Nagy Zoltán András*

Kiberháborúk kora

1. Bevezető rövid történelmi visszatekintéssel

Napjainkban a valós térben a béke[1] relativizálódásának, reálisan erodálásának folyamatát éljük át. A valóságos térben – ellentmondásos módon – a második világháborúban a teheráni találkozón megalapozott, Európát felosztó nagyhatalmi alku[2] során létrejött megosztottságban leélt évtizedeket békés időszakok közé sorolhatjuk az atomfegyverek árnyékában. Bár ádáz küzdelmet vívott Nyugat- és Kelet az élet minden területén, sőt politikai, gazdasági, katonai szerepvállalásuk tetten érhető.[3] Az el nem kötelezett országok a neokolonizáció, a függetlenség, szegénység ellen hirdetett harcot Jugoszlávia, India, Indonézia, Egyip-

* *Dr. Nagy Zoltán András, tanszékvezető egyetemi docens, Nemzeti Közszolgálati Egyetem, Rendészettudományi Kar, Kiberbűnözés Elleni Tanszék, Budapest*

[1]A békét csak meghatározott földrajzi és időbeli határok között államok közötti fegyveres harcok, ideértve, polgárháborút és élet kioltásával vagy anyagi javak pusztításával együtt járó terrorcselekményt, mint állapotot értelmezzük.

[22] https://history.state.gov/milestones/1937-1945/tehran-conf, [A letöltés dátuma: 2018. 10. 20.] majd 1944.október 11-én Eden és Molotov Moszkvában kötött szégyenletes alkuja nyomán például Magyarország 80/20 %-ban orosz befolyási övezetté lett nyilvánítva. RADZINSKY, E. (1977): *Stalin. The First In-Depth Biography Based on Explosive New Documents from Russia's Secret Archives*. Anchor, 497.

Churchill szenvtelenségét a közép-kelet-európai népek iránt és Sztálin iránti elkötelezettségét az a megjegyzése is jól jellemzi, amikor a katyni mészárlásról Sikorski lengyel tábornok előtt úgy nyilatkozott: „Ha már meghaltak, akármit is tesz is, nem hozhatja vissza őket az életbe." CHURCHILL, W. (1989): *A második világháború*, 2. kötet, 1989, 211.

A fultoni beszédben pedig beismerte, hogy „megértjük; hogy Oroszországnak szüksége van a biztonságra nyugati határait illetően a német agresszió minden megismétlődésével szemben. Szívesen látjuk Oroszországot az őt megillető helyen a világ vezető nemzetei között."

http://www.okm.gov.hu/letolt/retorika/ab/szoveg/szov/chur.htm [A letöltés dátuma 2018. 10. 20.]

Ennek sajnálatos következménye, hogy Magyarország gazdasági (jóléti) lemaradása végzetes lett a nyugat-európai országokhoz képest.

[3] Koreai (1950-53), indokinai háború (1955-75), arab – izraeli háborúk, Afrika-szarván zajlott háborúk (1977-78 majd 1982), Szovjetunió Vietnam mellé állt a konvencionális kínai – vietnami háborúban (1979).

tom vezetésével. Nyugat és Kelet között a clausewitzi fogalom szerinti háború nem történt.[4] Más katonai összecsapásra nem került sor sem Európában,[5] sem az Észak-Amerikai kontinensen. A nagyhatalmi befolyáson kívül eső szélsőséges vagy palesztin terrorcsoportok (Baader-Meinhoff, Fekete Szeptember, Rote Armee Fraktion és mások) cselekményei tették viszonylagossága a békét Nyugat-Európában az 1990-es évekig.

Az összeurópai békét Tito 1980-ban törte meg. Tito halálával szertefoszlott a „testvériség – egység" elve és a tízéves (három) balkáni háború legnagyobb vesztesei a délszláv nemzetiségek.

