

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 képező, 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 szélesebb 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. Bárdy Tamás et al. Kaposvár, Valhalla Páholy, 1997. 205–232.

című novellájában, majd a *Neuromancer*³ című regényében. A kibertér fogalma az elmúlt évtizedekben folyamatos változás alatt állt, tartalma a fejlődés ütemével párhuzamosan 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 kibertér a 90-es évek mozgalmai leginkább a vadnyugathoz hasonlítoták, 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: *Neuromanc.* 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.

résében”, 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 legmesszemenőbb 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 szoftver-rendszert, 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 -átírányítás. Mindemellett Kína, amennyiben politikai érdekei úgy kívánják, sokkal keményebb eszközök alkalmazására is képes. 2009-ben az Urumcsiben (Hszincsiang tartomány fővárosa) történt ujjur 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 jogositványt 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 Frédéric 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 szintéren, 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 hadszíntérévé 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 Közzolgálati Egyetem Allamtudományi 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 hadművelleti fölénné válása, 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 kognitív²² 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 folytatott 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 megfélemlítést, 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, megtevesztő információk) vagy közvetett formában (az ellenfél rendszerének túlterhelése hamis adatokkal, megtevesztő 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 teleföntársaságok, bankok és médiacégek szerverei, tehát elsősorban az ország kritikus infrastruktúrái³⁰ 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 ágakat

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 megkérdőjelezhetlenné 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 elengedhetlenek a létfontosságú társadalmi feladatok ellátásához – így különösen az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához, az ország honvédelméhez – és amelyek 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 észtszágai 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 kibertérrel hivatalosan is műveleti dimenzióknak 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 kiberművelési erővel 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 harcér és a hátszág 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 csataterhez hasonló határok, frontok nehezen értelmezhetők. Ráadásul a virtuális csatater 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 Közszerződési 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-hadíjjal”, 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 ennél fogva 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 fogantatott 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 hacktívizmus, 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 Ibrv. 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 háttérében 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 ítélezési gyakorlatából következtethetünk. Az előbbi 3. cikk g) pontja kimondja, hogy agresszióknak 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 kibernézetek 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 megállapított⁶² 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 *azonnaliség* 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 Hamász⁶⁶ egyik kiberművelati 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 hadviselés⁶⁸ 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 Kézi-könyv 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 botnet-hálózatot hoztak létre, amely az orosz gépeken kívül még 178 ország területén található zombi-gépeket 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 eltekintենék 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 kibernyomozást hajtottak végre, jellemzően az ország kritikus infrastruktúrái ellen. 2015-ben az ukrainai, 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 veszítette, 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 – köztük 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 háttérében 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 válaszcsepást kell mérnie az elkövetőkre.⁸² Hiszen, amennyiben fegyveres támadásnak nyilvánul az incidens, úgy az Egyesült Államokat is megilleti az önvédelem jogának gyakorlása, így akár fegyveres válaszcsepást 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 művelési területet biztosít a katonai tevékenységek számára, amely a kiber-információszerzés és a kibervédelem területe mellett olyan kiber-támadások 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 erő 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 egyezményrel 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 a 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 Közszerződési 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, Frédéric: 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. Bárdy 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-fenyetegesek_a_cyberterb_1.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_kibert%C3%A9r_alanyai_%C3%A9s_sebezhet%C3%B6s%C3%A9ge
- 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.nemzetbiztonsag.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-kiberterven-2-resz/
- O’Neill, Patrick Howell: The Cyberattack that Changed the World. *The Daily Dot*, 2016. május 20. Online: www.dailymdot.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/

Legárd Ildikó

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_szo-veg-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/>