HADMÉRNÖK

XIV. Évfolyam 2. szám – 2019. június

A KIBERFEGYVER KONCEPCIÓ EVOLÚCIÓJA

CONCEPTUAL EVOLUTION OF CYBER WEAPONS

DÉVAI Dóra

(ORCID: 0000-0003-1024-4474)

thedevai@gmail.com

Absztrakt

Az utóbbi idők nagy erejű informatikai támadásai, mint például a BlackEnergy, NoPetya vagy a Stuxnet elodázhatatlanul felvetnek egy sor jogi, stratégiai és informatikai kérdést a nemzetállamok által politikai vagy katonai célokra felhasznált kibertámadásokkal kapcsolatban. A 1990-es évek vége óta naprenden van a kinetikus fegyverek analógiájára a kiberfegyverek szabályozásának a kérdése. Az analógia azonban nem is olyan egyértelmű. A közleményben megvizsgálom a kiberfegyverek különböző definícióit, és a koncepció lehetséges stratégiai vagy tudományos hasznosíthatóságát.

Kulcsszavak: *kiberfegyverek, nemzetközi jog, informatikai biztonság*

Abstract

Sweeping cyber attacks, for example BlackEnergy, NoPetya, or Stuxnet.have lately raised a number of urging strategic, legal and information technology-related questions concerning the use of cyber attacks by nation states. The idea to restrict the development and the use of cyber weapons have been on the agenda since the late 1990s. This article examines the range of cyber weapon definitions and their potential strategic and academic use.

Keywords: *cyber weapons, international law, information technology security*

A kézirat benyújtásának dátuma (Date of the submission): 2019.04.10.
A kézirat elfogadásának dátuma (Date of the acceptance): 2019.04.21.

BEVEZETÉS

Az elmúlt három évtizedben, a nemzetállamok és a tudományos közösségek részéről is egyre több figyelem hárult a kibertér politikai és katonai stratégiai jelentőségére. [1] Kovács László *A kibertér védelme* című könyvében részletesen tárgyalja, hogy a különböző állami és nem állami szereplők hogyan használjak ki informatikai rendszerek sérülékenységeit. [2] Haig Zsolt pedig részletesen bemutatja a kibertér, mint katonai stratégiai környezet értelmezését. [3]

A számítástechnika fejlődése a kezdetektől fogva szorosan összefonódik a katonai célokra történő alkalmazásával, ugyanakkor korán fény derült azok sérülékenységére is. Edward Hunt [4] amerikai történész korabeli források alapján illusztrálja, hogy maga az informatikai biztonság, mint diszciplína megszületése is szorosan köthető a Pentagonhoz és az ARPA-hoz[1], valamint a RAND és még egy sor hasonló, a Védelmi Minisztériumhoz tartozó stratégiai kutatóintézethez. A 1960-as években ezekben az intézményekben a mai számítógépek elődjének számító *'time-sharing'* komputerek sérülékenységének szisztematikus vizsgálatakor született eredmények nagyban hozzájárultak a mai sérülékenységvizsgálat (*pentesting*) szakterület kialakulásához. [4] Így az amerikai hadsereg informatikai szakemberei számára már korán tudatosult ezen eszközök inherens sérülékenysége, és a sérülékenységek kiaknázásának lehetősége is. Haig Zsolt [3] hívja fel a figyelmet arra, hogy az első feljegyzett vírust, a Creepert 1971-ben fedezték fel, amely az ARPANET hálózaton terjedt, és hatástalanítására alkották meg a Reaper rendszert. Mára az informatikai és kommunikációs eszközök széles körű elterjedése nyomán kialakult digitális társadalmak digitális hadseregeket hoznak létre. A kiberműveletek, vagyis az informatikai rendszerek támadása és védelme a katonai és politikai stratégiaalkotás integráns, és egyre nagyobb arányú részét képezik. [2]

Egy sor stratégiai célpont ellen intézett kifinomult informatikai támadás után, mint többek között a Stuxnet, Duqu, vagy a Red October, jött létre az igény *az informatikai rendszerekbe történő behatolás, adatlopás, rongálás céljából megalkotott rosszindulatú informatikai programok, malwerek,*[2] nemzetállamok általi fegyverként való alkalmazásának szabályozására. A kibertér és a kiberfegyverek tudományos és szakpolitikai értelmezése multidiszciplináris megközelítést igényel. A tudományos közösség részéről részben a tudományelméleti alapok elhatárolására, megteremtésére és értelmezése a cél, és elsősorban az informatikai biztonság, a nemzetközi jog, a hadtudomány, a nemzetközi kapcsolatok tudományterületeire támaszkodik. Másrészről a politikai és a védelmi szféra vezetői megalapozott stratégiai és szakpolitikai döntések kialakítására törekszenek, az adott nemzetállam érdekeinek legmegfelelőbb módon.

