még ennél is nagyobb horderejű politikai alapelvben öltött formát. A tétel lényege: a támadó sokszor azért támad, mert úgy érzi, hogy nem maradt számára más lehetőség érdekei képviseletére vagy védelmére. Ebből következően a támadó, ellenséges magatartás meggátolására nemcsak a megtorlással való fenyegetés vagy az akció kilátástalanságának bizonygatása szolgálhat, hanem az: meggyőzni az ellenfelet, hogy szükségtelen, indokolatlan az agresszív fellépése. Ezt a megoldást talán az „okafogyottság bizonyításának" lehetne nevezni.

Jól látható tehát, hogy valójában az „elrettentés" kifejezés használatakor ma már egy jóval átfogóbb koncepcióra gondolunk: amiről itt valójában szó van, az a „stratégiai stabilitás keresése". Az egyes (egymással szemben álló) államok[11]

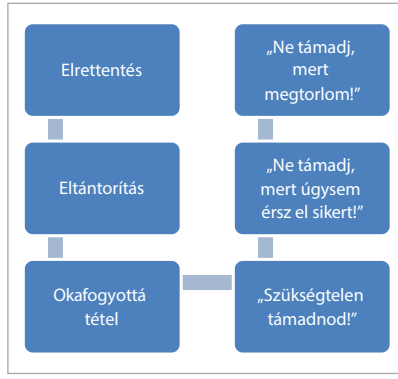
[8] Aihito Yamashita: Glenn Snyder's Deterrence Theory and NATO's Deterrence Strategy during the Cold War. *Air Power Studies,* 6. (2020). 69–116.; valamint Satoshi Yamamoto: On Thomas Schelling's Deterrence Theory. *Air Power Studies,* 6. (2020). 117–144.

[9] Martin C. Libicki: *Cyberdeterrence and Cyberwar.* Santa Monica, RAND Air Force Project, 2009; valamint Martin C. Libicki: Expectations of Cyber Deterrence. *Strategic Studies Quarterly,* 12. (2018), 4.

[10] Az angol szakmai nyelv az utóbbi időben lassan elkezdte erre az intézkedéscsoportra a *dissuasion* kifejezést használni a korábban általános *deterrence* helyett.

[11] Itt szeretnénk megjegyezni: a szakirodalomban és a szakmai gondolkodásban az elrettentés, így tehát a kiberelrettentés is alapvetően az államközi kapcsolatok jelenségeként tűnik fel. Ahol tehát egy szuverén állam próbálja meg stratégiai stabilitását biztosítani egy másik szuverén állami szereplővel kapcsolatban. A valóságban azonban az elrettentés problémája – különösen a kibertér világában – egyre gyakrabban merül fel nem állami szereplőkkel összefüggésben is. A 2021-es

ezt a stabilitást különböző megközelítésmódok alkalmazásával kísérelhetik meg biztosítani. A stratégiai stabilitást garantálni hivatott három alapvető mechanizmus demonstratív ábráját az *1. ábrán* látható formában lehet megrajzolni (ne feledjük, hogy ezt a három módszert, megközelítést osztatlanul „elrettentésnek" nevezi a szakirodalom túlnyomó része):



1. ábra: Törekvések a stratégiai stabilitás biztosítására
Forrás: a szerző szerkesztése

A hatalmi politika furcsa paradoxona: miközben a szakemberek egyöntetű meggyőződése az, hogy a fenyegetés, a tulajdonképpeni „elrettentés" a stratégiai stabilitás biztosításának legkevésbé sikeres módszere (és az esetleges támadás sikertelenségét garantáló megközelítés, de főleg a támadó fellépést eleve megelőző perspektíva a legeredményesebb), mégis ez a legelterjedtebb megközelítés a kibertérben is.[12]

év nagy „újdonsága", hogy kiberbűnözői csoportok akciói immár nemzetbiztonsági fenyegetést jelentenek szuverén államok számára. A kiberelrettentés lehetőségeit ezért egyre gyakrabban fogják a nem szuverén államok közötti, de nemzetközi kapcsolatrendszer kontextusában vizsgálni.

[12] Azzal a megjegyzéssel, hogy ezen a téren bizonyos lassú elmozdulás jelei éppen mostanában érzékelhetőek, elsősorban a meghatározó szereplőnek tekinthető USA vonatkozásában, ahogy arra a későbbiekben még utalni fogunk.

Emlékek a múltból: a hidegháború és a nukleáris elrettentés

Az „elrettentés”,[13] annak mindhárom fentebb bemutatott módozata valószínűleg ősi, és bizonyára egyidős az egymás mellett élésre kényszerülő emberi közösségekkel (a „közösségközi” konfliktusokkal, háborúkkal).[14] Jelen témánk szempontjából ezért a múlt tapasztalatainak feltérképezését arra a korszakra érdemes korlátozni, amelyben az elrettentés kérdéskörének tudományos igényű vizsgálata és leírása megkezdődött, majd szárba szökkent. Ez a tudomány- és politikatörténeti kutatóút a hidegháború időszakába vezet minket vissza.[15]

Az elrettentéssel kapcsolatos kérdések vizsgálatában, az ahhoz kapcsolódó elméletek alapjainak kidolgozásában az amerikai tudományos élet tagjai játszottak kiemelkedő szerepet, különösen Thomas Schelling, akinek a munkássága korszakalkotónak bizonyult ezen a területen.[16] A közgazdász végzettségű Schelling, aki tudományos pályafutása mellett számos meghatározó kormánytanácsadói posztot is betöltött, a hidegháborús konfrontáció csúcspontján, 1960-ban publikálta első, meghatározó írását a „konfliktusviselkedés” témakörében.[17] Ez a munka (amelyet később a 20. század második fele egyik legbefolyásosabb tudományos alkotásaként aposztrofáltak) a „stratégiai viselkedés” és az államok közötti alkufolyamatok kérdéskörét vizsgálta. A könyvben lényegében lefektette az elrettentés elméleti vizsgálatának számos fogalmi alapját. Néhány évre rá, eredeti gondolatait továbbfejlesztve, újabb korszakos írásban fejtette ki immár az elrettentés elvi lehetőségeinek szinte minden fontos elemét.[18] Munkásságának (amelyet a kor olyan drámai válsághelyzeteihez kapcsolódó kormányzati döntésekre alapozva fogalmazott meg, mint a berlini válság vagy a kubai atomrakéta-krízis) legfontosabb mondandója

[13] Noha már látjuk, hogy az „elrettentés” kifejezés helyett indokoltabb volna más, inkluzívabb terminust (mint amilyen például a stratégiai stabilitás keresése) alkalmazni. Ugyanakkor az „elrettentés” kifejezés az elmúlt fél évszázad szakmai és politikai szóhasználatában annyira meggyökeresedett, hogy a helyesebb kifejezésre váltás súlyos konfúzióhoz vezethetne. Ezért a szövegben mi is szinonimaként használjuk majd e szót.

[14] Robert P. Haffa Jr.: The Future of Conventional Deterrence: Strategies for Great Power Competition. *Strategic Studies Quarterly,* 12. (2018), 4. 94–115.

[15] Temi Davis Biddle: Coercion Theory: A Basic Introduction for Practitioners. *Texas National Security Review,* 3. (2020), 2. 94–109.

[16] Robert Ayson: *Thomas Schelling and the Nuclear Age. Strategy as Social Science*. London, Frank Cass, 2004.

[17] Thomas C. Schelling: *The Strategy of Conflict*. Cambridge, Harvard University, 1960.

[18] Thomas C. Schelling: *Arms and Influence: with a New Preface and Afterword*. New Haven, Yale University Press, 1966.

az volt, hogy a katonai erőnek, a primér erőszakos alkalmazásán túl, az államok közötti alkufolyamatokban is fontos szerep juthat az erőegyensúly-állapotok kialakításában és garantálásában.

Schelling és a nyomában járó amerikai társadalomtudós-nemzedék fogalmazta meg az államok közötti nyílt összecsapások megelőzésére, megakadályozására szolgáló elrettentési stratégiák számos nélkülözhetetlen elemét, illetve kellékét.

Ekkor jelenik meg a tudományos közgondolkodásban az elrettentés két lehetséges megközelítése (a tulajdonképpeni elrettentés, a *deterrence,* és a megakadályozás, amelyet ekkor a *denial* kifejezéssel illetnek), azok specifikumaival, sajátos feltételeivel és mechanizmusaival.[19] Érdemes megjegyezni: a kor viszonyai természetesen alapvetően befolyásolták a tudományos közgondolkodást, ami az elrettentéssel foglalkozó szakemberek esetében is jól érzékelhető. A 20. század közepe a roppant pusztító erejű nukleáris arzenálok kiépülésének kora, így érthető módon az offenzív megközelítések domináltak mindkét nagyhatalom stratégiai elképzeléseiben. Ennek megfelelően ebben az időben a megtorlással való fenyegetésre épülő elrettentés koncepciója, illetve stratégiája vitte a prímet.[20]

William Kaufmann érdeme volt annak a felismerése, hogy a sikeres elrettentés csak olyan stratégia köré épülhet, amely egyszerre tartalmazza az ellenfél elleni csapáshoz szükséges kapacitásokat és az erőszakos (válasz-) csapással kapcsolatos szándékot (eltökéltséget).[21] A felismerés lényege ugyanis az volt, hogy az elrettentés működéséhez elengedhetetlen, hogy a szemben álló felet meggyőzzük arról, hogy tartózkodjon az agresszív fellépéstől.[22] Thomas Schelling ezt azzal a fontos kitétellel fejelte meg, hogy a sikeres elrettentésnek lényeges eleme továbbá az is, hogy egy ellenséges fellépés nyomán alkalmazott megtorlás következményeit, illetve a válaszlépésre való elszántságot világosan kommunikálni kell a potenciális agresszor felé. A téma klasszikusai (különösen Schelling) már bő fél évszázada világosan megfogalmazták tehát a jó (hatásos, eredményes) elrettentési stratégia

[19] A tulajdonképpeni elnevezés ekkor még *deterrence by punishment,* azaz a megtorlás fenyegetésével való elrettentés, illetve a *deterrence by denial,* azaz a megakadályozás kilátásba helyezésével való elrettentés. Az egyik első klasszikusnál: Glenn H. Snyder: Deterrence and power. *The Journal of Conflict Resolution,* 4. (1960), 2. 163–178.

[20] Alexander L. George – Richard Smoke: *Deterrence in American Foreign Policy: Theory and Practice.* New York, Columbia University Press, 1974.

[21] William Kauffman: The Requirements of Deterrence. In P. Bobbitt et al. (szerk.): *US Nuclear Strategy.* London, Palgrave Macmillan, 1989.

[22] Krista Langeland – Derek Grossman: *Tailoring Deterrence for China in Space*. Santa Monica, RAND, 2021.

lényegét – ami azonban a mai napig gyakran elkerüli a témával foglalkozók figyelmét. A jó elrettentési stratégia tulajdonképpen nem „elrettenti" (a várható súlyos megtorlással) vagy „eltántorítja" (az akció megakadályozásával) az ellenfelet. Hanem elhiteti az ellenféllel, hogy képesek vagyunk a megtorlásra vagy a cselekvés megakadályozására – és azt meg is fogjuk tenni.[23]

Érdemes röviden megjegyezni: a hidegháború időszakában, amely egyben az atomfegyverkezés hajnala is volt, szinte kezdettől nyilvánvalóvá vált, hogy az elrettentés stratégiái és mechanizmusai máshogy működhetnek a hagyományos fegyverekkel, illetve az atomképességekkel kapcsolatosan.[24] Első pillantásra a nukleáris fegyverzet ideális elrettentő „fedezetnek" tűnhetett; valójában, éppen a totális pusztítást hozó jellege miatt, kevéssé volt alkalmas (ugyanis nem számított hihető fenyegetésnek) a megtorlásra épülő elrettentés eszközeként.[25] A hagyományos fegyverzet, amely nagy erejű, ám mégis korlátozott pusztítást garantált, sokkal hatékonyabbnak bizonyult a válaszcsapással fenyegető megelőzés szempontjából.

Üzenet a jövőből: elrettentés a világűrben

A kiberelrettentés kérdéseinek vizsgálatánál érdekes támpontokat, gondolati pilléreket biztosíthat egy másik *domén,* a világűr speciális elrettentési tematikája.[26] A világűr – hasonlóan a föld, víz, levegő térhármasához – szintén természetes közeg, ellentétben az egyértelműen ember alkotta kibertér világával. Ugyanakkor az űr jelentősen eltérő sajátosságokat mutat, és ilyenformán hasznos analógiákat kínálhat a kiberelrettentés szempontjainak tanulmányozásához.[27]

[23] Langeland–Grossman (2021): i. m.

[24] James J. Wirtz: How Does Nuclear Deterrence Differ from Conventional Deterrence? *Strategic Studies Quarterly,* 12. (2018), 4. 58–75.

[25] Joseph S. Nye Jr.: Nuclear Lessons for Cyber Security? *Strategic Studies Quarterly,* 5. (2011), 4. 18–38.

[26] Noha a világűr mint a jelentős hatalmak közötti békés (és kevésbé ártatlan) vetélkedés színtere legalább 1957 óta jelen van a globális konfliktusmezők rendszerében, és a 20. század hidegháborús évtizedeinek zömében kiélezett „űrverseny" zajlott a Szovjetunió és az USA között, az elrettentés problematikája szempontjából csupán mostanában nő meg a jelentősége. A világűrbeli elrettentés elméleti alapozása ezért csaknem párhuzamosan folyik a kiberelrettentés teóriáinak kimunkálásával.

[27] Az egyik legelgondolkodtatóbb munka a témáról: Bleddyn E. Bowen: From the Sea to Outer Space: The Command of Space as the Foundation of Spacepower Theory. *Journal of Strategic*

Az első fontos megállapítás a világűr nemzetbiztonsági jelentőségére vonatkozik.[28] Kétség sem fér hozzá, hogy az elmúlt évtizedek fejlesztései nyomán az űr olyan rendszerek telepítési és működési területévé változott, amelyek ma már nélkülözhetetlenek a modern társadalmak működéséhez. A műholdas helymeghatározó rendszerektől a banki adatforgalmat bonyolító adatátviteli hálózatokig a modern társadalmak szinte minden artériája a világűrön fut keresztül. Az ott telepített rendszerek minden szempontból kritikus infrastruktúrát jelentenek.[29]

Az egyik legfontosabb megfigyelés, elméleti alapvetés az űrelrettentés átfogó jellegére vonatkozik.[30] Valójában nem is maga a konfrontáció színteréül szolgáló *domén* a lényeg, hanem a célpont jellege. Itt nem a fegyver az elsődleges, hanem a célpont milyensége. Egyszerű, de plasztikus és érvényes analógiával élve: a kibervilágban egy nagy adatközpont elleni robbantásos (tehát nem kibernetikai, hanem abszolút hagyományos „kinetikus") támadás éppen olyan drámai hatásokkal járhat, mint ha egy zsaroló vírusos támadás blokkolja az adatbázisokhoz való hozzáférést. Ez a nézőpont persze már eleve jelzi a célpontok milyenségéből eredő különbségtétel fontosságát: ahogy egészen más fenyegetést jelent egy Planet Lab kereskedelmi fényképező műhold blokkolása békeidőben, mint egy amerikai Keyhole nemzeti felderítő műhold megbénítása válságidőszakban, éppen annyira különbözik a felhasználók véletlenszerű csoportjai elleni primitív zsaroló vírusos támadás egy nagy energiaelosztó cég szervereinek megbénításától.

Az űrelrettentés érdekes sajátossága – megint egy használható analógia – az, hogy olyan (állami és nem állami) aktorok is támadhatnak űreszközöket, amelyek maguk nem rendelkeznek hasonló képességekkel. A válaszcsapás, illetve az azzal való fenyegetés tehát nem lehet szimmetrikus.[31] Ez világosan mutatja, hogy a korszerű (űr-, illetve kiber-) elrettentés mindenképpen több doménre kiterjedő megtorlással fenyegetve hatásos.[32]

A nukleáris hadviseléshez (válaszcsapáshoz) kapcsolódó űrrendszerek sérülékenysége különleges jelentőségű, a hozzájuk kötődő elrettentési stratégiának ezt

Studies, 42. (2019), 3–4. 532–556.

[28] Forrest E. Morgan: *Deterrence and First-Strike Stability in Space. A Preliminary Assessment*. Santa Monica, RAND Air Force Project, 2010.

[29] Dean Cheng – John Klein: A Comprehensive Approach to Space Deterrence. *The Strategy Bridge,* 2021. március 31.

[30] Langeland–Grossman (2021): i. m.

[31] Bleddyn E. Bowen: The Art of Space Deterrence. *European Leadership Network,* 2018. február 20.

[32] James P. Finch: Finding Space in Deterrence: Toward a General Framework for „Space Deterrence". *Strategic Studies Quarterly,* 5. (2011), 4. 10–17.

figyelembe kell vennie.[33] Újfent egy hasznos, elgondolkodtató analógia a kibertér viszonyaira vetítve.

Az űreszközök (műholdak) egy része, támadás esetén, érzékeny, de nem életbe vágó fontosságú veszteséget jelenthet civil használók tömegeinek. Ilyen esetekben viszonylag gyenge a fenyegetéshez kapcsolódó érzelmi és politikai töltés, ami a kapcsolódó elrettentés eredményességét csökkentheti.[34]

Bizonyos űrtámadások (az általuk okozott kiterjedt létfenyegetés miatt) olyan erősen eszkalatórikus jellegűek (hasonlóan a nukleáris arzenálokhoz), hogy az kétségessé teszi azok alkalmazhatóságát, s így a hozzájuk kapcsolható elrettentő potenciál is viszonylag csekély.[35]

A kibertér sajátos világa

A földrajzi tér alapvető kiterjedései, a szárazföldek és a vizek ősidőktől az államok közötti érdekérvényesítési küzdelmek állandó színterei. Melléjük a 20. század első harmadától felzárkózott a levegő, majd a hidegháború korszakában az űr dimenziója is. A 21. század újdonságaként ez a sokrétű geopolitikai világ újabb versengési területtel bővült ki. A formálódó kibertér lett a geopolitikai szembenállás, érdekérvényesítés ötödik dimenziója.[36] Az informatika, a számítógépes hálózatok, a mobiltechnológiák rohamos fejlődése szülte ezt az új „érdekmezőt", ebben az értelemben tehát tényleg ízig-vérig korunk terméke. Mint annyi fogalom, a „kibertér" is sok értelmezést, értelmezési árnyalatot takar.[37]

[33] Steve Lambakis: A Guide for Thinking About Space Deterrence and China. *Comparative Strategy,* 38. (2019), 6. 497–553.

[34] Michael Krepon – Julia Thompson (szerk.): *Anti-Satellite Weapons, Deterrence and Sino-American Space Relations.* Washington, Stimson, 2013.

[35] A világűrbeli elrettentés különösen érdekes körülményeként szokták említeni az óriási mennyiségben keletkező űrtörmelék szempontját. Az elmélet úgy szól, hogy az ellenfél űreszközének kinetikus (tehát nem informatikai, kibernetikai) megsemmisítése, az ennek eredményeként keletkező törmeléktömeg révén, a támadó fél rendszereire is óriási fenyegetést jelentene. Következésképpen ez erős visszatartó erővel bír (illetve jelentősen csökkenti az űrellencsapással való fenyegetés elrettentő erejét).

[36] A kibertér geopolitikai jellegének egyik első megfogalmazását Szilágyi István: *A geopolitika elmélete* című kiváló munkája adja (Budapest, Pallas Athéné, 2018).

[37] A kibertér sajátosságaihoz áttekintést ad Nyáry Gábor: Kiberdiplomácia: hatalom, politika és technológia a geopolitika ötödik dimenziójában. In Török Bernát (szerk.): *Információ- és kiber-*

A kifejezés nem új keletű: egy William Gibson nevű íróhoz kötődik, aki 1982-ben kiadott novellájában használta első ízben ezt a fordulatot, egy számítógép által kreált virtuális valóságmező bemutatására. Ma már az internet egész világot körbefonó, számítógépes hálózatainak szinonimájaként használatos. A kibertér „térbeli" mivoltával kapcsolatban a szakirodalom nem egységes. Egyes szerzők, különösen a kiberhadviselés problematikájával foglalkozó stratégiatudományi szakértők a sokdimenziós geopolitikai közeg fokozatos virtualizálódásáról beszélnek. E szerint a hagyományos tereket a csupán átvitt értelemben létező, konkrét alakot nélkülöző tér, egyfajta „térnélküliség" váltja a geopolitika összefüggésrendszerében.[38]

Másfelől viszont a kiberkomplexum technológiai aspektusaival vagy a digitalizáció társadalmi összefüggéseivel foglalkozó kutatóknál hangsúlyosan merül fel a kibertér térjellege, azaz nagyon is valóságos, fizikai térstruktúrákhoz integránsan kapcsolódó mivolta. Ebben a felfogásban a kibertérfogalom térbelisége különböző szinteken jelenik meg. A fogalomnak elsőként is van egy technikai jelentésszintje, amely a kibertérnek nevezett fogalom együttes technológiai infrastruktúráját írja le. A fogalomnak van ugyanakkor egy tényleges földrajzi jelentésrétege is, amely az IKT-hálózatokat és azok csomópontjainak valóságos térbeni kiterjedését öleli fel. Ugyanakkor tartalmaz egy harmadik, társadalmi jelentésréteget is, amely az IKT-hálózatokat használó emberek térbeli szerveződéseit írja körül. A kibertér, ez a sokszor virtuálisnak nevezett világ tehát nagyon is valóságos térbeliséggel rendelkezik.

Komplex jellege magyarázza, hogy a kibertér miért számít speciális közegnek az elrettentés stratégiái szempontjából is. A teljesség igénye nélkül érdemes emlékeztetni néhány fontos specifikumra. A legfontosabb talán az, hogy a kibertér technológiai komponensei alapvetően kettős rendeltetésű elemekre épülnek. A polgári alkalmazást sokszor lehetetlen megkülönböztetni a támadó célú eszközöktől. Lényeges jellegzetesség az is, hogy a kibertérben folyó rosszindulatú műveletek olyan széles spektrum mentén zajlanak, amelyek sokszor nem érik el a „harci cselekménynek" minősülő konfliktusok határát. Emellett nehéz a támadó cselekmények észlelése, felderítése, ami értelemszerűen visszahat az elrettentés eredményességére is. A kibertérben mozgó ellenfelek igyekeznek az online terek

biztonság. Fenntartható biztonság és társadalmi környezet tanulmányok V. Budapest, Ludovika Egyetemi Kiadó, 2020. 321–343.

[38] Szilágyi István: *A geopolitika elmélete*. Budapest, Pallas Athéné, 2018.

sötétjében meghúzódni, ezért a próbálkozások, behatolások észlelése nem könnyű feladat.

A kibervilág legfontosabb sajátossága kétségtelenül az attribúció nehézsége.[39] A tettes egyértelmű azonosítása olyan vizsgálati folyamat, amelynek során kiberbiztonsági szakemberek bizonyító erejű információkat gyűjtenek, eseményidőrendeket állítanak össze, és mindezekből fáradságos munkával összerakják a hálózatot vagy gépet ért támadást. A tevékenység célja az, hogy bizonyítható módon megállapítsa, hogy ki volt egy-egy kiberakció végrehajtója, illetve ki lehet az, aki egy támadó akcióért a tényleges felelősséget viseli.[40]

Sokan állítják: az attribúció egyáltalán nem lehetetlen. Mindig sok olyan nyom marad egy-egy támadó akció után, amelyből aprólékos munkával összeállítható az elkövető képe. Ennek azonban ellentmondani látszik, hogy a szinte korlátlan erőforrásokkal és hatalmas tudáskapacitásokkal rendelkező hatalmak is csupán a legritkább esetben prezentálnak evidenciát egy-egy támadás feltételezett elkövetőjének megnevezésekor. Az attribúciók az esetek túlnyomó részében számos hipotetikus elemet tartalmaznak, illetve a bizonyító anyag ereje nézőpont kérdése, tehát jogilag korántsem egyértelmű.

Mechanizmusok és modellek

A kiberelrettentés lehetséges modelljének kialakításához, a digitális doménben is működőképes elrettentési stratégia bemutatásához érdemes egy pillantást vetni a hagyományos konfliktustér elrettentési mechanizmusára.

Az elrettentés elmélete és működése a hidegháború időszakában

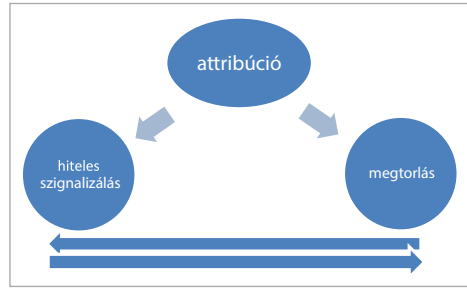
A téma egyik elismert kutatója, Mariarosariaria Taddeo sematikus összefoglalója ma már klasszikusnak számít az irodalomban.[41] Ebben – tehát a hagyományos

[39] Clara Assumpção: The Problem of Cyber Attribution Between States. *E-International Relations,* 2020. május 6. Átfogóan vizsgálja a problémát Will Goodman: Cyber Deterrence. Thougher in Theory than in Practice? *Strategic Studies Quarterly,* 4 (2010), 3. 102–135.

[40] Nicholas Tsagourias – Michael Farrell: Cyber Attribution: Technical and Legal Approaches and Challenges. *European Journal of International Law,* 31. (2020), 3. 1–27.

[41] Mariarosariaria Taddeo: *How to Deter in Cyberspace*. Strategic Analysis. Helsinki, Hybrid CoE, 2018b.

elrettentés viszonyrendszerében – kulcsszerepet kap az attribúció. Ez (legyen szó hagyományos vagy nukleáris fegyverzetről) nagyobb nehézségek nélkül érvényesíthető. Ezzel szemben – mint feljebb láttuk – a kibertér viszonyai között az attribúció roppant problematikus, és a hatékony elrettentés legfőbb akadálya.[42]



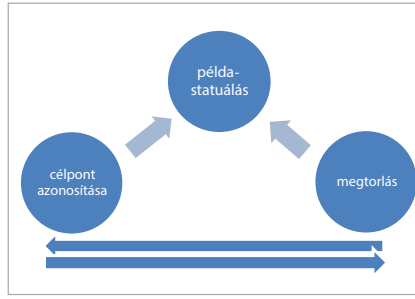
2. ábra: A hagyományos elrettentésmodell
Forrás: Taddeo (2018a): i. m.

Az ábra egyértelműen mutatja azt is: a szignalizáció (a képességek és az elszántság kommunikálása) az elrettentés másik fontos eleme. Taddeo azonban úgy véli, hogy a kibertér viszonyai között ez a létfontosságú jelzés is csupán tökéletlenül működhet. Egyszerűen azért, mert egy-egy állam „kiberreputációja" nem feltétlenül esik egybe tényleges kiberkapacitásaival (és ez utóbbit, mint az előző fejezetben utaltunk rá, gyakorta tartják az érdekelt felek homályban). A modell harmadik fontos összetevője, a megtorlás mind a hagyományos, mind pedig a kibertérségben jól működhet. A kiberdoménben azonban a megtorlás (tehát a kibertérben történő támadáshoz hasonlóan ugyanezen doménben történő válaszcsapás) rendkívüli kockázatokat rejt, a könnyű eszkalálódás lehetősége folytán.[43]

[42] Richard J. Harknett: Leaving Deterrence Behind: War-Fighting and National Cybersecurity. *Journal of Homeland Security and Emergency Management,* 7. (2010), 1. 1–24. Fontos elméleti alapvetést hoz továbbá Mariarosaria Taddeo: Deterrence and Norms to Foster Stability in Cyberspace. *Philosophy and Technology,* 31. (2018a), 4. 323–329.
[43] Alexander A. Ghionis: *The Limits of Deterrence in the Cyber World. An Analysis of Deterrence by Punishment*. Brighton, University of Sussex, (é. n.).

A kiberelrettentés lehetséges modellje

Taddeo hangsúlyozza: a kiberelrettentés koncepciójának kialakításánál fontos, hogy ne engedjünk a hagyományos elrettentésmodellek hamis analógiájának. A kibertér sajátosságai döntően befolyásolják a használható elrettentési stratégiát. Fontos emlékeznünk rá: a kibertér az állandó támadás terepe. A támadás taktikai és stratégiai értelemben egyaránt előnyösebb, mint a védekezés.[44]



3. ábra: A kiberelrettentés modellje
Forrás: Taddeo (2018a): i. m.

A kibertér sajátos viszonyaihoz alkalmazkodó, speciális elrettentési elmélet és stratégia kialakításánál Taddeo szokatlan és merész fordulattal azt javasolja: az attribúciót (a támadó hiteles megállapítását) ki kell hagyni az egyenletből. Helyette egy plauzibilis „célpont" azonosítására kell koncentrálni, amelyre a másik fő komponens, az ellencsapás (megtorlás) irányulhat. Így valósulhat meg az elrettentő erő demonstrálása.[45]

Az elmélet szerint, ha az azonosított (bár nem bizonyított) célpontra ellencsapást mérünk, akkor az eredeti támadó művelet így előidézett megszakítása jelenti majd a „bizonyítékot".[46] Ez a megközelítés azonban nem csupán roppant

[44] Taddeo (2018a): i. m. Ez a szemléletmód tükröződik abban a váltásban is, amely az USA kiberbiztonsági koncepcióját jellemzi. A klasszikus (passzív) védekezés egyre inkább átadja a helyét az (aktív) „előretolt védelem" szisztémájának.

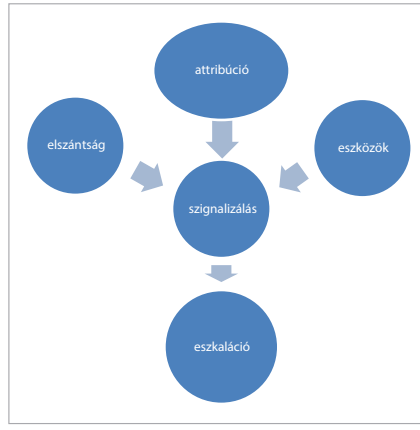
[45] További részleteket hoz Mariarosaria Taddeo: The Limits of Deterrence Theory in Cyberspace. *Philosophy and Technology,* 31. (2018c), 4. 323–329.

[46] Taddeo kétségtelenül szokatlan felvetése arra az állításra alapul, hogy manapság a támadó (akár a folyamatokat automatizáló gépi tanuló rendszerek segítségével) viszonylag jó hatékonysággal

kockázatos, de ráadásul tulajdonképpeni elrettentésre sem alkalmas. Legfeljebb csak egy „majdani" második támadás megelőzésére bizonyulhat használhatónak.

Az összefüggések jobb megértése felé

A fenti javaslat egyelőre csupán gondolatkísérletnek tekinthető, és mindenképpen érdemes mérlegre tenni egy ilyen megközelítés veszélyeit és sok szempontból beláthatatlan (nemzetközi jogi, etikai és természetesen politikai) következményeit.[47] Célszerű ugyanakkor egy sémában bemutatni a kibertérben megvalósítható (megtorlásra épülő, tehát „valódi") elrettentés fontos elemeit és azok összefüggésrendszerét.



4. ábra: Az elrettentés összefüggései a kibertérben
Forrás: a szerző szerkesztése

Az általunk vázolt modell a jelenleg alkalmazott rendszert demonstrálja. Egyértelmű szakmai igény mutatkozik arra, hogy az elrettentés rendszerét az egyes elemek hatékonyságának a növelésével dinamizálják.[48] Az egyik fő irány

azonosítható, „csupán" ennek bizonyítása ütközik nehézségbe. Érdemes azonban megfontolni: ez a „csupán" szócska az a hajszál, amely a jogállami normák érvényesüléséhez köt minket.

[47] Taddeo (2018b): i. m.

[48] Joseph Nye Jr.: Deterrence and Dissuasion in Cyberspace. *International Security,* 41. (2016–17), 3. 44–71. Összehasonlításként érdemes áttekinteni: Rod Thornton – Marina Miron: Deterring Rus-

nyilvánvalóan az attribúcióval kapcsolatos vizsgálati rendszer tökéletesítése (nem kis részben a mesterségesintelligencia-alapú technológiákra támaszkodva).[49] De nem ez a dolog kulcsa. Az általunk kiegészített modell – visszanyúlva az elrettentéselmélet klasszikusainak megállapításaihoz – azt kívánja demonstrálni, hogy az elrettentés, ahogy régebbi korokban és doménekben, úgy a mostani kibervalóságban sem technikai kérdés. Ennek megfelelően – hiszen valójában döntően percepciós kérdésről van szó – az igazi kulcs a szignalizáció hatékonyságának növelése lehet: a rendelkezésre álló erőforrások (hiteles) bemutatása, és az azok alkalmazására való készség demonstrálása.[50] A felrajzolt séma ugyanakkor rámutat az esetleges nem kívánatos kimenetelekre, a folyamatban rejlő inherens veszélyekre is. A kibertér sajátosságai ugyanis mindenképpen megnövelik a gyors és könnyű eszkalálódás veszélyét.[51]

Útkeresések, megoldási irányok

A kiberelrettentés hatékony stratégiájának kialakításánál érdemes visszakanyarodni ahhoz a kezdő gondolathoz, miszerint a tulajdonképpeni elrettentés csupán egy elem az államok stratégiai stabilitását biztosítani hivatott mechanizmusok között. Talán nem is a legfontosabb. Korábban rámutattunk: a hidegháború idején ténylegesen az offenzív fellépés, a fenyegetésre alapozott elrettentés volt a stabilitás vágyott kulcsa. Ugyanakkor abban is egyetértenek a szakértők, hogy ez a fenyegetés mindig is a legkevésbé hatékony biztonságteremtő eszköznek számított.[52] Célszerű lehet tehát, ha a stabilitás biztosítására hivatott eszközrendszeren belül a másik kettőre kerülne a hangsúly: a támadást értelmetlenné tevő, illetve a táma-

sian Cyber Warfare: The Practical, Legal and Ethical Constraints Faced by the United Kingdom. *Journal of Cyber Policy,* 4. (2019), 2. 257–274.

[49] Tim Stevens: A Cyberwar of Ideas? Deterrence and Norms in Cyberspace. *Contemporary Security Policy,* 33. (2012), 12. 148–170.

[50] Sico van der Meer: *Signalling as a Foreign Policy Instrument to Deter Cyber Agression by State Actors.* Hague, Clingendael, 2015.

[51] Jun Osawa: The Escalation of State Sponsored Cyberattacks and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem? *Asia-Pacific Review,* 24. (2017), 2. 113–131.

[52] Ehhez ad érdekes kiegészítést Eric Sterner: Retaliatory Deterrence in Cyberspace. *Strategic Studies Quarterly,* 5. (2011), 1. 62–80. A vezető kibernagyhatalom, az USA stratégiájába illesztve vizsgálja ugyanakkor ezt a kérdést Michael E. O'Hanlon: Deterrence. US Grand Strategy and the Wisdom of Bob Gates. *The Brookings Institution,* 2021. június 7.

dást feleslegessé tevő intézkedések erősítésére. Már csak azért is, mivel az elmúlt évtizedben mindkét területen fontos lépések történtek.

Felderítés, verifikálás: „nyitott kiberégbolt"

Mielőtt az agressziót értelmetlenné, illetve feleslegessé tevő megoldásokról ejtenénk szót, érdemes még egy pillanatra elidőzni egy olyan témánál, amely elsődlegesen a (fenyegetésen alapuló) elrettentés összefüggésében játszhat szerepet, ugyanakkor a stabilitás erősítését célzó teljes ökoszisztéma profitálhat az eredményeiből. A felderítés, az ellenfelek kölcsönös (intézményi keretek közt folyó) monitorozása, tehát az ellenfél kapacitásainak és szándékainak verifikálása minden stabilitást szolgáló intézkedéscsomagban kulcselemként jelenik meg. A helyzet egyik nagy paradoxona, hogy miközben a kiterjedt ellenséges kiberfelderítési akciók jelentik ma a globális hatalmak közötti feszültségek egyik forrását, a kibertér zavartalan működését biztosítani hivatott kiegyezések (kiberfegyverszünetek, kiberfegyverzet-korlátozási megállapodások) egyik sarokköve, megvalósításának záloga éppen a kölcsönös „felderítés" erősítése lehet. A hidegháború nukleáris krízishelyzeteit vizsgáló tanulmányok sora világított rá: a (kölcsönös) hírszerzés, természetesen bizonyos szabályozott keretek között, éppen a bizalmatlanság, egzisztenciális fenyegetettségérzet eloszlatásában játszott meghatározó szerepet. Később, az enyhülés szakaszában az úgynevezett „nyitott égbolt" megállapodással intézményesült ez a lehetőség. A nagyhatalmak közötti kibertér-megállapodások, bilaterális kezdeményezések egyik eleme lehet egy ehhez hasonló konstrukció kiépítése, amely az elrettentés többi mechanikája esetében is erősítheti a hatékonyságot.

Reziliencia

A stratégiai stabilitást biztosítani hivatott mechanizmusok között a második blokk, az „eltántorítás" konkrét eszközrendszere különböző elemeket ölel fel. Mindegyik arra szolgál, hogy megüzenje a potenciális agresszornak: nem érdemes támadnia, mert úgysem jár sikerrel. Idő- és ráfordításigényes védekezési mód, ám a kutatók egy része szerint messze eredményesebb a reziliencia növelése, mint a fenyege-

tések rendszere.[53] A reziliencia, az ellenálló képesség erősítése maga is többfajta intézkedést ölelhet fel: a rendszerek redundanciáinak fokozása (például a sebesen elharapódzó zsaroló vírusos támadások célpontjául szolgáló adatkészletek duplikálása) mellett az informatikai rendszereket és eszközöket használók biztonsági képzettségének növelésén át az egyszerű kiberhigiénés szabályok rutinszerű intézményesítéséig.

A SolarWinds-támadás mély nyomokat hagyott a kiberbiztonsági szakértőkben. Terjed az a koncepció, hogy alapvetően új védekezési eljárásokat és taktikát kell kidolgozni, mert bebizonyosodott, hogy az ellenfél hackerei „ott vannak már a legbelső védvonalakon belül". Ennek megfelelően az úgynevezett „zéró bizalom modell" olyan belső védelmi technológiákra támaszkodik, amelyek folyamatosan ellenőrzik, hogy egy adott eszköz, felhasználó vagy szoftver az elvárásoknak megfelelően működik-e (azaz nem került-e illetéktelen befolyás alá). Ez a koncepció élesen szakít az eddigi szokványos kiberbiztonsági filozófiával, amely a rendszerekbe való illetéktelen behatolások megakadályozására fókuszált.

Az állami rendszerek szintjén is változik a védekezésről vallott hagyományos koncepció. Mindez jól tükröződik az Egyesült Államok kibervédelmi intézményrendszerének változó stratégiájában, amely a hagyományos (periméteralapú, passzív jellegű) védekezésről a „folyamatos harcérintkezésen" alapuló, „előretolt kibervédelem" aktív megközelítésére helyezte át a hangsúlyt.[54]

Felelős viselkedés, kiegyezés: normák és alkuk

Sokan rámutattak már: az offenzív kiberműveletek hátterében az esetek többségében nem holmi gonoszság, hanem emberi félelem, a cselekvési kényszer képzete áll. Azaz: egy támadóan fellépő állami kiberszereplő mozgatórugói között sokszor az a meggyőződés áll az első helyen, hogy (nemzeti érdekei érvényesítéséhez vagy azok megvédéséhez) kénytelen támadóan fellépni. Ne feledjük a klasszikus elrettentéselmélet alapvető megállapítását, axiómáját: az emberi játszmák (köztük az államközi összecsapások) nem hidegen gondolkodó logikai gépek között folynak; az elrettentés problematikájának a gyökerében emberi percepciók, hiedelmek állnak. Ez az oka, hogy az „elrettentés" (tehát a stratégiai stabilitás biztosítása)

[53] Nathan Ryan: Five Kinds of Cyber Deterrence. *Philosophy and Technology,* 31. (2018), 2. 331–338.
[54] Emily O. Goldman: Fresh Thinking and New Approaches Are Needed on Diplomacy's Newest Frontier. *Foreign Service Journal,* 2021. június.

legeredményesebb eszköze az lehet, amely meggyőzi az ellenfelet arról, hogy nincs szüksége arra, hogy támadjon.[55]

Az „okafogyottá tétel" mechanizmusának legfontosabb, legjellemzőbb eszköze a tárgyalás, a megállapodás. Thomas Schelling az elrettentés teóriáját megalapozó fél évszázaddal ezelőtti művében figyelmeztet: az igazi erő az alkuerő. Kiaknázása pedig a diplomácia dolga. Az igazság az, hogy a nemzetközi kiberdiplomácia nem is tétlenkedett az elmúlt évtizedekben. A kibertér biztonságát, élhetőségét előmozdító szabályozórendszer kialakítása folyamatosan napirenden van az utóbbi két évtizedben. Szereplők egész sora feszült neki a kibertérben való mértékadó viselkedés normarendszere kialakításának.[56] A kollektív szabályozórendszer hagyományos eszköze, a nemzetközi jog alapvetően államok és állami eredetű szervezetek viszonyrendszerének rendezésére szolgál.[57] A kibertér egyik szembeötlő sajátossága azonban éppen a szereplők sokasága és sokfélesége. Ennek fényében nem csoda, hogy jogi kötéssel bíró eszköz egyetlen esetet – a kiberbűnözésről szóló budapesti konvenciót – leszámítva nem is született mindeddig. Inkább az irányelvnél átfogóbb, a kívánt viselkedéssel kapcsolatban egyértelműen fogalmazó, de a nemzetközi törvénnyel ellentétben nem kötelező erejű normarendszerek kidolgozása került a kibertér-szabályozó törekvések középpontjába. Figyelemre méltóak ebben a tekintetben az úgynevezett *Tallinni kézikönyvek,* amelyek szakértői összefogásból, önkéntes alapon születtek meg.

Az új évezred elején állította fel az ENSZ Közgyűlése az első úgynevezett kormányzati szakértői munkacsoportot (*Group of Governmental Experts* – GGE), hogy megvizsgálja az IKT-eszközök fejlődésének hatását a nemzetközi biztonság alakulására. Az elmúlt évtizedekben hat ilyen munkacsoport működött. Témájuk: a kibertérben való állami viselkedés kívánatos szabályainak, irányelveinek és normáinak kérdései; a nemzetközi szabályrendszerek érvényesülését segítő bizalomépítő intézkedések és kapacitásépítés. Részleges eredménytelenségek után a világszervezet normaalkotó szerepvállalásának dinamizálása érdekében egy új testület, a Nyílt végű Munkacsoport (OEWG) kezdte meg működését. Az ENSZ

[55] Timothy M. McKenzie: *Is Cyber Deterrence Possible?* Maxwell AFB, Air University Press, 2017. A nemzetközi közösséget átfogó normarendszereknek az elrettentésben betöltött hangsúlyos szerepére hívja fel a figyelmet Mariarosariaria Taddeo: Deterrence by Norms to Stop Interstate Cyber Attacks. *Minds and Machines,* 27. (2017). 387–392.

[56] Nyáry Gábor: Felelősségteljes állami viselkedés a kibertérben. Az ENSZ átfogó normaalkotó erőfeszítései. *Új Magyar Közigazgatás,* 14. (2021b), 3. 33–40.

[57] Christian Ruhl: *Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at Crossroads.* Washington, Carnegie Endowment, 2020.

munkaszervezetei összességében nagyon fontos szerepet játszottak a kibertér szabályozottabbá tételében.

Az elrettentés elméletének kiemelkedő kutatói azonban már a 20. század második felében leszögezték, hogy a stratégiai stabilitásra irányuló valóban hatékony alkufolyamatok mindig egyedi jellegűek. Középpontjukban ugyanis valós emberek percepciói és félelmei állnak. Talán ez az oka annak, hogy a stabilitást célzó kollektív normarendszerek hatékonysága miért csekély. Ez különösen felértékeli az egyes hatalmak közötti bilaterális megegyezéseket. Az amerikai és orosz elnök közötti genfi csúcstalálkozó 2021 júniusában egyenesen korszakosnak nevezhető.[58] A hidegháború kezdete óta a szuperhatalmak egyezkedéseiben az atomfegyverkezés kérdései álltak a középpontban. Ez a mostani volt az első amerikai–orosz csúcstárgyalás, ahol a stratégiai stabilitás problémakörében alapvetően a kibertér viszonyai és fejleményei kerültek a fókuszba. Az ENSZ égisze alatt kidolgozott kiberszabályok fontos iránymutatást jelentenek – ám alapvetően önkéntesek, tehát jogi kötöttséggel nem járnak. Az amerikai–orosz csúcstalálkozó felvetése: egyetlen meghatározó témára kell fókuszálni az erőfeszítéseket, ám az így születő egyezségnek bilaterális, jogi érvénnyel kötelező megállapodási formát kell adni.[59]

A tárgyalások témáját a „célpontok korlátozásában" jelölték meg. Az elképzelés az, hogy a két állam abban állapodjon meg, hogy kölcsönösen tartózkodni fognak a jövőben egymás „kritikus polgári infrastruktúráinak" támadásától.[60] Az amerikai fél egészen szűkre szeretné szabni az egyeztetések fókuszát, és kizárólag a zsaroló vírusos kibertámadások megakadályozása-megelőzése szerepel a napirendjén. Az oroszok ugyanakkor ennél szélesebb kontextusban szeretnének megállapodást tető alá hozni. A tét nagy, hiszen a fenyegetésen alapuló hagyományos elrettentés alig működik a kibertérben. A bilaterális tárgyalással viszont esély nyílik a támadó fellépés kölcsönösen okafogyottá tételére.[61]

[58] Nyáry Gábor: A stratégiai stabilitás keresése. Amerikai–orosz kiberfegyverszüneti tárgyalások. *Ludovika Cyberblog,* 2021a. augusztus 5.

[59] *UNGGE Final Report 2019–2020*. New York, UNODA, 2021; valamint *OEWG Final Substantial Report*. New York, UNODA, 2021.

[60] Egy korábbi amerikai nézőpontot érdemes ezzel összevetni: Alex S. Wilner: Cyber Deterrence and Critical-Infrastructure Protection: Expectation, Application and Limitation. *Comparative Strategy,* 36. (2017), 4. 309–318.

[61] Alex S. Wilner: Us Cyber Deterrence: Practice Guiding Theory. *Journal of Strategic Studies,* 43. (2019), 2. 245–280.

Elágazások, további kutatási irányok

Az elrettentés problematikája a kibertérben egy különös benyomással gazdagítja a vizsgálódót. A téma kutatói (és ez elsősorban az elrettentés kérdéseinek elméleti részleteire fókuszálókat jelenti) szinte kivétel nélkül az államok közötti kapcsolatrendszer vonatkozásában veszik szemügyre az elrettentés, illetve a stratégiai stabilitást biztosító alkufolyamatok állapotát.[62] Eközben azonban a globális kibertér biztonsági környezete sebes tempóban alakul át, és ebben a transzformációban a koronavírus-világjárvány közel két esztendeje különösen markáns változásokat hozott. A kibertér, a számítógépes hálózatokat, a gépeket, a rajtuk futó szoftvereket és az őket használó embereket felölelő új társadalmi dimenzió rohamos gyorsasággal sötétül el a fölé boruló fenyegetésektől.[63] 2017-ben derült ki: a Yahoo cégtől 3 milliárd felhasználói adatelem jutott évekkel korábban illetéktelenekhez. 2018-ban az Equifax nevű amerikai hitelinformációs cég hálózatai váltak támadás áldozataivá, és mintegy 143 millió amerikai polgár személyes adatai kerültek ki a rendszerből. Még ugyanabban az évben jelentette a Marriott hotellánc, hogy 383 millió szállóvendégük adataihoz fértek hozzá illetéktelenek. Az elmúlt másfél évben szédületes növekedésnek indult (az esetszámokat és az eltulajdonított összegeket tekintve egyaránt) a zsaroló vírusos támadások „divatja": a nagy áttörést itt is a járványos 2020-as esztendő hozta meg a támadások meghétszereződésével. A kiberbűnözés esetszámai, a támadások súlya, a károkozás mértéke egyértelműen növekvő tendenciát mutat.

A zsaroló vírusos akciók egyre inkább a modern társadalmak (elsősorban az Egyesült Államok) alapvető működési rendjét biztosító hálózatokat, a legszorosabban vett társadalmi kritikus infrastruktúrát veszik célba. 2021 nyarára a helyzet súlyosbodása nyomán az amerikai kormányzat a nemzetközi terrorizmussal azonos súlyú fenyegetésnek minősítette az informatikai hálózatok és adatbankok zsaroló

[62] Ebben a tekintetben a néhány eddig publikált vállalati kutatás jelenti az egyedüli támpontot. Kiemelkedően magas elméleti színvonalon tárgyalja a kibertérben működő magánszereplőkkel szembeni elrettentés témakörét az egyik jelentős tanácsadó cég közelmúltban megjelent tanulmánya: Jesse Goldhammer et al.: *Leading the Way With an Adversary Focus. Government's Role in Deterring Cyber Attacks.* London, Deloitte, 2021. Különleges esetet vizsgál Thomas Rid: Deterrence Beyond the State: The Israeli Experience.*Contemporary Security Policy,* 33. (2012), 12. 124–147. munkája, amely a terrorszervezetek elrettentésének kérdésére fókuszált. Ehhez kapcsolódik, de a hagyományos doménekben: John Gearson: Deterring Conventional Terrorism: From Punishment to Denial and Resilience. *Contemporary Security Policy,* 33. (2017), 1. 171–198.

[63] Nyáry (2021b): i. m.

vírusokkal történő megtámadását. A nem kormányzati kiberszereplők (bűnözői csoportok) által végrehajtott támadások immár nemzetbiztonsági fenyegetéssel érnek fel a világ leghatalmasabb államában is.

Ez a drámai változás arra mutat, hogy az elrettentés problematikájának vizsgálatában egyfajta elágazáshoz értek a kutatók. A hagyományos – állami szereplőkre fókuszáló – témafelvetés mellett külön fejezetet szükséges nyitni a nem állami kiberaktorok elrettentésének is.[64] A csekély számú korábbi kutatás alapján máris jól látható, hogy az elrettentés valamennyi eddigi elméleti modellje (és az azokra épülő konkrét intézkedések és eszközök) újragondolandók. A magánszereplők által végrehajtott, közvetlenül más magánentitásokat vagy állami intézményeket érő, de nemzetbiztonsági súlyú kiberakciók elrettentésére a korábban alkalmazott megközelítések némelyike aligha működhet.[65] Nyilvánvaló az is: a jogi keretek drasztikus átalakítása (új jogszabályok alkotása, speciális bilaterális jogsegélyrendszerek kialakítása) nélkül nehéz lesz eredményesen szembeszállni ezzel a kihívással.[66] A probléma pedig végképp komplex megközelítést követel majd, ha a nem állami csoportok a világűr eszközeinek kiberrendszereit veszik célba.

Irodalomjegyzék

Általános elmélet és hagyományos elrettentés:

Ayson, Robert: *Thomas Schelling and the Nuclear Age. Strategy as Social Science*. London, Frank Cass, 2004.

[64] Eugenio Lilli: Redefining Deterrence in Cyberspace: Private Sector Contribution to National Strategies of Cyber Deterrence. *Contemporary Security Policy,* 42. (2021), 2. 163–188.

[65] Itt elsősorban az államok közötti viszonyrendszerben a legnagyobb eredményességgel kecsegtető „okafogyottá tétel" az, ami bűnözőkkel kapcsolatban nem jöhet szóba. A fenyegetésen alapuló elrettentés pedig még a hagyományos (hidegháborús) viszonyoknál is kevesebb eredményességgel kecsegtet ebben a közegben. Ugyanakkor az „eltántorítás" számos eszköze (zéró bizalom alapú védelem, reziliencia erősítése, felhasználói kiberhigiéné erősítése) jól használhatónak látszik a szervezett kiberbűnözői közeggel szemben is. A téma érdekes exponálását adja Elisabeth Braw – Gary Brown: Personalised Deterrence of Cyber Agression. *The RUSI Journal,* 165. (2020), 2. 48–54. A nemzetbiztonsági szempontból egyre képlékenyebbé, világos határokat nélkülözővé váló kibertér különös „ügyszövetségeiről", magán- és állami aktorok összefogásáról különösen érdekes perspektívákat vázol fel Herbert Lin – Amy Zegart: *Bytes*, *Bombs and Spyes. The Strategic Dimensions of Offensive Cyber Operations*. Washington, Brookings Institution, 2018.

[66] Duncan Hollis: *A Brief Primer on International Law and Cyberspace*. Washington, Carnegie Endowment, 2021.

Biddle, Tami Davis: Coercion Theory: A Basic Introduction for Practitioners. *Texas National Security Review,* 3. (2020), 2. 94–109. Online: http://dx.doi.org/10.26153/tsw/8864

George, Alexander L. – Richard Smoke: *Deterrence in American Foreign Policy: Theory and Practice.* New York, Columbia University Press, 1974.

Gray, Colin S.: Geopolitics and Deterrence. *Comparative Strategy,* 31. (2012), 4. 295–321. Online: https://doi.org/10.1080/01495933.2012.711116

Haffa, Robert P. Jr.: The Future of Conventional Deterrence: Strategies for Great Power Competition. *Strategic Studies Quarterly,* 12. (2018), 4. 94–115.

Kauffman, William: The Requirements of Deterrence. In Philip Bobbitt – Lawrence Freedman – Gregory F. Treverton (szerk.): *US Nuclear Strategy.* London, Palgrave Macmillan, 1989.

Mazarr, Michael J.: *Understanding Deterrence*. Santa Monica, RAND, 2018.

Morgan, Patrick M.: *Deterrence. A Conceptual Analysis*. London, Sage Publications, 1977.

Morgan, Patrick M.: The State of Deterrence in International Politics Today. *Contemporary Security Policy,* 33. (2012), 12. 85–107. Online: https://doi.org/10.1080/13523260.2012.659589

Quackenbush, Stephen L.: *Understanding General Deterrence Theory and Application*. New York, Palgrave Macmillan, 2011.

Rid, Thomas: Deterrence Beyond the State: The Israeli Experience. *Contemporary Security Policy,* 33. (2012), 12. 124–147. Online: https://doi.org/10.1080/13523260.2012.659593

Schelling, Thomas C.: *The Strategy of Conflict*. Cambridge, Harvard University, 1980.

Schelling, Thomas C.: *Arms and Influence: with a New Preface and Afterword*. New Haven, Yale University Press, 2008.

Snyder, Glenn H.: Deterrence and power. *The Journal of Conflict Resolution,* 4. (1960), 2. 163–178.

Stone, John: Conventional Deterrence and the Challenge of Credibility. *Contemporary Security Policy,* 33. (2012), 12. 108–123. Online: https://doi.org/10.1080/13523260.2012.659591

Wirtz, James J.: How Does Nuclear Deterrence Differ from Conventional Deterrence? *Strategic Studies Quarterly,* 12. (2018), 4. 58–75.

Yamashita, Aihito: Glenn Snyder's Deterrence Theory and NATO's Deterrence Strategy during the Cold War. *Air Power Studies,* 6. (2020). 69–116.

Yamamoto, Satoshi: On Thomas Schelling's Deterrence Theory. *Air Power Studies,* 6. (2020). 117–144.

Elrettentés a világűrben:

Bowen, Bleddyn: The Art of Space Deterrence. *European Leadership Network,* 2018. február 20. Online: www.europeanleadershipnetwork.org/commentary/the-art-of-space-deterrence/

Bowen, Bleddyn E.: From the Sea to Outer Space: The Command of Space as the Foundation of Spacepower Theory. *Journal of Strategic Studies,* 42. (2019), 3–4. 532–556. Online: https://doi.org/10.1080/01402390.2017.1293531

Cheng, Dean – John Klein: A Comprehensive Approach to Space Deterrence. *Strategy Bridge,* 2021. március 31. Online: https://thestrategybridge.org/the-bridge/2021/03/31/a-comprehensive-approach-to-space-deterrence

Finch, James P.: Finding Space in Deterrence: Toward a General Framework for „Space Deterrence". *Strategic Studies Quarterly,* 5. (2011), 4. 10–17.

Krepon, Michael – Julia Thompson (szerk.): *Anti-Satellite Weapons, Deterrence and Sino-American Space Relations.* Washington, Stimson, 2013.

Langeland, Krista – Derek Grossman: *Tailoring Deterrence for China in Space.* Santa Monica, RAND, 2021.

Lambakis, Steve: A Guide for Thinking About Space Deterrence and China. *Comparative Strategy,* 38. (2019), 6. 497–553. https://doi.org/10.1080/01495933.2019.1674081

Morgan, Forrest E.: *Deterrence and First-Strike Stability in Space. A Preliminary Assessment*. Santa Monica, RAND Air Force Project, 2010.

Kibertér és elrettentés:

Assumpção, Clara: The Problem of Cyber Attribution Between States. *E-International Relations,* 2020. május 6. Online: www.e-ir.info/2020/05/06/the-problem-of-cyber-attribution-between-states/

Braw, Elisabeth – Gary Brown: Personalised Deterrence of Cyber Agression. *The RUSI Journal,* 165. (2020), 2. 48–54. Online: https://doi.org/10.1080/03071847.2020.1740493

Gearson, John: Deterring Conventional Terrorism: From Punishment to Denial and Resilience. *Contemporary Security Policy,* 33. (2017), 1. 171–198. Online: https://doi.org/10.1080/13523260.2012.659600

Ghionis, A. Alexander: *The Limits of Deterrence in the Cyber World. An Analysis of Deterrence by Punishment.* Brighton, University of Sussex, é. n.

Goldhammer, Jesse – Joe Mariani – Matt Stapleton – Akash Keyal: *Leading the Way With an Adversary Focus. Government's Role in Deterring Cyber Attacks.* London, Deloitte, 2021. Online: www2.deloitte.com/za/en/insights/industry/public-sector/government-deter-cybersecurity-adversary.html

Goldman, Emily O.: Fresh Thinking and New Approaches Are Needed on Diplomacy's Newest Frontier. *Foreign Service Journal,* 2021. június. Online: https://afsa.org/cyber-diplomacy-strategic-competition

Goodman, Will: Cyber Deterrence. Tougher in Theory than in Practice? *Strategic Studies Quarterly,* 4. (2010), 3. 102–135.

Harknett, Richard J.: Leaving Deterrence Behind: War-Fighting and National Cybersecurity. *Journal of Homeland Security and Emergency Management,* 7. (2010), 1. 1–24.

Hollis, Duncan: *A Brief Primer on International Law and Cyberspace*. Washington, Carnegie Endowment, 2021.

Iasiello, Emilio: Is Cyber Deterrence an Illusory Course of Action? *Journal of Strategic Security,* 7. (2021), 1. 55–67. Online: http://dx.doi.org/10.5038/1944-0472.7.1.5

Libicki, Martin C.: *Cyberdeterrence and Cyberwar.* Santa Monica, RAND Air Force Project, 2009.

Libicki, Martin C.: Expectations of Cyber Deterrence. *Strategic Studies Quarterly,* 12. (2018), 4.

Lilli, Eugenio: Redefining Deterrence in Cyberspace: Private Sector Contribution to National Strategies of Cyber Deterrence. *Contemporary Security Policy,* 42. (2021), 2. 163–188. Online: https://188. doi.org/10.1080/13523260.2021.1882812

Lin, Herbert – Amy Zegart (szerk.): *Bytes, Bombs, and Spies. The Strategic Dimensions of Offensive Cyber Operations*. Washington, Brookings Institution, 2018.

McKenzie, Timothy M.: *Is Cyber Deterrence Possible?* Maxwell AFB, Air University Press, 2017.

Nyáry Gábor: A stratégiai stabilitás keresése. Amerikai–orosz kiberfegyverszüneti tárgyalások. *Ludovika Cyberblog,* 2021a. augusztus 5. Online: www.ludovika.hu/blogok/cyberblog/2021/08/05/a-strategiai-stabilitas-keresese/

Nyáry Gábor: Felelősségteljes állami viselkedés a kibertérben. Az ENSZ átfogó normaalkotó erőfeszítései. *Új Magyar Közigazgatás,* 14. (2021b), 3. 33–40.

Nyáry Gábor: Kiberdiplomácia: hatalom, politika és technológia a geopolitika ötödik dimenziójában. In Török Bernát (szerk.): *Információ- és kiberbiztonság. Fenntartható biztonság és társadalmi környezet tanulmányok V.* Budapest, Ludovika Egyetemi Kiadó, 2020. 321–343.

Nye, Joseph S. Jr.: Deterrence and Dissuasion in Cyberspace. *International Security,* 41. (2016–17), 3. 44–71. Online: https://doi.org/10.1162/ISEC_a_00266

Nye, Joseph S. Jr.: Nuclear Lessons for Cyber Security? *Strategic Studies Quarterly,* 5. (2011), 4. 18–38.

OEWG Final Substantial Report. New York, UNODA, 2021.

Osawa, Jun: The Escalation of State Sponsored Cyberattacks and National Cyber Security Affairs: Is Strategic Cyber Deterrence the Key to Solving the Problem? *Asia-Pacific Review,* 24. (2017), 2. 113–131. Online: https://doi.org/10.1080/13439006.2017.1406703

Ruhl, Christian: *Cyberspace and Geopolitics: Assessing Global Cybersecurity Norm Processes at Crossroads.* Washington, Carnegie Endowment, 2020.

Ryan, Nathan: Five Kinds of Cyber Deterrence. *Philosophy and Technology,* 31. (2018), 2. 331–338. Online: https://doi.org/10.1007/s13347-016-0251-1

Sterner, Eric: Retaliatory Deterrence in Cyberspace. *Strategic Studies Quarterly,* 5. (2011), 1. 62–80. Online: www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-05_Issue-1/Sterner.pdf

Stevens, Tim: A Cyberwar of Ideas? Deterrence and Norms in Cyberspace. *Contemporary Security Policy,* 33. (2012), 12. 148–170. Online: https://doi.org/10.1080/13523260.2012.659597

Stevenson, Jonathan: Cyber Conflict and Deterrence. *Strategic Comments,* 22. (2016), 7. Online: https://doi.org/10.1080/13567888.2016.1237761

Szilágyi István: *A geopolitika elmélete*. Budapest, Pallas Athéné, 2018.

Taddeo, Mariarosaria: Deterrence by Norms to Stop Interstate Cyber Attacks. *Minds and Machines,* 27. (2017). 387–392. Online: https://doi.org/10.1007/s11023-017-9446-1

Taddeo, Mariarosaria: Deterrence and Norms to Foster Stability in Cyberspace. *Philosophy and Technology,* 31. (2018a), 3. 323–329. Online: https://doi.org/10.1007/s13347-018-0328-0

Taddeo, Mariarosaria: *How to Deter in Cyberspace.* Strategic Analysis. Helsinki, Hybrid CoE, 2018b.

Taddeo, Mariarosaria: The Limits of Deterrence Theory in Cyberspace. *Philosophy and Technology,* 31. (2018c), 4. 323–329. Online: https://doi.org/10.1007/s13347-017-0290-2

Thornton, Rod – Marina Miron: Deterring Russian Cyber Warfare: The Practical, Legal and Ethical Constraints Faced by the United Kingdom. *Journal of Cyber Policy,* 4. (2019), 2. 257–274. Online: https://doi.org/10.1080/23738871.2019.1640757

Tsagourias, Nicholas – Michael Farrell: Cyber Attribution: Technical and Legal Approaches and Challenges. *European Journal of International Law,* 31. (2020), 3. 1–27. Online: https://doi.org/10.1093/ejil/chaa057

UNGGE Final Report 2019-2020. New York, UNODA, 2021.

Van der Meer, Sico: *Signalling as a Foreign Policy Instrument to Deter Cyber Agression by State Actors.* Hague, Clingendael, 2015.

Wilner, Alex S.: Cyber Deterrence and Critical-Infrastructure Protection: Expectation, Application and Limitation. *Comparative Strategy,* 36. (2017), 4. 309–318. https://doi.org/10.1080/01495933.2017.1361202

Wilner, Alex S.: Us Cyber Deterrence: Practice Guiding Theory. *Journal of Strategic Studies,* 43. (2019), 2. 245–280. Online: https://doi.org/10.1080/01402390.2018.1563779

4. fejezet

Hírszerzés a kibertérben

Deák Veronika

Bevezetés

A technológia rohamos fejlődésének következtében a kibertámadások száma folyamatosan nő. Emellett egyre komplexebb és kifinomultabb támadások jelennek meg, amelyek eredményes elhárításához elengedhetetlen a mögöttes cél, a motiváció, valamint a támadási alternatívák mélyebb ismerete.

Az elmúlt években számos olyan eset látott napvilágot, amelyben állami szervek kerültek a kibertámadások középpontjába. A különféle elektronikus információs rendszerek vagy szolgáltatások működésének korlátozásától kezdve az anyagi haszonszerzésen át egészen a bizalmas információk megszerzéséig bezárólag számtalan motiváció azonosítható a támadások hátterében.

A központi, állami szerveket célzó támadások sok esetben az adott államra vonatkozó belső és bizalmas információk megszerzésére irányulnak, a saját nemzeti érdekek védelme, érvényesítése és támogatása céljából. Ezen támadások vonatkozásában kiemelt figyelmet kell fordítani a katonai hírszerzést megvalósító kibertámadásokra, hiszen segítségükkel számtalan hasznos információ megszerezhető az adott ország céljairól, szándékairól, alapvető működéséről, erőforrásairól és védelmi mechanizmusairól, amely a későbbiekben egy esetleges katonai művelet során eredményesen felhasználható. A hagyományos és a kiberhadviselésben egyaránt fölényt jelent a megfelelő mennyiségű és minőségű információ megszerzése, hiszen nemcsak az ellenséges félről szerezhetők meg hasznos információk, hanem a saját védelmi képességek hatékonysága és eredményessége is jelentősen fejleszthető, aminek következtében a hírszerzés stratégiai és taktikai előnyt is jelenthet a saját erők számára.

A kibertérben megvalósuló katonai célú hírszerzés már az 1980-as években megjelent, azonban a technológia fejlődésével a hírszerző módszerek is folyamatosan változnak. Így például az ötödik generációs technológia, az IoT-eszközök, a mesterséges intelligencia új hírszerző támadási technikák megjelenéséhez vezet. Éppen ezért elengedhetetlen a már rendelkezésünkre álló módszerek

https://doi.org/10.36250/01079_04

működési mechanizmusának megismerése, azok fejlődési jellemzőinek azonosítása a jövőbeli változások hatékony előrejelzése érdekében.

Jelen fejezet célja az elmúlt évtizedek legjelentősebb katonai célú hírszerző támadásainak azonosítása és elemzése. A támadások elemzése során megvizsgáljuk, hogy miért lehettek sikeres támadások, illetve mitől váltak meghatározó esetté a történelemben. Bemutatjuk, hogy az idő előrehaladtával és a technika fejlődésével miképpen változtak meg a támadások motivációi és célpontjai.

A kibertámadások természetesen válaszlépéseket indukálnak, amelyek során különböző, a kibervédelmi képességek nemzeti szintű fejlesztését nagyban befolyásoló védelmi stratégiai lépések jelentek meg. Mindezek miatt jelen fejezet további célja, hogy a nevezett hírszerzést célzó kibertámadások tapasztalatain alapuló legfontosabb kibervédelmi eszközöket, eseményeket, mechanizmusokat is bemutassa.

Végül egy esetleges előrejelzés keretében ismertetjük, hogy a katonai hírszerzés milyen irányokat és célokat tűzhet ki maga elé az elkövetkezendő néhány évben és évtizedben.

Alapfogalmak

A kibertérben megvalósuló katonai hírszerzés főbb eseményeinek feltárásához, a hírszerző, felderítő technikák elemzéséhez elengedhetetlen a hírszerzéssel összefüggő főbb definíciók áttekintése. Jelen fejezet olyan hírszerzésre alkalmas támadások feltárását és elemzését tűzte ki célul, amelyek végrehajtása a kibertérben zajlott le.

Ahogy azt az előző fejezetekben láthattuk, a kibertérnek számos definíciója létezik, aszerint, hogy milyen aspektusból vizsgáljuk azt. Szempontok lehetnek akár a kibertér térgeometriai jellemzői, az egyén, a társadalom, a gazdaság és a kibertér viszonya is. Donna Haraway szerint a kibertér nem az információ szállítására, feldolgozására van a legnagyobb hatással, hanem a társadalmi viszonyok, kapcsolatok alakulására.[1] Általában az a vélemény, hogy az egész világra kiterjedő, globalizáló közeget bárhonnan el lehet érni, ha rendelkezésre áll a technikai apparátus és az annak működtetéséhez szükséges pénz. A kibertér

[1] Donna Haraway: A Cyborg Manifesto: Science, Technology and Socialist-Feminism in the Last Twentieth Century. In Donna Haraway: *Simians, Cyborgs and Women: The Reinvention of Nature.* New York, Routledge, 1991. 149–181.

használatával együtt járó társadalmi, politikai és gazdasági előnyök a hagyományos térbeli és társadalmi megoszlások mentén helyezkednek el, hiszen az internetes hozzáférés nagy területi és társadalmi egyenlőtlenségeket okoz.[2] Egy másik megfogalmazás szerint az elektronikus információs rendszerek és infrastruktúrák, valamint az ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét nevezzük kibertérnek.[3] A *Nemzeti Kiberbiztonsági Stratégia* szerint 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.[4] Ebben a fejezetben a *Nemzeti Kiberbiztonsági Stratégia* meghatározása alapján választottuk ki a hírszerzésre alkalmazott kibertámadásokat.

A kibertér fogalmának vizsgálata azért is szükségszerű, mert a 2016 júliusában megrendezett varsói NATO-csúcstalálkozón hivatalosan deklarálták, hogy a kibertér az ötödik hadszíntérnek tekinthető.[5] Ennek oka, hogy a NATO szerint a számítógépes támadások jelentős kihívást jelentenek a szövetség tagjainak biztonságára nézve, és hatásaikat tekintve ugyanolyan károsak lehetnek, mint a korábbi négy fizikai dimenzióban (szárazföldi, légi, tengeri, kozmikus) végrehajtott hagyományos támadások.[6] Erről szintén részletesen szóltunk az 1. fejezetben.

A hírszerzés és a felderítés fogalmának tisztázása elengedhetetlen a kibertérben megvalósuló katonai hírszerzés vizsgálata során, hiszen gyakran egymás szinonimáiként is használják e definíciókat, köszönhetően annak, hogy mindkét kategória hasonló tevékenységet és célt foglal magában, továbbá a nemzetközi szakirodalomban az *intelligence* szó jelenik meg, amely felderítésként és hírszerzésként egyaránt fordítható.[7]

[2] Mészáros Rezső: A kibertér társadalomföldrajzi megközelítése. *Magyar Tudomány,* 48. (108.) (2001), 7. 769–779.

[3] Mészáros (2001): i. m.

[4] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról.

[5] *State and Government Participating in the Meeting of the North Atlantic Council in Warsaw 8–9 July 2016.* Press Release 100. North Atlantic Treaty Organization, 2016. július 9.

[6] Kovács László: *Biztonságpolitika: a kibertérben*. Budapest, Nemzeti Közszolgálati Egyetem, 2019.

[7] Füzesi Ottó: *A felderítés elméleti és gyakorlati kérdéseinek vizsgálata, különös tekintettel, az emberi erővel folytatott felderítésére.* Doktori (PhD-) értekezés. Zrínyi Miklós Nemzetvédelmi Egyetem, 2004.

A *Magyar Hadtudományi Lexikon* szerint a hírszerzés „a titkosszolgálati tevékenység egyik alapvető szolgálati ága, amely külföldi bizalmas politikai, gazdasági, technikai, tudományos, katonai híranyagok, adatok, információk tervszerű gyűjtését, elemzését, értékelését végzi nyílt és titkosszolgálati erőkkel, eszközökkel, módszerekkel".[8]

Egy másik megfogalmazás szerint a hírszerzés az állam egyik funkciójaként értelmezhető, amelynek célja a nemzeti érdekek védelme és érvényre juttatása az erre a feladatra létrehozott, közvetlenül a kormányzati irányítás alatt működtetett szervezetek által végrehajtott titkos és nyílt forrású információk megszerzése által.[9] Fontos kiemelni, hogy jelen meghatározás a hírszerzés bizonyos területét jelöli, hiszen fejlődésének köszönhetően a társadalom számos szegmensében megtalálható (például gazdasági, politikai hírszerzés).[10]

Az állam a hírszerző tevékenység végrehajtására hírszerző szervezeteket (szolgálatokat, hivatalokat) működtet, amelyek célja, hogy megfelelő információkkal támogassák a döntéshozatalt. A hírszerző szolgálatok katonai és polgári hírszerző tevékenységet folytatnak. A hírszerzés tevékenységi rendszere magába foglalja az adat- és információszerzést, az elemzés-értékelést, valamint a hírszerző műveletek végrehajtását. Ezen tevékenységek folyamatos kölcsönhatásban vannak, egymással elválaszthatatlan egységet képezve.[11]

A katonai hírszerzés a katonai felderítő szervek által békeidőben és háborúban folytatott megszakítás nélküli tevékenység, amelynek célja az ellenséges vagy várhatóan ellenséges ország, állam katonapolitikai helyzetére, hadigazdasági potenciáljára, fegyveres erőire, valamint a hadszínterekre vonatkozó adatok megszerzése és elemzése.[12]

A polgári hírszerzés feladata az ország elleni politikai és gazdasági törekvések feltérképezése, valamint a kormányzat külpolitikai és külgazdasági érdekeinek érvényesítése, támogatása.[13] Mindezek megvalósítását bizalmas információk megszerzésével segíti elő, amelyek a politikai és kormányzati döntések meghozatalához elengedhetetlenek.

[8] *Magyar Hadtudományi Lexikon.* Budapest, Magyar Hadtudományi Társaság, 1995. 558.

[9] Izsa Jenő: A hírszerzés céljáról és rendszeréről. *Hadtudomány,* 19. (2009), 1–2. 72.

[10] Dobák Imre: *A nemzetbiztonság általános elmélete*. Budapest, Nemzeti Közszolgálati Egyetem Nemzetbiztonsági Intézet, 2014.

[11] Dobák (2014): i. m.

[12] *Magyar Hadtudományi Lexikon* (1995): i. m.

[13] Börcsök András – Vida Csaba: A nemzetbiztonsági szolgálatok rendszere. (Nemzetközi gyakorlat a nemzetbiztonsági rendszer kialakítására.) *Nemzetbiztonsági Szemle,* 2. (2014), 1. 63–100.

A felderítés a *Hadtudományi Lexikon* értelmezése szerint:

> „az állami apparátus vezető szervei és a különböző szintű parancsnokságok azon intézkedéseinek, rendszabályainak és tevékenységeinek összessége, amelyek egy ország vagy országcsoport érdekeiről, célkitűzéseiről, szándékáról, terveiről, tevékenységéről, erőforrásairól, helyzetéről, fegyveres erőinek felépítéséről, csoportosításáról, haditechnikájáról, kiképzettségi helyzetéről és a hadszíntérré váló terület előkészítéséről szóló adatok megszerzését, gyűjtését, tanulmányozását célozzák."[14]

Ezek alapján a felderítés a katonai műveletek támogatásán belül értelmezhető tevékenység, amely magában foglalja a vezetéshez szükséges ellenségre, terepre és egyéb tényezőkre vonatkozó adatok, információk megszerzését, feldolgozását és elemzését.[15]

A kibertérben megvalósuló hírszerzés során érdemes megemlíteni a számítógép-hálózati műveletek fogalmát, amely a másik fél hálózatos számítógépes rendszerei felderítésére, adatok megszerzésére, működésük korlátozására, akadályozására, befolyásolására irányul a számítógép-hálózati felderítés és támadás módszereivel, továbbá mindemellett a saját hasonló hálózatok működését biztosítja.[16]

A hírszerzés alapjául szolgáló lehetséges kiberműveletek

A következőkben néhány lehetséges kibertérben megvalósuló, a hírszerzés alapjául szolgáló, az elmúlt néhány évtizedben jellemző kiberműveleti technika definícióját mutatjuk be.

A *zero-day exploit,* más néven nulladik napi támadás egy olyan biztonsági rés, sebezhetőség, amelyet még azelőtt képes kihasználni a támadó, mielőtt felfedezték vagy nyilvánosságra hozták volna azt.[17]

A DoS *(denial of service),* más néven *szolgáltatásmegtagadással járó támadás* lényege, hogy olyan sok kéréssel támadják meg a hálózatot, vagy azon keresztül valamelyik alkalmazást, amennyit a fogadó oldal már nem tud feldolgozni. Ennek következtében nem lesz elérhető a szolgáltatás, mivel nem tud kiszolgálni egyszerre ennyi kérést a szerver.[18] A támadás irányulhat a célpont

[14] *Magyar Hadtudományi Lexikon* (1995): i. m. 339.
[15] Börcsök–Vida (2014): i. m.
[16] Haig Zsolt: *Információs műveletek a kibertérben*. Budapest, Dialóg Campus, 2018.
[17] Animesh Kumar: Zero Day Exploit. *SSRN,* 2014. január 14.
[18] Fehér Krisztián: *Kezdő hackerek kézikönyve*. Budapest, BBS-INFO, 2016. 202–204.

hálózati kapcsolatának vagy a célpont rendszerben működő valamely – szolgáltatást nyújtó – alkalmazásának túlterhelésére, amely során a támadó célja a célpont erőforrásainak lefoglalása.[19]

A *hátsóajtó*-alkalmazás *(backdoor)* a felhasználók számára általában nem látható elem, amely a telepítést követően egy vagy több távoli személynek lehetőséget biztosít a számítógép elérésére és irányítására. Ennek segítségével a támadó megtekintheti a másik eszközön tárolt adatokat, információkat, de akár módosíthatja vagy törölheti is ezeket. A program veszélyessége abban rejlik, hogy nemcsak távoli elérést biztosíthat idegeneknek, hanem rendszeradminisztrációs jogok megszerzését is lehetővé teheti.[20]

A *vírus* rosszindulatú program, amely jellemzően saját programkódját fűzi hozzá egy másik programhoz, illetve az által, hogy elhelyezi a másik programban saját másolatait, annak segítségével szaporodik, de más programok megfertőzésére is képes. A rendszerbe a felhasználó engedélye nélkül kerül be, általában valamilyen adathordozó eszköz (pendrive, CD, DVD, SD-kártya, merevlemez, MP3- és videólejátszó, mobiltelefon stb.) vagy akár hálózati kapcsolat (internet) segítségével. Ezen vírusok károsíthatják, illetve törölhetik a számítógépek vagy egyéb infokommunikációs eszközök adatait, de akár a merevlemez tartalmát is törölhetik vagy módosíthatják, valamint a különféle levelezőprogramok segítségével továbbíthatják is a vírust más eszközökre. Fontos, hogy nemcsak adathordozó eszközök által terjedhetnek, hanem elektronikus levelezés során az üzenetek részeként (például csatolmányként), vagy akár az internetről letöltött tartalmakon, dokumentumokon keresztül is.[21]

A *trójai programok* látszólag vagy akár valójában is hasznos funkciókat látnak el, de emellett végrehajtanak olyan nem kívánt műveleteket is, amelyek adatvesztéssel járnak, például adatokat módosítanak, könyvtárakat vagy adatállományokat törölnek. Tehát a program a felhasználó tudta nélkül a háttérben nem kívánt műveleteket is végrehajthat, mint például vírustelepítés, titkos információk megszerzése (például banki adatok, jelszavak, PIN-kódok), hátsó ajtó létrehozása vagy akár közvetlen károkozás is.[22]

[19] Gyányi Sándor: DDOS támadások veszélyei és az ellenük való védekezés. *Hadmérnök,* (2007), különszám. 1788–1919.

[20] Deák Veronika: Kártékony programok terjedése social engineering technikákon keresztül. *Hadmérnök,* 14. (2019), 2. 256–271.

[21] Haig Zsolt – Kovács László: *Kritikus infrastruktúrák és kritikus információs infrastruktúrák*. Budapest, Nemzeti Közszolgálati Egyetem, 2012.

[22] Kovács László: Az információs terrorizmus eszköztára. *Hadmérnök,* (2006), különszám.