A Szovjetunió meggyöngülését (mezőgazdaság, afganisztáni háború gazdasági – ember és erkölcsi vereségei, a hidrogénbomba atyja, Teller Ede által kitalált SDI-program meghirdetése stb.) követően a két világrendszer felbomlásával európai béke még inkább viszonylagossá vált.[6] Szovjetunió által kordában tartott (arab, afrikai, távol-keleti) or-

---

[4] „a háború …. mindenkor két élő erőnek egymás ellen intézett lökeméből áll" CLAUSEVITZ C. (1917): *A háborúról*. Budapest, 16.

[5] Extrém esetként említhetjük az angolok beavatkozását görög polgárháborúban, továbbá az egyesült államokbeli U2-es kémrepülőgép lelövését 1960-ban a szovjet területen.

[6] Országok szakadtak szét, békés különválás mellett, másutt polgárháborúkba torkollottak az elfojtott feszültségek, érdekek és érzelmek. A „nagy Oroszország kovácsolta frigy" vagy a „bratstvo i jedinstvo" erővel összetartott eszméi elillantak. Kaukázusban a háború esélye a mai napig nem csökkent. A „balkáni lőporoshordó" még mindig füstölög, sőt a volt Jugoszlávia területén zajlott háborúban a szaúd-arábiai pénz és csecsen fegyveresek által támogatott dél-balkáni vahabita közösség muszlim államról szőtt „álmának" (Bosna-Sandžak-Kosovo) végkifejlete korántsem látható előre. Ma még csak évente népszavazásokkal, kinyilatkoztatásokkal, propagandával harcolnak a függetlenségükért. De fegyverraktárak, kiképzőtáborok léte már fizikai valóság. http://kitekinto.hu/europa/2007/04/20/vahhabitak_tzharca_szerbiaban/ [A letöltés dátuma: 2018.10.20.]

Ezt a veszélyes folyamatot implicite megalapozza az, hogy a pénzügyi segítséggel és békefenntartó katonákkal támogatott soknemzetiségű- és vallású Bosznia egységének fennmaradása erősen kétséges, inkább három részre szakadása a reális, de nem kívánatos alternatíva. PIERRE-CAPS S. (1997): *Soknemzetiségű világunk*. Budapest, 6.

Napjaink Európát érintő legkomolyabb veszélyforrására utalva, a Maghreb-országok „arab szocializmusa" több országban diktatúrává változott, és mára az ISIS térnyerésének egyik oka. Ennek két közvetlen következménye az, hogy az ISIS terroristái európai célpontokat szemeltek (szemelnek) ki terrorcselekményeik végrehajtásához, másrészt a nagyhatalmak szembenállása gyengíti az ISIS elleni fellépés sikerességét, és a végeláthatatlan háború a migráns áradat legfőbb oka, amely sok millió ember Európába érkezését jelenti.

ságok, terrorcsoportok önjáróvá váltak, új terrorszervezetek jöttek létre, amelyek gátlástalanul kihasználták a világban drasztikusan létrejött differenciálódást, politikai-, vallási, nemzetiségi és más problémákat,[7] az arab világ többrétegű és megoldatlan problémáit,[8] valamint a volt gyarmatosító „nyugattal" szembeni ellenséges hangulatot.

Az Iszlám Államnak nevezett terrorszindikátusa Korán és Mohamed leegyszerűsített tanai alapján az iszlám vallás erőszakos térhódítására törekedett.

A terrorcselekmények célpontjai áttevődnek, áttevődtek Európára és Észak-Amerikára.[9] Kína gazdasági potenciálját a politikai befolyásra kívánja és fogja felhasználni, érvényesíteni Ausztrália kivételével az egész világon, öntudatosabban hallatja szavát a politikai konfliktusban. Oroszország terjeszkedési törekvései, kaukázusi háborúi, Kínához való közeledése, gazdasági problémái[10] szintén „örök" kockázati tényezők Európa számára is. Ahogy az észak-koreai atomrakéta kísérletek is nyugtalanítók.