A nemzetközi szakirodalomban a kilencvenes évek végétől foglalkozik a kiberfegyverek koncepcionalizálásával, így a definíciók halmaza még nagyon kezdetleges képet mutat. Kérdéses egyáltalán, hogy mennyire „életképes" szakkifejezésről van szó, hiszen az alkalmazott szakterületek nagyon heterogének, ráadásul az informatikai hadviselés és az ide vonatkozó katonai stratégiák többnyire titkosítottak. Ugyanakkor a kiberműveletek egyre szélesebb körű alkalmazása szükségessé teszi a párbeszédet a különböző döntéshozók és tudományos körök között nemzeti és nemzetközi relációban. Munk Sándor a kibertér fogalmi evolúcióját vizsgáló megállapításai sok tekintetben megfigyelhetőek a kiberfegyverek koncepcionális fejlődésénél is. Munk kiemeli, hogy egy adott szakterület alapfogalmainak és szakkifejezések vizsgálata, a szakterületi

[1] Advanced Research Projects Agency

[2] Az angol malware kifejezés az angol malicious software (rosszindulatú szoftver) összevonásából kialakított mozaikszó. Mint ilyen, a rosszindulatú számítógépes programok összefoglaló neve. Ide tartoznak a vírusok, férgek (*worm*), kémprogramok (*spyware*), agresszív reklámprogramok (*adware*), a rendszerben láthatatlanul megbúvó, egy támadónak emelt jogokat biztosító eszközök (*rootkit*). http://ethical.inf.elte.hu/wiki/V%C3%ADrusv%C3%A9delem

ismeretanyag cseréjének kulcsfontosságú feltételei. [5] Ugyanez még inkább igaz, ha különböző szakterületek, sőt nemzetállamok között kell egy közös értelmezési keretet kialakítani.

Kutatásom során szekunder és primer források alapján áttekintettem a kiberfegyverek különböző megközelítéseit a következő tudományterületekre koncentrálva: az informatikai biztonsági, hadtudományi, katonai doktrínális, politikai, nemzetközi jogi és diplomáciai értelmezését. Ez a komplex megközelítés egyben arra is rávilágít, hogy a kiberfegyverek meghatározása, vagy éppen annak hiánya nagy mértékben függ a nemzetállamok politikai érdekeitől is. A kutatásom célja továbbá, annak megállapítása, hogy a kiberfegyverek különböző megközelítése milyen mértékben alapul a kinetikus fegyverek analógiáján, illetve milyen mértékben veszi figyelembe a kibertér sajátosságait.

A magyar szakirodalom és az elsődleges stratégiai források a kiberműveletekkel és a vonatkozó nemzetközi jogi kérdésekkel foglalkoznak elsősorban, viszont a kiberfegyverek koncepciója egyáltalán nem, vagy csak a közkeletű értelemben és nem tudományos megközelítésben jelenik meg. Ezért a magyar források inkább a szűkebb téma kontextuális áttekintésére adnak módot.

A KIBERFEGYVEREK MŰSZAKI MEGKÖZELÍTÉSE

Ahogy említettük, az informatikai biztonsági szakterület fejlődése szorosan köthető a védelmi szektorhoz, azonban a személyi számítógépek, az internet és az internetes kereskedelem terjedésével egyre nagyobb szerephez jutottak a kereskedelmi cégek, melyek mára már meghatározó szerepet töltenek be malwer elemzés területén. A malwarek, vagy az un. *exploitok*[3] és a felhasználásukkal elkövetett informatikai támadások kategorizálása nyilvánvalóan az informatikai biztonság műszaki alapelvein nyugszik, ezen túl pedig kidolgozták a saját modelljeiket. Ezek többnyire a fenyegetések célpontjait és a hatásmechanizmusát helyezik a középpontba. [6,7,8] A malwerek fegyverként való értelmezése nem jellemző.