A *zsaroló program,* más néven *ransomware* célja egy adott infokommunikációs eszközhöz vagy információs rendszerhez hozzáférve olyan információk megszerzése, amelyek zsarolás alapját szolgálhatják. A zsaroló programok megszakítják egy információs rendszer működését, korlátozva a felhasználót az eszköz használatában, ezt követően a támadó zsaroló üzenetben közli az áldozattal, hogy bizonyos összeg fejében visszaállítja az eszközt vagy rendszert a korábbi állapotra. Abban az esetben, ha a célszemély nem teljesíti a támadó kérését, akkor a zsaroló sok esetben kiterjeszti a fizetésre rendelkezésre álló időt, vagy törli az adatokat a felhasználó infokommunikációs eszközéről.[23]

A *social engineering* az ember megtévesztésével, kihasználásával és manipulálásával teszi lehetővé belső és bizalmas információk megszerzését vagy akár egy infokommunikációs eszköz megfertőzését kártékony programmal.

A *whaling* az adathalászat egyik típusa, lefordítva bálnavadászatot jelent; talán azért is, mert a „nagy halakat", vagyis egy szűkebb felhasználói kört, a vállalatok, szervezetek vezetői csoportját célozza. Ennél a technikánál az adathalász üzenetek általában valamely üzleti partnertől vagy állami intézménytől, hatóságtól érkeznek.[24]

Katonai hírszerzés a kibertérben

A katonai hírszerzés már az 1980-as évek kezdetétől jelen van a kibertérben. A technológiai fejlődés következtében pedig ezek a támadások egyre kifinomultabbak a támadás céljait és a végrehajtás módját tekintve.

Szeretnénk időrendi áttekintést nyújtani a leglényegesebb hírszerzési műveletekről és az így azonosítható fejlődési/változási görbéről. Elsősorban megvizsgáljuk a kibertámadások típusainak fejlődését, majd azonosítjuk a támadás létrehozásához és végrehajtásához kapcsolódó erőforrások változását, végül megnézzük, hogy az idő előrehaladtával hogyan változtak meg a hírszerzési műveletek céljai.

[23] Ibrar Yaqoob et al.: The Rise of Ransomware and Emerging Security Challenges in the Internet of Things. *Computer Networks,* 129. (2017). 444–458.

[24] Pavel Y. Leonov et al.: The Main Social Engineering Techniques Aimed at Hacking Information Systems. *2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT),* IEEE, 2021. 0471–0473.

Áttekintés

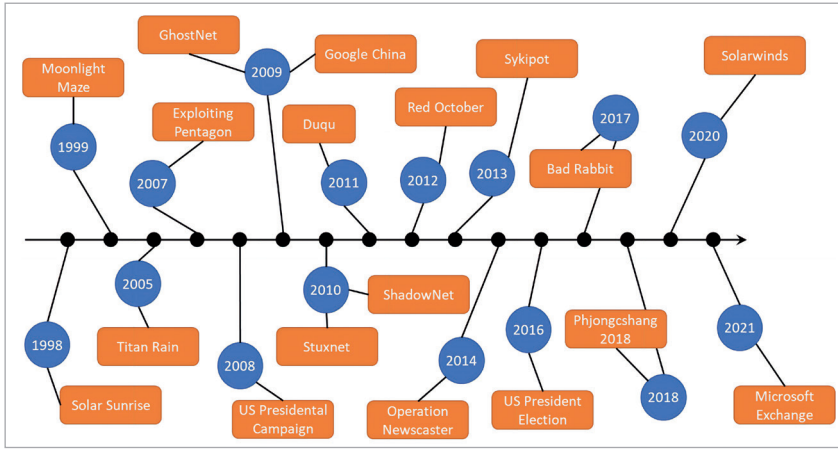
Az első kibertámadások az 1980-as évekre tehetőek, és elsősorban magánszemélyek által készített vírusok voltak, nem kapcsolódtak szorosan a katonai hírszerzéshez. A 80-as évek végén már megjelentek a katonai hírszerzéshez kapcsolódó támadások is, elsősorban az egykori NDK, az Egyesült Államok és a Szovjetunió területén. Az igazi áttörést a 90-es évek vége hozta el, ahol már célzottan történtek hírszerző akciók a kibertérben. Míg a 20. század végén, illetve a 2000-es évek elején még csak évente egy-egy nagyobb horderejű támadást jegyzett fel a történelem, a 2010-es évektől kezdődően havonta rögzítettek újabb és egyedibb támadásokat a világ minden tájáról.

A katonai hírszerzést megvalósító kiberműveletek kapcsán fontos kiemelni az APT- *(Advanced Persistent Threat)* támadásokat is, amelyek folyamatos, tartós kiberbiztonsági fenyegetettséget jelentenek. Ezen támadások végrehajtásáért szervezett kiberbűnözői csoportok felelősek. Az e csoportok által végrehajtott támadások céljai, motivációi és felhasznált eszközei hasonlóak, sok esetben megegyeznek a katonai hírszerző kiberműveletek során alkalmazott módszerekkel, technikákkal. Ilyen csoportok a teljesség igénye nélkül például az alábbiak:

a) *APT1* (Unit 61398 néven is ismert, a kínai hadsereg által felügyelt csoport, amely 2006 óta folytat kiberkémkedési tevékenységet, és erőssége, hogy azonos időben több tucat szervezettől képes volt információkat eltulajdonítani.)
b) *APT4* (Más néven Maverick Panda, Sykipot Group, kínai hátterű, és főként a repülőgépipar, az autóipar, a távközlés, valamint a kereskedelmi szervezetek támadását célozta.)
c) *APT28* (Fancy Bear és Sandworm néven is ismert orosz csoport, körülbelül 2000 óta hajt végre kibertámadásokat elsősorban kormányzati, katonai és biztonsági szervezetek ellen.)
d) *APT29* (Dukes és Cozy Bear néven egyaránt ismert orosz csoport, amely feltételezhetően az orosz Külföldi Hírszerző Szolgálat [SVR] irányítása alatt működik, és számos amerikai, európai és NATO-tagállam kormányzati hálózatait, kutatóintézeteit célzó kibertámadás végrehajtásáért felelős.)
e) *APT35* (Irán által szponzorált csoport, amely 2014 óta elsősorban a Közel-Keleten tevékenykedik, és számos kibertámadás fűződik a nevéhez, amely kormányzati, energia-, közlekedési, technológiai és távközlési szektorokat is érintett.)

f) *APT37* (Észak-koreai, 2012 óta kiberkémkedést végrehajtó csoport, többek között a dél-koreai, vietnámi, japán és közel-keleti közlekedési, egészségügyi, autóipari, repülőgépgyártási szektorokat célozta.)
g) *APT38* (2009 óta aktívan tevékenykedő észak-koreai csoport, amely Lazarus Group néven is ismert; támadásai mögött főként pénzügyi motiváció áll, ennek következtében elsősorban bankokat, pénzügyi intézményeket céloz.)
h) *APT41* (2012 óta aktív, kínai, államilag támogatott kémtevékenységet is végző csoport, amely többek között egészségügyi, távközlési, energia- és technológiai ágazatokat érintő támadásokat hajt végre.)
i) *G0010* (WhiteBear néven is ismert, 2004 óta tevékenykedő orosz csoport, amely már több mint 45 országban fertőzte meg kormányzati, katonai, oktatási, egészségügyi, kutatási szektorok szervezeteit.)[25]

Az *1. ábrán* látható idővonalon a legfontosabb katonai APT- és katonai hírszerzési támadások szerepelnek:



1. ábra: Hírszerzési célú kibertámadások 1998–2021 között
Forrás: a szerző szerkesztése

[25] MITRE ATT&CK: Groups. 2021.

1. táblázat: Az elmúlt évek hírszerzést megvalósító kibertámadásai

1998:	Solar Sunrise	Az eredeti feltevések szerint az amerikai védelmi minisztérium hálózatát támadta meg Irak hírszerzési célból. Később kiderült, hogy egy izraeli mentor irányításával két amerikai tinédzser felelős a támadásért, de emiatt bizonyosodott be, hogy a kritikus infrastruktúrák kibertámadások célpontjai lehetnek. A támadás során számos kormányzati számítógéphez szereztek hozzáférést, közülük 11 az amerikai légierő és haditengerészet bázisain volt megtalálható. A Solar Sunrise arra is figyelmeztetett, hogy a jelentős támadási képességek nem csak szakértők által találhatók meg. Utóbb kiderült, hogy semmilyen titkos anyag nem került ki a minisztérium hálózatából.[26]
1999:	Moonlight Maze	Bár magát az esetet 1999-re datáljuk, mivel a nyomozás ekkor fejeződött be, a kibertámadás már 1996 óta folyamatosan tartott az Egyesült Államok ellen. Érintette többek között a Pentagont, a National Aeronautics and Space Administrationt (NASA), katonai és kormányzati szervezeteket, kutatóintézeteket, egyetemeket, valamint az amerikai Energiaügyi Minisztériumot is. A Moonlight Maze nyílt forráskódú Solaris rendszereket célzó Unix-alapú támadás. A támadás elkövetése Oroszországra, a feltételezések szerint a G0010 vagy más néven Snake csoportra volt visszavezethető, amelynek során több ezer titkos dokumentum vándorolt az egyik nagyhatalomtól a másikhoz.[27]
2005:	Titan Rain	Az előző esethez hasonlóan ebben az esetben is korábban, már 2003 óta zajlott a kibertámadás az Egyesült Államok védelmi hálózatai ellen. A támadások nemzetbiztonsági információk megszerzését tűzték ki célul, a támadóknak számos kormányzati és védett hálózatba sikerült bejutniuk, így például többek között a Pentagon és a NASA rendszereibe is képesek voltak behatolni. A támadásokat Kínáig tudták visszanyomozni, egyes feltételezések szerint az APT1 (Unit 61398) csoport volt az elkövető. Az eset különlegessége, hogy itt már nem egyetlen sérülékenységet használtak ki a támadók, hanem jól megtervezett támadások sorozatát hajtották végre.[28]
2007:	Exploiting Pentagon	Az amerikai védelmi miniszter magán-e-mail-fiókját ismeretlenek törték fel, így képesek voltak a Pentagon hálózataihoz hozzáférni, és titkosított adatokat eltulajdonítani. A feltételezett elkövetők kínai hackerek voltak, azonban a kínai állam ezt hivatalosan tagadta.[29]

[26] Kenneth J. Knapp – William R. Boulton: Cyber-Warfare Threatens Corporations: Expansion Into Commercial Environments. *Information Systems Management,* 23. (2006), 2. 76.

[27] Azhar Ushmani: Cyberwarfare History and APT Profiling. Advance Online Publication. *International Journal of Computer Science Trends and Technology (IJCST),* 7. (2019), 4.

[28] Dana Rubenstein: *Nation State Cyber Espionage and its Impacts.* Washington University in St. Louis, 2014. december 1.

[29] Robert N. Charette: DoD Admits to Being Severely Hacked. *IEEE,* 2008.

2008:	Presidential Campaign	A kiberhírszerzés eljutott arra a pontra, ahol már a választások kapcsán is képes volt beleszólni az amerikai politikai játszmákba. 2008-ban mind a demokratikus, mind a republikánus párt kampányához kapcsolódó adatokat tulajdonított el egy kínai hackercsoport.[30]
2009:	GhostNet	A GhostNet összehangolt kibertámadás-sorozat volt, a világ 103 országában működött, és állami, pénzügyi, illetve ipari titkok megszerzését célozta. A GhostNet-rendszer arra irányítja a fertőzött számítógépeket, hogy töltsenek le egy gh0st RAT (remote access tool) néven ismert trójai programot, amely lehetővé teszi a támadók számára, hogy teljes, valós idejű irányítást szerezzenek az eszköz felett. A támadássorozat során kormánytagokat és kormányközeli szervezeteket is megfigyeltek. A megfigyelő kémprogramok mögött Kína állt, és elsősorban a dél-ázsiai országokban ténykedett. Érdekesség, hogy a kémprogramot először a dalai láma számítógépén fedezték fel. A támadássorozat nevét az elkövetőiről, a GhostNet APT-csoportról kapta.[31]
2009:	Google	Kínai hackerek törték fel a Google vállalati szervereit, és hozzáférést kaptak egy olyan adatbázishoz, amely titkos információkat tartalmazott gyanúsítottakról, kémekről, ügynökökről és az amerikai kormány által megfigyelt terroristákról. Ezenkívül a támadók információt szerezhettek az amerikai nemzetbiztonsági és bűnüldöző szervek dokumentumairól, valamint a kapcsolódó titkosszolgálati tevékenység végrehajtásával és ellenőrzésével összefüggő bírósági végzések tartalmáról.[32]
2010:	Shadow-Network	A ShadowNetwork a GhostNet folytatásának tekinthető. Miután a GhostNethez kapcsolódó sérülékenységeket megszüntették, a támadások száma továbbra sem csökkent. Így térképezték fel a ShadowNetworköt, amelynek célja továbbra is elsősorban India vezetőinek megfigyelése, illetve titkos anyagok Kínába továbbítása volt. A kiberhadművelet során a támadók *social media* és felhőszolgáltatásokat biztosító platformokat (Twitter, Google, Yahoo) használtak arra, hogy a vírusokat az áldozatok gépére telepítsék.[33]

[30] Morgan Swartley: Political Marketing: How Social Media Influenced the 2008–2016 US Presidential Elections and Best Practices Associated. *Senior Honors Theses,* 726. 2018. szeptember 4.

[31] Ronald J. Deibert – Rafal Rohozinski: Tracking GhostNet: Investigating a Cyber Espionage Network. *Information Warfare Monitor,* 2009. március 29.

[32] Ellen Nakashima: Chinese Hackers Who Breached Google Gained Access to Sensitive Data, U.S. Officials Say. *The Washington Post,* 2013. május 20.

[33] Steven Adair et al.: *Shadows in the Cloud: Investigating Cyber Espionage 2.0.* A Joint Report of the Information Warfare Monitor and Shadowserver Foundation. Toronto, 2010. április 6.

2010:	Stuxnet	A Stuxnet egy 2010-ben felfedezett féreg volt, amely a hírszerzési tevékenység megvalósítása mellett az iráni nukleáris létesítmények, ipari vezérlők felügyeleti és adatgyűjtési (SCADA) rendszereinek újraprogramozását célozta. A kibertámadáson keresztül konkrét fizikai támadásokat voltak képesek elérni a támadók. A Stuxnet elsődleges célja Irán nukleáris programjának teljes megakadályozása volt. Ennek megvalósítására több nulladik napi sérülékenységet használtak ki a számítógépek megfertőzésére. A fájlok megfertőzésével a féreg hozzá tudott férni a programozható logikai vezérlőkhöz (PLC), amelyeket a számítógépek az ipari eszközök teljesítményének szabályozására használnak. Ezáltal a Stuxnet képes volt az urándúsító centrifugák észrevétlen tönkretételére és a dúsítási folyamat megzavarására. Legalább 1000 centrifugát tett használhatatlanná a Natanzban lévő dúsítóban, és szakértők szerint legalább két évvel vetette vissza az iráni atomprogramot.[34]
2011:	Duqu	A Duqu a korábbi Stuxnet hasonmása, a magyarországi Crysys kutatólaboratórium ismerte fel. Fontos, hogy bár nagyon hasonló kialakítással rendelkezett, mint a Stuxnet, nem volt teljesen ugyanaz. A Duqu egy kifinomult, információszerzésre alkalmas kártékony program. A Duqu Microsoft Windows operációs rendszerek nulladik napi sérülékenységei felhasználásával szerzett meg bizalmas információkat. Újdonságként értelmezhető a Duqu azon jellemzője, hogy a támadások mögött álló szervezetek kapcsolatban állnak egymással, közös belső információs platformmal rendelkezhetnek *zero-day* támadási felületekkel kapcsolatban. A támadás az izraeli Unit 8200 csoporthoz köthető.[35]
2012:	Red October	A Vörös Október nevű vírust az orosz Kaspersky Lab fedezte fel 2012-ben, és állításuk szerint a vírus már 2007 óta gyűjtött információkat Microsoft Excel- és Word-felhasználók gépeiről. A vírus elsősorban nagykövetségeket, diplomáciai szervezeteket, egyetemeket, tudományos kutatást folytató cégeket, ipari és kereskedelmi szervezeteket, repülőgépészeti intézményeket, valamint katonai szervezeteket célzott. A Red October legfőbb célja bizalmas, titkos dokumentumok megszerzése és a megfertőzött hálózatok feltérképezése volt. A vírus előnye, hogy addig ismeretlen metódus alkalmazásával fertőzte meg a számítógépeket, ám a terjedéshez a korábban bevált módszereket, így például adathalász leveleket, fertőzött weboldalakat és Microsoft Office-, PDF-, Java-programok sebezhetőségeit alkalmazta.[36]

[34] Marie Baezner – Patrice Robin: Stuxnet. *ETH Zurich*, 4. (2017).

[35] Bencsáth Boldizsár et al.: Duqu: Analysis, Detection, and Lessons Learned. *ACM European Workshop on System Security (EuroSec),* 2012.

[36] Henry Mwiki et al.: Analysis and Triage of Advanced Hacking Groups Targeting Western Countries Critical National Infrastructure: APT28, RED October, and Regin. In *Critical Infrastructure Security and Resilience. Advanced Sciences and Technologies for Security Applications*. Springer, Cham, 2019.

2013:	Sykipot	A kínai hackerek a Sykipot néven ismert rosszindulatú programmal fertőzték meg az Egyesült Államok kormányzati és védelmi szervezeteit, valamint a piaci szektort is, például banki intézményeket, a távközlést, illetve az energiaszektort. A Symantec szerint a Sykipotot már 2006 óta használták célzott támadásokban. A Sykipot *malware* adathalász e-maileken keresztül terjedt, rosszindulatú csatolmányok vagy linkek útján. A kártékony program lehetővé teszi fájlok feltöltését, letöltését, így bizalmas információk megszerzését vagy további rosszindulatú programok telepítését. A támadás végrehajtásáért az APT4 vagy más néven Sykipot Group volt felelős.[37]
2014:	Operation Newscaster	A támadás során *social engineering* technikák segítségével tudtak támadók eljutni a célszemélyekhez. A bizalom kiépítésére 14 álszemélyt alakítottak ki, akik aktívan részt vettek a *social media* platformokon (Facebook, Twitter, LinkedIn), és folyamatosan publikáltak posztokat saját blogjaikon. Ezáltal valós személyek látszatát keltve kerülhettek fontos emberek közelébe. A támadók a hamis személyek alkotta összetett és összehangolt hálózat támogatására egy konkrét „virtuális rendszert" is felállítottak, és fiktív hírportál (NewsOnAir.org) biztosította az álszemélyek háttértörténeteinek hitelességét. A hálózat létrehozását követően az iráni támadók megkezdték a kapcsolatfelvételt a közigazgatásban, kormányzati szervezetekben dolgozó személyekkel a megfelelő szintű bizalom kiépítése érdekében. A célszemélyekből több mint 2000 fős hálózatot hoztak létre, a megszerzett információk köréről azonban nincs információ.[38]
2016:	President Election Campaign	A támadás célja a 2016-os amerikai választások befolyásolása volt, ahol több e-mail és titkosított dokumentum szivárgott ki. A kiszivárogtatások mögött a választók véleményének befolyásolása volt a feltételezett cél. Az amerikai közvélemény szerint az orosz kormányzat közvetve, információs műveletekkel és az ehhez információt szolgáltató kiberkémkedéssel próbálta befolyásolni az amerikai elnökválasztás eredményét. A támadók e-mail-fiókokat törtek fel, az ott megszerzett információkat nyilvánosságra hozták, továbbá számtalan álhírt jelentettek meg a közösségi médiában. A támadások végrehajtása az orosz APT28 (Cozy Bear) és APT29 (Fancy Bear) csoporthoz köthető.[39]
2017:	WannaCry, NotPetya, BadRabbit	A 2017-es évben kerültek elő először a zsaroló vírusok. Rögtön három híres eset is bekerült a hírekbe: WannaCry, NotPetya és BadRabbit. Céljuk minden esetben a célpontok sérülékenységének vizsgálata, információszerzés és a megtámadott szervezetek működésének korlátozása volt. Feltételezések szerint a WannaCry-támadást az észak-koreai Lazarus csoport, a NotPetya-műveletet pedig az orosz Sandworm csoport hajtotta végre.

[37] Hippolyte Djonon Tsague – Bheki Twala: *Reverse Engineering Smart Card Malware Using Side Channel Analysis With Machine Learning Techniques.* IEEE International Conference on Big Data (Big Data), 2016. 3713–3721.

[38] Gabi Siboni – Sami Kronenfeld: Iranian Cyber Espionage: A Troubling New Escalation. *INSS Insight,* 2014. június 16. 561.

[39] Kovács László – Krasznay Csaba: „Mert övék a hatalom": Az internet politikát (is) befolyásoló hatása a 2016-os amerikai elnökválasztás során. *SVKK Elemzések,* (2017), 9.

2018:	False-flag	A Dél-Koreában rendezett téli olimpián használt rendszerekhez, adatbázisokhoz és adatokhoz jutottak hozzá a támadók. A támadás érdekessége azonban leginkább az, hogy mestersségesen Észak-Koreára és Kínára terelték a támadás gyanúját. Az információszerzés mellett a támadóknak sikerült megzavarni az olimpia internetes és televíziós közvetítéseit, valamint leállítani a jegynyomtatási rendszert.[40]
2020:	SolarWinds	A SolarWinds egy amerikai magánvállalat, amelynek szoftverét világszerte rengetegen használták, köztük távközlési vállalatok, katonai és kormányzati szervezetek, így például a Pentagon, a NASA és a National Security Agency (NSA) is. A SolarWinds az Orion nevű szoftverrel támogatja az informatikai hálózatok felügyeletét és kezelését, beleértve az adatok összesítését, elemzését és megjelenítését. A FireEye kezdeti felfedezését követő vizsgálatok azt mutatták, hogy a hackerek már 2019 októberében megfertőzték a SolarWinds Orion szoftverét, lehetővé téve számukra, hogy 2020 márciusában egy szoftverfrissítésen keresztül rosszindulatú szoftvereket telepítsenek a vállalat ügyfeleinek hálózatába. A támadás érdekessége, hogy a támadók képesek voltak hosszú ideig észrevétlenül ügyködni, illetve hogy a cég szoftverét használókon keresztül az Egyesült Államok prominens vezetőiig is képes volt eljutni a kártékony program. A támadás előnye, hogy a biztonsági frissítésben könnyedén elrejthető a kártékony kód. A támadás kifinomultságára és komplexitására utal, hogy több mint 1000 képzett mérnök részvételével hajtották végre.[41] Feltételezések szerint az orosz Cozy Bear csoport felelős a támadás végrehajtásáért.
2021:	Microsoft Exchange	A Microsoft Exchange Server elleni támadásban több mint 30 000 egyesült államokbeli, világszerte pedig több tízezer vállalat rendszerei érintettek. A szakértők szerint kínai állami hackerek találtak egy olyan hibát, amelynek segítségével tetszőleges programot voltak képesek telepíteni a vállalatok szervereire. Így a biztonsági réseken keresztül úgynevezett hátsóajtóprogramokat *(backdoor)* telepítettek a támadók a rendszerekbe.[42]

Megjegyzés: Az évek során sokkal több támadás valósult meg, nem csak a nagyhatalmak között, azonban az itt felsoroltak gyakorolták a legnagyobb hatást a kibertér hadszíntérré válására. Érdemes azt is megjegyezni, hogy a lista csak a katonai hírszerzéshez kapcsolódó kibertámadásokkal foglalkozik, így a fontosabb magánakciók, illetve egyéb információs műveletek (például lélektani hadviselés) vagy szolgáltatások működésének korlátozását célzó támadások nem jelennek meg a felsorolásban.

Forrás: a szerző szerkesztése

[40] Joseph Marks: The Cybersecurity 202: Russia's False Flags in Winter Olympics Cyberattack Herald a More Complicated Future. *The Washington Post,* 2019. október 21.

[41] Marcus Willett: Lessons of the SolarWinds Hack. *Survival,* 63. (2021), 2. 7–26.

[42] Matthieu Faou – Mathieu Tartare – Thomas Dupuy: Exchange Servers Under Siege From at Least 10 Apt Groups. *WeLiveSecurity,* 2021. március 10.

A sikerek okai

A bemutatott támadások korábban nem ismert új technológiára, sebezhetőségre épültek. Ebben a részben azt szeretnénk bemutatni, hogy milyen újdonságok jelentek meg az egyes támadásokban, amelyek miatt azok sikeresek lehettek. Alapvetően három fő időszakot vizsgálunk meg. Először az internet kialakulásának kezdetét elemezzük, majd a 2000-es éveket, végül napjaink kibertámadásait vesszük górcső alá.

A kezdetek

Az internet kialakulását az 1980-as évek végére tehetjük, amikor még jellemző volt, hogy nem igazán számítottak támadásokra. A szoftverek fejlesztése során egyáltalán nem gondoltak a készítők arra, hogy támadások használhatják ki sérülékenységeiket. A támadások így könnyen kivitelezhetőek voltak, akár egyetlen ember is képes volt óriási káoszt teremteni.

Az első ismert kibertámadást 1988-ra lehet datálni, amikor is Robert Tappan Morris frissen végzett diák kíváncsi volt, hogy mekkora is az internet jelenleg. Ezért írt egy egyszerű programot, amely számítógépről számítógépre vándorolt, és mindig küldött egy jelet Morrisnak az újonnan megismert gépről. A program azonban annyira gyorsan reprodukálódott, és küldte az üzeneteket Morrisnak, hogy a hálózat nem bírta kellően gyorsan továbbítani a jeleket Morris gépére, blokkolta a kommunikációhoz kapcsolódó hálózati részt, így kialakítva az első DoS *(denial of system)* támadást. Hivatalosan Morris az első személy, akit ténylegesen el is ítélt a bíróság.[43]

Az egyik legnagyobb hírszerzési akció ebben az időben a Moonlight Maze támadás volt, amely valószínűsíthetően 1996-tól egészen 1999-ig tartott, illetve amelynek során sikerült adatokat továbbítani az Egyesült Államokból Oroszországba. A támadás során csak publikusan elérhető hibákat használtak ki a hackerek. Egész egyszerűen azért, mert abban az időben, ha a rendszergazdák találtak valamilyen hibát a rendszerben, azt megosztották másokkal is, ám a szoftverekhez ezekben az időkben még nem jártak olyan gyorsan frissítések,

[43] Hilarie Orman: The Morris Worm: A Fifteen-Year Perspective. *IEEE Security & Privacy,* 1. (2003), 5. 35–43.

mint napjainkban. Volt, hogy fél év vagy akár egy év is kellett, amíg a publikusan is ismert biztonsági réseket sikeresen javították a szoftverekben.[44]

2000-es évek

A 2000-es évek hajnalán az internet mérete és felhasználási köre rendkívüli iramban növekedett. Egyre több és több online szolgáltatás vált elérhetővé, amely akár már magában is nagy károkat tudott okozni. Azonban erre az időre jellemző volt, hogy már nem csak diákcsínyként megvalósított támadásokat hajtottak végre, és a fejlesztők elkezdtek foglalkozni a szoftverek és rendszerek védelmével annak érdekében, hogy a hackerek ne legyenek képesek könnyedén hozzájutni a titkos és védett dokumentumokhoz, információkhoz.

A támadások sikerét a 2000-es évek elejétől az biztosította, hogy a hackerek jelentős csoportokat alkottak, és a támadásokat rendkívül precízen tervezték meg. Nemcsak egyetlen sérülékenységet használtak ki az adott támadás során, hanem több irányból támadtak, és több típusú támadást is bevetettek.

Talán a legismertebb ilyen támadássorozat a GhostNet és annak folytatása, a ShadowNet volt. A támadás során e-maileket küldtek a támadók kormányzati és gazdasági szervezetek tagjainak, amelyek számukra a saját területükön hasznos és érdekes információkat tartalmaztak. A megnyitott üzenet azonban rosszindulatú programot tartalmazott, amelyet ha elindítottak az áldozatok, akkor engedélyezték egy trójai program futtatását. A rosszindulatú kód Microsoft Windows operációs rendszereken működött, és a támadók képesek voltak valós időben teljesen átvenni az irányítást az áldozatok gépe felett, illetve a kamerát bekapcsolni, és videóképet rögzíteni, továbbá a mikrofont bekapcsolva hangot is rögzíteni.[45]

Ebből a támadásból is látszik, hogy nem pusztán dokumentumok ellopása volt a cél, hanem teljes megfigyelés és lehallgatás. A támadók mindezt úgy voltak képesek megtenni, hogy több éven keresztül senkinek sem tűnt fel. Ez a tény arra enged következtetni, hogy rendkívül precízen és szervezetten hajtották végre az akciót.

A másik fontos említendő eset a Stuxnet, amelynek különös jelentősége a hírszerzés mellett, hogy ez volt az első fizikai károkat okozó kibertámadás.

[44] Ushmani (2019): i. m.

[45] Nart Villeneuve – David Sancho: *The "Lurid" Downloader.* Trend Micro Incorporated, 2011.

Elsősorban programozható logikai vezérlőket (PLC) támadott, olyan ipari gépek vezérlő egységeit, amelyekkel például jármű-összeszerelést automatizálnak, vagy rostos üdítők palackozását. A Stuxnet során ezeket a vezérlőket nukleáris anyagok szétválasztására használták, és egész egyszerűen minden este, miután a gyár dolgozói hazamentek, a vírus bekapcsolta a vezérlőket, és maximális teljesítményen üzemeltette őket, aminek hatására másnap már nem működtek tovább.[46] A Stuxnet után a magyar CrySyS laboratórium felfedezte a Duqu vírust is, amelyről feltételezhető, hogy vagy a Stuxnet fejlesztői készítették, vagy a Duqut fejlesztő csapat már korábban látta és ismerte a Stuxnet forráskódját. A Duqu célja azonban nem fizikai károkozás volt, hanem egyértelműen katonai hírszerzés.

A Stuxnet és a Duqu sikeressége, mindamellett, hogy *zero-day* sebezhetőségeket használtak ki, abban rejlett, hogy valós nagyvállalatok elektronikus aláírásaival rendelkeztek. A legtöbb operációs rendszer már a 2000-es években is ismerte az elektronikus aláírás fogalmát, és ha valaki olyan szoftvert szeretett volna telepíteni (tudtával vagy tudta nélkül), amely nem megbízható forrásból származik, vagyis nem rendelkezik hiteles aláírással egy, már ismerten megbízható szolgáltatótól, akkor csak nagy nehézségek árán lehetett feltelepíteni. A Stuxnet és a Duqu is használt megbízható szolgáltatóktól eltulajdonított aláírásokat. Míg a Stuxnet egy RealTek-aláírást használt, addig a Duqu a C-Media aláírását tulajdonította el. Mindkét cég rengeteg audiohardvert gyártott abban az időben személyi számítógépekhez, és a hardverükhöz kapcsolódó *driverszoftverekhez* használták az elektronikus aláírásokat.[47]

Napjaink támadásai

A *social media* platformok (Facebook, Twitter, LinkedIn), a különféle videómegosztó és streamingportálok (YouTube, Twitch, Videa), valamint a blogoldalak (Blogger.com, Wix) lehetőséget adnak, hogy minél több információt osszunk meg magunkról. Ezeket a felületeket pedig külső szemlélőként arra is használhatjuk, hogy eldöntsük valakiről, hogy milyen személyiség, megbízható-e, szeretnénk-e vele együtt dolgozni stb. Tehát ezen platformok alkalmasak arra, hogy bizalmat érezhessünk a *social* platformon megjelenő személy iránt.

[46] Baezner–Robin (2017): i. m.
[47] Bencsáth et al. (2012): i. m.

A bizalomépítésre épülő támadás egyik példája az Operation Newscaster, amelynek célja az volt a támadók részéről, hogy kormányzati tagok, nagyvállalatok vezető pozícióiban lévő személyek számítógépét fertőzzék meg. Ahhoz, hogy ezeknek az embereknek a közelébe kerüljenek, a támadóknak újságírói és kormányzati állásokat kellett szerezniük. Ez természetesen nem egyszerű feladat egy külföldi katonai feladatokat ellátó személynek sem. A támadók mögé tehát álszemélyiségeket építettek fel, akik rendszeresen használták a különböző *social platformokat,* így képesek voltak bizalmat kiépíteni a munkaadókkal, megbízható munkaerővé váltak. Az Operation Newscaster volt 2014-ben az addigi legnagyobb kiberkémkedés, amelyhez *social engineering* technikát alkalmaztak rendkívül magas szinten.[48]

Amellett, hogy a *social engineering* ekkora teret nyert a kibertámadások során, egy másik aspektusa is továbbfejlődött a hírszerzésnek. Méghozzá a nyomok eltüntetése és a hamis nyomok előállítása is fontos célként jelent meg; többször is előfordult, hogy a támadás elkövetésének gyanúja más nemzetre, hackercsoportra terelődött, sok esetben nem is sikerült feltárni az elkövetők pontos körét.

Utóbbi aspektusra kiváló példa a 2018-as téli olimpia során végrehajtott, és később False-flagnek keresztelt támadás, amely során a hackerek észak-koreai IP-címeket használtak a támadások során, hogy tovább fokozzák a már akkor is jelentős feszültséget Dél-Koreával szemben. Egyértelmű bizonyítékot azonban senki sem talált arra, hogy ki volt az elkövető, bár a politikai helyzet miatt elsősorban Oroszországot tekintik a támadó félnek.

A 2020-as évekre a felhőalapú szolgáltatások és az óriási méretű információs rendszerek száma megsokszorozódott. Számos nagyvállalat esetében megfigyelhető, hogy nem éri meg minden rendszert saját kézben tartani, helyette olyan szolgáltatók jöttek létre, amelyek egy cég vezetését segítve biztosítanak eszközöket (szoftvereket, mérnököket), hogy a vállalat rendszereit kezeljék.

Ezért is kavart akkora port a SolarWinds elleni támadás. A támadás célja továbbra is a magas beosztású vállalati személyek és kormánytagok lehallgatása és megfigyelése volt, de ebben az esetben nem konkrétan az adott személyeket keresték meg, vagy a vállalatokhoz/kormányzati szervekhez törtek be a támadók, hanem egy szolgáltató céget, a SolarWindset támadták meg, amely több mint 30 000 vállalat számára üzemeltetett és menedzselt IT-erőforrásokat. A támadás sikere abban rejlett, hogy nem magában a szoftverben helyeztek el vírust, hanem

[48] Siboni–Kronenfeld (2014): i. m.

egy frissítésben. A rendszereket természetesen időnként frissítik, javítják, hogy még jobban működjenek, és ha egy ilyen frissítésbe rosszindulatú kódot helyezünk el, akkor az egy idő után minden vállalathoz, aki a szolgáltatást igénybe veszi, eljut. További érdekessége volt a támadásnak, hogy a rosszindulatú programkód egy idő után törölte önmagát. Emiatt a SolarWinds szoftverét használó vállalatok nagy része soha sem tudja meg, áldozatul esett-e a támadásnak, vagy sem.[49]

A célok változása

Érdemes megfigyelni, hogyan változtak a hírszerzési műveletek céljai az évek előrehaladtával, elsősorban a technikai, technológiai fejlődés következtében. Azonban minél több szenzort és beavatkozó egységet kötnek a hálózatra vagy az internetre, annál bonyolultabb hírszerzési támadások valósulhatnak meg. A 2. ábra összefoglalja, hogy melyek a támadásokból azonosítható főbb célok.

2. ábra: A hírszerzési kibertámadások céljai
Forrás: a szerző szerkesztése

[49] Willett (2021): i. m.

a) *Dokumentumok, statikus adatok megszerzése.* Az internet korai fázisában elsősorban bizalmas dokumentumok gyűjtése volt a cél. A Moonlight Maze vagy a Titan Rain elsősorban titkos információk, dokumentumok megszerzésére irányult. Az így megszerzett dokumentumokat a támadó nemzet saját céljaira használta fel.
b) *Folyamatos megfigyelés.* Amint eljutottunk arra a pontra az internet és az eszközök fejlődése folyamán, hogy kamerákat és mikrofonokat telepítettek a számítógépekbe, a hackerek ezeket a perifériákat kihasználva képesek voltak valós idejű lehallgatásra és megfigyelésre is, mint a GhostNet- és a ShadowNet-támadások esetén.
c) *Befolyásolás.* A dokumentumokat és a lehallgatás eredményeit elsősorban belső célokra használták fel, de számos olyan támadást is végrehajtottak, amelynek célja a másik fél befolyásolása volt. A 2016-os amerikai választásokon például kibertámadások segítségével próbálták befolyásolni a választási eredményeket, illetve a választók döntését. Mindemellett fontos megemlíteni a különféle *social engineering* technikákat is, hiszen sok esetben ezek elsődleges célja és eszköze a befolyásolás (például Operation Newscaster).
d) *Beavatkozás, korlátozás és fizikai károkozás.* A katonai hírszerzéshez kapcsolódó műveletek egyre inkább kiegészülnek olyan eszközökkel, amelyek be akarnak avatkozni a rendszerek működésébe, korlátozni szeretnék a rendszereket, szolgáltatásokat, és fizikai károkat is megpróbálnak okozni. Az első ismert példa a Stuxnet, ahol az eszközök egy, az internettől elzárt hálózaton voltak megtalálhatók. Érdemes megjegyezni, hogy ezért is jelent kiberbiztonsági szempontból hatalmas kockázatot az IoT- (dolgok internete) és CPS-rendszerek (kiberfizikai rendszerek) terjedése napjainkban, ahol egyre több és több szenzort, illetve beavatkozó egységet szeretnénk hálózatba kötni.
e) *Káoszteremtés.* A kibertérben végzett katonai hírszerzés során nem csak konkrét dokumentumok eltulajdonítása vagy személyek lehallgatása jelenhet meg célként. A káoszteremtés is rendkívül fontos információval bír, hiszen segítségével megfigyelhető, hogy mely rendszerek sérülékenyek, milyen gyors az áldozat reakcióideje, illetve milyen fejlett helyreállítási stratégiával rendelkezik. Az Észtország ellen indított 2007-es szolgáltatásmegtagadásos támadás célja az ország kormányzati hálózatának blokkolása volt. De idesorolhatjuk a 2017-ben népszerűnek számító zsaroló vírusok megjelenését, ahol az adatlopások mellett ellehetetlenítették az áldozatok saját eszközeihez való hozzáférést is.

A védekezési mechanizmusok fejlődése

A támadások folyamatos fejlődése következtében természetesen a védekezési mechanizmusok is folyamatosan fejlődtek annak érdekében, hogy a korábbi esetek többször már ne fordulhassanak elő. Jelen fejezetben azt vizsgáljuk, hogy miként fejlődtek a védelmi mechanizmusok az évek/évtizedek során a feltérképezett kibertámadások következtében.

Az első vírusirtó 1987-ben került piacra McAfee néven.[50] A vírusirtók akkoriban elsősorban a kártékony programok lenyomatait egy adatbázisban tárolták. A vírusirtó olyan lenyomatokat keresett a számítógépeken, amelyek egyeztek valamely elemmel az adatbázisban.

Hálózati rendszerek már az internet előtt is léteztek (például: ARPANET), és kialakultak az első tűzfalak is a hálózat védelme érdekében. Érdekes tény, hogy az első tűzfal leírását szintén 1987-ben publikálták. A kezdeti tűzfalak egyszerűen működtek: egy hozzáférési listát tartottak fent azokkal az IP-címekkel, ahonnan a hálózat tagjai fogadhattak üzenetet. A tűzfal működés közben ellenőrzött minden csomagot, amely a hálózathoz érkezett, és megvizsgálta, hogy a listában megtalálható címről érkezett-e az üzenet.[51]

Mindezek csak kezdetleges védekezési mechanizmusok voltak, és, mint ismerjük a történelmet, a támadó csoportok mindig egy lépéssel a fejlesztők előtt jártak.

Az Egyesült Államokban több, nem célzottan katonai hírszerzési célú kibertámadás is történt, az azonban egyértelművé vált, hogy az ország kritikus infrastruktúrái veszélynek vannak kitéve a kibertámadásokkal szemben. Ennek következménye volt az 1997-ben végrehajtott Eligible Receiver projekt, amely, jelenlegi terminológiánk szerint, célzott sérülékenységvizsgálat volt. Etikus hackerek első alkalommal támadták meg szándékosan országuk belső infrastruktúráit, hogy felkészülhessenek a lehetséges kibertámadásokra.[52] Sajnos a felkészülés nem volt tökéletes, hiszen mint utóbb kiderült, a Moonlight Maze támadás már 1996-tól tulajdonított el dokumentumokat az Egyesült Államokból.

[50] Jeffrey S. Kline: *McAfee Associates, Inc. Competitive Strategies for the Computer AntiVirus Industry.* 1998.

[51] Kenneth Ingham – Stephanie Forrest: *A History and Survey of Network Firewalls.* Technical Report. Albuquerque, University of New Mexico, 2002-37.

[52] James Adams: Virtual defense. *Foreign Affairs,* 80. (2001), 3. 98–112.

A kibervédelem felmérésének következő jelentős pontja a 2002-ben kivitelezett Digital Pearl Harbour[53] gyakorlat, sérülékenységi vizsgálat volt, összekötve azonnali védekezési stratégiákkal: kiberháborút szimulálva bizonyíthatóvá vált, hogy kiberterroristák súlyos gazdasági és társadalmi problémákat okozhatnak. Biztonsági szakértők egy csoportja azt a feladatot kapta, hogy tervezzen meg 4 különböző iparág elleni támadást.

2008-ban az Egyesült Államok elszenvedte az addigi legnagyobb katonai hírszerzési támadást, amikor a Közel-Keleten egy amerikai katonai laptopba helyezett adathordozó segítségével rengeteg titkos információt tulajdonítottak el. Az Egyesült Államok ennek hatására riadót fújt a kibertámadás kivédésével kapcsolatban. Az Operation Buckshot Yankee hadművelet fordulópontot jelentett az amerikai kibervédelmi stratégiában. Az akció során többrétegű és robusztus katonai védelmi hálózatot építettek a Pentagon köré. A Pentagon ettől a ponttól kezdve szorosan együttműködik az NSA-vel, hogy együttes erővel védjék és ellenőrizzék a kormányzati hálózatokat és kritikus infrastruktúrákat. A védelmi stratégiát az USA a legközelebbi szövetségeseire is kiterjesztette.

Ez a fajta törekvés 2013-ra eljutott arra a pontra, hogy a NATO védelmi miniszterei megegyeztek abban, hogy az együttműködésben részt vevő tagállamok által üzemeltetett hálózatokhoz kapcsolódó kibervédelmi intézkedések szintén összefogást igényelnek, hiszen ha az egyik tagállam kibertámadást szenved, más tagállamok is könnyű célponttá válhatnak. Hozzátéve azt is, hogy a megegyezés előtti évben, 2012-ben több mint 2500 szignifikáns kibertámadás történt a NATO területén belül, azonban egyik támadás sem járt sikerrel.[54]

Konklúzió és jövőbeli kitekintések

Ebben a fejezetben történeti áttekintést adtunk a kibertérben megvalósuló katonai hírszerzésről az internet és a számítógépek létrejöttekor megismert támadásoktól kezdve egészen napjaink támadásaiig. Megvizsgáltuk, hogy miképpen változtak a hírszerzési technikák az idő előrehaladtával, illetve bemutattuk, hogy milyen

[53] Eric Purchase – Caldwell French: Digital Pearl Harbor: A Case Study in Industry Vulnerability to Cyber Attack. In *Guarding Your Business.* Boston, Springer, 2004. 47–64.

[54] Liu Yi: The Thoughts On Our Army Security Management of Removable Mass Storage Device. *Information Security and Technology,* (2012), 10.

stratégiák és fontosabb döntések történtek a kibervédelem megvalósítása során, hogy az esetleges támadásokat a nemzetek képesek legyen elhárítani.

A történeti áttekintést az 1998-ban azonosított Solar Sunrise esetével kezdtük, majd tovább vizsgáltuk a kibertérben azonosított támadásokat, így például az első szolgáltatásmegtagadásos támadást, zsaroló vírusokat, teljes megfigyeléssel és lehallgatással kapcsolatos eseteket, egészen a napjainkban történt eseményekig, mint a SolarWindset és a Microsoft Exchange-et érintő hírszerző támadások.

Ezt követően a történeti áttekintés során megvizsgált támadások sikerességét azonosítottuk. Jól látható, hogy a támadások folyamatosan fejlődtek az évek alatt, így minden egyes támadás valamiben új és egyedi megoldást alkalmazott. Továbbá az egyes támadások során más és más aspektusban fejlődtek. Ezek alapján megismerkedtünk többek között az első támadási technikákkal, a videós és audiós megfigyelésekkel, valamint az olyan támadásokkal, amelyek fizikai károkat is képesek voltak okozni.

Bemutattuk, hogyan változtak a támadók céljai a technika fejlődése során. Míg korábban csak titkos anyagok, dokumentumok jelentették a támadások céljait, később jellemzővé váltak a megfigyeléssel kapcsolatos támadások, illetve a káoszteremtésből megszerezhető információgyűjtés is.

Végül azonosítottuk a védekezéssel kapcsolatos lépéseket: az 1997-es Eligible Receiver projekttel kezdtük tanulmányozni, majd a különböző sarkalatos pontok alapján létrejövő események keretében láthattuk, ahogy a NATO tagjai egységesen lépnek fel a kibertérben megvalósuló katonai hírszerzés ellen. 2016-ban a NATO kijelentette, hogy az operatív hadviselés területét kiterjeszti a kibertérre is.

Összességében elmondható, hogy a bemutatott támadások és a hozzájuk kapcsolódó védelmi döntések már részét képezik történelmünknek, és formálták a világot is, hogy eljussunk oda, ahol jelenleg is tartunk.

Jövőbeli kitekintés

Egyértelmű, hogy ez még csak a kezdet; olyan új technológiák születnek napjainkban, mint a dolgok internete (IoT), a kiberfizikai rendszerek (CPS), az okosvárosok *(smart cities),* amelyek középpontjában a különböző információs eszközök közötti kommunikáció áll.

Ezen technológiák esetében különböző szenzorok adatokat (kép, hang, hőmérséklet, koordináta) szolgáltatnak egy központi (elosztott) irányítás számára,

amely képes utasítani a rendszerhez kapcsolt beavatkozókat. Az eszközök minden esetben egyetlen hálózaton találhatóak, ahol maga a hálózat lehet nyitott, vagyis kapcsolódik az internetre, vagy zárt, tehát az internettől elzárt.

3. ábra: Az IoT-rendszerek koncepciója
Forrás: Zigurat: *What Do the Next Five Years Hold for the IoT?* é. n.

A korábban bemutatott támadások között voltak olyanok, amelyek nyitott és zárt hálózatokon keresztül is képesek voltak információkat szerezni, illetve egyéb károkat okozni. Látható, hogy a jövő technológiái is nagy veszélyben vannak, illetve szinte biztosra vehető, hogy ezeket a technológiákat is képesek lesznek a hírszerző támadások a saját irányításuk alá vonni.

Míg napjainkban a különféle platformok leginkább információt gyűjtenek (például: Google, Facebook stb.), és a felhasznált adatokat egy-egy mesterséges intelligencia által kezelt támogató rendszer számára továbbítják (az általunk megadott adatokból a mesterséges intelligencia képes mintákat felfedezni, és következtetéseket levonni arra vonatkozóan, hogy mit szeretünk csinálni, mit fogunk a jövőben tenni stb.), addig a jövőben egyre több beavatkozó egység is a hálózatra lesz kapcsolva, amely ténylegesen képes lesz befolyásolni a környezetét.

A károkozás, valamint a káoszteremtés így sokkal nagyobb méreteket is ölthet (például: önvezető autókat hamis információval manipulálva tetszőleges helyre irányíthatók), illetve azáltal, hogy minél több szenzort kapcsolunk az internetre, saját magunkról szolgáltatunk egyre több és több információt a hírszerzők számára.

A kibervédelem szempontjából a legfőbb cél, hogy ne engedjük meg, hogy harmadik fél képes legyen beleszólni az eszközök közötti kommunikációba.

Összegezve: a jövő egyik legfontosabb kérdése, hogy az eszközök közötti kommunikációs csatornákat a nemzetek mennyire lesznek képesek biztonságossá tenni, illetve ha mégis történik behatolás, milyen gyorsan képesek azokat azonosítani, kezelni, és az okozott károkat helyreállítani.

Irodalomjegyzék

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

Adair, Steven et al.: *Shadows in the Cloud: Investigating Cyber Espionage 2.0.* A Joint Report of the Information Warfare Monitor and Shadowserver Foundation. Toronto, 2010. április 6.

Adams, James: Virtual defense. *Foreign Affairs,* 80. (2001), 3. 98–112. Online: https://doi.org/10.2307/20050154

Baezner, Marie – Patrice Robin: Stuxnet. *ETH Zurich,* 4. (2017). Online: https://doi.org/10.3929/ethz-b-000200661

Bencsáth Boldizsár – Buttyán Levente – Pék Gábor – Félegyházi Márk: Duqu: Analysis, Detection, and Lessons Learned *ACM European Workshop on System Security (EuroSec)*, 2012. Online: www.hit.bme.hu/~buttyan/publications/BencsathPBF12eurosec.pdf

Börcsök András – Vida Csaba: A nemzetbiztonsági szolgálatok rendszere. (Nemzetközi gyakorlat a nemzetbiztonsági rendszer kialakítására.) *Nemzetbiztonsági Szemle,* 2. (2014), 1. 63–100. Online: http://epa.oszk.hu/02500/02538/00002/pdf/EPA02538_nemzetbiztonsagi_szemle_2014_01_063-100.pdf

Charette, Robert N.: DoD Admits to Being Severely Hacked. *IEEE*, 2008. Online: https://spectrum.ieee.org/riskfactor/computing/it/dod_admits_to_being_severely_h

Deák Veronika: Kártékony programok terjedése social engineering technikákon keresztül. *Hadmérnök,* 14. (2019), 2. 256–271. Online: https://doi.org/10.32567/hm.2019.2.21

Deibert, Ronald J. – Rafal Rohozinski: Tracking GhostNet: Investigating a Cyber Espionage Network. *Information Warfare Monitor,* 2009. március 29. Online: https://bit.ly/3OfhOnA

Dobák Imre: *A nemzetbiztonság általános elmélete*. Budapest, Nemzeti Közszolgálati Egyetem Nemzetbiztonsági Intézet, 2014.

Faou, Matthieu – Mathieu Tartare – Thomas Dupuy: Exchange Servers Under Siege From at Least 10 Apt Groups. *WeLiveSecurity,* 2021. március 10. Online: www.welivesecurity.com/2021/03/10/exchange-servers-under-siege-10-apt-groups/

Fehér Krisztián: *Kezdő hackerek kézikönyve*. Budapest, BBS-INFO, 2016.

Füzesi Ottó: *A felderítés elméleti és gyakorlati kérdéseinek vizsgálata, különös tekintettel, az emberi erővel folytatott felderítésére.* Doktori (PhD-) értekezés. Zrínyi Miklós Nemzetvédelmi Egyetem, 2004. Online: https://bit.ly/3n5MTOK

Gyányi Sándor: DDOS támadások veszélyei és az ellenük való védekezés. *Hadmérnök,* (2007), különszám. 1788–1919. Online: http://hadmernok.hu/kulonszamok/robothadviseles7/gyanyi_rw7.html

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

Haig Zsolt – Kovács László: *Kritikus infrastruktúrák és kritikus információs infrastruktúrák*. Budapest, Nemzeti Közszolgálati Egyetem, 2012.

Haraway, Donna: A Cyborg Manifesto: Science, Technology and Socialist-Feminism in the Last Twentieth Century. In Donna Haraway: *Simians, Cyborgs and Women: The Reinvention of Nature.* New York, Routledge, 1991. 149–181.

Ingham, Kenneth – Stephanie Forrest: *A History and Survey of Network Firewalls.* University of New Mexico, Tech. Rep., 2002.

Izsa Jenő: A hírszerzés céljáról és rendszeréről. *Hadtudomány,* 19. (2009), 1–2. 72–83. Online: www.mhtt.eu/hadtudomany/2009/1_2/072-083.pdf

Knapp, Kenneth J. – William R. Boulton: Cyber-Warfare Threatens Corporations: Expansion Into Commercial Environments. *Information Systems Management,* 23. (2006), 2. 76.

Kovács László: Az információs terrorizmus eszköztára. *Hadmérnök,* (2006), különszám. Online: https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/2062/kovacs_rw6.pdf?sequence=2

Kovács László: *Biztonságpolitika: a kibertérben*. Budapest, Nemzeti Közszolgálati Egyetem, 2019.

Kovács László – Krasznay Csaba: „Mert övék a hatalom”: Az internet politikát (is) befolyásoló hatása a 2016-os amerikai elnökválasztás során. *SVKK Elemzések,* (2017), 9. Online: https://bit.ly/3Ox1FKi

Kumar, Animesh: Zero Day Exploit. *SSRN,* 2014. január 14. Online: https://doi.org/10.2139/ssrn.2378317

Leonov, Pavel Y. et al.: The Main Social Engineering Techniques Aimed at Hacking Information Systems. *2021 Ural Symposium on Biomedical Engineering, Radioelectronics and Information Technology (USBEREIT),* IEEE, 2021. 0471–0473.

Magyar Hadtudományi Lexikon. Budapest, Magyar Hadtudományi Társaság, 1995.

Marks, Joseph: The Cybersecurity 202: Russia's False Flags in Winter Olympics Cyberattack Herald a More Complicated Future. *The Washington Post,* 2019. október 21. Online: https://wapo.st/3OwdiRu

Mészáros Rezső: A kibertér társadalomföldrajzi megközelítése. *Magyar Tudomány,* 48. (108.) (2001), 7. 769–779. Online: http://epa.oszk.hu/00700/00775/00032/769-779.html

MITRE ATT&CK: Groups. 2021. Online: https://attack.mitre.org/groups/G0010/

Morgan Swartley: Political Marketing: How Social Media Influenced the 2008–2016 US Presidential Elections and Best Practices Associated. *Senior Honors Theses,* 726. 2018. szeptember 4. Online: https://digitalcommons.liberty.edu/honors/726/

Mwiki, Henry et al.: Analysis and Triage of Advanced Hacking Groups Targeting Western Countries Critical National Infrastructure: APT28, RED October, and Regin. In *Critical Infrastructure Security and Resilience. Advanced Sciences and Technologies for Security Applications*. Springer, Cham, 2019. Online: https://doi.org/10.1007/978-3-030-00024-0_12

Nakashima, Ellen: Chinese Hackers Who Breached Google Gained Access to Sensitive Data, U.S. Officials Say. *The Washington Post,* 2013. május 20. Online: https://wapo.st/3xOCmfK

Orman, Hilarie: The Morris Worm: A Fifteen-Year Perspective. *IEEE Security & Privacy,* 1. (2003), 5. 35–43.

Purchase, Eric – French Caldwell: Digital Pearl Harbor: A Case Study in Industry Vulnerability to Cyber Attack. In Sumit Ghosh – Manu Malek – Edward A. Stohr (szerk.): *Guarding Your Business. A Management Approach to Security.* Boston, Springer. 47–64. Online: https://doi.org/10.1007/0-306-48638-5_4

Rubenstein, Dana: *Nation State Cyber Espionage and its Impacts.* Washington University in St. Louis, 2014. december 1. Online: www.cse.wustl.edu/~jain/cse571-14/ftp/cyber_espionage/

Siboni, Gabi – Sami Kronenfeld: Iranian Cyber Espionage: A Troubling New Escalation. *INSS Insight,* 2014. június 16. Online: www.inss.org.il/publication/iranian-cyber-espionage-a-troubling-new-escalation/

Tsague, Hippolyte Djonon – Bheki Twala: *Reverse Engineering Smart Card Malware Using Side Channel Analysis With Machine Learning Techniques.* IEEE International Conference on Big Data (Big Data), 2016. 3713–3721. Online: https://doi.org/10.1109/BigData.2016.7841039

Ushmani, Azhar: Cyberwarfare History and APT Profiling. Advance Online Publication. *International Journal of Computer Science Trends and Technology (IJCST),* 7. (2019), 4. Online: www.ijcstjournal.org/volume-7/issue-4/IJCST-V7I4P1.pdf

Villeneuve, Nart – David Sancho: *The "lurid" downloader.* Trend Micro Incorporated, 2011.

Willett, Marcus: Lessons of the SolarWinds Hack. *Survival,* 63. (2021), 2. 7–26. Online: www.iiss.org/blogs/survival-blog/2021/04/lessons-of-the-solarwinds-hack

Yaqoob, Ibrar et al.: The Rise of Ransomware and Emerging Security Challenges in the Internet of Things. *Computer Networks,* 129. (2017). 444–458. Online: https://doi.org/10.1016/j.comnet.2017.09.003

Yi, Liu: The Thoughts On Our Army Security Management of Removable Mass Storage Device. *Information Security and Technology,* (2012), 10.

Zigurat: What Do the Next Five Years Hold For the IoT? é. n. Online: www.e-zigurat.com/innovation-school/blog/what-do-the-next-five-years-hold-for-the-iot/

5. fejezet

A proxycsoportok alkalmazásának taktikája: a hacktivisták

Krasznay Csaba

Bevezetés

A 2007-es Észtország ellen végrehajtott kibertámadás sok tekintetben egészen új helyzetet teremtett a kibertéri műveletek világában. Jelen fejezet szempontjából talán az attribúció körüli polémiát érdemes kiemelni. A nemzetközi sajtó és a politika ugyanis szinte azonnal Oroszországot mint államot vélte felfedezni a támadás mögött, az orosz kormányzat viszont akkor és azóta is folyamatosan tagadja a részvételét a műveletben. Rain Ottis, Észtország egyik legismertebb kiberbiztonsági szakértője 2008-ban így foglalta össze a rendelkezésre álló tényeket:

> „Az orosz kormány folyamatosan tagadta direkt részvételét a kibertámadásban, amely kiütötte Észtországot 2007 tavaszán. A szerző tudomása szerint ez az állítás igaz. De meg kell jegyezni, hogy semmilyen bizonyíték nem áll rendelkezésre arra vonatkozóan, hogy az orosz kormányzat bármit is tett volna a helyzet megoldása érdekében. Az észt nyomozással kapcsolatos együttműködés hiánya arra utal, hogy az orosz kormány nem volt érdekelt a támadók kilétének felfedésében, így röviden szólva védte őket. Más szavakkal a politikai elit által alkalmazott ellenséges retorika arra ösztönözte az embereket, hogy támadják Észtországot, és semmit nem tettek annak érdekében, hogy ezt a támadást leállítsák. Ez a csendes támogatás pedig úgy értelmezhető mint egyfajta implicit állami támogatás, mivel a retorziótól való félelem hiányában szabadon lehetett támadni az észtországi célpontokat."[1]

Ottis azt is hozzáteszi, hogy a támadás végrehajtásával kapcsolatos információkat orosz nyelvű fórumokon osztották meg egymás között a résztvevők. Ezeken pontosan meg volt határozva a célpont, az időzítés, a végrehajtás módja, valamint az ideológiai motiváció is. A támadást végül a Nasi („Mieink") ifjúsági

[1] Rain Ottis: *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective*. Cooperative Cyber Defence Centre of Excellence, 2008. március 2.

https://doi.org/10.36250/01079_05

https://orcid.org/0000-0003-3216-2592

mozgalom aktivistája, Konsztantyin Goloskokov vállalta magára, tagadva, hogy bármilyen utasítást kapott volna az orosz hivatalos szervektől.[2] Érdekesség, hogy 2016-ban az ukrán biztonsági szervek már mint az orosz katonai titkosszolgálat, a GRU, azaz az Oroszországi Föderáció Fegyveres Erői Vezérkarának Felderítő Főcsoportfőnöksége tisztjeként hivatkoznak Goloskokovra.[3]

A *Meduza* nevű orosz oknyomozó portál tényfeltáró riportja a támadás végrehajtásának koordinátoraként Pjotr Levasovot nevezi meg, aki „főállásban" az egyik legnagyobb kéretlen levélküldő szolgáltatást, a Kelihost üzemeltette, amíg 2017-ben az FBI nyomozása után le nem tartóztatták Barcelonában. A *Meduza* forrásai szerint Levasov legalább 2005 óta együttműködött az orosz állami szervekkel, és aktívan támogatta bizonyos műveleteit a Kelihos infrastruktúráját felhasználva.[4] Ezért cserébe érinthetetlen volt, így bár az amerikai nyomozóhatóság már 2007-ben vádat emelt ellene, 10 éven keresztül lehetetlen volt elfogni.[5]

Érdemes még megemlíteni Danyiil Turovszkij, a *Meduza* újságírójának orosz hackerekről szóló könyvének egy bekezdését, ahol a 2000-es évek közepének történéseit dolgozza fel, beleértve a 2007-es incidenst is. Ebben az időben egy Anton Moszkal nevű szentpétervári programozót keresett fel a belbiztonsági és kémelhárítási feladatokat ellátó Szövetségi Biztonsági Szolgálat, az FSZB munkatársa, és arról beszélt neki, hogyan lehetne küzdeni a „terrorista-weboldalak ellen", illetve mit jelent számára a patriotizmus. Bár a megkeresés félrement, a fentiek egyértelműen jelzik, hogy a 2000-es évek közepétől az orosz biztonsági szervek aktívan keresték a kapcsolatot a hazafias érzelmeket tápláló hackerekkel és kiberbűnözőkkel.[6]

[2] Christian Lowe: Kremlin Loyalist Says Launched Estonia Cyber-Attack. *Reuters,* 2009. március 13.

[3] UCMC Press Center: Security Service of Ukraine Possesses Audio Records of Krasnov's Conversations With His Russian Supervisor. 2016. március 3.

[4] Daniil Turovsky: "It's Our Time to Serve the Motherland." How Russia's War in Georgia Sparked Moscow's Modern-Day Recruitment of Criminal Hackers. *Meduza,* 2018. augusztus 7.; Department of Justice of Public Affairs: *Russian National Who Operated Kelihos Botnet Pleads Guilty to Fraud, Conspiracy, Computer Crime and Identity Theft Offenses* (2018. szeptember 12.).

[5] United States District Court: *United States Versus Peter Yuryevich Levashov* (2017. április 4.).

[6] Danyiil Turovszkij: *Orosz hekkerek.* Budapest, Athenaeum, 2020. 143.

A hacktivizmus alapvető fogalmai

Játsszunk el egy pillanatra azzal a gondolattal, hogy ismerve az események utáni közel 15 év történetét és az orosz kibertéri műveletek fejlődését talán a 2007-es esemény mégis egyfajta offenzív katonai kiberművelet volt, és nem tisztán az állampolgári elégedetlenség szülte azt! Tételezzük fel, hogy az orosz katonai vezetés már a korai 2000-es években felismerte annak lehetőségét, hogy az ország stratégiai érdeke megkívánja az információs műveletek során azokat az akciókat, amelyeket nem lehet közvetlenül összekötni a kormányzattal, hanem azokat látszólag független személyekre és csoportokra bízza! Amennyiben így történt, Oroszország sikerrel alkalmazta a fizikai hadviselésből jól ismert proxycsoportok taktikáját. Ráadásul nem is elsőként tette ezt, ahogy látni fogjuk, de a téma megértéséhez tisztázni szükséges néhány alapfogalmat!

Proxycsoportok a kibertérben. Michael N. Schmitt és Liis Vihul, a kiberhadviselés legismertebb nemzetközi jogi szakértői szerint akkor beszélhetünk proxycsoportokról a kibertérben, ha egy nem állami szereplő az adott állam utasításai szerint cselekszik, vagy az adott állam kontrollálja, illetve irányítja a nem állami szereplő cselekedeteit, kivéve akkor, ha az állami szereplő túllépi a hatáskörét, és úgy befolyásolja a nem állami szereplőket. Ha tehát „rendes ügymenet" szerint egy állami titkosszolgálat hatással van egy hackerre, kiberbűnözői csoportra, laza, informális csoportra, vállalatra vagy akár egy terrorista-, felkelőcsoportosulásra proxyműveletről beszélhetünk. A lényeg, hogy bár mindezt esetileg kell megítélni, legyen egyértelmű irányítási kapcsolat az állam és a nem állami szereplő között.[7]

Hacktivizmus. A fogalom magyarázatára számos forrást lehet találni, de érdemes visszamenni az ősforrásig, amely így határozza meg a hacktivizmust: „Az emberek felhatalmazásának célként való kitűzése, hogy a világ tudomást szerezzen az igazságtalanságokról, az emberi jogok megsértéséről. Más szóval, az információáramlás megszervezése világszerte, korlátozások és cenzúra nélkül. Ez a hacktivizmus." A hacktivizmus szó Omegától származik, a fogalmat pedig Count Zero írta le. Oxblood Ruffin így egészítette ezt ki: „a technológia használata az elektronikus médián keresztül az emberi jogok fejlesztése érdekében." Mindhárman a *Cult of the Dead Cow* (cDc) nevű hackercsapat tagjai

[7] Michael N. Schmitt – Liis Vihul: Proxy Wars in Cyberspace. *Fletcher Security Review,* 1. (2014), 2. 54–73.

voltak, a fogalom maga pedig az 1990-es évek közepén alakult ki, amikor a cDc igen aktív közéleti tevékenységet is folytatott.[8]

Hacktivista. Az előző gondolatmenet alapján következik, hogy a hacktivista az, aki részt vesz a hacktivizmusban. A 90-es évek óta viszont annyiféle megjelenését láttuk a hacktivistamozgalmaknak, hogy érdemes tágabban értelmezni a résztvevőket! Tim Jordan és Paul Taylor hacktivizmust feldolgozó könyvében így írja le a jelenséget:

> „A hacktivizmus a népszerű politikai akciók továbbfejlődése, embercsoportok saját akciói a kibertérben. A politikai tiltakozások és a számítógépes hackelés kombinációja. A hacktivisták a kibertér keretein belül működnek, küzdenek a virtuális életben technikailag lehetséges dolgokért, és kinyúlnak a kibertérből, a virtuális erők felhasználásával alakítják az offline életet. A társadalmi mozgalmak és a népi tiltakozás a 21. századi társadalmak szerves részét képezik. A hacktivizmus tulajdonképpen az aktivizmus elektronikussá válása."[9]

Hacktivista tehát az, aki egy politikai ideológia mentén szervezett kibertéri akcióban vesz részt, amelynek hatása van a fizikai világra is.

Patrióta vagy hazafias hacker. A katonai kiberműveletek szempontjából nagyon fontos csoportot alkotnak a hacktivistákon belül a patrióta vagy hazafias hackerek. Athina Karatzogianni hacktivizmusról szóló könyvében úgy írja körbe a patrióta hackereket, mint akik a nemzetük tisztaságáért küzdenek az online média ügyes felhasználásával. Paradox módon tehát a nacionalizmus mint politikai ideológia jelenik meg a klasszikus hacktivista akciók mögött, kihasználva az internetet mint globális médiát.[10]

Hacktivistacselekmény. A hacktivistaakciók eszköztára közel sem annyira összetett, mint amilyet egy kiváló műveleti tervező képességekkel rendelkező állami szereplő kivitelezni tudna. A hacktivistacsoportok ereje ráadásul a láthatóságban van, így nem érdekeltek abban, hogy a művelet rejtve legyen, illetve tipikusan csoportosan követik el a cselekményt, sokszor egymást nem is ismerve, akár nagyon eltérő földrajzi helyekről. A konspiráció tehát nem feltétlen cél. Romagna összefoglalója alapján így egy hacktivistacselekmény jellemzően az elosztott túlterheléses támadásokra (DDoS), a weboldalak átírására *(defacement)*

[8] Oxblood Ruffin: Hacktivism: From Here to There. *Threatpost,* 2010. december 9.

[9] Tim Jordan – Paul A. Taylor: *Hacktivism and Cyberwars. Rebels with a cause?* New York, Routledge, 2004. 1.

[10] Athina Karatzogianni: *Firebrand Waves of Digital Activism 1994–2014: The Rise and Spread of Hacktivism and Cyberconflict*. Basingstoke, Palgrave Macmillan, 2015. 22.

és az adatlopásra korlátozódik. Időnként előfordulhat kártékony kódok alkalmazása, de ennek meglehetősen negatív visszhangja van a közösségben.[11]

Hacktivizmus a *Tallinni kézikönyv* szerint

A proxycsoportok alkalmazásának tilalma a kibertéri műveletek során egyértelműen megjelenik az ENSZ 2012–2013 között működő Group of Governmental Experts (GGE) csoportjának zárójelentésében. A GGE feladata a tagállamok konszenzusát elérni bizonyos alapvető kibertéri szabályok és normák tekintetében. Az A/68/98 számú ENSZ-határozat 23. pontja világosan megfogalmazza ezt az elvárást:

> „Az államoknak teljesíteniük kell azon nemzetközi kötelezettségüket, hogy a nemzetközi jogot sértő cselekmények nekik legyenek tulajdoníthatók. Az államok nem használhatnak proxykat a nemzetközi jogot sértő cselekmények elkövetése során. Az államoknak biztosítaniuk kell azt, hogy a területüket ne használhassák olyan nem állami szereplők, akik jogtalanul használják az infokommunikációs technológiákat."[12]

Természetesen a fenti követelmény esetén is az ördög a részletekben rejlik. Egyrészt, nem egyértelmű, hogy hol is van a határa a nemzetközi jogot sértő cselekményeknek. Másrészt, igen nehezen bizonyítható, hogy az állam ténylegesen kontrollálta-e a nem állami szereplőt a cselekmény végrehajtása során. Harmadrészt, az internet határtalan, tehát a proxycsoportoknak nem feltétlenül kell abban az országban működnie, ahonnan az utasításokat kapják, a fogadó ország pedig nem biztos, hogy rendelkezik olyan képességekkel, amelyekkel meg tudja akadályozni a nemzetközi jogba ütköző cselekmény végrehajtását.

A *Tallinni kézikönyv* azért kísérletet tesz arra, hogy pontosítsa a proxycsoportok, ezen belül is a hacktivisták alkalmazásának szabályait. Legpontosabban a 17. szabály fogalmazza meg azt a követelményt, amelyet korábban már ismertettünk, egyben a GGE-határozat lényegét is tartalmazza. Eszerint tehát a kiberműveleteket végrehajtó nem állami szereplők tevékenysége akkor tulajdonítható egy államnak, amikor azok az állami szereplő utasításai szerint

[11] Marco Romagna: Hacktivism: Conceptualization, Techniques, and Historical View. In Thomas J. Holt – Adam M. Bossler (szerk.): *The Palgrave Handbook of International Cybercrime and Cyberdeviance*. London, Palgrave Macmillan, 2020.

[12] ENSZ: Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Document A/68/98 (2013. június 24.).

cselekszenek, illetve irányítása és kontrollja alatt állnak, valamint az állami szereplő tudomásul veszi és felhasználja a műveletet saját céljai érdekében.[13]

A 69. szabály próbálja meghatározni, hol kezdődik a nemzetközi jogot sértő cselekmények határa. Eszerint a kiberműveletek erőszakos cselekménynek minősülnek, amennyiben azok mértéke és hatása összehasonlítható az erőszakos cselekménynek minősülő nem kibertéri műveletekkel. A magyarázatban az szerepel, hogy például egy hacktivistacsoportnak pusztán a finanszírozása nem minősül erőszakos cselekménynek, abban az esetben, ha az adott csoport egy felkelés részese egy másik ország ellen.[14] Ez magyarázatot ad arra, hogy miért lehet hasznos az olyan országon belüli hacktivistacsoportok támogatása, mint például a CyberBerkut, egy Ukrajnán belül működő oroszbarát csoportosulás, amely aktívan kivette a részét a Kelet-Ukrajnában zajló fegyveres konfliktus kibertéri részéből.[15]

A 82. szabály tovább pontosítja, hogy egy kibertéri művelet milyen esetben minősül fegyveres konfliktusnak, és hol van a helye mindebben a hacktivistacsoportoknak. Fegyveres konfliktusról akkor beszélünk, amikor ellenséges cselekmények történnek két állam között, beleértve ebbe akár a pusztán kiberműveleteket alkalmazó akciókat is. A szabály magyarázata szerint az Észtországgal szemben végrehajtott művelet nem minősül fegyveres cselekménynek, mivel nincsen bizonyíték arra, hogy az abban részt vevő személyek valamely állam iránymutatása szerint cselekedtek volna, illetve valamely állam szervezte vagy jóváhagyta volna a műveletet. Ráadásul kérdéses, hogy egyáltalán volt-e fegyverhasználat, tehát a bevetett eszközök kiberfegyvernek minősülnek-e. A magyarázatból látszódik tehát, hogy bár számos jel utal titkosszolgálat által összehangolt műveletre, bizonyítékok hiányában a nemzetközi jog alapján nem lehetett eszkalálni a válaszadást.[16]

A 95. szabály szerint ráadásul egy fegyveres konfliktusban mindaddig civilnek kellene tekinteni egy személyt, ameddig egyértelműen be nem bizonyosodik, hogy az illető nem civil. Egy hacktivista esetében éppen ezért különösen nehéz bármilyen ellenintézkedést foganatosítani mindaddig, amíg direkt módon részt

[13] Michael N. Schmitt (szerk.): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge, Cambridge University Press, 2017. 94.

[14] Schmitt (2017): i. m. 330.

[15] Nikolay Koval: Revolution Hacking. In Kenneth Geers (szerk.): *Cyber War in Perspective: Russian Aggression against Ukraine*. Tallinn, NATO CCD COE Publications, 2015. 55–58.

[16] Schmitt (2017): i. m. 379.

nem vesz az ellenséges tevékenységben.[17] A 97. szabály szerint viszont a direkt részvétel megfosztja őt a civil státusztól. A magyarázat szerint, ha például egy hacktivista többször egymás után is megpróbál megtámadni egy vezetési pontot, mindaddig támadható marad, ameddig a támadásokat elköveti, tehát nemcsak a konkrét támadás idején, hanem a támadások között is. Sőt, amennyiben fennáll a lehetősége annak, hogy támadásait folytatni fogja hosszabb kihagyás után is, mindaddig célpont maradhat, ameddig a műveleti képessége fennmarad.[18]

A hacktivizmus gyökerei

Ahogy láthattuk, a *Tallinni kézikönyv* már tényként kezeli a hacktivistacsoportok offenzív kibertéri felhasználását, hosszú volt azonban az út, amíg idejutottunk. Érdemes tehát röviden áttekinteni, hogyan alakult ki a hackerszcéna, milyen fázisokon ment át a hacktivizmus, és hogyan kapcsolódtak ezek a csoportok az állami szereplőkhöz! Ahogy a történelmi áttekintésben látni fogjuk, Oroszország katonai szervei egyáltalán nem véletlenül kerültek közel ezekhez a csoportokhoz, de nem elsőként használták ki a bennük rejlő potenciált.

Maga a hackelés fogalma több évtizedre tekint vissza. A *hacking* szó eredeti jelentése valaminek a véletlenszerű levágását jelenti nehéz ütésekkel, és már az 1200-as évek Angliájában használták. Modern értelmében először 1955-ben írták le a Massachusetts Institute of Technology (MIT) modellvasútklubjának jegyzőkönyvében: „Mr. Eccles kéri, hogy bárki, aki az elektromos rendszeren dolgozik, vagy azt hackeli, legyen szíves lekapcsolni az áramot, hogy a biztosíték ne égjen le."[19] A „hackelés" ezen az egyetemen ettől kezdve azt jelentette, hogy valaki egy technikai problémán dolgozik szokatlan, kreatív megoldásokat keresve. Magyarul talán a buherálás, berhelés szavakkal lehetne a legjobban lefordítani. Nem meglepő módon a kifejezést elsősorban a *signals and power subcommitte*-ban, azaz az irányítástechnikai csoportban használták, innen ered az, hogy a *hackinget* a modellvasút minél hatékonyabb irányításának kifejezésére használták. Mivel a számítógépek civil környezetben elsők között az MIT-n jelentek meg, és ezekhez elsősorban azok a diákok fértek hozzá, akik szabadidejükben a modellvasutakat „programozták", törvényszerűen a hackelés kifejezés tőlük

[17] Schmitt (2017): i. m. 424.
[18] Schmitt (2017): i. m. 428.
[19] Ben Yagoda: A Short History of "Hack". *The New Yorker,* 2014. március 6.

ragadt át az informatika világára is. Nekik köszönhetjük egyébként a hackeretikát és az egész „cyber életérzést" is. Mivel az MIT diákjai között kialakult sajátos nyelvezetet kívülálló nem igazán érthette, megírták a *The Jargon File*-t, amely az általuk használt kifejezések magyarázatát tartalmazta. Ebben találhatjuk a hacker definícióját is.

1. Olyan személy, aki élvezi a programozható rendszerek részleteinek feltárását és a képességei kibővítését, szemben a legtöbb felhasználóval, akik inkább csak a szükséges minimumot tanulják meg. Az RFC1392 szerint olyan személy, aki örömmel ismeri meg a rendszer, különösen a számítógépek és a számítógépes hálózatok belső működését.
2. Aki lelkesen (akár rögeszmésen) programoz, vagy aki sokkal inkább élvezi magát a programozást, mint a programozásról való elmélkedést.
3. Olyan személy, aki képes értékelni a *hack* értékét.
4. Olyan ember, aki jól tud gyorsan programozni.
5. Egy adott program szakértője, vagy aki gyakran dolgozik a programon vagy annak segítségével (lásd a „Unix hacker" definícióját).
6. Bármilyen szakértő vagy rajongó. Lehet valaki például csillagász hacker is.
7. Aki élvezi a korlátok kreatív legyőzésének vagy megkerülésének intellektuális kihívását.
8. [elavult] Rosszindulatú beavatkozó, aki kényes információkat próbál felfedezni próbálkozással. Ezek a jelszóhackerek vagy hálózati hackerek. Ma már a helyes kifejezés ezekre a cracker.[20]

Az 1970-es években a hackerszubkultúra folyamatosan terjedt, elsősorban a Szilícium-völgyben és a nagy amerikai műszaki egyetemeken. Ennek folyamatát és történetét Steven Levy 1984-es könyve írja le, egyben itt található meg a hackeretika leírása is, amely szerint az ősi hackerek a világhoz viszonyultak.

1. A számítógépekhez való hozzáférésnek – és bárminek, ami megtaníthat valamit arról, hogy a világ hogyan működik – korlátlannak és totálisnak kellene lennie.
2. Minden információnak hozzáférhetőnek kellene lennie.
3. Ne bízz a hatóságban – támogasd a decentralizációt!
4. A hackereket az általuk elkövetett tettek alapján kellene megítélni, nem pedig iskolai végzettség, kor, faj vagy pozíció alapján.

[20] Eric S. Raymond: The Jargon File, version 4.4.8. *Eric S. Raymond's Home Page,* 2004. október 1.

5. Művészetet és szépséget kreálhatsz a számítógépeden.
6. A számítógépek jobbá tehetik az életedet.[21]

Érdemes kiemelni, hogy a negyedik pont szerint a hatóságokkal való együttműködés nemkívánatos, ami annak is köszönhető, hogy ekkoriban jelent meg az amerikai büntetőjogban az első olyan passzus, amely szankcionálta a számítógépes bűncselekményeket. Ezután a hackerközösség tagjai egyre gyakrabban kerültek szembe a törvénnyel és a bűnüldöző szervekkel. Ennek tragédiáját fogalmazza meg Loyd Blankenship, a Legion of Doom tagjának nagy hatású írása, *A hacker kiáltványa,* amelynek utolsó sorai így hangzanak Voyager2 fordításában:

> „Igen, bűnöző vagyok. A bűnöm a kíváncsiság. A bűnöm az, hogy azután ítélem meg az embereket, amit mondanak és gondolnak, és nem a külsejük alapján. A bűnöm, hogy okosabb vagyok, mint ti, ez olyan dolog, amit soha nem fogtok nekem megbocsátani. Hacker vagyok, és ez a kiáltványom. Megállíthatjátok az egyént, de nem állíthattok meg minket… végül is, mind egyformák vagyunk."[22]

Nem tett jót az állam és a hackerek közötti kapcsolatnak az sem, hogy a hatósági érdeklődés pont 1984-ben erősödött fel. George Orwell világhírű regényének címe és tartalma, valamint az aktuális évszám és a közösséget érő csapások közötti látszólagos összefüggések ugyanis nagy hatást tettek az arra érzékeny közönségre, és nem javították az USA kormányával szembeni bizalmat. Lassan 30 éves távlatból viszont úgy látszódik, hogy sokkal inkább véletlen egybeesések alakították ezt a viszonyt. Az 1980-as évek elejétől az amerikai háztartásokban is széles körben elérhetővé váltak a számítógépek, fiatalok százezrei ismerkedtek meg a programozás alapjaival. 1983-ban vetítették a *Háborús játékok* című amerikai filmet, amely széles körben ismertté tette a hackerizmust. 1984-ben megtartották az első hackerkonferenciát, a Hackers Conference-t, elindult az első hackermagazin, a *2600,* illetve ehhez kapcsolódóan megjelent Steven Levy már említett könyve. A hacker tehát bekerült az amerikai közbeszédbe, aminek a hatására létrejöttek az első szervezett hackercsoportok, amire viszont már lépnie kellett a jogalkotónak, és meg kellett szabnia azokat a határokat,

[21] Steven Levy: *Hackers: Heroes of the Computer Revolution*. Garden City, Anchor Press/Doubleday, 1984. 458.