Az Egyesült Államok (NATO) és Oroszország konfliktusai pedig önmagukban veszélyforrások Európa és Észak-Amerika számára is.

A Bismarck által emlegetett balkáni lőporoshordó, ha gyengébben is de pislákol (a török kiűzését követően itt maradt vahabita vallású lakosság Bosznia- Szandzsák – Koszovó egyesített államban bízik, Boszniát a pénz és külföldi katonaság tartja egyben).

Az európai kisebbségi problémák is csupán szunnyadnak Katalóniától, Korzikán át Erdélyig. A Brexit végig vitele sem csak gazdasági problémát jelent Nagy-Britanniának, hanem a brit tagállamokat is szembe állíthatja.

---

[7] BALLA P. (1995): Adalékok a terrorizmus fogalmához, *Belügyi Szemle*, XXXIII. 10. 32.

[8] Mesterséges határok a sivatagban, vallási megosztottság (siita-szunnita ellentét), megoldatlan (megoldhatatlan?) a palesztinok és az öt országban szétszórtan élő kurdok önálló állama.

[9] A terrorcselekmények halottainak száma is sokkolóak.2001-es több egyesült államokbeli várost érintő támadás, 2004. Madrid 191 halott, 2005. London 52 halott, 2015. január Párizs 20 halott, novemberben 137 halott és sajnos lehetne folytatni és folytatni fogjuk (!).

[10] Az orosz költségvetés bevételeit csökkentő alacsony olajár, az ukrajnai háború, az annektált ukrán területek gazdasági, pénzügyi támogatása, a távoli Szíriában vívott háború kiadásai pedig a költségvetés kiadási oldalát apasztják.

Ha a valós térben viszonylagos békéről beszélhetünk, a virtuális tér folyamatos háborúkat vélelmezünk. A valós térbeli politikai ellenérdekek küzdelme - jellemzően, és bár az ellenségek kárt okoznak, kémkednek, de a harc vértelen - a virtuális térre tevődik át. Mivel ez háború rejtve marad és – általában – nem okoz valós térbeli sérelmet, így a háborúzó felek gyakran nyúlnak ehhez az eszközökhöz.

A kibertámadások egy része közvetlenül, más részük közvetetten veszélyeztetheti a támadott állam békéjét, biztonságát.

De tegyük hozzá, hogy a háborúskodás nemcsak államok között politikai célból folynak, hanem államon belül politikai ellenfelek között politikai céllal, államhatárok nélkül gazdasági céllal és magánszemélyek által indított támadással folynak.

Jelen tanulmányunk az államok közötti politikai célú virtuális térben zajló támadásokra fókuszál.

2. Dübörgő háború a kibertérben

A kibertér ember alkotta tér, ahol nincsenek politikai vagy természeti határok, és teszi lehetővé távoli célpontok elérésére.

A kibertérből érkező támadások típusai, formái és intenzitásai függenek a támadás (valódi) céljától. Különböző sértettek ellen – különböző támadások jelezhetők előre.[11]

Ha kibertérben vívott háborúról, terrorcselekményről beszélünk, nem szükséges minden esetben új típusú cselekményekre gondolnunk. A számítógépes hálózatokon is elkövethetők olyan támadások, amelyek a *valós térben is* megvalósíthatók. Így a célpont felderítése, a kémkedés, a propaganda – hírverés az ellenség irányában (információk – dezinformációk terjesztése), az ellenség/ellenzék hangjának elfojtása, az ellenség kommunikációjának kiiktatása és egyéb cselekmények- természetesen más eszközökkel, más technikai feltételekkel, más módon és élő erővel.[12]

---

[11] MEZEI K. – NAGY Z. (2017): A zsarolóvírus és a botnet, mint napjaink két legveszélyesebb számítógépes vírusa. *Pécsi Határőr Tudományos Közlemények XIX. kötet*. Pécs, 155–163.