A militarizált értelmezés azonban nem újdonság. Az informatikai biztonsági szakirodalomban elterjedt, a támadás fázisait leíró *kill chain* modellt a Lockheed-Martin munkatársai a katonai támadások mintájára hozták létre. Hét szakaszra bontja a kifinomult, gyakran *Advanced Persistant Threat*-nek is nevezett kibertámadások folyamatát, illetve a támadó és a védelmi oldal lépéseket. [9]

Egy szoftver program mikor tekinthető fegyvernek?

Szinte az összes kiberfegyverekkel kapcsolatos irodalomban az egyik kiemelt szempont a kiberkémkedés éles elhatárolása a kibertámadásoktól és a kiberfegyverektől. A leggyakrabban idézett érvelés, miszerint csak a károkozás, vagyis közvetlenül az informatikai eszközben, az azon tárolt adatokban, vagy közvetve az informatikai eszköz által irányított fizikai rendszerek működésében okozott fennakadás vagy fizikai kár okozására használt malware nevezhető kiberfegyvernek. [10,11] Technikai és taktikai szemszögből ez meglehetősen mesterkélt megkülönböztetés, mivel a sikeres kibertámadás előfeltétele a támadás alatt álló rendszer minél alaposabb előzetes felderítése. Informatikai biztonsági szempontból pedig már az informatikai eszközbe való behatolás is támadásnak minősül, mert megsérti a bizalmasság követelményét. Az adott malware tehát a sikeres célba jutás után még sokáig észrevétlen maradhat a

[3] Az exploit olyan kód vagy bináris program, amelynek segítésével a támadó kihasználja a programozási hibával rendelkező programok sebezhetőségét. Informatikai biztonság kézikönyve. p.24.

rendszerben, miközben egy hátsó ajtó (*backdoor*)[4] segítségével folyamatos hozzáférést biztosít, és a megfelelő pillanatban aktivizálhatja a destruktív programot (*payload*). [1] Ezért zavaros a kiberfegyverekkel gyakran azonosított *Advanced Persistent Threat* elnevezés is. Fejlett (*advanced)*: a támadás olyan magas szintű, hogy képes bejutni a magas védettségű rendszerekbe, majd pedig ott észrevétlenül maradni, miközben érzékeny adatokhoz fér hozzá. Tartós (*persistent):* nagyon nehéz a megtámadott rendszerből eltávolítani. Veszély (*threat*): rosszindulatú behatolás. Ez a tökéletes kémkedés eszköze, mégis az igen nagy erőforrás igény miatt gyakran tekintik a nemzetállamok által alkalmazott kiberfegyverként. [12] Jelentős viszont a különbség a jogi szabályozás tekintetében, mivel azon eszközök, amelyek nem minősülnek fegyvernek, használhatók békeidőben is, és nem esnek jogi ellenőrzés alá LEGAL REVIEWS OF CYBER WEAPONS.

Dorothy Denning informatikus és a Naval Postgraduate School kutatója az elsők között vetette fel a kiberfegyverek és a biztonság kérdéskörét. Denning egy 2000-ben megjelent cikkében három csoportra osztja a kiberfegyvereket, melyeket néhány jellegzetes példán keresztül mutat be. Azokat a szoftvereket tekinti támadó jellegűnek, amelyeket kizárólag károkozásra használnak, és szerinte ide tartozik a legtöbb számítógépes vírus és féreg, trójai faló, email bomba, DDOS eszközök, *exploit*[5] *script*ek[6], *rootkitek*, hátsókapuk. Védelmi jellegű szoftverek szerinte a titkosítás, hitelesítés, hozzáférés korlátozások, tűzfalak, vírus védelmi szoftverek, audit eszközök, behatolásvédelmi programok. A kettős felhasználású kiberfegyverekhez sorolja a szuperszámítógépeket, a titkosítási eszközöket, vagy például a TEMPEST-t.[7][12] Ez a megközelítés több szempontból is ellentmondásosnak tekinthető. A kettős felhasználású logikai eszköz köre nagyon tág, valamint rengeteg logisztikai eszköz, például a különböző sérülékenységvizsgálatokra használt programok tulajdonképpen védelmi célokat szolgálnak. Továbbá minimális átalakítással számos program rosszindulatúvá alakítható át. A legkifinomultabb kiberfegyverek e három kategória elemit egyszerre tartalmazzák.