[22] The Mentor: The Conscience of a Hacker. *Phrack Inc.,* 1. (1986), 7. Phile 3 of 10.

amelyeket a számítógépes tevékenységek nem léphetnek át. Ez viszont érdekellentétet és meglehetős bizalmatlanságot szült.

Az első hacktivistacsoportok

Az amerikai hackercsoportok gondolkodásában eközben egyre inkább megjelentek az ideológiai vonások is. Ez egyenesen következik a keleti és nyugati parti amerikai egyetemek klasszikus szabadelvűségéből és a korszellemből, amely előbb a vietnámi háborúval, majd később a Ronald Reagan nevével fémjelzett mély konzervatív gondolkodással való szembenállásban manifesztálódott az amerikai fiataloknál. A hacker nem bízott az államban, és meg akarta mutatni, hogy az állam hazudik. Éppen ezért, ahogy a hackeretika második pontjában olvashatjuk is, az információt sokan hozzáférhetővé akarták tenni. Beleértve ebbe az állam titkait is. Ezt a mozgalmat az „Information wants to be free", azaz az információ szabad akar lenni mottóval indították el, eredete az MIT modellvasútklubjának két tagjához, Jack Dennishez és Peter Samsonhoz nyúlik vissza. A kifejezést viszont Stewart Brand alkotta meg, aki 1984-ben, a Hackers Conference-en ezt mondta:

> „Egyrészt az információ drága akar lenni, mert nagyon értékes. A megfelelő információk a megfelelő helyen egyszerűen megváltoztatják az életedet. Másrészt az információ ingyenes akar lenni, mert a kinyerésének költsége folyamatosan csökken. Tehát ez a kettő harcol egymás ellen."[23]

Az 1980-as évek közepén, 1990-es évek elején számos hackercsoport jött létre, így volt táptalaja ennek a gondolkodásnak. A legnagyobb ilyen csoportok: a Cult of the Dead Cow 1984-ben, Texasban alakult meg; a Legion of Doom, szintén 1984-es alapítással, szerte az USA-ban rendelkezett tagokkal; a Masters of Deception az 1980-as évek végétől New Yorkban működött; és ott volt még a bostoni L0pht Heavy Industries, 1992-es indulással. Ahogy korábban olvasható volt, a cDc tagjai megalkották a hacktivizmus kifejezést, a hackercsoportok pedig egyre többször szerepeltek a nyilvánosság előtt. Talán a legemlékezetesebb ebből az időszakból a L0pht kongresszusi meghallgatása volt 1998-ban, amelyet

[23] Cory Doctorow: Saying Information Wants to Be Free Does More Harm Than Good. *The Guardian,* 2010. május 18.

az első, széles körben ismertté vált kiberbiztonsági ülésként tartanak számon. Ennek témája az USA kibertéri kitettsége volt. A hackerek segítettek rávilágítani arra, hogy milyen súlyos sebezhetőségek vannak az interneten és a kritikus infrastruktúrákban.[24] Érdekesség, hogy a meghallgatáson fontos szerepet játszott Peiter „Mudge" Zatko, a L0pht tagja, aki 2004-től kezdve hosszabb ideig a DARPA-nak dolgozott, katonai kibervédelmi projekteken.

A hacktivizmus ekkoriban találkozott a digitális aktivizmussal, és nagyon hasonló eszköztárral ugyan, de nagyon különböző háttérrel két irányzat erősödött meg. Az egyiket tömegmozgalmi hacktivizmusnak nevezték, és sokkal inkább a politikai aktivizmus jegyeit mutatta, de már kihasználta az internetben rejlő lehetőségeket. Az első ilyen mozgalmat Ricardo Dominguez alapította, aki művész és író volt. Mozgalmának neve The Electronic Disturbance Theater volt, és 1997-ben indította el. Ez volt az első olyan polgárjogi mozgalom, amely számítógépeket használt aktivistatevékenysége során. Legismertebb akciója a FloodNet volt, amelynek segítségével DDoS-t indítottak a mexikói zapatista felkelők támogatása érdekében. A célpontok között volt a mexikói és az amerikai elnök weboldala is.[25]

A másik irányzatot digitálisan korrekt hacktivizmusnak hívták. Ez a Cult of the Dead Cow-ból indult mozgalom volt, Oxblood Ruffin vezetésével.[26] Elsődleges célkitűzése az információhoz való hozzáférés és a szólásszabadság biztosítása volt az interneten. 2001. július 4-én, a függetlenség napján adták ki a *Hacktivismo Declarationt,* amelyben az internet szabadságának máig ható alapértékeit fogalmazták meg. Ebben többek között foglalkoznak az internethozzáférés szabadságával, az elektronikus információ cenzúrájának kérdésével és a szólásszabadsággal is.[27] Ők kezdik el propagálni az anonim kommunikációs megoldások használatát az információ szabad áramlása érdekében, ami a 2020-as évek elejére annyira általánossá vált, hogy már a nemzetbiztonságot fenyegeti ezen platformok lehallgathatatlansága.

A 90-es évek végén az amerikai hacktivistacsoportok már a globális biztonságpolitikába is belekeveredtek, valószínűleg nem is sejtve, hogy ezzel elindítják a proxycsoportok alkalmazásának taktikáját a 2000-es években. Az egyik nagy visszhangot kiváltó akciót az utókor Blondie Wong és a Hong Kong Blondes

[24] Rosemary Tropeano: Landmark Senate Hearings Exposed Risks and Threats That Are Still Being Confronted. *National Security Archive,* 2019. január 9.

[25] Jordan–Taylor (2004): i. m. 69.

[26] Jordan–Taylor (2004): i. m. 98.

[27] Cult of the Dead Cow: *Hacktivismo Declaration* (2001. július 4.).

néven ismeri. Az 1995–1998 között zajló történet lényege, hogy állítólag Oxblood Ruffin kapcsolatba került egy kínai disszidens csoporttal, amely a kínai triádok segítségével csempészett nyugatra olyan másként gondolkodókat, akik szembekerültek a kínai kormánnyal. A Blondie Wong néven ismert kapcsolattartó és a Hong Kong Blondes-nak nevezett csoportja Ruffin segítségével kapcsolatba került a cDc-vel és más hackercsoportokkal is, amelyek segítségével egyrészt sajtónyilvánosságot kaptak, másrészt elsajátítottak hackertechnikákat, és hozzáfértek olyan támadóeszközökhöz, mint például a Back Orifice 2000 nevű, távoli hozzáférést lehetővé tevő szoftver, amelynek segítségével sikeresen támadtak kínai célpontokat. A részletek nem ismertek, de Ruffin évekkel későbbi beszámolója arra enged következtetni, hogy a művelet nem nélkülözte a titkosszolgálati jelleget.[28] Már ha megtörtént egyáltalán, és nem a cDc hatalmas médiahackje volt, a kínai szakirodalomban ugyanis nyoma sincsen a sztorinak.[29] Az amerikai média mindenesetre felkapta a történetet, és széles körben ismertté vált a hacktivizmus.

A másik ilyen akcióra 1998 végén került sor, amikor a Legions of the Underground nevű csoport kiberháborút hirdetett Kína és Irak ellen, az emberi jogok megsértése miatt. A felhívás lényege az volt, hogy néhány napon keresztül a közösség tagjai célzottan támadják a két ország informatikai infrastruktúráját, ezzel ellehetetlenítve az országok normális működését. Ez hatalmas vihart kavart, a legjelentősebb hackercsoportok, mint a cDc, a L0pht vagy a német Chaos Computer Club, közös közleményben határolódtak el a felhívástól, jelezve azt, hogy elfogadhatatlannak tartják az ilyen beavatkozást más országok működésébe.[30] A beszámolók szerint egyébként a Legions of the Underground is tagadta, hogy köze lenne a felhíváshoz. A felhívást a csoport egyik tagjának, Staktonnak tulajdonították, viszont ő saját bevallása szerint a felhívás idején két hétig nem volt online, a nevében nyilatkozott valaki, akit utána soha többet nem láttak.[31] A támadást végül nem hajtották végre, a történeti visszatekintésekben viszont egyre többször merül fel, hogy az érintett titkosszolgálatok beépültek ezekbe a közösségekbe. Ezt erősíti meg az FBI-tól kikért akták sokasága is, amelyek szerint legkésőbb az 1995-ös DefCon hackerkonferencián már műveleti célból

[28] Oxblood Ruffin: Blondie Wong And The Hong Kong Blondes. *Medium,* 2015. március 23.

[29] Wei Honker: cDc Created Hong Kong Blondes and ‚Hacktivism' as a Media Hack. *Seclist.org,* 2012. május 3.

[30] International Coalition of Hackers: „Hackers Don't Go To War" (1999. január 7.).

[31] James Glave: Confusion Over 'Cyberwar'. *Wired,* 1999. január 12.

vettek részt FBI-ügynökök.[32] Ezen a rendezvényen azóta is rendszeres esemény a „Spot the Fed", azaz a „Szúrd ki az ügynököt" játék.

Hacktivizmus a keleti nagyhatalmakban

Turovszkij orosz hackerekről szóló könyvéből az olvasható ki, hogy nagyon más fejlődési úton ugyan, de a 2000-es évek elejére Oroszországban is kialakult a hacktivizmus útját járó közösség. Az orosz hackerszcéna a számítógépekhez való szabad hozzáféréssel kezdődött a 90-es évek elején, majd az IRC-csatornák, az orosz nyelvű *Hacker* magazin és nem utolsósorban a kiváló matematikaoktatás folyamatosan kitermelte az erre fogékonyak közül az első generációs hackereket. Az orosz vadkapitalizmus során ezek a fiatalok elsősorban klasszikus kiberbűncselekményeket követtek el, nyugati, elsősorban amerikai áldozatok bankszámláit és kártyáit csapolták meg. Az orosz hatóságok egy ideig képtelenek voltak ellenük bármit is tenni, majd megszületett az a hallgatólagos megállapodás, hogy ameddig nem hazai célpontokat támadnak, addig nem is tesznek hatalmas erőfeszítéseket az elkövetők kézre kerítése érdekében. Ami rossz Amerikának, de nem fáj Oroszországnak, az elfogadható, azaz az ellenségem ellensége a barátom. Ez az évtizedek során azt eredményezte, hogy a külföldön elkövetett gazdasági bűncselekmények „elnézése" fejében ezeket a kiberbűnözői csoportokat és a támadó infrastruktúráikat egyre gyakrabban használták fel proxyként az Oroszország érdekében álló műveletek végrehajtása során, ahogy azt az észtországi példában is láthattuk.[33]

Az orosz állampolgár és az orosz államhatalom közötti, évszázadok alatt kialakult sajátos kapcsolat miatt a hacktivizmus itt nem a liberális, szólásszabadságot és állami túlhatalmat ellenző irányban jelent meg hangsúlyosan – bár ilyen irányzatokkal is lehet találkozni –, hanem kitermelte a hazafias hackerek irányzatát. Ez hangsúlyosan a második csecsen háborútól érződik, amikor önszerveződő csoportok kaukázusi internetes célpontok ellen hajtottak végre támadásokat, majd 2005-től egyértelműen megjelentek azok a szervező erők a fórumokon, amelyekre 2007-ben már támaszkodni lehetett.

[32] JPat Brown: FBI Files on Def Con Show "Spot the Fed" Contest a Sore Spot for Feds. *Muckrock,* 2015. május 6.

[33] Turovszkij (2020): i. m. 27–59.

A nyugati olvasók számára talán kevésbé ismert, de a kínai hacktivista-csoportok létrejötte és politikai célok mentén történő aktivizálódása megelőzte orosz társaikét. Scott J. Henderson könyvében részletesen feldolgozta a kínai hackerközösség történetének első évtizedét; kiderül, hogy a kínai internet 1994-es indulása után szinte azonnal megjelentek azok a fórumok, ahol a téma iránt érdeklődő tízezrek egymásra tudtak találni. Az első szervezettebb csoport a Zöld Hadsereg (Green Army) volt, amelyet az első kommunista katonai akadémia, a Whampoa Academy után neveztek el. Nem sokkal ezután indult a Kínai Sasszövetség (China Eagle Union). Mindkét csoport indulása 1997-re datálható.

A legjelentősebb csoportosulás azonban a 90-es évek végén, különböző csoportok egyesülése után jött létre. Az önmagát Vörös Hackerek Szövetségének (Red Hacker Alliance) nevező csoport több tízezer tagot számlált, és kimondottan a patrióta hackerek jellemzőit viselte magán. A csoport első komoly hacktivistatevékenysége 1998-ra tehető, amikor tömeges *deface* támadásokat intéztek indonéz kormányzati célpontok ellen, mivel ebben az időben a kínai kisebbséget jelentős támadás érte az indonéz többség részéről. Később célponttá vált Tajvan és Japán is, minden esetben a kínai nacionalizmust sértő lépések miatt.

A Vörös Hackerek Szövetsége valószínűleg a kínai kormányzattól függetlenül jött létre, ráadásul az is valószínű, hogy a kínai kultúra sajátossága miatt a kínai titkosszolgálatok nem vettek részt aktívan az első hacktivistaakciók szervezésében, azt a kínai hackerek ténylegesen saját patrióta beállítottságuk miatt hajtották végre. Az azonban Henderson kutatásai szerint biztosnak tűnik, hogy a csoport felbomlásának idején, 2005-ben a kínai hadsereg már aktívan toborzott a tagok között, illetve a 2000-es évek elején már létezett olyan kiberhadviseléssel foglalkozó csoport a Kínai Népi Felszabadító Hadseregen belül, amely az amerikai és izraeli példa alapján szerveződött.[34] Ezzel véget is ért a kínai hacktivizmus első generációjának aktivitása, de jöttek a következő generációk, amelyeknek egyre inkább a kontrollált kínai interneten kellett működniük, az érdeklődés azonban nem csökkent, éppen ellenkezőleg, nőtt a hackerizmus iránt.[35]

[34] Scott J. Henderson: *The Dark Visitor. Inside the World of Chinese Hackers.* Scott Henderson, 2007.

[35] Craig Webber – Michael Yip: The Rise of Chinese Cyber Warriors: Towards a Theoretical Model of Online Hacktivism. *International Journal of Cyber Criminology,* 12. (2018), 1. 230–254.

Következtetések

Jelen fejezet a 2000-es évek első felében hagyja abba a hacktivistacsoportok történetének bemutatását, nem foglalkozik az Anonymous vagy a LulzSec csoporttal, nem részletezi a WikiLeaks tevékenységét és Edward Snowden vagy Bradley (ma már Chelsea) Manning szerepét sem elemzi. A 2007-es észtországi események ugyanis teljesen új világot teremtettek a kiberhadviselésben, és a nagyhatalmak inkább az ilyen proxycsoportok integrálására törekedtek. Ennek oka egyrészt a nemzetközi kapcsolatokban keresendő, de valószínűleg nagyobb súllyal esett latba az, hogy a hackerek kevéssé kontrollálhatóak, egyáltalán nem biztos, hogy egy titkos művelet nem kerül napvilágra egy sértett hacker miatt. Ha ugyanezek az emberek fegyveres testületen belül, annak szabályait követve dolgoznak, valószínűleg sokkal hatékonyabbak is.

Ha megnézzük a nagyhatalmak hozzáállását a hacktivistacsoportokhoz, ugyanazt az utat látjuk. Az Egyesült Államokban az első generációs hacktivisták eltűntek, sokan közülük valószínűleg, Mudge-hoz hasonlóan, kormányzati szolgálatba álltak. Az biztos, hogy az Anonymous csoportra már rendvédelmi problémaként tekintettek az amerikai rendvédelmi szervek, a szétzüllesztésére és felszámolására törekedtek. Az USA-ra egyébként sem volt jellemző a hacktivisták proxyként való felhasználása. Oroszország hibrid hadviselése során továbbra is széles körben alkalmaz proxykat, de ezek ma már szinte kizárólag magánbiztonsági cégek. Ezek közül talán a legismertebb az Internet Research Agency, amelyet a 2016-os amerikai elnökválasztás befolyásolási kísérlete során használtak, de számos más, hasonló cég megtalálható az amerikai embargós listán, amelyet az őket ért kiberincidensek nyomán bővítenek. Emellett természetesen minden lehetőséget kihasználnak, így Julian Assange, a WikiLeaks vezetőjének gyakori szereplése az orosz RT nevű propagandatévében sem véletlen. Kína esetében pedig a hacktivisták és az állam motivációi sosem álltak egymástól távol, így aránylag könnyen integrálták és integrálják jelenleg is a hackerizmus iránt érdeklődő fiatalokat a hadseregbe.

A hacktivisták proxyként való felhasználása offenzív kiberműveletekben tehát inkább a 2000-es évekre jellemző. De hacktivizmus mindig lesz. Egészen pontosan mindig lesznek olyan lánglelkű fiatalok, akik rendszerkritikusságukat vagy éppen hazafiságukat a hackerizmus eszközeivel élik meg. Amennyiben egy ország tudatosan törekszik ezen fiatalok honvédelembe való integrálására – hasonlóan a nagyhatalmakhoz –, akár rövid távon is megvalósítható az offenzív kiberképességek létrehozása. Egy 2012-es felmérés szerint

Magyarországon az információbiztonságban dolgozó vagy az iránt érdeklődő személyek 59%-a akár ingyen is szolgálná a hazáját, míg 27%-uk pénzt kérne ezért. Csupán 14% válaszolt úgy, hogy nem venne részt a honvédelemben.[36] Bár a felmérés régi, feltehetően továbbra is sikerrel lehetne meríteni a magyar hackerek közül, ami tudatos tervezéssel a magyar kiberhadviselési képességek fejlesztésének egyik fontos eleme lehet.

Irodalomjegyzék

Brown, JPat: FBI Files on Def Con Show "Spot the Fed" Contest a Sore Spot for Feds. *Muckrock,* 2015. május 6. Online: www.muckrock.com/news/archives/2015/may/06/def-cons-spot-fed-contest-sore-spot-feds/

Cult of the Dead Cow: *Hacktivismo Declaration* (2001. július 4.). Online: https://blog.9while9.com/manifesto-anthology/2001.html

Department of Justice Office of Public Affairs: *Russian National Who Operated Kelihos Botnet Pleads Guilty to Fraud, Conspiracy, Computer Crime and Identity Theft Offenses* (2018. szeptember 12.). Online: www.justice.gov/opa/pr/russian-national-who-operated-kelihos-botnet-pleads-guilty-fraud-conspiracy-computer-crime

Doctorow, Cory: Saying Information Wants to Be Free Does More Harm Than Good. *The Guardian,* 2010. május 18. Online: www.theguardian.com/technology/2010/may/18/information-wants-to-be-free

ENSZ: *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Document A/68/98* (2013. június 24.). Online: https://undocs.org/A/68/98

Glave, James: Confusion Over ‚Cyberwar'. *Wired,* 1999. január 12. Online: www.wired.com/1999/01/confusion-over-cyberwar/

Henderson, Scott J.: *The Dark Visitor. Inside the World of Chinese Hackers*. Scott Henderson, 2007.

International Coalition of Hackers: „Hackers Don't Go To War" (1999. január 7.). Online: http://lists.jammed.com/ISN/1999/01/0019.html

Jordan, Tim – Paul A. Taylor: *Hacktivism and Cyberwars. Rebels with a Cause?* New York, Routledge, 2004.

[36] Krasznay Csaba – Varga-Perke Bálint: Ifjúságvédelem a hacker szubkultúrában. In Bíró A. Zoltán – Gergely Orsolya (szerk.): *Ártalmas vagy hasznos internet? A média hatása a gyermekekre és fiatalokra*. Csíkszereda, Státus, 2013. 179–202.

Karatzogianni, Athina: *Firebrand Waves of Digital Activism 1994–2014: The Rise and Spread of Hacktivism and Cyberconflict*. Basingstoke, Palgrave Macmillan, 2015.

Koval, Nikolay: Revolution Hacking. In Kenneth Geers (szerk.): *Cyber War in Perspective: Russian Aggression against Ukraine*. Tallinn, NATO CCD COE Publications, 2015. 55–58.

Krasznay Csaba – Varga-Perke Bálint: Ifjúságvédelem a hacker szubkultúrában. In Bíró A. Zoltán – Gergely Orsolya (szerk.): *Ártalmas vagy hasznos internet? A média hatása a gyermekekre és fiatalokra.* Csíkszereda, Státus, 2013. 179–202.

Levy, Steven: *Hackers: Heroes of the Computer Revolution.* Garden City, Anchor Press/ Doubleday, 1984.

Lowe, Christian: Kremlin Loyalist Says Launched Estonia Cyber-Attack. *Reuters*, 2009. március 13. Online: www.reuters.com/article/us-russia-estonia-cyberspace-idUSTRE52B4D820090313

Ottis, Rain: *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective.* Cooperative Cyber Defence Centre of Excellence, 2008. március 2. Online: https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

Raymond, Eric S.: The Jargon File, version 4.4.8. *Eric S. Raymond's Home Page,* 2004. október 1. Online: http://catb.org/jargon/

Romagna, Marco: Hacktivism: Conceptualization, Techniques, and Historical View. In Thomas J. Holt – Adam M. Bossler (szerk.): *The Palgrave Handbook of International Cybercrime and Cyberdeviance*. London, Palgrave Macmillan, 2020. Online: https://doi.org/10.1007/978-3-319-90307-1_34-1

Ruffin, Oxblood: Hacktivism: From Here to There. *Threatpost,* 2010. december 9. Online: https://threatpost.com/hacktivism-here-there-120910/74759/

Ruffin, Oxblood: Blondie Wong And The Hong Kong Blondes. *Medium,* 2015. március 23. Online: https://medium.com/emerging-networks/blondie-wong-and-the-hong-kong-blondes-9886609dd34b

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

Schmitt, Michael N. – Liis Vihul: Proxy Wars in Cyberspace. *Fletcher Security Review,* 1. (2014), 2. 2014. 54–73. Online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2388202

The Mentor: The Conscience of a Hacker. *Phrack Inc.,* 1. (1986), 7. Phile 3 of 10. Online: http://phrack.org/issues/7/3.html

Tropeano, Rosemary: Landmark Senate Hearings Exposed Risks and Threats That Are Still Being Confronted. *National Security Archive,* 2019. január 9. Online: https://bit.ly/3I1jNKh

Turovsky, Daniil: "It's Our Time to Serve the Motherland." How Russia's War in Georgia Sparked Moscow's Modern-Day Recruitment of Criminal Hackers. *Meduza*, 2018. augusztus 7. Online: https://meduza.io/en/feature/2018/08/07/it-s-our-time-to-serve-the-motherland

Turovszkij, Danyiil: *Orosz hekkerek*. Budapest, Athenaeum, 2020.

UCMC Press Center: Security Service of Ukraine Possesses Audio Records of Krasnov's Conversations With His Russian Supervisor. 2016. március 3. Online: https://uacrisis.org/en/40837-sbu-3

United States District Court: *United States Versus Peter Yuryevich Levashov* (2017. április 4.). Online: www.justice.gov/opa/press-release/file/956511/download

Webber, Craig – Michael Yip: The Rise of Chinese Cyber Warriors: Towards a Theoretical Model of Online Hacktivism. *International Journal of Cyber Criminology,* 12. (2018), 1. 230–254. Online: http://cybercrimejournal.com/Webber&YipVol12Issue1IJCC2018.pdf

Wei Honker: cDc Created Hong Kong Blondes and ‚Hacktivism' as a Media Hack. *Seclist.org,* 2012. május 3. Online: https://seclists.org/fulldisclosure/2012/May/30

Yagoda, Ben: A Short History of "Hack". *The New Yorker,* 2014. március 6. Online: www.newyorker.com/tech/annals-of-technology/a-short-history-of-hack

6. fejezet

Magánbiztonsági vállalatok szerepe az állami műveletekben

Koller Marco

Bevezetés

Az elmúlt évtizedekben a biztonsággal kapcsolatos általános felfogás módosult. A világban, így Európában is negatív irányban változott a biztonsági helyzet, ami kihat a kibertér biztonságára is. Az utóbbi évtizedekben a technológiát jellemző robbanásszerű fejlődés, kiemeltképpen a kiberteret érintően, a fejlődés mellett egyértelműen indukálta a biztonsági kockázatok növekedését is.[1]

Megállapítható, hogy a fentiekben is említett fejlődés mentén létrejövő digitális társadalmak digitális hadsereget hoztak és hoznak létre. A kibertér, kiberfegyverek és kiberműveletek értelmezése multidiszciplináris megközelítést igényel, figyelemmel arra, hogy ezen témakörök több tudományterületet is átfednek, továbbá a kiberműveletek egyre szélesebb körű alkalmazása szükségessé teszi a különböző állami szervek, illetve a kutatók és a magánvállalatok közötti kommunikációt és összefogást, hiszen a „kibertérben végrehajtott műveletek, azaz a kiberműveletek, vagyis az informatikai rendszerek támadása és védelme a katonai és politikai stratégiaalkotás részét képezi".[2]

A kibertérben végbemenő különböző támadások elhárítása a mai világban kiemelt prioritással rendelkező problémává vált a világ országai számára. A kiberbiztonság fejlesztése elengedhetetlen a különböző információs rendszerek védelme érdekében, kiemeltképpen a létfontosságú intézmények esetén kell elhárítani a különböző kibertámadásokat.[3]

[1] Kovács László: A kiberbiztonság és a kiberműveletek megjelenése Magyarország új Nemzeti Biztonsági Stratégiájában. *Honvédségi Szemle,* 148. (2020), 5. 3–18.

[2] Dévai Dóra: A kiberfegyver koncepció evolúciója. *Hadmérnök,* 14. (2019), 2. 273.

[3] Nagy Zoltán András: Kiberháborúk kora. In *Magyar Tudomány Napja a Délvidéken – 2018. Tanulmánykötet.* Vajdasági Magyar Tudományos Társaság, 2018. 174–193.

https://doi.org/10.36250/01079_06

Egy-egy állam saját képességeinek fokozása mellett a biztonsági szektorban lévő hiátusok megoldása érdekében kiszervezheti tevékenységét magánbiztonsági vállalatoknak, vagy egyes esetekben olyan szolgáltatásokat vehet igénybe, amelyekkel az adott kormányzati szervezet a saját képességeit fejlesztheti mind humán, mind technikai téren.

A kutatás célja, módszertana

„A nemzetek szigorúan titkosan kezelik a kiberképességeikre vonatkozó adatokat, és a kiberműveleti stratégiáik is csak részben nyilvánosak, ezért csak korlátozott mennyiségű adat áll rendelkezésre."[4] Jelen fejezet célja, hogy bemutassa a magánszektor, magánbiztonsági cégek szerepvállalását az állami műveletekben, azon belül is kiemelten az állami kiberműveletekben. A tanulmány aktualitását magyarázzák a fentiekben már kifejtettek, azaz a kibertér növekvő szerepe a mindennapokban, valamint az állami felelősség növekedése. A növekedő felelősség növekvő felelősségvállalást, így humán, illetve technikai fejlődést is megkíván, amihez szinte nélkülözhetetlen a magánszektor bevonása is. A kutatás során a vonatkozó hazai és nemzetközi szabályozókat tekintettük át, kiemelten a magyar *Nemzeti Biztonsági Stratégiát* és *Kiberbiztonsági Stratégiát,* továbbá a *Tallinni kézikönyvet.* A jogi szabályozók mellett a hazai és a nemzetközi szakirodalmat vizsgáltuk meg, majd elemeztük a(z állami) kiberműveletekről, a magánbiztonsági vállalatokról és az azok kapcsolatáról szóló részeket. A tanulmány során a fogalmi háttér bemutatásán túl esettanulmányon keresztül kívánom ismertetni a magánbiztonsági vállalatok szerepét az állami műveletekben.

Fogalmi háttér

A következő fejezetben a témakör, illetve kontextusának komplex értelmezéséhez szükséges nagyobb és fontosabb definíciókat mutatom be, hogy az olvasó a későbbiekben kifejtetteket megfelelő minőségben tudja absztrahálni.

[4] Dévai (2019): i. m. 278.

A kibertér fogalma

A fogalmat a korábbi fejezetekben már több szempontból is körbejártuk, így emlékeztetőül csak annyit írunk, hogy a szót William Gibson alkotta meg az 1982-ben megjelent *Burning Chrome* című novellájában, illetve az 1984-ben kiadott *Neoromancer* című regényében. A kibertér fogalmát rendkívül sok szervezet próbálta megfogalmazni, így több adekvát definíció is létezik. Az Egyesült Államok Védelmi Minisztériuma által kiadott és 2016 februárjában pontosított katonai terminológiai szótárban meghatározottak 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 számítógép-rendszereket, valamint a beágyazott feldolgozó és vezérlő elemeket”.[5] Továbbá ki kell emelni a Magyarország hálózati és információs rendszerek biztonságára vonatkozó stratégiájáról szóló 1838/2018. (XII. 28.) Korm. határozatot, amely úgy fogalmazza meg a kiberteret, hogy: „globálisan összekapcsolt, decentralizált, folyamatosan változó elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti”.[6] A fenti megfogalmazásokon túl Haig Zsolt adja a legszélesebb körű megfogalmazását a kibertérnek, amely részletesen taglalja a definíció egyes elemeit, azok jelentőségét.

> „Az ember által mesterségesen létrehozott, dinamikusan változó tartomány, amelyben az információ gyűjtését, tárolását, feldolgozását, továbbítását és felhasználását végző, egymással hálózatba kapcsolt és az elektromágneses spektrumot is felhasználó infokommunikációs eszközök és rendszerek működnek, lehetővé téve ezzel az emberek és a különféle eszközök közötti folyamatos és globális kapcsolatot.”[7]

[5] Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms (2010. november 8.); Berki Gábor: Kiberháború, kiberkonfliktusok. In Pintér István (szerk.): *A virtuális tér geopolitikája. Tanulmánykötet.* Budapest, Geopolitikai Tanács Közhasznú Alapítvány, 2016. 248.

[6] A hálózati és információs rendszerek biztonságára vonatkozó Stratégia. Lásd: https://bit.ly/39PHBE4

[7] Haig Zsolt: *Információs műveletek a kibertérben.* Dialóg Campus, 2018. 15.

A kiberbiztonság és a kibertérben jelen lévő fenyegetések

A téma szempontjából elengedhetetlen tisztázni azt, hogy mit jelent a kiberbiztonság, illetve a kibertérben milyen jellegű fenyegetések vannak jelen. Magyarország hálózati és információs rendszerek biztonságára vonatkozó stratégiája szerint a kiberbiztonság:

> „a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez."[8]

A kormányhatározat jól szemlélteti, hogy a kiberbiztonság egy folyamat, illetve aktuális állapotot is jelöl, amely multidiszciplináris megközelítést igényel. Ahhoz, hogy egy adott állam vagy bármilyen szervezet szavatolhassa a kiberbiztonságot, tudni kell, hogy milyen típusú fenyegetések jelentkezhetnek a kibertérben. A kibervédelmi kihívások megfelelő kezeléséhez kiemelten fontos a kibertér és az abban előforduló események definiálása, a kibervédelmi fenyegetések tipizálása, a kibertérben tapasztalt incidensek kezeléséből levonható következtetések rendszerezése.[9]

A támadások alapvetően az informatikai rendszereken tárolt és kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, illetve a rendszerelemek rendelkezésre állása és funkcionalitása ellen irányulhatnak. Az adatok bizalmassága pedig azt jelenti, hogy azokat csak a jogosultak ismerhetik meg, használhatják fel, az adatok jogosultsági szintjének megfelelően. A sértetlenség azt jelenti, hogy nem történt benne illetéktelen változtatás. A rendelkezésre állás arra vonatkozik, hogy az adatot az arra jogosultak a szükséges helyen és időben elérhessék, használhassák.[10] A rendelkezésre álló szakirodalom több módon csoportosítja a kibertéri fenyegetéseket, azonban a legegyszerűbben és legérthetőbben Berki Gábor írta le, miszerint ezek: kiberbűnözés, kiberkémkedés, hacktivizmus, kiberterrorizmus, kiberhadviselés.[11]

[8] A hálózati és információs rendszerek biztonságára vonatkozó Stratégia.

[9] Fekete-Karydis Klára – Lázár Bence: A kibervédelem katonai dimenziói. *Honvédségi Szemle,* 148. (2020), 3. 44.

[10] Muha Lajos – Krasznay Csaba: *Az elektronikus információs rendszerek biztonságának menedzselése.* Budapest, Nemzeti Közszolgálati Egyetem, 2014. 13–14.

[11] Berki (2016): i. m. 250.

Kiberműveletek

Haig Zsolt *Információs műveletek a kibertérben* című munkája alapján kiberműveletnek az alábbiakat nevezzük:

> „a kibertérben érvényesülő információs képességek integrált, összehangolt és koordinált alkalmazására irányuló tevékenységek összessége, amelyek a műveletek célkitűzéseinek elérése érdekében, a kibertéri hálózatos infokommunikációs rendszereket felhasználva, a kognitív képességekkel közvetlenül, illetve a technikai képességekkel közvetetten hatásokat gyakorolnak a műveletekben részt vevő célközönség szándékára, helyzetértelmezésére és képességeire."[12]

A fentiek alapján jól látható, hogy a kiberművelet mint fogalom a legkönnyebben úgy írható le mint a kibertéri képességek alkalmazása, az adott célok elérésének érdekében. A Berki Gábor *Kiberháború, kiberkonfliktusok* című tanulmányában lefektetettek szerint a kiberműveleteket az alábbiak szerint lehet rendszerezni:

- *Támadó kiberműveletek.* Céljuk az ellenség hálózatba kötött informatikai rendszereinek feltérképezése, működésük befolyásolása, lerontása, megbénítása.
- *Védelmi kiberműveletek.* A saját informatikai rendszereink megvédése az ellenség támadó tevékenységével szemben (például vírusvédelmi szoftverek, tűzfalak).
- *Katonai információs hálózati műveletek*.[13] Céljuk a fentiekben leírtak támogatása, azok hátterének biztosítása (például felhasználói képzések, üzemeltetés és karbantartás).

Magánbiztonság

A magánbiztonságot gyakran relatíve új jelenségként tartják számon, holott a valóság az, hogy egyes formái már évszázadok óta léteznek. Nehéz adekvát fogalmat meghatározni a magánbiztonsággal kapcsolatban, figyelemmel arra, hogy a szakirodalomban rendkívül sok definíciót alkottak. A Christián László által meghatározott fogalom a következőképpen hangzik:

[12] Haig Zsolt: *Információs műveletek a kibertérben*. Budapest, Dialóg Campus, 2018. 15.
[13] Berki (2016): i. m. 262–263.

> „A magánbiztonság egy olyan ellenszolgáltatás keretében, piaci alapon működő, engedéllyel rendelkező vállalkozás (vagy természetes személy) által nyújtott szolgáltatás, amely a megbízó személyes biztonságát, tulajdonát védelmezi, elősegíti a jogainak teljesebb körű gyakorlását. A magánbiztonság felfogható egy halmazként, amely egyre nagyobb közös részhalmazt alkot a közrend, közbiztonság által képzett halmazzal, és van egy önálló, tekintélyes részhalmaza is."[14]

Látható, hogy nem lehet éles határvonalat húzni a közrend és közbiztonság, valamint a magánbiztonság fogalomkör közé, hiszen céljuk egy irányba mutat, azaz közös társadalmi és nemzeti érdek. Általában magánbiztonság alatt az alábbiakat értik: személyvédelem, magánnyomozás, közrend fenntartása, biztonsági ellenőrzések hatósági intézkedésre. Azonban a tágabban vett értelmezésben már idetartoznak a biztonsági szakértők, a biztonságtechnológiai szakemberek, a biztonsági képzés oktatói, továbbá a magánkatonai haderő (*private military company,* PMC). A magánbiztonsági tevékenységek köre nagyon sokszínű, mivel azok legfőképpen a megbízók igényeitől, szükségleteitől függnek.[15] Egy 2009-es ASIS-szimpóziumon[16] a szakértők a magánbiztonság tizennyolc alapkövét határozták meg az alábbiak szerint:

1. objektumvédelem,
2. személyvédelem,
3. információs rendszerek biztonsága,
4. nyomozások,
5. veszteségmegelőzés,
6. kockázatelemzés,
7. jogi aspektusok,
8. sürgősségi és veszélyhelyzeti tervezés,
9. tűzvédelem,
10. kríziskezelés,
11. katasztrófamenedzsment,
12. terrorelhárítás,
13. üzleti hírszerzés,
14. végrehajtói védelem,

[14] Christián László: Magánbiztonsági számvetés. In Dobák Imre – Hautzinger Zoltán (szerk.): *Szakmaiság, szerénység, szorgalom. Ünnepi kötet Boda József 65. születésnapja alkalmából.* Budapest, Dialóg Campus, 2018. 147–148.

[15] Rottler Violetta: Gondolatok a magánbiztonság köréből. *Magyar Rendészet,* 19. (2019), 4. 81–95.

[16] ASIS: American Society for Industrial Security, amelyet 1995-ben alapítottak. A közösség a magánbiztonsági szektor egyik legnagyobb szövetsége, már nemzetközi szinten működik.

15. munkahelyi erőszak elleni fellépés,
16. bűnmegelőzés,
17. bűnmegelőzés környezeti tervezéssel,
18. biztonsági építészet és mérnöki munka.[17]

A hagyományos őrzés-védelem mellett egyre hangsúlyosabb szerephez jut a magánbiztonság területén az információbiztonság, az adatvédelem, a logisztikai szolgáltatások, az üzleti hírszerzés stb. A magánbiztonsági iparág egyre fontosabb szerepet kap a nemzetközi biztonság területén.

A magánszektor és a kiberbiztonság kapcsolatának megjelenése a magyar stratégiai dokumentumokban

A 2020-as *Nemzeti Biztonsági Stratégiában* (a továbbiakban: Stratégia) 33 alkalommal szerepel a „kiber" kifejezés különböző kontextusokban. A „magán" kifejezés 2 alkalommal. Egyértelműen meghatározó szerep jut a kiberbiztonságnak a 2020-as *Nemzeti Biztonsági Stratégiában,* hiszen a jelenlegi technológiai fejlődés mellett az annak eredményeképpen létrejövő új típusú kihívások és kockázatok sem hagyhatók figyelmen kívül, az államnak muszáj volt reagálnia[18] a korábbi, 2012-ben megjelent stratégia óta bekövetkezett változásokra. A Stratégia alapvető érdekként definiálja, hogy: „A forradalmi technológiák fejlesztése stratégiai fontosságú kérdés. Hazánk biztonsága megkívánja, hogy a kulcsfontosságú területeken – mint például a kibervédelem, a mesterséges intelligencia, az autonóm rendszerek, a biotechnológia – kiemelt figyelmet fordítsunk a kutatás-fejlesztésre és annak védelmi összetevőjére."[19] Ehhez kapcsolható elem a Stratégiában a kibervédelemhez tartozó, hazai bázisú kutatás-fejlesztés: „A kibervédelmi feladatok összetettsége miatt partnerséget kell kialakítani az állami és a magánszektor szereplői, az oktatási és a tudományos intézmények és az egyéni felhasználók között."[20] Jelen pont világít rá, hogy az állam már a stratégiaalkotáskor is figyelembe vette azt, hogy szüksége van a magánszektorban jelen lévő, kiemelt fontosságú kibertudással rendelkező

[17] Nagyné Bereczki Szilvia – Nagy József: *Magánbiztonság és kritikus infrastruktúra védelem.* Budapest, 2014.
[18] Kovács (2020): i. m.
[19] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról, 106. pont.
[20] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról, 160. pont.

szakismeretre, szakemberekre, akiknek az integrálása a hazai kibervédelembe rendkívül fontos. Ugyanakkor kiemelendő, hogy a Stratégia kockázati faktorként is deklarálja a különböző magánszervezeteket a kibertérben, itt kifejezetten magánbiztonsági cégeket említ a jogalkotó.

> „A technikai fejlődéssel és vívmányainak elterjedésével folytatódik a biztonságot veszélyeztető, nehezen kontrollálható nem állami szereplők – például szervezett bűnözői körök, nemzetközi terrorszervezetek, kiberbűnözői csoportok, szélsőséges vallási közösségek, magán biztonsági cégek, egyes nem kormányzati szervezetek és egyéb transznacionális hálózatok – súlyának növekedése a nemzetközi biztonságpolitikában. Ezek mögött sokszor nehezen azonosítható érdekek és csoportok húzódnak meg, és könnyen szolgálhatnak rejtett állami szándékokat. Mindez átrendezi és áttekinthetetlenebbé teszi egyes térségek biztonsági helyzetét, ami hazánk számára is kihívást jelent."[21]

A fentiek okán egyértelműsíthető, hogy a magyar állam olyan nézőpontot képvisel, amely a kiberképességek állami növelését tűzte ki célul, annak érdekében, hogy a más szereplőkkel szemben csökkentse saját sebezhetőségét. A Stratégia megfogalmazza, hogy a kiberbiztonságot és a vonatkozó képességeket is növelni kell:

> „A kibertérben jelentkező kihívások, kockázatok és fenyegetések kezelésére, a megfelelő szintű kiberbiztonság garantálására, a kibervédelmi feladatok ellátására, a nemzeti létfontosságú információs infrastruktúra zavartalan működésének biztosítására Magyarországnak készen kell állnia."[22]

Azonban jól látható, hogy ennek szavatolása érdekében nem fogalmazza meg a magánszektor szerepkörét, annak ellenére, hogy elvitathatatlan e vállalatok szakértelme. Természetesen megérthető a magyar döntéshozók ódzkodása a biztonság kiszervezésével kapcsolatban, hiszen jól látható következményei lehetnek, amelyek a későbbi fejezetekben lesznek olvashatóak. A Stratégia továbbá kitér a katonai kiberműveletek témakörére is, deklarálja a kiberműveleti erők fejlesztését. Kiemelendő, hogy nem csupán a védekezésre alkalmas képességek fejlesztését,[23] hanem az offenzív képességek erősítését is leírja a stratégia, ami

[21] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról, 69. pont.
[22] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról, 159. pont.
[23] Kovács (2020): i. m.

nagy előrelépés ahhoz képest, hogy sokáig még szakmai körökben is csak nagyon óvatosan fogalmazódott meg a támadó kiberképességek fejlesztésének igénye.[24]

Hazánk jelenleg hatályban lévő kiberbiztonsági stratégiájában, bár nem mondható a legfrissebbnek, már deklarálták a kiberbiztonsággal kapcsolatos alapvető értékeket és szemléletmódot. A kiberbiztonsági stratégia, akárcsak a nemzeti biztonsági stratégia, kimondja, hogy a kibertér védelme nemzeti érdek, az ország szuverenitásának része, annak szavatolása állami érdek és feladat. A kiberstratégia egyszer sem hivatkozik sem magánszektorra, sem magánbiztonsági vállalatokra, a „gazdasági szféra" kifejezést alkalmazza. Kijelenti, hogy: „Magyarországon a kibertér szabadságának és biztonságának szavatolása a kormányzat, a tudományos, a gazdasági és a civil szféra közös felelősségvállaláson alapuló, szoros együttműködésével, összehangolt tevékenységével valósul meg."[25]

A civil szféra inkább a nem kormányzati szervekre érthető. További pontokban erősíti meg a kiberstratégia a különböző területek közötti együttműködés fontosságát, sőt, a szabályozás esetében is úgy fogalmaz, hogy: „A többlépcsős jogalkotási tevékenység mellett szükséges a civil, a gazdasági és a tudományos terület szereplőivel együttműködési megállapodásokat kötni, amelyek megfelelő alapot és szabályozást biztosítanak a közös felelősségvállaláson alapuló kiberbiztonság hatékony működtetéséhez."[26]

Habár az újonnan elfogadott magyar *Nemzeti Katonai Stratégia* egyáltalán nem említi kifejezetten a magánszektor szerepét a kiberbiztonságban és a kiberműveletekben, azonban úgy fogalmaz a *Megújuló Magyar Honvédség* című fejezetben, hogy a haza védelmének nemzeti elemeit egyéb biztonsági együttműködések is kiegészítik, illetve megállapítja, hogy növekedni fog a civil-katonai együttműködés hatékonysága.[27]

[24] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról, 159. pont.
[25] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról, 6. pont.
[26] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról, 10/d. pont.
[27] 1393/2021. (VI. 24.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról, 5. pont.

Koller Marco

A *Tallinni kézikönyv* szerepe a kiberműveletek értelmezésében

A NATO Kibervédelmi Kiválósági Központot (a továbbiakban: CCDCOE) 2008. május 14-én létesítették Tallinnban, célja a védelmi képességek erősítése volt a kiberbiztonság területén. A Cambridge University Press 2013-ban adta ki a *Tallinn Manual on the International Law Applicable to Cyber Warfare* címet viselő kézikönyvét (a továbbiakban: Kézikönyv). A CCDCOE hívta meg a Kézikönyv szerzőit és közreműködőit, a felsőoktatási intézmények képviselőit, nemzetközi jogászszakértőket, technikai szakértőket. A munka célja, amelynek elérése három évet vett igénybe, az volt, hogy az új típusú hadviselés, a kiberhadviselés terén vizsgálja az alkalmazható jogi és katonai lépéseket. A fő hangsúly a békeidőben végzett ellenséges kibertevékenységekkel szemben alkalmazható jogi lehetőségek vizsgálatán volt. Megállapították, hogy egy kiberművelet csak akkor minősül (katonai) erő alkalmazásának, amennyiben a kiberművelet okozta hatás összemérhető egy hagyományos fegyveres támadással. Ilyen esetben adott államnak joga van az önvédelemhez, azonban jelen esetben is szem előtt kell tartani a szükségesség és az arányosság elvét. Megfogalmazták azt is, hogy az állam jogosult a kibertámadás ellen fellépni, nem csupán akkor, amikor bekövetkezett, hanem akkor is, ha már fenyegető közelségben van az esemény bekövetkezése. Egy művelet akkor minősül a kibertérben elkövetett támadásnak, ha hatására személyek sérülnek vagy halnak meg, illetve vagyontárgyak rongálódnak vagy semmisülnek meg. A támadások célszemélyei lehetnek a fegyveres testületek és szervezetek tagjai.

Jelen fejezet szempontjából kiemelendő, hogy a kiberműveletekben részt vevő zsoldosok nem tekinthetők harcoló félnek, ami megalapozhatja azt, hogy egyes államok kiberműveletek végrehajtására zsoldosokat bérelnek fel, hogy az általuk végrehajtani akart művelet ne számítson állam által végbevitt fegyveres agressziónak. A nemzetközi jog a kibertérben is tiltja a terrorizmust és annak eszközeit. A kiberműveletekben a szemben álló feleknek figyelembe kell venni a polgári személyek védelmét, valamint ügyelni kell a támadási módszerek megválasztására, a célok kiválasztására, a támadás előtti figyelmeztetésre, illetve a megtámadott fél védelmi kötelezettségére.[28] A Kézikönyv folytatása 2017 februárjában jelent meg, kiegészítve az előző kézikönyv alkalmazási területét. A folytatás jogi keretet ad minden rosszindulatú kiberművelet kezeléséhez. Deklarálták a NATO

[28] Gyebrovszki Tamás: Stuxnet – mint az első alkalmazott kiberfegyver – a Tallini Kézikönyv szabályrendszere szempontjából. *Hadmérnök,* 11. (2014), 1. 164–174.

együttműködésének növelését az iparral. A Kézikönyv folytatásában áttörést jelentett a 2016. júliusi varsói csúcstalálkozó, amikor a Szövetség a műveletek negyedik színterévé minősítette a kiberteret.[29] 2021-ben a CCDCOE elindította a Tallinn Manual 3.0 projektet, egy ötéves vállalkozást: felülvizsgálják a meglévő fejezeteket, és további fontos új témákat tárnak fel. Figyelembe veszik a nemzetközi és regionális szintű tevékenységeket és nyilatkozatokat.[30]

Magánbiztonsági vállalatok alkalmazása

Az alábbi alfejezetben a magánbiztonsági vállalatok alkalmazásának kérdéskörét két részre osztva mutatjuk be: egyrészt a témakörben megkerülhetetlen országban, az Amerikai Egyesült Államokban alkalmazott jelenlegi trendeket és területeket, hogy tágabb perspektívát kapjon az olvasó. Másrészt a magánbiztonsági vállalatok kiberműveletekben történő alkalmazását.

A magánbiztonság szerepe az Egyesült Államokban

Az Egyesült Államokat tartjuk a magánbiztonsági iparág bölcsőjének, itt alakult ki a szektor a 19. század második felétől. Az USA-ban a 2001. szeptember 11-i terrortámadások idézték elő a magánszektor alkalmazásának előretörését. Egyre szélesebb körű együttműködés vette kezdetét, azóta az államokban olyan új területeken is bevonják a magánbiztonsági szektort, mint többek között a nemzetbiztonsági tevékenység háttértámogatása vagy a katonai műveletek.

Már a statisztikai adatok is jól mutatják, milyen nagy volumenű ez az iparág. 2012 év végén a magánbiztonság 350 milliárd dolláros piac volt az USA-ban. Ebből 282 milliárd dollár – mintegy 80% – a magánszektor részesedése, 69 milliárd dollár – hozzávetőleg 20% – állami megrendelés, amely mutatja, hogy a biztonsági megrendelések nagy része így a piacról érkezett, és nem az állami beruházások uralták a megrendeléseket. Mindenesetre a 69 milliárd dolláros állami beruházást sem lehet félvállról venni.[31] Az IT-biztonsági szolgáltatá-

[29] Fekete-Karydis–Lázár (2020): i. m. 47.

[30] NATO CCDCOE: *The Tallinn Manual.* 2021.

[31] Christián László: A magánbiztonság aktuális nemzetközi trendjei, rövid hazai helyzetértékeléssel. In *Modernkori veszélyek rendészeti aspektusai.* Pécs, Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport – Magyar Rendészettudományi Társaság, 2015. 57–63.

sok 80 milliárd dollárt tettek ki a 350 milliárdból, és ez érzékelhetően elég nagy szelet. Az igény a magánbiztonság iránt folyamatosan növekszik, az IT-biztonsági üzletág esetén az előre jelzett növekedési ütem 9%[32] volt. A magánbiztonsági szervezetek egyre fontosabb szerepet játszanak az országban, ami mögött a folyamatos biztonsági kiszervezések állnak az USA-ban, például meg lehet említeni a büntetés-végrehajtás privatizációját, illetve a különböző infrastruktúrák védelmét is. Habár az állami szereplők és a magánbiztonsági vállalatok között javult az együttműködés, ennek ellenére a rendvédelem terén a privát szolgáltatókkal kapcsolatban folyamatos a kritika (figyelemmel arra, hogy egyre nagyobb piacot nyernek). A leggyakrabban felhozott, hogy habár hatékonyabban láthatják el az egyes feladatokat, mint az állami szereplők, a kereskedelmi alapon nyugvó vállalkozás mindig profitorientált, így egyes esetekben az ezen vállalatok által alkalmazott metódusoknál megkérdőjeleződhet a humán biztonság, az emberi jogok témaköre is. Ez hatványozottan igaz a büntetés-végrehajtásra.[33]

További kérdéseket vet fel a katonai magánvállalatok témaköre, amely az elmúlt évtizedben rendkívül felkapott lett mind a külföldi, mind a magyar médiában, főként a PMC alkalmazása miatt Irak és Afganisztán kapcsán.[34] A téma rendkívül kényes, ugyanis a katonai magánvállalatok megítélése a közvéleményt, a szakértőket és a témával foglalkozó tudósokat is egyaránt megosztja, hiszen akármennyire is hatékony egy ilyen jellegű cég alkalmazása a hadműveletek során (még ha csak az objektumok őrzése-védése területén is), egy sor emberi jogi és nemzetközi jogi kérdést vet fel, ha egy állam nem a lobogója alá tartozó erőt alkalmaz, hanem egy kvázi független, kívülálló személyi kört, hiszen a PMC-k által esetlegesen elkövetett etikai vagy szakmai hibák esetén az adott alkalmazó állam saját felelőssége megkérdőjeleződhet, a kormányzat viszont megpróbálhatja elbagatellizálni azt.

[32] Christián László – Rottler Violetta: A magánbiztonság és az önkormányzati rendészet fogalomrendszere. In Christián László – Major László – Szabó Csaba (szerk.): *Biztonsági vezető kézikönyv*. Budapest, Dialóg Campus, 2019. 13–36.

[33] Pap András László: *A megfigyelés társadalmának proliferációjától az etnikai profilalkotáson át az állami felelősség kiszervezéséig.* Budapest, L'Harmattan, 2012.

[34] Varga Krisztián: Katonai biztonsági magánvállalatok amerikai alkalmazása Irakban. *Nemzet és Biztonság,* 2. (2009), 3. 57–69.

A magánszektor állami alkalmazása a kiberbiztonság területén

A különböző magánbiztonsági vállalatok részvétele már-már elkerülhetetlen a kibertérben végrehajtott műveletek esetén, már ha csak a kibertér fogalmának jellemzőire gondolunk is. A kiberműveletek során alkalmazott eszközök és módszerek esetén nincs teljesen éles határ a katonai és a polgári célú alkalmazás között. A kiberbiztonság mindennapjaink szerves részévé válásával, illetve növekedése miatt egy adott államnak nincsenek meg azok a képességei, hogy teljes mértékben meg tudja védeni saját állampolgárait, ezért a magánvállalatok bevonása elengedhetetlen; ugyanakkor, ahogy a PMC-k esetén is felmerülnek a nemzetközi jogi kérdéskörök és felelősségek, úgy ez szintén elmondható a kiberműveletekben alkalmazott magáncégek esetén. Továbbá a „zsoldos" vállalatok esetén felmerülhet annak lehetősége, hogy mint technikai szolgáltató esetleg ellenséges ország is alkalmazhatta őket.

A támadó jellegű kiberműveletekben a magánszektor alapvetően két funkciót tölthet be. Az egyik a hírszerzési műveletek, a másik pedig a tervező-támogató műveletek terepe. A Stanford Egyetem által készített tanulmány is kimondja,[35] hogy a magánvállalatok ezirányú alkalmazása kockázatokkal és előnyökkel egyaránt jár. Az előnyök főként a gyorsan fejlődő technológia és a hatékony képesség alkalmazásának kategóriájába tartoznak. A hátrányok közé a belső szabályozások és a nemzetközi kapcsolatok esetleges megsértése. Az előnyök közé sorolja a tanulmány a képességek növelésének lehetőségét, hiszen az ilyen cégek munkatársait nem kell kiképezni, alkalmazásuk rugalmas, olykor olcsóbb, mint a hivatásosoké, főként rövid távon.[36]

A kiberműveletek esetében rendre felmerül a kérdés, hogy egy állam vagy állami szervezet milyen mértékben támaszkodhat, illetve mennyire indokolt egyáltalán támaszkodnia magánbiztonsági cégekre. Figyelembe kell azonban venni a technológia rohamos fejlődését és azt a tendenciát, hogy konfliktushelyzetben a nem katonai eszközök (diplomáciai, gazdasági vagy jogi intézkedések) sikertelensége esetén egy támadó kiberművelet lehet az első katonai csapásmérés eszköze. A rendelkezésre álló jogi dokumentumok, hazai és nemzetközi szakirodalom alapján arra a következtetésre jutottam, hogy a támadó jellegű kiberműveletek esetén a magánbiztonsági vállalatok közvetlen alkalmazása

[35] Irving Lachow: The Private Sector Role in Offensive Cyber Operations: Benefits, Issues and Challenges. *SSRN Electronic Journal,* (2016).

[36] EGov: *A támadó kiberműveletek stratégiája* (2019. március 31.).

aggályos lehet, azonban az állam saját szakértőinek képzéséhez, illetve a megfelelő technikai háttér megszerzéséhez és fejlesztéséhez elengedhetetlen az ezen a területen dolgozó magánbiztonsági vállalatok alkalmazása.

Esettanulmány a magánbiztonsággal kapcsolatos vállalatok szerepéről – Stuxnet

Az egyik legkülönösebb kibertámadás, a Stuxnet a kiberháborúk új dimenzióját nyitotta meg. A 2009–2010. évben egy ismeretlen *malware* (Stuxnet) megbénította az iráni natanzi atomerőmű dúsítóját, amit Irán 2010. szeptember 25-én ismert el, azaz, hogy az atomerőmű nukleáris centrifugáiban mechanikai hibák vannak, amelyeket egy kártékony szoftver és annak mutálódott verziói okoztak. Feltételezések szerint Barack Obamához és elődjéhez, George W. Bush elnökhöz köthető a Stuxnet, megbízásukra amerikai és izraeli titkosszolgálati szakemberek hozták létre, és célja az iráni atomprogram akadályozása, illetve megbénítása volt.[37]

A támadó kiberművelet végrehajtása előtt a szakembereknek mérlegelniük kellett az atomprogram akadályozásának mikéntjét, és mivel azt fegyveresek őrizték, egy hagyományos katonai akció nagyobb kihívást jelentett volna. Az izraeli hadvezetésnek kockázatok sorával kellett számolnia az iráni atomerőművek megtámadásának tervezése során, például az 1800 km-es távolság áthidalásával, katonai veszteségekkel, a nemzetközi közvélemény negatív viszonyulásával. Gondoljunk arra, hogy az Európai Unió is óvatos az iráni atomkísérletek megítélésében! Előfordulhatott volna továbbá azonnali, nyílt bosszú Iránról vagy iránbarát terroristacsoportoktól a világ bármely pontján, bármikor izraeli, egyesült államokbeli polgárok (turisták, sportolók) ellen. A Stuxnet csak az adott környezetben, azt felismerve funkcionált, más környezetben passzív maradt. A Stuxnetet úgy kellett megírni, hogy más rendszerekben, funkciókban ne tehessen kárt, hiszen ha felfedezik, akkor az a fő célt veszélyeztette volna. Célzottan a centrifugák működésének megzavarására alkották meg. A vírus hatása (feladata) a centrifugarotorok forgási sebességének lelassítása, majd felgyorsítása volt.[38]

[37] Nagy (2018): i. m. 186.
[38] Gyebrovszki (2014): i. m. 169–170.

A kártékony szoftvert 2010 júniusában a Fehéroroszországban alapított VirusBlokAda cég fedezte fel. A cég tevékenységi köre a víruskereső szoftverek gyártása, illetve az ehhez kapcsolódó szoftverelemző és értékelő munka. Így jól látható, hogy a védelmi tevékenység területén sem elhanyagolható az egyes magánbiztonsági vállalatok szerepe. Amennyiben nem alkalmazták volna a céget, nem tudható, hogy a kártékony szoftver milyen jellegű károkat okozott volna, a fentiekben leírtak szerint akár súlyosabb következményei is lehettek volna.[39] A vírus elemzésében, illetve korábbi verziójának megállapításában hathatós szerepe volt a szintén a magánszektorhoz tartozó Symantec nevű cégnek.

Összegzés

Összefoglalásul elmondható, hogy a technológiai fejlődés következményeként a kiberbiztonság és a kibertér kiemelt prioritássá vált. Már-már közhely, hogy a nemzetközi összefogás elengedhetetlen a kiberbűnözés és a terrorizmus visszaszorítása érdekében, azonban érdekes perspektívákat tár fel a magánszektor, azon belül is a magánbiztonsági vállalatok bevonása a különböző kiberműveletek végrehajtásába, illetve az állami szervezetek alkalmazottainak szakirányú képzésébe.

Az elkövetkezendő években egyre nagyobb szerepet fognak játszani a kibertérben végbemenő műveletek, amelyeknek nem csupán katonai[40] célpontjai lehetnek, hanem polgári, kiemeltképpen kritikus infrastruktúrabeliek. A Stuxnet esetében is láttuk, hogy a kártékony szoftver felismerésében, illetve elemzésében egyértelmű szerepe volt a különböző cégeknek. Azok az országok, amelyek nem fejlesztik kiberképességeiket, rendkívüli hátrányba kerülhetnek, így az állam feladata, hogy a lehető legszélesebb körű együttműködés keretei között védje a kiberbiztonságot, amelybe beletartozik a kutatások szorgalmazása, egyetemi képzések indítása, illetve a megfelelő *know-how*-val rendelkező szakemberek alkalmazása. Mindezek megteremtéséhez elengedhetetlen a magánszektor közreműködése, illetve bevonása az állam kibertérben végzett tevékenységébe. A kiberhadviselés területén is előszeretettel alkalmaznak nem állami, hanem kvázi magánszektorbeli hackereket, hiszen a *Tallinni kézikönyv* kimondta: a zsol-

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

[40] Berki (2016): i. m.

dosok más megítélés alá esnek, mint egy állam hivatásos katonái, így a jövőben várható tendencia, hogy az egyes állami szereplők saját identitásuk leplezése érdekében zsoldosokat alkalmaznak a kibertérben, akik végrehajtják a támadó műveleteket az ellenséges ország valamilyen infrastruktúrája ellen, így próbálva csökkenteni az esetleges nemzetközi botrányt vagy a jogszerű lehetséges katonai retorzió esélyét. A fentiek nyomán jó eséllyel kijelenthető, hogy az egyes PMC-k működési területe a jövőben lehetséges irányváltás elé néz, és a hagyományos őrzési-védési, logisztikai feladatok mellett sokkalta hangsúlyosabb szerepet kap az egyes kiberműveletekben történő részvétel. Figyelemmel arra, hogy egy adott állam saját infrastruktúrájának (főként, ha kritikus infrastruktúra) kibertéri védelmét a megfelelő ellenőrzés alatt akarja tudni, valószínűbb, hogy a magáncégeket nem védelmi, hanem támadó jellegű műveletek során fogják inkább alkalmazni, esetleg az állam saját alkalmazottainak kiképzése során kaphatnak nagyobb szerepet a kiberbiztonság területén jártas magánszektorbeli szakértők.

Irodalomjegyzék

Berki Gábor: Kiberháború, kiberkonfliktusok. In Pintér István (szerk.): *A virtuális tér geopolitikája. Tanulmánykötet.* Budapest, Geopolitikai Tanács Közhasznú Alapítvány, 2016. 247–284.

Christián László: A magánbiztonság aktuális nemzetközi trendjei, rövid hazai helyzetértékeléssel. In *Modernkori veszélyek rendészeti aspektusai.* Pécs, Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport – Magyar Rendészettudományi Társaság, 2015. 57–63. Online: https://core.ac.uk/download/pdf/356664168.pdf

Christián László: Magánbiztonsági számvetés. In Dobák Imre – Hautzinger Zoltán (szerk.): *Szakmaiság, szerénység, szorgalom. Ünnepi kötet Boda József 65. születésnapja alkalmából.* Budapest, Dialóg Campus, 2018.

Christián László – Rottler Violetta: A magánbiztonság és az önkormányzati rendészet fogalomrendszere. In Christián László – Major László – Szabó Csaba (szerk.): *Biztonsági vezető kézikönyv.* Dialóg Campus, 2019. 13–36.

Dévai Dóra: A kiberfegyver koncepció evolúciója., *Hadmérnök,* 14. (2019), 2. 272–280. Online: https://doi.org/10.32567/hm.2019.2.22

EGov: *A támadó kiberműveletek stratégiája* (2019. március 31.). Online: https://hirlevel.egov.hu/2019/03/31/a-tamado-kibermuveletek-strategiaja/

Fekete-Karydis Klára – Lázár Bence: A kibervédelem katonai dimenziói. *Honvédségi Szemle,* 148. (2020), 3. 44–54. Online: https: //doi.org/10.35926/HSZ.2020.3.4

Gyebrovszki Tamás: Stuxnet – mint az első alkalmazott kiberfegyver – a Tallini Kézikönyv szabályrendszere szempontjából. *Hadmérnök,* 11. (2014), 1. 164–174. Online: http://hadmernok.hu/141_16_gyebrovszkyt.pdf

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

Haig Zsolt: *Információ, társadalom, biztonság.* Budapest, Nemzeti Közszolgálati Egyetem, 2015.

Irving Lachow: The Private Sector Role in Offensive Cyber Operations: Benefits, Issues and Challenges. *SSRN Electronic Journal,* (2016). Online: https://dx.doi.org/10.2139/ssrn.2836201

Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms (2010. november 8.). Online: https://irp.fas.org/doddir/dod/jp1_02.pdf

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

Kovács László: A kiberbiztonság és a kiberműveletek megjelenése Magyarország új Nemzeti Biztonsági Stratégiájában. *Honvédségi Szemle,* 148. (2020), 5. 3–18. Online: http://dx.doi.org/10.35926/HSZ.2020.5.1

Kovács László – Sipos Marianna: A Stuxnet és ami mögötte van: Tények és a cyberháború hajnala. *Hadmérnök,* 5. (2010), 4. 163–172. Online: http://hadmernok.hu/2010_4_kovacs_sipos.pdf

Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról szóló 1838/2018. (XII. 28.) Korm. határozat alapján a hálózati és információs rendszerek biztonságára vonatkozó Stratégia. Online: https://bit.ly/3u0ohee

Muha Lajos – Krasznay Csaba: *Az elektronikus információs rendszerek biztonságának menedzselése.* Budapest, Nemzeti Közszolgálati Egyetem, 2014.

Nagy Zoltán András: Kiberháborúk kora. In *Magyar Tudomány Napja a Délvidéken – 2018. Tanulmánykötet.* Vajdasági Magyar Tudományos Társaság, 2018. 174–193.

Nagyné Bereczki Szilvia – Nagy József: *Magánbiztonság és kritikus infrastruktúra védelem*. Budapest, 2014. Online: https://securimaster.com/maganbiztonsag-es-kritikus-infrastruktura-vedelem/

NATO CCDCOE: *The Tallinn Manual.* 2021. Online: https://ccdcoe.org/tallinn-manual.html

Pap András László: *A megfigyelés társadalmának proliferációjától az etnikai profilalkotáson át az állami felelősség kiszervezéséig.* Budapest, L'Harmattan, 2012.

Rottler Violetta: Gondolatok a magánbiztonság köréből. *Magyar Rendészet,* 19. (2019), 4. 81–95. Online: http://doi.org/10.32577/mr.2019.4.6

Varga Krisztián: Katonai biztonsági magánvállalatok amerikai alkalmazása Irakban. *Nemzet és Biztonság,* 2. (2009), 3. 57–69. Online: www.nemzetesbiztonsag.hu/cikkek/varga_krisztian-katonai_biztonsagi_maganvallalatok_amerikai_alkalmazasa_irakban.pdf

Jogi szabályozók

JP 1-02 Department of Defense Dictionary of Military and Associated Terms
1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról
1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról
1393/2021. (VI. 24.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról

7. fejezet

Nyomásgyakorlás a kritikus információs infrastruktúrák támadásán keresztül

A Digital Pearl Harbortól a digitális ökoszisztéma teljes támadásáig

Kovács László

Bevezetés

Digitálissá vált világunk azokra az eszközökre és rendszerekre épül, amelyeket összefoglaló néven kritikus infrastruktúráknak hívunk. Ezekben számos infokommunikációs rendszer található, amelyek szintén kritikusak vagy más szóval létfontosságúak a 21. század társadalmának működéséhez. A kritikus információs infrastruktúrák testesítik meg korunk legjellemzőbb vonását, amikor digitális ökoszisztémáról beszélünk.

A digitális kor és az annak idegrendszereként is felfogható kritikus információs infrastruktúrák az 1970-es évek óta hatalmas fejlődésen mentek keresztül. Ma nyugodtan kijelenthetjük, hogy nincs olyan területe az életünknek, ahol ne lennének jelen, vagy legalább ne lenne hatásuk ezeknek az infrastruktúráknak, illetve azok egyes elemeinek. A digitalizációnak és az információtechnológiai forradalomnak köszönhetően a mai terminológiával élve fizikai vagy hagyományos infrastruktúrák kiegészülnek olyan információs rendszerekkel, eszközökkel és berendezésekkel, amelyek szintén elengedhetetlen részei a mindennapjainknak. Ebből következően ezek az információs infrastruktúrák szintén nélkülözhetetlenek, azaz kritikusak, létfontosságúak. Ráadásul „hagyományos" infrastruktúráink jelentős részében ezek megtalálhatóak, hiszen azok vezérlése vagy irányítása ezeken a nélkülözhetetlenné vált információs rendszereken keresztül valósul meg.

A fentiek azonban nemcsak olyan előnyöket hordoznak magukban, mint például a globális szolgáltatások és azok napi 24 órás elérése, hanem bizony

https://doi.org/10.36250/01079_07

https://orcid.org/0000-0002-6403-0650

hatalmas kihívás elé is állítják magát a társadalmat is, hiszen ezeknek az infrastruktúráknak – lévén létfontosságúak – minden nap minden percében zavartalanul és kielégítő módon kell működniük ahhoz, hogy a társadalom különböző funkciói működjenek.

Az viszont már az 1990-es években világossá vált, hogy az infokommunikációs rendszerek hatalmas ütemű fejlődését azok védelme nem mindig, vagy csak késve tudja követni. Ezek a rendszerek, legyen szó kritikus infrastruktúráról vagy kritikus információs infrastruktúráról, sebezhetőek, sőt önmagukban is számos sérülékenységet hordozhatnak. Ezeket pedig ártó szándékkal – akár előre nem is mindig jelezhető módon és nem megjósolható időben – valakik ki fogják használni.

Anakronisztikus ellentétnek tűnik tehát az a kettősség, amely egyrészt ezen rendszerek létfontosságúvá válásában, másrészt azok támadhatóságában jelentkezik. Ha ezek a rendszerek valóban elengedhetetlenek a mindennapi élet működőképességének fenntartásában, akkor azok működésbeli kiesése nem megengedhető, viszont ennek biztosítása majdhogynem lehetetlen vállalkozásnak tűnik.

Több olyan elképzelt forgatókönyv is született, amely pont a fent említett, a kritikus infrastruktúrákat célzó támadásokat és azok hatásait kívánta megvizsgálni. Ezek közül a Digitális Pearl Harbor *(Digital Pearl Harbor)* a 2000-es évek elején az Amerikai Egyesült Államokban, a Digitális Mohács pedig a 2000-es évek végén Magyarországon született. Mindkét forgatókönyv meglehetősen nagy, de sok esetben vegyes véleményeket kiváltó visszhangot kapott. Jelen fejezetünk arra keresi a választ, hogy a két elképzelt forgatókönyvben is felvázolt támadássorozattal valóban nyomást lehet-e gyakorolni egy országra ma, a 21. század első évtizedeiben.

A kritikus infrastruktúrák és a kritikus információs infrastruktúrák, valamint azok szerepe

Az Európai Unió 2020 végén megjelent új kiberbiztonsági stratégiája egyenesen globális kockázatnak tekinti a kritikus infrastruktúrák rosszindulatú támadását. A stratégia rámutat, hogy az internet decentralizált kialakítású és felépítésű, egyértelműen meghatározható központi szervezet vagy struktúra nélkül, amely hozzájárul a (hálózati) forgalom exponenciális növekedéséhez, miközben viszont állandósultak a rosszindulatú – sok esetben célzott – támadások. Ugyanakkor az internet működése szempontjából olyan kiemelten fontos szolgáltatások,

mint többek között a DNS (*domain name system,* domén név rendszer) vagy az alapvető szolgáltatásokat nyújtó megoldások egyre inkább néhány magáncég tulajdonában koncentrálódnak. Mindez „[…] az európai gazdaságot és társadalmat kiszolgáltatottá teszi olyan zavaró geopolitikai vagy technikai események számára, amelyek érintik az internet lényegét vagy ezek közül egy vagy több társaságot. A világjárvány miatt megnövekedett internethasználat és a változó szokások még inkább rávilágítottak a digitális infrastruktúrától függő ellátási láncok törékenységére."[1]

Természetesen az olyan nemzetközi szervezetek, mint az Európai Unió vagy akár az egyes országok nem 2020-ban vették először górcső alá a kritikus infrastruktúrákat, illetve a kritikus információs infrastruktúrákat, valamint azok védelmének szükségességét.

Az Európai Unióban már a 2000-es évek elején megkezdődött – nemcsak a gondolkodás, hanem – a kritikus infrastruktúrák védelmével foglalkozó gyakorlati és jogszabályalkotó munka. Az olyan előkészítő munkák után, mint például az EU zöld könyve – hivatalos címén *Zöld könyv a létfontosságú infrastruktúrák védelmére vonatkozó európai programról*[2] –, az unió 2006-ban jelentette meg az úgynevezett kritikusinfrastruktúra-védelem európai programját (*European Programme for Critical Infrastructure Protection,* röviden: EPCIP). Az EPCIP valódi áttörésként értelmezhető, hiszen egységes szerkezetbe foglalta az EU gondolkodását a területen, valamint kötelező érvényű szabályozást jelentett a tagállamok számára.[3]

> „Az EPCIP lefektette a kritikus infrastruktúrák védelmének növelését célzó minden olyan tevékenységnek az általános kereteit, amelyek az EU minden tagországára, valamint minden ágazatra érvényesek. A korábbi irányelvektől eltérően az EPCIP már nemcsak a terrorizmust tekintette fő fenyegetésnek, hanem az egyéb bűncselekményeket, illetve a természeti és ipari katasztrófákat is ide sorolta."[4]

Az európai uniós szabályozási munka, és nem utolsósorban a kritikus infrastruktúrák kitettsége felismerésének eredményeként hazánkban is megkezdődött a terület szabályozása. Az első kézzelfogható hazai szabályozó 2008-ban jelent

[1] JOIN(2020) 18 final. Közös közlemény az Európai Parlamentnek és a Tanácsnak. Az EU kiberbiztonsági stratégiája a digitális évtizedre.

[2] COM(2005) 576. Az Európai Közösségek Bizottsága: *Zöld könyv a létfontosságú infrastruktúrák védelmére vonatkozó európai programról.*

[3] European Commission: *European Programme for Critical Infrastructure Protection* (2006).

[4] Kovács László: *A kibertér védelme*. Budapest, Dialóg Campus, 2018. 223.

meg kormányhatározat formájában.[5] Ennek egyik legnagyobb eredménye – azon kívül, hogy megjelent, és ezzel nem csak bizonyította a terület fontosságát, hanem el is kezdődött a védelem szabályozott, nemzeti szinten is koordinált módú szervezése – az volt, hogy számbavette és felsorolta azokat az infrastruktúra-ágazatokat és -alágazatokat, amelyek valóban kritikusnak tekinthetők Magyarország vonatkozásában is.

Hazánkban a kritikusinfrastruktúra-védelem területén az igazi áttörést azonban 2012 hozta meg. Ekkor jelent meg hosszas előkészítő munka után a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény, amelyet röviden csak kritikus-infrastruktúra-törvényként vagy a hivatalos címe első két szava alapján rövidítve csak Lrtv.-ként azonosítunk.[6] Meg kell jegyezni, hogy jelen fejezetben is – a törvényi szabályozás által használt létfontosságú rendszerek és rendszerelemek kifejezések mellett – a kritikus infrastruktúra, illetve a kritikus információs infrastruktúra terminológiát használjuk azok elterjedtsége miatt.

Az Lrtv. szerint a kritikus infrastruktúra

> „meghatározott ágazatok valamelyikébe tartozó eszköz, létesítmény vagy rendszer olyan rendszereleme, amely elengedhetetlen a létfontosságú társadalmi feladatok ellátásához – így különösen az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához –, és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna."[7]

Fontos megemlíteni, hogy a törvény meghatározza az európai értelemben vett kritikus infrastruktúra fogalmát is: „a törvény alapján kijelölt olyan létfontosságú rendszerelem, amelynek kiesése jelentős hatással lenne – az ágazatokon átnyúló kölcsönös függőségből következő hatásokat is ideértve – legalább két EGT-államra."[8]

E meglehetősen bonyolult megfogalmazás azonban leegyszerűsítve azt takarja, hogy a 21. század társadalmi működése feltételez számos olyan rendszert, amelyek nélkül nem, vagy csak nagyon nehezen tudnánk elképzelni életünket. Ennek megfelelően valóban teljes joggal használhatjuk a *létfontosságú*

[5] 2080/2008. (VI. 30.) Kormányhatározat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról.

[6] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.

[7] 2012. évi CLXVI. tv. 1. § *f.* pont.

[8] 2012. évi CLXVI. tv. 1. § *c.* pont.

jelzőt, hiszen ezeknek a rendszereknek, vagy akár ezek egyes rendszerelemeinek a folyamatos működése ma már nem csak a kényelem és az életminőség javításában jelentkezik, hanem ezek nélkül gyakorlatilag nem jutnánk hozzá azokhoz a szolgáltatásokhoz, amelyek a mindennapi életünk alapjai. Nagyon leegyszerűsítve: e rendszerek nélkül emberek sokaságának az élete kerülne – akár már rövid időn belül is – veszélybe.

Az említett rendszerek azonban ma már nemcsak fizikai objektumok, hanem nagyon sok esetben információs vagy infokommunikációs rendszerek, amelyek önmagukban vagy az adott kritikus infrastruktúra részeként szintén kritikusak, azaz működésük létfontosságú a társadalom egésze szempontjából. Az említett hazai kritikusinfrastruktúra-védelmi törvény végrehajtási rendeleteként kiadott kormányrendelet meghatározza a kritikus információs rendszer és létesítmény fogalmát is: „a társadalom olyan hálózatszerű, fizikai vagy virtuális rendszerei, eszközei és módszerei, amelyek az információ folyamatos biztosítása és az informatikai feltételek üzemfolytonosságának szükségességéből adódóan önmagukban létfontosságú rendszerelemek, vagy más azonosított létfontosságú rendszerelemek működéséhez nélkülözhetetlenek.”[9] Ez a meghatározás nagyon jól összefoglalja, hogy ma már nemcsak a hagyományos értelemben vett infrastruktúrák, hanem az ezek vezérlését, működését ellátó információs rendszerek közül önmagában is nagyon sok kritikus infrastruktúrának minősül. A jogszabály 10 fő ágazatot – energia, közlekedés, agrárgazdaság, egészségügy, társadalombiztosítás, pénzügy, infokommunikációs technológiák, víz, honvédelem, közbiztonság-védelem – és több mint 30 alágazatot határoz meg kritikus infrastruktúraként.[10]

A kritikus információs infrastruktúrák európai szabályozásában 2016-ban született meg az úgynevezett NIS direktíva azzal a legfontosabb feladattal, hogy olyan egységes követelményrendszert határozzon meg, amely az összes európai uniós tagországban garantálhatja azt, hogy a hálózati és információs rendszerek egyformán biztonságosak legyenek.[11] Legalábbis elvileg. Ugyanis a NIS megalkotását pont az a felismerés indukálta, hogy az EU tagországainak információs rendszerei eltérő fejlettségűek, és eltérő biztonsági állapotban vannak. Ugyanakkor ezek a rendszerek a hálózatokon keresztül összeköttetésben

[9] 65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról. 1. § 3. pont.

[10] 1. melléklet a 2012. évi CLXVI. törvényhez.

[11] 2016/1148. Az Európai Parlament és a Tanács (EU) irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről.