[12] GRAGIDO, W. – PIRC, J. (2013.): *Cybercrime and Espionage*. Amsterdam-Heidelberg-London. 3-5.; CHAWKI, M. – A. DARWISH, A. – KHAN, M. – TYAGI, S (2015.): *Cybercrime, Digital Forensics and Jurisdiction*. Springer International Publishing, Switzerland, 7–8.; NAGY Z. (2009.) *Bűncselekmények számítógépes környezetben*. Budapest, Ad-Librum Kiadó, 189–191.

Ugyanakkor, akár a kibertérben a fentiekkel paralel megvalósíthatók olyan cselekmények, amelyek *kibertérhez, számítástechnikai eszközökhöz kötöttek*, azaz e technikai feltételek hiányában nem hajthatók végre. E körben említhetők a hacking (elektronikus betörés), malwareek (malicious software – rosszindulatú szoftverek) megosztása, célzott feltöltése, terheléses támadás végrehajtása, programok manipulálása, szabotálása, e technika teremtette kommunikáció (e-mail, videókommunikáció) kifürkészése, lehetetlenné tétele, a tájékoztatást nyújtó web-oldalak felülírása (defacing) és más cselekmények.

A kibertérben valamennyi támadás-típust általában *bármely időpontban, bármely felhasználó ellen és többféle célból* el lehet követni. Potenciális áldozat lehet minden olyan intézmény, szervezet, amelynek tevékenysége döntő mértékben függ a számítógépes hálózatok és adatbázisok működőképességétől.[13] Azonban egyes támadás-típusok jellemzően egy-egy felhasználói kör ellen irányul, így például egy terheléses támadást az átlag-felhasználónak általában nem kell elszenvednie, de kritikus infrastruktúrák vagy más politikai, gazdasági, katonai célpontok már veszélyeztettek lehetnek, hasonlóan a Stuxnet, amely egy meghatározott művelet (urándúsítás) szabotálására íródott, és amely hosszas előkészület és alapos célfelderítés előzött meg. De mivel a Stuxnet, és klónja (?),[14] a DuQu már „kinn van a szabadpiacon", így az a technika-technológia, ötlet, amely egyetlen célra, egyetlen művelet megbénítására szolgál, felhasználható a katonai ellenség, a gazdasági és a politikai ellenfelekkel szemben is.

A Flame, a Gauss és más szuper kémprogramok pedig azt jelzik, hogy már nemcsak egy-egy alkalmazásra, műveletre, személyre stb. vonatkozó információgyűjtésre írt programok léteznek, hanem ennél összetettebb, több funkciót tudó programok is, amely minden olyan információt összegyűjthet, ami az adatbázisról, az adatkezelés menetéről, a felhasználókról nyújt egyszerre információkat.

A kibertérbe lépéssel a hadviselés és a terror is átlép egy határt, - nemcsak a valóságban, hiszen a hadviselő felek a velük hadban álló ország területét sértik meg, de - jelképesen is, mivel a hadviselés egy új dimenzióját jelentik, amelyek a propagandától a pusztításig terjedhet-

[13] *NBH Évkönyv 2006* (2007). Budapest, 58.

[14] Bár ma még nem (köz)ismert, hogy melyik malware volt előbb, melyiket fejlesztették ki a másikból. Egyáltalán van-e közük egymáshoz.

nek, és amelyek akár önállóan, akár a valós térbeli harci tevékenységekkel egy időben, azokat megelőzve, vagy követve azokat.

A számítástechnika tehát hadviselő felek számára egyfelől e cselekmények végrehajtásához új eszközt és/vagy helyszínt nyújt, másfelől új veszélyforrást is teremtett, mert védelmezni kell a számítógépes hálózatokat, az azokat érő támadásokat elhárítani, és ha szükséges újraépíteni, újratelepíteni kell.