Trey Herr a George Washington Egyetem, kutatója jutott eddig talán a legmeggyőzőbb eredményre a kiberfegyverek informatikai alapon történő meghatározásban. Bár 2015-ben leírt kritikája, miszerint a kereskedelmi IT biztonsági cégek malwer-kutatásai megragadnak az egyes malwerek vagy exploitok elemzésénél, vagyis a taktikai szinten, nem egészen helytálló. [10] A közelmúltban kezd kialakulni az igen átfogó, és jelentős forrásokat igénylő komplex, stratégiai szintű fenyegetettség elemzés (*threat intelligence*). Itt a cél az informatikai támadások hátterének lehető legszélesebb körű, beleértve a nemzetbiztonsági szintű felderítését. [13] A Trey által javasolt kategorizálás nem a támadás szakaszai, a felhasználó célja, vagy az egyes

[4] A hátsó ajtó olyan eszköz, amelyhez hozzáférhet egy számítógépes rendszerhez vagy titkosított adatokhoz, amelyek megkerülik a rendszer szokásos biztonsági mechanizmusait. A támadók gyakran használnak hátsó ajtókat, amelyeket egy kihasználás részeként észlelnek vagy telepítenek. Bizonyos esetekben egy féreg vagy vírus célja, hogy kihasználja a korábbi támadás által létrehozott hátsó ajtót. https://searchsecurity.techtarget.com/definition/back-door. Letöltés: 2019.03.06.

[5] Az exploit olyan kód vagy bináris program, amelynek segítésével a támadó kihasználja a programozási hibával rendelkező programok sebezhetőségét. Informatikai biztonság kézikönyve. p.24.

[6] Utasítássor.

[7] A Tempest egy titkos amerikai kormányzati projekt neve volt a 1960-as évek végén, melyben az vizsgálták, hogy a számítógépes és távközlési készülékek elektromágneses sugárzásából rekonstruálhatók-e az eredeti adatok. Ma a *Telecommunications Electronics Material Protected from Emanating Spurious Transmissions* kifejezés rövidítésére használják, ami különböző elektromágneses és akusztikus jelek távolról, kémek által történő detektálásával, valamint értelmezésével, illetve ezek megakadályozásával foglalkozik. https://searchsecurity.techtarget.com/definition/Tempest Letöltés: 2019.03.06.

támadások elemzéséből indul ki, hanem a rosszindulatú programok moduláris elemire épül. Az úgynevezett „*PrEP*” módszer a kiberfegyverek összetevőit osztja fel három nagy funkcionális csoportra. A terjesztés (*propagation method -Pr*) arra vonatkozik, hogy a malware hogyan jut el a célba vett programhoz vagy rendszerhez, például egy USB drive-on vagy egy emailen keresztül. Az *Exploit* (E) a program azon része, amely valamilyen sérülékenység kihasználásra íródott, és ez által a rendszerhez való hozzáférést biztosítja. A *Payload* (P) a célba juttatott kártevő program, amely a céleszközbe bejutva lefuttatja a megadott kódokat. Herr szerint a kiberfegyver olyan malware, amely mindhárom elemet tartalmazza és *fizikai vagy digitális kárt* okoz. [10] Ami a valódi újdonságot jelenti Herrnél, legalábbis a nyilvánosan hozzáférhető kutatások terén, az a hipotézis, miszerint a moduláris elemek összetettsége alapján tendenciózusan megkülönböztethető a nemzetállamok által használt *milware* a nem állami szereplők által használt malware-től. A vizsgálathoz egy részt a nyilvánosan elérhető elemzéseket használták fel (Stuxnet, Duqu, Duqu2, Red October) másrészt a saját maguk által elvégzett malware elemzésre (*reverse engineering*) támaszkodtak. Négy szempont alapján hasonlították össze a malwereket: a terjesztés, a célponton belüli mozgás, a payload célra szabottsága, az exploit erőssége. A lenti táblázat mutatja az eredményeiket.