állnak egymással, így az egyik tagország hiába rendelkezik megfelelő biztonsági szintű információs rendszerrel, ha egy másik ország kevésbé biztonságos rendszerén keresztül az támadhatóvá válik. A NIS nagy előrelépés lehet abban, hogy a tagországok egyformán értékeljék a hálózati és információs rendszerek biztonságát, legyen – többé-kevésbé – homogén és egységes stratégiájuk ezek megvédésére, illetve a biztonságuk folyamatos fejlesztésére. A NIS meghatározza azokat a legfontosabb kritikus információs infrastruktúrákat, amelyek védelme az egész unióban a lehető legmagasabb szinten meg kell hogy valósuljon. Ezek az infrastruktúrák, illetve ágazatok – nem meglepő módon – sok esetben egybeesnek a hazai kritikusinfrastruktúra-ágazatokkal. Ezek az ágazatok: az energia, a közlekedés, a banki szolgáltatások, a pénzügyi piaci infrastruktúrák, az egészségügy, az ivóvízellátás és -elosztás, valamint a digitális infrastruktúra. A felsorolásból jól látszik, hogy ezek mindegyike olyan szolgáltatás, illetve rendszer, amely határokon átnyúlik, és úgy hálózza be a tagországok mindegyikét, hogy gyakorlatilag az összes EU-országot összeköti egymással. Ezek esetében a(z) – határokon átnyúló – interdependencia, illetve az ágazatok jellegéből adódó gazdasági és társadalmi működés függősége nem szorul magyarázatra. Ennek megfelelően a közös elvek mentén történő egységes, a biztonság magas szintjének megvalósulására irányuló szabályozás szükségessége teljes mértékben indokolt. A probléma azonban a szabályozás betartásának az ellenőrzésében van, hiszen abból a szempontból nagyon liberális ez a szabályozás.

Ugyanakkor azt ma már világosan lehet látni, hogy az egyes kritikus információs infrastruktúrákon belül is vannak olyan rendszerek, rendszerelemek vagy akár szolgáltatások, amelyek nélkül maga az adott rendszer sem lenne képes működni. Az internet esetében ilyen szolgáltatás például a DNS-szolgáltatás. A doménnévrendszer-szolgáltatás nélkül rövid ideig még működik az interneten elérhető szolgáltatások egy része, de hiányában hamar érezhető szolgáltatáskiesés lép fel, hosszabb idő után pedig már nagyon nehézkesen vagy egyáltalán nem érhetők el a szolgáltatások. A DNS-rendszer támadására, illetve annak kísérletére több alkalommal volt példa, az egyik legsikeresebb támadás 2016 októberében következett be az Egyesült Államokban. Ekkor a Dyn nevű keleti parti DNS-szolgáltató szervereit érte olyan DDoS-támadás (*distributed denial of service,* elosztott túlterheléses támadás), amely miatt a cég szolgáltatásai leálltak. Jól felépített támadássorozat volt több hullámban, amelyben több tízezer, egyes elemzések szerint akár százezer[12] IoT- (*Internet of Things,* a dolgok internete)

[12] Trend Micro: Operation Pawn Storm: Fast Facts and the Latest Developments (2016. január 16.).

eszköz vett részt, amelyek túlnyomó részben Mirai *malware*-rel fertőződtek meg korábban. A bekövetkezett szolgáltatáskiesés messze túlmutatott az Egyesült Államok határain,[13] mert számos Ázsia irányába menő IP-cím-tartománynév feloldása is ezeken a megtámadott szervereken keresztül valósult meg, így azok a szolgáltatások is elérhetetlenné váltak.[14]

Az egyes kritikus információs infrastruktúrákon belül meglévő függőségre a DNS mellett másik például a felhőszolgáltatások adódnak. Azok a felhőszolgáltatások, amelyek a nagy közösségi platformoknak nyújtanak létfontosságú háttértámogatást, szintén kritikusak. Az ezekben a szolgáltatásokban bekövetkező rendszer- vagy működéskiesés súlyos, akár globális kihatással lehet azokra a rendszerekre, amelyeket emberek (felhasználók) milliói naponta használnak. A szolgáltatáskiesés banalitására, illetve ezeknek a rendszereknek a ma már nélkülözhetetlen voltára az egyik legjobb példa az az eset, amely 2021. május közepén történt. A Fastly felhőszolgáltató cég, amely többek között az Amazonnak, a Redditnek és számos online folyóiratnak, hírportálnak, közösségimédia-felületnek is szolgáltat háttérmegoldásokat, egyik ügyfele megváltoztatta a szolgáltatási beállításait. Az új beállítás teljesen legitim módon történt, azonban annak nem várt hatása lett. A beállítás olyan hibát *(bug)* generált, amely következtében a Fastly ügyfeleinek 85%-a hibát tapasztalt az általa igénybe vett folyamatokban, és a szolgáltatásai leálltak.[15] A működéskiesés, bár nagyon rövid ideig – csak egy órán keresztül – tartott, jól rávilágít arra, hogy ma már az internetes szolgáltatások mögött is kritikus infrastruktúrák – legyenek azok informatikai eszközök és rendszerek vagy informatikai szolgáltatások – működnek, amelyek kiesése akár világméretű hatással jár.

Támadások a kritikus rendszerek ellen: elképzelt támadások és az azokból levonható következtetések

A 2000-es évek elején több olyan elméleti forgatókönyv is született, amely azt volt hivatott felmérni, hogy az egyre komplexebbé váló infrastruktúrák egyes elemeinek támadása milyen közvetlen vagy nem várt közvetett hatással

[13] Lily Hay Newman: What We Know About Friday's Massive East Coast Internet Outage. *Wired.com,* 2016. október 21.

[14] Kovács (2018): i. m. 92.

[15] Jane Wakefield: One Fastly Customer Triggered Internet Meltdown. *BBC News,* 2021. június 9.

járna. Ezek közül a szcenáriók közül az egyik legnagyobb hatású forgatókönyv 2002-ben az amerikai Naval War College és a Gartner cég együttműködésében, ipari szereplők bevonásával készült. Egy úgynevezett hadijáték alkalmával azt vizsgálták, hogy a kibertérben elkövetett terrortámadások mennyiben és milyen mértékben lennének hatással az Egyesült Államok gazdaságára és politikai vezetésére. A több mint 80 fő bevonásával lezajlott hadijáték szereplőit, akik között voltak különböző informatikai szolgáltatók, illetve olyan kritikusinfrastruktúra-üzemeltetők is, mint például villamosenergia-ellátás, kommunikációs rendszerek vagy internetszolgáltatás, több csapatra osztották. Az egyik csoport, a támadó, azaz Red Team az Egyesült Államok kulcsfontosságú rendszerei elleni kibertámadásokat szimulált. A támadások az előre kiválasztott négy kritikusinfrastruktúra-ágazat – a telekommunikáció, az internet és a számítógép-hálózati szolgáltatások, a villamosenergia-ellátás, valamint a pénzügyi szektor – ellen irányultak. A négy ágazatot négy különválasztott kiberterrorista-csoportot szimuláló csapat támadta különböző kibertéri eszközökkel, egy ötödik csoport pedig a négy támadó csapat akcióit koordinálta. A szimulált kiberterrorista-csoportok dedikáltan államnál kisebb csoportokat jelentettek, és az államok feltételezhető erőforrásainál kevesebb lehetőséggel rendelkeztek. A kevesebb mint 50 millió dollár költségvetéssel megvalósított – hangsúlyosan – kibertámadások mellett, korlátozott fizikai támadások szimulált kivitelezésére volt csak mód. Mind a négy támadó csoport csak 8-8 fizikai támadásra kapott lehetőséget, ezzel ösztönözve azt, hogy ezek célpontjait úgy válasszák ki, hogy az azokkal párhuzamosan elkövetett kibertámadások egymás hatásait felerősítsék. A kivitelezés minden kritikusinfrastruktúra-szektorban stratégiai tervezéssel kezdődött, majd következett a felderítés, amely során meghatározták a legfontosabb célpontokat és azok támadásának célszerű és hatékony módját. Az ezeket a fázisokat követő támadások szimulációja során azt vizsgálták, hogy azok mennyire hatékonyak, illetve az okozott károkat mennyi időn belül tudja a célpont felszámolni.

A Digitális Pearl Harbor, a szimulált, kritikus infrastruktúrákat ért kibertámadások forgatókönyve számos érdekes és fontos tanulsággal járt. A villamosenergia-ellátás vonatkozásában az a megállapítás született, hogy egyes kibertámadásokkal nem okozható nagy méretű szolgáltatáskiesés, azok csak szigetszerűen következnek be.[16] Az ipari SCADA-k (*supervisory control and data acquisition,*

[16] Eric Purchase – French Caldwell: Digital Pearl Harbor: A Case Study in Industry Vulnerability to Cyber Attack. In Malek Manu – Ghosh Sumit – Edward A. Stohr (szerk.): *Guarding Your Business: A Management Approach to Security.* Boston, Spinger, 2004. 49.

felügyeleti, irányító- és adatgyűjtő rendszerek) esetében is hasonló megállapítás született, azaz azok az esetek többségében – ne felejtsük el, hogy ekkor még csak 2002-t írtunk! – nem csatlakoznak az internethez, azaz azok támadása nem elhanyagolható veszélyforrás, de azokkal sok esetben szintén csak szigetszerűen bekövetkező rendszerkiesések okozhatók.[17] Ugyanakkor a pénzügyi szektor kiváló célpontja lehet a kibertámadásoknak, ugyanis ezekkel előidézhető a közvetlen károkon túl az adott ország kormányába vetett bizalom megrendülése. Az internet és az IT-szektor támadása már egészen más eredményt mutatott. Bár ezeket is nehéz támadni, mert ezekhez megfelelő szakértelem szükséges, azonban az interneten a terrorcsoportok hatékonyabban tudnak rejtőzködni akár az akcióik szervezésekor, akár az egymással történő kommunikációjuk alatt.

A Digitális Pearl Harbor legnagyobb tanulsága az, hogy a kritikus infrastruktúrák komplex és összehangolt akciókkal eredményesen támadhatók, és bár a különböző ágazatokban eltérő mértékű kár okozható, azok összekapcsoltsága révén a jól megválasztott célpontok támadása ágazatokon átnyúló, súlyos károkat képes okozni. A végső konklúzió tehát az, hogy a felvázolt veszélyek nagyon is reálisak.

Ezt erősíti az a tény is, hogy a 2000-es évek óta eltelt időszak alatt az IoT-eszközök elterjedése robbanásszerű volt, ugyanakkor biztonságuk ezt a fejlődést nem követte. Az IoT-eszközökön keresztül viszont számos olyan támadás indítható, amely már az OT-n (*operational technology,* működési technológia) keresztül fejti ki hatásait, sokszor a fizikai térben. Ezt nagyban segíti az IoT- és az OT-eszközök nagy fokú konvergenciája, amely leginkább a SCADA, az ICS (*industrial control system,* ipari irányítási rendszer), illetve az RTU-k (*remote terminal unit,* távoli irányítási egység) összekapcsoltságában jelentkezik.[18]

A Digitális Pearl Harbor szcenárió sok kritikát is kapott, amely elsősorban a kissé hatásvadász címéből eredt, mégis pont ez az, amely felhívja a figyelmet még ma is a kritikus infrastruktúrák területének fontosságára, nemcsak a mindennapi civil életünkben, hanem akár a hadseregek vonatkozásában is:

> „[k]ritikusai ellenére a Pearl Harbor-analógia kitart, mert hasznos keretet ad arra, hogy a kibertértől való függőség hogyan generál sebezhetőségeket, amelyeket az ellenségek kihasználhatnak. […] Figyelmeztetés arra nézve is, hogy az Egyesült Államok és szövetségesei jelenlegi taktikai háborús képességének nagy része attól függ, hogy

[17] Purchase–Caldwell (2004): i. m. 50.

[18] Anna Ribeiro: Protecting Critical Infrastructure Supply Chain Security From Cyber Attacks. *Industrial Cyber,* 2021. május 6.

> képesek-e tájékozódni, és biztonságossá tenni azt a kiberteret, ahol erőik és fegyverrendszereik összekapcsolódnak, és azok vezetése megtörténik."[19]

A Digitális Pearl Harborhoz hasonló, de magyarországi forgatókönyv született 2009-ben Digitális Mohács címmel. Az analógia, azaz az országok egy nevezetes, de annál inkább tragikus történelmi eseményének mint hívónévnek a választása korántsem a véletlen műve. A Digitális Mohács forgatókönyv fő célja az volt, hogy felhívja a figyelmet arra a tényre, amelyet a Digitális Pearl Harbor esetében már láthattunk, nevezetesen, hogy a kritikus infrastruktúrák és ezen belül is a kritikus információs infrastruktúrák támadhatók, aminek következményei beláthatatlanok. A Digitális Mohács egy elképzelt támadássorozat egyes elemeit mutatja be, majd azok hazánk gazdasági és politikai életére gyakorolt hatásait elemzi. A történet pénzügyi manipulációt sejtető megtévesztő médiaművelettel indul, majd ezt követi annak vizsgálata, hogy a pénzügyi rendszer mennyire támadható a kibertérből. Ezzel a fázissal párhuzamosan az internet támadhatósága is vizsgálat tárgya volt. A szcenárió egy következő támadási fázist feltételezve azt is megvizsgálta, hogy a közlekedési infrastruktúra különböző vezérlőrendszerei hogyan reagálnának, illetve milyen következményei lennének egy-egy kibertérből érkező támadásnak. Ugyanakkor a támadási sorozat befejező, ámde legnagyobb kárt okozó fázisa az energiaszektor, ezen belül is a villamosenergia vezérlőrendszereinek a támadása volt.

A Digitális Mohács forgatókönyv rendkívül egyszerűen kivitelezhető, de hatásaiban messze az egyes ágazatokon túlnyúló támadássorozatot vázolt fel. Az ezek elemzéséből levont legfőbb következtetés olyan megállapításokat tett, amelyek a védelem közös felelősségében és az állami szinten koordinált védekezés szükségességében összegezhetőek. A tanulmány mindezt így foglalta össze:

> „[t]ermészetesen a különböző infrastruktúrákat üzemeltetők bizonyos szintig fel vannak készülve az esetleges támadásokra, illetve ezek kezelésére. Abban az esetben azonban, ha az ország több kritikus információs infrastruktúráját éri egyszerre, párhuzamosan komplex – tehát egy időben jelentkező informatikai és fizikai – támadás is, akkor koordináció hiányában nem biztosítható megfelelő szintű védelem. Mindezeknek megfelelően a védelem területén egy átfogó – a kritikus információs infrastruktúrák komplex védelmére vonatkozó – védelmi stratégia kidolgozása az első lépés, amelyet meg kell tenni."[20]

[19] Emily O. Goldman – Michael Warner: Why a Digital Pearl Harbor Makes Sense … and Is Possible. In George Perkovich – Ariel E. Levite (szerk.): *Understanding Cyber Conflict. 14 Analogies.* Washington (DC), Georgetown University Press, 2017. 147.

[20] Kovács László – Krasznay Csaba: Digitális Mohács. Egy kibertámadási forgatókönyv Magyarország ellen. *Nemzet és Biztonság,* 3. (2010), 1. 56.

Támadások a kritikus rendszerek ellen: a nyomásgyakorlás módszerei és az azokból levonható következtetések

Az kétségtelen módon kiderül a fenti, elméletben felállított szcenáriókból – azaz a Digitális Pearl Harbor, illetve a Digitális Mohács forgatókönyvből, majd az azokból levonható következtetésekből –, hogy a kritikus információs infrastruktúrákon keresztül egy fejlett digitális ökoszisztémával rendelkező országra jelentős nyomás gyakorolható ezeken a rendszereken keresztül. Ez a nyomásgyakorlás, függetlenül annak céljától, amely lehet politikai, gazdasági, társadalmi vagy akár katonai, minden valószínűséggel több fázisból áll. A fázisok közül az első és a legtöbb időt igénybe vevő az információszerzés, valamint a megszerzett adatok és információk feldolgozása, illetve kiértékelése, majd ezt követi a tervezés és a célmeghatározás, a támadás végrehajtása, végül pedig a hatáselemzés.

Annak vizsgálatára, hogy valóban működik-e egy adott ország vonatkozásában a nyomásgyakorlás a kritikus infrastruktúrákon, illetve a kritikus információs infrastruktúrákon keresztül, az egyik kínálkozó módszer, ha felidézünk néhány, az elmúlt időszakban a kritikus infrastruktúrát ért támadást.

2020 áprilisában az egyébként súlyos vízellátási problémákkal küzdő Izrael vízszolgáltatását érték támadások. Az egyik támadás mezőgazdasági vízszivattyúkat célzott Galilea felső részén, ahol azok leállását sikerült elérni, míg egy másik az ország közepén lévő ivóvízellátási rendszereket támadta a kibertérből. Az ország vízügyi hatósága megerősítette a támadások tényét, de közleményük szerint Izrael vízrendszerében nem történt jelentős kár. A hivatalos források nem erősítették meg, de hírügynökségek Iránt sejtették a támadások hátterében. Ugyanakkor ezek a nem hivatalos források a támadások más dimenzióit is felvázolták, amely szerint Irán nemcsak a vízszivattyúk leállítását célozta, hanem az ivóvízrendszer klórszintjének emelését is el akarta érni. Abban az esetben, ha a támadásnak ez a szakasza bekövetkezett volna, akkor emberek százait betegíthette volna meg a magas klórkoncentráció.[21] Ugyanakkor az izraeli Nemzeti Kiberügyi Igazgatóság akkori vezetője, Yigal Unna egy hivatalos nyilatkozatában, bár név szerint nem említette Iránt, azt elmondta, hogy a támadások nemcsak az ivóvíz klórszintjének emelésére, hanem a klór mellett más vegyi anyagok bejuttatására is kísérletet tettek. Nyilatkozatában Unna a kibertéri támadások

[21] Times of Israel: Cyber Attacks Again Hit Israel's Water System, Shutting Agricultural Pumps. *Times of Israel,* 2020. július 17.

fizikai térben megnyilvánuló hatásait vetítette előre: „[v]alami olyasminek lehetünk tanúi, aminek célja a valós élet, és nem az informatika vagy az adatok károsítása."[22]

2020 decemberében egy másik, első ránézésre nem a kritikus infrastruktúrákkal összefüggő támadásra derült fény. 2020. december 8-án a FireEye amerikai kiberbiztonsági vállalat egyik hivatalos blogjában beszámolt egy, a cég rendszereit ért szofisztikált támadásról. A bejegyzés szerint a FireEye cég kormányzati szereplők biztonsági tesztelésére is használt szoftvereit lopták el a támadók. A cég vizsgálatai kiderítették, hogy elsőként nem is az ő, hanem az egyik szoftverkomponensüket gyártó cég, a SolarWinds rendszereibe hatoltak be hónapokkal korábban, és ott kém-, valamint egyéb rosszindulatú programokat helyeztek el. A SolarWinds a FireEye-on kívül közel 18 ezer további vállalatnak és szervezetnek szállított szoftvereket. Az elemzések azt mutatták, hogy a SolarWinds érintett szoftvereibe azok gyári frissítésén keresztül hatolhattak be a támadók még 2020 áprilisában. A SolarWinds által gyártott szoftvereken keresztül bekövetkezett támadások érintették többek között az Egyesült Államok olyan szoftverfejlesztő és IT-szolgáltató vállalatait, mint például a Cisco, az Intel, az NVIDIA, a Deloitte, az SAP, a Check Point, illetve a szövetségi kormányzat szervezeteit, mint például a Védelmi Minisztérium, a Belbiztonsági Minisztérium, az Államkincstár, illetve a NASA. Az Egyesült Államokon kívül világszerte számos ország kormányzati rendszere szintén érintett volt a támadásban, amelynek egyik bizonyítható célja az adatlopás volt.[23] A fenti felsorolásból is látható, hogy a SolarWinds-támadás néven elhíresült akciósorozat érintette az infokommunikációs ágazat mellett a pénzügyi szektort, de a közigazgatást is mint kritikusinfrastruktúra-ágazatot. A SolarWinds-ügy világszerte hatalmas visszhangot váltott ki, hiszen nagyon jól rávilágított a beszállítói lánc – angol terminológiával élve: *supply chain* – biztonságának kérdéseire. A támadás hátterében szakértők Oroszországot sejtik.[24]

Egy másik eset, a Colonial Pipeline esete szintén nagyon jól mutatja a kibertérből érkező támadások fizikai térben kifejtett hatását, amely ráadásul egy olyan kritikus infrastruktúra esetében jelentkezett, amely a világ legerősebb

[22] Associated Press – Times of Israel: 'Cyber Winter Is Coming,' Warns Israel Cyber Chief After Attack on Water Systems. *Times of Israel,* 2020. május 8.

[23] Christina Zhao: SolarWinds, Probably Hacked by Russia, Serves White House, Pentagon, NASA. *Newsweek,* 2020. december 14.

[24] David E. Sanger: After Russian Cyberattack, Looking for Answers and Debating Retaliation. *The New York Times,* 2021. február 23.

országában okozott számottevő fennakadásokat és károkat. A Colonial Pipeline az Egyesült Államok egyik legnagyobb üzemanyag-szállító csőhálózata, amely az USA keleti partja mentén, Houstontól az észak-keleti New Jersey-ig fut, közel 9000 km hosszúságban. A keleti part napi üzemanyag-mennyiségének 45%-a ezen a hálózaton jut el az elosztókig, a benzinkutakig, illetve a felhasználókig. 2021 áprilisában nem hivatalos információk szerint egy orosz, de nem állami kötődésű kiberbűnözői csoport, a DarkSide megtámadta a csőhálózatot üzemeltető vállalat informatikai rendszereit, amelyekben *ransomware*-t helyezett el. A támadás sikerességét mutatja, hogy a vállalat kénytelen volt leállítani a teljes irányítórendszert, elkerülendő a zsaroló vírus további eszkalációját. Ugyanakkor ez azt okozta, hogy számos államban, így Észak-Karolinában, illetve Georgiában a benzinkutak nem jutottak üzemanyaghoz, azok kifogytak, súlyos ellátási problémát okozva ezzel az egyébként is nagyban a közúti közlekedési infrastruktúrára alapozott szállításban és közlekedésben. A cég döntése az volt, hogy kifizetik a támadók által bitcoinban kért „váltságdíjat", amelyért cserébe megkapták a zsaroló vírus által titkosított adatok feloldásához szükséges kódokat. Ugyanakkor ez még nem jelentette automatikusan a rendszerek működésének azonnali helyreállíthatóságát, hiszen az egy ilyen nagyságú és komplexitású infrastruktúra esetében több napot is igénybe vehet. A támadó csoport, azaz a DarkSide az eset után közleményt adott ki, amelyben leszögezte, hogy nem politikai, geopolitikai vagy egyéb céljai voltak a támadással, hanem egyszerűen csak pénzszerzés volt a motiváció. Ez nagyon jól rávilágít arra a tényre, hogy a kritikus infrastruktúrák támadásának következményei függetlenek a támadások mögött lévő motivációtól.[25]

Mindemellett nemcsak a kritikus infrastruktúra jól látható elemeit érheti támadás, hanem az olyan, a háttérben működő rendszereket, illetve azok egyes elemeit is, mint például az élelmiszeripar. Ennek egyik példája a Brazília legnagyobb húsfeldolgozó vállalatát ért – nem meglepő, szintén *ransomware*-támadás 2021 tavaszán. A JBS nemcsak Brazília, hanem a világ egyik legnagyobb húsfeldolgozó és húsellátó cége is egyben, amely több mint 15 országban végzi tevékenységét közel 150 ezer alkalmazottal. A vállalat rendszereit ért támadás következtében „a vállalat számítógépes rendszerei megbénultak, az Ausztráliában, Kanadában és az Egyesült Államokban működő üzemeik közül pedig több

[25] BBC News: Colonial Pipeline Boss Confirms $4.4M Ransom Payment. *BBC News,* 2021a. május 19.

leállt".[26] Ez komoly húsellátási problémákat okozott az említett országokban, illetve azok környezetében regionálisan.[27]

A fenti, kritikus infrastruktúrák és kritikus információs infrastruktúrák ellen elkövetett, a kibertéren keresztül megvalósított támadásokból levonható az a következtetés, hogy egy adott országra, illetve akár nagyobb földrajzi régióra is nagy nyomás gyakorolható. A támadások következményeikben és hatásaikban eltérőek, de azok már jóval túlmutatnak a kibertéren, hiszen sok esetben a fizikai térben megnyilvánuló hatásokkal járnak. Ez abszolút jelentős nyomást gyakorol az adott országra.

A nyomásgyakorlást módszereiben és eszközeiben két csoportra oszthatjuk: közvetlen és közvetett eszközökre. A közvetlen eszközök közé tartozhat például a kritikus rendszerek bénítása. Ebben az esetben az olyan rendszerek támadása vagy működésének befolyásolása a cél, amelyek számos más létfontosságú rendszerre hatnak. Ilyen az energiaszektor és annak rendszerei. Nyilvánvalóan a villamosenergia-rendszer fizikai átviteli hálózatai (például az áramvezetékek) és azok akár fizikai támadása okozhatja a legnagyobb károkat. Főleg úgy, hogy ezek a rendszerek nem védettek, sok esetben nem is lehetnek teljesen védettek a fizikai támadásokkal szemben. Ennek több oka van, de az okokat itt is alapvetően a kockázatokkal arányos védelemben kell keresni. Azaz ezek esetében – elsősorban azok földrajzi kiterjedtsége miatt – nem éri meg olyan szintű fizikai védelmet kiépíteni, amely ezen rendszerek egyes elemeinek esetleges fizikai rombolása ellen nyújtanának maximális védelmet.

A nyomásgyakorlás közvetett eszközei lehetnek például a közigazgatási rendszerek működésének akadályozására irányuló akciók. Ezek a támadások, illetve a működés akadályozása ebben az esetben is információgyűjtéssel kezdődik. Az információgyűjtés az adott közigazgatási rendszer technikai információi (például alkalmazott hálózati megoldások, szoftverek, hardverek, illetve ezek birtokában az azokban meglévő és kihasználható sérülékenységek) mellett a rendszereket üzemeltető személyekről, illetve az ezeket a szolgáltatásokat használó közigazgatási dolgozókról szóló információk összegyűjtésével, azok elemzésével és értékelésével kezdődik. Itt már látható módon összekapcsolódik az üzemeltetői és felhasználói állomány biztonságtudatos – akár magánéletében is megvalósított – internet- és infokommunikációseszköz-használata, vagy a másik véglet: a biztonságtudatosság hiánya. A célzott támadások (például a *spear*

[26] BBC News: JBS: Cyber-Attack Hits World's Largest Meat Supplier. *BBC News,* 2021b. június 2.
[27] BBC News (2021b): i. m.

phishing) túlnyomó többsége a közösségimédia-platformok használata során megadott, majd a támadók által összegyűjtött és akár éveken keresztül szisztematikusan elemzett és értékelt információk felhasználására épül. Ugyanakkor az így megszerzett információk a *social engineering* támadások első fázisában is kiválóan használhatóak, hiszen a megtévesztésre vagy akár a humán zsarolásra épülő támadás megindításához ezek az információk elengedhetetlenek. Az így megszerzett információk birtokában a közigazgatási rendszerek támadása már viszonylag egyszerűen kivitelezhető. Sok esetben ehhez még ezeknek a rendszereknek a nem átgondolt és nem megfelelően megvalósított, illetve fenntartott biztonsági állapota is hozzájárul hatásnövelőként. A közigazgatási rendszerek szisztematikus támadása a fentiekben is említett, az állammal szembeni bizalom megbontásán túl súlyos ellátási, szervezési és nem utolsósorban közbiztonsági következményekkel járhat.

Összefoglalás

A fentiekben bemutatott, a kritikus infrastruktúrák támadhatóságát felvázolni hivatott szcenáriók esetében a használt Digitális Pearl Harbor vagy Digitális Mohács kifejezés mint metafora valószínűleg nem jó, figyelmeztetnek szakértők.[28] Ugyanakkor ennek oka nem az, hogy a kritikus infrastruktúrák nincsenek veszélynek kitéve, és azokban nem következhet be mohácsi tragédia, hanem az, hogy bár a veszély nagyon is reális, de nagy valószínűséggel nem egy támadás, hanem a kritikus infrastruktúrák, illetve kritikus információs infrastruktúrák elleni támadások jól összehangolt sorozata fogja csak előidézni azt, amit ezeknek a metaforaként használt történelmi eseményeknek a révén be szeretnénk mutatni, illetve amire a figyelmet ezek fel szeretnék hívni.

A fentiek alapján nem kétséges, hogy a kritikus infrastruktúrák területén jelentkező veszélyek valósak. A kérdés inkább az, hogy a felvázolt komplex támadások hogyan épülnek fel, és mely infrastruktúrák vagy azok mely elemei ellen fognak irányulni. Egy másik óriási kérdés, hogy hogyan lehet megvédeni ezeket a rendszereket, hiszen sok esetben önmagukban a védelmet jelentő biztonsági rendszerek is kritikus infrastruktúrának minősülhetnek, tovább bonyolítva a kérdést.

[28] Sharon Weinberger: Cyber Pearl Harbor: Why Hasn't a Mega Attack Happened? *BBC,* 2013. augusztus 20.

Azt azonban ki kell jelenteni, hogy a kritikus infrastruktúrák és különösen a kritikus információs infrastruktúrák egymással való – sok esetben mármár átláthatatlan és gyakorlatilag feltérképezhetetlen – kapcsolata, valamint azok interdependenciája, azaz egymástól való függősége azt is jelenti, hogy egy adott ország kritikus infrastruktúráját vagy kritikus információs infrastruktúráját ért bármilyen támadás kihatással van egy vagy több másik kritikus infrastruktúra vagy kritikusinformációsinfrastruktúra-elem működésére. Ugyanakkor ezek a hatások a földrajzi határokon átívelő módon jelentkeznek. Mindezekre a legjobb a példa a fentiekben említett SolarWinds-ügy, ahol már a beszállítói lánc biztonsága is komolyan érintett, de ugyanilyen jó példa a Dyn DNS-szolgáltató esete az infrastruktúrákon belül meglévő alrendszerek kritikusságára.

Csak két példa, amely rávilágít arra, hogy a fejezet címéből eredő kérdésekre adott válaszok rendkívül komplexek. A kibertámadásokkal a kritikus infrastruktúrákban okozható károk dominóeffektust hoznak létre, amely jóval a kibertér határain kívül is jelentkezik. Ezek a támadások a fizikai térben is éreztetik hatásukat, felerősítve a – jelen fejezet címében szintén megfogalmazott kvázi hipotézist, azaz a – nyomásgyakorlást egy adott országra.

A kritikus infrastruktúrák védelme nem pusztán szabályozási és nem pusztán technikai kérdés. A védelemnek dinamikusnak kell lennie, amely a felkészüléstől a közel valós idejű incidenskezelésen át a kutatás-fejlesztésig kell hogy tartson.

Mindezeken túl a védelem megvalósítása össztársadalmi tevékenységet igényel. Ahogy az amerikai Kibervédelmi Parancsnokság korábbi vezetője megfogalmazta: „[…] teljes mértékben tisztában vagyok azzal, hogy a kiberbiztonság nemzetbiztonsági kérdés, és olyan összkormányzati megközelítést igényel, amely nemcsak a kormányt, a minisztériumokat, a különböző ügynökségeket, hanem a magánszektort és a nemzetközi partnereinket is összefogja."[29]

[29] Committee on Armed Services United States Senate: United States Cyber Command Washington, D.C., 2018. február 17.

Irodalomjegyzék

2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről

2016/1148. Az Európai Parlament és a Tanács (EU) irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről. Brüsszel, 2016.

2080/2008. (VI. 30.) Kormányhatározat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról

65/2013. (III. 8.) Korm. rendelet a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény végrehajtásáról

Associated Press – Times of Israel: 'Cyber Winter Is Coming,' Warns Israel Cyber Chief After Attack on Water Systems. *Times of Israel,* 2020. május 8. Online: www.timesofisrael.com/israeli-cyber-chief-attack-on-water-systems-a-changing-point-in-cyber-warfare/

BBC News: Colonial Pipeline Boss Confirms $4.4M Ransom Payment. *BBC News,* 2021a. május 19. Online: www.bbc.com/news/business-57178503

BBC News: JBS: Cyber-Attack Hits World's Largest Meat Supplier. *BBC News,* 2021b. június 2. Online: www.bbc.com/news/world-us-canada-57318965

COM(2005) 576. Az Európai Közösségek Bizottsága: Zöld könyv a létfontosságú infrastruktúrák védelmére vonatkozó európai programról. Brüsszel, 2005. november 17. COM(2005) 576 végleges.

Committee on Armed Services United States Senate: *United States Cyber Command.* Washington, D.C. 2018. február 17. Online: www.armed-services.senate.gov/imo/media/doc/18-17_02-27-18.pdf

European Commission: *European Programme for Critical Infrastructure Protection.* Brüsszel, 2006.

Goldman, O. Emily – Michael Warner: Why a Digital Pearl Harbor Makes Sense … and Is Possible. In George Perkovich – Ariel E. Levite (szerk.): *Understanding Cyber Conflict. 14 Analogies.* Washington (DC), Georgetown University Press, 2017. 147–157. Online: https://carnegieendowment.org/2017/10/16/why-digital-pearl-harbor-makes-sense-.-.-.-and-is-possible-pub-73405

JOIN(2020) 18 final. Közös közlemény az Európai Parlamentnek és a Tanácsnak Az EU kiberbiztonsági stratégiája a digitális évtizedre. Brüsszel, 2020. december 16.

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

Kovács László – Krasznay Csaba: Digitális Mohács. Egy kibertámadási forgatókönyv Magyarország ellen. *Nemzet és Biztonság,* 3. (2010), 1. 44–56. Online: www.nemzetesbiztonsag.hu/cikkek/kovacs_laszlo__krasznay_csaba-digitalis_mohacs_.pdf

Newman, Lily Hay: What We Know About Friday's Massive East Coast Internet Outage. *Wired.com,* 2016. október 21. Online: www.wired.com/2016/10/internet-outage-ddos-dns-dyn

Purchase, Erik – French Caldwell: Digital Pearl Harbor: A Case Study in Industry Vulnerability to Cyber Attack. In Sumit Ghosh – Manu Malek – Edward A. Stohr (szerk.): *Guarding Your Business: A Management Approach to Security.* Boston, Spinger, 2004. 47–64. Online: https://doi.org/10.1007/0-306-48638-5_4

Ribeiro, Anna: Protecting Critical Infrastructure Supply Chain Security From Cyber Attacks. *Industrial Cyber,* 2021. május 6. Online: https://industrialcyber.co/article/protecting-critical-infrastructure-supply-chain-security-from-cyber-attacks/

Sanger, E. David: After Russian Cyberattack, Looking for Answers and Debating Retaliation. *The New York Times,* 2021. február 23. Online: www.nytimes.com/2021/02/23/us/politics/solarwinds-hack-senate-intelligence-russia.html

Times of Israel: Cyber Attacks Again Hit Israel's Water System, Shutting Agricultural Pumps. *Times of Israel,* 2020. július 17. Online: www.timesofisrael.com/cyber-attacks-again-hit-israels-water-system-shutting-agricultural-pumps/

Trend Micro: Operation Pawn Storm: Fast Facts and the Latest Developments (2016. január 16.). Online: www.trendmicro.com/vinfo/us/security/news/cyber-attacks/operation-pawn-storm-fast-facts

Wakefield, Jane: One Fastly customer triggered internet meltdown. *BBC News,* 2021. június 9. Online: www.bbc.com/news/technology-57413224

Weinberger, Sharon: Cyber Pearl Harbor: Why Hasn't a Mega Attack Happened? *BBC,* 2013. augusztus 20. Online: www.bbc.com/future/article/20130820-cyber-pearl-harbor-a-real-fear

Zhao, Christina: SolarWinds, Probably Hacked by Russia, Serves White House, Pentagon, NASA. *Newsweek,* 2020. december 14. Online: www.newsweek.com/solar-winds-probably-hacked-russia-serves-white-house-pentagon-nasa-1554447

8. fejezet

Az ellátási láncok támadása, azaz mi történik, ha már a nyomtatott áramkör sem megbízható?

Koczka Ferenc

Bevezetés

Az 1994-ben még könyvkereskedelemmel foglalkozó webshopból a világ egyik legnagyobb vállalatává fejlődött amerikai vállalat, az Amazon 2015-ben már a videostreaming-piacon igyekezett stabilizálni a helyzetét. Olyan szoftverre volt ehhez szükség, amely lehetővé teszi nagy méretű videofile-ok tömörítését és gyors konverzióját úgy, hogy azok különböző platformokon is lejátszhatók legyenek. Akkoriban egy alig ismert startup, az Elemental Technologies (ET) már kifejlesztett erre egy kiváló referenciákkal rendelkező megoldást. A szoftvert nemcsak a Központi Hírszerző Ügynökség (CIA) alkalmazta, hanem kritikus alkalmazásokban, például a Nemzetközi Űrállomással való kapcsolattartásban is használták. Az Amazon számára kézenfekvő megoldás volt a startup felvásárlása, így a jól ismert recept szerint meg is kezdte a cég beolvasztását. A termékre nemcsak az Amazon Prime Video szolgáltatás továbbfejlesztését alapozták, ugyanez a technológia került be a CIA számára épített különleges biztonsági követelményeket támasztó felhőbe is. Ez – a korábbiakkal ellentétben – megkövetelte az alkalmazott elemek szigorú auditját; a részletes átvizsgálási folyamat során kiderült, hogy a startup Supermicro gyártmányú szervereinek alaplapjai egy, az eredeti dokumentációban nem szereplő, rendkívül kis méretű chipet is tartalmaznak.[1] Mivel a chipet ismeretlen helyen, valószínűsíthetően a gyártást követően építették be, az incidenst jelentették az amerikai hatóságoknak. Hamarosan világossá vált, hogy a népszerű szervergyártó így módosított kiszolgálói számos más kormányzati szervezet informatikai rendszerében is megtalálhatók,

[1] Bodnár Zsolt: Rizsszemnyi mikrochipekkel hajthatta végre Kína a legnagyobb USA elleni támadást. *Qubit.hu,* 2018. október 5.

https://doi.org/10.36250/01079_08

https://orcid.org/0000-0002-7541-6495

többek közt a Védelmi Minisztérium adatközpontjában és az Amerikai Haditengerészet hadihajóinak fedélzeti hálózatában is.

Az érintett szerverek nagy száma miatt az eset kivizsgálása évekig tartott. Amerikai elemzők megállapítása szerint a chip az operációs rendszer magját módosította úgy, hogy lehetővé tette annak későbbi megváltoztatását, hátsó ajtót nyitott[2] az érintett szerverekben, amely lehetővé tette a gépek azonosítását és további kódok lefuttatását. A chipeket kínai alvállalkozók gyáraiban ültethették be azokba az alaplapokba, amelyeket összeszerelésre szállítottak oda.[3] Mivel a Supermicro az egyik legnagyobb szervergyártó, gépei a világ számos hálózatában működnek, így világszerte lehetnek olyan gépek, amelyek ezzel a módosítással sérülékennyé váltak.

Különböző források eltérően nyilatkoztak az esetről, és több cég nem ismerte el az érintettségét. Ilyen reakció 2015-ben az informatikai incidensek 20%-ában fordult elő.[4] Ügyfelei és reputációja megőrzése érdekében ugyanis számos szervezet igyekszik megakadályozni, hogy incidensei napvilágra kerüljenek. Az Apple például annak ellenére, hogy állítása szerint nem talált érintett Supermicro gépet a hálózatában, közel 7000 ilyen gyártmányú szervert cserélt le. Híradások szerint legalább 30 amerikai nagyvállalat volt érintett az esetben, ugyanakkor a hatásokról alig áll rendelkezésre hiteles információ. Az érintettek teljes köre és az idegen áramkör beültetését végző cég is ismeretlen maradt, egyes források az utóbbi létezését is igyekeznek cáfolni.

Az eset egyike volt azoknak, amelyek új fejezetet nyitottak az incidensek történetében, mivel a támadás a korábbiaktól eltérően nem valamilyen szoftverhiba kihasználásán alapult. A kompromittált alaplapok felfedezésének valószínűsége eléggé csekély, hiszen csak egy olyan vizsgálat deríthetett fényt a chip jelenlétére, amelyet a legtöbb szervezet soha nem végez el. Az a lehetőség, hogy akár kritikus infrastruktúrák működtetésében szerepet játszó kiszolgálók adattartalma tartósan lehallgatható, azok adatai módosíthatók, működésük megváltoztatható,

[2] A hátsó ajtó *(backdoor)* elnevezésű (szoftver-) komponens ahhoz nyújt lehetőséget, hogy egy rendszerhez annak üzemeltetője által nem ismert és nem szándékozott hozzáférést biztosítson. A *backdoorok* telepítését a támadók a rendszer sikeres feltörése után végzik, ezzel biztosítják, hogy ahhoz az eredeti biztonsági hiba elhárítása után hozzáférjenek. Mivel erre rengeteg megoldás létezik, és az üzemeltetők nem feltétlenül ismerik ezeket, ezért egy rendszer kompromittálódása esetén a legtöbbször arra kényszerülnek, hogy tiszta forrásból teljes egészében újratelepítsék azt.

[3] Jordan Robertson – Michael Riley: The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies. *Bloomberg Businessweek,* 2018. október 4.

[4] Javvad Malik: *Ethics, Security and Getting the Job Done.* AlienVault, 2015. november.

adott esetben akár el is pusztítható, bármely kormányzat számára elfogadhatatlan kockázatot jelent. A Supermicro története egy olyan, kifejezetten nehezen felderíthető támadómódszer tömeges elterjedésének lehetőségére világított rá, amelytől a biztonsági szakemberek talán leginkább tartanak: a célzott APT-támadások[5] sikeres kivitelezésére kritikus információs infrastruktúrákban.

Visszatekintve a Supermicro-ügyre ma már elmondható, hogy az egyáltalán nem volt egyedi. Az olvasó számára minden bizonnyal ismert a Huawei esete, amikor az Egyesült Államok mellett többek közt Svédország, Nagy-Britannia és Lengyelország is megtiltotta, hogy stratégiai rendszereit a gyártó eszközeiből építsék fel. Bár ebben az ügyben sem került napvilágra egyértelmű bizonyíték, számos ország szűkítette az informatikai eszközeinek beszállítói körét, előnyben részesítve így a saját politikai vagy katonai közössége által megbízhatókat. Több EU-tagállam ezért leginkább az európai és amerikai gyártmányú termékkör alkalmazását részesíti előnyben.

Az informatikai rendszerek valódi támadóit annak ellenére rendkívül nehéz teljes bizonyossággal azonosítani, hogy a motivációelemzéstől a forenzikus vizsgálatokig számos módszer alkalmazható annak eldöntésére, hogy egy magányos támadó akciójával, egy csoport által kivitelezett kibertámadással vagy éppen katonai célú kiberművelettel, esetleg annak előkészítésével állunk szemben. Általános vélemény, hogy az említett támadásokat elsősorban nemzetállamok által finanszírozott csoportok képesek megvalósítani, és ezek célja elsősorban gazdasági, politikai vagy katonai előny megszerzése. A katonai műveletekben egyre nagyobb szerep jut a kibertérnek, mivel az információ megszerzése, az ellenség döntéseinek befolyásolása és erőforrásainak pusztítása ebben is eredményes lehet. Ennek következtében az elmúlt évtizedben felértékelődött az a képesség, amely a szemben álló fél informatikai rendszereinek lehallgatását, befolyásolását vagy működésének megzavarását a kibertérben teszi lehetővé.

A kritikus infrastruktúrák működőképessége valamennyi ország működőképességének fenntartásához elengedhetetlen. A magyar politikai vezetés számára már a 2010-es években is világossá vált a kibertér stratégiai szerepe. A kibertérbe helyezett funkciók bizalmasságának, rendelkezésre állásának és sértetlenségének fenntartása és fejlesztésének szükségessége a Magyarország

[5] APT: *Advanced Persistent Threat.* A támadás célja egy rendszer feltörése és a folyamatos, rejtett hozzáférés hosszú időn át történő fenntartása. Az APT-támadások célja rendszerint kormányzati, pénzügyi, gazdasági és katonai szervezetek rendszereiben tárolt adatok szivárogtatása.

Nemzeti Biztonsági Stratégiájáról szóló 1163/2020. (IV. 21.) Korm. határozat szövegében is megjelenik:

> „31. Hibrid támadással szembeni ellenálló képességünket növeli a nemzet egysége, demokráciánk szilárdsága, a közös nyelv, a felgyorsított döntéshozatali képesség, valamint a honvédelmi és rendvédelmi erők szoros együttműködése egymással és a releváns polgári infrastruktúrával. Az új biztonsági kihívások miatt azonban folyamatosan szükséges fejleszteni az információs és kiberhadviselés elleni védekezés rendszerét."

> „32. Magyarország Kormánya mindent megtesz hazánk kiberbiztonsága érdekében, kapacitásainkat e területen is folyamatosan fejlesztjük. Tekintettel arra, hogy a kormányzati és más kulcsfontosságú infokommunikációs rendszerek elleni támadások száma növekszik és kifinomultságuk erősödik, folyamatos erőfeszítés szükséges az infokommunikációs rendszerek védelmének erősítése érdekében. Általános jelenség továbbá a felhasználók információbiztonsági tudatosságának alacsony szintje, holott a felhasználók megfelelő információbiztonsági tudatossága a kiberincidensek megelőzésének egyik kulcseleme."

Nem ismert a Supermicro-gépekre alapozott támadás kivitelezőinek indítéka. Lehetséges, hogy az informatikai rendszereken nyitott hátsó ajtók tömegét csak alkalomszerűen megvalósított támadásokra akarták felhasználni. Elképzelhető, hogy a terv további elemei csak a szerverek üzembe állítása után alakultak ki. Ha feltételezzük, hogy ismert lehetett számukra a gyártó vásárlói köre, esetleg be tudtak avatkozni a szállítási folyamatokba, akkor elképzelhető, hogy egy célzott támadást ilyen „messziről" indítottak. Tekintettel a valószínűsíthető megbízói körre azonban számolni kell a kritikus infrastruktúrák működését biztosító szűkebb terület, az *ellátási lánc* támadásával, vagy akár az ellátási láncon keresztül megvalósított további műveletek előkészítésével.

Az ellátási lánc

Az ellátási lánc *(supply chain)* meghatározására több különböző forrást is találhatunk. A hazai szakirodalom egyik elfogadott meghatározása szerint az „ellátási láncok […] egy adott fogyasztói igény kielégítésére szerveződő, egymással lineáris és vertikális kapcsolatban lévő vállalatokból állnak".[6] Az egyes szakterületek specifikus meghatározásokat adnak, és esetükben hiba lenne a hagyományos értelemben vett termékekre és szolgáltatásokra szorítkozni. A NIST-

[6] Chikán Attila: *Vállalatgazdaságtan*. Budapest, Aula, 2004.

800-161 az információs és kommunikációs technológiák (ICT)[7] ellátási láncát a beszerzők, integrátorok és beszállítók közötti erőforrások, folyamatok összekapcsolt halmazaként definiálja, amely az ICT-termékek és -szolgáltatások tervezésétől a fejlesztésén, beszerzésén, gyártásán át a végfelhasználóhoz jutásáig tart.[8] Az Amerikai Védelmi Minisztérium az ellátási lánc három meghatározását is alkalmazza, amelyek elsősorban a fegyverrendszerekhez kapcsolódnak. Ezek: a mikroelektronikai berendezések beszerzésére szolgáló globális lánc, a beszerzési ellátási lánc, valamint a fenntartási ellátási lánc.[9] Ezeket a termékek előállításában, kezelésében, elosztásában és feldolgozásában részt vevő szervezetek és folyamatok rendszereként definiálják, amelynek célja a termékek, az információ, a tudás és a financiális források biztosítása az előállító és a fogyasztó között.

A meghatározások értelmében az *ellátási lánc támadása* olyan művelet, amelynek célja az ellátási lánc működési folyamataiba történő beavatkozás azért, hogy a támadó elérje a szándékának megfelelő hatást.

Nemzetbiztonsági szempontból az ellátási lánc szerepe leginkább a gazdasági, közmű-, ipari, pénzügyi, kormányzati és közigazgatási, távközlési, média-, valamint a katonai szervezetek folyamataiban kiemelkedő, de szinte bármilyen szervezet működésében alapvető. Mind alkalmaz eszközöket, igénybe vesz szolgáltatásokat, amelyek nélkül nem lenne képes teljeskörűen ellátni feladatát. A működéshez szükséges összetevőket szintén az ellátási lánc elemeinek tekintjük, amelyek kiesése nemcsak az adott szervezetben okoz zavart, hanem a ráépülő továbbiak működésében is.

Az ellátási láncra történő első szakirodalmi utalások a rendszerelmélet kialakulásával az 1940-es évekre tehetők. Addig a gyártók határozták meg a termelés körülményeit, és jórészt a kereskedelmet is. A fogyasztó felértékelődése a 70-es évek Amerikájában kezdődött meg, kialakult a termékek összehasonlíthatósága és az árverseny. A kereskedők szerepe kulcsfontosságúvá vált, csökkentek a haszonkulcsok, kiemelt szerepet kaptak a vevői elégedettséget növelő szolgáltatások, mint például a gyorsaság, a garancia vagy éppen a termék visszaválthatósága. Kialakult a gyártók és a kereskedők kölcsönös függősége, a korábbi,

[7] Az ICT ebben az értelmezésében magában foglalja az információ összegyűjtésére, tárolására, továbbítására, lekérdezésére és feldolgozására használt valamennyi technológia minden kategóriáját (például mikroelektronika, nyomtatott áramkörök, szoftverek, informatikai rendszerek, feldolgozók, kommunikációs hálózatok).

[8] NIST Computer Security Center: Definitions.

[9] DoD Defense Science Board: DSB Task Force Report on Cyber Supply Chain, 2017.

push rendszerű elosztórendszereket a *pull* váltotta fel, azaz csak azok a termékek kerültek a kereskedelembe, amelyekre létezett vásárlói igény.

Az elmúlt évtizedekben az informatikai fejlődés a gazdasági rendszerek szervezésében is jelentős változásokat hozott.[10] A nagy gyártók és beszállítók az igények gyors kielégítése érdekében eleinte óriási, csak költségesen fenntartható raktárkészletekkel dolgoztak. Ezeket tette szükségtelenné a gyors kommunikációs csatornákra alapozott új logisztikai módszer, a gyártók számára jelentős költségmegtakarítást eredményező *just in time* (JIT). A JIT a raktározási feladatok csökkentését célozta úgy, hogy a beszállítók a szükséges elemeket csak a felhasználáshoz közeli időpontban szállították. A JIT azonban kényes kockázati elem, akár egyetlen komponens, szélső esetben még egy csavar késedelmes beszállítása is a teljes termelési folyamat elakadását okozhatja. Bár a gyártók igyekeznek szerződésekkel védeni magukat, számos olyan helyzet alakulhat ki, amely ily módon nem kezelhető. A helyzetet tovább rontja, hogy a beszállítók működése szinte minden esetben további beszállítóra alapozott. A nagy gyártók igyekeznek minimalizálni ilyen irányú kitettségüket, ezért a minőségbiztosítás érdekében beszállítóiktól is megkövetelik működésük szabályzását, folyamataik dokumentálását és termékeik azonosíthatóságát, nyomon követhetőségét.[11]

A JIT gyengesége a váratlan katasztrófák, előre nem látható akadályok esetén mutatkozik meg igazán. A kockázatkezelés kialakítása során annak módszertana következtében kevéssé veszik figyelembe a ritkán bekövetkező, ugyanakkor nagy hatású eseményeket. Tűzesetek, hóviharok, földrengés, sztrájk és különféle terrorcselekmények ezért hirtelen nagy hatással lehetnek egy ország kulcsfontosságú területeire. A 9/11-es terrortámadásokat követően, amelyek egyik fő célpontja a New-York-i Világkereskedelmi Központ volt, súlyos zavarok keletkeztek az ellátási láncban.[12] Szinte azonnal leállt a teljes légi közlekedés, korlátozták a határok forgalmát, de a belföldi áruszállításban

[10] Sarah Hippold: 5 Trends From the Gartner Hype Cycle for Supply Chain Strategy. *Gartner,* 2020. október 2.

[11] A gyártók számos különböző szabvány szerinti minősítést követelhetnek meg. Magyarországon jellemzően az ISO 9001 szabványcsalád az elvárt követelmény, de egyes iparágak további elvárásokat is támaszthatnak, például az autóiparban a QS-9000 tartalmazza az ágazatspecifikus többletkövetelményeket.

[12] Bányász Péter: Az ellátási lánc kiberfenyegetettsége, különös tekintettel a közlekedési alrendszer biztonságára, a szervezett bűnözés hatásai. In Kállai Attila et al.: *Humánvédelem – békeműveleti és veszélyhelyzet-kezelési eljárások fejlesztése. Tanulmánygyűjtemény.* Budapest, Nemzeti Közszolgálati Egyetem, 2016.

is nagy veszteségek forrása volt az a körülmény, hogy a hatóságok a gyanús kereskedelmi konténerek tartalmát is átvizsgálták. 2021-ben az Ever Given konténerszállító hajó egy manőverezési hiba következtében elzárta a Szuezi-csatornát, és így a világkereskedelem 12%-át bonyolító útvonalat tett hetekre használhatatlanná, amivel nemcsak a beszállítási folyamatokat akasztotta meg, hanem világgazdasági szinten érzékelhető zavart okozott. A Covid–19 hatása az ellátási láncban közismert; több autógyár is felfüggesztette gyártási folyamatait az ellátási láncban keletkezett zavarok következtében. Az ilyen típusú eseményekre nehéz költségarányosan felkészülni úgy, hogy minden negatív következmény kizárható legyen, így inkább a kialakult helyzet megfelelő kezelésére érdemes erőforrásokat biztosítani.

A fejlődés nem állt meg a JIT szintjén, az Ipar 4.0 – amelyet negyedik ipari forradalomként is szokás említeni – alapkoncepciója a gyártók és beszállítóik rendszereinek, akár magát a (rész)termékek előállítását végző gépeknek az adatszintű összekapcsolása. Ellentétben a JIT logisztikájával, amely alapvetően emberek munkájára épül, az Ipar 4.0 esetében a gépek közti kommunikációra kerül a hangsúly. E koncepció Achilles-sarka az időzítés, amely még inkább magában hordozza a könnyű célponttá válás lehetőségét egy ellenséges támadás megtervezése vagy kivitelezése során.

A pénzügyi rendszerek működése szintén az ellátási láncra épül. A kereskedelem ma már nem működhetne a banki rendszerek támogatása nélkül,[13] és azok sérülése a gazdasági rendszer működésére nézve is katasztrofális következményekkel járna. A fejlett gazdasági rendszerrel rendelkező társadalmak visszaszorították a készpénzforgalmat, aminek következtében a banki rendszerek üzemzavara esetén nemcsak a gazdasági szféra működése bénulna meg, hanem a lakosság is csak korlátozottan lenne képes akár egyszerű vásárlásokat is lebonyolítani. A pénzügyi rendszer kitettsége már 2007-ben, az Észtország ellen irányuló kiberműveletben[14] is nyilvánvalóvá vált. A szektor kiemelt szerepét mutatja, hogy a készpénzellátás, a bank- és hitelintézeti biztonság és a pénzügyi eszközök kereskedelmi, fizetési, klíring- és elszámolási infrastruktúrái és rendszerei a nemzeti létfontosságú rendszerelemek pénzügyi ágazatának kiemelt elemei. A pénzügyi rendszer zavaraiból származó károk mértéke mérhető volt azokban az országokban, ahol politikai okokból az internet lekapcsolása mellett

[13] Juhász Péter – Száz János – Misik Sándor: Ellátási láncok versenyképessége és finanszírozása – gondolatok az optimumról. *Közgazdasági Szemle,* 64. (2019), 1. 53–71.

[14] Andreas Schmidt: The Estonian Cyberattacks. *Researchgate.net,* 2013. január.

döntöttek. Esetükben 2015-ben az ebből eredő veszteség elérte a 2,4 milliárd dollárt.[15] Ez világossá teszi a pénzügyi rendszerek kiemelt védelmét: egy sikeresen végrehajtott kiberművelet az érintett ország teljes gazdaságán végiggyűrűzne, és amellett, hogy óriási károkat okozna, annak reputációját is jelentősen meggyengítené.[16]

A kormányzatok alapvető érdeke az ellátási láncok működőképességének fenntartása, ezért legfontosabb elemeit kritikus infrastruktúraként azonosítják, így rájuk szabott jogszabályok határozzák meg a működésüket. Ezen túl további szervezetek foglalkoznak a működés szervezésével. 1996-ban több iparág összefogásával alakult meg a Supply Chain Council (SCC), amely kidolgozta az ellátásilánc-menedzsment ipari szabványának tekintett Supply Chain Operations Reference Modelt (SCOR). A téma fontosságát jól szemlélteti, hogy a NIST az amerikai szövetségi ügynökségek számára külön készített kockázatkezelési gyakorlati információkat tartalmazó ajánlást.[17]

Az ellátási lánc támadása tehát kézenfekvő lehetőség egy ország vagy szervezet funkcióinak megzavarásához. Ez nem feltétlenül kötődik a kibertérhez, számos olyan incidens ismert, ahol egyáltalán nem kaptak szerepet elektronikai eszközök. A 2010-es évek gondolatkísérlete, a Digitális Mohács[18] több olyan elképzelt lehetőséget ír le, amely kisebb-nagyobb előkészületet igénylő szabotázsakcióval zavarokat idézhet elő a kritikus infrastruktúrákban, miközben azok egy része egyáltalán nem igényel informatikai tudást. Mivel könyvünk elsősorban a kibertérrel kapcsolatos problémákra koncentrál, a kérdést elsősorban ebből a szemszögből vizsgáljuk.

[15] Darrell M. West: *Internet Shutdowns Cost Countries $2.4 Billion Last Year*. Center for Technology Innovations at Brookings, 2016.

[16] Steven S. DeBusk: *What Happens When the Supply Chain Breaks? Implications for the Army Supply Chain Under Attack*. Fort Leavenworth, School of Advanced Military Studies United States Army Command and General Staff College (First Term AY 02-03), 2003.

[17] Jon Boyens et al.: *Supply Chain Risk Management Practices for Federal Information Systems and Organizations.* National Institute of Standards and Technology, 2015.

[18] Kovács László – Krasznay Csaba: Digitális Mohács. Egy kibertámadási forgatókönyv Magyarország ellen. *Nemzet és Biztonság,* 3. (2010), 1. 44–56.

Az ellátási láncok támadásainak elemzése

Az ellátási láncokra irányuló incidensek elemzéséhez érdemes megvizsgálni az azok ellen indított eddigi támadásokat, és a konkrét esetek alapján levonni azokat a következtetéseket, amelyek betartásával a működésük biztosítható. Felkutatásuk nem egyszerű, mivel szinte mindegyikük tartalmaz nem publikálható elemeket. Megállapításainkat ezért csak közvetetten, az Amerikai Védelmi Minisztérium (DoD) által elkészített keretrendszer és az abban közzétett 41 konkrét eset katalógusa alapján tesszük meg.[19]

Célok

A MITRE 2017-es *technical reportja*[20] az ellátási lánc támadását *(supply chain attack)* a következőképp határozza meg: szándékos rosszindulatú cselekmény, amelynek célja az információs és kommunikációs technológia *(hardver, szoftver, firmware)* sebezhetőségének létrehozása és végső soron kihasználása az ellátási lánc bármely pontján azzal az elsődleges céllal, hogy megfigyeljen vagy megzavarjon egy műveletet a kibertér erőforrásainak felhasználásával.

A támadó elsődleges szándéka tehát az ellátási lánc működésének megzavarására, a rendszerben tárolt információ megszerzésére, módosítására vagy elpusztítására irányulhat, de általánosságban a CIA-elvek megsértése is lehet cél. Ugyanakkor egy sikeres támadás megnyitja a lehetőségét, hogy egy támadó annak működését a későbbiekben is a saját érdekeinek megfelelően befolyásolja. Ebben az esetben az ellátási lánc támadása valószínűsíthetően egy magasabb taktikai cél eléréséhez szükséges eszköz.

Az ellátási lánc kifinomult támadása az elmúlt évtizedben volt jellemző. A 2010-es évekig még alig fordult elő, hogy az ellátási lánc támadása egy ország gazdaságában jelentősebb problémát okozott volna. Két eset igazán közismert; a 2007-es észt–orosz konfliktus során Észtország gazdasági működése néhány napra gyakorlatilag megbénult. A különlegesen kifinomult Stuxnet pedig 2010-ben akadályozta meg az atomfegyver kifejlesztését, évekkel kitolva

[19] Melinda Reed – John F. Miller – Paul Popick: *Supply Chain Attack Patterns: Framework and Catalog.* Office of the Assistant Secretary of Defense for Research and Engineering, 2014.

[20] William J. Heinbockel – Ellen R. Laderman – Gloria J. Serrao: *Supply Chain Attacks and Resiliency Mitigations, Guidance for System Security Engineers.* MITRE, 2017. október.

az iráni atomprogram végrehajtását.[21] A kibertámadások száma és természete azóta jelentős változáson ment keresztül. Bár a magyar kibervédelmi szakemberek többsége egyetért abban, hogy Magyarország fenyegetettsége ma nem számottevő, ez inkább a célzott támadásokra vonatkozik. Nincsenek közismert célzott, magyar létfontosságú rendszerekre irányuló kibertámadások. A nem célzott támadások tekintetében a magyar informatikai rendszerek fenyegetettsége már nem ilyen alacsony, mivel az egyes rendszerek sérülékenységeit kihasználó automaták, amelyek a megtámadott eszközöket a hálózati címek szkennelésével végzik, a megtévesztő levelek mellékleteiként terjedő kriptovírusok által okozott károk a magyar kibertérre ugyanúgy kiterjednek, mint más országokéra. A véletlenre bízott támadások által okozott kár a legtöbb esetben lényegesen kisebb, mint a célzott támadásoké, de az ellenkezőjére is voltak már példák.

Támadási típusok

Az ellátási lánc támadásának operatív célja a konkrét esetek katalógusának elemzése alapján három területre irányul, és mindhárom esetében elérhető a bizalmasság, a sértetlenség és a rendelkezésre állás sérülése.

Egy rosszindulatú hardverelem elhelyezésére részben jó példa a Supermicro esete. Ilyen incidens nem csak a rendszer kialakításának fázisában fordulhat elő, a teljes életciklus alatt további belépési pontok vannak egy meglevő hardverelem kicserélésére vagy módosítására. A hardverelemek manipulálásával végzett támadás a prototípus kialakításától a sorozatgyártáson és a karbantartási folyamatokon keresztül bármikor, szélső esetben akár a rendszer kivezetése után is kivitelezhető. A hardverelemek nemcsak funkcionalitásban, hanem rendelkezésre állásban is jelenthetnek kockázatot. Az Amerikai Légierő már 2012-ben szembesült azzal, hogy a jellemzően külföldről származó, katonai minősítésű elektronikai részegységek nem képesek teljesíteni a velük szemben támasztott követelményeket, egyes esetekben pedig akár újnak látszó, de valójában csak felújított elemek kerülnek a beszállítói láncba. A kezdeti teszteken még jól teljesítő elemek élettartama sokkal rövidebb az elvártnál, ami a légierő gépei esetében katasztrofális következménnyel járhat.[22]

[21] Cserháti András: A Stuxnet vírus és az iráni atomprogram. *Nukleon,* 4. (2011), 1. 1–7.

[22] Flying Fraudulently – How a Weak Supply Chain Became the Usaf's Worst Enemy. *Airforce Technology,* 2012. szeptember 24.

A szoftverelemek cseréje egy információs rendszerrel szemben végrehajtott kiberműveletben kézenfekvő eszköznek tűnik. Sikeres támadás során a számítógépen tárolt szoftverkomponensek módosítása már egyszerű feladat lehet a támadó számára. De nem csak a hagyományos szoftverelemek lehetnek érintettek, a Supermicro esetében a hardverelemekhez közvetlenül kapcsolódó *firmware* is kulcsszerepet játszott a támadó céljának elérésében. A Stuxnet esetében a kritikus elemekben (PLC-kben) is kicserélt/módosított szoftver működött, ez okozta a dúsítók közel 20%-ának megsemmisülését.

Annak ellenére, hogy a szoftverelemek cseréje könnyebben kivitelezhetőnek tűnik, a 41 publikált esetben azonos számban fordult elő szoftverfejlesztők és hardverfejlesztők ellen irányult támadás.

Szintén jellemző támadási típus egy rendszerrel kapcsolatos *adat jogtalan felhasználása* vagy *rosszindulatú módosítása*. Ebbe a típusba nem csak olyan esetek tartoznak, amelyek közvetlenül a kifejlesztett rendszerre vonatkoznak, mert a rendszer megtervezésében és kifejlesztésében részt vevő teljes környezet is támadható. Amennyiben egy kifejlesztendő rendszer kezdeti fázisában felállított követelményrendszert egy támadó képes módosítani, annak funkciói a saját érdekei mentén működhetnek majd a kifejlesztett rendszerben. Ugyanez történhet egy rendszer biztonsági elemzésével, *hardeningdokumentációjával* kapcsolatban is. Módosíthatók lehetnek a rendszer fejlesztői és felhasználói dokumentációi.

Nem túl gyakori, de korántsem példa nélküli lehetőség a fejlesztőeszközök módosítása. Efféle támadás esetén a támadó a fejlesztők által alkalmazott szoftverkörnyezetet módosítja azért, hogy például egy manipulált fordítóprogram a lefordított programkódokban a programozó tudta nélkül káros kódot helyezhessen el. Egy ilyen típusú támadás 2015-ben vált ismertté, amikor az Apple XCode nevű fejlesztőeszközét módosították, majd Kínában az Apple forrásain kívül terjeszteni kezdték. Az ezzel készült alkalmazások egy XCodeGhost nevű kártékony kódot tartalmaztak, átmentek az Apple ellenőrzési eljárásán, és bejutottak az App Store-ba is, így végül hozzávetőleg 500 millió felhasználó vált érintetté.[23]

Támadási pontok

A fenti támadási típusok azonban nemcsak az ellátási láncok közvetlen környezetében, hanem azon kívül is alkalmazhatók, így a védekezés során érdemes

[23] Lin Yang – Quan Yu: *Dynamically Enabled Cyber Defense.* H. n., World Scientific, 2021. 26–28.

azonosítani a lehetséges támadási pontokat is. A MITRE tanulmányában dokumentált 41 eset 81 támadási pontot azonosít, és bemutatja, hogy ezek nem csak egyetlen pontra irányulnak.

Egy rendszer támadása akkor a leghatékonyabb, ha az életciklusának minél korábbi pontján történik meg. Egy *elemzési fázisban* levő rendszer megismerése információt nyújt az azzal szemben támasztott funkcionális követelményrendszerről, a rendszer céljai mellett az azon kívül eső területeket is definiálja. Már ez a fázis is információt nyújthat a műszaki környezetről. Az elmúlt évben a távmunka térnyerésével sok szervezet alakított ki távoli hozzáférést, a rövid határidők miatt nem mindig szem előtt tartva az információbiztonsági követelményeket. Ez a tény is közrejátszhat a jogosulatlan hozzáférések kockázatának megemelkedésében. Ebben a fázisban 3, *a kockázatok elemzésének és csökkentésének fázisában* már 12 támadás volt érintett.

A mérnöki tervezés és gyártmányfejlesztés a leginkább veszélyeztetett fázis, ebben regisztrálták a legtöbb incidenst, a MITRE kutatásában 28-at. Ebben a szakaszban a támadó célja, hogy kifejlessze és konfigurálja a támadó eszközeit, bejuttassa, és aktiválja azokat a célkörnyezetben. A célpontok közt nemcsak a fő-, hanem az alvállalkozói rendszerek is szerepelnek, a kifinomultabb módszerek a szoftver- és hardverfejlesztőkre irányulnak akár úgy, hogy a köztük folyó információáramlásba ékelődnek be.

A gyártás és telepítés során végzett támadás pontos technikai információkat szolgáltat a támadó számára a már működő rendszerről, erre alapozva további támadóeszközök fejleszthetők ki, és juttathatók tovább. Egy tesztfázisban levő rendszer védelmére sok esetben még kevesebb energiát fordítanak, ami nagyban megkönnyítheti a támadó kódok elrejtését. Ez a fázis 24 támadásban volt érintett.

A működés és támogatás szakaszában működő rendszerek már védett környezetben, a *hardeningeljárásokat* már elvégezve működnek, így azok eredményes kompromittálása már nehezebb feladat. Annak ellenére, hogy ez a fázis az életciklus várhatóan leghosszabb szakasza, a katalógusban csak 22 esetben fordult elő. A SolarWinds rendszerében ezt a szakaszt támadták úgy, hogy a támadó kódot szoftverfrissítéssel juttatták be különböző rendszerekbe. Az akció az ellátási láncon keresztül történő támadás tiszta esete volt, ami világossá teszi a beszállítói informatikai rendszerek kockázatának hatását a rájuk épülő rendszerekre.

A támadók

A kibertámadások megbízóinak, illetve kivitelezőinek rendszerezésére számos forrás tett kísérletet. Ezek az aktorok eltérő motivációkkal és eltérő eszközrendszerrel rendelkeznek, profiljaik ismeretében meghatározhatók motivációik, az általuk alkalmazott technológiák, és kidolgozhatók a megelőzési és védelmi módszerek. A támadók kategóriákba sorolására számos forrást találhatunk,[24] a Hackmageddon[25] adatai alapján korreláció fedezhető fel a támadó csoportba tartozása és a támadás célja közt.

A motivációk azonosításával szintén több forrás foglalkozik, az azonosítás alapjai az ismertté vált incidensek elemzése és az azokból alkotott statisztikák lehetnek. Az informatikai incidensek bejelentési kötelezettsége az Amerikai Egyesült Államokban 2004-re nyúlik vissza, ma már ezek bárki számára elérhetők és tanulmányozhatók. A Hackmageddon havi rendszerességgel készít statisztikákat. Az elmúlt évek motivációit és azok változását mutatja be az 1. táblázat, amelyben a kiberkémkedés és a kiberhadviselés arányának csökkenése mellett a kiberbűnözés egyre magasabb arányban jelenik meg. Az ilyen típusú statisztikák adatai és a tényleges állapot közt valószínűsíthetők eltérések, aminek leggyakoribb oka az esetek egy részének felderítetlensége és a nyilvánosság tájékoztatásának ellenérdekeltsége.

1. táblázat: A kiberbűnözés motivációinak változásai, 2018–2020

Év	Kiberbűnözés	Kiberkémkedés	Hacktivizmus	Kiberhadviselés	Ismeretlen
2018	81,82%	12,86%	2,84%	2,47%	n. a.
2019	83,96%	11,21%	3,05%	1,55%	0,17%
2020	85,17%	9,94%	2,34%	1,83%	0,64%

Forrás: www.hackmageddon.com

Az ellátási láncok támadására itt csak közvetett statisztikák állnak rendelkezésre. A tendenciát azonban jól érzékelteti az Identity Theft Resource Center (ITRC) 2021. első negyedéves adata, amelyben 137 szervezet 27 különböző

[24] Lásd például Kovács László: *A kibertér védelme*. Budapest, Dialóg Campus, 2018. 171.; az Intel pedig publikálta a kiberbűnözés motivációinak személyközpontú referenciatáblázatát, lásd Tim[othy] Casey: Understanding Cyberthreat Motivations to Improve Defense. *Intel White Paper,* 2015. február 16. 8. (Függelék.)

[25] Lásd: www.hackmageddon.com.

beszállítójával kapcsolatban jelzett a kibertérből származó támadást – ez az előző időszak esetszámánál 42%-kal magasabb volt. Bár a MITRE 2017-es jelentésében a kifinomult eljárásokat alkalmazó támadásokat nemzetállamoknak tulajdonítja,[26] felmerül a kérdés, hogy mely szereplők milyen célok érdekében hajtanak végre kifejezetten az ellátási láncokra irányuló támadásokat.

Katonai célú kiberműveletek

A katonai szervezetek és stratégiák a történelem során folyamatos változáson mentek keresztül, hajtómotorjukat a technikai és logikai fejlődés jelentette. A kezdetleges fegyverektől a modern légierőig számos példa igazolta, hogy a modern technikai eszközök nélkülözhetetlenek a katonai műveletek támogatásában, ugyanakkor a harcászati műveletek eredményessége nem csak ettől függ. A saját ellátási lánc fenntartása és az ellenség ellátási láncainak támadása kiemelt szereppel bír a modern hadviselésben, bár maga a módszer egyáltalán nem új. A modern hadviselés viszont már nem jár minden esetben együtt a konfliktus nyílt vállalásával, a jelen háborúi már nem feltétlenül a harcmezőn dőlnek el. Az elmúlt évtizedekben nagyobb szerepet kapott az elrettentés, az USA 2003-ban az iraki háborúban demonstrálta információs fölényének elsöprő hatását. A fejlett országok által vívott hagyományos háborúkat felváltotta a hibrid háború, amely már nem csak katonai szereplők közt zajlik, abban a civil szféra és helyettesítő szervezetek is részt vesznek. Az ellátási lánc támadása reális cél, mert annak fenyegetettsége már önmagában elég lehet ahhoz, hogy a hatalom aktuális gyakorlójával szembeni bizalmat megingassa, és elérje a civil lakosság szembefordulását a hatalommal.[27]

Az ellátási lánc támadásának a hírszerzésben betöltött szerepét aligha kell részletesen bemutatni, az ellenség ellátási folyamatairól, annak tartalmáról, az alkalmazott eszközökről, az utánpótlás útvonaláról, idejéről és tartalmáról szerzett információk képet adhatnak az ellenséges haderők mozgásáról, és kikövetkeztethetők a lehetséges jövőbeni lépések. Ezek ismerete lerövidíti a katonai vezetés döntési ciklusát, és hathatós támogatást nyújt az információs fölény elérésében és megtartásában.

[26] Heinbockel–Laderman–Serrao (2017): i. m. 1–5.

[27] Bodoróczki János: A modern hadviselés logisztikája – a katonai logisztika jövője. *Hadtudomány,* 30. (2020), 2. 98–108.

Az utánpótlási logisztika információinak megszerzése mellett annak lehetőség szerinti befolyásolása, valamint az ellátási lánc működésének meghiúsítása a fejlettebb technikával rendelkező haderőket is vesztes helyzetbe hozhatja. A befolyásolás célja általában a megtévesztés, és ezt kihasználva olyan helyzet kialakítása, amelyben adott szereplő akaratát a szemben álló félre kényszerítheti. Az ellátási lánc támadása, pusztítása már a hadviselés történetének korai szakaszában is fontos stratégiai elem volt, a hadianyag- és az élelmiszer-utánpótlás elvágása számtalanszor bizonyult ütőképes lépésnek. Az ellátási lánc zavaraira a modern logisztika is érzékeny. A modern, hálózati kommunikációra alapozott rendszerek esetében ezek a zavarok a hagyományos támadóeszközök igénybevétele nélkül is előállíthatók.

A hadviselésben a számítógép-hálózatokra alapozott információs műveleti tevékenységek alkalmazása először 1998-ban, az Egyesült Államokban jelent meg, ekkor adták ki JP 3-13 jelzéssel az első összhaderőnemi információs műveleti doktrínát.[28] Az anyag az információs műveleteket támadó és védelmi kategóriákba sorolja, a hangsúlyt a saját információk és információs rendszerek megvédésére helyezi úgy, hogy közben a szemben álló fél információinak megszerzésére és a rendszereinek támadására törekszik. A doktrína megjelenését követően további országok is felismerték a kibertér jelentőségét a műveleti tevékenységekben, így hamarosan Kína és Oroszország is megkezdte ez irányú képességeinek kifejlesztését.[29]

Háború, lövések nélkül

A Supermicro esetéhez hasonló támadás kivitelezésére magányos támadóknak, terroristáknak vagy hackercsoportoknak jelen tudásunk szerint nem volt még lehetőségük. A negyedik generációs hadviselésben ugyan szinte bármely csoport képes lehet érdekeinek érvényesítésére, akár még nemzetállamokkal szemben is úgy, hogy támadásai célpontjául kritikus infrastruktúrákat jelöl ki,[30] erre jelenleg kevés példa van. Ha meg is tudnának egy alaplapra ültethető chipet tervezni, annak gyártása már nehezen lenne titokban tartható, nem beszélve

[28] Joint Publication 3-13, Information Operations. 2012.

[29] Haig Zsolt: *Információs műveletek a kibertérben*. Budapest, Dialóg Campus, 2018. 170.

[30] Deák Veronika (szerk.).: *Célzott kibertámadások. Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára.* Budapest, Nemzeti Közszolgálati Egyetem, 2018. 161.

az alaplapok gyártási folyamatába való beavatkozásról vagy a minőségellenőrzés kijátszásáról. Egy ilyen feladat megvalósítására csak olyan szervezet képes, amelynek kapcsolatai minden részterületen érvényesülni tudnak, és ez leginkább az államhatalom esetében áll fenn. De mi motiválja a kibertámadások kivitelezésére alkalmas Supermicro-szerű incidensek kitervelőit ilyen költséges és nagy szervezési feladatot igénylő módszer alkalmazására azért, hogy tartósan rejtett hozzáférést biztosítsanak maguk számára, annak ellenére, hogy idővel szinte biztosan fény derül az incidensre? A történelem során az államok mindig is igyekeztek egymás titkait kifürkészni, és eközben soha nem válogattak különösebben a módszerekben. Nincs ez másképp a modern informatika világában sem, de az ehhez szükséges erőforrások ma szinte kizárólag az államok által támogatott csoportok számára állnak rendelkezésre. Így többségében három általános cél valószínűsíthető: az információszerzés, a befolyásolás és a pusztítás képességének elérése. A titkosszolgálatokhoz köthető incidensek jórészt az első két területet célozzák, míg a pusztítás inkább a nemzetbiztonsági vagy katonai akciók során jelenik meg.

Míg a hadviselés korai szakaszában a fizikai pusztítás volt az elsődleges cél, később az elrettentés is hatékony fegyvernek bizonyult. Az erőfölény nyilvánvalóvá tétele már önmagában képes biztosítani a domináns fél akaratának érvényesülését, ugyanakkor képet ad az azt biztosító környezetről. Az elrettentés a kibertérben is kiválóan alkalmazható eszközzé vált, mivel az informatikai berendezések működésének zavarait a társadalom egy része jól érzékeli, miközben annak lehetséges következményeitől a társadalom egészének tartania kell. Az ellátási láncban keletkezett zavarok hatása a létfontosságú rendszerelemek esetén ennél is továbbmegy, nemcsak az adott szolgáltatás eshet ki, hanem az arra épülő továbbiakban is problémát okozhat. Ez magyarázatot ad arra, hogy egy támadó számára miért nem feltétlenül jelent problémát, ha támadó célú kiberképessége ismertté válik az ellenfél számára. A nyilvánosság előtt természetes az ilyen irányú tevékenység tagadása, de a napvilágra kerülő incidensek minden szereplő számára nyilvánvalóvá teszik a támadó erejét és azt a tényt, hogy ellenséges hírszerzők az informatikai rendszerében szinte bárhol jelen lehetnek. Az APT-támadásokhoz kötődő befolyásolási képesség réme pedig a kibertér legerősebb országait is visszatartja egy kiberkonfliktus nyílt kezdeményezésétől.