A virtuális térben végrehajtott támadások lehetőségével a – fentebb idézett - clausewitzi háború fogalma is eltűnik, a háború fogalmát is újra kell gondolni.

A hadviselés során alkalmazható információs műveletek elemei:

- lélektani műveletek,
- katonai megtévesztés,
- műveleti biztonság,
- fizikai megsemmisítés,
- elektronikus hadviselés,
- számítógép-hálózati műveletek.[15]

Ez utóbbi műveletek közül a számítógép – hálózati támadásokat emeljük ki, bár hálózati támadás lehet a web-tartalmak defacelése, amelynek célja a köznyugalom megzavarása, lakosság megtévesztő tájékoztatásával köznyugalom megzavarása (a harctéri eseményekről, külés belpolitikai történésekről), illetőleg cél lehet a megfélemlítés is. Továbbá terheléses támadás vagy egy-egy malware alkalmas a megtámadott számítógép működésének szabotálására, megbénítására

A támadások végrehajtói – szemben egy átlagos kiberbűncselekménnyel – felsőfokú képzésben részt vett, felkészült profik, akiknek ez a terület a hivatása. Ma az Egyesült Államoknak, Izraelnek és más nyugat-európai országnak kiberhadserege van, amelyet kiegészíthetnek önkéntesek, akik magukkal hozzák ismeretüket, netán botnetjeiket a támadások végrehajtásához.

3. Néhány epizód a kibertéri támadások történetéből

Az államok egymás elleni és a terroristák által alkalmazott kibertérbeli támadásainak története többféle tapasztalattal szolgál, nevezete-

[15] HAIG Zs. - KOVÁCS L. – VÁNYA L. (2011): Az elektronikus hadviselés a SIGINT és cyberhadviselés kapcsolata. *Felderítő Szemle.* Budapest, MK KFH. 1 – 2. sz., 185.

sen a támadásokat a háborús vagy más harci cselekmények mely fázisában követték el és milyen támadás-típusokat alkalmaztak.

1999. május 4-én a NATO Jugoszlávia elleni légitámadása során a belgrádi kínai nagykövetséget bombatalálat érte, amelynek következtében három kínai állampolgár vesztette életét. Ezt követően kínai hackerek amerikai web-oldalak meghackelésével kísérleteztek.[16]

Az USA Jugoszlávia elleni légicsapásaival párhuzamosan Szlobodan Milosivics szerb államfő virtuális térben tett tevékenysége után intenzíven nyomozott hackerek segítségével, abból a célból, hogy nemzetközi bíróság elé állíthassák háborús és emberiességi bűncselekmények miatt.[17] Az amerikai hadsereg hackereinek (homályos) akcióival szemben voltak ellenérzések is. Egyszerűen bűncselekménynek minősítették ezeket a hacker-támadásokat.[18] Bár mára elfogadjuk azt a tényt, hogy igen az ilyen jellegű cselekmények is részei, sőt szerves részei a hadműveleteknek.

2001. április 1-én a dél-kínai partoknál, Hainan-sziget közelében egy amerikai felderítőgépet kínai harci gépek üldözték, amelyek leszállásra akarták kényszeríteni az amerikai gépet. Az üldözés során az egyik kínai harcigép és az amerikai kémrepülő összeütközött, aminek következtében a kínai repülőgép lezuhant, és az amerikai kémrepülőgép kényszerleszállást hajtott végre. Hosszas és feszült diplomáciai tárgyalások eredményeként engedték el a kínaiak az amerikai katonákat. Ez alatt az idő alatt egy kínai hackercsapat az USA ellen, több különböző kibertámadást hajtott végre. Számtalan hacker támadás érte mindkét ország szervereit. A washingtoni Fehér Ház szervereit órákra le kellett kapcsolni, a kaliforniai Igazságügy-minisztérium gépei vírusfertőzöttek lettek, és az Bellair Iskolaközpont számítógépei a kínai himnuszt játszották folyamatosan. Kínában megfertőződött szerverekről nem ismerhetünk meg részleteket. A támadások jó része grafitti-támadás volt, azaz üzeneteket jelenítettek meg egymás gépein az amerikai és a kínai hackerek.[19]

---

[16] https://sg.hu/cikkek/54768/kinanak-nincsenek-katonai-hackerei [A letöltés dátuma: 2018.10.20.]