Minta	**Terjesztés**	**Exploit módszer**	**Payload**	**CVSS pontszám (az exploitok átlaga)**
Milware - Sandworm	Tailored Spear Phishing	CVE-2014-4114	BlackEnergy	9.3
Milware - Sony Attacks	Tailored Spear Phishing, Physical Access	SMB Worm Tool	Listening Implant Lightweight Backdoor Proxy Tool, Destructive Hard Drive Tool, Network Propagation Wiper	N/A
Malware - Game Over Zeus	Email Spam & Compromised Web Hosts	Blackhole Exploit Kit	GOZ Server	5.0
Malware - Tiny Banker	Email Spam & Generic Spear Phishing	Blackhole Exploit Kit	Tinba Server	6.3

1. **táblázat** A malware elemzés áttekintő táblázata [14]

A KIBERFEGYVREK POLITIKAI MEGKÖZELÍTÉSE

1998 októberében nyert geopolitikai értelmezést a kiberfegyver koncepció, amikor is Oroszország az ENSZ Közgyűlés Első Bizottsága elé terjesztette a különösen veszélyes kiberfegyverek fejlesztését, előállítását és használatát tiltó szerződés kérdését. Ezt azután majd 10 évig napirenden is tartotta, azonban az Egyesült Államok beszélni sem volt hajlandó a felvetésről. 2009-ben következett be az áttörés. Az Obama kormányzat erőteljes nemzetközi diplomáciai kampányba kezdett a kibertámadások és kiberfegyverek nemzetállamok általi használatának szabályozására. Michele G. Markoff az amerikai Külügyminisztérium kiberszakértője volt 1998 és 2017 között. Elmondása szerint, az USA szintén régóta vizsgálta, hogy mivel is jár valójában az informatikai eszközök és hálózatok széles körű katonai

alkalmazása, azaz műveleti területként való kezelése. A 2007-es észt támadást követően, az USA elérkezettnek látta az időt, hogy feladja a tagadást, és kézbe vegye egy nemzetközi szabályrendszer kialakítását, a saját stratégiai érdekeinek megfelelően. Prioritása volt, hogy a kiberfegyvereket ne korlátozzák semmilyen formában, viszont kívánatos egy stratégiai stabilitás és egyensúly kialakítása, ami nem egy új, formális szerződésen alapul, hanem a nemzetállamok közötti megegyezés alapján kialakított szokásjogi normák alapján működik. Ezért azt az álláspontot kell erősíteni, hogy a nemzetállamok döntő többsége által elismert nemzetközi hadijog szabályai érvényesek az informatikai támadásokra is. A kiberfegyverek előállításához szükséges hardware és szoftver technológiát nem lehet a már meglévő fegyverzetkorlátozási rezsimekhez hasonlóan korlátozni. Így a támadható célpontokat kell korlátozni. [15]. 2009-ben megjelent az USA Nemzetközi Kiberbiztonsági Stratégiája is.

Az USA lépése felfogható válaszképpen is az Oroszország és Kína által vezetett nemzetközi csoportosulás álláspontjával szemben is. 2008-ban a Sanghaji Együttműködési Szervezet kiadta a Nemzetközi Információbiztonsági Együttműködési megegyezést. 2011-ben Oroszország, Kína, Tádzsikisztán, Üzbegisztán határozati javaslatot nyújtott be az ENSZ Biztonsági Tanácsban Nemzetközi Információbiztonsági Viselkedési Kódex címmel. A két tábor között jelentős különbségek vannak a kiber- vagy információbiztonság és a kiber- vagy információs fegyverek meghatározásában. Ez utóbbit sokkal tágabban értelmezik, mint a kiberfegyvereket. Az Együttműködési szervezet definíciója szerint az információs fegyver „*információs technológia, információs háborús módszerek*." [11] Az orosz politikai diskurzusban az információs fegyver fogalom kronológiailag tehát előbb jelent meg, mint az amerikaiban. A nyugati forrásokban is gyakran idézett S.P. Rastorguyev az orosz információs hadviselés egyik teoretikusa így határozza meg az információs fegyvereket: „*Olyan eszköz, amely azon információs rendszerek folyamatainak aktiválására (vagy blokkolására) irányul, amelyekben a fegyvereket használó személy érdekelt. Az információs fegyver bármely olyan technikai, biológiai vagy társadalmi eszköz vagy rendszer lehet, amely az adatokkal és az adatokkal működő folyamatok célszerű előállításához, feldolgozásához, továbbításához, bemutatásához vagy blokkolásához használható*." [16:6-7]