A legnagyobb kárt talán az elektromos hálózat sikeres támadásával lehetne előidézni bármely országban; ez szinte a teljes ellátási láncban kifejtené a hatását. Elektromos áram nélkül szinte semmilyen terület nem tudja ellátni feladatát, és más kritikus infrastruktúrákkal szemben a kiesése teljes összeomlást váltana

ki. Az elektromos hálózat elemei ráadásul akár több évtizeddel ezelőtt épültek, régi, elavult technológiát használhatnak, ezért leváltásuk nem triviális feladat, és támadhatóságuk is egyszerűbb. Érdekes, de ez a probléma ráadásul épp a fejlett országokat érinti, hiszen a teljes ország elektromos rendszerének folyamatos korszerűsítése lehetetlen, így szükségszerűen megtalálhatók benne régi, elavult elemek. A hálózat kitettségét szinte minden nemzetállam érzékeli. Az Amerikai Egyesült Államok kitettségét a villamosenergia-rendszer elleni támadásoknak jól jellemzi, hogy Donald Trump egy 2020-as *executive orderben* az ezzel kapcsolatos kockázatok csökkentését írta elő. A rendeletben, amelynek létrejöttét minden bizonnyal titkosszolgálati információkra alapozták, Trump így fogalmaz:

> „[…] megállapítom, hogy a külföldi ellenfelek egyre inkább sebezhető pontokat hoznak létre és használnak ki az Egyesült Államok nagyfeszültségűvillamosenergia-rendszerében, amely biztosítja a nemzeti védelmünket, a létfontosságú vészhelyzeti szolgáltatásokat, a kritikus infrastruktúrát, a gazdaságot és a [mindennapi] életünkhöz szükséges villamos energiát. A nagyfeszültségűvillamosenergia-rendszer célpontja azoknak, akik rosszindulatú cselekményeket akarnak elkövetni az Egyesült Államok és az Egyesült Államok népe ellen, beleértve a rosszindulatú kibertevékenységeket is, mivel a nagyfeszültségűvillamosenergia-rendszerünk elleni sikeres támadás jelentős kockázatot jelentene gazdaságunkra […]”

Az elnök az energiaellátó rendszer fő gyengeségét a nem megbízható forrásból származó rendszerkomponensekkel azonosítja:

> „Megállapítom továbbá, hogy a külföldi ellenfelek tulajdonában lévő, általuk ellenőrzött, illetve joghatóságuk vagy irányításuk alá tartozó személyek által tervezett, fejlesztett, gyártott vagy szállított, az Egyesült Államokban lévő nagyfeszültségű elektromos berendezések korlátlan beszerzése vagy használata növeli a külföldi ellenfelek képességét, hogy potenciálisan katasztrofális következményekkel járó sebezhetőségeket hozzanak létre és használjanak ki a nagyfeszültségű elektromos berendezésekben. Ezért megállapítom, hogy a nagyfeszültségű elektromos berendezések korlátlan külföldi szállítása szokatlan és rendkívüli fenyegetést jelent az Egyesült Államok nemzetbiztonságára.”

A rendelet tiltásokat vezet be az energiaellátó rendszer komponenseinek elemeire:

> „[a tiltás] olyan elektromos hálózati berendezéseket érint, amelyeket olyan személyek terveztek, fejlesztettek, gyártottak vagy szállítottak, amelyek külföldi ellenfél tulajdonában vannak, annak ellenőrzése alatt állnak, annak joghatósága vagy irányítása alá tartoznak […] az Egyesült Államokban lévő nagyfeszültségűvillamosenergia-rendszer tervezése, integritása, gyártása, előállítása, termelése, elosztása, telepítése, üzemeltetése vagy karbantartása elleni szabotázs vagy felforgatás indokolatlan kockázatát hordozza magában.”

Egy 2021-ben megjelent utasítás ennél is tovább megy,[31] és megköveteli a kereskedelmi minisztertől a félvezetőgyártással, a védelmi minisztertől a kritikus ásványi anyagokkal kapcsolatos rizikófaktorok, az egészségügyi minisztertől a gyógyszerek és hatóanyagaik kockázatainak azonosítását és kezelésükre vonatkozó ajánlásokat. A rendelet az energiaügyi, a közlekedési és a mezőgazdasági minisztérium mellett a kereskedelmi és belbiztonsági tárca vezetőit utasítja, hogy

> „[…] a megfelelő ügynökségek vezetőivel konzultálva jelentést nyújtsanak be az információs és kommunikációs technológiai (IKT) ipari bázis kritikus ágazatainak és alágazatainak ellátási láncáról (a kereskedelmi miniszter és a belbiztonsági miniszter által meghatározottak szerint), beleértve az IKT-szoftverek, az adatok és a kapcsolódó szolgáltatások fejlesztésének ipari bázisát."[32]

Az elnöki utasítások tartalmát valószínűsíthetően titkosszolgálati információkra alapozták, és akár korábbi példákra is támaszkodhattak. A támadás nem lenne példa nélküli: Ukrajna elektromosenergia-ellátási hálózatával szemben már hajtottak végre sikeres kibertámadást, amely a feltételezések szerint egy BlackEnergy nevű trójaira volt visszavezethető.[33]

A támadás eszközeinek vizsgálata önmagában is könyvet alkothatna. Szakemberek körében sokszor említett gyenge pont az Internet of Things (IoT) és az olcsó távol-keleti berendezések beépítése kritikus informatikai rendszerekbe. Az IoT-eszközökkel szembeni leggyakoribb kritika a futtatott szoftver ellenőrizhetetlensége és a minimális számítási kapacitásból adódó kriptográfiai eljárások alkalmazhatóságának hiánya. Ezek az eszközök ugyanis rendszerint nem rendelkeznek elég erőforrással ahhoz, hogy erős titkosítási algoritmusokat hajthassanak végre, így védelmük nehézségekbe ütközhet. Az ellenőrizetlen olcsó berendezések üzleti alkalmazása erősen ellenjavallt, mivel nem tudható, hogy azokba a gyártó milyen rejtett funkciókat épített be. Mivel Kína berendezkedése lehetőséget nyújt arra, hogy az állami vezetés bármikor előírja, hogy egy gyártó az érdekeinek megfelelően módosítsa a termék funkcionalitását, ezeket az üzleti szempontból kritikus területeken nem célszerű használni.

Ugyanakkor az ellenőrzési eljárásokat sikeresen teljesítő eszközökben is lehetnek hibák, amelyek jelentős értéket képviselnek, és mivel nem közismertek,

[31] White House: *Executive order EO14017: America's Supply Chains. Executive Office of the President on 03/01/2021.*

[32] White House: *Executive Order on Securing the United States Bulk-Power System* (2020. május).

[33] Robert Lipovsky: Back in BlackEnergy: 2014 Targeted Attacks in Ukraine and Poland. *WeLiveSecurity.com*, 2014. szeptember 22.

piaci értékük van, amellyel kereskednek is. A sérülékenységek vásárlói a magas ár következtében általában kormányzati szereplők.[34]

Terrorszervezetek, vallási csoportok

A terrorcselekmények célja rendszerint a lakosság megfélemlítése, a kormányzat rákényszerítése valamilyen intézkedésre vagy egy ország politikai, alkotmányos vagy gazdasági destabilizálása. A legtöbb esetben ezért védtelen civileket támadnak, mivel ennek kivitelezése a legegyszerűbb, és nem is kötődik különösebben a kibertérhez. Bár a terrorszervezetek számára ideális lehetőség lehetne egy szervezet informatikai infrastruktúrájának támadása, eddig elenyésző számban fordultak elő olyan esetek, amikor terrortámadás okozta informatikai üzemzavarral érték volna el az említett célok valamelyikét. Eszközként azonban ez a kör alkalmazza a kibertér szolgáltatásait. Az Európai Unió 2018-as állásfoglalása az alábbi szerint fogalmazza meg a terroristacsoportok és a kibertér kapcsolatát:[35]

> „Mivel számos terrorista csoport és szervezet toborzásra, radikalizálásra és a terrorista propaganda terjesztésére szolgáló olcsó eszközként használja a kiberteret; mivel terrorista csoportok, nem állami szereplők és nemzetközi bűnszövetkezetek arra használják a kiberműveleteket, hogy a névtelenség leple alatt szerezzenek pénzforrásokat, hírszerzési információkat gyűjtsenek és kiberterror-kampányok indításához kiberfegyvereket fejlesszenek ki, kritikus infrastruktúrákat romboljanak szét, tegyenek tönkre vagy semmisítsenek meg, pénzügyi rendszereket támadjanak meg és egyéb illegális tevékenységeket folytassanak, amelyek kihatással járnak az európai polgárok biztonságára nézve."

A magyar kibevédelmi szakemberek szinte egyöntetű véleménye, hogy Magyarország a jelenlegi politikai helyzetben nem célpontja az ellátási láncra irányuló cselekményeknek. Ahogyan a már említett Digitális Mohács szerzői is utalnak rá, feltehetően ennek köszönhető, hogy bár az elektromos távvezetékek, optikai kábelek támadása aránylag sikeresen végrehajtható lenne, mégsem történnek ilyen incidensek. Az egyszerű szolgáltatáskiesések valószínűleg nem segítenék

[34] A közismert Chrome böngésző esetében egy távoli kódfuttatást lehetővé tevő sérülékenység demonstrálása e sorok írásakor 500 000 dollárt ér a Zerodiumnál, lásd: https://zerodium.com/program.html.

[35] Európai Parlament: Az Európai Parlament 2018. június 12-i állásfoglalása a kibervédelemről (2018/2004(INI)). 2018. június 12.

az elkövetőket eléggé a céljaik elérésében, a civil szféra számára okozott kényelmetlenség miatt esetleg épp az elvárttal ellenkező hatást érnének el: a közvélemény ellenük fordulna. Természetesen elképzelhető, hogy előbb-utóbb terroristák által végrehajtott kibertámadás is bekövetkezik, de ahhoz ezeknek a csoportoknak olyan szakmai hátteret kell felépíteniük, amelyhez szükséges anyagi háttér jelenleg valószínűsíthetően nem áll rendelkezésükre.

Rosszindulatú hackerek

Az ellátási láncban a fentiektől eltérő célú kibertámadások is okoztak zavarokat. Az anyagi haszonszerzés érdekében készített támadó szoftverek meghiúsítják az informatikai rendszerek működését. Az elmúlt évek legjellemzőbb eszközei a kriptovírusok különböző változatai voltak, amelyek sikeresen okoztak zavarokat a gazdasági szereplők informatikai rendszereiben. A NotPetya *ransomware*-rel elkövetett támadás által okozott károk hosszan sorolhatók, nem ritkák az olyan üzemzavarok sem, mint a csernobili atomerőmű ipari telephelye automatikus ellenőrző rendszerének ideiglenes leállása. A 2017-ben indított WannaCry legalább 150 országban hozzávetőleg 300 000 számítógép adatait tette elérhetetlenné, és az egészségügyi ellátási láncban is súlyos zavarokat okozott. A legtöbb fertőzést Oroszországban regisztrálták, ahol a legnagyobb vállalatok mellett a Sberbank és különböző minisztériumok számítógépei is áldozatul estek. Más európai országok is nagy károkat szenvedtek, több esetben kórházak is működésképtelenné váltak, így az egészségügyi ellátásban keletkezett zavarok következtében halálesetek is történtek. A *ransomware*-támadások előtt nem voltak ismertek ilyen súlyos következményekkel járó esetek.

Érdekes tény, hogy a WannaCry működése azokon a kiberfegyvereken alapult, amelyeket az NSA fejlesztett ki, és tartalékolt egy esetleges kiberművelet végrehajtásához. Az NSA eljárási rendjében levő hiba következtében a szoftverek a támadókhoz kerültek, majd később a dark neten is megvásárolhatók voltak.

Az ellátási lánc támadása a rosszindulatú hackerek számára a legtöbb esetben anyagi haszonszerzésről szól, valódi céljuk nem az ellátási lánc működésének megzavarása, azt csupán fenyegetésként használják anyagi céljaik eléréséhez. Kiváló lehetőség számukra, hiszen ezzel könnyen rá tudják kényszeríteni áldozataikat arra, hogy fizessenek nekik.

Ellentevékenységek

Az ellátási láncok alkotóelemeinek kifejlesztése és felépítése több ország szervezeteinek összetett hálózatán át történik. Számos elem komplexitása olyan nagy, hogy az hagyományos módszerekkel vagy eszközökkel nem ellenőrizhető. A helyzet kezelését tovább nehezíti, hogy a különféle ellenőrzéseket a rendszerek minden egyes változása esetén újra és újra el kellene végezni. Mivel ennek végrehajtása nagyon költséges lenne, nem zárhatók ki a hibák, a védekezés módszertanában így hangsúlyos szerep jut a kockázatkezelésnek, az ajánlások, jó gyakorlatok és szabványok alkalmazásának. Mivel mindig lesznek olyan pontok, amelyeket egy művelet során ki lehet majd használni, az ellátási lánc ellen indított műveletek időnként sikeresek lesznek, ezt nem lehet elkerülni. A védelem célja ezért a kiemelt fontosságú elemek költségarányos, ugyanakkor minél magasabb szintű védelme, felkészülés a lehetséges kockázatokra és azok szakszerű kezelésére.[36]

A kockázatkezelés elterjedt módszertanában egy esemény kockázatát a bekövetkezés valószínűségének és az okozott kár nagyságának együttesével határozzák meg. Így a gyakran bekövetkező, de kis kárértékű esemény kezelésére hozzávetőleg ugyanakkora erőforrást kell biztosítani. A nagy kárt okozó események azonban rendszerint csak nagy költségű megoldásokkal előzhetők meg, és anyagi források hiányában vagy a költségarányos védelem következtében elmarad a megfelelő eljárások bevezetése.

A termelőkből, alvállalkozókból, szállítókból, kereskedőkből és fogyasztókból álló ellátási láncban a rendszeresen előforduló zavarok kivédésére fordítanak kiemelt figyelmet. A láncok rendszerint hierarchikus szervezésűek, csúcsukon a megrendelő áll. Az elsődleges beszállítók csomópontokat alkotnak, amelyekhez további elemek, az alvállalkozók kapcsolódnak. A csomópontoknak megfelelően integrálódni kell a felettük elhelyezkedő elembe. A struktúrában akár egyetlen láncszem a teljes folyamatra nézve kritikus lehet, mivel a láncok működését ugyanakkor olyan globális beszállítók is befolyásolják, amelyek kiesése katasztrofális hatású, és a keletkező hullámhatás a teljes rendszeren végighalad.

Az ellátási láncok életciklusának tervszerű kialakítása az egyik leghatékonyabb módszer a működési biztonság szintjének emelésére. Ez következetesen összehangolt tevékenységet igényel, amelynek biztosítania kell az életciklus

[36] Supply Chain Attacks, Cybersecurity & Regulations: What to Expect in 2021. *Quointelligence,* 2021. január 27.

minden pontján az átláthatóságot és az ellenőrizhetőséget. Mivel a mai rendszerek fejlesztése már nem egy helyen történik, ezt nehéz teljes egészében elérni.[37] Az Egyesült Államokban az ICT-rendszerek hibáiból eredő kár már 2003-ban meghaladta a 60 milliárd dollárt,[38] így az ezekre épülő szolgáltatások védelmére az ország kockázatkezelési gyakorlati programokat kínál. Az alkalmazhatóság és az érvényesség érdekében ezek a programok célszerűen a korábbi precedenseken alapulnak, és azokat időről időre aktualizálni kell. Az életciklus folyamatainak standardizálására gyakran mintákba foglaló keretrendszerek kidolgozása és közzététele a megoldás.

A MITRE tanulmányában bemutatott, az ellátási lánc támadását célzó esetek elemzésével készült el a *potenciális ellenintézkedések katalógusa,* amely 20 csoportba sorolva foglalja össze az ellátási láncokhoz kapcsolódó intézkedéseket. Ezek részben más ajánlások testreszabott adaptációi, részben kifejezetten ellátásilánc-specifikusak (Reed, Miller és Popick alapján). A katalógus az alábbi védelmi pontok mentén javasolja az ellentevékenységek felépítését.

A *szoftverek biztonságos konfigurációkezelése* a fejlesztési rendszer általános felügyeletét, a hozzáférések ellenőrzését, a rendszer és a termék sértetlenségének, integritásának ellenőrzését, a konfigurációkezelés kritériumainak meghatározását és alkalmazását emeli ki.

A *kritikus komponensek manipulálásának megelőzésére* számos, az adott komponensre kialakított eljárást kell biztosítani. Ebben a legegyszerűbb, de esetenként hatékony módszer a szemrevételezés, amely során pusztán külső nyomok alapján szűrhető ki a manipuláció. Általános szabály a *névtelenség biztosítása,* azaz, amennyiben lehetséges, a potenciális támadók elől el kell fedni a végfelhasználó kilétét. A rendszer komponenseinek *anonim vásárlása* a rendszer kialakításának korai fázisában segít megelőzni a kompromittált változatok bejuttatását. Az egyedi konfigurációk alkalmazásakor az anonimitás már nehezebben biztosítható, így érdemes mérlegelni ennek elkerülését. A *megbízható szállítás* különösen kritikus pont, mert ennek során a biztonsági eljárásokat nem védett környezetben kell érvényesíteni. A jogosulatlan hozzáférés, az adattartalom megismerése, a hamisítás, a csere vagy a módosítás elkerülését fizikai és logikai mechanizmusokon keresztül lehet biztosítani a fejlesztési, az üzembehelyezési

[37] Christopher J. Alberts – Audrey J. Dorofee: *A Framework for Categorizing Key Drivers of Risk*. Carnegie Mellon, 2009.

[38] Michael Newman: Software Errors Cost U.S. Economy $59.5 Billion Annually. *National Institute of Standards and Technology (NIST News Release),* 2002. június 28.

és az üzemeltetési fázisban is. Az ellátási lánc elemeinek javítása, a cserealkatrészek szállítása során célszerű hologramokat, optikai vagy RFID-azonosítókat és egyedi vagy speciális csomagolást alkalmazni. Különös figyelmet érdemes szánni a szoftverkomponensek megváltoztatásának elkerülésére, amelyre szintén számos módszer ismert, de biztonságuk csak az eljárási rend maradéktalan betartásával garantálható. Az *elektromágneses vagy termikus elemzés* lehetőséget nyújt a hardverelemek módosításának detektálására. Valószínűleg egy ilyen vizsgálat mutatta ki a Supermicro alaplapjának módosítását. Az *ellátási lánc átláthatósága* a felhasználó számára biztosítja az abban rejlő kockázatok azonosítását és azok kezelését. *A teljes ellátási láncban vizsgálni kell a komponensek származását,* lehetőség szerint ugyanarra a komponensre *több beszállítóval* is ki kell alakítani a kapcsolatot, és *értékelni kell a kritikus elemek beszállítóinak megbízhatóságát*.

A *biztonságra összpontosító programozási nyelvek alkalmazása* már a tervezési fázisban meghatározható. Ebbe a kategóriába nem csak maguk a programozási nyelvek értendők, idetartoznak a különböző programkönyvtárak, harmadik féltől származó szoftverelemek, futtató környezetek is. A biztonságra nem eléggé összpontosító fejlesztőeszközre az Adobe által 1996-ban kifejlesztett Flash az egyik legismertebb példa, amelyet elsősorban webböngészőkben futó alkalmazások fejlesztésére terveztek. A Flash technológiája szinte teljes élete során biztonsági hibáktól szenvedett, és teljesen ellehetetlenült, miután a legtöbb böngésző letiltotta annak működését.

A *biztonságközpontú tervezési és kódolási szabványok* beépítése és rendszeres felülvizsgálata nemcsak a rendszer rendelkezésre állásának garanciáját teremtheti meg, hanem biztosítja adattárolásának és kommunikációjának bizalmasságát is. Egy rendszer megtervezésekor nem csak annak funkcióira, hanem az üzemelési környezet meghatározására is ki kell térni. Az olyan kritikus rendszerek működését, amelyektől rendkívül magas szintű rendelkezésre állást követelnek meg, nem lehet egyetlen szerverrel megoldani, ehhez több, szétszórtan elhelyezkedő, elosztott működésű kiszolgálóra van szükség. Ennek megvalósítását sokan üzemeltetési feladatnak tekintik, valójában egy ilyen rendszert akkor lehet létrehozni, ha ezt a kritériumot már a tervezési fázisban beépítették. A biztonságos adattárolás legtöbbször kriptográfiai eljárások alkalmazásával valósul meg, de ezek sem örökéletűek, így már a tervezési fázisban érdemes kidolgozni a későbbi cseréjük eljárását.[39] A *hálózati forgalom korlátozásának*

[39] Mary Cindy Ah Kioon – Zhao Shun Wang – Shubra Deb Das: Security Analysis of MD5 algorithm in Password Storage. *ResearchGate, Proceedings of the 2nd International Symposium on*

szabályait a rendszerben megvalósított kommunikációs folyamatok alapján már a tervezési folyamat során dokumentálni kell, és a telepítési és tesztelési fázisban alkalmazni kell.

Red Team és Bug Bounty programok. Sajnos az informatikai rendszerek támadására alkalmazott módszerek mindig is túl változatosak voltak ahhoz, hogy azokat részletesen nyomon lehessen követni. A sérülékenységek technikai tartalmának vizsgálata, azok nyomon követése, a támadó kódok elemzése és az ellentevékenység kidolgozása egy szűk szakmai réteg feladata, amely idővel mindig meghaladja a legjobb szakemberek képességeit is. A sérülékenységek hatalmas száma szinte lehetetlenné teszi a teljes körű védettség kialakítását. A CVE-adatbázis[40] e sorok írásakor 156 019 rekordot tartalmaz, amelyek az egyes szoftvereket, rendszerkomponenseket érintő sérülékenységekről részletes leírást tartalmaznak. A támadók mindig újabb és újabb módszereket találnak majd arra, hogy a rendszerekbe behatoljanak, és ezt valószínűleg nem tudjuk megakadályozni. Az informatikai rendszerek üzemeltetői rendszerint sémák mentén végzik a feladataikat. Frissítéseket és új szoftvereket telepítenek, elvégzik az adatvagyon mentését. A legtöbbjük nem rendelkezik napi ismeretekkel a különböző sérülékenységekről, pusztán az eljárásrendet követve végzi el a feladatát. Egy rendszer biztonságos működtetésében sokat segít, ha az üzemeltetők ismerik azokat a módszereket és eszköztárakat, amelyeket a támadók is használnak, hiszen a legtöbb esetben nem önálló fejlesztést végeznek, csupán meglevő eszközöket alkalmaznak. A sérülékenységek felderítésére érdemes erre a célra fejlesztett célszoftvert használni,[41] és legalább a külvilág számára elérhető gépek esetén elvégezni a *hardeningbeállításokat.*[42] A különböző időszaki jelentések képet adnak az elkövetkező időszak fenyegetettségeinek változásairól, ami alapul szolgálhat a jövőbeni felkészüléshez. A *Red Team* alkalmazása egy fajta megoldást jelenthet a problémák kezelésére. Ez a csoport az ellátási láncot alkotó rendszerre, az annak működését biztosító személyzetre, valamint a felhasználóira irányuló behatolásvizsgálatokat végez, amelyekkel feltárhatók a sérülékenységek, és begyakorolhatók a veszélyhelyzeti eljárások.[43] A *Bug*

Computer, Communication, Control and Automation, 2013.

[40] Lásd: https://cve.mitre.org

[41] Ilyen szoftver a Nessus, amelynek a korlátozott számú számítógép ellenőrzésére szolgáló tesztverziója ingyenesen letölthető: www.tenable.com.

[42] A *hardeningeljárás* a biztonsági beállítások lehetőség szerinti legszigorúbb szintjét jelenti.

[43] Egy Red Team program nem feltétlenül valamiféle bonyolult műszaki megoldás, számos cég teszteli például a munkatársait megtévesztő vagy káros mellékletet tartalmazó levelekkel úgy, hogy

Bounty programok bizonyos keretek közt bárki számára lehetőséget adnak biztonsági hibák felderítésére, és annak jelzése esetén jutalmazzák annak jelzését.

Tartalék eszközök rendelkezésre állása. A tervezés alapvető fontosságú az ellentevékenység végrehajtásában, ez biztosítja az egyes eljárások meghatározását és az ahhoz szükséges erőforrások rendelkezésre állását. A lehetséges zavarok előzetes számbavétele, a kiesésük vagy zavaruk esetében keletkező kár felmérése, a kezelésben részt vevők szerepköreinek definiálása, a szervezet vészhelyzeti működésének meghatározása tudja biztosítani a megfelelő kezelést. A pótalkatrészek JIT-rendszerű rendelkezésre állása lerövidíti az adott komponens által okozott szolgáltatás kiesésének idejét, a bevizsgált raktárkészlet csökkenti a kompromittált komponens beépítését. A katasztrófatervek kidolgozása, azok megismertetése és gyakorlása, valamint az ahhoz szükséges tartalék eszközök rendelkezésre állása helyettesítheti az ellátási lánc kieső elemeit. Tipikus eszközök a szünetmentes tápegységek, az aggregátorok, a tartalék internetkapcsolatok és szerverek, a számítógépek, a hálózati elemek. Az ellátási lánc működőképességének biztosítására további hatékony védelmet nyújt a kritikus pontokon kialakított redundancia. Ez a tartalékokkal szemben a működő rendszerelemek olyan többszörözését jelenti, amelyben a kulcsfeladatok kezelését esetenként akár földrajzilag is elválasztott rendszerelemekre bízzák. A teljes rendszer így képes elviselni összetevői egy részének kiesését. A tartalékok kezelésének megléte, rendszeres frissítése, betartása és annak ellenőrzése szintén alapvető az ellátási láncot támogató informatikai rendszerek működtetése során.

A felhasználók informatikai képzését nem lehet elég alkalommal hangsúlyozni. A kibertámadások még mindig leginkább e-mail-mellékletek vagy megtévesztő weboldalakról letöltött alkalmazások útján válnak aktívvá a kliensszámítógépeken. Az incidens gyakran ilyen jellegű felhasználói hibával indul, és bár egy részük teljesen nyilvánvalóan hamis, adott helyzetben még az üzemeltetők is becsaphatók.[44] A kulcsfelhasználók és üzemeltetők megbízhatóságának sérülése fokozott veszélyforrás, mivel ők a magasabb jogosultsági szintjük következtében a rendszer komponenseinek szélesebb köréhez férnek hozzá, így az általuk szándékosan vagy véletlenül okozott kár mértéke sokkal jelentősebb lehet. A védelmi feladatok ellátásában a felelősség többrétű, és sok esetben

amennyiben a munkatárs arra nem az elvárt módon reagál, oktatási programban kell részt vennie.

[44] Ha például egy munkatárs gyakran fogad csomagküldeményeket, valószínűleg nehezebben tűnik fel számára, ha egy *ransomware*-t tartalmazó levél a megszokott csomagküldő nevében érkezik.

a szakmai vélemények is eltérnek arról, hogy egy incidens bekövetkezésekor végső soron kinek kell a morális felelősséget viselnie.[45]

A célzott támadásokkal szemben már sokkal nehezebb a hatékony védekezés kialakítása. Az átláthatóság érdekében a szervezetek közzéteszik tevékenységüket, referenciáikat, az adott terület vezetőjének, munkatársainak elérhetőségeit, így a nyílt forrású felderítés (*open source intelligence* – OSINT) alkalmazásával nagy mennyiségű információt nyújtanak egy ilyen támadás megalapozásához.

A *szoftverfrissítés biztonsága* a SolarWinds esete óta közismert kockázati tényező a módosított rendszerkomponensek célba juttatására.[46] A nagyvállalatok informatikai szabályzatai a rendelkezésre állás biztosításáért gyakran tiltják a frissítések azonnali telepítését, azok előzetes ellenőrzését írják elő. A magas biztonsági szintet elváró szervezetek egy köre a dobozos szoftverek auditálását is megköveteli, vagy a Common Criteria valamely szintje szerinti megfelelőséget vár el.[47] A *zero-day* sérülékenységek hatásának elkerülése szinte lehetetlen. Ezek alapján kimondható, hogy csak kevés informatikai rendszer képes arra, hogy a teljes életciklusa során incidensmentes legyen. Szabályzati szinten az üzletfolytonossági terv határozza meg az üzemzavar esetén végrehajtandó ellentevékenységek körét. A hatékony adminisztratív védelem kidolgozásának egyik nehézsége az összetett események kezelése és azok másodrendű hatásainak elemzése.

Összefoglalás

Az ellátási láncban keletkezett zavarok minden ország esetében jelentős problémát okoznak, amit számos kormány felismert, és erőforrásokat fordít annak védelmére. Valószínű, hogy a láncok komplexitása tovább növekszik, az internetes lefedettség egyre nagyobb területek számára jelent majd alig érzékelhető támadási lehetőséget. Az 5G hálózatokra alapozott fejlesztési tervek, az önvezető járművek, okosvárosok, okosotthonok kényelme egyre értékesebb támadási pontot nyújt, és egyre inkább növeli a társadalom kitettségét az infrastruktúra és az arra épülő ellátási lánc sérülékenységeinek. A fenyegetettség mértéke

[45] Vélemény: A sírás határán – a WannaCry-probléma. *Hwsw.hu,* 2017. május 16.

[46] FireEye: Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor. *Fireeye.com,* 2020. december 13.

[47] A Common Criteria informatikai biztonsági keretrendszere különféle védelmi profilok mentén garantálja egy szoftver vagy eszköz biztonságos működését.

a társadalom számára alig érezhető, miközben egyes források az ellátási lánc elemei közé már olyan termékeket is besorolnak, mint a Microsoft Office szolgáltatásai. A hadviselés kiterjed a kibertérre is, miközben a kiberképességek fejlesztésére a legnagyobb hangsúlyt fektető országok, Nagy Britannia, Izrael, Kína, Oroszország és az Egyesült Államok saját rendszerei is sérülékenyek. Az ellátási láncok ellen indított kiberműveletek száma bár rendkívül alacsony, egy sikeres támadás közvetett és közvetlen hatásai súlyos kockázati tényezőket jelentenek. Az olyan rendkívüli események, mint a Covid–19, amelynek kezelése során az informatikai rendszerek rutinszerű működését az alkalmi megoldások kényszere váltotta fel, a jövőben is kiváló alkalmat nyújt majd érzékeny célpontok felkutatására és megtámadására, miközben a „láthatatlan ellenség" elleni védekezés fontossága is felértékelődik.

Irodalomjegyzék

Ah Kioon, Mary Cindy – Zhaoshun Wang – Shubra Deb Das: Security Analysis of MD5 algorithm in Password Storage. *ResearchGate, Proceedings of the 2nd International Symposium on Computer, Communication, Control and Automation,* 2013.

Alberts, Christopher J. – Audrey J. Dorofee: *A Framework for Categorizing Key Drivers of Risk.* Carnegie Mellon, 2009. Online: https://resources.sei.cmu.edu/asset_files/TechnicalReport/2009_005_001_15104.pdf

Bányász Péter: Az ellátási lánc kiberfenyegetettsége, különös tekintettel a közlekedési alrendszer biztonságára, a szervezett bűnözés hatásai. In Kállai Attila et al.: *Humánvédelem – békeműveleti és veszélyhelyzet-kezelési eljárások fejlesztése. Tanulmánygyűjtemény.* Budapest, Nemzeti Közszolgálati Egyetem, 2016. 643–673. Online: http://real.mtak.hu/id/eprint/94339

Bodoróczki János: A modern hadviselés logisztikája – a katonai logisztika jövője. *Hadtudomány,* 30. (2020), 2. 98–108. Online: www.mhtt.eu/hadtudomany/2020/2020_2szam/098-108_Bodoroczki.pdf

Bodnár Zsolt: Rizsszemnyi mikrochipekkel hajthatta végre Kína a legnagyobb USA elleni támadást. *Qubit.hu,* 2018. október 5. Online: https://qubit.hu/2018/10/05/rizsszemnyi-mikrochipekkel-hajthatta-vegre-kina-a-legnagyobb-usa-elleni-hackertamadast

Boyens, – Celia Paulsen – Rama Moorthy – Nadya Bartol: *Supply Chain Risk Management Practices for Federal Information Systems and Organizations.* National Institute of Standards and Technology, 2015. Online: https://doi.org/10.6028/NIST.SP.800-161

Casey, Tim[othy]: Understanding Cyberthreat Motivations to Improve Defense. *Intel White Paper,* 2015. február 16. Online: www.intel.com/content/dam/www/public/us/en/documents/white-papers/understanding-cyberthreat-motivations-to-improve-defense-paper.pdf

Chikán Attila: *Vállalatgazdaságtan*. Budapest, Aula, 2004.

Cserháti András: A Stuxnet vírus és az iráni atomprogram. *Nukleon,* 4. (2011), 1. 1–7. Online: https://nuklearis.hu/sites/default/files/nukleon/Nukleon_4_1_85_Cserhati_.pdf

Deák Veronika (szerk.): *Célzott kibertámadások. Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára.* Budapest, Nemzeti Közszolgálati Egyetem, 2018.

DeBusk, Steven S.: *What Happens When the Supply Chain Breaks? Implications for the Army Supply Chain Under Attack.* Fort Leavenworth, School of Advanced Military Studies United States Army Command and General Staff College (First Term AY 02-03), 2003.

DoD Defense Science Board: DSB Task Force Report on Cyber Supply Chain, 2017. Online: www.hsdl.org/?view&did=799509

Európai Parlament: Az Európai Parlament 2018. június 12-i állásfoglalása a kibervédelemről (2018/2004(INI)). 2018. június 12. Online: www.europarl.europa.eu/doceo/document/TA-8-2018-0258_HU.html

FireEye: Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor. *Fireeye.com,* 2020. december 13. Online: https://bit.ly/3yoJq4r

Flying Fraudulently – How a Weak Supply Chain Became the Usaf's Worst Enemy. *Airforce Technology,* 2012. szeptember 24. Online: www.airforce-technology.com/features/featuresupply-chain-us-air-force-fraudulent-parts

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

Heinbockel, William J. – Ellen R. Laderman – Gloria J. Serrao: *Supply Chain Attacks and Resiliency Mitigations, Guidance for System Security Engineers*. MITRE, 2017. október. Online: www.mitre.org/sites/default/files/publications/pr-18-0854-supply-chain-cyber-resiliency-mitigations.pdf

Hippold, Sarah: 5 Trends From the Gartner Hype Cycle for Supply Chain Strategy. *Gartner,* 2020. október 2. Online: www.gartner.com/smarterwithgartner/5-trends-from-the-gartner-hype-cycle-for-supply-chain-strategy-2020.

Joint Publication 3-13, Information Operations, 2012. Online: www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_13.pdf

Juhász Péter – Száz János – Misik Sándor: Ellátási láncok versenyképessége és finanszírozása – gondolatok az optimumról. *Közgazdasági Szemle,* 56. (2019), 1. 53–71. Online: http://dx.doi.org/10.18414/KSZ.2019.1.53

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

Kovács László – Krasznay Csaba: Digitális Mohács. Egy kibertámadási forgatókönyv Magyarország ellen. *Nemzet és Biztonság,* 3. (2010), 1. 44–56. Online: www.nemzetesbiztonsag.hu/cikkek/kovacs_laszlo__krasznay_csaba-digitalis_mohacs_.pdf

Krasznay Csaba: A polgárok védelme egy kiberkonfliktusban. *Hadmérnök,* 7. (2012), 4. 142–151.

Lipovsky, Robert: Back in BlackEnergy: 2014 Targeted Attacks in Ukraine and Poland. *WeLiveSecurity.com,* 2014. szeptember 22. Online: www.welivesecurity.com/2014/09/22/back-in-blackenergy-2014/

Malik, Javvad: *Ethics, Security and Getting the Job Done.* AlienVault, 2015. november. Online: https://cdn-cybersecurity.att.com/docs/whitepapers/rsa-survey-report.pdf

Newman, Michael: Software Errors Cost U.S. Economy $59.5 Billion Annually. *National Institute of Standards and Technology (NIST News Release),* 2002. június 28. Online: www.abeacha.com/NIST_press_release_bugs_cost.html

NIST Computer Security Center: Definitions. Online: https://csrc.nist.gov/glossary/term/ict_supply_chain

Reed, Melinda – John F. Miller – Paul Popick: *Supply Chain Attack Patterns: Framework and Catalog.* Office of the Assistant Secretary of Defense for Research and Engineering, 2014. Online: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.648.6043&rep=rep1&type=pdf

Robertson, Jordan – Michael Riley: The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies. *Bloomberg Businessweek,* 2018. október 4. Online: www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

Schmidt, Andreas: The Estonian Cyberattacks. *Researchgate.net,* 2013. január. Online: www.researchgate.net/publication/264418820_The_Estonian_Cyberattacks

Supply Chain Attacks, Cybersecurity & Regulations: What to Expect in 2021. *Quointelligence,* 2021. január 27. Online: https://quointelligence.eu/2021/01/supply-chain-attacks-cybersecurity-regulations-in-2021

Vélemény: A sírás határán – a WannaCry-probléma. *Hwsw.hu,* 2017. május 16. Online: www.hwsw.hu/hirek/57252/microsoft-wannacry-it-biztonsag-kocsis-tamas-balazs-zoltan.html

West, Darrell M.: *Internet Shutdowns Cost Countries $2.4 Billion Last Year.* Center for Technology Innovations at Brookings, 2016. Online: www.brookings.edu/wp-content/uploads/2016/10/intenet-shutdowns-v-3.pdf

White House: *Executive Order on Securing the United States Bulk-Power System* (2020. május). Online: https://trumpwhitehouse.archives.gov/presidential-actions/executive-order-securing-united-states-bulk-power-system/

White House: *Executive order EO14017: America's Supply Chains. Executive Office of the President on 03/01/2021.* Online: www.federalregister.gov/documents/2021/03/01/2021-04280/americas-supply-chains

Yang, Lin – Quan Yu: *Dynamically Enabled Cyber Defense.* H. n., World Scientific, 2021.

9. fejezet

A katonai információs rendszerek elleni műveletek – az informatikai megsemmisítés a valós szőnyegbombázástól a precíziós *malware*-ig

Üveges András József

Bevezetés

A digitális társadalom gyors előretörésének következtében felmerülő kiberbiztonsági kockázatok a mindennapi élet mellett számos ágazatot érintenek. Napjainkra a védelempolitikai nyilatkozatokban és elgondolásokban alapvetővé vált az, hogy a jelenlegi és jövőbeli katonai műveletekben a fizikai csapásmérő erőkkel együtt vagy önállóan alkalmazott kiber- és hibrid hadviselési módszerek dominanciája emelkedő tendenciát mutat. A NATO álláspontja szerint ez már a negyedik dimenziója a hadviselésnek. Mint minden katonai műveletet, a kiberműveleteket is fegyverekkel vívják meg. Ilyen eszközök a rosszindulatú szoftverek is, amelyek napjainkra a kiberhadviselés egyik alapeszközévé váltak, amelyekkel az egyes reguláris vagy irreguláris erők sikeres műveleteket képesek végrehajtani a katonai információs rendszerek ellen.

A NATO 2007-től kiemelt figyelmet fordít a kibervédelemre és a kiberhadviselésre. A 2012-es évben a kibervédelem mint koncepció vagy elgondolás bekerült a NATO védelmi tervezési folyamatába is. A legjelentősebb esemény viszont a 2014-es walesi csúcs[1] egyik döntése volt, amellyel elfogadták a NATO kibervédelmi szakpolitikai irányait.[2]

Ezt követően 2016-ban a varsói csúcsértekezleten a szövetséges erők amellett, hogy megerősítették a NATO védelmi jellegét, műveleti területté nyilvánították a kiberteret is.[3]

[1] NATO e-Library: *Wales Summit Declaration, Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Wales*. 2014.

[2] *Wales Summit Declaration* (2014): i. m. 72–73.

[3] NATO e-Library: *Warsaw Summit Communiqué: Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Warsaw.* 2016.

https://doi.org/10.36250/01079_09

https://orcid.org/0000-0002-5860-2405

Általánosan elmondható, hogy a kiberhadviselés vonatkozásában a műveleteket állami szereplők, jellemzően hírszerzésre, disztruptív vagy destruktív céllal, közvetlenül – vagy proxyfelhasználó segítségével – hajtják végre. A kiberhadviselés témaköréhez tartozik minden olyan kibertérben végrehajtott offenzív művelet is, amelynek a támadást végrehajtó ország – tágabb értelemben szélsőséges szervezet – szemszögéből katonai vagy politikai értelemben véve értékelhető (hasznos) eredménye van.

Az előbbiekben említett támadásokat rosszindulatú szoftverek segítségével lehet a leghatékonyabban végrehajtani a kibertérben, ahol használhatjuk ezeket széleskörűen (globálisan vagy mondhatjuk, szőnyegbombázás formájában) vagy csak konkrétan egy adott célpont ellen, testre szabva. Utóbbi esetben kifejezetten a célba vett rendszerre írt kártékony szoftverrel hajtják végre a támadást.

A *malware*-eket hatékonyan alkalmazzák egymás ellen akár békeidőszakban is az ellenérdekeltségű országok. Ezek a műveletek a kibertérben követik a valóságban fennálló geopolitikai ellentéteket. Ilyen geopolitikai ellentét húzódik például Kína és India viszonylatában, illetve India és Pakisztán vonatkozásában. A szemben álló felek előszeretettel alkalmaznak precíziós *malware*-eket arra, hogy a kibertérből támadva megbénítsák vagy rombolják az ellenérdekeltségű ország infrastruktúráját, gyengítve ezzel annak gazdaságát. Rosszabb esetben destabilizálják annak alkotmányos rendjét egy nagyobb támadással. Ezekkel az eseményekkel a sajtóban többször is találkozhatunk.

Egy jól időzített *malware*-támadással (*fake news, defacement* stb.) hiteltelenné lehet tenni egy kormányt vagy egy szervezetet is. Akár választásokat is befolyásolhatunk velük. Azaz a *malware*-kampányok kiválóan alkalmasak az információs műveletek kivitelezésére a kibertérben.

A kínai kormány és az indiai vezetés között 2021-ben többször kiújult az ellentét egy határvita miatt. A kasmíri térséghez tartozó Ladakban a kínai kormány 90 ezer négyzetkilométeres területet követel magának. Az indiai rezsim szerint a kínai fennhatóság alatt álló Akszai Csin-fennsík 38 ezer négyzetkilométere Ladak eredeti része, amelynek ezért Indiához kell tartoznia.

2021 márciusában a *The Hindu* sajtóinformációi szerint a kínai kormányhoz köthető hackercsoport kártékony szoftvert juttatott be az indiai villamosenergia-elosztó rendszer egy részét kiszolgáló infrastruktúrába.

A támadást az amerikai érdekeltségű Recorded Future kiberbiztonsági vállalat fedte fel. A támadást 21 IP-címről indították 10 energetikai vállalat ellen.[4]

Rosszindulatú szoftverek

Mielőtt a témát részletesen tárgyalnánk, szükséges pontosítani a *malware* fogalmát. A *malware* kifejezés alapvetően és döntően gyűjtőfogalom. Magába foglal számos rosszindulatú szoftvert, mint például a trójai programok, a zsaroló vírusok, a klasszikus értelemben vett vírusok, férgek és banki kártevők. A médiában többször szinonimaként használják a kártevő szoftver, a kártékony szoftver és a káros szoftver fogalmát is.

Fajtájukat tekintve részletes leírást lehet olvasni Kovács László *A kibertér védelme* című művében, ahol a szerző részletesen kifejti az egyes csoportok jellemzőit.[5]

A káros szoftverek közös tulajdonsága az, hogy a készítőik rosszindulatú szándékkal, károkozás, illegális anyagi haszonszerzés vagy hírszerzés céljából készítették el ezeket. Ha még pontosabban megpróbáljuk definiálni, akkor mondhatjuk azt is, hogy olyan szoftverek, amelyek más szoftverek vagy rendszerek üzemszerű működését megakadályozzák,[6] onnan illegális módon adatokat tulajdonítanak el további felhasználás céljából.

Általánosságban az is elmondható róluk, hogy gyakran az elavult rendszerek sebezhetőségeit, a nem naprakész biztonsági rendszabályok okozta biztonsági réseket kihasználva terjednek, vagy a memóriában elfedve várakoznak, és csak egy előre programozott esemény során aktiválják magukat. Egyes esetekben ismert alkalmazásokat utánozva maradnak észrevétlenek. De az sem ritka, hogy a pszichológiai manipulációs módszerek segítségével emberi mulasztás vagy figyelmetlenség során jutnak be a célba vett rendszerekbe.

A *malware*-ek másik tulajdonsága, hogy kiválóan alkalmasak arra, hogy hatékony eszközei legyenek a korszerű kiberműveleti tevékenységeknek.[7]

[4] Regionális árufeladó központ *(regional load despatch centres)* és állami együttműködők, két tengeri kikötő.

[5] Kovács László: *A kibertér védelme*. Budapest, Dialóg Campus, 2018. 122. 5. táblázat.

[6] Simon Kramer – Julian C. Bradfield: A General Definition of Malware. *Journal in Computer Virology,* (2010), 6. 105–114.

[7] Haig Zsolt: *Információs műveletek a kibertérben*. Budapest, Dialóg Campus, 2018. 271.

A téma relevanciája és nagysága miatt alapvetően a *malware*-ek két típusával foglalkozunk. Az egyik csoportba azok tartoznak, amelyeket széles körben terjesztenek a készítőik, és céljuk, hogy úgynevezett széles merítést alkalmazva nagy mennyiségű adatot gyűjtsenek az internetről. A folyamatban nincs konkrét célpontja a *malware* alkalmazójának. Célja, hogy globális méretekben fertőzzön meg informatikai rendszereket, majd a befolyt adatokat szintetizálva, szűrve felhasználja a későbbiekben. Azaz a nagy adattömegben olyan részinformációkat keresnek az elkövetők, amelyek egy későbbi támadás során felhasználhatóak. Természetesen egyes esetekben az ilyen fajta támadás során is lehet célirányosan adatokat keresni.

A védelmi szektor esetében ilyen adatok lehetnek például csoportos e-mail-címek, amelyek köthetőek valamilyen hadiipari vállalathoz. Vagy ilyen módszer alkalmazása során nagy méretű adathalászatból származó, nem rendszerezett adatokban olyan e-mail-címeket keresnek, amelyek köthetőek valamilyen kormányzati vagy hatósági szervezethez. Ebben az esetben akár a keresés (szűrés) paramétere lehet az, hogy az e-mail-cím tartalmazzon olyan tartománynevet mint például a gov.xxx.[8] A közelmúltban kitudódott SolarWinds-botrány is példa egy ilyen tevékenységre. A kormányzati intézmények és nagyvállalatok által is előszeretettel és széles körben használt rendszerfelügyeleti programokat fejlesztő SolarWinds 2020. december elején bejelentette, hogy nagyon komplex és megtervezett módon, vélhetően egy állami támogatású hackercsoport rosszindulatú kódot helyezett el az Orion nevű szoftverük frissítésében. Itt fontos hangsúlyozni azt, hogy ez érintette többek között az amerikai energiaügyi minisztérium nukleáris laboratóriumait is.

A másik csoportba pedig olyan szoftverek tartoznak, amelyeket célirányosan alkalmaznak egy adott célpont ellen. Mivel ezek a szoftverek az információs műveletek részét is képezik, ezért a későbbiekben mindenképpen tisztázni kell röviden az információs műveletekben betöltött szerepüket, valamint magukat az információs műveleteket is.

[8] Konkrét országhoz köthető kormányzati weboldal, amely a legfelső szintű tartománynév alá berendelt második szintű tartománynév.

Katonai információs rendszerek

A *malware*-ek definiálása után érdemes röviden megemlíteni, mit is értünk katonai információs rendszereken.

A katonai információs rendszereket alapvetően és meghatározóan az információs térben értelmezzük, ahol „az információs környezet a fizikai, az információs és a kognitív dimenziót magában foglaló információs műveleti tartomány, amelyben a különféle információkezelési és döntési folyamatok zajlanak, illetve az információs képességek megvalósulnak”.[9]

A katonai információs rendszerek alapvető célja, hogy biztosítsa az információáramlást a vezetési és irányítási, valamint a felderítési rendszerek részére, valamint, hogy biztosítsa a katonai műveletek vezetéséhez szükséges információkat. Ezeken a rendszereken strukturálatlan és strukturált adatok cseréje zajlik, valamint már megvalósul az automatizált adatkezelés, az automatizált adatmegosztás és az alkalmazott információmegosztás is.

Egy korszerű haderő számos ilyen rendszert üzemeltet béke-, valamint különleges jogrendi időszakban. Ilyen például a NATO SECRET WAN, a NATO UNCLASSIFIED WAN, illetve a NATO WWW.[10] Az egyik legkomplexebb és legjobb példa a NATO BICES-rendszer,[11] amely számos katonai információs rendszert egyesít. Természetesen ide értendők az egyes haderők által működtetett C4ISR-rendszerek[12] is.

De nemcsak a műveleteket támogató rendszereket kell idesorolni, hanem még idetartoznak a védelmi szektorbeli kormányzati intézmények (védelmi minisztérium szintű szervezetek, katonai felderítő és elhárító szolgálatok) minősített rendszerei, a minősített haditechnika beszállítói, hadigazdasági információs rendszerek (állami érdekeltségű hadigazdasági vállalatok, állami tulajdonú haditechnikai cégek stb.), valamint a haderőt támogató infrastruktúra (energiahordozók szállításáért és elosztásáért felelős rendszerek, logisztikai, egészségügyi hálózatok stb.) működéséért felelős információs rendszerek is.

A legfontosabb és közös jellemzőjük az, hogy ha működésükben hiba lép fel, akkor kiemelt biztonsági kockázatot jelentenek a katonai és nemzetbiztonsági műveleti tevékenységekre, valamit a rutinszerű napi tevékenységre egyaránt.

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

[10] *World Wide Web,* WWW.

[11] BICES: *Battlefield Information Collection and Exploitation System.*

[12] C4ISR: *Command, Control, Communications, Computers, Intelligence, Surveillance, Reconnaissance* (vezetés, ellenőrzés, kommunikáció, számítógépek, hírszerzés, megfigyelés és felderítés).

Ezek a rendszerek napjainkban már korszerű informatikai rendszerek, amelyek rejtjelező eszközökön keresztül továbbítják a vezetési szintek közötti információkat. Ezek az informatikai rendszerek a polgári életben megtalálható rendszerekhez hasonlóan sérülékenyek, egy megfelelő időben és helyben alkalmazott kártékony szoftverrel jelentős károkat lehet okozni bennük. Működésük és céljuk hasonló a klasszikus értelemben vett létfontosságú infrastruktúrához.

Információs műveletek

Az információs hadviselés jelenleg gyorsan fejlődő és egyelőre nehezen definiálható terület. A katonai műveletek tervezése és szervezése során napjainkban egyre nagyobb figyelmet fordítanak erre a területre a katonai felsővezetők és a politikai döntéshozók is. A digitális ökoszisztéma gyors fejlődése és az információs környezet térnyerése következtében a katonai és politikai döntéshozók egyre több lehetőséget látnak az információs műveletekben.

Kiberműveletek

A *malware*-ek alkalmazását az információs műveleteken belül elsősorban a kiberműveletek vonatkozásában érdemes vizsgálni.

Ennek egyik oka, hogy a kiberműveletek egyik eszköze lehet a kártékony szoftver, amelynek segítségével viszonylag gyorsan, költséghatékonyan és célirányosan lehet bénítani, lerombolni, megzavarni az ellenérdekeltségű ország információs rendszereit, és nem mellesleg információt szerezni. Azaz megkímélhető a haderő humánerőforrása, valamint már a kinetikus műveletek megkezdése előtt meg lehet kezdeni az ellenség vezetési rendszerének lerombolását, az ellenség befolyásolását.

Az előbbiekben említett előnyök érvényesítésének eszközei lehetnek a kártékony szoftverek, amelyeket két csoportba lehet osztani: olyan *malware*-ek, amelyek alkalmazása széles spektrumban hatékony, valamint a precíziós csapáshoz előre elkészített kártékony szoftverek.

Malware-ek széles spektrumú alkalmazása (szőnyegbombázás)

Az információs műveletek során végrehajtott kiberműveleteknek több célja lehet. Ezek közé tartozik a megtévesztés, a katonai hálózatok üzemszerű működésének megakadályozása, az informatikai rendszerek ideiglenes megbénítása, valamint ugyanezen rendszerek fizikai rombolása és az információ gyűjtése.

A *malware*-ek széles spektrumú használatát az alábbiak szerint érdemes csoportosítani:

– érzékeny adatok gyűjtése;
– véletlenszerű és nagy méretű rombolás (kiberterrorizmus);
– esetleges későbbi kibertámadás előkészítése.

Érzékeny adatok gyűjtése

Honvédelmi vonatkozásban az információgyűjtés esetében értelemszerűen csak a honvédelemmel kapcsolatos információk a relevánsak. Az adatgyűjtésnek több ismert módszere létezik, viszont katonai viszonylatban a legcélravezetőbb az, ha nagy mennyiségű adatot begyűjtünk az ellenérdekeltségű célpontról, majd a megszerzett adatokat szintetizáljuk és szűrjük. A tisztított adatot a későbbiekben relevancia szerint klaszterekbe rendezzük,[13] vagy az általunk meghatározott struktúrába csoportosítjuk a gyors és hatékony kereshetőség érdekében.

Ennek a folyamatnak a terjedése növekvő tendenciát mutat az elmúlt időszakban. Elég csak felfigyelni arra, hogy erre a tevékenységre szolgáltatási iparág is épült. A kártékony szoftverek üzemeltetését egyes hackercsoportok már szolgáltatják is, és ezt általában a számítógépes támadások végrehajtására szolgáló szoftver és hardver bérbeadásaként is nevesítik (MaaS).[14] A MaaS-szerverek tulajdonosai fizetett hozzáférést biztosítanak egy rosszindulatú programokat terjesztő botnethez.[15] Az ilyen szolgáltatások ügyfeleinek általában személyes fiókot kínálnak, amelyen keresztül irányíthatják a támadást, valamint technikai támogatást nyújtanak részükre. Ez a szolgáltatás kiemelten alkalmas a katonai

[13] A klaszteranalízis során olyan dimenziócsökkentő eljárást alkalmazunk, amely által megpróbáljuk a klasztereket tartalmi relevanciájuk szerint csoportosítani. Az automatizált osztályozást követően viszont ilyenkor sajnos manuálisan kell ellenőrizni a csoport homogenitását.

[14] KasperskyLab: Malware-as-a-service (MaaS).

[15] Más néven zombihálózathoz: olyan számítógépek hálózatához, amelyek úgy szolgálják a hackerek céljait, hogy azok tulajdonosa nem is tud róla.

információs infrastruktúra elleni támadásra is, hiszen a támadó anonim módon csak egy szolgáltatást bérel, amelyet könnyűszerrel testre szabhat.[16] A gyártó emellett műszaki segítséget nyújt a *malware* továbbfejlesztésére. De a leglényegesebb paraméter az anyagiak és az idő ráfordítása a támadásra, hiszen ilyen szolgáltatással költséghatékony és gyors dinamikájú műveleteket lehet végrehajtani.[17]

Ilyen adatszerzésre kiválóan alkalmasak a kiberhírszerzés során használt kártékony szoftverek, amelyeket kémprogramoknak vagy más néven kémszoftvernek *(spyware)* neveznek. Általában az interneten terjedő azon számítógépes programok összességét nevezik így, amelyek célja, hogy a felhasználó tudomása nélkül megszerezzék az érintett informatikai eszközök felhasználójának érzékeny adatait.

A legtöbb *spyware* a felhasználó tudomása nélkül, valamilyen megtévesztésen alapuló módszerrel kerül bele az informatikai rendszerbe. A megtévesztés egyik módja, hogy hasznos, a felhasználó számára releváns alkalmazásba kerül be.[18] A másik módszer a böngészőn keresztüli bejutás. Ebben az esetben a felhasználó egy már megfertőzött internetes felületre navigál,[19] majd lefut a fertőző kódsor, és a kártékony program a rendszerre települ.

Adattípusok

A széles spektrumú adatgyűjtés a katonai rendszerek vonatkozásában az esetek túlnyomó többségében az alábbi információkra korlátozódik:

- hadiipari és hadigazdasági vállalkozások üzleti adatai;
- hadiipari beszállítók érzékeny adatai;
- haditechnikai vállalatok műszaki megoldásai;
- katonai létfontosságú rendszerek sérülékenysége;
- létfontosságú információs infrastruktúra rendszerelemeinek sérülékenysége;

[16] Dark net C&C vezérlőpult, késleltetett indítás, *delayed encryption, mutex,* feladatkezelő/*registry editor disabler, UAC bypass, desktop wallpaper change, offline encryption, unkillable process.*

[17] EnigmaSoft: *'Malware-as-a-service' Market Booms as Prices for Malware and Botnet Creation Tools Decline.*

[18] Például a Gator (GAIN).

[19] Például az Internet Optimizer vagy más néven DyFuCA.

- a haderő személyi állományával kapcsolatos adatok (személyes vagy akár biometrikus);
- technológiai és ipari vállalatok érzékeny adatai;
- kormányzati és hatósági rendszerek adatai;
- valamint a haderőt érintő ipari vezérlő rendszerekkel kapcsolatos információk, mint például nukleáris erőművekben működő vezérlő és irányító rendszerek adatai, hadiipari gyártók vállalatirányítási rendszerei, közfeladatot ellátó állami tulajdonú gazdasági társaságok.

Természetesen ezen rendszerek a fent felsorolt adatok mellett számos olyan információt gyűjtenek, amely közvetve érinti a haderőt, és nem alkalmas arra, hogy egy információs rendszert megbénítson.

A *malware*-ek több esetben véletlenszerűen katonai információs rendszereket kiszolgáló informatikai infrastruktúrát is rombolhatnak. Ennek oka, hogy a nem precíziós *malware*-ek széles körben terjednek. Az elmúlt évek során több esetben történt meg az, hogy ipari rendszerekbe vagy létfontosságú infrastruktúrák egyes rendszereibe kerültek be *malware*-ek. Ezek nagy része nem az ipari rendszerek elleni célzott támadáshoz kifejlesztett *malware* volt, hanem csak általános kártevő, amely bejutott az ipari vezérlő rendszerbe (*Industrial Control System:* ICS).[20] Közöttük legnagyobb számban a gyorsan terjedő *malware*-családok képviselői találhatóak meg. Ilyen például a szaúd-arábiai olajfinomítók elleni kibertámadásról híressé vált[21] Triton *malware,*[22] amelyre a későbbiekben Triton/TriSIS néven hivatkoztak. Ritkábban a különböző trójaiak is jelen lehetnek ezekben a rendszerekben, amelyek viszont már hozzáférést is adhatnak a támadóknak a megtámadott ICS-rendszerhez. Az utóbbi *malware*-ek, bár nem célzott támadások eszközei, mégis jelentős károkat okozhatnak az ipari rendszerekben.

A Dragos Inc. tanulmánya szerint éves szinten megközelítőleg 3000 ipari rendszerben tűnhetnek fel klasszikus IT-*malware*-ekre visszavezethető, nem célzott támadásból származó fertőzések.[23]

[20] Malware in Modern ICS. Understanding Impact While Avoiding Hype. *POWER,* 2017. május 1.

[21] Az amerikai NSA, az FBI, a DHS és a DARPA vizsgálatokat folytatott, mivel meg nem erősített információk szerint a támadók célja nem csupán az olajipari létesítmény működésének megbénítása volt, hanem fizikai pusztítást akartak előidézni a biztonsági rendszer kompromittálásával.

[22] Davide Franzetti: Oil & Gas Cybersecurity and Process Safety Converge Thanks to TRITON. *Security Boulevard,* 2019. február 26.

[23] Dragos Inc.: *Industrial Control System Threats.* 2019. február 14.

Az adatgyűjtő módszerek célja

A *malware*-ekkel folytatott széles körű adatgyűjtés célja valamilyen előny (gazdasági, technológiai, döntéstámogató) költséghatékony és gyors megszerzése. A jelenlegi tendenciák szerint több esetet kell megkülönböztetni. Célszerű elkülöníteni a támadó entitást, a megszerzendő információkat, valamint a támadás célját. Napjainkban az autokratikus országok esetében jellemzően valamilyen haditechnikai információ, érzékeny honvédelmi adat, harcértékadat megszerzése a cél. Ezen információk részletes ismerete szükséges ahhoz, hogy a környező országokkal szemben műveleti előnyt szerezzen az érintett ország.

Erre talán a legjobb példa az észak-koreai kormány stratégiája. A nemzetközi sajtóban szinte folyamatosan egymást követik az olyan cikkek, ahol Phenjant globális méretű kiberhírszerző kampányokkal vádolják meg. Ahogy számos autokratikus kormány proxyfelhasználókat használ, Észak-Korea esetében is számos, *malware*-ekkel végrehajtott támadással hozták összefüggésbe a rezsimhez tartozónak gondolt csoportokat.[24]

Ha csak két évet vizsgálunk is, az észak-koreai kormányhoz köthetően számos hír jelent meg a sajtóban.[25] Az országot nemzetközi import- és exportkorlátozások sújtják. Korea gazdasági helyzetét mutatja az is, hogy Kim Dzsongun vezető 2021 júniusában beismerte, az ország élelmezési gondokkal küzd.[26] A kieső gazdasági forrásokat a rezsim a viszonylag fejlett, de mindenképpen globálisan jelen lévő kiberképességeivel próbálja meg pótolni. Azaz például globálisan alkalmaz kriptopénzbányász-szoftvereket illegálisan. A feltelepült *malware*-ek több milliárd amerikai dollár értékű károkat okoznak a kriptopénz-kereskedelemben.[27]

Az észak-koreai állam által támogatott Lazarus csoport 2020-ban feltételezhetően megközelítőleg 12 országban folytatott kiberhírszerző tevékenységet katonai beszállítók irányában. A KasperskyLab kutatói[28] szerint a kiberhírszerző

[24] A támadók előnye, hogy jogilag bonyolult nekik tulajdonítani a támadást, és minden ország másmás megfontolások alapján dönti el, hogy diplomáciailag felvállalja-e az elkövetők megnevezését. A célország szempontjából hátrány, hogy teljes biztonsággal aligha lehet megnevezni az elkövetőt, és nehéz ellenlépéseket is tenni, akár technikailag, akár diplomáciailag.

[25] Vyacheslav Kopeytsev – Seongsu Park: *KasperskyLab ICS CERT Lazarus targets defense industry with ThreatNeedle*. Kaspersky ICS CERT, 2021. február 25.

[26] Lin Yoon: Kim Jong Un Acknowledges Food Crisis in North Korea. *Hrv.org,* 2021. június 17.

[27] Dan Mangan: North Korean Hackers Charged in Massive Cryptocurrency Theft Scheme. *CNBC,* 2021. február 17.

[28] Kopeytsev–Park (2021): i. m.

tevékenységet adathalász levelekkel kezdték meg. A levelek túlnyomó többségének témája vagy a Covid–19-járvánnyal kapcsolatban érkezett, vagy a célba vett vállalat munkatársainak ajánlottak benne hamis munkalehetőséget a védelmi szektor területén.[29] Ezekben a levelekben a Microsoft Word makrójának segítségével az elkövetők telepíteni tudták az áldozatok informatikai eszközére a ThreatNeedle elnevezésű *malware*-t. A kártékony szoftver ezt követően hátsóajtó-alkalmazást telepített, amelynek a segítségével a támadók képesek adatokat megszerezni a megfertőzött informatikai eszközökről.

Másik eset: a Reuters londoni székhelyű világhírügynökség 2020. áprilisi cikke szerint a kínai kormányhoz köthető hackercsoport hónapokon át végzett kiberhírszerző tevékenységet amerikai hadiipari vállalatok ellen. A támadás során a virtuális magánhálózatokat (*virtual private network:* VPN) vették célba, és ezen rendszereken keresztül szerezték meg az érzékeny adatokat. Ezekre az incidensekre a *Cybersecurity and Infrastructure Security Agency* (USA CISA) is felhívta a figyelmet, miszerint a támadók a VPN-hálózatokba juttathatják a SUPERNOVA elnevezésű kártékony alkalmazást.[30]

Precíziós malware alkalmazása

Az ipari vezérlőrendszerek (*Industrial control systems:* ICS) kiberbiztonsága egyre meghatározóbbá válik a folyamatosan fejlődő és automatizálódó digitális ökoszisztémában. A létfontosságú infrastruktúrák megfelelő működése meghatározóan függ az ICS-rendszerek kiberbiztonságától. Ezek a rendszerek számos elemből állnak, idetartoznak a SCADA-rendszerek *(Supervisory Control and Data Acquisition),* a HMI-k *(Human-Machine Interface),* a programozható logikai vezérlők (*Programmable Logic Controller:* PLC), a távoli diagnosztikai és karbantartó eszközök, az ipari szenzorok.

Az informatikai hadviselés hatékony és sikeres alkalmazásának több előnye is van. Viszonylag kevés anyagi ráfordítással és az élő erő megkímélésével súlyosabb károkat lehet okozni az ellenérdekeltségű fél vezetési-irányítási rendszerében.

[29] Derek B. Johnson: Threatneedle Malware Tied to Year-Long North Korean Espionage Campaign Against Global Defense Industry. *Scmagazine,* 2021. február 25.

[30] Justin Katz: Cisa Issues Warning on Exploited VPN Flaw. *GCN.com,* 2021. április 23.

Más esetben békeidőszakban lehet a létfontosságú infrastruktúrákban kártékony szoftverekkel jelentős fizikai károkat okozni. Ezeknek az incidenseknek kiemelt jelentősége van, hiszen ezek a támadások nem kizárólag katonai létfontosságú rendszerelemek ellen irányulnak, hanem a polgári lakosságot is érinthetik. Emellett a létfontosságú rendszerek interdiszciplináris jellege miatt több rendszert is érinthet a támadás.

A precíziós *malware*-ek hatékonyan alkalmazhatóak katonai információs rendszereket kiszolgáló infrastruktúra-vezérlő rendszerek ellen. Ezen *malware*-ek egy részét célirányosan erre a feladatra készítik fel.

Az ICS-rendszerek ellen készült *malware*-ek száma viszonylag alacsony, a legjelentősebb ezek közül a Stuxnet, a Havex és a BlackEnergy2.

Természetesen azért vannak kivételek is, az ukrán áramszolgáltatók elleni 2015. decemberi támadás megmutatta azt is, hogy egy támadónak nem szükséges magas szinten specializált *malware*-t használni ahhoz, hogy súlyos üzemzavart tudjon előidézni komplexebb ipari vezérlő rendszerben. Az ICS-rendszerek ellen készített *malware*-ek egy kis csoportját a támadók olyan ICS-alkalmazásnak álcázzák, amely hivatalosan is használatban lévő vezérlő szoftver. Egy ilyen *malware* akkor hatékony, ha mögötte állami szereplő áll, ami biztosítja a szakértőket, a katonai és mérnöki tanácsadókat. Emellett rendelkezésre áll a megfelelő teszt- és laborkörnyezet, valamint a megfelelő anyagi források. A szoftver esetleges célba juttatását pedig titkosszolgálati műveleti tevékenység biztosítja. Ha az előbbiekben említett feltételek együttesen rendelkezésre állnak, akkor nagy eséllyel már számottevő károkat lehet okozni.

Létfontosságú rendszerek

A precíziós *malware*-ekkel végrehajtott támadások kiemelt célpontjai katonai viszonylatban a katonai létfontosságú rendszerelemek lehetnek. Interdiszciplináris jellegük miatt ezek a rendszerek kiemelt kockázatot jelentenek.

Fontos megjegyezni, hogy ez a probléma nem új keletű. Hasonló jelentősebb esemény bekövetkeztének lehetőségét és forgatókönyvét kifejtették a 2010-ben megjelent *Digitális Mohács* című tanulmányban is.[31] A létfontosságú

[31] Kovács László – Krasznay Csaba: Digitális Mohács. Egy kibertámadási forgatókönyv Magyarország ellen. *Nemzet és Biztonság,* 3. (2010), 1. 44–56.

infrastruktúra és a kapcsolódó információs rendszerek viszonylatába a folytatás ad részletes betekintést.[32] Ezeket az előzőekben részletesen bemutattuk.

A honvédelemmel kapcsolatba hozható létfontosságú rendszerek közül is kiemelkedően fontosak például az energetikai, valamint a fosszilis energiahordozók szállítását és elosztását biztosító információs rendszerek, esetlegesen a fegyverirányítási, illetve az előre jelző rendszerek. Ezeknek a rendszereknek az üzemszerű működéstől való eltérése különleges jogrendi, valamint békeidőszakban is jelentős problémát okozhat. Ennek oka az, hogy „[a]mennyiben ezek közül a rendszerek közül néhány kiesik, vagy működésében sérül akár időlegesen is, az beláthatatlan következményekkel jár a társadalom említett funkcióinak ellátásában. […] hogy egy-egy rendszer vagy rendszerelem kiesésének másik rendszerre gyakorolt valamennyi hatása csak nagyon nehezen jelezhető előre teljes bizonyossággal".[33]

Napjainkban erre az egyik legjobb példa a Colonial Pipeline-incidens. Egy zsaroló vírussal végrehajtott kibertámadás miatt egész üzemanyagvezeték-hálózatát lezárta a Colonial Pipeline vállalat. Ez a fosszilisenergia-hordozó rendszer az Amerikai Egyesült Államok keleti partvidékének közel felét látja el vezetékein keresztül.[34] A zsaroló vírus működése és az okozott gazdasági károk elemzése nélkül is látható, hogy egy ilyen *malware*-típus komoly károkat tud okozni, főleg, hogy a hajtóanyag, a benzin és a gázolaj kiesése jelentősen hátráltathat egy katonai műveletet. Így megállapítható, hogy a zsaroló vírusokkal is hatékonyan lehet akadályozni egy támadó katonai műveletet vagy a haderő logisztikai rendszerét. Ebben az esetben persze nem beszélhetünk szó szerinti pusztításról, de az is egyértelmű, hogy precízen kivitelezett támadás zajlott le, hiszen emiatt az üzemanyag-szállítás az egész hálózaton leállt, és a vállalat informatikai rendszerét is részben le kellett kapcsolni.[35.]

A Colonial Pipeline esetében ráadásul az információs rendszerben közvetett károk is keletkeztek, mivel nemcsak támadásról volt szó, hanem nagy méretű

[32] Kovács László – Krasznay Csaba: Digitális Mohács 2.0: kibertámadások és kibervédelem a szakértők szerint. *Nemzet és Biztonság,* 10. (2017), 1. 3–16.

[33] Kovács László: *A kibertér védelme.* Budapest, Dialóg Campus, 2018. 212.

[34] Megközelítőleg 9000 kilométeres vezetékhálózatán benzint, gázolajat, repülőgép-hajtóanyagot és egyéb finomított kőolajszármazékokat szállít, napi mintegy 2,5 millió hordó mennyiségben.

[35] Andrew Ginter: Ransomware Targets Largest Gasoline Pipeline in USA. *Waterfall,* 2021. május 10.

adatlopásról is. Amint azt már említettem, az információs rendszerek elleni támadásnak több területet is érintő, rendszereken átívelő hatása van.[36]

A támadók jelezték közleményükben, hogy az eltulajdonított adatok között a vállalat szállításainak teljes listája, köztük a hadászati célúak is szerepeltek, amelyekből következtetni lehet az Amerikai Egyesült Államok műveleti képességeire is (katonai logisztika). A gazdasági károk szintén jelentősek voltak, hiszen az Amerikai Egyesült Államok adminisztrációja a támadás után vészhelyzeti rendelkezést adott ki, amely engedélyezi, hogy a kőolajszármazék-szállításban részt vevő logisztikusok többet dolgozzanak a normális üzemszerű időnél, a szállítás zavartalanságának biztosítása érdekében.[37] A vezetékrendszer nagyságából arra is lehet következtetni, mekkora gazdasági kár érte napi szinten a vállalatot. A támadás és a leállás ráadásul nemzetközi viszonylatban is jelentős kiesést jelentett, mert a Brent olaj[38] és más termékek ára emelkedni kezdett, ahogy a szolgáltatók igyekeztek más forrásból beszerezni a kiesést.

A támadások 2021-ben egyre nagyobb számban fordulnak elő. A közlekedési rendszerek szintén ilyen támadás alatt állhatnak, és egyes esetekben az elkövetők nem kiberbűnözők, hanem államilag finanszírozott csoportok. 2021. július 10-ei sajtóinformációk szerint például az iráni közlekedési minisztérium informatikai rendszerét kibertámadás érte. A támadás során az iráni vasúthálózat forgalomfigyelő rendszereleme nem működött üzemszerűen, valamint a vasúti forgalomban is fennakadások jelentkeztek. Az Iranian Students News Agency (ISNA) szerint viszont nem történt olyan méretű támadás, amely befolyásolta volna a személy- és teherszállítást, valamint a nemzetközi vasúti forgalmat. Ezzel szemben a Fars hírügynökség képein látható, hogy a vasúti menetrendkijelzőkön számos késést mutatnak.[39] Az eset információs műveletekhez való tartozását jelzi, hogy a késések alatti telefonszám állítólag Irán egyházi vezetőjének, az ajatollahnak a magántelefonszáma volt.

[36] Joe Panettieri: Colonial Pipeline Ransomware Attack Timeline and Status Updates. *MSSP Alert,* 2021. június 7.

[37] The White House: *Remarks by President Biden on the Colonial Pipeline Incident* (2021. május 13.).

[38] Globálisan megközelítőleg 200 féle kőolaj létezik, ezek közül egyes fajták az úgynevezett *„marker"* olajok. Ezek egyike a Brent-típusú kőolaj, amely az északi-tengeri kőolajnak felel meg.

[39] Cyber-Attack' Hits Iran's Transport Ministry and Railways. *The Guardian,* 2021. július 11.

SCADA

A létfontosságú infrastruktúrákat vezérlő rendszerek már több esetben estek áldozatul *malware*-ekkel végrehajtott támadásoknak. Az ilyen típusú támadások jellemzője, hogy magasan képzett programozók hajtják végre, akik jártasak a PLC-programozásban, valamint jól ismerik az ICT-rendszereket[40] és a támadásban érintett iparágat.

A támadások célja, hogy a rendszert üzemszerű működésétől eltérítsék, vagy olyan paramétereket adjanak meg az egyes üzemi eszközöknek, amelyek következtében fizikai károsodás éri a hálózatot vagy magát az eszközt. Például téves adatokat adnak meg a vezérlőrendszernek, vagy a szenzorok alapértékeit állítják át.

A SCADA esetében is meg kell jegyezni azt, hogy ezek a rendszerek több technológiát ötvöznek. Az ilyen rendszerek sokkal sérülékenyebbek a *malware*-ekkel szemben, hiszen a támadóknak lehetőségük van több ponton is bejutni. Ilyen lehet az ICT-sérülékenység, a tévesen beállított protokoll vagy a napjainkban egyre jobban terjedő szolgáltatási láncba beágyazott támadás is, ahogy azt a korábbiakban olvashattuk. Mivel az információs és kommunikációs technológia komplex, globálisan elosztott és összekapcsolt ellátásilánc-rendszereken alapul, ezért

> „az ICT-ellátásilánc-kockázatok magukban foglalhatják hamisítások beillesztését, jogosulatlan gyártást, hamisítást, lopást, rosszindulatú szoftverek és hardverek beillesztését, valamint az ICT-ellátási lánc rossz gyártási és fejlesztési gyakorlatait. Ezek a kockázatok azzal járnak, hogy a szervezet rálátása és megértése csökken az általuk megszerzett technológiák fejlesztésének, integrálásának és bevezetésének módjáról."[41]

Egy cikk 2009-ben már arra hívta fel a figyelmet, hogy a SCADA-rendszerek távközlési összeköttetése, valamint hálózatba szervezése súlyos biztonsági kockázatot jelent az egész infrastruktúrára nézve, valamint hogy a klasszikus értelemben vett ICT-védelmi megoldások egyáltalán nem védenek a speciálisan SCADA-ra tervezett *malware*-támadások ellen. Például egy SCADA-specifikus *malware* ellen az ICT-védelmi eljárások teljesen hatástalanok. A cikk szerint

[40] Information Communication Technologies.

[41] Deák Veronika (szerk.): *Kibertéri fenyegetések. Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára*. Budapest, Nemzeti Közszolgálati Egyetem, 2020. 55.

a kísérleti tesztek alapján a rosszindulatú programok képesek voltak teljesen kijátszani a hagyományos biztonsági mechanizmusokat. A fertőzés *ad hoc* jellege miatt a program hatékonyan megfertőzte a jelentősebb szenzorokat és jelző egységeket.[42]

Hadiipari kémkedés

Míg egyes kártékony szoftvereket arra készítenek fel, hogy látványos – esetleg sajtóvisszhangot keltő – fizikai pusztítást okozzanak, addig más szoftvereket amiatt hoznak létre, hogy a megfertőzött rendszerben megbújva hosszabb ideig adatot szerezzenek. A védelmi szektor viszonylatában ezek a szoftverek nagy biztonsági kockázatot jelentenek. Az esetek többségében ezekkel a szoftverekkel hadiipari beszállítókat, honvédelmi érdekeltségű fejlesztő intézeteket céloznak meg. Itt a cél a hosszan tartó rejtett jelenlét és a maximális adatkinyerés. Kiemelten olyan technológiát érintő dokumentumok eltulajdonításáról van szó, amelyek valamilyen katonai célú fejlesztést is érintenek. Hiszen sokkal gyorsabb és költséghatékonyabb ellopni egy katonai eszköz dokumentációját és terveit, mint kifejleszteni ugyanezt.

Emellett nemcsak a fejlesztés területén jelentősek ezek az információk, hanem védelmi területen is. Hiszen egy offenzív technológiáról előzetesen megszerzett információk nagyban segítik a felkészülést a technológia ellen, ha már rendelkezünk előzetesen ellopott tervezetekkel. A FireEye 2016-os elemzése is rámutat arra, hogy az államilag finanszírozott hackercsoportok is ezeket az információkat keresik, amivel elsősorban az állam által működtetett védelmi rendszer fejlesztését tudják támogatni.

Globális viszonylatban – sajtóinformációk és internetbiztonsági vállalatok szerint – a kínai kormányhoz köthető hackercsoportok jelentik ezen a területen a legnagyobb kockázatot. Az ellopott dokumentációkat a haderőfejlesztés során használja fel a kormány, valamint ezek a támadások az úgynevezett előzetes felderítő tevékenység részét is képzik, amelyeket a későbbiekben továbbfejlesztenek, és még több érzékeny adatot tudnak eltulajdonítani.

[42] Igor Nai Fovino et al.: An Experimental Investigation of Malware Attacks on Scada Systems. *International Journal of Critical Infrastructure Protection,* 2. (2009), 4. 139–145.

A védelmi ipari szektor információs rendszereit számos kártevő veszi célba. A teljesség igénye nélkül a legjelentősebb védelmi szektort érintő *malware*-ek: a GhOst RAT, a PcClient, a ZXShell, az NS01, a WITCHCOVEN.[43]

A védelmi szektor információs rendszerei napjainkban is támadás alatt állnak.[44] A Mandiant jelentése szerint ezt a szektort 2020-ban nemcsak a kínai kormány, hanem az észak-koreai vezetés által finanszírozott csoportok is célba vették. Céljuk, hogy az Amerikai Egyesült Államok védelmi és légügyi információs rendszeréből érzékeny adatokat tulajdonítsanak el.[45]

Dél-koreai sajtóinformációk szerint feltételezhetően észak-koreai elkövetők a Korea Aerospace Industries (KAI) repülőgépipari vállalat informatikai rendszeréből eltulajdonították a KF-21 (HAWK)[46] típusú vadászrepülőgép minősített tervét.[47] A Daewoo vállalatot hasonló kár érte az elmúlt időszakban, amely során feltehetően észak-koreai hackerek érzékeny adatokat távolítottak el a vállalat szervereiről.

Kitekintés

A fokozódó kibertámadások és a kiberbűnözői tevékenység Európában és globálisan is – párhuzamosan a katonai incidensekkel – egyre gyakoribbá és egyre komplexebbé válik. Ez a tendencia várhatóan tovább fog erősödni, mivel 2024-re megközelítőleg 22 milliárd készülék kapcsolódik majd az internetre (*Internet of Things:* IoT).

Ezeknek a támadásoknak egy része közvetlenül vagy közvetve is érinteni fogja a katonai információs hálózatokat. Nem beszélve arról, hogy ezen információs hálózatok egy része a jövőben az IoT-eszközökre is épülhet. Hiszen a polgári technológiák is megjelennek a katonai technológiák között, például a DIoT- eszközök *(Defence Internet of Things)* csoportjába tartozó WINLANS-rendszer[48] a városi harcászati rendszereket támogatja majd a későbbiekben.[49]

[43] FireEye: *Cyber Threats To The Aerospace And Defense Industries.* 2016

[44] FireEye: *FireEye-Mandiant Special report: M-Trends 2021.* 2021.

[45] CuteLoop-kampány.

[46] Ismertebb nevén KF-21 Boramae.

[47] Elizabeth Shim: Maker of South Korea's Kf-21 Indigenous Fighter Hacked. *UPI.com*, 2021. június 30.