[17] *Newsweek*, May 31. 1999. p.8.

[18] http://www.zdnet.com/article/cias-cyberwar-is-just-computer-crime/ [A letöltés dátuma: 2016.05. 10.]

[19] http://query.nytimes.com/gst/fullpage.html?res=9C04E4D61E3BF930A25756C0A9679C8B63&partner=rssnyt&emc=rss [A letöltés dátuma: 2018.10.20.]

Vélhetően a „Honker Union” (紅客) hackercsoport[20] hajtotta végre a támadásokat, köztük terheléses támadást amerikai katonai szerverek ellen. A hackercsoport azóta is hallat magáról, például 2013-ban 270 japán szerver ellen intézett támadást.

2002-ben pakisztáni és indiai hackerek támadták egymás szervereit, 111 támadás ért különféle indiai szervert.[21]

2006 júniusában marokkói szerverekről támadtak 750 izraeli szervert a palesztinok elleni akció „megtorlásaként”, amely egy izraeli katona elrablása miatt indult. Ebből is világosan kitűnik, hogy végeláthatatlan a bosszú-sorozat a három vallás közös földjén, a Szentföldön.[22]

2007 áprilisában zajlott le az államok közötti az első kiberháborúnak nevezhető (WW1 - Web War 1) kölcsönös támadás-sorozat.[23] Az orosz-észt konfliktus okául (ürügyül?) a szovjet háborús emlékművek áprilisban történő eltávolítása és a kettős (köztük orosz) állampolgárok választásból történő kizárása szolgált. Oroszországban az észt politikai döntések ellen utcai tiltakozások és kibertérben háború zajlott. Orosz hackerek Internetes fórumokon, blogokban, bulletin boards-kon botneteket szerveztek, majd ezeket egyeztetve egy időben hajtottak végre támadásokat észt miniszterelnök, miniszterek. kormányzati szerverek ellen. A támadások néhány bank pénzügyi tevékenységét sikerrel zavarták meg. A terheléses támadások mindennap zajlottak. A kiberháború Győzelem Napján csúcsosodott ki, amikor is 95 Mbps adatforgalmat regisztráltak. Naivitás volna azt hinni, hogy mindez orosz patrióták, nacionalisták hazafias akciója lett volna. 2008-ban a NATO a Cooperative Cyber Defence Center of Excellence nevű „hivatalt” hozott létre az észt fővárosban, amely a kiberháború körülményeit vizsgálta.

Ugyanebben az évben izraeli ügynökök vezető szír politikusok számítógépére *spyware-(eke)t* telepítettek egy londoni szállodában, amikor a politikusok laptopjaikat a szobájukban hagyva eltávoztak. A cél az volt, hogy a Szíriában titokban, észak-koreai segítséggel épülő alkibari atomerőműről minden információt begyűjthessenek. Ezen infor-

[20] www.w4rri0r.com/hacker-group-**honker-union**.html [A letöltés dátuma: 2018.10.20.]

[21] http://tech.transindex.ro/?hir=867 [A letöltés dátuma: 2018.10.20.]

[22] http://www.haaretz.com/hasen/spages/732465.html [A letöltés dátuma: 2018.10.20.]