NEMZETKÖZI JOGI KÉRDÉSEK A KIBERFEGYVEREK HASZNÁLATÁT ILLETŐEN

A nemzetállamok által politikai vagy katonai célból végrehajtott informatikai támadások nemzetközi jogi felelőséget vonnak maguk után. Ebből fakadóan, a támadáshoz használható eszközök köre és a felhasználás módja is nemzetközi jogi és belső jogi szabályozás alá esik, különösen, ha egyértelműen fegyvernek minősül az adott eszköz. Jelen pillanatban azonban az informatikai hadviselés hadijogi szabályozása tisztázatlan kérdés. Az informatikai támadások és kiberfegyverek nemzetközi jogi megközelítése a legtöbb esetben szándék, illetve hatás-alapú, azaz az alkalmazott eszközök és módszerek által okozott hatás jellegéből kiindulva határozza meg az esetleges jogi kötelezettségeket. [11,17] A NATO tagországok többsége által elfogadott Tallini Kézikönyv 2.0 a következőképpen határozza meg a kiberfegyvereket: „*a hadviselés kibereszközei, amelyek jellegüknél, az alkalmazás módjából vagy tervezett módjából adódóan képesek halál vagy sérülés okozására, vagy tárgyakban olyan károkozására, illetve azok megsemmisítésére, ami elegendő a kiberművelet támadásként való értelmezéséhez*." [17:452]

„*A humanitárius nemzetközi jog elveinek alapul vételével képesek lehetünk a létező előírások megfelelő, adott esetben akár kiterjesztő értelmezésével olyan analógiák felállítására, amelyek meghatározhatnak egy „kiberháború" során alkalmazandó korpuszt. Az 1977-es I. Kiegészítő jegyzőkönyv például számos olyan hadviselési normát tartalmaz, amely megfelelő arra, hogy informatikai támadások esetében is alkalmazható legyen*" írja Lattmann Tamás. [18:8] Így

alkalmazható két irányadó alapelv, a katonai szükségesség elve[8] és a diszkrimináció elve[9]. Mindkettőt előírja a Tallini Kézikönyv 2.0 is. A kiberfegyverek tekintetében a polgári célpontok védelme különösen nehéz követelmény, tekintve, hogy az informatikai hálózatok nagy része polgári tulajdonban van, és az informatikai támadások, még az olyan specifikus malwerek esetében is mint a Stuxnet beláthatatlanul terjedhetnek tovább a világhálón.

A humanitárius nemzetközi jogon nyugszik számos fegyverzet korlátozási és leszerelési egyezmény is. Közös jogalap az 1949-es Genfi Egyezmény Első Kiegészítő jegyzőkönyvének 36 Cikkelye: „*Valamely új fegyver, hadtechnikai eszköz, vagy mód tanulmányozása, kifejlesztése, bevezetése, illetve rendszeresítése során az érintett Magas Szerződő Fél köteles megállapítani, hogy annak alkalmazása nem esik-e minden, vagy bizonyos körülmények között a jelen Jegyzőkönyv, vagy a Magas Szerződő Felet kötelező valamely más nemzetközi jogi szabály tilalma alá.*" [19:21] Ez a jogelv szintén alkalmazható a kiberfegyverekre, sőt a Genfi Egyezmény Kiegészítő jegyzőkönyveit aláíró nemzeteknek, mint például Magyarországnak is, kötelessége figyelembe venni az új hadviselési módszerek és technológiák beszerzésekor és alkalmazásakor.

A KIBERFEGVEREK A KATONAI DOKTRÍNÁKBAN

Mint említettük, a nemzetek szigorúan titkosan kezelik a kiberképességeikre vonatkozó adatokat, és a kiberműveleti stratégiáik is csak részben nyilvánosak, ezért csak korlátozott mennyiségű adat áll rendelkezésre. Az Egyesült Államok doktrínáinak vizsgálata iránymutatónak tekinthető. A nyilvánosan elérhető katonai forrásokban folyamatosan változik a kiberműveletek elnevezése: 1998-tól a *Computer Network Operations* (Összhaderőnemi Információs Műveletek Doktrína *3-13*), az offenzív és defenzív kiberműveletek (2013 március *Department of Defense Dictionary of Military and Associated Terms*). A 2018 júliusban megjelent Összhaderőnemi Doktrína már külön tárgyalja a kiberellentevékenységeket és a kibervédelmi műveleteket, és a támadó kiberműveleteken belül a különböző támadási formákat. [20: II-5-8.]