[48] WINLANS: Wireless Sensor Networks for urban Local Areas Surveillance.

[49] Ignacio Montiel-Sánchez: *Defence Internet of Things (DIOT).* European Defence Matters, (é. n.).

A hálózati és információs rendszerek biztonságáról szóló európai irányelv 2016-ban lépett életbe, és az első olyan, unió területén alkalmazandó jogalkotási intézkedést jelenti, amelynek célja, hogy elmélyítse a tagállamok közötti kiberbiztonsági tevékenységekre vonatkozó együttműködést a létfontosságú rendszerek területén.

Az irányelv meghatározza az alapvető szolgáltatásokat nyújtó gazdasági szereplők és a digitális szolgáltatók biztonsági kötelezettségeit. Az Európai Bizottság 2020 decemberében javaslatot tett a 2016-os irányelv helyébe lépő módosított kiberbiztonsági irányelvre.[50] Az új szabályok szerint szigorítani fogják a vállalkozások biztonsági kötelezettségeit, fokozzák az ellátási láncok biztonságát, szigorúbb felügyeleti intézkedéseket fognak bevezetni a nemzeti hatóságok számára, tovább fokozzák majd az információmegosztást és az együttműködést. A javaslatot a fejezet írásának idején a Tanács tárgyalja.

Az Európai Bizottság és az Európai Külügyi Szolgálat (EKSZ) új uniós kiberbiztonsági stratégiát terjesztett elő 2020 decemberében. A cél, hogy megerősödjön az európai információs infrastruktúra a kiberfenyegetésekkel szemben. Az új stratégia konkrét javaslatokat tartalmaz szabályozási, beruházási és szakpolitikai eszközök bevezetésére. A tanúsítás[51] alapvető szerepet játszik az IKT-termékek és -szolgáltatások, valamint -folyamatok magas szintű kiberbiztonságának biztosításában.[52]

Az Európai Unió és tagállamai határozottan egy olyan nyitott és stabil, valamint biztonságos kibertér létrejöttét támogatják, amelyben megvalósul az emberi jogok, az alapvető szabadságok és a jogállamiság tiszteletben tartása. Emellett a társadalmi stabilitást, a gazdasági növekedést, a jólétet és a szabad és demokratikus társadalmak integritását kívánják elősegíteni.

Az EU nagy erőfeszítéseket tesz annak érdekében, hogy megvédje magát az ellenérdekeltségű országokból érkező kibertámadásokkal szemben. Erre jó lehetőséget nyújtanak a közös uniós intézkedések, azaz a kiberdiplomácia eszköztára, amelynek eleme többek között a diplomáciai együttműködés és párbeszéd, a kibertámadások megelőzését célzó intézkedések, valamint ezek szankcionálása. Az Európai Bizottság és az EKSZ által 2020 decemberében elfogadott

[50] NIS 2 irányelv.

[51] European Commission: *Shaping Europe's Digital Future. The EU Cybersecurity Certification Framework*. 2021.

[52] Az egyes uniós országok jelenleg más-más biztonsági tanúsítási rendszereket alkalmaznak, és ez a piac széttöredezettségéhez és szabályozási akadályokhoz vezet. Európai Tanács: *Kiberbiztonság: hogyan kezeli az EU a kiberfenyegetéseket?* 2021.

uniós kiberbiztonsági stratégia megerősíti a kibertámadásokra adandó uniós diplomáciai válaszintézkedéseket.

A Tanács 2019 májusában létrehozta a jogszabályi keretet, amely lehetővé teszi az unió számára, hogy célzott szankciókat vezessen be az olyan kibertámadásoktól való elrettentés és az azokra való reagálás érdekében, amelyek kívülről érkező fenyegetést jelentenek a tagállamokra. Ez lehetővé teszi, hogy szankciókat vessen ki olyan támadókra, akik kibertámadásokért felelősek, akik esetleg pénzügyi, technikai vagy anyagi támogatást nyújtanak ilyen támadásokhoz, vagy akik azokban egyéb módokon közreműködnek. Itt számos kérdés is felmerülhet, például, hogy a támadókat hogyan és melyik szervezet azonosítja hivatalosan, illetve hogyan bizonyítható a tényleges pénzügyi támogatás a gyakorlatban.

A kibertér védelmével kapcsolatos uniós együttműködés az Európai Védelmi Ügynökség (*European Defence Agency:* EDA) tevékenységeinek keretében, az Európai Uniós Kiberbiztonsági Ügynökség (*European Union Agency for Cybersecurity:* ENISA) és a European Police Office (EUROPOL) részvételével zajlik. Az EDA segítséget nyújt a tagállamoknak ahhoz, hogy szakképzett katonai kibervédelmi személyzettel rendelkezzenek, és biztosítja a proaktív és reaktív kibervédelmi technológia meglétét.[53]

A 2020 decemberében a Bizottság és az EKSZ által elfogadott uniós kiberbiztonsági stratégia a következőket kívánja megerősíteni:

– a kibervédelem koordinálása,
– az együttműködés és a kibervédelmi képességek kiépítése.

Összefoglalás

A szőnyegbombázás-szerű kibertámadások és a precíziós *malware*-ek elleni védekezés fokozása ma már nemcsak a polgári vagy kereskedelmi/ipari szektort érinti, hanem jelentős kockázati tényezőként jelenik meg a katonai információs rendszerek vonatkozásában is.

Emiatt szükségessé vált a kiberreziliencia növelése, a kiberbűnözés elleni fellépés, a kiberdiplomáciai tevékenység fokozása. Emellett prioritássá vált a kibervédelem folyamatos erősítése, valamint a meglévő rendszerek revíziója is. Az előbbiekben említett feladatok mellett fokozni kell a kutatást és az inno-

[53] EDA: *Cyber Defence Summary: Training & Exercises.* 2021.

vációs tevékenységet, valamint kiemelten kell kezelni a létfontosságú infrastruktúra védelmét.

Véleményem szerint a katonai információs rendszerek vonatkozásában jellemzően a precíziós *malware*-ekkel végrehajtott támadások lesznek a mérvadók az elkövetkező években. Mivel maguk a katonai információs rendszerek is egyre több elemből és alrendszerből állnak majd, valamint ezek komplex és összekapcsolt hálózatokat alkotnak, csak olyan kibertámadások lehetnek hatékonyak, amelyek olyan *malware*-eket használnak, amelyeket a célba vett rendszerre írtak.

Irodalomjegyzék

Deák Veronika (szerk.): *Kibertéri fenyegetések. Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára*. Budapest, Nemzeti Közszolgálati Egyetem, 2020. Online: https://bit.ly/3I7EeVN

Dragos Inc.: *Industrial Control System Threats.* 2019. február 14. Online: www.dragos.com/resource/dragos-releases-industrial-control-systems-2018-year-in-review-reports/

EDA: *Cyber Defence Summary: Training & Exercises.* 2021. Online: https://eda.europa.eu/what-we-do/all-activities/activities-search/cyber-defence

EnigmaSoft: *'Malware-as-a-service' Market Booms as Prices for Malware and Botnet Creation Tools Decline.* Online: www.enigmasoftware.com/malware-service-market-booms-prices-malware-botnet-tools-decline/

Európai Tanács: *Kiberbiztonság: hogyan kezeli az EU a kiberfenyegetéseket?* 2021. Online: www.consilium.europa.eu/hu/policies/cybersecurity/

European Commission: *Shaping Europe's Digital Future. The EU Cybersecurity Certification Framework.* 2021. Online: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies

FireEye: *Cyber Threats to The Aerospace And Defense Industries.* 2016. Online: www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/ib-aerospace.pdf

FireEye: *FireEye-Mandiant Special Report: M-Trends 2021.* 2021. Online: https://content.fireeye.com/m-trends/rpt-m-trends-2021

Fovino, Igor Nai et al.: An Experimental Investigation of Malware Attacks on Scada Systems. *International Journal of Critical Infrastructure Protection,* 2. (2009), 4. 139–145. Online: https://doi.org/10.1016/j.ijcip.2009.10.001

Franzetti, Davide: Oil & Gas Cybersecurity and Process Safety Converge Thanks to TRITON. *Security Boulevard,* 2019. február 26. Online: https://securityboulevard.com/2019/02/oil-gas-cybersecurity-and-process-safety-converge-thanks-to-triton/

Ginter, Andrew: Ransomware Targets Largest Gasoline Pipeline in USA. *Waterfall,* 2021. május 10. Online: https://waterfall-security.com/ransomware-targets-largest-gasoline-pipeline-usa/

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

Johnson, Derek B.: Threatneedle Malware Tied to Year-Long North Korean Espionage Campaign Against Global Defense Industry. *Scmagazine,* 2021. február 25. Online: www.scmagazine.com/news/apt/threatneedle-malware-tied-to-year-long-north-korean-espionage-campaign-against-global-defense-industry

KasperskyLab: Malware-as-a-service (MaaS). Online: https://encyclopedia.kaspersky.com/glossary/malware-as-a-service-maas/

Katz, Justin: Cisa Issues Warning on Exploited VPN Flaw. *GCN.com,* 2021. április 23. Online: https://gcn.com/articles/2021/04/23/cisa-supernova.aspx

Kopeytsev, Vyacheslav – Seongsu Park: *KasperskyLab ICS CERT Lazarus Targets Defense Industry with ThreatNeedle.* Kaspersky ICS CERT, 2021. február 25. Online: https://ics-cert.kaspersky.com/media/Kaspersky-ICS-CERT-Lazarus-targets-defense-industry-with-Threatneedle-En.pdf

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

Kovács László – Krasznay Csaba: Digitális Mohács. Egy kibertámadási forgatókönyv Magyarország ellen. *Nemzet és Biztonság,* 3. (2010), 1. 44–56. Online: www.nemzetesbiztonsag.hu/cikkek/kovacs_laszlo__krasznay_csaba-digitalis_mohacs_.pdf

Kovács László – Krasznay Csaba: Digitális Mohács 2.0: kibertámadások és kibervédelem a szakértők szerint. *Nemzet és Biztonság,* 10. (2017), 1. 3–16. Online: https://folyoirat.ludovika.hu/index.php/neb/article/view/3780

Kramer, Simon – Julian C. Bradfield: A General Definition of Malware. *Journal in Computer Virology,* (2010), 6. 105–114. Online: https://doi.org/10.1007/s11416-009-0137-1

Malware in Modern ICS. Understanding Impact While Avoiding Hype. *Power,* 2017. május 1. Online: www.powermag.com/malware-in-modern-ics-understanding-impact-while-avoiding-hype/

Mangan, Dan: North Korean Hackers Charged in Massive Cryptocurrency Theft Scheme. *CNBC,* 2021. február 17. Online: www.cnbc.com/2021/02/17/north-korean-hackers-charged-in-massive-cryptocurrency-theft-scheme.html

Montiel-Sánchez, Ignacio: *Defence Internet of Things (DIOT).* European Defence Matters, (é. n.). Online: https://eda.europa.eu/webzine/issue14/cover-story/defence-internet-of-things-(diot)

NATO e-Library: *Wales Summit Declaration, Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Wales.* 2014.

NATO e-Library: *Warsaw Summit Communiqué: Issued by the Heads of State and Government Participating in the Meeting of the North Atlantic Council in Warsaw.* 2016.

Panettieri, Joe: Colonial Pipeline Ransomware Attack Timeline and Status Updates. *MSSP Alert,* 2021. június 7. Online: www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/colonial-pipeline-investigation/

Shim, Elizabeth: Maker of South Korea's Kf-21 Indigenous Fighter Hacked. *UPI.com*, 2021. június 30. Online: www.upi.com/Top_News/World-News/2021/06/30/skorea-South-Korea-KAI-aerospace-hack/5591625059379/

Cyber-Attack' Hits Iran's Transport Ministry and Railways. *The Guardian,* 2021. július 11. Online: www.theguardian.com/world/2021/jul/11/cyber-attack-hits-irans-transport-ministry-and-railways

The White House: *Remarks by President Biden on the Colonial Pipeline Incident* (2021. május 13.). Online: www.whitehouse.gov/briefing-room/speeches-remarks/2021/05/13/remarks-by-president-biden-on-the-colonial-pipeline-incident/

Yoon, Lin: Kim Jong Un Acknowledges Food Crisis in North Korea. *Hrv.org,* 2021. június 17. Online: www.hrw.org/news/2021/06/17/kim-jong-un-acknowledges-food-crisis-north-korea

10. fejezet

Nemzeti kiberhadviselési stratégiák, végrehajtó szervezetek

Dévai Dóra

Bevezetés

Mára a nemzetállamok stratégiai versengése a kibertérben is jól láthatóvá vált. Az informatikai rendszerek sérülékenységének kihasználása nemzetbiztonsági célok érdekében több évtizedre tekint vissza. Ellenben ezen képességek stratégiai szintű kiaknázása a nemzeti érdekek és célkitűzések megvalósításáért teljesen új biztonságpolitikai paradigma. A nagyhatalmi ambíciókkal rendelkező államok számára a nagyhatalmi politika részét képezi a kibertér gazdasági, diplomáciai és katonai értelemben egyaránt, ahol a stratégiai kultúrájuknak megfelelően alakítják ki képességeiket és politikájukat. A fejezetben a stratégiaelmélet és azon belül a stratégiaikultúra-koncepció felhasználásával mutatjuk be az USA és Oroszország kibervédelmi stratégiai gondolkodását és evolúcióját.

Elméleti alapvetések

Jelen tanulmány abból a hipotézisből indul ki, hogy a kiberfegyverek megjelenésekor nem csupán egy új fegyvernemről beszélhetünk,[1] hanem egy sokkal átfogóbb jelenségről, amely a technológiai fejlődés következtében hatással van a nemzetállamok közötti kapcsolatokra és a hadviselés fejlődésére is. A kibertér így stratégiai értelmet nyer egyrészt azáltal, hogy befolyásolja a nemzetállamok hatalomérvényesítési képességét, másrészt a nemzetállamok versengenek a kibertér feletti ellenőrzés jogáért. A második hipotézisünk tehát, hogy a kibervédelmi stratégia a nemzeti stratégiai kultúra szerves része, és így a doktrinális, szakpolitikai és operatív képességek kialakítása és rendszerszintű integrálása során

[1] Kovács László: *Kiberbiztonság és stratégia*. Budapest, Dialóg Campus, 2018.

https://doi.org/10.36250/01079_10

https://orcid.org/0000-0003-1024-4474

szintén megfigyelhető a kapcsolat a társadalom alapvető értékei és a nemzetállam stratégiai viselkedése között.

A stratégiaelméleti kutatások régóta keresik azokat a tényezőket, amelyek hatást gyakorolnak a stratégiai döntésekre. Az 1970-es években a nukleáris stratégiát vizsgálva alakult ki a stratégiai kultúra fogalma. Felismerve, hogy a szovjet és amerikai stratégák is bizonyos kulturális környezetben szocializálódott gondolkodók. A szocializációs folyamat során a nukleáris stratégiával kapcsolatban kialakult alapelvek, gondolkodásmód és viselkedésminták viszonylagos állandóságra tettek szert, beépülve ezáltal a kultúrába és felülemelkedve a nukleáris politika szintjén.[2] Ez a kapcsolat nem azt jelenti, hogy az adott kultúra meghatározza a stratégiaalkotás és a hadviselés valamely jellemzőjét, hanem láthatóan befolyásolja annak minden elemét. Egyes teoretikusok szerint a stratégia nemzeti szinten a társadalomnak a katonai erő használatával kapcsolatos értékrendjét tükrözi. Míg a második szint, a katonai kultúra fejezi ki azt, hogy az adott nemzet hogyan háborúzik.[3]

Az általános stratégiaelmélet a stratégiaalkotás folyamatában az első,[4] kulcsfontosságú lépésként azonosítja a stratégiai környezet értelmezését. Ez alapvetően a biztonsági környezet értelemzése, a stratégiai szintű nemzeti lehetőségek és az ezeket veszélyeztető fenyegetések azonosítása, beleértve a stratégiai vetélytársak vagy potenciális ellenfelek képességeit.[5] A célkitűzések eléréséhez használt stratégiai módszerek sokfélék lehetnek. Tipikusan ilyen az elrettentés két alapvető változata: a megtorló vagy büntető elrettentés *(deterrence by punishment),* valamint a védelem és az ellenállóképesség növelése *(deterrence by denial).* Stratégiai módszer lehet még például a szövetségesekkel való együttműködés vagy pont ellenkezőleg, a nemzetközi jogi normák ambivalenciáinak a kihasználása *(lawfare).* A stratégiai hármas utolsó eleme az erőforrások vagy eszközök hozzárendelése az adott célkitűzésekhez.[6] Ilyen eszköz például a katonai erő, a képzés és kutatás-fejlesztés, a diplomácia stb. A stratégiai kultúra tehát

[2] Szegő László: Az Amerikai Egyesült Államok stratégiai kultúrája. *Hadtudomány,* 24. (2014), 1–2. 25–34.

[3] Thomas G. Mahnken: *United States Strategic Culture.* (H. n.), Defense Threat Reduction Agency – Comparative Strategic Cultures Curiculum, 2006.

[4] Harry R. Yarger: *Strategic Theory for the 21st Century: The Little Book on Big Strategy.* U.S. Army War College Strategic Theory. Carlisle, Army War College Carlisle Barracks, Strategic Studies Institute, 2006.

[5] Yarger (2006): i. m.; Kovács (2018): i. m. (1. lj.).

[6] Yarger (2006): i. m.

kihat a stratégiaalkotás teljes folyamatára. Így a két szemlélet szintéziséből még teljesebb képet kaphatunk egy-egy nemzet stratégiai gondolkodásáról.

A kiberképességek kialakítása és integrálása az Amerikai Egyesült Államokban[7]

Az Egyesült Államok védelmi döntéshozatali és tervezőrendszerében a politikai-stratégiai szintet az elnök, a Nemzetbiztonsági Tanács, a védelmi miniszter és a Védelmi Minisztérium képviseli. A katonai-stratégiai szintet a Vezérkari Főnökök Egyesített Bizottságának (VFEB) főnöke *(Chairman of the Joint Chiefs of Staff)* és az egyesített műveleti parancsnokságok *(Unified Combatant Commands)* alkotják.

Az USA-ban a technikai fejlődés és a hadügy nagyon szorosan összefonódik. Edward Hunt amerikai történész például korabeli források alapján feltárta, hogy maga az informatikai biztonság mint diszciplína megszületése hogyan köthető a Pentagonhoz és még egy sor, a Védelmi Minisztériumhoz tartozó kutatóintézethez és vállalathoz, mint az IBM. A 1960-as években ezekben az intézményekben a komputerek sérülékenységének szisztematikus vizsgálatakor született eredmények nagyban hozzájárultak a mai sérülékenységvizsgálat *(pentesting)* szakterület kialakulásához.[8]

A hetvenes években, a számítógépek terjedésével felgyorsult a folyamat. Az 1990–91-es Öbölháború látványos sikereit követően sorra jelentek meg

[7] Az Egyesült Államok haderejében a katonai kiberműveletek (*cyberspace operations:* CO) jelenlegi fogalmi rendszerét konszolidáló 2018-as szakdoktrína, a Joint Publication 3-12 Cyberspace Operations, I-4. a következőképpen határozza meg a kiberképességet *(cyberspace capability):* „olyan eszköz vagy számítógépes program, beleértve a *software, firmware* vagy *hardware* bármilyen kombinációját, amelynek a célja, hogy valamilyen hatást érjen el a kibertérben vagy a kibertéren keresztül." Ez tehát a kiberképességek szűk, kizárólag technológiai értelmezése. Azonban, ahogy a fentiekben megfogalmaztuk, a kutatás a kiberműveletekkel kapcsolatos átfogó haderőfejlesztést vizsgálja. Ezért az amerikai hadseregben általánosan elterjedt doktrína, szervezet, kiképzés, hadfelszerelés, vezetés, állomány, infrastruktúra, szakpolitika (*doctrine, organization, training, material, leadership, personnel, facility, policy*: DOTMLPF-P) modellen keresztül értelmezem a képességeket. A doktrína szerint a kiberműveletek definíciója: „A kiberképességek alkalmazása olyan esetekben, amelyekben az elsődleges cél valamilyen feladat megvalósítása a kibertérben vagy azon keresztül." Cyberspace Operations, Joint Publication 3-12.

[8] Edward Hunt: US Government Computer Penetration Programs and the Implications for Cyberwar. *IEEE Annals of the History of Computing,* 34. (2012), 3. 4–21.

az egyes haderőnemi doktrínákban és védelmi minisztériumi iránymutatásokban az információs hadviselés, később információs műveletek gyűjtőnév alatt említett új hadviselési elvek. Végül a számítógép-hálózati műveletek (*computer network operations* – CNO) három fajtája, a támadó *(computer network offense),* védekező *(computer network defense)* és felderítő műveletek *(computer network exploitation)* először 1996-ban, az információs műveleteken belül, mint annak az egyik opcionális eleme jelentek meg.[9] Az amerikai haderőnél hagyományos, nagy fokú haderőnemi önállóság keretében a kilencvenes évek közepéig még nem szabályozták összhaderőnemi szinten a CNO vagy éppen az információs műveleti képességek kialakítását.[10]

A doktrínafejlesztésben a CNO-terminológia bevezetése után a következő központosítási kísérlet 2006-ban az első önálló nemzeti katonai kiberműveleti stratégia volt,[11] sokáig csak titkosított dokumentumként. Ez a következőképpen határozza meg a kiberteret: „olyan közeg, amely az elektronikai eszközök és az elektromágneses spektrum felhasználásával adatokat tárol, módosít és továbbít hálózatos eszközökön és fizikai rendszereken keresztül."[12] A kibertérre tehát mint önálló, védendő műveleti területre tekint, amelynek integrációja a többi műveleti közeggel és a fizikai térrel prioritás. Stratégiai célként a katonai kiberfölény *(cyberspace superiority)* kivívását jelöli meg, a tágabb nemzeti érdekek védelmét még nem említi. A központosítás a szervezet szintjén is megindult. 1998 decemberében a stratégiai szintű informatikai támadásokkal szembeni központosított védelem érdekében hozták létre az Összhaderőnemi Számítógéphálózati Védelmi Alkalmi Kötelék *(Joint Task Force – Computer Network Defence)* nevű egységet, amely kezdetben mindösszesen 24 főt számlált.[13]

[9] Az információs műveletek: „az elektronikai hadviselés, a számítógép-hálózati műveletek, a pszichológiai műveletek, a katonai megtévesztés és a műveleti biztonság integrált alkalmazása, összehangoltan bizonyos támogató és kapcsolódó képességekkel, amelyekkel befolyásolja, megzavarja, lerontja vagy korlátozza a szemben álló fél humán és automatizált döntéshozatali folyamatát, miközben megvédi a saját hasonló képességeket." (JP 3-13 2006, I-1). Haig Zsolt: *Információs műveletek a kibertérben*. Budapest, Dialóg Campus, 2018. 176., 246.

[10] James Mulvelon (szerk.): *Addressing Cyber Instability.* Vienna (VA), Cyber Conflict Studies Association, 2012.

[11] The Chairman of the Joint Chefs of Staff: *National Military Strategy for Cyberspace Operations*. 2006.

[12] *National Military Strategy for Cyberspace Operations* (2006): i. m.

[13] U.S. Government Accountability Office: *Defense Department Cyber Efforts: DoD Faces Challenge in its Cyber Activities.* Report GAO-11-75. Washington D.C., 2011. július 25. 18.; Jeffrey L.

A következő fordulópont 2011-ben történt, amikor is az Obama-adminisztráció a kibervédelmi stratégia teljes körű megújításához fogott. Ne felejtsük el, hogy ekkorra túl voltunk néhány stratégiai jelentőségű eseményen a globális kibertérben, úgymint a 2007-es Észtország elleni informatikai támadás, a 2008-as grúz–orosz háború alatt indított kiberműveletek vagy 2010-ben az Egyesült Államokkal is kapcsolatba hozott Stuxnet. A Fehér Ház kidolgozta az USA első Nemzetközi Kiberstratégiáját, amelyben deklarálták, hogy a kibertérben az amerikai érdekeket akár fegyveres erővel is megvédik. Ugyanakkor a demokrata kormányzatokra jellemzően a diplomáciai eszközök és a szövetségesi együttműködés jelentősége nagymértékben felértékelődött. A Külügyminisztériumban kialakították a Kiberkoordinátori Irodát *(Office of the Coordinator for Cyber Issues),* és az USA, felvállalva a nemzetközi vezető szerepet, minden eddiginél nagyobb arányú kampányt indított a nemzetközi multilaterális diplomáciai fórumokon.

Szükség is volt a nemzetközi környezet megnyugtatására, mert a katonai kiberképességek kialakításában és alkalmazásában is léptékváltás történt. 2009 júniusában létrehozták az első Kiberparancsnokságot (*U.S. Cybercommand:* USCYBERCOM) mint Egyesített Alparancsnokságot *(Subordinate Unified Command).* Továbbá, az egyes haderőnemeknek 2010-re szintén meg kellett szervezniük a saját kiberparancsnokságukat. 2011-ben megújították a Védelmi Minisztérium Kibertérműveleti Stratégiáját, ezúttal nyilvánosságra hozva egy kivonatot. Először jelent meg az elrettentés koncepciója a kibervédelemmel kapcsolatban. Stratégiai célkitűzésként hangsúlyos az összkormányzati fellépés is. 2011-ben a Kongresszus jóváhagyta a nemzetközi támadó kiberműveleteket. Az USA ezzel egyértelműen deklarálta, hogy stratégiai szintű katonai kiberképességeket fejleszt annak érdekében, hogy megőrizze stratégiai dominanciáját, és megvédje az amerikai nemzeti érdekeket a kibertérben.

2013-ban újabb fordulópont jött. Bár először csak minősített dokumentumként, de megjelent az első összhaderőnemi kiberműveleti doktrína (JP3-12 Cyberspace Operations). Az összhaderőnemi kiberműveleti tervezés és végrehajtás eljárásrendjét megalkották, a szerep- és felelősségi köröket meghatározták, a hatásköröket kijelölték. Szervezetileg is előrelépés volt a Kiberműveleti Erők

Caton: *Army Support of Military Cyberspace Operations: Joint Contexts and Global Escalation Implications*. U.S. Army War College, 2015.

(*Cyber Mission Forces:* CMF) koncepciójának kialakítása[14] és a Kiberparancsnokság, a haderőnemek[15] és a stratégiai szintű Összhaderőnemi Műveleti Parancsnokságok *(Unified Combattant Commands)* közötti együttműködés rendszere. Kitűzték a Kiberparancsnokságon belül 6500 fővel felállítandó kiberműveleti erők kiképzésének menetrendjét és a csapatok feladatrendszerét, beleértve a nemzeti védelmi célokat.

A 2015-re megújult védelmi minisztériumi kiberstratégia összefoglalja a fenti változásokat. Ezen kívül minden eddiginél részletesebben fejti ki egy komplex elrettentés koncepcióját, amely egy átfogó megközelítés jegyében magába foglalja mind a büntető, mind a „megtagadó" elrettentés számos eszközét. Az elrettentés komplex megközelítésének szintén fontos eleme az attribúció, a támadó kilétének azonosítása, amelynek érdekében a stratégia tovább erősíti a hírszerzés, a felderítés és a korai előrejelzés képességét. A stratégiában a kiberképességek fejlesztésében kiemelt stratégiai cél a kutatás-fejlesztés.[16]

2018-ra bontakozott ki az amerikai stratégiai gondolkodásban a kiberképességek kialakításával, integrációjával és alkalmazásával kapcsolatos rendszerszintű látásmód. 2018. május 4-én a Kiberparancsnokság tizedik egyesített műveleti parancsnoksággá való átszervezése megtörtént. A kiberműveleti erők elérték a teljes műveleti képességüket. Még ugyanebben az évben megjelent a kiberműveleti doktrína újabb kiadása. 2018-ra tehát kialakult a kiberképesség stratégiai szintű szervezetének alapvető struktúrája.

A következőkben az újonnan létrehozott kiberműveleti erők[17] tevékenységét tekintjük át. A CMF a haderőnemek legkiemelkedőbb tehetségeiből összeállított elit egységek, de nem tagozódnak be a haderőnemi hadosztályokba. Amint az *1. táblázat* mutatja, felosztásuk a feladatkör és a parancsnokság alapján történik.

Az úgynevezett National Mission Teams sokrétű feladatkörrel rendelkeznek, ők azok, akik elsősorban részt vesznek a Védelmi Minisztérium és a haderő védelmén túli nemzetvédelmi feladatokban. Egyfajta előretolt állásban gyakran a Védelmi Minisztérium információs hálózatain kívül eső, globális ellenséges *(red space)* vagy semleges hálózatokon *(grey space)* végeznek feladatokat a stratégiai jelentőségű fenyegetések felderítése és elhárítása (korai figyelmeztetés, támadó

[14] National Security Archive: *Preparing for Computer Network Operations: USCYBERCOM Documents Trace Path to Operational Cyber Force.* George Washington University, 2019. május 3.

[15] Szárazföldi erő, légierő, haditengerészet, tengerészgyalogság.

[16] Department of Defence: *The DoD Cyber Strategy.* 2015.

[17] Az elnevezés a szerző fordítása.

műveletek stb.) érdekében.[18] Jól ismerik a kibertérben ellenséges tevékenységet végző szereplőket, és így a válaszlépéseket célra szabottan tervezik meg.[19]

1. táblázat: A kibererők feladatkör szerinti felosztása

Csapat típusa	Feladatkör
13 nemzeti kiberműveleti csapat(National Mission Teams)	Nemzeti szintű védelmi és támadó képességek
27 harci kiberműveleti csapat (Combat Mission Teams)	Az Egyesített Műveleti Parancsnokságok támogatása
18 nemzeti kibervédelmi csapat (National Cyber Protection Teams [CPTs])	A Védelmi Minisztérium információs hálózatainak a védelme
24 haderőnemi kibervédelmi csapat (Service CPTs)	A Védelmi Minisztérium információs hálózatainak a védelme
Egyesített védelmi minisztériumi információs hálózati kibervédelmi csapatok (DODIN CPTs)	A Védelmi Minisztérium információs hálózatainak a védelme
26 műveleti parancsnoksági kibervédelmi csapat (Combatant Command CPTs)	Az Egyesített Műveleti Parancsnokságok támogatása

Forrás: A JP3-12 alapján a szerző szerkesztése

A Védelmi Minisztérium információs hálózatainak védelméért a haderőnemek felelősek a saját használatukban lévő szegmensekben. Feladataik közé tartozik a hálózat konfigurálása, üzemeltetése és védelme. Jelentős előrelépés volt, amikor 2017-ben a Védelmi Minisztérium utasítása alapján a haderőnemi kiberparancsnokságok állandó tervező sejteket hoztak létre az egyesített műveleti parancsnokságokon belül.

A 2010-es évek végére megteremtették a kiberműveletek új osztályozási rendszerét is. A 2018-as kiberműveleti doktrína a műveletek célkitűzése vagy szándéka, valamint a műveleti környezet alapján három fő küldetési *(mission)* kategóriába osztja fel a kiberműveleteket: a Védelmi Minisztérium információs hálózatain végzett műveletek[20] *(DODIN operations);* kibertéri védelmi

[18] Mark Pomerleau: Here's How DoD Organizes Its Cyber Warriors. *C4ISRNet,* 2017. július 25.

[19] *Cyberspace Operations* (2018): i. m. I-9.

[20] A DODIN-műveletek magukba foglalják a már meglévő DOD-kibertér konfigurálását, üzemeltetését, kibővítését, informatikai biztonságát (CIA-követelmények). Ezek a tevékenységek tehát a hálózatra és annak sérülékenységeire fókuszálnak annak érdekében, hogy proaktív módon felkészüljenek a kibertérből érkező lehetséges fenyegetésekre.

műveletek (*defensive cyberspace operations:* DCO); és támadó kibertéri műveletek (*offensive cyberspace operations:* OCO).[21]

A stratégiai szintű Kiberparancsnoksággal párhuzamosan a négy fő haderőnem önállóan, a saját kötelékében alakította ki a kiberképességeit. A 6500 fős létszám tehát csak a közvetlenül a CYBERCOM-nak alárendelt erőket jelenti. A haderőnemek kötelékébe tartozó hadműveleti és harcászati szintű alakulatok ezenfelül szintén többezres létszámot tesznek ki.

2018 mérföldkő a hadsereg nemzeti kibervédelemben betöltött szerepének szempontjából is. Az ebben az évben kiadott nemzeti kiberbiztonsági stratégia kodifikálja a támadó kiberműveleteket a fegyveres konfliktusokon kívül is. Stratégiai célként az elrettentésre helyezi a hangsúlyt. Szintén ebben az évben a védelmi tervezés költségvetési aspektusának csúcsát jelentő nemzeti védelmi törvény *(National Defence Authorization Act)* stratégiai iránymutatásként jóváhagyta az úgynevezett „előretolt védelem" *(defend forward)* és az „állandó jelenlét" *(persistent engagement)* műveleti koncepcióját. Az előbbi felhatalmazást ad a Kiberparancsnokságnak a rosszindulatú kibertámadások megszakítására azok kiindulópontjában, tehát akár más országok területén is, beleértve a háborús küszöb alatti tevékenységet is, például a befolyásoló műveleteket. Az állandó jelenlét, tulajdonképpen a már meglévő gyakorlatot szentesítve, jóváhagyja az USA területén kívüli informatikai hálózatokban történő állandó jellegű felderítést és megfigyelést, valamint megelőző csapást is.[22] A politikai szintű stratégiai iránymutatások alapján tehát a hadsereg feladata nemcsak a katonai értelemben vett kibertér védelme, de már nem is csak a nemzeti kibertér védelme, hanem fokozatosan kiterjed a nemzeti érdekek globális kibertérben történő állandó, a fegyveres konfliktusokon kívüli védelmére is.

Az eddigiek alapján láthattuk, hogy az USA esetében a stratégiai kultúra miként befolyásolja a kiberhadviselési stratégia fejlődését. A katonai erő és a politika kapcsolata tekintetében az amerikai társadalomban, a nyugati társadalmakhoz hasonlóan, a háború a béke ellentéte, és nem a politika más eszközökkel történő folytatásának minősül. A hadsereg tevékenysége békeidőben és a hazai lakosság tekintetében szigorúan korlátozott. A rendelkezésre álló nagy mennyiségű erőforrás, az azonnali intézkedést és eredményeket elváró

[21] Caton (2015): i. m. 50.

[22] 115th Congress (2017–2018): H.R.2810 – National Defense Authorization Act for Fiscal Year. 2018; Greg Myre: ‚Persistent Engagement': The Phrase Driving A More Assertive U.S. Spy Agency. *National Public Radio,* 2019. augusztus 26.

és általában nem hosszú időre előre tekintő társadalom a döntő csaták lehetőségének keresését és a teljes erőkifejtést várja el, ami direkt stratégiai elgondolásokhoz vezet.[23] Az elrettentés tekintetében például a teoretikusok egy része éppen ezért túlfegyverkezést javasol *(overkill),* vagyis a katonai képességek jól látható maximalizálása az elrettentés részét képezi. A számbeli fölény mellett a katonai képességek és az erő meghatározója a technológiai fejlettség szintje. Ebből adódóan a felmerülő problémák megoldása során előszeretettel használják az innovatív technológiai megoldásokat.[24]

A kiberképességek kialakítása és integrálása Oroszországban

Ahogyan látni fogjuk, Oroszországban a hadelméletben a kiberképességek elemzése elválaszthatatlan az információs hadviseléstől. Jelenlegi állapotát a cári időkig visszanyúló, ciklikus megújuláson átesett fejlesztések csúcspontjának tekinthetjük. Az 1970-es évek felgyorsult számítástechnikai fejlődésére reagálva az 1980-as évekre a Szovjetunióban kidolgozták a katonai technikai forradalom elméletét, vagyis hogy a technológia hogyan fogja megváltoztatni a hadviselést. Olyan hadviselési formát vizionáltak rádióelektronikai hadviselés néven, amelyben nem szükséges az ellenfelet kinetikus csapásokkal legyőzni, hanem a kommunikációs és vezetési-irányítási, felderítő, megfigyelő, kommunikációs és informatikai képességek zavarására, lehallgatására vagy elpusztítására kell törekedni.[25] Azonban, míg az USA-ban a technológiai innováció játssza a legfontosabb szerepet a haderőfejlesztésben, addig Oroszországban – részben a korlátozott mértékben rendelkezésre álló anyagi források, részben pedig a hatalom eszközeinek teljesen más koncepcionális megközelítése miatt – a technológiai és a kognitív szféra sohasem vált el egymástól.

A kilencvenes években Oroszországra is nagy hatással volt az amerikai információs hadviselési képességek fejlesztése, és arra késztette, hogy kialakítsa saját koncepcióját ezen a téren. Az amerikai helyzethez hasonlóan ez az útkeresés időszaka volt.[26] Az információs háború kifejezésből a háború szót többféleképpen

[23] Szegő (2014): i. m. 30.

[24] Szegő (2014): i. m. 30–31.

[25] Dimitry Adamsky: *Cross-Domain Coercion. The Current Russian Art of Strategy*. Paris, The Institut Français des Relations Internationales, 2015. november.

[26] Az orosz stratégák természetesen felhasználták a saját tapasztalataikat is. Tanultak például az 1994–1996 között lezajlott első csecsen háborúból is, ahol a csecsenek rendkívül jól kihasználták

is lefordították oroszra: *informacionnaja vojna, informacionnaja borba* vagy *informacionnoje protyivoborsztvo.* Az elsőt inkább a média, míg a *protyivoborsztvo* kifejezést, amely küzdelmet, ellentevékenységet vagy konfliktust is jelenthet, illetve a *borba* kifejezést inkább a hadsereg használja.[27]

Első alkalommal a 2000-es nemzeti biztonsági koncepció osztotta az információs hadviselést két alcsoportra: technikai és pszichológiai információs képességekre. A technikai információs képességek alatt a következőket értették: a hírszerzés technikai formáit, az információvédelmet, a szupermagas elektromágneses frekvenciájú fegyvereket, az ultraszonikus fegyvereket, a rádióelektronikai ellentevékenységet, az elektromágnesesimpulzus-alapú fegyvereket, valamint az informatikai hardvert és szoftvert. A pszichológiai információs képességekhez sorolták a tömegtájékoztatást, a nem halálos fegyvereket, a pszichotróp szereket és egyéb kemikáliákat.[28] Egy másik beszámoló 2003-ból szintén a pszichológiai információs képességek között említi a dezinformációt, *maszkirovkát,* a kriptológiát és a *szteganográfiát.*[29]

A technológiai pillér a katonai technikai forradalom 1970-es évekbeli koncepciójáig nyúlik vissza. Mivel az információs hadviselés az ellenfél döntéshozatali folyamatára igyekszik hatást gyakorolni, az „aktív intézkedések" *(aktyivnije meroprijatyija)*, a *reflexív kontroll* és a *maszkirovka* kézenfekvő stratégiai módszernek bizonyul a pszichológiai információs hadviseléshez. Legfőbb eszközeik a megtévesztés, a dezinformáció, a propaganda, az álca, a rejtőzködés és a tagadás. Céljuk a célcsoport valóságészlelésének és azon keresztül a döntéshozatalának a befolyásolása olyan módon, amely az orosz érdekeket szolgálja. Ez tehát egy, a kognitív szférában történő hadviselés.[30] A célcsoport lehet a saját lakosság is.[31] Az orosz stratégiai gondolkodásban az „információs tér" *(informacionnoje prosztransztvo)* mindig is megbonthatatlan egységként kezelte a technikai

a modern információs környezet és a média által nyújtott lehetőségeket. Ezenkívül különösen nagy hatással voltak az orosz elit gondolkodására a színes forradalmak és az arab tavasz eseményei.

[27] Timothy L. Thomas: Russian Views on Information-Based Warfare. *Air Power Journal,* Special Edition, 1996.

[28] Timothy L. Thomas: *Comparing US, Russian, and Chinese Information Operations Concepts*. Foreign Military Studies Office, Fort Leavenworth, 2004b.

[29] Thomas (2004a): i. m.

[30] Timothy L. Thomas: Russia's Reflexive Control and the Military. *Journal of Slavic Military Studies,* 17. (2004b), 2.; Mark Galeotti: *Active Measures: Russia's Covert Geopolitical Operations.* Marshall Center, 2019. június.

[31] Vö. az USA jogrendje (Title 10 US Code 2241) tiltja a Honvédelmi Minisztérium számára a hazai propagandatevékenységet.

és a kognitív elemeket. A kibertér *(kiberprosztansztvo)* kifejezést először csak a nyugati szövegek fordításakor vagy az amerikai kibercsapásokkal kapcsolatosan használták. Ez az elmúlt öt-tíz évben kezdett megváltozni, és az orosz stratégiai diskurzusban megjelent a vita más országok koncepciójának átvételéről.[32]

Az orosz fenyegetettségpercepció az információs térben a politikai rendszer biztonságát veszélyeztető fenyegetésekre helyezi a hangsúlyt. A 2000-es nemzeti biztonsági koncepció[33] kifejti, hogy Oroszország folyamatos küzdelemben áll a nyugati hatalmakkal, akik titkosszolgálati eszközökkel szünet nélkül azon munkálkodnak, hogy befolyásolással a politikai rendszer ellen hangolják a közvéleményt. Az információs térben folytatott küzdelem olyannyira felértékelődött, hogy akár a stratégiai győzelem eszköze is lehet, és így az orosz stratégiai elrettentés részét képezi.[34]

A 2010-es évekre érett be az a fordulat az orosz politikai és katonai gondolkodásban, amely során – a nyugati katonai technikai képességfejlesztéshez képesti lemaradást ellensúlyozandó – egy indirekt stratégián alapuló, a katonai és a nem katonai eszközöket (politikai, hírszerzési, diplomáciai, információs, gazdasági stb.) vegyítő stratégiát vezettek be.[35] 2013. március 24-én Valerij Geraszimov hadseregtábornok a Hadtudományi Akadémia plenáris ülésén mondta el híres beszédét az ezen elveket összegző új generációs hadviselésről.[36] A 2008-as orosz–grúz háborút követően átfogó modernizáció indult meg, amelyben kiemelt szerepet kap az információs képességek fejlesztése. Nem véletlen, hogy az információs háború új, átfogó definíciója is ekkor jelent meg a stratégiai dokumentumokban. 2011-ben az Oroszországi Föderáció fegyveres erejének információs térbeli tevékenységének koncepciója így fogalmaz:

> „Az információs háború *(informacionnaja vojna)* egy, az információs térben két vagy több állam között történő konfrontáció, amelynek a célja az információs rendszerekben, folyamatokban és erőforrásokban történő károkozás, a politikai, gazdasági és társadalmi rendszerek gyengítése érdekében, a népesség masszív pszichológiai manipulációja az állam és a társa-

[32] Timothy L. Thomas: Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts? *The Journal of Slavic Military Studies,* 2014.

[33] A nemzeti biztonsági koncepció 2009-től nemzeti biztonsági stratégia.

[34] M. A. Garejev: Sztratyegicseszkoje szderzsivanyije. Problemi i resenyija. *Krasznaja Zvezda,* No. 183., 2008. február 8.

[35] Timothy L. Thomas: *Russia. Military Strategy.* Fort Leavenworth, Foreign Military Studies Office, 2015; Valerij Geraszimov: Cennoszty Nauki v Predvigyinyiji. *Vojenno-Promislennyij Kurjer Online,* 2013. február 27.

[36] Geraszimov (2013): i. m.

> dalom destabilizálása érdekében, valamint kényszerítő eszköz, hogy az állam az ellenfél számára kedvező döntéseket hozzon."[37]

Az információs tevékenységet folytató szervezetek rendszere és működése sokkal kevésbé ismert, mint az USA esetében. A Szövetséges Biztonsági Szolgálat (*Fegyeralnaja szluzsba bezopasznosztyi Rosszijszkoj Fegyeraciji* – FSZB), az Állambiztonsági Bizottság (*Komityet goszudarsztvennoj bezopasznosztyi* – KGB) utódszervezete főként a belbiztonságért felel, beleértve az infokommunikációs rendszerek biztonságát. Nyugati szakértők az FSB-hez kötik például a Turla Advanced Persistent Threat- (APT-) csoportot.[38] A katonai hírszerző szolgálat, az Oroszországi Föderáció Fegyveres Erői Vezérkarának Felderítő Főcsoportfőnöksége (*Glavnoje razvegyivatyelnoje upravlenyije* – GRU) az FSB-vel közösen hajtotta végre, többek között, a 2007-es észtországi és a 2008-as Grúzia elleni informatikai támadást, a 2016-os amerikai félidős választások alatti kampányt vagy a NotPetya-műveletet. Egységei rendelkeznek az információs műveletek technikai és pszichológiai eszköztárával. Egy-egy tevékenységre specializálódnak, mint például a *malware*-fejlesztés, a szivárogtatás vagy a propaganda. A 85. Különleges Szolgálati Központ (az úgynevezett 26165-ös egység) például rádióelektronikai felderítést és kriptológiai tevékenységet folytat, de ezt hozzák összefüggésbe az APT28-as csoporttal is, amely ismert Fancy Bear, Pawn Storm, Sofacy, Strontium néven is. Egy másik ismertté vált alakulat, a Különleges Technológiai Főközpont (az úgynevezett 74455-ös egység) kiberműveleteket végez, példának okáért a 2016-os amerikai kampányt vagy az ukrajnai infrastruktúra elleni támadásokat.[39] A harmadik nagyobb szervezet, amelyet gyakran hoznak kapcsolatba az információs térben történő tevékenységekkel, az Oroszországi Föderáció külföldre irányuló polgári hírszerző szervezete, a Szluzsba vnyesnyej razvedki Rosszijszkoj Federaciji (SZVR), amelyet APT29 vagy Cozy Bear hackercsoportként azonosítottak. Ezt teszik felelőssé például a Covid–19-vakcinákkal vagy a SolarWindsszel kapcsolatos kémkedésért is. Mindkét szervezet létszáma titkos, de orosz források szerint a GRU személyi állománya többszöröse a polgári hírszerző szolgálatának. A GRU-val ellentétben, amely szabotázs-, kiber- és információs műveleteket is végrehajt, az SZVR inkább hagyományos

[37] The Russian Ministry of Defense: *Russian Federation Armed Forces' Information Space Activities Concept*. Moszkva, 2011.

[38] Janne Hakala – Jazlyn Melnychuk: *Russia's strategy in cyberspace.* Riga, NATO Strategic Communications Center of Excellence, 2021.

[39] Hakala–Melnychuk (2021): i. m.

hírszerző tevékenységet folytat.[40] A „klasszikus" hírszerző szervezetek mellett számos egyéb, homályos hátterű szervezet is folytat tevékenységeket az információs térben. Ilyenek például az úgynevezett katonai tudományos cégek *(naucsnyije kompanyiji),* a félkatonai hazafias hackercsoportok, mint a CyberBerkut, a különböző bűnözői csoportok vagy a hírhedtté vált, szentpétervári trollfarm, az Internetkutató Ügynökség *(Agentsztvo Internet-Isszledovanyij),* amely egy, a Kremlhez szorosan köthető magánvállalat.

Összességében elmondható, hogy az orosz stratégiai gondolkodásban az információs konfrontáció megközelítése holisztikus, ötvözi a digitális-technológiai megoldásokat a kognitív pszichológiai eszközökkel. Egységesen használható stratégiai eszköznek tekinti a katonai és a nem katonai, a kinetikus és a nem kinetikus megoldásokat, illetve az állami és nem állami szereplőket. Továbbá, nem választja el élesen a háború és a béke állapotát, a lakosságot a fegyveres erőktől vagy a hazai és a nemzetközi népességet mint célközönséget. Előszeretettel választja a megtévesztés, rejtés és álcázás módszereit, és így a stratégiai célokhoz jellemzően titkosszolgálati vagy zavaros hátterű végrehajtó szervezeteket rendel.

Esettanulmány

Az elmúlt időszak egyik legjelentősebb informatikai ellátási láncot ért eseménye a SolarWinds Orion hálózatkezelő szoftverén keresztül több ezer számítógép-hálózaton elhelyezett kémprogram volt. Az úgynevezett Sunburst rosszindulatú programot használó műveletet 2020 decemberében fedezték fel, de szakértők szerint egészen 2019 októberéig nyúlik vissza. Több száz amerikai szervezet érintett az adatlopásban, köztük egy tucat kormányhivatal, mint például a Pénzügyminisztérium, a Pentagon, a Belbiztonsági Minisztérium és azon belül a szövetségi számítógép-hálózatok biztonságáért felelős ügynökség (*Cybersecurity and Infrastructure Security Agency* – CISA), de érintett a Microsoft, az Intel és a Cisco is.[41]

Az eset a célpontok, a kompromittált adat mennyisége és a támadás jellege miatt különösen érzékeny nemzetbiztonsági szempontból, illetve még nem lehet

[40] Hakala–Melnychuk (2021): i. m.

[41] Justin Katz: Cyber Exec: 50 Orgs 'Genuinely Impacted' by Solarwinds Hack. *FCW,* 2020. december 21.

biztosan tudni, hogy csak kémkedésre használták-e, vagy további károkozásra alkalmas mechanizmusokat is bejuttattak az elkövetők.

További kérdéseket vet fel a hatékony és jogszerű válaszlépés. A hálózatok működését akadályozó vagy az informatikai rendszereket romboló beavatkozások esetén a nemzetközi jog felhatalmazást ad a károkozás megszüntetésére irányuló és azokkal arányos ellenlépésekre.[42] Ugyanakkor önmagában a kémkedést a nemzetállamok hallgatólagos megegyezése alapján nem bünteti a nemzetközi jog. A nemzetállamok a saját hatáskörükben foganatosíthatnak diplomáciai vagy büntetőjogi lépéseket. 2016 óta az USA élen jár a gazdasági és pénzügyi szankciók alkalmazásában a jelentős kibertámadások elkövetőivel szemben.

A korábbi esetekhez hasonlóan ebben az esetben is komplex, „látható és nem látható" lépésekből álló válaszadás történt. 2021 áprilisában Joseph Biden átfogó elnöki rendeletben megnevezte az SVR APT29 csoportját mint a SolarWinds-kémkedésikampány elkövetőjét, és újabb pénzügyi szankciókat vetett ki Oroszország káros nemzetközi tevékenysége ellen, beleértve a kiberteret. Ezen kívül kiutasítottak 10 orosz diplomatát.[43]

A SolarWinds-kampányt az amerikai kiberhadviselési stratégia kontextusában is kiértékelték. Szakértők rámutattak, hogy ez nem az előretolt védelem és az állandó jelenlét koncepciójának kudarcát jelenti, hanem arra hívja fel a figyelmet, hogy ez a két műveleti koncepció és az offenzív kiberműveleti képesség önmagában nem nyújt elégséges elrettentő erőt. Sokkal nagyobb hangsúlyt kell fektetni a kormányzati és a magánszektor informatikai védelmének szabályozására.[44]

Irodalomjegyzék

115th Congress (2017-2018): H.R.2810 – National Defense Authorization Act for Fiscal Year 2018. Online: www.congress.gov/bill/115th-congress/house-bill/2810/text

Adamsky, Dimitry: *Cross-Domain Coercion. The Current Russian Art of Strategy.* Paris, The Institut Français des Relations Internationales, 2015. november. Online: www.ifri.org/sites/default/files/atoms/files/pp54adamsky.pdf

[42] Michael M. Schmitt (szerk.): *Tallin Manual 2.0.* Cambridge, Cambridge University Press, 2017.

[43] The White House: *Fact Sheet. Imposing Costs for Harmful Foreign Activities by the Russian Government* (2019. április 15.).

[44] Robert Morgus: The SolarWinds Breach Is a Failure of U.S. Cyber Strategy. *Lawfare,* 2020. december 18.

Caton, Jeffrey L.: *Army Support of Military Cyberspace Operations: Joint Contexts and Global Escalation Implications.* U.S. Army War College, 2015.

Department of Defence, Joint Staff: *Cyberspace Operations. Joint Publication J-P 3-12.* Washington D.C., 2018.

Department of Defence, The Chairman of the Joint Chiefs of Staff: *National Military Strategy for Cyberspace Operations.* 2006. Online: www.hsdl.org/?abstract&did=35693

Department of Defence: *The DoD Cyber Strategy.* 2015.

Galeotti, Mark: *Active Measures: Russia's Covert Geopolitical Operations.* Marshall Center, 2019. június. Online: www.marshallcenter.org/en/publications/security-insights/active-measures-russias-covert-geopolitical-operations-0

Garejev, M. A.: Sztratyegicseszkoje szderzsivanyije. Problemi i resenyija. *Krasznaja Zvezda,* No. 183., 2008. február 8.

Geraszimov, Valerij: Cennoszty Nauki v Predvigyinyiji. *Vojenno-Promislennyij Kurjer Online,* 2013. február 27. Online: https://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_20160228_art008.pdf.

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

Hakala, Janne – Jazlyn Melnychuk: *Russia's strategy in cyberspace.* Riga, NATO Strategic Communications Center of Excellence, 2021.

Hunt, Edward: US Government Computer Penetration Programs and the Implications for Cyberwar. *IEEE Annals of the History of Computing,* 34. (2012), 3. 4–21. Online: https://doi.ieeecomputersociety.org/10.1109/MAHC.2011.82

Katz, Justin: Cyber Exec: 50 Orgs 'Genuinely Impacted' by Solarwinds Hack. *FCW,* 2020. december 21. Online: https://fcw.com/articles/2020/12/21/sunburst-hack-fifty-orgs-russia.aspx

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

Mahnken, Thomas G.: *United States Strategic Culture.* (H. n.), Defense Threat Reduction Agency – Comparative Strategic Cultures Curiculum,Comparative Strategic Cultures Curiculum, 2006. Online: https://irp.fas.org/agency/dod/dtra/us.pdf

Morgus, Robert: The SolarWinds Breach Is a Failure of U.S. Cyber Strategy. *Lawfare,* 2020. december 18. Online: www.lawfareblog.com/solarwinds-breach-failure-us-cyber-strategy

Mulvelon, James (szerk.): *Addressing Cyber Instability*. Vienna (VA), Cyber Conflict Studies Association. 2012.

Myre, Greg: ‚Persistent Engagement': The Phrase Driving A More Assertive U.S. Spy Agency. *National Public Radio,* 2019. augusztus 26. Online: www.npr.org/2019/08/26/747248636/persistent-engagement-the-phrase-driving-a-more-assertive-u-s-spy-agency

National Security Archive: *Preparing for Computer Network Operations: USCYBERCOM Documents Trace Path to Operational Cyber Force*. George Washington University, 2019. május 3. Online: https://nsarchive.gwu.edu/news/cyber-vault/2019-05-03/preparing-computer-network-operations-uscybercom-documents-trace-path-operational-cyber-force.

Pomerleau, Mark: Here's How DoD Organizes Its Cyber Warriors. *C4ISRNet,* 2017. július 25. Online: www.c4isrnet.com/workforce/career/2017/07/25/heres-how-dod-organizes-its-cyber-warriors/

Schmitt, Michael. M. (szerk.): *Tallin Manual 2.0.* Cambridge University Press, 2017.

Szegő László: Az Amerikai Egyesült Államok stratégiai kultúrája. *Hadtudomány,* 24. (2014), 1–2. 25–34. Online: www.mhtt.eu/hadtudomany/2014/1_2/2014_1_2_3.pdf

The Russian Ministry of Defense: *Russian Federation Armed Forces' Information Space Activities Concept.* Moszkva, 2011. Online: https://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle

The White House: *Fact Sheet. Imposing Costs for harmful foreign activities by the Russian Government* (2019. április 15.). Online: www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/

Thomas, Timothy L.: *Russia. Military Strategy.* Fort Leavenworth, Foreign Military Studies Office, 2015.

Thomas, Timothy L.: Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts? *The Journal of Slavic Military Studies,* 2014. Online: https://doi.org/10.1080/13518046.2014.874845.

Thomas, Timothy L.: *Comparing US, Russian, and Chinese Information Operations Concepts*. Fort Leavenworth, Foreign Military Studies Office, 2004a.

Thomas, Timothy L.: Russian Views on Information-Based Warfare. *Air Power Journal,* Special Edition, 1996. Online: https://apps.dtic.mil/sti/pdfs/ADA529685.pdf

Thomas, Timothy L.: Russia's Reflexive Control and the Military. *Journal of Slavic Military Studies,* 17. (2004b), 2. Online: www.rit.edu/~w-cmmc/literature/Thomas_2004.pdf

U.S. Government Accountability Office: *Defense Department Cyber Efforts: DoD Faces Challenge in its Cyber Activities*. Report GAO-11-75. Washington D.C., 2011. július 25.

Yarger, Harry R.: *Strategic Theory for the 21st Century: The Little Book on Big Strategy*. U.S. Army War College Strategic Theory. Carlisle, Army War College Carlisle Barracks, Strategic Studies Institute, 2006.

11. fejezet

Szövetségi stratégiák – Az EU–NATO-együttműködés

Molnár Anna

Bevezetés

Napjainkban az információs és kommunikációs technológiák (IKT) gyakorlatilag minden területre kiterjedő használata egyszerre szolgál a gazdasági növekedés és az innováció elősegítőjeként, valamint az aszimmetrikus kiberfenyegetések forrásaként. Az elmúlt évtizedekben az egyénekkel, vállalatokkal és kritikus infrastruktúrákkal szembeni növekvő számú kibertámadás egyre inkább felhívta a figyelmet a kibertérrel kapcsolatos fenyegetésekre és kockázatokra. Tekintettel arra, hogy a számítógépes bűnözés nem ismeri a nemzeti határokat, és egyes államok támadó és védelmi jellegű kiberképességeiket egyaránt fejlesztik, e területen is szükségessé vált a nemzetközi normák és együttműködés feltételrendszerének kiépítése. A genfi internetplatform (*Geneva Internet Platform* – GIP) adatai szerint 2021-ben a támadó kiberképességekkel rendelkező államok száma elérte a 23-at, emellett további 30 állam tervezi ilyen típusú képességek fejlesztését.[1]

A kritikus infrastruktúrák növekvő kitettsége miatt a nemzetközi rendszer szereplői riasztóan kiszolgáltatottá váltak a rosszindulatú kiberaktivitásokkal szemben. Ma már közhelynek számít, hogy a kibertér teljesen megváltoztatta életmódunkat, gazdaságainkat és a társadalmi folyamatokat. A digitális forradalom kínálta előnyök sokoldalú kihasználását azonban a kibertér háborús célú felhasználásának lehetősége veszélyezteti. A kibertér az elmúlt évtizedek alatt szabályos harctérré és stratégiai prioritássá vált számos állam és nemzetközi szervezet számára. Miközben a gazdasági fejlődés és az emberi jogok tiszteletben tartása érdekében kiemelkedően fontos e terület nemzetközi szintű szabályozása, addig a támadó jellegű kibereszközök és kiberműveletek elszaporodása elkerülhetetlenné tette fokozatos militarizálódását. Nem véletlen, hogy a kibertér rendszerszintű

[1] Digwatch: *UN GGE and OEWG*. 2021.

https://doi.org/10.36250/01079_11

https://orcid.org/0000-0002-7958-6985

kockázata áll a szabályozásáról szóló többoldalú tárgyalások hátterében.[2] E fejezet célja, hogy a Magyarország szempontjából kiemelten fontos nemzetközi szervezetek, az ENSZ, az EU és a NATO kibervédelmi stratégiáit bemutassa. Emellett kitér az EU és a NATO közötti együttműködés vizsgálatára is.

Az egyre gyakoribb és nagyobb hatású számítógépes támadások a globális politikai és gazdasági kapcsolatokra is jelentős hatást gyakoroltak, és az államokat a tárgyalóasztalhoz kényszerítették. Az ENSZ Közgyűlése és Biztonsági Tanácsa, a NATO, az EU, a G7, a G20, a WTO, valamint a különböző regionális szervezetek, például az AU, az EBESZ és az ASEAN keretein belül az államok egyre inkább rákényszerültek, hogy diplomáciai lépéseket tegyenek a biztonságos kibertér megvalósítása érdekében. A modern gazdaság szinte minden területe, a kritikus infrastruktúrák és az alapvető szolgáltatások is egyre inkább az információs és kommunikációs technológiákra támaszkodnak. Mivel a kiberbiztonság a nemzetközi békére, a fenntartható fejlődésre, a digitális együttműködésre, az emberi jogokra, a magánéletre, valamint a globális digitális üzleti környezetre is kihat, így a legtöbb globális, transzatlanti és regionális nemzetközi szervezet ezzel összefüggő szakpolitikákat és intézményesített eszközöket dolgozott ki a kibertámadások egyre kifinomultabb kezelése érdekében.[3]

Az Európai Unió 2013-ban közös közleményt tett közzé kiberbiztonsági stratégiájáról. Ez volt az első kísérlet egy átfogó uniós szakpolitikai dokumentum kidolgozására ezen a területen. Az Afrikai Unió 2014-ben fogadta el a kiberbiztonságról és a személyes adatok védelméről szóló egyezményét, amely alapvetően az afrikai államok elektronikus kereskedelemre, adatvédelemre, kiberbiztonsági kormányzásra és a számítógépes bűnözés ellenőrzésére vonatkozó törvényeinek összehangolására irányult.[4]

A rosszindulatú kiberaktivitások évtizedek óta érintik a magánszemélyeket, a magánvállalkozásokat, a kormányzati intézményeket és a nem kormányzati szervezeteket. A kiberfenyegetések kiszámíthatatlan jellege miatt egy incidens, amely kezdetben hacktivizmusnak vagy pénzügyi kiberbűnözésnek tűnhet, gyorsan nagy nemzetbiztonsági kockázattá vagy akár kiberhadviselési eszközzé is

[2] Piret Pernik: *Improving Cyber Security: NATO and the EU.* International Centre for Defence Studies, 2014. szeptember.

[3] Pernik (2014): i. m.

[4] Uchenna Jerome Orji: The African Union Convention on Cybersecurity: A Regional Response Towards Cyber Stability? *Masaryk University Journal of Law and Technology,* 12. (2018), 2. 91–129.; African Union: *African Union Convention on Cyber Security and Personal Data Protection.* 2014.

válhat. Annak ellenére, hogy nincs konszenzus arról, hogy pontosan mi minősül kiberháborúnak vagy kiberterrorizmusnak, a kormányoknak biztosítaniuk kell az infrastruktúrájuk védettségét és ellenállóképességét a különböző típusú kiberfenyegetésekkel szemben. A szövetségi rendszereken belüli stratégiai gondolkodást jelentős mértékben segíti, hogy jogi és intézményi rendszereik lehetővé tegyék az esetleges kibertámadások hatékony megelőzését, elrettentését, megvédését és enyhítését.[5]

2016-tól, a NATO varsói csúcstalálkozón kiadott nyilatkozata óta a kibertér is egy a műveleti területek közül.[6] A 2018-as európai uniós kibervédelmi szakpolitikai keret szerint „a kibertér az ötödik műveleti terület a szárazföld, a tenger, a légtér és a világűr mellett: az uniós missziók és műveletek végrehajtásának sikere egyre nagyobb mértékben függ a biztonságos kibertérhez való zavartalan hozzáféréstől, ezért szilárd és ellenálló kiberműveleti képességeket igényel."[7]

Az ENSZ normaalkotó szerepe

A különböző nemzetközi, regionális és nemzeti szereplők által javasolt stratégiák, a nemzetközi megállapodások, valamint a kiberbiztonsággal foglalkozó egyéb kezdeményezések jelentősen eltérhetnek terjedelmükben, céljukban és sikereikben, de mind a kibertér nemzetközi dimenzióját hangsúlyozzák. Így nem véletlen, hogy az ENSZ leszereléssel és nemzetközi biztonsággal foglalkozó Első Bizottsága *(UN First Committee, Disarmament and International Security)* évtizedek óta aktívan vizsgálja az információ és a telekommunikáció terén elért fejleményeket a nemzetközi biztonság összefüggésében. Az ENSZ a kilencvenes évek vége óta foglalkozik az információs és kommunikációs technológiák biztonságával összefüggő kérdésekkel. 2004 óta összesen hat, az ENSZ Közgyűlésének Első Bizottsága által felállított Kormányzati Szakértői Csoport (*Group of Governmental Expert* – GGE) vizsgálta az IKT-k használatával összefüggő veszélyeket. A Genfben és New Yorkban ülésező szakértői csoportok

[5] Anna-Maria Talihärm: *Towards Cyberpeace: Managing Cyberwar Through International Cooperation.* United Nations, 2013. augusztus.

[6] Fekete-Karydis Klára – Lázár Bence: A kibervédelem katonai dimenziói. *Honvédségi Szemle,* 148. (2020), 3. 47.

[7] Az Európai Unió Tanácsa: *Uniós kibervédelmi szakpolitikai keret (2018. évi naprakésszé tett változat).* Brüsszel, 2018. november 19. (OR. en) 14413/18. 2.; Molnár Anna – Szabolcs Laura: Megerősített együttműködés, változó geometria, PESCO. *Hadtudomány,* 30. (2020), 4. 77–106.

munkája az államok kibertérben megvalósuló állami viselkedési normáinak vizsgálatára, a nemzetközi jog IKT-területen történő alkalmazására és a bizalomépítő intézkedések előmozdítására összpontosított. A csoportok munkájának köszönhetően több fontos jelentés is született. A 2012–2013-as GGE-jelentés fontosságát az adta, hogy a nemzetközi jog kibertérben történő alkalmazását hangsúlyozta. Emellett kiállt az IKT és a kritikus infrastruktúrák védelme érdekében megvalósított tevékenységek területén az állami szuverenitás megerősítése mellett. A 2015-ös jelentés nem kötelező jellegű ajánlásokat fogadott el az állami magatartás nemzetközi jogi normáinak és a bizalomépítő intézkedések előmozdítása érdekében. A következő években a viták elsősorban a nemzetközi humanitárius jog (*international humanitarian law* – IHL) és a nemzetközi emberi jogi normák (*international human rights law* – IHRL) köré csoportosultak, a tárgyalások viszont – elsősorban a nyugati szövetségesek és Oroszország közötti viták miatt – elakadtak. 2017-ben a szakértői csoport végül nem tudott megegyezni egy konszenzusos jelentés megalkotásáról. A viták mélységét jól mutatja, hogy 2018-ban Antonio Guterres ENSZ-főtitkár egy beszédében hangsúlyozta: „Az államok közötti kiberhadviselés elemei már léteznek. A legroszszabb az, hogy az ilyen típusú hadviselésnek nincs szabályozási rendszere, nem világos, hogy a genfi egyezmény vagy a nemzetközi humanitárius jog hogyan vonatkozik rá."[8]

2018-ban a vitás kérdések tárgyalása érdekében az ENSZ Közgyűlése két új folyamatot indított el. A 2019 és 2021 közötti időszakban a Nyílt végű Munkacsoport (*Open-ended Working Group* – OEWG) és a Kormányzati Szakértői Csoport ülésezett. Mindkét csoport 2021 tavaszán fejezte be a munkát, és publikálta jelentéseit.[9] A OEWG 2019/2020 feladata volt az államok felelős magatartási szabályainak, normáinak és alapelveinek továbbfejlesztése, a végrehajtásuk módjának megvitatása, valamint az ENSZ égisze alatt széles körű részvétellel folytatott rendszeres intézményi párbeszéd kialakításával kapcsolatos lehetőségének tanulmányozása.[10]

A UN GGE 2019–2021-es konszenzusos jelentése a nemzetközi jog kibertérben történő alkalmazására vonatkozó alapelveket fogadott el. A jelentés kiemelte

[8] Digwatch (2021): i. m.

[9] Reaching Critical Will: *Information and communications technology (ICT)* (é. n.); Molnár Dóra: Nagyhatalmi kiberdiplomácia – az Egyesült Államok, Kína és Oroszország a nemzetközi kiberporondon. In Török Bernát (szerk.): *Információ- és kiberbiztonság.* Budapest, Ludovika Egyetemi Kiadó, 2020. 357–373.

[10] UNGA: *Resolution adopted by the General Assembly on 5 December 2018.* A/RES/73/27.

a kritikus infrastruktúrákkal – ideértve a kritikus információs és a lakosság számára alapvető szolgáltatásokat nyújtó infrastruktúrákat, az internet széles körű elérhetőségéhez szükséges infrastruktúrákat és az egészségügy működéséhez szükséges kapacitásokat – szemben alkalmazott káros IKT-tevékenységek jelentette fenyegetéseket. A 2019-es jelentés megerősíti az állami magatartás 2015-ben megalkotott nem kötelező jellegű nemzetközi jogi normáit. A dokumentum hangsúlyozza, hogy a kialakított normák nem kívánják korlátozni vagy megtiltani a nemzetközi joggal egyébként összhangban álló cselekvéseket. A normák tükrözik a nemzetközi közösség elvárásait, és meghatározzák a felelős állami magatartás szabályait. A jelentés megerősíti a nemzetközi jog és különösen az ENSZ Alapokmányának teljes alkalmazhatóságát az IKT-környezetre is. A jelentés hangsúlyozza, hogy az ENSZ Alapokmánya teljes egészében alkalmazandó, és felsorolja annak alapelveit. A GGE 2019/2021 jelentés szerint ebben az esetben a nemzetközi humanitárius jog csak fegyveres konfliktusok esetén alkalmazandó. Ez a megállapítás lényeges, hiszen a korábbi GGE-jelentések és az OEWG 2021-es jelentése nem jutott konszenzusra a kérdésben. A jelentés fontosnak tartja a nemzetközi jogi elvek (ideértve az emberiesség, a szükségesség, az arányosság és a megkülönböztetés alapelvét) alkalmazásának további vizsgálatát az IKT-k területein. A dokumentum azonban nem tesz javaslatot arra, hogy mely fórumok végezzék el ezt a vizsgálatot, noha szorgalmazza az ENSZ égisze alatti és más nemzetközi szervezetek keretein belüli, illetve a bi- vagy multilaterális tárgyalások folytatását.[11] A nemzetközi humanitárius jog alkalmazásáról szóló vitával kapcsolatban érdemes megemlíteni Tilman Rodenhäuser, a Nemzetközi Vöröskereszt nemzetközi humanitárius joggal és kiberhadviseléssel foglalkozó szakértőjének véleményét. Szerinte a nemzetközi humanitárius jog egyértelműen korlátozza a kiberműveleteket a fegyveres konfliktusok során, ugyanúgy, mint bármely (új vagy régi) fegyver, eszköz és módszer használatát. Ennek oka, hogy például egy modern kórház működésében nem csupán a hagyományos fegyverek, hanem egy kibertámadás is jelentős, akár emberéleteket követelő károkat okozhat.[12]

Ezt követően a 2021 és 2025 közötti időszakra újabb Nyílt végű Munkacsoport munkája kezdődött el.[13] Az ENSZ napjainkban is a vitás kérdések rendezésére szolgáló elsődleges és meghatározó fórum szerepét tölti be.

[11] Andrijana Gavrilović: What's New With Cybersecurity Negotiations? The UN GGE 2021 Report. *Diplo,* 2021. június 6.

[12] International Committee of the Red Cross: *Cyber Warfare: does International Humanitarian Law apply?* (2021. február 25.).

[13] Digwatch (2021): i. m.

NATO

Noha a NATO kezdetektől jelentős figyelmet fordított a kommunikációs és információs rendszereinek védelmére, csupán a 2002. évi prágai csúcstalálkozó foglalkozott először a kibervédelemmel politikai napirendjei között. A szövetség vezetői a 2006-os rigai csúcstalálkozón megerősítették az információs rendszerek védelmének szükségességét. Az észt állami és magánintézmények elleni 2007-es kibertámadásokat követően a szövetséges védelmi miniszterek egyetértettek az új kihívásokkal kapcsolatos sürgető feladatok megvalósításában. Ennek eredményeként a NATO 2008 januárjában jóváhagyta első kibervédelmi politikáját *(Policy on Cyber Defence).* 2008 nyarán az Oroszország és Grúzia közötti konfliktus ismét bebizonyította, hogy e területen további együttműködés és képességfejlesztés szükséges. Még ebben az évben létrejött a Szövetség kiválósági központjainak egyike, a tallinni székhelyű NATO Kooperatív Kibervédelmi Kiválósági Központ (*Cooperative Cyber Defence Centre of Excellence* – CCDCE).[14] A NATO folyamatosan alkalmazkodott a változó kihívásokhoz. Az adaptációs folyamatot gyorsította, hogy az USA az európai szövetségeseket megelőzve fejlesztette védelmi és támadó jellegű kiberképességeit.[15]

A NATO a 2010-es lisszaboni csúcstalálkozón új stratégiai koncepciót fogadott el. A csúcstalálkozó az Észak-atlanti Tanács (NAC) feladatául tűzte ki egy mélyreható kibervédelmi politika kidolgozását és annak végrehajtására cselekvési terv elkészítését. 2011 júniusában a NATO védelmi miniszterei jóváhagyták a második kibervédelmi politikát, amely a gyorsan változó fenyegetettség és a technológiai környezet összefüggésében vázolta fel a kibervédelem összehangolt erőfeszítéseit, és a végrehajtásra vonatkozó cselekvési terv is elkészült. 2012 áprilisában a kibervédelem a NATO védelmi tervezési folyamatába is bekerült.[16] A felkészülést segítette, hogy a tallinni kiválósági központ keretein belül 2009-től egy szakértői csoport megkezdte a nemzetközi háborús jog *(jus ad bellum)* és a nemzetközi humanitárius jog alkalmazásának vizsgálatát egy lehetséges kiberkonfliktus vagy -háború esetében. A szakértői munka eredményképpen 2013-ban elkészült *A kiberháborúra alkalmazandó nemzetközi jog tallinni kézikönyve,* az úgynevezett

[14] NATO: *Cyber Defence.* 2021a.

[15] Joe Burton: NATO's Cyber Defence: Strategic Challenges and Institutional Adaptation. *Defence Studies,* 15. (2015), 4. 297–319.

[16] NATO (2021a): i. m.

Tallinni kézikönyv.[17] A nem kötelező jellegű dokumentum jelentős szerepet játszik a nemzetközi jogi vitás kérdések tisztázásában.

A 2012. májusi chicagói csúcstalálkozón a tagállamok állam- és kormányfői megerősítették elkötelezettségüket a szövetség kibervédelmének javítása mellett. Célul tűzték ki, hogy a NATO hálózatát központosított védelem alá helyezik. 2012 júliusában a NATO ügynökségeinek reformja során létrehozták a NATO Kommunikációs és Információs Ügynökségét (*NATO Communications and Information Agency* – NCIA). 2014 februárjában a szövetséges védelmi miniszterek egy új, fokozott kibervédelmi politika kidolgozásáról döntöttek. Az új politikai keret magában foglalta a kollektív védelem, a szövetségeseknek nyújtott segítség, az egyszerűsített kormányzás, a jogi megfontolások és az iparral fenntartott kapcsolatok területeit is.[18] A döntések jelentőségét elsősorban az adta, hogy ekkor határozták el először, hogy a Szövetség egy tagja elleni kibertámadás kollektív válaszadást igényel. Az új feladatokkal kapcsolatos nehézséget kezdetben elsősorban az okozta, hogy a kibertérben a támadás forrásának azonosítása jóval nehezebb, mint a valóságos térben.[19]

A szövetségesek a 2014. szeptemberi wales-i csúcstalálkozón jóváhagyták az új kibervédelmi politikát, és elfogadtak egy cselekvési tervet, amely a Szövetség alapfeladatainak teljesítését segíti. A kibervédelmet elismerték a NATO kollektív védelmi feladatának részeként, és egyetértettek abban, hogy a kibertérben a nemzetközi jog alkalmazandó.[20]

2016-ban a NATO és az EU technikai megállapodást kötött a kibervédelemről. 2016-ban a szövetséges védelmi miniszterek megállapodtak abban, hogy a varsói NATO-csúcstalálkozón a kiberteret műveleti területként ismerik el. A Szövetség ugyanakkor üdvözölte a más nemzetközi fórumokon tett erőfeszítéseket a felelős állami magatartás normái és a bizalomépítő intézkedések kidolgozására az átláthatóbb és stabilabb kibertér elősegítése érdekében.[21]

A szövetséges állam- és kormányfők a 2016. júliusi varsói csúcstalálkozón megerősítették a NATO védelmi feladatát, és a kiberteret olyan műveleti területnek

[17] Michael N. Schmitt (szerk.): *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge, Cambridge University Press, 2013; Iain Sutherland et al.: The Geneva Conventions and Cyber-Warfare. *The RUSI Journal,* 160. (2015), 4. 30–39.

[18] NATO (2021a): i. m.

[19] Burton (2015): i. m.

[20] Elie Perot: The Art of Commitments: NATO, the EU, and the Interplay Between Law and Politics Within Europe's Collective Defence Architecture. *European Security,* 28. (2019), 1. 40–65.

[21] NATO (2021a): i. m.

ismerték el, amelyben a NATO-nak ugyanolyan hatékonyan kell védekeznie, mint a levegőben, a szárazföldön és a tengeren. A szövetségesek kibervédekezésre tett kötelezettségvállalásuk mellett prioritásként fokozták a nemzeti hálózataik és infrastruktúráik kibervédelmét, és elköteleződtek amellett is, hogy gyorsan és hatékonyan reagálnak a kibertámadásokra, beleértve a hibrid kampányokat is.[22]

2017 februárjában a szövetséges védelmi miniszterek jóváhagytak egy frissített kibervédelmi akciótervet, valamint ütemtervet a kibertér mint műveleti terület megvalósítására. A miniszterek megállapodtak abban is, hogy lehetővé teszik a szövetségesek nemzeti kiber-hozzájárulásainak integrálását a szövetség műveleteibe és misszióiba.[23] 2017 decemberében a NATO és az EU miniszterei megállapodtak a két szervezet közötti együttműködés fokozásáról számos területen, ideértve a kiberbiztonságot és a kibervédelmet is. 2017-ben a tallinni kiválósági központ keretein belül megszületett a *Tallinni kézikönyv 2.0,* amely elsősorban a napi rendszerességgel megvalósuló kiberincidensek esetében alkalmazandó nemzetközi jog területeit vizsgálta.[24]

A szövetséges vezetők a 2018-as brüsszeli csúcstalálkozón megállapodtak egy új kibertérműveleti központ felállításáról a NATO megerősített parancsnoki struktúrájának részeként. A cél a NATO kibervédelmének megerősítése és a kiberterület integrálása a NATO tervezésébe és műveleteibe minden szinten. A szövetségesek abban is egyetértettek, hogy a NATO missziói és műveletei során felhasználhatja a nemzeti kiberképességeket. A szövetségesek számba vették a nemzeti ellenállóképesség fokozása érdekében tett lépéseiket.[25]

2019 februárjában a NATO védelmi miniszterei jóváhagyták az új útmutatót, amely a NATO képességeit megerősítő eszközöket tartalmaz a jelentős rosszindulatú kiberaktivitások esetére.[26]

A NATO-nak minden rendelkezésére álló eszközt fel kell használnia, beleértve a politikai, diplomáciai és katonai intézkedéseket is, a kiberfenyegetések leküzdésére. Az útmutatóban felvázolt válaszlehetőségek segíteni fogják a NATO-t és szövetségeseit abban, hogy fokozzák a kibertérben zajló helyzettel

[22] 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.).

[23] NATO (2021a): i. m.

[24] NATO CCDCOE: *The Tallinn Manual.* Tallinn, 2021; Michael N. Schmitt (szerk.): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge, Cambridge University Press, 2017.

[25] NATO (2021a): i. m.

[26] Laura Brent: *NATO's Role in Cyberspace*. NATO, 2019. február 12.

kapcsolatos tudatosságukat, növeljék ellenállóképességüket, és a partnerekkel együttműködve elrettentsék, kivédjék és ellensúlyozzák a kiberfenyegetések teljes spektrumát.[27]

Az Észak-atlanti Tanács 2020. június 3-án nyilatkozatot adott ki, amelyben elítélte a koronavírus-járvány összefüggésében zajló destabilizáló és rosszindulatú kibertevékenységeket. A nyilatkozatban a szövetségesek szolidaritását és kölcsönös támogatását fejezte ki azok számára, akik e rosszindulatú kibertevékenységek következményeit elszenvedik, beleértve az egészségügyi szolgáltatásokat, a kórházakat és a kutatóintézeteket. A nyilatkozat felszólította továbbá a nemzetközi jog és a felelős állami magatartás normáinak betartását a kibertérben.[28]

2021-ben a tallinni kiválósági központ keretein belül megkezdődött a *Tallinni kézikönyv 3.0* kidolgozása. Az ötéves projekt célja a meglévő fejezetek átdolgozása és a tagállamok számára fontos új témák vizsgálata.[29] A 2021. júniusi brüsszeli csúcstalálkozón a szövetségesek tudomásul vették a változó fenyegetettséget, és új átfogó kibervédelmi politikát fogalmaztak meg a NATO három alapvető feladatának, a kollektív védelemnek, a válságkezelésnek és a kooperatív biztonságnak a támogatására. A döntéseknek megfelelően a NATO-nak mindenkor – békeidőben, válságban és konfliktusok idején is, valamint politikai, katonai és technikai szinten is – aktívan el kell hárítania a kiberfenyegetések teljes spektrumát, védekeznie kell ellenük, és szembe kell néznie velük.[30]

Az Európai Unió[31]

Az EU első átfogó kiberbiztonsági stratégiájának kidolgozására 2013-ban került sor.[32] E dokumentum említette először az EU nemzetközi kiberbiztonsági politikáját és kibervédelmi céljait. A NATO hasonló stratégiáival összehasonlítva

[27] NATO (2021a): i. m.
[28] NATO (2021a): i. m.
[29] CCDCOE (2021): i. m.
[30] NATO (2021a): i. m.
[31] Az Európai Unió kiberbiztonsági politikájának fejlődéséről részletesebben lásd Molnár Dóra: Egységes európai kibertér? Az Európai Unió kiberbiztonsági politikájának fejlődése. *Hadmérnök,* 12. (2017), 1. 255–267.
[32] Európai Bizottság: *Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér.* JOIN/2013/01 final. 2013.

(2008, 2011) az uniós dokumentum nem csupán a saját informatikai hálózatának védelmére szorítkozott, hanem szinte minden uniós kompetenciába tartozó területre – az egységes piactól a külső és belső biztonság kérdéseiig – kiterjedt.[33] Míg a NATO kezdetektől inkább a keményebb stratégiai eszközök elfogadását tartotta fontosnak, addig az EU a puha szakpolitikai keret megvalósítására összpontosított.[34] A kiberbiztonság területe csak fokozatosan vált védelmi jellegű kérdéssé.[35]

A 2013-as stratégia az EU nemzetközi kiberpolitikájával kapcsolatos céljait is meghatározta. Az új szakpolitika a szabad és nyitott internet védelme mellett célul tűzte ki a felelősségteljes állami magatartás nemzetközi jogi normáinak és a bizalomépítő intézkedések előmozdítását a kibertérben és az EU stratégiai partnereivel történő együttműködés javítását. Az uniós kiberdiplomácia részeként számos nagyhatalommal tárgyalások kezdődtek a kibertérben zajló nemzetközi biztonság, az ellenállóképesség, a kiberbűnözés elleni fellépés és az internet szabályozása érdekében. E folyamatokkal párhuzamosan az Európai Unión belüli, kiberbiztonsággal összefüggő diplomáciai eszköztár megerősítése is szükségessé vált, és egyre intenzívebb lett e terület szabályozási folyamata.

Az EU 2016-os globális stratégiája a kiberdiplomáciával kapcsolatos alapvető célokat is megfogalmazta.[36] Az unió 2016-ban meghozta az első kiberbiztonságra vonatkozó uniós jogi aktust, a hálózati és információs rendszerek biztonságáról szóló irányelvet (NIS).[37] Az Európai Bizottság irányításával 2017-ben elkészült az EU új, felülvizsgált kiberbiztonsági stratégiája.[38]

Az unió érdekeinek átfogó védelme érdekében 2017-ben az EU Tanácsa megállapodott arról, hogy az állami és nem állami szereplők részéről mutatkozó rossz szándékú és tudatos kibertevékenységekkel szembeni közös uniós diplomáciai intézkedések keretét, az úgynevezett kiberdiplomáciai eszköztárat *(EU Cyber-diplomacy Toolbox)* kidolgozza. Az új eszköztár az EU közös kül- és bizton-

[33] Jochen Rehrl (szerk.): *Handbook on cyber security. The Common Security and Defence Policy of the European Union.* Directorate for Security Policy of the Federal Ministry of Defence of the Republic of Austria, 2018. 18.

[34] Burton (2015): i. m.

[35] James Sperling – Mark Webber: The European Union: security governance and collective securitisation. *West European Politics,* 42. (2019), 2. 228–260.

[36] Európai Külügyi Szolgálat: *Közös jövőkép, közös fellépés: Erősebb Európa. Globális stratégia az Európai Unió kül- és biztonságpolitikájára vonatkozóan.* 2016. 35.

[37] Eur-lex: *Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve* (2016. július 6.).

[38] Európai Bizottság: *Közös közlemény az Európai Parlamentnek és a Tanácsnak: Az „Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése".* Brüsszel, 2017. szeptember 13. JOIN(2017) 450 final.

ságpolitikai eszköztárára támaszkodik. A tanácsi döntéssel összhangban azon információs és kommunikációs technológiák (IKT) felhasználásával végrehajtott tevékenységekkel szemben, amelyek kimeríthetik a nemzetközi jogot sértő cselekmény fogalmát, az EU kész a közös kül- és biztonságpolitikai intézkedésekkel, ideértve a korlátozó, esetleg szankciós intézkedéseket is, fellépni.[39] Döntés született arról is, hogy az alkalmazott intézkedéseknek – a nemzetközi joggal összhangban – arányosnak kell lenniük a rossz szándékú kibertevékenységgel. Az EU egyúttal megerősítette, hogy „elkötelezett a kibertérben folyó nemzetközi viták békés úton történő rendezése mellett".[40]

A Politikai és Biztonsági Bizottság 2017. október 11-én a kiberdiplomáciai eszköztárra vonatkozóan végrehajtási iránymutatásokat fogadott el. A dokumentum a kiberdiplomáciai eszköztáron belül *öt intézkedéskategóriát* sorolt fel: *1.* a megelőző intézkedéseket, *2.* az együttműködési intézkedéseket, *3.* a stabilitást szolgáló intézkedéseket, *4.* a korlátozó intézkedéseket és *5.* a lehetséges uniós támogatást a tagállamok jogszerű válaszaihoz. A dokumentum tartalmazza az ezen intézkedések bevezetésére vonatkozó eljárást is.[41] A lehetséges uniós támogatások között a dokumentum a lisszaboni szerződés kölcsönös segítségnyújtási klauzuláját (42.7 cikk) is megemlíti.[42] E klauzula alkalmazásának lehetősége az EU kollektív védelmi jellegét erősíti a kiberbiztonság területén is.

A 2018-as kibervédelmi szakpolitikai keret szerint a korábbi évek eseményei még inkább rávilágítottak arra a tényre, hogy a nemzetközi közösségnek együtt kell működnie a konfliktusok megelőzése és a kibertér stabilitásának erősítése érdekében.

> „Az EU más nemzetközi szervezetekkel, elsősorban az ENSZ-szel (Egyesült Nemzetek Szervezete), az EBESZ-szel (Európai Biztonsági és Együttműködési Szervezet) és az ASEAN (Délkelet-ázsiai Nemzetek Szövetsége – Association of Southeast Asian Nation) regionális fórummal együtt elő kívánja mozdítani egy olyan, a konfliktusmegelőzésre, az együttműködésre és a kibertér stabilitásának erősítésére vonatkozó stratégiai keretet, amely magában foglalja a következőket: a nemzetközi jognak és különösen

[39] Az Európai Unió Tanácsa: *Informatikai támadások: az EU készen áll az ellenintézkedésekre, ideértve a szankciókat is.* 2017.

[40] Európai Unió Tanácsa (2017): i. m.

[41] Council of the European Union: *Draft Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities – Approval of the Final Text.* Brussels, 2017b. október 9. (OR. en); A Tanács (KKBP) 2019/797 határozata (2019. május 17.) az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről.

[42] Európai Unió Tanácsa (2017): i. m.

> az ENSZ Alapokmányának teljes körű alkalmazása a kibertérben; a kibertérben tanúsított felelősségteljes állami magatartásra vonatkozó egyetemes, nem kötelező erejű normák, szabályok és elvek tiszteletben tartása; regionális bizalomépítő intézkedések kidolgozása és végrehajtása. Ezt a törekvést az uniós kibervédelmi szakpolitikai keretnek is támogatnia kell."[43]

2019-ben az EU jelentős előrehaladást ért el a rossz szándékú kibertevékenységekkel szembeni közös uniós kiberdiplomáciai eszköztár működőképessé és hatékonnyá tétele érdekében. Az Európai Tanács 2018. júniusi és 2018. októberi következtetéseiben megfogalmazott célok elérése érdekében olyan uniós korlátozó intézkedések bevezetéséről döntött, amelyek segítik a kibertámadásokkal kapcsolatos reagálási és elrettentési képesség javítását. 2019. május 17-én döntés született az uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről szóló KKBP-határozatról[44] és a tanácsi rendeletről.[45] A határozat a rossz szándékú és szándékos kibertevékenységekkel szembeni közös uniós korlátozó intézkedések alkalmazhatóságáról döntött, a rendelet pedig a jelentős hatású kibertámadások esetén szankciók alkalmazását teszi lehetővé az EU részéről.

Az új jogi keret így már lehetővé tette az EU számára, hogy szankciókat is kivethessen (például eszközök befagyasztása, utazási tilalom) az unióra vagy a tagállamaira külső fenyegetést jelentő kibertámadásoktól való elrettentés, valamint az azokra való reagálás érdekében.[46] A szankcióknak hatékonynak, arányosnak és visszatartó erejűnek kell lenniük (A Tanács [EU] 2019/796 rendelete 15. cikk). 2019-ben megszületett az EU új kiberbiztonsági jogszabálya, illetve megújult az Európai Uniós Kiberbiztonsági Ügynökség, az ENISA, és kibővült a hatásköre.[47]

2020 decemberében elkészült az Európai Bizottság és az Európai Külügyi Szolgálat új uniós kiberbiztonsági stratégiája. A stratégia célja a kiberfenyegetésekkel szembeni ellenállóképesség megerősítése, valamint a polgárok

[43] Az Európai Unió Tanácsa (2018): i. m. 8.

[44] A Tanács (KKBP) 2019/797 határozata… i. m.

[45] A Tanács (EU) 2019/796 rendelete… i. m.

[46] Európai Bizottság: *Jelentés a dezinformációval szembeni közös cselekvési terv végrehajtásáról. Közös közlemény az Európai Parlamentnek, az Európai Tanácsnak, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának*. Brüsszel, 2019. június 14. JOIN (2019) 12 final, 9.

[47] Council of the European Union: *Cybersecurity in Europe: stronger rules and better protection.* 2020.

és a vállalkozások számára megbízható szolgáltatások és digitális eszközök biztosítása.[48] A stratégia hangsúlyozza, hogy az EU hatékony diplomáciai reagálásához szilárd, közös helyzetismeretre és a közös uniós álláspont gyors előkészítésére van szükség. Az unió külügyi és biztonságpolitikai főképviselője ösztönzi a tagállamok kiberfenyegetésekkel és -tevékenységekkel kapcsolatos stratégiai hírszerzési együttműködését. Annak érdekében, hogy az EU megakadályozza, elriassza és reagáljon a virtuális térben történő rosszindulatú tevékenységekre, a főképviselő a Bizottság bevonásával javaslatot terjeszt elő az EU számára, hogy meghatározza a kiberelrettentési képességeit. Az EU-nak további erőfeszítéseket kell tennie a nemzetközi partnerekkel, köztük a NATO-val való együttműködés megerősítése érdekében a fenyegetettség közös megértésének előmozdítása, az együttműködési mechanizmusok kidolgozása és az együttműködő diplomáciai válaszok meghatározása érdekében. Ezenkívül az EU-nak tovább kell integrálnia a kiberdiplomácia eszköztárát az EU válságmechanizmusaiba, szinergiákat kell keresnie a hibrid fenyegetések, a dezinformációk és a külföldi beavatkozások elleni küzdelemre irányuló erőfeszítésekkel. Az EU-nak tükröznie kell a kiberdiplomáciai eszköztár és az EUSZ 42. cikk (7) és (EUMSZ) 222. cikk közötti lehetséges kölcsönhatásokat.[49]

A Tanács a 2021. márciusi, a kiberbiztonsági stratégiáról szóló következtetéseiben hangsúlyozta, hogy a kiberbiztonság alapvető fontosságú a reziliens, zöld és digitális Európa építéséhez. Az uniós miniszterek a nyitott gazdaság megőrzése mellett a stratégiai autonómia megvalósítását is célul tűzték ki annak érdekében, hogy az EU a kiberbiztonság területén autonóm döntéseket hozhasson.[50]

Az EU–NATO-együttműködés

Noha a NATO továbbra is a kollektív védelem elsődleges szervezete a szövetségesek számára, az EU is fontos szerepet tölthet be egy jelentős kibertámadás esetén.

[48] European Commission (2020): *Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade.* Brussels, 2020. december 16. JOIN(2020) 18 final.

[49] European Commission (2020): i. m. 16–17.

[50] Az Európai Unió Tanácsa: *A Tanács következtetései a digitális évtizedre vonatkozó uniós kiberbiztonsági stratégiáról.* Brüsszel, 2021. március 9. (OR. en) 6722/21.

Az európai szövetségesek a NATO 5. cikke vagy az EUSZ 42.7 cikke (mint „fegyveres támadás/agresszió") keretében vagy az EU működéséről szóló szerződés 222. cikke (szolidaritási klauzula) keretei között (mint „terrortámadás") nyújthatnak segítséget egymásnak. Az EUMSZ 222. cikkével összefüggésben az EU 2013. évi kiberbiztonsági stratégiája szerint egy különösen súlyos számítógépes esemény vagy támadás elegendő feltétele, hogy egy tagállam az EU szolidaritási záradékára hivatkozhasson. A NATO 5. cikkével kapcsolatban a Szövetség walesi csúcstalálkozója döntött. Ennek megfelelően egy kibertámadás „fegyveres támadásnak" minősülhet.[51] Az EU 2017-es kiberdiplomáciai eszköztára a lisszaboni szerződés kölcsönös segítségnyújtási klauzuláját (42.7 cikk) is megemlíti a válaszadási lehetőségek között.

A NATO és az EU közötti intenzívebb kapcsolatok kiépítésére a 2010-es évektől került sor. A 2015-ös kiberdiplomáciáról szóló tanácsi következtetésekkel összhangban az EU a legfontosabb partnerekkel és a nemzetközi szervezetekkel stratégiai együttműködést kíván kialakítani, és hangsúlyozza, hogy a kibertérrel kapcsolatos kérdésekben hozott szakpolitikai döntések többsége szükségessé teszi az aktív nemzetközi párbeszédet, együttműködést és koordinációt.[52] Mindezzel összefüggésben a NATO-val kiépített kapcsolatok jelentősége is fokozatosan növekedett.

Az EU és a NATO közötti együttműködés területén kialakított folyamat valódi lendületet 2016-tól kapott. Az EU globális stratégiájának elfogadását követő végrehajtási folyamatban a két nemzetközi biztonsági szervezet között a kiberbiztonság és kibervédelem területén egyre intenzívebb kapcsolat jött létre.[53] A globális stratégia hangsúlyozta, hogy míg a NATO a kollektív védelem elsődleges keretét biztosítja a legtöbb tagállam számára, addig az EU elsősorban az olyan belső és külső kihívásokkal szemben kíván fellépni, mint a terrorizmus, a hibrid fenyegetések, a kiber- és energiabiztonság, a szervezett bűnözés és a külső határok igazgatása.

2016. július 8-án a NATO-csúcson Varsóban az EU részéről az Európai Tanács elnöke és az Európai Bizottság elnöke, illetve a NATO főtitkára együttes nyilatkozatot írt alá az EU és a NATO közötti együttműködésről. A nyilatkozat aláírását követően a két szervezet közötti együttműködés új lendületet kapott,

[51] Perot (2019): i. m.

[52] Az Európai Unió Tanácsa: *A Tanács következtetései a kiberdiplomáciáról.* Brüsszel, 2015. február 11.

[53] Európai Külügyi Szolgálat (2016): i. m.

és kiterjed a hibrid fenyegetések elleni küzdelemre, a kiberbiztonság és -védelem területeire is.[54] Az együttes nyilatkozat konkrét célkitűzéseket fogalmazott meg a kibervédelmi együttműködés előmozdítása érdekében: a kibervédelmi interoperabilitás megerősítése a missziók és a műveletek során; az együttműködés erősítése a képzéseken és a gyakorlatokon; a kibervédelmi kutatásokkal és technológiai innovációval kapcsolatos együttműködés előmozdítása; valamint a kibernetikus szempontok beépítése a válságkezelésbe.[55]

2016 februárjában az EU és a NATO képviselői aláírták az EU hálózatbiztonsági vészhelyzeteket elhárító csoportja (*Computer Emergency Response Teams* – CERT) és a NATO hálózatbiztonsági incidenskezelő csoportja (*NATO's Computer Incident Response Capability* – NCIRC) közötti technikai megállapodást. A megállapodás célja a technikai információk megosztásának megkönnyítése a számítógépes események megelőzése érdekében, illetve a kiberbiztonsági események felderítése és az azokra való reagálás erősítése mindkét szervezetben. Az e területeken megvalósuló tevékenységek mind a mai napig a két szervezet közötti együttműködés alapját képezik.

Az együttműködés másik legfontosabb eredménye, hogy – finn kezdeményezésre, de az EU és a NATO támogatásával – 2017-ben Helsinkiben létrejöhetett a Hibrid Fenyegetések Elleni Kiválósági Központ *(European Centre of Excellence for Countering Hybrid Threats),* amelynek feladata az elsősorban Oroszország felől érkező kiberbiztonsági kihívások, a dezinformációs műveletek és a stratégiai kommunikáció elemzése, valamint a kihívásokra hatékony és közösen koordinált válaszok kidolgozása.[56] Az új központ felállítása lehetőséget biztosított az Észak-atlanti Tanács és az uniós Politikai és Biztonsági Bizottság közötti informális találkozók megszervezésére, és így a hibrid fenyegetéssel szembeni koordinált fellépés kidolgozására.[57]

A NATO és az EU közötti együttműködést vizsgáló 2017. novemberi második előrehaladási jelentésben első helyen szerepelt az új központ felállítása. A jelentés emellett kiemelte a kiberbiztonsági és a védelmi fejlesztés területén elért eredményeket, illetve ezek közül a képzések és gyakorlatok területén megvalósuló

[54] Az Európai Unió Tanácsa: *EU–NATO együttműködés: A Tanács következtetéseket fogadott el az együttes nyilatkozat végrehajtása céljából.* 2016.

[55] Council of the European Union: *Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organisation.* 2016.

[56] Hybrid CoE: *European Centre of Excellence for Countering Hybrid Threats.* (É. n.)

[57] Hybrid CoE: Hybrid CoE Supports Informal NAC-PSC Discussion. 2018. szeptember 28.

együttműködések fontosságát. A NATO-alkalmazottak például részt vehettek az uniós ügynökség, az ENISA (*European Union Agency for Cybersecurity,* Európai Uniós Kiberbiztonsági Ügynökség) kiberbiztonsági gyakorlatán. Ezt követően a fejlesztési duplikációk elkerülése érdekében folyamatossá vált az együttműködés.[58]

2017-ben és 2018-ban a NATO és az Európai Unió párhuzamos és összehangolt gyakorlatokat folytatott egy hibrid forgatókönyvre reagálva, annak érdekében, hogy javítsák az EU válaszadási képességét a hibrid fenyegetés esetén, és továbbfejlesszék az EU és a NATO közötti együttműködést. 2017-ben NATO-irányítással, 2018-ban pedig az unió vezetésével hajtották végre a gyakorlatokat. A 2018-as „EU-HEX-ML 18 (PACE)" gyakorlat jelentősen segítette a szervezetek személyi állománya közötti együttműködést.[59] 2017-ben a Tallinnban szervezett közös kibergyakorlat során a NATO és az EU tisztviselői a NATO 5. cikkének vagy az EUSZ 42.7 cikknek az aktiválást is tárgyalták.[60] 2019-ben a jól bevált gyakorlat folytatódott, és a NATO CMX 19 gyakorlat is kiterjedt a személyi állományok közötti együttműködésre az EU intézményeivel (EKSZ, EK és a Tanács).[61]

A 2021-es hatodik előrehaladási jelentés hangsúlyozta, hogy az EU és a NATO személyzete rendszeres kapcsolatot és információcserét tartott fenn az egyes kibertevékenységekkel kapcsolatban. Az együttműködés a koronavírus-járvány idején is hatékonynak bizonyult. 2021 májusában az EU Integrated Resolve 20 (EU IR20) gyakorlat keretében is folytatódott a személyi állományok közötti együttműködés. Az EU és a NATO kiberbiztonsági és védelmi személyzetének éves megbeszéléseit 2021 januárjában tartották, és lehetőséget kínáltak az aktuális szakpolitikai fejlemények és prioritások aktualizálására, egyúttal felmérve a további együttműködés lehetőségeit.[62]

[58] Council of the European Union: *Second Progress Report on the Implementation of the Common Set of Proposals Endorsed by NATO and EU.* 2017a.

[59] European External Action Service: *Crisis Preparedness: EU Launches Civil-Military Crisis Management Exercise.* Bruxelles, 2018. november 16. – 15:25, UNIQUE ID: 181116_7.

[60] Perot (2019): i. m.

[61] George Allison: NATO Conducts Crisis Management Exercise. *UK Defence Journal,* 2019. május 9.

[62] NATO: *Sixth Progress Report on the Implementation of the Common Set of Proposals Endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017.* 2021b. június 3. 5–6.; Molnár Anna: A kiberdiplomácia fejlődése az Európai Unióban. In Molnár Anna – Molnár Dóra (szerk.): *Kiberdiplomácia.* Budapest, Ludovika Egyetemi Kiadó, 2022. 55–71.

Következtetések

A 2000-es évek elejétől az ENSZ meghatározott szerepet játszott a kiberhadviseléssel kapcsolatos nemzetközi jogi viták rendezése és a jogi normák megalkotása területén. 2007 után, az észt magán- és közintézmények, illetve infrastruktúra ellen elkövetett orosz eredetű elosztott szolgáltatásmegtagadással járó támadásokat (DDoS) követően az EU és a NATO egyre nagyobb hangsúlyt fektetett az információ- és hálózatbiztonság megerősítésére. Napjainkban a kibertér a nemzetközi kapcsolatok kiemelt területévé vált. Ez az új szegmens nemcsak a nemzeti, tagállami szintű stratégiaalkotásban[63] öltött testet, hanem az elmúlt évtizedekben nemzetközi szervezetek, szövetségi rendszerek is megkezdték a kiberdiplomáciával és a kibervédelemmel összefüggő eszköz- és intézményrendszereik kiépítését.

E területen a Magyarország számára kiemelkedően fontos két nemzetközi szervezet, az EU és a NATO élen járt. Míg a NATO elsősorban a katonai és védelmi területre összpontosított, addig az EU *sui generis* (azaz egyedi) jellegéből fakadóan a gazdaság, illetve a külső és belső biztonság minden területére kiterjedő, átfogó kiberbiztonsági megközelítést alkalmazott. Az Európai Unióhoz hasonlóan egyre több tagállam alkalmazta ezt a fajta átfogó megközelítést, a leglátványosabban először Németország, a gazdasági összetevőkre helyezve a hangsúlyt.[64]

Irodalomjegyzék

African Union: *African Union Convention on Cyber Security and Personal Data Protection.* 2014. Online: https://au.int/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

Allison, George: NATO Conducts Crisis Management Exercise. *UK Defence Journal,* 2019. május 9. Online: https://ukdefencejournal.org.uk/nato-conducts-crisis-management-exercise/

[63] A nemzeti szintű kiberstratégiaalkotás kérdéseivel részletesen foglalkozik Molnár Dóra kismonográfiájában. Lásd Molnár Dóra: *Törékeny nagyhatalmiság: a kiberbiztonság. Az európai kibertér brit, német és francia szegmensei.* Budapest, Nemzeti Közszolgálati Egyetem Közigazgatási Továbbképzési Intézet, 2019.

[64] Lásd ehhez Molnár Dóra: Kiberbiztonság Németországban. Pillanatkép a német digitális térről. *Nemzet és Biztonság,* 11. (2018), 1. 142–156.

A Tanács (EU) 2019/796 rendelete (2019. május 17.) az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről. Online: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=uriserv:OJ.LI.2019.129.01.0001.01.HUN&toc=OJ:L:2019:129I:TOC5

A Tanács (KKBP) 2019/797 határozata (2019. május 17.) az Uniót vagy annak tagállamait fenyegető kibertámadások elleni korlátozó intézkedésekről. Online: https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32019D0797&from=EN

Az Európai Unió Tanácsa: *A Tanács következtetései a digitális évtizedre vonatkozó uniós kiberbiztonsági stratégiáról.* Brüsszel, 2021. március 9. (OR. en) 6722/21. Online: https://data.consilium.europa.eu/doc/document/ST-6722-2021-INIT/hu/pdf

Az Európai Unió Tanácsa: *A Tanács következtetései a kiberdiplomáciáról.* Brüsszel, 2015. február 11. Online: http://data.consilium.europa.eu/doc/document/ST-6122-2015-INIT/hu/pdf

Az Európai Unió Tanácsa: *EU–NATO együttműködés: A Tanács következtetéseket fogadott el az együttes nyilatkozat végrehajtása céljából.* 2016. Online: www.consilium.europa.eu/hu/press/press-releases/2016/12/06/eu-nato-joint-declaration/

Az Európai Unió Tanácsa: *Informatikai támadások: az EU készen áll az ellenintézkedésekre, ideértve a szankciókat is.* 2017. Online: www.consilium.europa.eu/hu/press/press-releases/2017/06/19/cyber-diplomacy-toolbox/

Az Európai Unió Tanácsa: *Uniós kibervédelmi szakpolitikai keret (2018. évi naprakésszé tett változat).* Brüsszel, 2018. november 19. (OR. en) 14413/18. Online: http://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/hu/pdf

Brent, Laura: *NATO's Role in Cyberspace.* NATO, 2019. február 12. Online: www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html

Burton, Joe: NATO's Cyber Defence: Strategic Challenges and Institutional Adaptation. *Defence Studies,* 15. (2015), 4. 297–319. Online: https://doi.org/10.1080/14702436.2015.1108108

Council of the European Union: *Cybersecurity in Europe: stronger rules and better protection.* 2020. www.consilium.europa.eu/en/policies/cybersecurity/

Council of the European Union: *Draft Implementing Guidelines for the Framework on a Joint EU Diplomatic Response to Malicious Cyber Activities – Approval of the Final Text.* Brussels, 2017b. október 9. Online: https://data.consilium.europa.eu/doc/document/ST-13007-2017-INIT/en/pdf

Council of the European Union: *Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organisation*. 2016. Online: www.consilium.europa.eu/media/36096/nato_eu_final_eng.pdf

Council of the European Union: *Second Progress Report on the Implementation of the Common Set of Proposals Endorsed by NATO and EU.* 2017a. Online: www.consilium.europa.eu/media/35577/report-ue-nato-layout-en.pdf

Digwatch: *UN GGE and OEWG.* 2021. Online: https://dig.watch/processes/un-gge

Eur-lex: *Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve* (2016. július 6.). Online: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A32016L1148

Európai Bizottság: *Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér.* JOIN/2013/01 final. 2013. Online: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52013JC0001

Európai Bizottság: *Jelentés a dezinformációval szembeni közös cselekvési terv végrehajtásáról. Közös közlemény az Európai Parlamentnek, az Európai Tanácsnak, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának.* Brüsszel, 2019. június 14. JOIN (2019) 12 final. Online: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52019JC0012&from=EN

Európai Bizottság: *Közös közlemény az Európai Parlamentnek és a Tanácsnak: Az „Ellenálló képesség, elrettentés, védelem: az Unió erőteljes kiberbiztonságának kiépítése".* Brüsszel, 2017. szeptember 13. JOIN(2017) 450 final. Online: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52017JC0450&from=en

Európai Külügyi Szolgálat: *Közös jövőkép, közös fellépés: Erősebb Európa. Globális stratégia az Európai Unió kül- és biztonságpolitikájára vonatkozóan.* 2016. Online: http://eeas.europa.eu/archives/docs/top_stories/pdf/eugs_hu_.pdf

Európai Parlament: *Az Európai Parlament állásfoglalására irányuló indítvány a kibervédelemről*. 2018. Online: www.europarl.europa.eu/doceo/document/A-8-2018-0189_HU.html

European Commission: *Joint Communication to the European Parliament and the Council: The EU's Cybersecurity Strategy for the Digital Decade.* Brussels, 2020. december 16. JOIN(2020) 18 final. Online: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

European External Action Service: *Crisis Preparedness: EU Launches Civil-Military Crisis Management Exercise.* Bruxelles, 2018. november 16. – 15:25, UNIQUE ID: 181116_7. Online: https://eeas.europa.eu/headquarters/headquarters-Homepage/53926/crisis-preparedness-eu-launches-civil-military-crisis-management-exercise_en

Fekete-Karydis Klára – Lázár Bence: A kibervédelem katonai dimenziói. *Honvédségi Szemle,* 148. (2020), 3. 44–54. Online: https://doi.org/10.35926/HSZ.2020.3.4

Gavrilović, Andrijana: What's New With Cybersecurity Negotiations? The UN GGE 2021 Report. *Diplo,* 2021. június 6. Online: www.diplomacy.edu/blog/whats-new-cybersecurity-negotiations-un-gge-2021-report

Hybrid CoE: *European Centre of Excellence for Countering Hybrid Threats* (é. n.). Online: www.hybridcoe.fi/

Hybrid CoE: *Hybrid CoE Supports Informal NAC-PSC Discussion.* 2018. szeptember 28. Online: www.hybridcoe.fi/news/hybrid-coe-supports-informal-nac-psc-discussion/

International Committee of the Red Cross: *Cyber Warfare: does International Humanitarian Law apply?* (2021. február 25.). Online: www.icrc.org/en/document/cyber-warfare-and-international-humanitarian-law

Molnár Anna: A kiberdiplomácia fejlődése az Európai Unióban. In Molnár Anna – Molnár Dóra (szerk.): *Kiberdiplomácia.* Budapest, Ludovika Egyetemi Kiadó, 2022. 55–71.

Molnár Anna – Szabolcs Laura: Megerősített együttműködés, változó geometria, PESCO. *Hadtudomány,* 30. (2020), 4. 77–106. Online: http://real.mtak.hu/124268/1/077-106_Molnar_Szabolcs.pdf

Molnár Dóra: Egységes európai kibertér? Az Európai Unió kiberbiztonsági politikájának fejlődése. *Hadmérnök,* 12. (2017), 1. 255–267. Online: http://hadmernok.hu/171_20_molnar2.pdf

Molnár Dóra: Kiberbiztonság Németországban. Pillanatkép a német digitális térről. *Nemzet és Biztonság,* 11. (2018), 1. 142–156. Online: www.nemzetesbiztonsag.hu/cikkek/neb_2018-01-09_molnar_dora_-_kiberbiztonsag_nemetorszagban-pillanatkep_a_nemet_digitalis_terrol.pdf

Molnár Dóra: Nagyhatalmi kiberdiplomácia – az Egyesült Államok, Kína és Oroszország a nemzetközi kiberporondon. In Török Bernát (szerk.): *Információ- és kiberbiztonság.* Budapest, Ludovika Egyetemi Kiadó, 2020. 357–373.

Molnár Dóra: *Törékeny nagyhatalmiság: a kiberbiztonság. Az európai kibertér brit, német és francia szegmensei.* Budapest, Nemzeti Közszolgálati Egyetem Közigazgatási Továbbképzési Intézet, 2019.

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.). Online: www.nato.int/cps/en/natohq/official_texts_133169.htm

NATO: *Cyber Defence.* 2021a. Online: www.nato.int/cps/en/natohq/topics_78170.htm

NATO: *Sixth Progress Report on the Implementation of the Common Set of Proposals Endorsed by EU and NATO Councils on 6 December 2016 and 5 December 2017.* 2021b. június 3. Online: www.nato.int/nato_static_fl2014/assets/pdf/2021/6/pdf/210603-progress-report-nr6-EU-NATO-eng.pdf

NATO CCDCOE: *The Tallinn Manual.* Tallinn, 2021. Online: https://ccdcoe.org/research/tallinn-manual/

Orji, Uchenna Jerome: The African Union Convention on Cybersecurity: A Regional Response Towards Cyber Stability? *Masaryk University Journal of Law and Technology,* 12. (2018), 2. 91–129. Online: https://doi.org/10.5817/MUJLT2018-2-1

Pernik, Piret: *Improving Cyber Security: NATO and the EU.* International Centre for Defence Studies, 2014. szeptember. Online: https://icds.ee/wp-content/uploads/2010/02/Piret_Pernik_-_Improving_Cyber_Security.pdf

Perot, Elie: The Art of Commitments: NATO, the EU, and the Interplay Between Law and Politics Within Europe's Collective Defence Architecture. *European Security,* 28. (2019), 1. 40–65. Online: https://doi.org/10.1080/09662839.2019.1587746

Reaching Critical Will: *Information and communications technology (ICT)* (é. n.). Online www.reachingcriticalwill.org/disarmament-fora/ict

Rehrl, Jochen (szerk.): *Handbook on cyber security. The Common Security and Defence Policy of the European Union*. Directorate for Security Policy of the Federal Ministry of Defence of the Republic of Austria, 2018. Online: https://publications.europa.eu/en/publication-detail/-/publication/63138617-f133-11e8-9982-01aa75ed71a1

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

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

Sperling, James – Mark Webber: The European Union: security governance and collective securitisation. *West European Politics,* 42. (2019), 2. 228–260. Online: https://doi.org/10.1080/01402382.2018.1510193

Sutherland, Iain – Konstantinos Xynos – Andrew Jones – Andrew Blyth: The Geneva Conventions and Cyber-Warfare. *The RUSI Journal,* 160. (2015), 4. 30–39. Online: https://doi.org/10.1080/03071847.2015.1079044

Talihärm, Anna-Maria: *Towards Cyberpeace: Managing Cyberwar Through International Cooperation*. United Nations, 2013. augusztus. Online: www.un.org/en/chronicle/article/towards-cyberpeace-managing-cyberwar-through-international-cooperation

UNGA: *Resolution adopted by the General Assembly on 5 December 2018*. A/RES/73/27. Online: https://undocs.org/A/RES/73/27

Vákát

12. fejezet

Lehetőségek a magyar kiberműveleti képességek fejlesztésére

Ambrus Éva

Bevezetés

A háború gyakran a technológia fejlődésének hajtóereje volt, és segített új és innovatív módszerek bevezetésében, hogy ezáltal harcászati vagy stratégiai szintű előnyhöz juttasson egy nemzetet az ellenfelével szemben. Repülőeszközöket már az I. világháborúban is használtak, meghódítva ezzel a légteret. Két évtizeddel később, a II. világháború során pedig már teljes értékű haderőnemként volt képes dönteni nemcsak csaták, hanem egész frontszakaszok sorsáról a légierő. Ahogyan a II. világháború alatt a technológia meghódította a légteret, úgy tette lehetővé a 20. század fordulóján a hozzáférést a kibertérhez. Ám míg a légtérben lehetőség van a civil és a katonai felhasználást megkülönböztetni, a kibertér esetében a jelen lévő szereplők és szándékok nehezebben szétválaszthatók.

A kibertér gyűjtőfogalma alatt azon felhasználókat, eszközöket, szoftvereket, folyamatokat, információkat, szolgáltatásokat és rendszereket értjük, amelyek közvetlenül vagy közvetetten számítógép-hálózathoz vannak kapcsolva.[1] Az elmúlt évtizedek fejlődése által előidézett összekapcsoltság szintje emeli ki ezt a területet mind a lehetőségek (például e-kereskedelem elterjedése, okosotthonok), mind a fenyegetettség (például hackertámadások sűrűsége, adatok gyűjtése és felhasználása) szempontjából. Újra elolvasva az előbb idézett definíciót, érdemes tudatosítani az egyéni szinten is, hogy hány szállal kötődik a legtöbb ember a kibertérhez, és hogy – általánosságban – milyen természetesnek vehető, hogy létezik.

Azonban a kibertér korántsem tekinthető békés dimenziónak, hiszen egyik hatása biztonsági szempontból, hogy „fegyvert" képes adni olyan csoportok és entitások számára a nagyobb világhatalmak ellen, amelyekkel kinetikus

[1] Kovács László: *A kibertér védelme*. Budapest, Dialóg Campus, 2018. 18.

https://doi.org/10.36250/01079_12

https://orcid.org/0000-0002-8354-1296

műveletek során nem lennének képesek versenybe szállni. Kinetikus műveleteknek hívjuk az ellenség elsősorban fizikai energián alapuló fegyverek által történő pusztítását (például lövedék által), míg nem kinetikusnak azokat a műveleteket, amelyek nem ezen alapulnak (például információs vagy kiberműveletek).[2] A kiberműveletek alatt az informatikai rendszerekhez, illetve azon keresztül infrastruktúrához való hozzáférés és működésük, szolgáltatásaik befolyásolása értendő.[3] A képesség a NATO meghatározása szerint olyan

> „kritikus tulajdonság, amely ahhoz szükséges, hogy a NATO védelmi tervezési folyamata által kifejlesztett katonai tevékenység sikeres legyen. […] A képességek leírják, hogy a NATO katonai szervezeteinek mit kell tudniuk teljesíteni, hogy lefedjék a Szövetség katonai küldetéseinek teljes skáláját, és garantálják a NATO katonai hatékonyságát és szabad mozgását."[4]

A kiberképességek e követelmények megjelenését jelentik a kibertér dimenziójában. A kiberműveleti képességek területén – az ország egészét tekintve – több szervezet érintett, hiszen a kibervédelem és -biztonság szerteágazó terület. A könyvfejezet elsődlegesen a Magyar Honvédség kiberképességeire fókuszál, a két érintett szervezet a Katonai Nemzetbiztonsági Szolgálat Kiberbiztonsági Központja és a Magyar Honvédség Parancsnoksága Kibervédelmi Szemlélősége, beleértve a Magyar Honvédség Parancsnoksága Kiber Képzési Központját. Az információhozzáférés okán elsősorban ez utóbbiakra fogom helyezni a hangsúlyt.

A kiberképesség-fejlesztés szintéziseként az amerikai Correia által is ismertetett[5] DOTM(A)LPFI+P angol betűszó használatát javaslom, miután egyfelől kellőképpen részletes és árnyaltan közelíti meg a kérdést, másfelől hasonlóságot mutat a NATO általi megközelítéssel, ami konvergenciát biztosít. Az eredeti, DOTLMPF betűszó az Egyesült Államok által használt, a közös képességek integrációs fejlesztési rendszerét (*Joint Capabilities Integration Development System* – JCIDS) fedi. Ez a folyamat olyan megoldásteret biztosít, amely figyelembe veszi a feladat végrehajtásához szükséges tényezőket.[6] Az Egyesült

[2] Lóderer Balázs – Stohl Róbert (szerk.): *Fegyver nélküli műveletek és háttértényezők. Tanulmánykötet*. Budapest, Honvéd Tudományos Kutatóhely, 2019. 3.

[3] Munk Sándor: A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései. *Hadtudomány,* 28. (2018a), 1. 113–131.

[4] NATO ACT: *Framework for Future Alliance Operations 2018 Report.* 2018. 57.

[5] João Correia: Military Capabilities and the Strategic Planning Conundrum. *Security and Defence Quarterly,* 24. (2019), 2. 21–50.

[6] US Army War College: *How the Army Runs – A Senior Leader Reference Book 2019–2020.* 2–14.

Államok által használt eredeti DOTMLPF-hez a NATO az interoperabilitás követelményét illesztette (DOTMLPF-I),[7] illetve később az Egyesült Államok is kiegészítette a szakpolitikai irányelvvel (Policy, DOTMLPF-P).

A korábbi DOTMLPF-hez képest a kibertér beemelésével új elemek jelentek meg (a logisztika, az alkalmazkodóképesség, a modularitás, az információ és az intézményközi együttműködés).

A betűszó feloldása a következő:

- Doktrína *(doctrine):* a katonai stratégia módszereinek megfogalmazása.
- Szervezet *(organization):* a harc megszervezése a dandárok és ezredek szintjein.
- Képzés *(training):* a taktikai és műveleti szinten való kiképzés (az alapkiképzéstől a közös nemzetközi képzésekig).
- Felszerelés – logisztika *(material/equipment/logistics):* minden, ami a haderő felszereléséhez szükséges, de nem igényel új fejlesztési kapacitást (rendszeresített felszerelések). A modularitás is rendkívül kritikus, figyelembe véve a fenyegetések széles skáláját, amelyekkel szemben alkalmazkodó és rugalmas válaszokat kell tudni adni.
- Alkalmazkodóképesség *(adaptability):* az alkalmazkodóképesség és interoperabilitás olyan gondolkodásmód, amely nélkül nem lehetséges több tartományt érintő műveletek végrehajtása.
- Vezetés és oktatás *(leadership and education):* a vezetők szakmai felkészítésének módjai, eszközei (szakmai fejlődés).
- Személyzet *(personnel):* képzett személyek rendelkezésre állása béke- és háborús időben, valamint különféle rendkívüli műveletekhez.
- Létesítmények *(facilites):* ingatlanok és (ipari) létesítmények (például kiképző központok).
- Információ *(information):* Az információ célja a folyamatos átfogó tudatosság fenntartása a stratégiai környezet és a kívánt képességek közt. Enélkül a stratégiai környezeti változások nyomon követésének módja elsősorban a doktrínákon keresztül történne, ami a mai gyorsan változó környezetben szükségtelen kockázatot jelenthet.
- Intézményközi együttműködés és szakpolitikai irányelvek *(interagency and policy):* minisztériumok, háttérintézmények közötti együttműködés vagy olyan nemzetközi irányelv, amely befolyásolja e lista elemeit.[8]

[7] NATO AAP-06. NATO Glossary Of Terms And Conditions. 2019.

[8] Correia (2019): i. m. 25.

Egyszerű, ám fontos megállapítás, amely az új típusú kihívásokból, a gyorsan változó biztonsági környezetből adódik: nem lehetséges megvárni az egyértelmű fenyegetések megjelenését, mielőtt létrehoznák az azok kezeléséhez szükséges struktúrákat, ezt a modern katonai képességek fejlesztésébe fektetett idő kockázatossá teszi.[9] Ezért fontos a stratégia a képességalapú tervezési folyamatban, és a fenti katonai képességdefiníció alapján lehetséges azonosítani Lykke stratégiájának három vektorát – célokat, módokat és eszközöket–, amelyekhez még figyelembe kell venni a kockázatot.[10] Mindazonáltal a célok, módok és eszközök az elmúlt időszakban született új nemzeti stratégiákban megjelentek, így a hazai helyzet elemzéséhez végül más eszközt vettem alapul.

SWOT-elemzés

A kiberműveleti képességek fejlesztési lehetőségeinek feltérképezéséhez egy jelenlegi pillanatképből kiindulva lehetséges eljutni. Ehhez az úgynevezett SWOT-elemzést[11] veszem alapul. A SWOT-elemzés egy stratégiai tervezési technika, amely segít szervezeteknek azonosítani a projekttervezéssel kapcsolatos erősségeket, gyengeségeket, lehetőségeket és veszélyeket.[12] Általánosságban a SWOT-mátrix az erősségeket és a gyengeségeket belső, azaz szervezeten belüli, míg a lehetőségeket és a fenyegetéseket gyakrabban külső, azaz a szervezeten kívüli kategóriaként determinálja.

A hagyományosan államközpontú nemzetközi rendszerben az államok saját maguk biztonságáról, annak alkotóelemeiről, területeiről és az azt fenyegető tényezőkről alkotott képe jelenti a kiindulási pontot; megtestesülése a nemzeti biztonsági stratégia (NBS). A nemzeti katonai stratégia (NKS) mindig része a nemzeti stratégiának, azt támogatja, azaz megfelel a nemzeti politikának. Az NKS a nemzeti biztonsági erőforrások, valamint a fegyveres erők

[9] Joseph R. Cerami – Richard Lacquement Jr.: *Shaping American Military Capabilities After the Cold War.* London, Praeger, 2003. 161.

[10] Arthur F. Lykke: *Toward an Understanding of Military Strategy.* In Joseph R. Cerami – James F. Holcomb (szerk.): *Guide to Strategy. USA*. U.S. Army War College, 2001. 179.

[11] A mozaikszó az angol *strength* (erősség), *weakness* (gyengeség), *opportunity* (lehetőség) és *threat* (veszély) szó kezdőbetűiből tevődik össze. Magyarul GYELV-ként is előfordul.

[12] Magyar Kereskedelmi és Iparkamara: *Exportkalauz*. (É. n.)

fejlesztésével kapcsolatos komplex nézet- és tevékenységrendszer. Az NKS már nem ismétli meg a NBS általános megállapításait.[13]

1. táblázat: A kiberképességek SWOT-mátrixa

Erősségek	**Gyengeségek**
– új biztonsági és katonai stratégia erősödő kiberszemlélete (doktrína) – szervezeti megújulás (szervezet) – képzés és oktatás (képzés, kiberakadémia, Nemzeti Közszolgálati Egyetem kiberbiztonsági mesterképzési szak) – felszerelés (Zrínyi Haderőfejlesztési Program)	– civil és katonai „kibertér” – koordináció – szakemberek vonzása és megtartása (személyzet)
Lehetőségek	**Veszélyek**
– rugalmas reagálás (alkalmazkodóképesség) – intézményközi és nemzetközi együttműködések	– gyorsan változó technológia, lekövetési nehézség – adaptábilitás lassúsága (információ)

Forrás: a szerző szerkesztése

Erősségek

Az új biztonsági és katonai stratégia erősödő kiberszemlélete (doktrína)

Az új, 2020. évi *nemzeti biztonsági stratégia* (NBS)[14] kiemeli, hogy

> „Magyarország és a magyar állampolgárok mindenoldalú […] információs és kibertérbeli biztonsága *alapvető érték*. Kiemeli a honvédelmi és rendvédelmi erők szoros *együttműködés*ének fontosságát egymással és a releváns polgári infrastruktúrával, és hogy az új biztonsági kihívások miatt *folyamatosan szükséges fejleszteni* a […] kiberhadviselés elleni védekezés rendszerét. Az információbiztonság *tudatosság*ának alacsony szintjére is felhívja a figyelmet és megállapítja, hogy a kibertér ma már […] *külön műveleti tér*nek számít”.

Az NBS egyik legfontosabb eleme, hogy „Magyarország a fizikai biztonságot veszélyeztető vagy jelentős anyagi károk okozására képes *kiberképességeket*

[13] Mező András: *A katonai stratégiaalkotás és doktrínafejlesztés Magyarországon.* Doktori (PhD-) értekezés. Budapest, Nemzeti Közszolgálati Egyetem, 2019. 34–35.

[14] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról.

fegyvernek, alkalmazásukat fegyveres agressziónak tekinti, amelyre a fizikai térben megvalósuló válaszadás is lehetséges",[15] mindazonáltal kitér a kiberműveletek (támadások) attribúciós nehézségeire is.

A honvédelemmel kapcsolatosan újfent kiemeli a kiberteret mint műveleti területet, és hogy a „katonai kibervédelmet növekvő mértékben alkalmassá kell tenni a haderő kinetikus műveleteinek kibertérbeli támogatására, ki kell alakítani a kiberműveletekben alkalmazható *offenzív képességek*et. Ennek érdekében fejleszteni kell a Magyar Honvédség kibervédelmi és kiberműveleti erőit",[16] pontos irányvonalat kijelölve ezáltal. Nagy lépés, hogy megjelenik az offenzív képességek fontossága.

Továbbá elsődleges feladatként tekint többek között a *kormányzati koordináció* erősítésére, a kibertér *jogi szabályozásának* fejlesztésére, valamint a kiberbiztonsággal kapcsolatos *nemzetközi együttműködés* bővítésére.[17]

Kovács László összefoglalója alapján elmondható, hogy a stratégiában markánsan megjelenik a Magyar Honvédség kibertéri szerepe és feladatai is, meghatározza, hogy a fejlesztéseknek a kibervédelmi *(defenzív)* és kiberműveleti *(offenzív)* erői a kinetikus erők műveleteinek támogatására is alkalmasak legyenek. A főbb irányvonalak megadása után szükséges a végrehajtást elősegítő ágazati stratégiák átalakítása, létrehozása, ami tükrözi ezeket a fejleményeket. Ilyen a 2021. évi *nemzeti katonai stratégia,* illetve az előkészület alatt álló *nemzeti kiberbiztonsági stratégia,* amelyekben megjelenik a katonai kiberműveleti képességek helye és szerepe.[18]

A katonai stratégia „a katonai végcélok, a katonai módszerek és a végrehajtásra biztosított katonai eszközök együttese".[19]

A 2021. évi *nemzeti katonai stratégia*[20] (NKS) meghatározza, hogy a hagyományos (katonai, gazdasági, politikai, társadalmi és környezeti) biztonsági elemek mellett azt a kiber- és az információs dimenziók is alkotják.[21] Ahogyan az NBS-ben, úgy itt is megjelenik az a fajta szemlélet, hogy a hazánk „fizikai biztonságát veszélyeztető vagy jelentős anyagi károk okozására képes

[15] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról.
[16] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról.
[17] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról.
[18] Kovács László: A kiberbiztonság és a kiberműveletek megjelenése Magyarország új Nemzeti Biztonsági Stratégiájában. *Honvédségi Szemle,* 148. (2020), 5. 3–18.
[19] Lykke (2001): i. m. 3.
[20] 1391/2021. (VI. 24.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról.
[21] 1391/2021. (VI. 24.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról.

kiberképességeket fegyvernek, alkalmazásukat pedig akár *fegyveres támadásnak tekinti,* amelyre adott esetben katonai válaszadás is lehetséges",[22] amelyhez szükséges többek között a kibertér-eszközrendszerek fejlesztése. A *katonai kibertérműveleti erők* a kibertérben végrehajtott (offenzív vagy defenzív) műveleteikkel támogatják a haderőnemeket, és aktívan közreműködnek a nemzeti kibervédelmi feladatokban.

Az alkalmazkodóképességet erősíti az a megállapítás is, hogy a Magyar Honvédség képességei *moduláris rendszerben* épülnek fel annak érdekében, hogy a műveleti igények szerint lehessen őket alakítani. Ehhez szükséges, hogy minden műveleti szinten *passzív és aktív* kibervédelmi *képességeket* alakítsanak ki.

Az NBS-hez képest az NKS tovább bontja a feladatokat a kiberműveletek tekintetében, amikor részletezi, hogy azoknak offenzív jellegűnek is kell lenniük, támogatniuk kell a szárazföldi és légierő műveleteit passzívan és aktívan, és ehhez moduláris, rugalmas rendszerű képességekre van szükség.

Szervezeti megújulás (szervezet)

A honvédelmi miniszter 32/2021. (VII. 23.) HM utasítása[23] rendelkezett a Magyar Honvédség Kiber- és Információs Műveleti Központ (MH KIMK) kialakításával összefüggő egyes feladatokról. Ennek eredményeként a Magyar Honvédség parancsnokának alárendeltségébe tartozó kiber- és információs műveleti feladatokat ellátó honvédségi szervezetek szervezeti felépítése és feladatrendszere átalakul.

Az MH katonai kibertérműveleti képességeinek fejlesztése érdekében az *MH Civil-katonai Együttműködési és Lélektani Műveleti Központ* 2021. december 31-ei hatállyal megszűnt, és annak jogutódszervezeteként az MH PK közvetlen szolgálati alárendeltségében 2022. január 1-jei hatállyal MH KIMK megnevezéssel új költségvetési szerv jött létre.

Kovács László kibervédelmi főszemlélő korábbi cikkében utalt a szervezet lehetséges átfogóbb feladataira is:

> „Az MH fejlesztése során általánosságban a kibertér műveleti képességek fejlesztése, illetve a kibertéri műveletek tervezéséhez, szervezéséhez és vezetéséhez szükséges szervezeti keretrendszer kialakítása az első cél. Az ezeket a feladatokat a jövőben megvalósító

[22] 1391/2021. (VI. 24.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról.
[23] *Hivatalos Értesítő. A Magyar Közlöny Melléklete.* 6. 2021. július 23. 3482–3483.

szervezetnek három nagy csoportra osztható feladategyüttese várható: 1. kibervédelmi és kiberműveleti fejlesztések koordinálása és ezek vezetése; 2. a kiberműveleti tevékenységek vezetése és végrehajtása különböző szinteken (hadműveleti szint, harcászati szint); 3. a kiberműveletek integrálása a szárazföldi csapatok és a légierő műveleteibe."[24]

Képzés és oktatás (képzés, kiberakadémia)

A Magyar Honvédség kiberképzési központját (kiberakadémia) 2019 júniusában adták át. Ez a szervezet végzi az oktatási, képzési és kiképzési feladatokat, beleértve a honvédség felhasználóinak kibertudatossági képzését, illetve a jövőbeli kiberműveleti erők felkészítését.[25]

Az egyik ilyen feladat az oktatás, képzés és kiképzés rendszerének és akár intézményrendszerének a megteremtése. Ez nemcsak a saját állomány felkészítését jelenti, hanem a Magyar Honvédség egészére vonatkozó, elsősorban kibervédelmi képzéseket is. Ezekkel a képzésekkel lehetséges emelni a kiberbiztonsági tudatosság és elkötelezettség szintjén. Nyilvánvalóan ezek a képzések és kiképzések az eltérő szinteken eltérő célokkal is párosulnak, hiszen amíg az említett kiberbiztonsági tudatossági képzéseket minden szinten folytatni kell, addig a kiberműveletek stratégiai kérdéseit a katonai felső vezetés szintjén, de a konkrét technikai végrehajtást műveleti és harcászati szinten szükséges oktatni.

Benkő Tibor honvédelmi miniszter 2020. évi honvédelmi bizottsági ülésén elmondta, hogy a tárgyév decemberéig a kiberakadémián 19 tanfolyamot bonyolítottak le, és 3000 fő vett részt a biztonságtudatosítási tanfolyamon.[26]

Felszerelés (Zrínyi Honvédelmi és Haderőfejlesztési Program)

A 2021. évi honvédelmi költségvetés 778 milliárd forint volt, a 2022. évi 1003 milliárd forint, amely 28,9%-os nominális emelést jelent. A nemzeti összterméhez viszonyítva is jelentős a bővülés, az idei 1,66% után jövőre meghaladja az 1,7%-ot a honvédelmi kiadások GDP-hez viszonyított aránya, így

[24] Kovács (2020): i. m. 16.

[25] Draveczki-Ury Ádám: „Egy korszerű harckocsi is számítógép-hálózat, csak 70 tonna vas veszi körül". *Honvédelem.hu,* 2020. július 3.

[26] Jegyzőkönyv az Országgyűlés Honvédelmi és rendészeti bizottságának 2020. december 8-án, kedden, 11 óra 04 perckor az Országház Széll Kálmán termében (főemelet 64.) megtartott részben zárt üléséről. 29.

egyre közeledünk a NATO által elvárt 2%-os mértékhez, amelyet a vállalások alapján 2024-re kell elérni.[27] Ennek a költségvetési növekedésnek központi eleme a Zrínyi Honvédelmi és Haderőfejlesztési Program, amely egyszerre jelent hadiipari és haderőfejlesztést. A két elem egymást támogatva hosszabb távon képes biztosítani a honvédség ütőképességét, hogy a befektetések ne egyszeriek legyenek, hanem folyamatosan fenntartsák és igazítsák képességeiket a kor követelményeihez.

Gyengeségek

Civil és katonai „kibertér" és koordináció

Alapvetésnek tűnik, de érdemes újra felidézni azt a tényt, hogy a kibertérben nehezen elkülöníthető a katonai és a civil „szféra". Maga a kibertér és az abból fakadó fenyegetések bonyolultak, összetettek és változékonyak. Ezek mellett a kiberműveletek száma és sebessége is növekszik. A fenyegetések korábban a fizika korlátjához igazodtak, azonban a kibertérben folyamatosak. Ez elkerülhetetlenül kihívások elé állítja a döntés- és reagálási képességet. Nem utolsósorban nemcsak a civil és katonai megkülönböztetés, hanem az attribúció, azaz egy-egy kiberművelet „gazdájának" a meghatározása is időigényes, továbbá más-más következménye lehet annak, hogy egy kiberműveletet támadásnak, kémkedésnek vagy bűncselekménynek tekintenek-e.

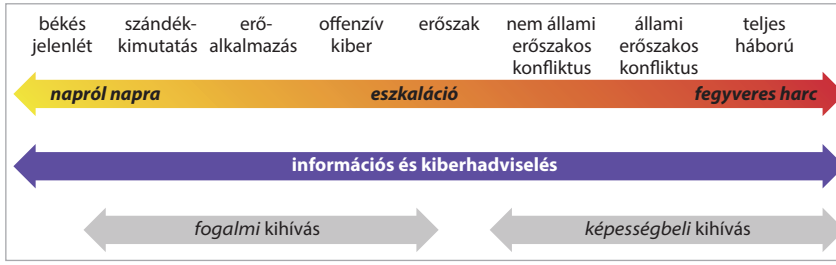
A hazai kibervédelmi szervezeti rendszer mind a civil, mind a katonai térben két részre bontható, egy stratégiaira (koncepciók kidolgozása, koordináció) és egy operatívra (gyakran hatósági funkciót ellátva, gyakorlati végrehajtás). A civil oldalon a stratégiai szinten a Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok találhatók,[28] míg az operatív szintet – több esetben hatósági funkciókkal is kiegészülve – a Nemzetbiztonsági Szakszolgálat keretein belül működő

[27] Baranyai Gábor: Jövőre is nő a honvédelemre fordítható összeg. *Magyar Nemzet,* 2021. május 1.

[28] A Nemzeti Kiberbiztonsági Koordinációs Tanács, valamint a Kiberbiztonsági Fórum és a kiberbiztonsági ágazati munkacsoportok létrehozásával, működtetésével kapcsolatos szabályokról, feladat- és hatáskörükről szóló 484/2013. (XII. 17.) Korm. rendelet módosításáról szóló 259/2021. (V. 20.) Korm. rendelet a közbiztonság erősítése érdekében egyes kormányrendeletek módosításáról.

Nemzeti Kibervédelmi Intézet jelenti.[29] A katonai oldalon található meg a MH Kibervédelmi Főszemlélősége, alatta a Kiberakadémiával, és a Honvédelmi Ágazati Elektronikus Információbiztonsági Eseménykezelő Központ a Katonai Nemzetbiztonsági Szakszolgálat égisze alatt.

A katonai és civil együttműködés fontosságát és összetettségét az *1. ábra* mutatja be.



1. ábra: A verseny-konfliktus spektrum a hatalom katonai dimenziójához

Forrás: US Navy Chief of Naval Operations: *A Design for Maintaining Maritime Superiority. Version 2.0.* 2018. december[30]

Még kevés konkrétum van arról, hogy a fegyveres erők hogyan tudnak hozzájárulni a nemzeti és nemzetközi kiberbiztonság védelméhez (egy fegyveres konfliktuson kívül), és összetett kérdéskör továbbra is, hogy a kormányok hogyan kezelik a kiberbiztonság és a létfontosságú infrastruktúra védelmének összehangolásával kapcsolatos feladatokat. Bár a fegyveres erők és a polgári hatóságok közötti szoros együttműködés szükségességét kifejezetten figyelembe veszik a különböző szakstratégiákban, kevés konkrétum elérhető ennek megvalósítása felől.

Az új szakpolitikai terület a szervezetek közötti küzdelemhez vezethet az erőforrásokat illetően, illetve fontos tisztázni a felelősségmegosztásokat is. Egy válsághelyzetben az ilyen bizonytalanság negatív hatással lehet a reagálás hatékonyságára, ezért is szükséges közös gyakorlatok szervezése minden érdekelt féllel.

[29] Kovács Zoltán: Kibervédelem és biztonság. In Kiss Tibor (szerk.): *Kibervédelem a bűnügyi tudományokban.* Budapest, Dialóg Campus, 2020. 65.; Munk Sándor: Kiberbiztonsági eseménykezelő szervezetek rendeltetése, feladatai. *Hadmérnök,* 13. (2018b), 3. 430.

[30] „Az Egyesült Államok Védelmi Minisztériuma (DoD) vizuális információinak megjelenése nem jelenti a DoD jóváhagyását."

Szakemberek vonzása és megtartása (személyzet)

Az elmúlt években érezhetően nőtt a verseny az informatikai munkaerőpiacon a világban. A kibervédelmet is érinti a megfelelően képzett munkaerő hiánya, azonban egy szervezet számára több lehetőség is kínálkozik, hogy könnyebben elérje vagy megtartsa a munkaerőt. A NATO Kooperatív Kibervédelmi Kiválósági Központjának tanulmánya[31] foglalkozott a kibervédelem területét érintő személyügyi problémákkal. A pénzügyi ösztönzést alapvetően rövid távú megoldásnak tekintették, meglátásuk szerint a munkaerő számára egy bizonyos fizetési szint felett a pénzügyi ellentételezés nem elsődleges motiváció. A nem pénzbeli ösztönzők, mint például az értelmes munka, a továbbképzési és fejlődési lehetőség, az elismerés vagy a munkakörnyezet, tekinthetőek hosszú távú megoldásnak a munkaerő megtartásában. A Rand Corporation tanulmánya azt támasztotta alá, hogy a közszférában egy kihívásokban gazdag feladat ellátása az (informatikában) átlagos fizetés mellett erős kapcsot teremtett a munkavállaló, a szervezet és annak küldetése között.[32]

A területen nem csupán a kiberbiztonsági szakértőkből van hiány, hanem az állami és a magánszektor is verseng a rendelkezésre álló tehetségekért. A szakképzett személyek toborzása és megtartása a fegyveres erőkben közös kihívás a legtöbb NATO-tagállamban, tekintettel a jövedelmezőbb civil területekre. Továbbá, bár a katonaság érdeke lehet, hogy a legjobb tehetségeket toborozza, az is a nemzeti érdeket szolgálja, hogy e személyek az iparban támogassák a nemzetgazdaságot.

A korábban említett Magyar Honvédség Kiber Képzési Központja nagyban hozzájárul a szakemberek át- és kiképzéséhez. További hazai jó gyakorlat a Honvédelmi Minisztérium által indított Mészáros Lázár-ösztöndíj, amely többek között az informatika területén is támogatást nyújt a hallgatók számára, vállalva, hogy a képzés befejezését követően az MH-val létesített szerződéses szolgálati viszonyát legalább az ösztöndíj folyósításával megegyező ideig fenntartja.[33] Továbbá fontos szerep jut a Nemzeti Közszolgálati Egyetem Államtudományi és Nemzetközi Tanulmányok Karán létrejött kiberbiztonsági mesterképzésnek.

[31] Erwin Orye – Gunnar Faith-Ell: *Cyber Workforce Recruitment and Retention: An Awareness Assessment.* CCDCOE, Tallinn, 2020. 14.

[32] Orye–Faith-Ell (2020): i. m. 15.

[33] Honvédelmi Minisztérium: *Pályázati felhívás honvédségi ösztöndíjra* (2021. június 1.).

Lehetőségek

Rugalmas reagálás (alkalmazkodóképesség)

A jelenlegi elképzelések szerint a többdimenziós műveletek (*multidomain operations* – MDO) biztosítják a rugalmas reagálást a haderőnek a változó kihívásokkal szemben. Az MDO alapgondolata a képességek mélyebb integrálása a különböző (szárazföldi, légi, tengeri, kiber-, információs) dimenziók között; az idő, a tér és a képességek konvergenciájának elérése érdekében, hogy független manővereket végezhessen, és dimenziók közötti csapásokat hajthasson végre.[34] A többdimenziós műveletek koncepciójának célja az ellenfél integrált védelmi képességeinek leküzdése, a dimenziók elszigetelésének elkerülése, valamint a cselekvési szabadság megőrzése.

Ennek továbbgondolt változata a NATO által is átvett közös össztartományi műveletek (*Joint All Domain Operations* – JADO) koncepció, amely figyelembe veszi a rendszerek összekapcsoltságát a mai haderőben. Ennek az elméletnek a meglátása, hogy a hagyományos haderőnemi struktúrák, amelyek elsődlegesen a saját tartományukra fókuszálnak, a jövőben is eredményesek lehetnek. Valószínűsíthető, hogy előnyösebb helyzetben lesz az a haderő, amelyik képes könnyedén, gyorsan, agilisan és szinkronban manőverezni az összes dimenzión keresztül, ezért tartja fontosnak a NATO az MDO kiterjesztését.[35]

Következő lépés lehetne a NATO-nak saját, különálló doktrína kifejlesztése a több dimenzióra kiterjedő műveletekről, amelyeket a szövetségesek a saját jövőbeli képességeikhez, erőforrásaikhoz és követelményeikhez tudnának igazítani, ezzel úgymond megelőlegezve az interoperabilitást ezen a területen is. A több dimenzióra kiterjedő műveletek sikere attól függ, hogy képesek vagyunk-e az elgondolást a doktrínához, a szervezethez, a képzéshez, a felszereléshez, a vezetéshez és az oktatáshoz, a személyzethez és a létesítményekhez szükséges képességekhez és az anyagkorszerűsítési követelményekhez igazítani. Ennek eléréséhez szükséges többek között a kiberképességek fejlesztése, amely hozzájárul a megfelelő információk biztonságos továbbításához a szervezeten belül, lehetővé téve a gyorsabb döntést és cselekvést, ugyanakkor korlátozva

[34] Franz-Stefan Gady – Alexander Stronnel: *Cyber Capabilities and Multi-domain Operations in Future High-Intensity Warfare in 2030.* CCDCOE, é. n. 155.

[35] 'NATO JADO': *A Comprehensive Approach to Joint All Domain Operations in a Combined Environment.* JAPCC, 2021.

az ellenfelek mozgásszabadságát az „elektronikus harctéren". A hazai fejlesztések ezen a területen is pozitív irányba mutatnak.

Intézményközi és nemzetközi együttműködések

Az intézményközi együttműködés fontos a tudástranszfer megvalósulásához; amennyire lehetséges, együtt kell működnie a polgári és a katonai területeknek, amennyiben hasonló technológiai megoldásokkal tudnak hozzájárulni a probléma megoldásához. Együttműködés lehetséges a kiberbűnözés-megelőzéssel foglalkozó hatóságokkal, amit például az EU kibervédelmi szakpolitikai keretrendszer javasol.[36] A polgári-katonai együttműködés a kiberügyek területén többek között a bevált jó gyakorlatok cseréje, az információcsere és a korai előre jelző mechanizmusok, az eseményekre adott kockázatértékelések és a figyelemfelkeltés, valamint a képzés és a gyakorlatok tekintetében lehet gyümölcsöző.

Regionális szinten fontos az ilyen típusú együttműködések tekintetében a PESCO. A PESCO (*Permanent Structured Cooperation,* állandó strukturált együttműködés) az Európai Unióban megteremti annak a lehetőségét, hogy a tagországok jobban összedolgozzanak a védelem és a biztonság terén. A tagállamok önkéntes alapon vesznek részt az együttműködésben, de a bekapcsolódáshoz vállalásokat kell tenniük az együttműködés előmozdítására.[37] Magyarország alapító tagként vesz részt Németország (koordinátor), Franciaország és Hollandia mellett a PESCO Kiber- és Információs Domain Koordinációs Központjának (*Cyber and Information Domain Coordination Center* – CIDCC) létrehozásában. A CIDCC célja az információcsere és -áramlás javítása, valamint uniós műveletek és missziók tervezése és vezetése a kiberdimenzióban, hozzáadott értéke az egységesített helyzetjelentések készítése a kiber- és információs térről, támogatva az uniós műveletek és missziók katonai tervezési és irányítási folyamatát.[38]

Ahogyan a kiberműveleti főszemlélő fogalmazott:

> „Az a közös tapasztalat, hogy komoly kihívást jelent a valós idejű – minden kibertéri és minden információs téri – veszélyhelyzetre történő, megfelelő hatékonyságú válaszadás.

[36] Council of the European Union: *EU Cyber Defence Policy Framework (2018 update) 14413/18.* 16.

[37] Az EU állandó strukturált együttműködéséről átfogó információk olvashatók: https://pesco.europa.eu/

[38] Bunderministerium der Verteidigung: *Cyber and Information Domain Coordination Centre (CIDCC).* (É. n.).

> […] Így szükségessé vált, hogy a szövetségünk 4000 kilométeres sugarú körében az EU által támogatott műveleteket kiber-helyzetképpel erősítsük meg. A CIDCC képes lesz arra, hogy a tagországok információit összegyűjtse és egységesítse, ezzel biztosítva az EU katonai törzsének a katonai feladatvégrehajtás során szükséges kiber-információkat."[39]

Veszélyek

Gyorsan változó technológia, lekövetési nehézség

Rob Murray, a NATO Innovációs Egysége vezetőjének véleménye, hogy „azok a nemzetek nyernek [a technológiai] versenyben, amelyek a leggyorsabb bürokráciával, nem pedig a legjobb technológiával rendelkeznek".[40] Az, hogy egy szervezet mennyire és milyen gyorsan képes alkalmazkodni, egyre nagyobb előnyt jelent. Azonban a gyorsan fejlődő technológiák mellett nem mindig egyértelmű, hogy milyen irányba érdemes befektetni.

Barno és Bensahel – megvizsgálva az Egyesült Államok erőfeszítéseit az iraki és afganisztáni operatív kihívások leküzdésére – állítja, hogy az alkalmazkodóképesség a háború alapvető tantétele. Meglátásuk szerint, miután a jövő kihívásait nehéz megjósolni, a stratégiai és taktikai sokkok leküzdésére irányuló szervezeti rugalmasság a legfontosabb, és ez az alkalmazkodóképességi követelmény a jövőben még hangsúlyosabb lesz.[41]

Az elmúlt bő másfél év felgyorsította az alkalmazkodás szükségességét több területen is. Ahogyan fizikailag távolságot kellett tartani, úgy kerültek testközelbe a kibervilág lehetőségei és veszélyei. Az online oktatás, a távmunka, a telemedicina előretörése többségünket érintette, a hálózatok védelmének fontosságára, a kritikus infrastruktúrák kibervédelmére így több figyelem jutott.

Az „alkalmazkodási ollónak" három hajtóereje van a szerzők szerint: *1.* számtalan potenciális ellenfél szembenállása (nagyhatalmi versenytársak, globális szereplők vagy rosszindulatú nem állami szereplő) és a globális események által okozott volatilitás (például az éghajlatváltozás, a tömeges migráció és a növekvő

[39] Ördög Kovács Márton: „Közös feladatot látunk el a kibertér védelme érdekében". Interjú prof. dr. Kovács László dandártábornokkal, kibervédelmi szemlélővel. *Honvedelem.hu,* 2020. november 30.

[40] Rob Murray: Building a Resilient Innovation Pipeline for the Alliance. *NATO Review,* 2020. szeptember 1.

[41] David Barno – Nora Bensahel: *Adaptation under Fire: How Militaries Change in Wartime.* Oxford Scholarship Online, 2020. 1–3.

városiasodás). A *2.* hajtóerő a közelmúltban két új műveleti dimenzió megjelenése: a világűr és a kibertér. A kiberműveletek következményeit ezeken a területeken még nem lehet felmérni az empirikus adatok hiánya miatt. A *3.* hajtóerő a technológiai fejlődés növekvő léptéke és üteme. A mesterséges intelligencia, a robotika és az új fegyverrendszerek megjelenése befolyásolja a hadviselés jellegét. Ezek a hajtóerők együttesen megnehezítik a konfliktusok előrejelzését, és alátámasztják a konfliktusokhoz való alkalmazkodóképesség szükségességét.[42]

Hogy hogyan lehet alkalmazkodni az állandóan változó környezetben, arra példát adhatnak a különböző online szolgáltatók, szolgáltatások, hiszen az üzemzavarok és a kiesések a legtöbbjüknél előfordulnak. Ahogyan egyre több szolgáltatás elérhető online – akár például az e-közigazgatás területén, akár a terjedő otthoni munkavégzés okán –, egyre fontosabb, hogy minden szervezet tudjon a megfelelő időben reagálni a váratlan eseményekre. Ehhez szükséges, hogy a szervezet számítson a váratlan helyzetre. Az első jeleknél érdemes a megfelelő biztonsági lépéseket megtenni. Tisztázni kell azt is a szervezeten belül, hogy a különböző szinteken a szereplők hogyan koordinálják tevékenységüket, hogy lépést tudjanak tartani az események tempójával. Fontos, hogy a reagálási készségek az események bekövetkezte előtt rendelkezésre álljanak a szervezet számára, és emellett folyamatos, proaktív tanulás jellemezze a szakembereket.[43] Mindez a kihívások, módszerek, készségek és képességek folyamatos felülvizsgálatát igényli.

Az adaptábilitás lassúsága (információ)

Az egyik visszatérő elem a szakirodalomban az információ központi kérdése a modern konfliktusokban, hadviselésben. A 21. században a rendelkezésre álló rengeteg információ ellenére a fegyveres erőknek nehézségeik voltak az ezen információk adta előnyök kiaknázásával kapcsolatban. Például Peter Mansoor kijelenti, hogy az Egyesült Államok kezdetben nem rendelkezett az iraki környezet megfelelő megértésével és a hatékony információs műveletek

[42] Barno– Bensahel (2020): i. m. 245–47.

[43] David D. Woods: The Strategic Agility Gap: How Organizations Are Slow and Stale to Adapt in Turbulent Worlds. In Benoît Journé et al. (szerk.): *Human and Organisational Factors*. Springer, 2020.

végrehajtásának képességével.[44] Egy másik megfigyelése az, hogy az iraki és az afganisztáni háborúkban a bevetett fegyveres erők elavult megközelítésekkel és elképzelésekkel dolgoztak, amelyek hangsúlyozták a kinetikai szerepvállalást, majd fokozatosan növelték képességeiket a nem kinetikus szerepvállalások területén (mint amilyen például a civil-katonai kapcsolatok).[45] A kialakulóban lévő, EU-s szintű kiberműveleti együttműködés (PESCO CIDCC) a kibertérben lévő információhiányt kívánja többek között pótolni, azonban ehhez tagállami együttműködés szükséges, a duplikációk elkerülése mellett, a szövetségi rendszerek között. A *2. ábra* fentebb szemlélteti azt a fajta széttöredezettséget, amely a kiberteret jellemzi, eszerint pedig fogalmi tisztázás szükséges, hogy a kibertérben mi számít szándékkimutatásnak vagy éppen offenzív kibertámadásnak, és hogy arra milyen válasz adható, adandó, és kinek. Sajnos vagy szerencsére, de ezen a területen még nem rendelkezünk elég tanulsággal, hogy kialakuljanak minták vagy jó gyakorlatok szövetségi szinten. Mindenesetre előremutató elem, hogy a hazai Kiber- és Információs Műveleti Központ (KIMK) magában foglalja majd a MH Civil-katonai Együttműködési és Lélektani Műveleti Központját, és a vitéz Szurmay Sándor Budapest Helyőrség Dandár szervezetéből és feladatrendszeréből az elektronikus eseménykezelői feladatokat végző szervezeti egység is átkerül.

Összegzés

A képességfejlesztés alapja a doktrínákban megjelenő politikai akarat. Ennek további leképeződése a szakstratégiák megjelenése, ahonnan pontosabb kép rajzolódik ki a cél megvalósulását illetően. A kibertér ötödik műveleti területté emelése mellett a fejlesztési akarat igen fontos kifejezése volt az offenzív kiberképességek szükségességének megfogalmazása. Ezen elgondolásoknak ad fizikai keretet a Honvédelmi és Haderőfejlesztési Program, amely nemcsak a (hadi-) technikákat, hanem a személyzetet is érinti. További lehetőségek vannak még az együttműködés fokozásában mind a hazai, mind a nemzetközi területen, ezzel is hozzájárulva a személyzet képzéséhez, motivációjához

[44] Peter R. Mansoor: Lessons of the Iraq War. In Thomas G. Mahnken (szerk.): *Learning the Lessons of Modern War*. Stanford (CA), Stanford University Press, 2020. 55–57.

[45] Carter Malkasian: Afghanistan and the Crisis of Counterinsurgency, 2001–2014. In Mahnken (2020): i. m. 109–115.

és a jó gyakorlatok elsajátításához. Szükséges a megújulás a rugalmas reagálás területén is, és habár e könyvfejezetben nem esett szó róla, a Magyar Honvédségen belül fontos szerep jut e területen a Transzformációs Parancsnokságnak. Nagyobb szervezeti átalakulást hozhat az átállás a többdimenziós műveletekre (MDO), amely elgondolást az Egyesült Államok és részben a NATO is kutatja. Ahogyan a technológiai fejlődés is folyamatos, úgy a szervezeti fejlődésnek is szükséges követnie azt. A nagyobb műveleti területről a kisebb egységekre fókuszálva látszik, hogy a kinetikus és nem kinetikus egységek együttes használatának fontossága tovább erősödik. Az intézményi keretrendszer kialakítása, a hamarosan létrejövő Kiber- és Információs Műveleti Központ egyik origója lehet mindennek, azonban mint a többi EU- és NATO-tagállamnak is, kihívást fog jelenteni a szakemberek toborzása, megtartása. A honvédség megújulása e területen is lehetőséget biztosíthat a munkakörülmények fejlesztése, az intézményközi együttműködések és az egyedi kihívások által. Nem lehet eléggé hangsúlyozni az információmegosztás fontosságát és gyorsaságát, egy-egy kiberművelet tempóját, és ezt tartania kell a döntéshozatalnak is a megfelelő válaszreagálás érdekében. Összességében: az elmúlt években a kiberműveletek területén Magyarországon nagy előrelépések történtek, lépést tartva a többi európai tagállammal, ezalatt közös kihívásokkal és lehetőségekkel szembenézve.

Irodalomjegyzék

1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról. Online: https://net.jogtar.hu/jogszabaly?docid=A20H1163.KOR&txtreferer=00000001.txt

1391/2021. (VI. 24.) Korm. határozat Magyaroszág Nemzeti Katonai Stratégiájáról. Online: https://magyarkozlony.hu/dokumentumok/2a94d595e4bc33b3515c09b0f6f04c4ca3df69c6/megtekintes

259/2021. (V. 20.) Korm. rendelete a közbiztonság erősítése érdekében egyes kormányrendeletek módosításáról. Online: https://magyarkozlony.hu/dokumentumok/9aa09f19cee0c53e21021218e25abe1d10f560c7/megtekintes

Baranyai Gábor: Jövőre is nő a honvédelemre fordítható összeg. *Magyar Nemzet,* 2021. május 10. Online: https://magyarnemzet.hu/belfold/2021/05/jovore-is-no-a-honvedelemre-fordithato-osszeg

Barno, David – Nora Bensahel: *Adaptation under Fire: How Militaries Change in Wartime*. Oxford Scholarship Online, 2020. Online: https://doi.org/10.1093/oso/9780190672058.001.0001

Bundesministerium der Verteidigung: *Cyber and Information Domain Coordination Centre (CIDCC).* (É. n.). Online: www.bundeswehr.de/en/organization/the-cyber-and-information-domain-service

Cerami, Joseph R. – Richard Lacquement Jr.: *Shaping American Military Capabilities After the Cold War.* London, Praeger, 2003.