Kirívó kivétel, amikor a kiberképességekről rendelkeznek 2011-ből a Légierő *Legal Reviews of Weapons and Cyber Capabilities* című szabályzata, amely egyben az első jogi felülvizsgálat a kiberképességekre vonatkozóan. Ebben felismerhető az arra tett kísérlet, hogy feloldják az ellentmondást a fegyverek eredeti definíciója a kiberképességek között:

Fegyverek: olyan eszközök, amely célja személyek megölése, megsebesítése vagy ideiglenes ártalmatlanná tétele, vagy épületek és anyagok megsemmisítésére, rongálására vagy ideiglenes kiiktatására alkalmas.	**Kiberképességek:** bármilyen eszköz vagy *software payload*, amelynek a célja az ellenséges számítógépes rendszerek, adatok, tevékenységek vagy képességek zavarása, akadályozása, megtagadása vagy rongálása.

2. **táblázat:** Légierő definíciói 2011 [21]

[8] 1989. évi 20. törvényerejű rendelet a háború áldozatainak védelmére vonatkozóan Genfben 1949. augusztus 12-én kötött Egyezmények I. és II. kiegészítő Jegyzőkönyvének kihirdetéséről. 35. Cikk: „2. Tilos olyan fegyvereket, lövedékeket és anyagokat, valamint olyan hadviselési módokat alkalmazni, amelyek felesleges károkat, vagy szükségtelen szenvedést okoznak. 3. Tilos olyan hadviselésimódokat, vagy eszközöket alkalmazni, amelyek célzatosan vagy valószínűen nagyarányú, hosszan tartó és súlyos károkat okozhatnak a természeti környezetben" https://net.jogtar.hu/jogszabaly?docid=98900020.TVR

[9] Ibid.: 51. Cikk, 52. Cikk a polgári lakosság és tulajdon védelméről.

Tovább bonyolítja a képet, hogy az egyes haderőnemek saját hatáskörben határozzák meg a fegyverek és kiberképességek fogalmát és jogi felülvizsgálatát.

KÖVETKEZTETÉSEK

A nemzetállamok ma már politikai vagy katonai stratégiai céljaik eléréséhez felhasználják a kibertámadásokat is. Ez egyrészt egy sor jogi kötelezettségeket ró a tagállamokra. Másrészt, annak ellenére, hogy az informatikai támadások tervezése, szabályozása és alkalmazása szigorúan titkos terület, a nemzetközi közösség vezető államai részéről felmerült az igény a kiberfegyverek használatának szabályozására, aminek előfeltétele egy egységes értelmezési keret kialakítása. Megvizsgálva a különböző szakpolitikai és akadémiai diszciplináris diskurzust, arra a következtetésre jutottam, hogy definíciós kérdéskört nagyban befolyásolja a szereplők politikai vagy szervezeti érdekei. Miután a nemzetállamok egy része, beleértve a NATO tagállamokat elismerik, hogy a jelenlegi nemzetközi jog szabályai érvényesülnek a kibertérben is, a humanitárius jogi irányelvekből levezethető egy minimális közös értelmezési platform a kiberfegyverekkel kapcsolatos normákkal kapcsolatban. Ugyanakkor az akadémiai és informatikai biztonsági szempontból a kiberfegyver koncepciók meglehetősen önkényesek, tudományosan nem kellő képpen megalapozottak és meglehetősen ellentmondásosak. Az igen eltérő kondíciók miatt, a kinetikus fegyverek analógiája önmagában nem nyújt elég leíró vagy magyarázó értéket. A hadtudomány szempontjából azonban, összehasonlító esettanulmányok keretében érdemes tovább tanulmányozni az orosz vagy a kínai stratégiai gondolkodás eltérő értelmezésének feltárásához.

FELHASZNÁLT IRODALOM

[1] *Evolution of the Cyber Domain: The Implications for National and Global Security*; IISS, 2015. https://www.iiss.org/publications/strategic-dossiers/evolution-of-the-cyber-domain. (letöltve: 2016.09.12.)

[2] KOVÁCS L.: *A kibertér védelme*; Dialóg Campus 2018.

[3] HAIG ZS.: *Információs műveletek a kibertérben*; Dialóg Campus 2018.

[4] HUNT, E.: *US Government Computer Penetration Programs and the Implications for Cyberwar*. IEEE Annals of the History of Computing, Volume 34, Number 3, July-September (2012) pp. 4-21. DOI: 10.1109/MAHC.2011.82

[5] MUNK, S.: *A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései;* HADTUDOMÁNY 2018. XXVIII. 1. 113 – 132. o.