Correia, João: Military Capabilities and the Strategic Planning Conundrum. *Security and Defence Quarterly,* 24. (2019), 2. 21–50. https://doi.org/10.35467/sdq/108667

Council of the European Union*: EU Cyber Defence Policy Framework (2018 update) 14413/18*. Online: https://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/en/pdf

Draveczki-Ury Ádám: „Egy korszerű harckocsi is számítógép-hálózat, csak 70 tonna vas veszi körül". *Honvedelem.hu,* 2020. július 3. Online: https://honvedelem.hu/hirek/hazai-hirek/egy-korszeru-harckocsi-is-szamitogep-halozat-csak-70-tonna-vas-veszi-korul.html

Gady, Franz-Stefan – Alexander Stronnel*: Cyber Capabilities and Multi-domain Operations in Future High-Intensity Warfare in 2030.* CCDCOE, (é. n.). Online: https://ccdcoe.org/uploads/2020/12/8-Cyber-Capabilities-and-Multi-Domain-Operations-in-Future-High-Intensity-Warfare-in-2030_ebook.pdf

Jegyzőkönyv az Országgyűlés Honvédelmi és rendészeti bizottságának 2020. december 8-án, kedden, 11 óra 04 perckor az Országház Széll Kálmán termében (főemelet 64.) megtartott részben zárt üléséről. Online: www.parlament.hu/documents/static/biz41/bizjkv41/HOB/2012081.pdf

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

Kovács László: A kiberbiztonság és a kiberműveletek megjelenése Magyarország új Nemzeti Biztonsági Stratégiájában. *Honvédségi Szemle,* 148. (2020), 5. 3–18. Online: http://dx.doi.org/10.35926/HSZ.2020.5.1

Kovács Zoltán: Kibervédelem és biztonság. In Kiss Tibor (szerk.): *Kibervédelem a bűnügyi tudományokban*. Budapest, Dialóg Campus, 2020. 65–90. Online: http://real.mtak.hu/107378/7/web_PDF_Kibervedelem_bunugyi_tudomanyokban-66-91.pdf

Lóderer Balázs – Stohl Róbert (szerk.): *Fegyver nélküli műveletek és háttértényezők. Tanulmánykötet.* Budapest, Honvéd Tudományos Kutatóhely, 2019.

Lykke, Arthur F. Jr.: *Toward an Understanding of Military Strategy.* In Joseph R. Cerami – James F. Holcomb (szerk.): *US Army War College Guide to Strategy.* (H. n.), Strategic Studies Institute, 2001. 179–185.

Magyar Kereskedelmi és Iparkamara: *Exportkalauz.* (É. n.). Online: https://mkikexport.uzletahalon.hu/?q=exportprojekt/elemzes/fogalomtar

Malkasian, Carter: Afghanistan and the Crisis of Counterinsurgency, 2001–2014. In Thomas Mahnken (szerk.): *Learning the Lessons of Modern War.* Stanford (CA), Stanford University Press, 2020. 102–121.

Mansoor, Peter R.: Lessons of the Iraq War. In Thomas Mahnken (szerk.): *Learning the Lessons of Modern War.* Stanford (CA), Stanford University Press, 2020. 55–57.

Mező András: *A katonai stratégiaalkotás és doktrínafejlesztés Magyarországon.* Doktori értekezés. Budapest, Nemzeti Közszolgálati Egyetem, 2019. Online: https://bit.ly/3Akcewh

Munk Sándor: A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései. *Hadtudomány,* 28. (2018a), 1. Online: https://doi.org/10.17047/HADTUD.2018.28.1.113

Munk Sándor: Kiberbiztonsági eseménykezelő szervezetek rendeltetése, feladatai. *Hadmérnök,* 13. (2018b), 3. 427–436. Online: http://hadmernok.hu/182_30_munk.pdf

Murray, Rob: Building a Resilient Innovation Pipeline for the Alliance. *NATO Review,* 2020. szeptember 1. Online: www.nato.int/docu/review/articles/2020/09/01/building-a-resilient-innovation-pipeline-for-the-alliance/index.html

NATO AAP-06. NATO Glossary Of Terms And Conditions. 2019. Online: https://nso.nato.int/natoterm/Web.mvc

NATO ACT: *Framework for future alliance operations 2018 report.* 2018. Online: www.act.nato.int/images/stories/media/doclibrary/180514_ffao18.pdf

NATO JADO: *A Comprehensive Approach to Joint All Domain Operations in a Combined Environment*. JAPCC, 2021. Online: www.japcc.org/portfolio/nato-joint-all-domain-operations/

Orye, Erwin – Gunnar Faith-Ell: *Cyber Workforce Recruitment and Retention: An Awareness Assessment.* CCDCOE, Tallinn, 2020. Online: https://ccdcoe.org/uploads/2021/02/Workforce-Sep_20_v5.pdf

Ördög Kovács Márton: „Közös feladatot látunk el a kibertér védelme érdekében". Interjú prof. dr. Kovács László dandártábornokkal, kibervédelmi szemlélővel. *Honvedelem.hu,* 2020. november 30. Online: https://honvedelem.hu/hirek/kozos-feladatot-latunk-el-a-kiberter-vedelme-erdekeben.html

US Army War College: *How the Army Runs – A Senior Leader Reference Book 2019–2020.* Online: https://ssl.armywarcollege.edu/dclm/pubs/HTAR.pdf

US Navy Chief of Naval Operations: *A Design for Maintaining Maritime Superiority. Version 2.0.* 2018. december. Online: https://media.defense.gov/2020/May/18/2002301999/-1/-1/1/DESIGN_2.0.PDF

Woods, David D.: The Strategic Agility Gap: How Organizations Are Slow and Stale to Adapt in Turbulent Worlds. In Benoît Journé – Hervé Laroche – Corinne Bieder – Claude Gilbert (szerk.): *Human and Organisational Factors*. Springer, 2020. Online: https://doi.org/10.1007/978-3-030-25639-5_11

13. fejezet

Következtetések a következő évtizedre

Molnár Dóra

Bevezetés

Az elmúlt évszázadban az emberi civilizáció drasztikusan megváltozott, és ezek a változások visszatükröződnek a hadviselésben alkalmazott stratégiákban és taktikákban is. A hadviselés jellemzője, hogy mindig is ember által irányított tevékenység volt, és ez a jövőben is így lesz. Még ha robotok is fogják uralni a harcteret, a humán tényező mindig fontos szerepet fog játszani a döntéshozatal és az irányítás folyamatában. A hadviselés ugyanakkor soha nem lesz kiszámítható, ezért a jövőbeli fejlemények előrejelzésére tett minden kísérlet valószínűleg csak korlátozott sikerrel járhat. Inkább kérdéseink vannak, semmint biztos válaszaink. Olyan kérdések, mint: a kibernetikai műveletek vajon elérik-e, elérhetik-e kitűzött céljaikat? Vagy: milyen kockázatokkal jár az eszkaláció? Vagy: milyen körülmények között vezethetnek az egyre gyakoribb és kifinomultabb kibertevékenységek akaratlan eszkalációhoz és katonai erő alkalmazásához?

Az utóbbi évtizedekben azt láthattuk, hogy a nagyhatalmi verseny egyre inkább magában foglalja a rivális államok közötti kibertevékenységeket is abban a kibertérben, amelyben a háború törvényei tisztázatlanok. Olyannyira, hogy egyenesen naivitásnak tűnik azt gondolni, hogy a nemzetközi közösség belátható időn belül széles körű konszenzusra jut a kiberhadviselés szabályait illetően, vagy azzal kapcsolatban, hogy a jelenlegi, a nemzetközi humanitárius jogra vonatkozó normák alkalmazhatók-e, és ha igen, hogyan, a kibertérre. S adódik a költőinek tűnő kérdés: egyáltalán érdekelt-e bármelyik fél a kiberhadviselés szabályozásában? Nem véletlenül fogalmazott úgy Barack Obama, az Egyesült Államok 44. elnöke 2015-ben, hogy a kibertér jelenleg egyfajta vadnyugat.[1]

A kibertér nemcsak felforgatta a politikai határokat, hanem megrendítette az államok számára keretet adó vesztfáliai rendszer gyökereit is. A földrajzi

[1] The White House: *Remarks by the President at the Cybersecurity and Consumer Protection Summit.* Stanford (CA), Stanford University, 2015. február 13.

https://doi.org/10.36250/01079_13

https://orcid.org/0000-0002-1476-5253

határok hiánya és a látszólagos átláthatatlanság a hadviselés ezen ötödik területén lehetővé tette, hogy a rosszindulatú nem állami szereplők sokasága biztonsági fenyegetésként legyen jelen. Ebben a térben a hírszerzés és az adatlopás láthatatlan, az információs kampányokat nem mindig lehet azonosítani, és gyakran a szabotázs sem különböztethető meg a balesetektől. A kibertérben kialakuló új konfliktusok sohasem fognak hasonlítani a múltbéli vagy a jelenlegi konfliktusokra. Olyan időket élünk, amikor azt sem tudjuk, hogy mikor kezdődik, és mikor végződik egy kibertámadás, béke van-e, vagy virtuális háború zajlik…

Ilyen viszonyok között vállalkozik ez a fejezet arra, hogy prognózisba bocsátkozzon a jövő kiberháborúját illetően. Ehhez először a nemzetállamok lépéseinek mögöttes mozgatórugóit kell megérteni, ugyanis ezek lényegében olyan prizmák, amelyeken keresztül láthatjuk, hogyan hajtják végre jövőbeni lépéseiket. Ez a gondolkodásmód az egyes állami politikákban és stratégiákban tükröződik. A kiberháborúkat meghatározó másik alapvető kérdés az új technológiák köre, amelyeket előbb-utóbb háborús céllal is használni fognak. Általánosságban elmondható, hogy a jelenlegi stratégiák túlzottan a technológiai kérdésekre és a nemzeti ellenállóképesség megteremtésére összpontosulnak, a normatív magatartás kialakulását elősegítő értékteremtés rovására. Tekintettel a nemzetek előtt álló kiberbiztonsági kihívások nagyságrendjére, a kibertér geopolitikai jövőjének mérséklésére irányuló nemzetközi konszenzus hiányára és arra, hogy az értékek érvényesítésének összehangolt törekvése hiányzik a kiberbiztonsági stratégiákból, sokat kell még tenni ahhoz, hogy a kibertérben békés viszonyok uralkodjanak. Az eddigi kibertér a politikai háborúskodás és a kényszerdiplomácia területe volt, és ha az államok nem változtatnak jelenlegi gyakorlatukon, akkor könnyen tényleges csatározások színterévé válhat.

A kibertér mint kiindulási pont és a kiberkonfliktusok

A jövő kiberbiztonságával kapcsolatban, még ha számos nyitott kérdés is akad, egy kérdést biztosan meg tudunk válaszolni: a kiberakciók és interakciók színterét, amely nem más, mint a kibertér.[2] A kibertér legfőbb jellemzőit ezért

[2] E közös tér elnevezése azonban nem egységes. Vannak államok, ahol több okból kifolyólag inkább az információs tér vagy digitális tér kifejezést használják, ilyen például Németország is. Erről részletesebben lásd Molnár Dóra: Kiberbiztonság Németországban. Pillanatkép a német digitális térről. *Nemzet és Biztonság,* 11. (2018), 1. 142–156.

érdemes közelebbről is megvizsgálni, ugyanis az ebben a speciális közegben zajló folyamatokat ezek az alapvető tulajdonságok nagymértékben determinálják. A kibertér számos jellemzője közül az alábbi öt az, amely a jövő kiberkonfliktusaival szoros összefüggésben állhat:[3]

1. A kibertér egyrészt – némiképp meglepő módon – egyben fizikai tér is. Ennek oka részben az, hogy az információ, amely keresztülhalad a kibertéren, a fizikai infrastruktúrában gyökerezik, amely létrehozza, majd tárolja az adatokat; részben pedig az, hogy a fizikai infrastruktúra (amelynek egyébiránt a kibertér létrejötte is köszönhető) általában a fizikai államhatárokon belül található. Amellett azonban, hogy a kibertér fizikai tér, egyben logikus térnek is nevezzük, mert az áthaladó információ egyeztetett útválasztási protokollokon megy keresztül. E kettőség az oka annak, hogy a történelemben ez idáig vagy széles körű, de időben korlátozott kibertámadásokat láthattunk, vagy elhúzódó, de kisebb hatást elérő támadásokat, és olyan támadás még nem volt (talán a SolarWinds-esetet leszámítva), amely huzamosabb időn át képes volt jelentős hatást elérni. A fizikai és logikai attribútumok ezen egyedi szintézise két fontos megállapításhoz vezethet. Egyrészt valamely fizikai tér tényleges részvétele nélkül nehezen képzelhető el egy, pusztán a kibertérben zajló nagyobb összecsapás, másrészt pedig támadó műveletek esetén azt jelenti, hogy azok bár gyorsan átlépik a határokat, azonban az elért hatások sokkal nagyobb valószínűséggel lesznek visszafordíthatók, mint más típusú katonai támadások esetén.
2. A kibertér domináns szereplője a magánszektor, amely nemcsak birtokolja, üzemelteti és irányítja a hálózatokat, hanem nagymértékben függ is az alapul szolgáló hálózatoktól és információtól. Ráadásul ez a kitettség a jövőben csak fokozódni fog. Kérdéseket vet fel, hogy kiberháború esetén milyen szerepet játszhat a hagyományos háborúk megvívásának főszereplője, az állam, és az állami szerepvállalás hogyan egyeztethető össze a magánszektor tevékenységével és érdekeivel, ezen műveletek koordinációja miként valósítható meg.
3. A kibertér további jellemzője, hogy taktikai szinten gyorsan reagál, de működését tekintve mégis lassú. Ennek oka, hogy bár az egyedi

[3] *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy.* Washington (DC), National Research Council, The National Academies Press, 2010. 78.

kiberakciókat gyorsan véghez lehet vinni, azonban valamennyi támadás tervezési ciklusa egy adott katonai hatás elérése érdekében ennél jóval hosszabb, és a kívánt hatás elérése sem azonnal következik be.

4. A kibertérben a támadás amolyan *primus inter pares* lehet a védelemmel összevetve. Ennek hátterében az áll, hogy gyakran nehéz különbséget tenni támadó és védekező jellegű lépés között, és egy alapvetően védelmi jellegű hozzáállás is támadónak tűnhet a szemben álló fél nézőpontjából. (Erről a kérdéskörről, valamint a védelem szerepéről a fejezet alább részletesen szól.)
5. A kibertér markáns jellemzője, hogy tele van bizonytalansággal. Ez következik a célok és a dinamika elégtelen ismeretéből, a lépcsőzetes hatások bizonytalanságából, valamint abból, hogy egy rendkívül összetett és gyorsan változó közegről van szó, ahol a változás irányát igen nehéz megjósolni. Ez a jellemző a jövő kiberháborújával kapcsolatos feltételezéseket nagymértékben determinálja.

A változás irányának előrejelzése nemcsak a kibertér jellemzőire vonatkozóan jelent kihívást, hanem a kibertérbeli viszonyok jövőbeli alakulását illetően is. Abban egyetértés mutatkozik, hogy a kibertér ma ellenséges környezet. Jól tükrözik ezt nemcsak a nemzetállamok kiberképességei, hanem az is, hogy a legtöbb vállalat és kormány rendelkezik biztonsági műveleti központokkal (*Security Operation Center:* SOC). Bár nem valószínű, hogy a kibertér ellenséges mivoltában a következő tíz évben változás állna be, azt mégsem zárhatjuk ki. Ez esetben 2030-ra egy hálózatvédelmi és hálózatirányítási mesterségesintelligencia-algoritmus olyannyira csökkentené a kiberkockázatokat, hogy kitörne a kiberbéke. Jelen állás szerint mégis az a forgatókönyv tűnik valószínűbbnek, hogy 2030-ra a világ már megvívta vagy éppen vívja az első kiberháborút: egy olyan hipersebességű háborút, amely kiterjedt nemzetállami támadásokat tartalmaz egymás kritikus infrastruktúrája ellen, beleértve a távközlést, a csővezetékeket, a pénzügyi rendszereket, valamint az elektromos áramtermelő és átviteli hálózatokat. Ha abból indulunk ki, hogy az ember veleszületett jellemzője a versengés és a túlélésért folytatott küzdelem, akkor elkerülhetetlennek látszik ez utóbbi szcenário bekövetkezte.

De ne szaladjunk ennyire előre, ugyanis a háború mindig a legmagasabb intenzitású konfliktus, amelyet általában egyéb, alacsonyabb intenzitású tevékenységek előznek meg! Ezek között a kibertérben több olyat is nevesíthetünk, amelyben a katonai elem domináns szerepet játszhat, és amellyel a jövőben reá-

lisan számolni kell.[4] A *kiberellenes tevékenységek (counter cyber)* az integrált védekező és támadó műveletek olyan átfogó kategóriája, amelyek célja a kívánt mértékű kiberfölény elérése és megtartása. A *tiltó műveletek (cyber interdiction)* az ellenség katonai kibernetikájának elterelésére, megzavarására, késleltetésére vagy megsemmisítésére irányuló akciókat jelentik, még mielőtt azokat a képességeket hatékonyan felhasználhatnák a baráti erők ellen vagy más módon céljaik eléréséhez. A *közeli kibertámogatás (close cyber support)* az olyan ellenséges célpontok elleni tényleges fellépést jelenti, amelyek a baráti erők közvetlen közelében találhatók, és veszélyeztetik az integrált kibermissziók sikerességét. Az eddigi művelettípusok inkább a védelmi műveletek körébe sorolhatók, szemben a továbbiakkal, amelyek már egyértelműen támadó szemléletűek. A *harcoló erők általi kiberfelderítés (cyber reconnaissance in force)* egy olyan katonai (és nem hírszerzési) támadó kiberműveletet jelent, amelynek célja az ellenség erejének felderítése vagy tesztelése vagy egyéb információk megszerzése. Az *ellenséges kibervédelem elnyomása (supression of enemy cyber defences)* olyan tevékenység, amely semlegesíti, megsemmisíti vagy ideiglenesen rontja az ellenséges kibervédelmet romboló és/vagy zavaró eszközök segítségével. S végül a *stratégiai kiberművelet (strategic cyber mission)* egy vagy több kiválasztott ellenséges kibercélpont ellen intézett széles körű támadás, amelynek célja a fokozatos pusztítás, valamint az ellenség háborúmegvívási képességének és akaratának megtörése. Ezek a műveletek tehát azok, amelyekkel a jövőben minden bizonnyal fogunk találkozni, egyes típusok esetében minden bizonnyal nagy számban.

A bevezető gondolatok zárásaként érdemes kitérni a kibertérben zajló műveletek funkcióira, amelyek közül az Egyesült Államok katonai doktrínája hármat nevesít: a támadó és a védekező kiberműveleteket, valamint a Védelmi Minisztérium információs hálózati műveleteit.[5] A doktrína értelmében a támadó kiberműveletek *(offensive cyber operations)* „célja az erő kivetítése erő alkalmazásával a kibertérben vagy azon keresztül”.[6] (A 2019-ben felállított Solarium Kibertér

[4] A részletes definíciókat lásd *Joint Publication 1-02 (JP 1-02): Dictionary of Military and Associated Terms*. Washington (DC), Department of Defense, 2019. október.

[5] *FM 3-38 Cyber Electromagnetic Activities*. Department of the Army HQ, 2014. február.

[6] *US Military Doctrine.*

Bizottság[7] is megismétli ezt a definíciót a 2020. március 11-i jelentésében.)[8] A szárazföldi erők ilyen támadó kiberműveleteket a katonai műveletek teljes spektrumában végeznek az ellenség, valamint az ellenséges tevékenységek és kapcsolódó képességek ellen a kibertérben és a kibertéren keresztül, azzal a céllal, hogy a parancsnok szándékát és céljait támogassák. Érdekes álláspontot képvisel ezzel szemben az Ausztrál Stratégiai Politikai Intézet, amely a támadó kiberműveletek és a támadó kiberképességek fogalmát szinonimaként használja.[9] A jövő zenéje még, hogy azon országok, amelyek támadó kiberképességekkel rendelkeznek, ténylegesen hogyan fogják e képességeiket a műveletek során is offenzív céllal használni, az azonban szinte bizonyos, hogy a két fogalom más jelentéssel bír. Ami a képességeket illeti, jelenleg 23 ország bizonyítottan is rendelkezik támadó kiberképességekkel, míg további 30 ország valószínűsíthetően.[10] (Magyarország is ez utóbbi körbe tartozik.)

Támadó kiberműveletek – kiberháború?

Leegyszerűsítve azt mondhatnánk, hogy minden kiberháború támadó kiberművelet, de nem minden támadó kiberművelet kiberháború. A kiberháborúnak ugyanis vannak olyan ismérvei, amelyeknek más támadó kiberművelet nem felelnek meg. Érdemes tehát megvizsgálni az egyes kategóriák közötti különbségeket, mert a jövőben ezekkel a fogalmakkal várhatóan sokkal gyakrabban fogunk találkozni, mint manapság.

Az egyes műveletek elhatárolásához a brit Nemzeti Kiberbiztonsági Központ egykori igazgatója, Ciaran Martin által felvázolt tipológiából indulunk ki, amely egy ötfokozatú skálán helyezi el a kiberműveleteket. A skála egyes elemeinek kezdőbetűi után ezt HACKS-struktúrának is nevezhetjük.[11] A HACKS-modell

[7] A Bizottságot (*Cyberspace Solarium Commission:* CSC) az Egyesült Államok Kongresszusa állította fel 2019-ben azzal a céllal, hogy konszenzust alakítson ki a jelentős következményekkel járó számítógépes támadásokkal kapcsolatban: hogyan lehet és kell megvédeni az Egyesült Államokat a kibertérben?

[8] *US Solarium Cyberspace Commission Report.* 2020. március. 36–144.

[9] Tom Uren – Bart Hogeveen – Fergus Hanson: *Defining Offensive Cyber Capabilities*. Australien Strategic Policy Institute, 2018. július 4.

[10] Digwatch: *UN GGE and OEWG*. 2021.

[11] Martin Ciaran: *Cyber-Weapons Are Called Viruses for a Reason: Statecraft and Security in the Digital Age.* London, King's College, 2020. november.

azért lehet különösen hasznos, mert egyrészt kiemeli az adott támadás súlyosságának spektrumát, másrészt pedig lefed valamennyi jövőbeni támadó kiberműveletet. Ahogyan haladunk a skálán felfelé, úgy találkozunk egyre kevesebb ténylegesen is megvalósult művelettel. A struktúra legalsó szintjén a hekkelés *(hacking)* található, ez nem más, mint konkrét nemzetvédelmi célok elérése érdekében folytatott számítógépes művelet, amely révén a beavatkozó hozzáférést szerez az ellenfél elektronikus eszközeihez. A második szint az ellenséges infrastruktúra megsemmisítése *(adverserial infrastructure destruction),* amely az ellenséges digitális infrastruktúra célzott megsemmisítését jelenti.[12] Széles körben ismert eset és jó példa erre az amerikai kiberparancsnokság, a Cyber Command 2018-as művelete az Internetes Kutatási Ügynökség szentpétervári trollgyárának infrastruktúrája ellen. A harmadik szintet az ellenhatás-műveletek *(counter-influencing)* alkotják, amelyek lényegében a támadó kiberműveletek elrettentéscélú alkalmazását foglalják magukban. Más szóval utóbbiakat nevezhetjük digitális zaklatásnak is, ennek jellemzője, hogy általában fedett műveletek képezik, passzívak (legalábbis kezdetben), és nem semmisítenek meg vagy rombolnak infrastruktúrát. A negyedik szint a *„kinetikus" támadás,* olyan offenzív kibernetikai művelet, amely jelentős kárt és fennakadást okoz az adott ország infrastruktúrájában (például megzavarja a város áramellátását, vagy kikapcsolja a televíziós hálózatot). Tehát itt már nemcsak az adott fenyegetés megszakítása a cél, hanem azon túl, mintegy válaszként, a tényleges károkozás. Bár kinetikus támadásra még kevés példát találunk, de a jövőben ezen esetek száma bizonyosan szaporodni fog. A példák közt említhetőek az orosz támadások: 2014-ben Oroszország hat órára lekapcsolta Kijev egyes részeinek áramellátását, majd egy évvel később a TV5 Monde francia televíziócsatorna működését bénította meg 11 órára. Végül az ötödik és egyben a legmagasabb szintet a rendszer egészére kiterjedő, katonai és polgári célpontok elleni *kibertámadások* jelentik fegyveres konfliktus során *(systems wide).* Ehhez hasonló, stratégiai szintű támadásra 2016-ban már majdnem sor került, amikor az amerikai Kiberparancsnokság Nitro Zeus néven széles körű támadást tervezett Irán ellen, ám az végül idő előtt kitudódott.[13] A kérdés tehát nem az, hogy sor fog-e kerülni ilyen kibertámadásra, hanem az, hogy mikor.

[12] Ez lényegében egybeesik az amerikai „kitartó elkötelezettség" *(persistent engagement)* fogalmával.

[13] Matthias Schulze: Cyber in War: Assessing the Strategic, Tactical, and Operational Utility of Military Cyber Operations. *12th International Conference on Cyber Conflicts.* Tallinn, NATO CCDCOE Publications, 2020.

A *kiberháborúval* mindenképpen részletesen is foglalkozni kell, mert a jövő háborúinak az egyik, ha nem is kizárólagos színtere a kibertér lesz. Ugyanakkor már a kiberháború fogalmának használatakor kérdésekbe ütközünk, mert annak tényleges tartalmát illetően a mai napig nincs egyetértés a nemzetközi közösségben. Az alapvető kérdés, hogy a hagyományos háborúfogalom használható-e a kiberháború esetében. A dilemma létjogosultságát már az is jól jelzi, hogy míg a hagyományos háborúkat nemzetállamok vívták egymás ellen, addig a kibertérben számos olyan nem állami szereplő tett szert jelentős hatalomra, amely képes lehet a jövő háborújának megvívására. Ehhez kapcsolódó további kérdéskör az attribúció, azaz hogy az adott háborús cselekedet végrehajtását kinek lehet tulajdonítani. Eddig ugyanis a hagyományos háborúk során nem jelentett akadályt a háborúban részt vevő felek beazonosítása és nevesítése. A kibertérben azonban ez a kérdés is más értelmet nyer, és könnyen előfordulhat, hogy a jövő kiberháborúiban (de nem is csak a háborúkban, hanem alsóbb szintű támadó kiberműveletek esetében is) adott támadó cselekmények mögött pontosan meg nem határozható entitások állnak majd.

Sokan – köztük Colin Gray is – amellett érvelnek, hogy a kibertámadások különböznek a hagyományos háborútól, mert nem felelnek meg a háború clausewitzi definíciójának, amely szerint a háború erőszakos, eszközszerű és politikai erőhasználat.[14] Ezen vélemények hátterében az áll, hogy sok stratéga a kibernetikai képességeket pusztán eszközként, és nem új háborús eszközként kezeli. Ehhez azért az is hozzátartozik, hogy Gray a kiberteret nem tekinti a taktikai alkalmazás és a stratégia szempontjából nagymértékben különbözőnek az eddigi működési területektől.[15]

Ugyanakkor, ha a háború három szükségszerű elemének tartalmára tekintünk, ezeknek mai korhoz adaptált tartalma megfelelhet a kibertérbeli háborúk ismérveinek is. Valóban helytelen lenne azt állítani, hogy Clausewitz elképzeléseit nem kell a jelenlegi biztonsági légkörnek megfelelően módosítani, hiszen korszakalkotó hadtudományi műve megjelenése (1832) óta igen sok minden megváltozott – különösen a kiberfegyverek megjelenése, amely aláásta nemcsak a maximális erőhasználatra vonatkozó kívánalmat, hanem egyúttal előtérbe helyezte Szun-ce minimális erőre és megtévesztésre vonatkozó gondolatait is.

[14] Carl von Clausewitz szerint a háború a politika folytatása más eszközökkel. Lásd Carl von Clausewitz: *A háborúról.* I. kötet. Budapest, Zrínyi, 1961. 56.

[15] Colin S. Gray: *Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling?* Strategic Studies Institute, 2013. április 1.

Szun-ce ugyanis azt tartja a legügyesebb megoldásnak, ha harc nélkül sikerül legyőzni az ellenfelet – amely a kibertérben könnyen megtörténhet, hiszen hagyományos fegyveres erő alkalmazására nem is kerül sor, és a célok eléréséhez elég lehet minimális erőkifejtés. Ez a korlátozott erőhasználat rögtön elvezet bennünket az első fogalmi elemhez, az erőszakos erőhasználathoz. Maga Clausewitz, bár egyértelművé teszi, hogy az erő a háború sarkalatos pontja, soha nem számszerűsíti, hogy mekkora erő szükséges ahhoz, hogy adott cselekmény háborús cselekedetnek minősüljön. Clausewitz pusztán kijelenti, hogy maximális erő kívánatos a fölény eléréséhez (amelyhez érdemes rögtön hozzáfűzni azt, hogy ez a kibertérben nem alkalmazható, mert a fölény megszerzése valójában minimális erővel is elérhető). Önmagában az erőhasználat korlátozott mivolta tehát nem jelenti azt, hogy a háború ezen fogalmi eleme csorbát szenvedne a kiberháború esetében. Az „erőszak" és az „erő" kifejezés nem összemosandó. Bár az utóbbinál kiberháború esetén korlátozottan, az előbbi vonatkozásában az elért eredményből következtethetünk annak mértékére. Egy kiberháború ugyanis hatalmas károkat tud okozni, amelyeket nem feltétlenül emberéletekben lehet számszerűsíteni. A nyilvánvaló, fizikai vagyont érintő kár mellett itt gondolni kell a támadásoknak az emberek pszichés jóllétére gyakorolt hatására és így az okozott pszichés sérülésekre is.[16] A másik két fogalmi elem, tehát az erőhasználat eszközszerű jellege és politikai motivációja különösebb magyarázatot nem igényel, hiszen ezek kiberháború esetében is adottak.

Jelen pillanatban azonban még nehéz elképzelni egy olyan háborút, amely kizárólag a kibertérben zajlik, nincs fizikai kapcsolata az egyéb terekkel, és azokra (vagy a gazdaságra) nem gyakorol közvetlen hatást. A jelenleg egyre általánosabban elterjedt, a háborús szintet még el nem érő támadó kiberműveletek jelentősége abban áll, hogy a hagyományos hadviselési eszközök és módszerek hatékonyságát képesek megerősíteni, valamint a katonai kommunikációt észszerűsítik, stratégiai előnyt biztosítva ezáltal az államoknak. Ezért az ezen műveletekkel való foglalkozás legalább annyira fontos lesz a jövőben, mint a kiberháború kérdésköre.

A háborúknak három alapvető típusuk van az alkalmazott erők és eszközök alapján: a hagyományos, a nukleáris és a kiberháború.[17] E három típusnak hétféle kombinációja képzelhető el elméletben: egyetlen eszközfajtával megvívva a háborút (három eset), kétféle eszköztípust alkalmazva (három eset), és ha mindhármat

[16] Harriet Charlotte Turner: Cyber War Forthcoming: "It Is Not a Matter of If, It Is a Matter of When". *E-International Relation,* 2020. július 8.

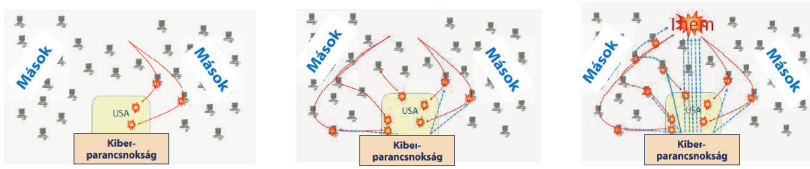
[17] *Proceedings of a Workshop…* (2010): i. m. 110.

egyszerre alkalmazzák. Ezek közül a kiberháború négy esetben juthat szerephez: ha más eszközök igénybevétele nélkül, pusztán kiberfegyverekkel vívják, ha párban áll vagy a hagyományos háborúval, vagy a nukleáris háborúval, vagy ha mindhárom típusú eszközt bevetik ugyanazon konfliktus során. Ezen kombinációk közül nem valószínű azok bekövetkezte, amelyekben a nukleáris erő jutna szerephez, és szintén nem várható, hogy kizárólag a kibertérben kibereszközökkel vívott háborúra kerülne sor. Ezért a legvalószínűbb, hogy a jövőben a hagyományos háborúknak lesz kibervetülete is. Az is kérdéses, hogy mely térben veszi kezdetét a konfliktus. Valószínűbb, hogy a kiberincidensek fognak elérni egy olyan háborús szintet, amely ellenségeskedést a felek hagyományos erők bevetésével a fizikai térben is folytatni fogják. Ugyanakkor nem kizárt a fordított sorrend sem: azaz a hagyományos háborúnak idővel lesz egy széles körű kibersíkja, kiegészítve a szárazföldi, légi vagy vízi műveleteket, és hozzájárulva azok sikeréhez – olyannyira, hogy akár egyes hagyományos elemeket kiberelemekre cserélhetnek le azok kisebb költségigénye és potenciálisan nagyobb hatékonysága okán.

Felmerülhet a kérdés, hogy milyen mögöttes motivációk mentén mehet végbe a jövő kiberháborúja.[18] Mindenekelőtt stratégiai megfontolások állhatnak az ilyen műveletek mögött, ami egyfajta nyomásgyakorlást jelent a másik fél akaratára és képességeire gyakorolt hatás elérése céljából. Műveleti oldalról közelítve a motiváció az ellenségeskedésben részt vevő ellenséges erők hagyományos, fizikai eszközeire hatást gyakorolni. Ezek mellett cél lehet az elrettentés, azaz egy másik állam azon szándékának letörése, hogy (kiber)támadást hajtson végre, valamint az aktív védelem is, amely olyan technikát jelent, amely korlátozza mások képességét kibertámadások végrehajtására, vagy segít a korábbi kibertámadásokat jellemezni és elkövetőit felderíteni. Végül speciális motivációkkal is találkozhatunk (a speciális műveletek analógiájára), amelyek bizonyos, időben és helyileg korlátozott hatások elérésére irányulnak, javarészt a fizikai küzdelem keretein kívül és általában titokban.

A kiberháborúk tényleges lefolyását illetően két, egymást részben fedő, részben kiegészítő megközelítés képzelhető el.[19] Haditechnikai oldalról közelítve: egy adott országot kibertámadás ér, amelyet a védekező fél ellentámadással megállít, és tovább védekezik az újabb esetleges támadásokkal szemben, visszaverve végül a támadást. Ezt a folyamatot szemlélteti az *1. ábra*.

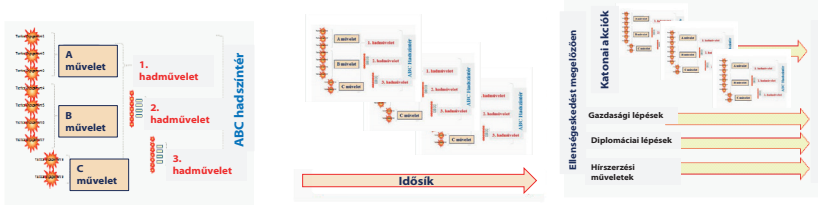
[18] Martin Libicki: Pulling Punches in Cyberspace. In *Proceedings of a Workshop…* (2010): i. m. 135.
[19] *Proceedings of a Workshop…* (2010): i. m. 96.



1. A támadás kezdete | 2. Védekezés, ellentámadás | 3. A támadás visszaverése

1. ábra: A kibertámadás haditechnikai vetülete
Forrás: Proceedings of a Workshop... (2010): i. m. 96.

A hagyományos hadviselés taktikai oldaláról nézve valószínűsíthető, hogy egy nagyszabású háború a kibertérben ugyanezt a sémát követné számos gyors, összekapcsolt (egymást követő vagy párhuzamos) támadással, amelyek mind részei egy nagyobb hadműveletnek – s akár nemcsak több hadszíntéren zajló műveletnek, hanem párhuzamosan gazdasági, diplomáciai és/vagy hírszerzési műveleteknek is.[20] Ezeknek a műveleteknek a vezetési-irányítási rendszere is nagyban eltér a hagyományos háborúkban alkalmazott megoldásoktól, köszönhetően annak, hogy virtuális cellákban kell gondolkodni. S míg a hagyományos műveletek esetén, ahol szükséges a fizikai jelenlét, egyszerre csak egy cellában tud ténylegesen ott lenni a harcoló katona, addig a kiberkatona egy időben több virtuális cellában is fogadni tudja az utasításokat.[21]



Egymást követő támadások | Párhuzamos támadások | Egyéb műveletek

2. ábra: A kibertámadás taktikai megoldása
Forrás: Proceedings of a Workshop... (2010): i. m. 97.

[20] *Proceedings of a Workshop...* (2010): i. m. 97.
[21] Norman R. Howes – Michael Mezzino – John Sarkesain: *On Cyber Warfare Command and Control Systems*. (H. n.), International Command and Control Institute, 2004.

A kiberháborúkkal kapcsolatosan azok befejezését illetően megállapíthatjuk, hogy az is nagyban eltér a hagyományos háborúkétól. Míg a fizikai háborúkban a békeszerződéseket gyakran követi egy- vagy többoldalú leszerelés, a leszerelés fogalma a kibertérben értelmezhetetlen, mivel a kiberháború sokkal inkább a sérülékenységekről szól, semmint a fegyverekről.[22]

Stratégiai gondolkodás a kiberháborúról

A kiberháború jövőjét meghatározó egyik alapvető tényező a nemzetállami gondolkodásmódban keresendő, amely az egyes állami stratégiákban ölt testet. A kibertér stratégiai szempontból jelenleg széttöredezett. Egyrészt Kína rohamos fejlődése és előretörése, másrészt számos más állam aktív – és egyre gyakrabban támadó jellegű – jelenléte miatt továbbra sem egyértelmű az Egyesült Államok dominanciája. Tekintettel arra, hogy a jövő háborújának jellemzőit nagymértékben fogja determinálni a stratégiai gondolkodás, röviden mindenképpen ki kell térni elsősorban az Egyesült Államok kibertérre vonatkozó stratégiai elképzeléseire, de nem mellőzhető a Kína és Oroszország egyre erőteljesebb lépései mögött megbújó gondolkodásmód ismertetése sem.

Az Egyesült Államok hosszú időn át a kiberháború hatásalapú megközelítésének híve volt.[23] Ennek értelmében nem az volt a fontos, hogy a hatás miként jön létre (kinetikus vagy kibernetikus síkon), hanem a cél, tehát hogy a kívánt hatást minden áron elérjék.[24] Ezen megközelítés ernyőjét az elrettentés koncepciója jelenti, amelyet az Egyesült Államok 2011 óta stratégiai szinten deklaráltan követ. Ezt a koncepciót először a kibertér nemzetközi stratégiájában *(Internations Strategy for Cyberspace)* rögzítették 2011-ben, majd 2015-ben a Védelmi Minisztérium is megerősítette azt. Az amerikai megközelítés szerint az elrettentés nem más, mint „a fellépés megakadályozása az elfogadhatatlan ellenintézkedések hiteles fenyegetésének puszta létezésével”.[25] Tehát az amerikai kibererő lényege, hogy az ellenfelek féljenek cselekedni Amerika ellen,

[22] Martin C. Libicki: *Cyberdeterrence and Cyberwar.* Santa Monica (CA), Rand Corporation, 2009. 135.

[23] Aaron Wright: The Future of Cyber Conflict. *The Cove,* 2020. augusztus 5.

[24] Jó példa erre a Stuxnet-támadás, amelyet katonai szempontból úgy terveztek meg, hogy járulékos károk nélkül érje el a kívánt hatást.

[25] *Joint Operations, 17 January 2017 Incorporating Change 1, 22 October 2018*. Joint Publications 3.0, 212.

tartva a megtorlástól. Az elrettentés alapját az erős védelem jelenti – szemben a hidegháború megtorlásalapú elrettentéskoncepciójával.

Az új évezredben az Egyesült Államok kiberpolitikája terrorcselekmények és kémkedési események árnyékában formálódott, aminek az lett a következménye, hogy a terület nagyban militarizálódott, és a Pentagon irányítása alá került.[26] Ezért normává vált a konkrét fenyegetések leküzdésére és a konkrét katonai műveletek támogatására irányuló politika. A jövőben e téren elképzelhető némi változás a magánszektor egyre dominánsabb jelenléte okán, azonban a katonai dominancia meg fog maradni – mert meg kell hogy maradjon a kibertér fokozatos militarizálódása miatt.

Az jelenleg nem kérdés, hogy technológiai szempontból az Egyesült Államok továbbra is a fejlesztés élvonalában áll hatalmas költségvetésének és a világ vezető magánszektorának köszönhetően, stratégiai szempontból azonban már nem olyan egyértelmű az amerikai dominancia. Az évtizedeken át alkalmazott hatásalapú megközelítést ugyanis az ellenfelek már kiismerték, és hatékonyan visszafordították az Egyesült Államok ellen 2013-tól kezdve – ahogyan az történt például a 2016-os elnökválasztásba történt orosz beavatkozás esetében. A 2018-ig eltelt öt évben az Egyesült Államok nem hajtott végre támadó kiberműveletet – ami nem azt jelenti, hogy a kibertérben Washington tétlenkedett volna, hanem azt, hogy ebben az időszakban ritkán vagy soha nem használta a kiberműveleteket nyílt válaszként vagy hatalmának rugalmasabbá tételére.[27] De felismerte, hogy lépnie kell, proaktívnak kell lennie.

Ezt az irányváltást jelezte 2018-ban a Trump-adminisztráció új nemzeti kiberstratégiája is.[28] A stratégiai irányváltás lényege, hogy az Egyesült Államok a pusztán taktikai hatások elérésétől az agresszívabb információs műveleti megközelítés felé kíván fordulni, azonban az, hogy ezt milyen lépések megtételével fogja megtenni, még erősen kérdéses.[29] Az elmozdulás első jele volt az egy hónappal később, 2018 októberében a Védelmi Minisztérium által kiadott kiberstratégia,[30] amely már új fogalomként az „előretolt védelem” *(defense forward)* koncepciót használja. Ennek lényege, hogy a Pentagon a külföldi hálózatokon

[26] Wright (2020): i. m.

[27] Marc Pomerleau: Two Years In, How Has a New Strategy Changed Cyber Operations? *C4ISRNet,* 2019a. november 11.

[28] Lásd *National Cyber Strategy of the United States of America*. 2018. szeptember.

[29] Kate Fazzini: Trump’s New Strategy Means the U.S. Could Get More Aggressive With Russia and China Over Hacking. *CNBC,* 2018. szeptember 21.

[30] *Department of Defense Cyber Strategy 2018*. (Summary.)

folyamatosan „munkálkodik" a támadások megelőzése érdekében, még mielőtt azok megtörténnének – tehát az ellenfél hálózataihoz és infrastruktúrájához hozzáférést biztosít, hogy lássa, mit is tervez.[31] Ez már ingoványos talaj a támadó műveletek felé, amit maga a stratégia is deklarál azáltal, hogy kimondja: a közös erők támadó kiberképességeket és innovatív koncepciókat fognak alkalmazni, amelyek lehetővé teszik a kibertérműveletek felhasználását a konfliktusok teljes spektrumában. Ezen is továbblépve a Kongresszus 2018 végén lehetővé tette a Kiberparancsnokságnak, hogy az Egyesült Államok hálózatain kívül, valamint a bejelentett harci zónákon (mint Szíria vagy Afganisztán) kívül is működhessen. Ez már egyértelműen „felhívás keringőre". Annak módját pedig, ahogyan a stratégiában lefektetett célokat az Egyesült Államok el kívánja érni, a „kitartó elkötelezettség" *(persistent engagament)* koncepció tartalmazza, amelynek lényege, hogy az ellenfél tevékenységét állandó nyomás alatt kell tartani, bárhol is működjön. Paul Nakasone, a Kiberparancsnokság négycsillagos parancsnoka találó hasonlatával élve: ahogyan a légierő sem tétlenkedik, a gépek nem állnak a hangárokban, hanem minden nap repülnek, információt hoznak, és ha kell, erőt demonstrálnak – ugyanez a koncepció a kibertérben is.[32] A „kitartás" a Kiberparancsnokság filozófiája szerint három részből tevődik össze: kitartó elkötelezettség, kitartó jelenlét és kitartó innováció. Ezáltal olyan új módszereket lehet és kell kifejleszteni, amelyek segítségével az ellenfelet megzavarják vagy pluszköltségek kiadására kényszerítik, elérve ezáltal azt a végcélt, hogy kétszer is meggondolja, támadni kíván-e.[33] Ez a koncepció azonban, ha (a hanyatló hatalomként épp globális jelentőségét visszanyerni igyekvő) Oroszország esetében működött is, nem biztos, hogy működni fog a felemelkedő Kínával szemben. Ahhoz, hogy a koncepció eredményesen megvalósuljon a jövőben, négy feltételnek meg kell felelnie. Ezek: a siker ütemterve (az amerikai agilitásnak költségnövelő hatása lesz, és visszatereli az ellenfelet a globális normákhoz); speciális kritériumrendszer arra az esetre, ha a koncepció működésképtelennek bizonyul; a politika fojtószelepszerepe (az amerikai elnök külföldi partnerrel való találkozása esetén a diplomácia előtérbe kerülése az ilyen műveletek lelassítása mellett); valamint

[31] Mark Pomerleau: Here's How Cyber Command's 'Defense Forward' Strategy Protects the Nation in Cyberspace. *C4ISRNet,* 2018. november 19.

[32] Ken Dilanian: Under Trump, U.S. Military Ramps up Cyber Offensive Against Other Countries. *NBCNews,* 2019. június 23.

[33] Mark Pomerleau: Cyber Command Changed Its Approach. Is the Difference Noticable? *C4ISRNet,* 2019b. augusztus 20.

az időbeli korlát (a felhatalmazások konkrét ideig szóljanak, hogy ezt követően a politikai döntéshozók áttekinthessék az elért eredményeket).[34]

A jövő kérdése, hogy ez az új stratégiai megközelítés mennyire lesz hatékony az egyre növekvő számú kibertámadással szemben. 2000 és 2016 között a rivális államok 272 dokumentált kiberműveletet hajtottak végre egymás ellen, három fő taktika mentén: a megzavarás, a kémkedés és a degradáció előnyös helyzet elérése érdekében.[35] Ezek közül mindössze 11 eredményeként sikerült olyan tartós végállapotot elérni, amely hatására a célállam viselkedése megváltozott.[36] Ez tehát nem egyértelmű siker. Kérdés továbbá, hogy megelőző jellegű támadó kiberháború esetében működésbe lép-e az úgynevezett biztonsági dilemma. Azaz egy támadó jellegű lépés más államokban félelmet kelt-e, és túlreagálást, vagy esetleg konfliktusspirált indukál. Nem kizárt ugyanis, hogy még a korlátozott célú, előretolt védelemként definiált kibernetikai támadó cselekmények is adott helyzetben félreértelmezhetők, és akaratlan eszkalációhoz vezethetnek.[37] Ez a jövőre nézve igen problémás, ugyanis az államok számára egyre nagyobb nehézséget okoz különbséget tenni a kémkedés és a nagyobb károkat okozó degradációs műveletek között. Amit az Egyesült Államok előretolt védelemnek nevez, azt Kína és Oroszország könnyen megelőző csapásnak tekintheti, ezért a következő lépés nem lesz más részükről, mint felkészülés a további támadó műveletekre. Ez az új stratégia „örök kiberháborúhoz" vezethet.[38] Ahhoz, hogy ez ne következzen be, az Egyesült Államoknak egy, az aktív védelem köré szervezett globális hálózatot kell kiépítenie, ahol a hírszerzési információkat megosztják egymással a résztvevők, és elérik azt, hogy jelentős mértékben csökkennek az ellenfelek kiberműveleteiből származó várható előnyök.

A formálódó újabb hidegháború másik, nevezzük keleti oldalának régi-új szereplője az *Orosz Föderáció,* ahol a kiberkérdések tárgyalása egészen más talajon áll. Az ország a kiber- és a kiberháború kifejezést sem alkalmazza, helyette az információs hadviselés *(informacionnoje protyivoborsztvo)* szóösszetételt használja a kiberhatások megvitatásakor. Ahogyan az Egyesült Államok

[34] Jason Healey: The Implications of Persistent (And Permanent) Engagement in Cyberspace. *Journal of Cybersecurity,* 5. (2019), 1. 1–15.

[35] Brandon Valeriano – Benjamin Jensen: The Myth of the Cyber Offense: The Case for restraint. *CATO Policy Analysis,* 2019. január 15.

[36] Ezek többsége Kína és Oroszország által az Egyesült Államok ellen irányuló, éveken át tartó kémkedés letörése volt.

[37] Valeriano–Jensen (2019): i. m.

[38] Jason Healey: Triggering the New Forever War, in Cyberspace. *The Cipher Brief,* 2018. április 1.

kiberpolitikáját a terrorizmus befolyásolta, úgy nyomták rá Oroszország ezirányú politikájára bélyegüket a Szovjetunó összeomlásából fakadó gazdasági és területi viták. Ez – instabil geopolitikai helyzettel párosulva – kettős következménnyel járt: erőteljes, proaktív összpontosítás a támadásra, valamint a kiberszuverenitásba vetett hit a szabad, nyitott információs tér helyett.[39] Ennek az orosz megközelítésnek két pillére van: az információs-technológiai és az információs-pszichológiai. Míg az előbbit a támadások jellemzik (a befolyásolási műveletektől kezdve a rosszindulatú programok ellenséges hálózatok elleni telepítéséig),[40] addig az utóbbit a botnetek és a közösségi médiában hamis felhasználói fiókok használatával lehet körülírni.[41] Ez utóbbi sikere különösen szembeötlő (volt a 2016-os amerikai elnökválasztáson is), és minden bizonnyal az információs hadviselés továbbra is kiemelkedően fontos eleme marad az orosz stratégiának – még inkább a támadó műveletekre összpontosítva.[42]

S végül: *Kína*. Az ország, amelyet már ma is a leghírhedtebb kiberháborús résztvevőnek tartanak, amely mindig arra törekszik, hogy másokkal is érzékeltesse hatalmát és befolyását.[43] Kína pártolja a kiberhatalom átfogó fogalmának használatát, amely magában foglalja egy ország cselekvésre és befolyásolásra vonatkozó képességét a kibertérben, és olyan elemekből tevődik össze, mint az IT és az IT-ipari képességek, az internetes piac és diplomáciaképességei, az internetes kultúra hatása, a katonai kibererő és a kiberstratégia-alkotásban való nemzeti érdek.[44] Oroszországhoz hasonlóan Kína is az információs műveletek kifejezést használja, és úgy véli, hogy az internetes szuverenitás nem különbözik a területi szuverenitástól. Kína végeláthatatlan háborút vív, amelyben nincs különbség békeidejű és háborús kiberműveletek között.[45] Ezen elképzeléseket a Népi Felszabadító Hadseregnél minden bizonnyal létező korlátlan hadviselés

[39] The Sinicization of Russia's Cyber Soverignty Model. *Council on Foreign Relations,* 2020. április 1.

[40] Sergei A. Medvedev: *Offense-Defense Theory Analysis of Russian Cyber Capabilities.* Calhoun Institutional Archive of the Naval Postgraduate School, 2015. március.

[41] Scott Shane: The Fake Americans Russia Created to Influence the Elections. *The New York Times,* 2017. szeptember 7.

[42] Michael Connell – Sarah Vogler: Russia's Approach to Cyber Warfare. *CNA,* 2017. március.

[43] Sachin Kumar Sahu et al.: A Review: Outrageous Cyber Warfare. *IEEE,* 2016.

[44] Li Zhang: A Chinese Perspective on Cyber War. *International Review of the Red Cross,* 94. (2012), 886.

[45] Elsa B. Kania: Cyber Deterrence in Times of Cyber Anarchy – Evaluating the Divergences in U.S. And Chinese Strategic Thinking. *International Conference on Cyber Conflict.* Washington DC., 2016. október 21–23.

doktrínája összegzi. A kifejezést először Csiao Liang és Vang Hsziang-szuj tábornok használta, kifejtve, hogy a hadviselés már nem szigorúan katonai művelet, és a harctérnek már nincsenek határai.[46] A stratégiai fordulópont dokumentáltan 2013 volt, amikor a kínai katonai doktrínában a kínai hadsereg holisztikus szempontból első alkalommal foglalkozott nyilvánosan a kiberháborúval, valamint a kiberteret a „gazdasági és társadalmi fejlődés új pilléreként és a nemzetbiztonság új területeként" határozta meg.[47] Az új offenzív kiberdoktrínát példázzák azok az esetek, amelyekben Kína a riválisaitól technológiai és szellemi tulajdont lop el katonai felhasználás céljából – mint ahogy történt az *Aurora* művelet esetében is, amikor kínaiak számos top 100 Fortune-vállalatot hekkeltek meg (úgymint a Google, a Yahoo vagy az Adobe). Egyébiránt egyedülálló a kínai doktrínában az, ahogyan az államhatalom teljes körű gyakorlásának részeként a Kínai Kommunista Párt céljainak elérése érdekében a kiberteret használja. S bár Kínával kapcsolatosan számos kérdést homály fed, afelől senkinek sem lehet kétsége, hogy Peking számára prioritás az amerikaihoz hasonló, de azt minden tekintetben felülmúló taktikai kibernetikai képesség fejlesztése. Mindezek alapján két következtetést bizonyosan le lehet vonni. Egyrészt Kína a kiberképességeit nem légüres térben fejlesztette, hanem más államok (és elsősorban az Egyesült Államok és Oroszország) változó kiberhadviselési megközelítésére és gyakorlatára válaszképp. Másrészt pedig a kínai kormány kibernetikus háborúval kapcsolatos nézetei összhangban állnak katonai stratégiájával, amelyet a biztonsági környezet változása, a hazai környezetváltozás és a külföldi hadseregek tevékenységének megfelelően időről időre módosítanak. E stratégia központi tétele az aktív védelem elve, amely alapján a kiberháborúban az elsődleges cél a védelmi képességek fokozása a túlélés és az ellensúlyozás érdekében egy támadó kibercsapás után. Kína szerint ugyanis „a legjobb védekezés a támadás" elve a kibertérben nem alkalmazható, mivel az első kibertámadás után a megcélzott fél pontos ellentámadással válaszolhat, amennyiben erős védelemmel rendelkezik. Ez esetben pedig a támadó lesz az, aki érzékeny veszteségeket szenved, ha nem rendelkezik kellőképp jó védelmi képességekkel.[48] Ennek az elméletnek a gyakorlati igazolása még a jövőre vár. Az azonban bizonyos, hogy a mai napig

[46] Jason Fritz: How China Will Use Cyber-Warfare to Leapfrog Military Competitiveness. *Culture Mandala,* 8. (2008), 1. 28–80.

[47] Lyu Jinghua: *What are China's Cyber Capabilities and Intentions?* Carnegie Endowment for International Peace, 2019. április 1.

[48] Jinghua (2019): i. m.

nincs megcáfolhatatlan bizonyíték arra vonatkozóan, hogy Kína a kibertérben támadó és megsemmisítő szándékkal lépett volna fel.

A jövő technológiái

A kiberháború jövőjét meghatározó tényezők másik csoportját az újabb és újabb eszközök kifejlesztése jelenti – ezek a jövő technológiái. A fejlődés olyan rohamos, hogy bármi konkrétumot igen nehéz lenne megjósolni, azonban az már most látszik, hogy mely technológiák azok, amelyek a jövőben meghatározóak lesznek. Ezek közül a terjedelmi korlátok okán kettőt emelek ki: a kvantumtechnológiát és a mesterséges intelligenciát.

Mi sem mutatja jobban a *kvantumtechnológia* fontosságát, mint az, hogy Hszi Csin-ping kínai elnök 2017-ben a kvantumkommunikációt és a számítástechnikát mint kiemelt „megaprojektet" nevesítette, hangsúlyozva a kvantumtechnológiák fontosságát a nemzetbiztonság szempontjából is.[49] A kvantumversenybe Kína és az Egyesült Államok is sokat fektet már most, mert pontosan tudják, hogy aki előnyre tesz szert, az büntetlenül képes lesz más államok adatbázisában bármit megtenni.[50] Sok nemzet már most olyan adatokat halmoz fel, amelyeket ma még ugyan nem tudnak visszafejteni, de kvantumszámítással megtehetnék, és a jövőben meg is fogják tenni. Emellett a kvantumszámítás alkalmazásai a kiberháborúban is korlátlanok. A 2030–2040-es évekre tehető, hogy a qubitszám (a számítógépes bitek kvantumegyenértéke) és a koherenciaidő (az az idő, amely alatt egy egység képes információt tárolni) is jelentősen meg fog nőni, olyan mértékben, hogy akár 10 másodperc alatt képesek lesznek feltörni a titkosításokat.[51] Az előrejelzések szerint a nagyszabású kvantumszámítógépek a laboratóriumokon kívül is elérhetővé válnak, ami nemcsak a kutatás számára teremt hatalmas új lehetőségeket, hanem új veszélyeket és kihívásokat is tartogat az államok számára.

[49] Elsa B. Kania – John K. Costello: Quantum Technologies, U.S.–China Strategic Competition, and Future Dynamics of Cyber Stability. *International Conference on Cyber Conflict.* Washington (DC), 2017.

[50] Matthew S. Williams: Life in 2050: A Glimpse at Warfare in the Future. *Interesting Engineering,* 2021. április 25.

[51] Jaime Sevilla – C. Jess Riedel: Forecasting Timelines of Quantum Computing. *ArXiv,* 2020. december 9.

A másik technológiai újítás, a *mesterséges intelligencia* (*artificial intelligence:* AI) számos új lehetőséget kínál a hatékonyság és az eredményesség növelésére mind a virtuális, mind a kinetikus csatatéren. Az első, aki új referenciaértékeket ér el az AI-ben, akkora erőre és előnyre tesz szert, amely lehetővé teszi számára több adat elemzését, jelentős stratégiai és taktikai előnyöket biztosítva a döntéshozatali folyamatokban. A hadműveletekben katonai előny elérése érdekében kétféleképp használható fel a mesterséges intelligencia. Vagy az aktuális katonai doktrínákba és koncepciókba épül be azzal a céllal, hogy a meglévő képességeket fokozza, vagy az emberi környezet cselekvési sebességét és hatékonyságát javítsa – ez az evolúciós út. Vagy – önállóan vagy más feltörekvő technológiákkal együtt – új doktrínák kifejlesztéséhez vezet, amelyek szembemennek a mai csatatér meglévő fizikai és jogi határaival – ez a forradalmi perspektíva.[52] Az egyes államok bármelyik utat is választják, a megszerzett előny igen jelentős lesz, és megindul a fejlődés az információs hadviseléstől az intelligens hadviselés felé. Ez a folyamat a nagyhatalmak esetében már most is zajlik, és 2030-ra látványos eredmények is várhatók.

Cyber Pearl Harbor vagy Cyber 9/11?

A válasz röviden: talán egyik sem. Ezek az elnevezések nagy háborúk, ütközetek vagy támadások tipikus jellegzetességeiből indulnak ki, és a jövő kiberháborúját igyekeznek ezen analógiák mentén vizionálni, felvázolva különböző szcenáriókat.[53]

Egy Pearl Harbor-jellegű kibertámadás hasonlóan meglepetésszerű volna, mint ahogyan a japánok 1941-ben meglepték az amerikaiakat Pearl Harbor kikötőjénél. Egy ilyen támadás, ahol a szemben álló felek állami katonai alakulatok, taktikai értelemben meglepetés volna, azonban részét képezné egy nagy hadműveletnek, geopolitikai kontextusba ágyazva. Ebből kifolyólag egy ilyen kezdeti gyors, meglepetésszerű, masszív és stratégiai hatással bíró kibertámadást minden bizonnyal egy nagy, alapvetően hagyományos háború követne, amely vélhetően a kiberhadszíntéren is folytatódna. Talán nem véletlen, hogy a 2003-as amerikai kiberstratégia még éppen egy ilyen jellegű kiberháborúval számol,

[52] Joe Burton – Simona R. Soare: *Understanding the Strategic Implications of the Weaponization of Artificial Intelligence.* 11th International Conference on Cyber Conflict, Tallinn, 2019.

[53] Részletesebben lásd: *Proceedings of a Workshop…* (2010): i. m. 86–92.

amikor kimondja, hogy „amikor egy nemzet, terroristacsoport vagy más ellenfél az Egyesült Államokat a kibertéren keresztül megtámadja, az Egyesült Államok válaszának nem kell csak a büntetőeljárásokra korlátozódnia. Az Egyesült Államok fenntartja a jogot, hogy megfelelő módon reagáljon."[54] Sőt, még 2011-ben is a CIA volt főigazgatója, Leon Panetta úgy fogalmazott, hogy a következő Pearl Harbor egy kibertámadás lehet.[55] Bár ilyen támadás azóta sem következett be, s még ha be is következne a következő tíz évben, nem valószínű, hogy azt nagyszabású, hagyományos háború követné.

Ezzel szemben a Cyber 9/11 koncepció alapján egy nem állami szereplő (például terroristacsoport) követ el kibertámadást egy állam ellen. Ez esetben a szintén meglepetésszerű és masszív támadás célpontjai azonban nem katonai, hanem civil célpontok, és az elérni kívánt hatás sem stratégiai, hanem műveleti szintű. Egy ilyen támadás egyszeri alkalom volna, az nem lenne része nagyobb műveletnek. Hatását tekintve az várható, hogy – hasonlóképp a szeptember 11-i terrortámadáshoz – bár a támadásnak sok szempontból tragikus kimenetele lenne, gazdasági hatása messze elmaradna a várttól, és az Egyesült Államok relatíve könnyen átvészelné a nehéz időszakot (ahogyan tette azt 2001-ben is a támadást követő hetekben). A támadók nem fognak elrettenni a megtámadott fél támadó kiberképességei láttán, így az nem fogja őket visszatartani tettük elkövetésétől, azonban a fizikai erővel való elrettentés adott esetben hatásos lehet. A vázolt két szcenárió kapcsolódási pontja, hogy az elnevezést adó eseményekre az Egyesült Államok válasza elhúzódó katonai kampányhoz vezetett mind konvencionálisan, mind irreguláris módon, és erre lehetne számítani a kibertérben is.

Ez a két forgatókönyv a legismertebb, azonban számos más jellegű kiberháború is elképzelhető. Ezek között említhető a különleges műveletekhez nyújtott közvetlen támogatás, a hagyományos műveletek operatív támogatása (az úgynevezett „St. Mihiel" kiberművelet), a kizárólag a kibertérben zajló háború támadó és védekező erőkkel (amely a brit légi csata után a „Cyber Battle of Britain" becenevet kapná) vagy az úgynevezett Cyber Vietnam, az online gerillaháború. A jövő több-kevesebb eséllyel ezek bármelyikét elhozhatja.

[54] *The National Strategy to Secure Cyberspace*. 2003. február. 65.

[55] Jason Ryan: CIA Director Leon Panetta Warns of Possible Cyber-Pearl Harbor. *ABC News,* 2011. február 11.

Záró gondolatok

Az elmúlt évtizedben tanúi lehettünk annak a folyamatnak, ahogyan a „kiberbiztonsági dilemma" átformálta az államok stratégiáit a növekvő kibernetikai képességeikből kiindulva. Elég, ha az észt példára gondolunk: az országot ért váratlan és nagy erejű 2007-es kibertámadást követően óriási kibernetikai képességeket fejlesztett ki, és 2008-ban a NATO is tallinni székhellyel nyitotta meg Kibervédelmi Kiválósági Központját.[56] De említhetjük a 2010-ben felállított amerikai Kiberparancsnokságot vagy annak Információs Biztonsági Bázis elnevezésű kínai mását is.[57] A politikai döntéshozók számára azonban még mindig sok a nyitott kérdés. Ezek között említhetjük, hogy vajon a hagyományos nukleáris stratégai koncepciók (mint a megelőző csapás vagy a kölcsönösen garantált megsemmisítés) használhatók lehetnek-e a mai realitás közepette.[58] Problémás továbbá, hogy a kormányok hogyan képesek reagálni a kibertér kérdéseire, amikor ennek a területnek a legnagyobb része a magánszektorban gyökerezik. Az Egyesült Államokban például a kritikus infrastruktúra mintegy 85%-át a magánszektor birtokolja vagy üzemelteti, és nem közvetlenül a szövetségi ügynökségek.[59]

A jövő bármit hozhat, hiszen háborúk vannak, voltak és lesznek. Azonban nem mindegy, hogy a jövő háborúit kik, milyen eszközökkel, hol és hogyan fogják megvívni. A számok azonban magukért beszélnek: míg 2000-ben csak hét állam[60] rendelkezett saját kibererővel, addig 2018-ban már 61.[61] Nem kérdés az ötödik hadszíntér léte és növekvő dominanciája, militarizálódásának mértéke azonban igen. A támadó kiberképességeket aszimmetrikus jellegük miatt sok olyan országban felkarolták, ahol nem rendelkeznének kellő forrással ahhoz, hogy katonai vagy gazdasági szinten versenyezni tudjanak a világ leghatalmasabb nemzeteivel. S nem szabad elfelejteni azt sem, hogy a világ egyetlen államának sincs technikai képessége a kibertámadások megelőzésére, függetlenül

[56] *NATO's Cooperative Cyber Defence Centre of Excellence.*

[57] Russell Hsiao: China's Cyber Command? *The Jamestown Foundation,* 2010. július 22.

[58] Nitin Menon: The Potential Impact of Cyber Capabilities on Future Strategy. *E-International Relations,* 2021. május 5.

[59] *Critical Infrastructure Protection, Information Sharing and Cyber Security.* U.S.

[60] Ezek: az Egyesült Államok, Oroszország, Kína, Izrael, Észak-Korea, Görögország és Thaiföld.

[61] Jason Blessing: The Global Spread of Cyber Forces, 2000–2018. In *13th International Conference on Cyber Conflict: Going Viral Proceedings 2021.* NATO CCDCOE Publications, 2021. 249.

attól, hogy azok közvetlenül egy országot céloznak-e meg, vagy annak iparát.[62] A támadások egyre szélesebb körűek lesznek, és a már most nyilvánvaló hatásukkal is minden jövőbeni fegyveres konfliktus esetén számolni kell. Kulcsszerepe lehet (és van) a nemzetközi közösségnek, amelynek meg kell találnia a módot a holnap normáinak együttes létrehozására. Ez az út azonban – már most látjuk, hogy – nagyon hosszú, buktatókkal teli, és kérdéses, hogy egyáltalán végig lehet-e menni rajta. Ugyanis az olyan legalapvetőbb jogi kérdéseket illetően is, mint a (kiber)szuverenitás, Kelet és Nyugat álláspontja gyökeresen eltér egymástól. Ha az informatikai területet az elmúlt 30 évben „fiatalnak" és „növekvőnek" nevezték, talán most eljött az idő, hogy „felnőtté" váljon.

Irodalomjegyzék

Blessing, Jason: The Global Spread of Cyber Forces, 2000–2018. In *13th International Conference on Cyber Conflict: Going Viral Proceedings 2021.* NATO CCDCOE Publications, 2021. 233–256. Online: https://ccdcoe.org/library/publications/13th-international-conference-on-cyber-conflict-going-viral-proceedings-2021/

Burton, Joe – Simona R. Soare: *Understanding the Strategic Implications of the Weaponization of Artificial Intelligence.* 11th International Conference on Cyber Conflict, Tallinn, 2019. Online: https://ccdcoe.org/uploads/2019/06/Art_14_Understanding-the-Strategic-Implications.pdf

Ciaran, Martin: *Cyber-Weapons Are Called Viruses for a Reason: Statecraft and Security in the Digital Age.* London, King's College, 2020. november. Online: https://s26304.pcdn.co/wp-content/uploads/Cyber-weapons-are-called-viruses-for-a-reason-v2-1.pdf

Clausewitz, Carl von: *A háborúról. I. kötet.* Budapest, Zrínyi, 1961.

Connell, Michael – Sarah Vogler: Russia's Approach to Cyber Warfare. *CNA,* 2017. március. Online: www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf

Critical Infrastructure Protection, Information Sharing and Cyber Security. U.S. Chamber of Commerce. Online: www.uschamber.com/issue-brief/critical-infrastructure-protection-information-sharing-and-cyber-security

Department of Defense Cyber Strategy 2018. (Summary.) Online: https://media.defense.gov/2018/Sep/18/2002041658/-1/-1/1/CYBER_STRATEGY_SUMMARY_FINAL.PDF

[62] Ivan Kwiatkowski: The Future of Cyberconflicts. *SecureList,* 2020. december 18.

Digwatch: *UN GGE and OEWG*. 2021. Online: https://dig.watch/processes/un-gge

Dilanian, Ken: Under Trump, U.S. Military Ramps up Cyber Offensive Against Other Countries. *NBCNews,* 2019. június 23. Online: www.nbcnews.com/politics/national-security/under-trump-u-s-military-ramps-cyber-offensive-against-other-n1019281

Fazzini, Kate: Trump's New Strategy Means the U.S. Could Get More Aggressive With Russia and China Over Hacking. *CNBC,* 2018. szeptember 21. Online: www.cnbc.com/2018/09/21/trump-cybersecurity-policy-offensive-hacking-nsa-russia-china.html

FM 3-38 Cyber Electromagnetic Activities. Department of the Army HQ, 2014. február. Online: https://fas.org/irp/doddir/army/fm3-38.pdf

Fritz, Jason: How China Will Use Cyber-Warfare to Leapfrog Military Competitiveness. *Culture Mandala,* 8. (2008), 1. 28–80. Online: www.international-relations.com/CM8-1/Cyberwar.pdf

Gray, Colin S.: *Making Strategic Sense of Cyber Power: Why the Sky Is Not Falling?* Strategic Studies Institute, 2013. április 1. Online: www.jstor.org/stable/resrep11496?seq=27#metadata_info_tab_contents

Healey, Jason: The Implications of Persistent (And Permanent) Engagement in Cyberspace. *Journal of Cybersecurity,* 5. (2019), 1. 1–15. Online: https://academic.oup.com/cybersecurity/article/5/1/tyz008/5554878

Healey, Jason: Triggering the New Forever War, in Cyberspace. *The Cipher Brief,* 2018. április 1. Online: www.thecipherbrief.com/triggering-new-forever-war-cyberspace

Howes, Norman R. – Michael Mezzino – John Sarkesain: *On Cyber Warfare Command and Control Systems*. (H. n.), International Command and Control Institute, 2004. Online: www.dodccrp.org/events/9th_ICCRTS/CD/papers/118.pdf

Hsiao, Russell: China's Cyber Command? *The Jamestown Foundation,* 2010. július 22. Online: https://jamestown.org/program/chinas-cyber-command/

Jinghua, Lyu: *What are China's Cyber Capabilities and Intentions?* Carnegie Endowment for International Peace, 2019. április 1. Online: https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pub-78734

Joint Operations, 17 January 2017 Incorporating Change 1, 22 October 2018. Joint Publications 3.0. Online: www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_0ch1.pdf

Joint Publication 1-02 (JP 1-02): Dictionary of Military and Associated Terms. Department of Defense. Washington, DC., 2019. október. Online: www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

Kania, Elsa B.: Cyber Deterrence in Times of Cyber Anarchy. Evaluating the Divergences in U.S. and Chinese Strategic Thinking. Washington (DC), International Conference on Cyber Conflict. 2016. október 21–23. Online: https://doi.org/10.1109/CYCONUS.2016.7836619

Kania, Elsa B. – John K. Costello: Quantum Technologies, U.S.–China Strategic Competition, and Future Dynamics of Cyber Stability. *International Conference on Cyber Conflict.* Washington (DC), 2017. Online: https://doi.ieeecomputersociety.org/10.1109/CYCONUS.2017.8167502

Kwiatkowski, Ivan: The future of cyberconflicts. *SecureList,* 2020. december 18. Online: https://securelist.com/the-future-of-cyberconflicts/99859/

Libicki, Martin C.: *Cyberdeterrence and Cyberwar.* Santa Monica (CA), Rand Corporation, 2009. Online: www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf

Libicki, Martin: Pulling Punches in Cyberspace. In *Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy.* Washington (DC), National Research Council, The National Academies Press, 2010. Online: www.nap.edu/download/12997

Medvedev, Sergei A.: *Offense-Defense Theory Analysis of Russian Cyber Capabilities.* Calhoun Institutional Archive of the Naval Postgraduate School, 2015. március. Online: https://core.ac.uk/download/pdf/36737355.pdf

Menon, Nitin: The Potential Impact of Cyber Capabilities on Future Strategy. *E-International Relations,* 2021. május 5. Online: www.e-ir.info/2021/05/05/the-potential-impact-of-cyber-capabilities-on-future-strategy/#_ftn2

Molnár Dóra: Kiberbiztonság Németországban. Pillanatkép a német digitális térről. *Nemzet és Biztonság,* 11. (2018), 1. 142–156. Online: www.nemzetesbiztonsag.hu/cikkek/neb_2018-01-09_molnar_dora_-_kiberbiztonsag_nemetorszagban-pillanatkep_a_nemet_digitalis_terrol.pdf

National Cyber Strategy of the United States of America. 2018. szeptember. Online: https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf

National Strategy to Secure Cyberspace. 2003. február. 6. Online: https://us-cert.cisa.gov/sites/default/files/publications/cyberspace_strategy.pdf

Pomerleau, Mark: Here's How Cyber Command's 'Defense Forward' Strategy Protects the Nation in Cyberspace. *C4ISRNet,* 2018. november 19. Online: www.fifthdomain.com/dod/2018/11/19/heres-how-cyber-commands-defend-forward-strategy-protects-the-nation-in-cyberspace/

Pomerleau, Mark: Cyber Command Changed Its Approach. Is the Difference Noticable? *C4ISRNet,* 2019b. augusztus 19. Online: www.fifthdomain.com/dod/cybercom/2019/08/20/cyber-command-changed-its-approach-is-the-difference-noticeable

Pomerleau, Mark: Two Years In, How Has a New Strategy Changed Cyber Operations? *C4ISRNet,* 2019a. november 11. Online: www.fifthdomain.com/dod/2019/11/11/two-years-in-how-has-a-new-strategy-changed-cyber-operations

Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy. Washington DC, National Research Council, The National Academies Press, 2010. Online: www.nap.edu/download/12997

Ryan, Jason: CIA Director Leon Panetta Warns of Possible Cyber-Pearl Harbor. *ABC News,* 2011. február 11. Online: https://abcnews.go.com/News/cia-director-leon-panetta-warns-cyber-pearl-harbor/story?id=12888905

Sahu, Sachin Kumar Kumar – Abhishek Anand – Aseem Sharma – Nidhi Nautiyal: A Review: Outrageous Cyber Warfare. *IEEE,* 2016. Online: https://doi.org/10.1109/ICICCS.2016.7542306

Sevilla, Jaime– Jess C. Riedel: Forecasting Timelines of Quantum Computing. *ArXiv,* 2020. december 9. Online: https://arxiv.org/pdf/2009.05045.pdf

Schulze, Matthias: Cyber in War: Assessing the Strategic, Tactical, and Operational Utility of Military Cyber Operations. *12th International Conference on Cyber Conflicts*. Tallinn, NATO CCDCOE Publications, 2020. Online: www.swp-berlin.org/fileadmin/contents/products/fachpublikationen/CyCon_2020_10_Schulze.pdf

Shane, Scott: The Fake Americans Russia Created to Influence the Elections. *The New York Times,* 2017. szeptember 7. Online: www.nytimes.com/2017/09/07/us/politics/russia-facebook-twitter-election.html

The Sinicization of Russia's Cyber Soverignty Model. *Council on Foreign Relations,* 2020. április 1. Online: www.cfr.org/blog/sinicization-russias-cyber-sovereignty-model

The White House: *Remarks by the President at the Cybersecurity and Consumer Protection Summit.* Stanford (CA), Stanford University, 2015. február 13. Online: https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/remarks-president-cybersecurity-and-consumer-protection-summit

Turner, Harriet Charlotte: Cyber War Forthcoming: "It Is Not a Matter of If, It Is a Matter of When". *E-International Relation,* 2020. július 8. Online: www.e-ir.info/2020/07/08/cyber-war-forthcoming-it-is-not-a-matter-of-if-it-is-a-matter-of-when

Uren, Tom – Bart Hogeveen – Fergus Hanson: *Defining Offensive Cyber Capabilities*. Australien Strategic Policy Institute, 2018. július 4. Online: www.aspi.org.au/report/defining-offensive-cyber-capabilities

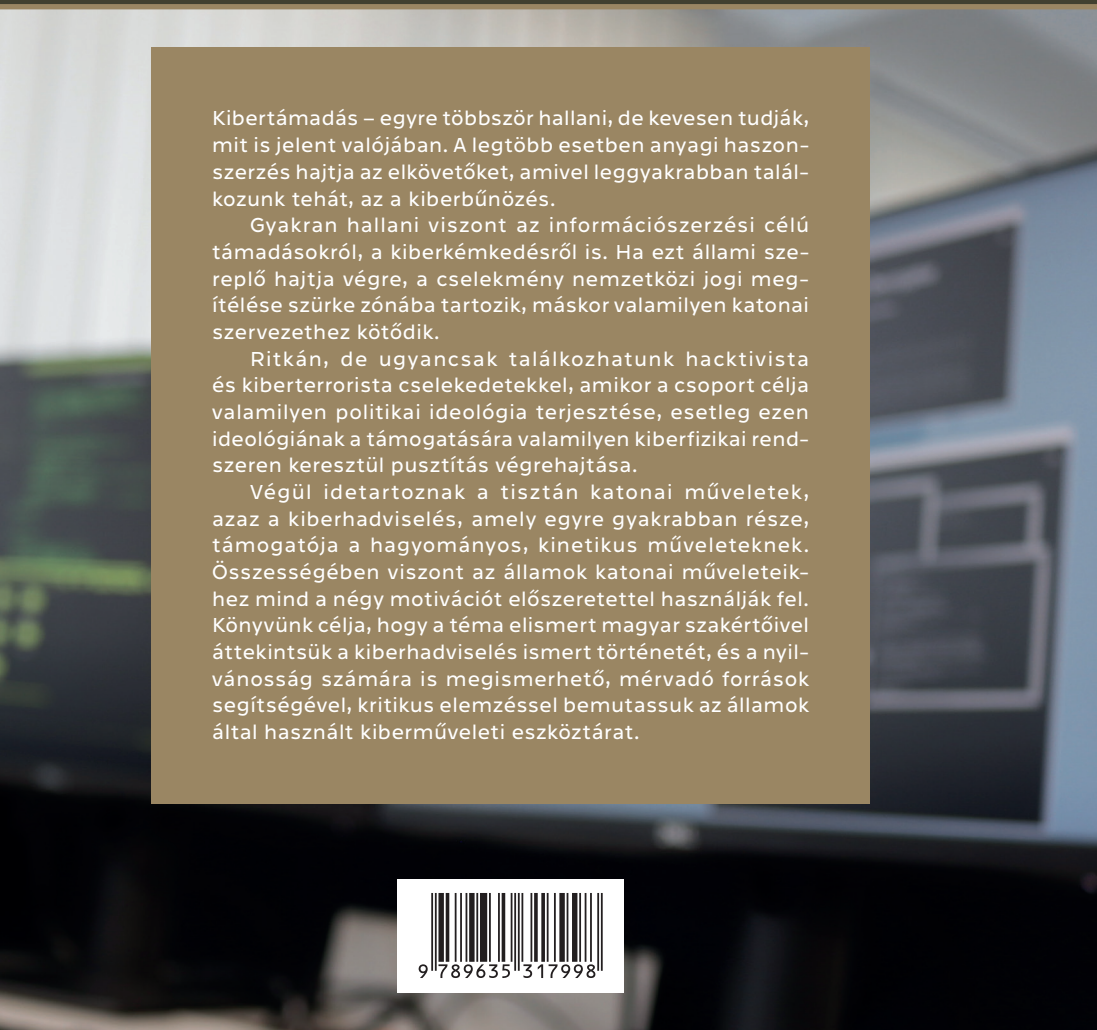
US Solarium Cyberspace Commission Report. 2020. március. Online: https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view

Valeriano, Brandon – Benjamin Jensen: The Myth of the Cyber Offense: The Case for restraint. *CATO Policy Analysis,* 2019. január 15. Online: www.cato.org/policy-analysis/myth-cyber-offense-case-restraint

Williams, Matthew S.: Life in 2050: A Glimpse at Warfare in the Future. *Interesting Engineering,* 2021. április 25. Online: https://interestingengineering.com/warfare-in-2050-what-to-expect

Wright, Aaron: The Future of Cyber Conflict. *The Cove,* 2020. augusztus 16. Online: https://cove.army.gov.au/article/the-future-cyber-conflict

Zhang, Li: A Chinese Perspective on Cyber War. *International Review of the Red Cross,* 94. (2012), 886. Online: https://international-review.icrc.org/sites/default/files/irrc-886-zhang.pdf



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