[6] KASPERSKY, 2013.: *Malware classifications|types of malware threats*; Kaspersky Lab https://www.securelist.com/en/analysis/204792265/Red_October_Detailed_Malware_Description_1_First_Stage_of_Attack. (Letöltve: 2017.01.02)

[7] SYMANTEC: *What are malware, viruses, Spyware, and cookies, and what differentiates them*? 2009. http://www.symantec.com/connect/articles/what-are-malware-viruses- spyware-and-cookiesand-what-differentiates-them. (letöltve: 2016.02.25)

[8] HYPPONEN, M.: *The Exploit Marketplace*. In: *The Fog of Cyber Defence*; National Defense University, 2013. pp. 231-234.

[9] LOCKHEED MARTIN COOPERATION: *Seven Ways to Apply the Cyber Kill Chain® with a Threat Intelligence Platform* https://www.lockheedmartin.com/content/dam/lockheed-

martin/rms/documents/cyber/Seven_Ways_to_Apply_the_Cyber_Kill_Chain_with_a_Threat_Intelligence_Platform.pdf. (letöltve: 2019.01.24).

[10] HERR,T.: *PrEP: A Framework for Malware & Cyber Weapons*; The Journal of Information Warfare, XIII. 1. 2014. http://dx.doi.org/10.2139/ssrn.2343798 (letöltve: 2019.01.24).

[11] ARIMATSU, L.: *A treaty for governing cyber-weapons: Potential benefits and practical limitations,* 4th International Conference on Cyber Conflict (CYCON 2012); NATO CCD COE Publication, Tallin, 2012. pp. 91-109. https://www.researchgate.net/publication/261044709_A_treaty_for_governing_cyber-weapons_Potential_benefits_and_practical_limitations

[12] MANDIANT: *APT1. Exposing One of China's Cyber Espionage Units*. USA, 2004. https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-areport.pdf (letöltve: 2017.01.23)

[13] DENNING, D. E.: *Reflections on Cyberweapons Controls*. Computer Security Journal, XVI 4 2000, pp. 43–53.

[14] ENISA: *Exploring the opportunities and limitations of current Threat Intelligence Platforms.* ENISA, 2017.ENISA:file:///C:/Users/D%C3%B3ra/Downloads/WP2017%20O.3.1.2u3%20-%20Limits%20of%20TISPs.pdf. (letöltve: 2019.01.02)

[15] HERR, T., ARMBRAST, E.: *Milware: Identication and Implications of State Authored Malicious Software.* New Security Paradigms Workshop 2015. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2569845. (Letöltés: 2019.02.25)

[16] MARKOFF, M., NICHOLAS, P., FINNEMORE, M., HOLLIS, D., MAUER, T.: *Cyber Norms Revisited: International Cybersecurity and the Way Forward.* Carnegie Endowement for International Peace, 2017. https://carnegieendowment.org/2017/02/06/cyber-norms-revisited-international-cybersecurity-and-way-forward-event-5490. (letöltve: 2019.01.02)

[17] RASTORGUYEV. S. P.: An Introduction to the Formal Theory of Information War. 2003. Moscow 2003, pp. 6 - 7. http://www.dodccrp.org/events/2004_CCRTS/CD/papers/064.pdf (letöltve:2019.02.25)

[18] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, 2nd Edition. Cambridge University Press, 2017.

[19] LATMANN, T.: A nemzetközi jog lehetséges szerepe az informatikai hadviselés területén. 12-23.o. In: CSAPÓ Zsuzsanna (szerk.): Emlékkötet Herczegh Géza születésének 85. évfordulójára – A ius in bello fejlődése és mai problémái. Kódex Nyomda, Pécs, 2013. 12-23.o.

[20] 1989. évi 20. törvényerejű rendelet a háború áldozatainak védelmére vonatkozóan Genfben 1949. augusztus 12-én kötött Egyezmények I. és II. kiegészítő Jegyzőkönyvének kihirdetéséről https://net.jogtar.hu/jogszabaly?docid=98900020.TVR (letöltve:2019.01.23)

[21] Joint Cyberspace Operations JP3-12. Department of Defence, Washington D.C., 2018.

[22] US Air Force Instruction 51-402. Legal Reviews of Weapons and Cyber Capabilities. 2011. https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-053.pdf. (letöltve:2019.01.23)