[23] WILSON, C. (2008): Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. *CRS Reports for Congress*, updated January, Washington, 7–9.

mációk alapján és az USA légi támogatásával bombázták le az Szíria északkeleti részén épülő al-kibari atomerőművet szeptember 6-án.[24]

2008. április 9-én az egyesült államokbeli CNN hírtelevízióban Jim Cafferty amerikai műsorvezető – riporter a Kínában rendezendő olimpiai játékok előkészülete kapcsán egy az ott élő embereket sértő megjegyzésre ragadtatta magát: „ők ugyanolyan buta emberek és gengszterek, akik voltak 50 éve is." Erre az otromba megjegyzésre kínai hackercsoportok többféle támadást indítottak a CNN televízió és más egyesült államokbeli szerverek ellen. Megpróbálták deface-elni a CNN web-oldalát. Ennél is veszélyesebb akció volta kínai nyelvű fórumokon terjesztett terheléses támadási módszerek alkalmazása a felhasználók által.

A támadás-sorozat a DDoS-hez használt „KernelBot" kínai klónjával az „Ice Kernelel" és a Netbot Attacker programmal zajlott, mindezek terheléses támadások végrehajtásához alkalmas.[25]

A 2000-es évektől az oroszok hadvezetés az általa valós térben vívott harci cselekmények mellett gyakran alkalmazott, alkalmaz (és alkalmazni fog) kibertérbeli támadást, jellemzően terheléses támadást.[26]

A 2008-ban vívott, 5 napos orosz – grúz háború előzménye az április elején lezajlott NATO-csúcs, amelyen a tagállamok közötti vita elodázta Ukrajna és Grúzia Szövetség Tagsági Akciótervéhez (Membership Action Plan – MAP) történő csatlakozást. Ez a határozott döntésképtelenség azonban Oroszországot arra bátorította, hogy a két exszovjet ország NATO-hoz való közeledését (melynek vége a csatlakozás lett volna) megakadályozza, ellehetetlenítse. Oroszország terveit segítette az, hogy a grúz kormány folyamatosan nyomást igyekezett gyakorolni Dél-Oszétiában és Abháziában, és már csak a háború időpontja volt kétséges. Oroszország áprilisban, két ízben is felderítő repüléseket végeztek Abházia légterében, a gépeket a grúz légierő ártalmatlanított. Majd májusban 400 katonát küldött Abháziába vasútépítés ürügyével. Még a valós térben lezajlott orosz provokációk sorát gyarapította, a va-

---

[24] http://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html [A letöltés dátuma: 2018.10.20.]

[25] NAZARIO J. (2009): Politically Motivated Denial of Service Attacks, in: *The Virtual Battlefield Perspectives on Cyber Warfare* (Editors: C. Czosseck – K. Geers), Amsterdam, 186.

[26] FARIVAR C.: A Brief Examination of Media Coverage of Cyberattacks, in: NAZARIO (2009.) (ps) 182- 186.

lóstérbeli konfliktus kirobbanása előtt július végén terheléses támadással megbénította Miheil Szaakasvili grúz elnök honlapját, a web-oldal több napig elérhetetlen volt. Majd a valós térben kirobbant háborúval egy időben a kibertérben az Észtország elleni óriási adatözönnel árasztották el az oroszok a grúz elnök, a minisztériumok, hírszolgáltatók web-oldalait. A források szerint az adatáramlás a 800 Mbps-t is elérte. Néhány ellencsapás detektálható volt a grúzok, illetőleg a Grúziával szimpatizálók részéről. Több grúz web-oldal „költözött" más államok szerveire, így például az elnök web-oldalát pl. az USA-ba tükrözték, de lengyelországi szerverekről is került hivatalos grúz tartalom Internetre. Ez volt az első alkalom, hogy a valós térbeli hadműveletekkel egy időben, a kibertérben is támadás zajlott le. Ugyanakkor mindenképp figyelmet érdemel az, hogy az orosz támadásokhoz török telefonhálózatot használtak.

2008. április 28-án a Szabad Európa/Szabadság Rádió web-oldalán éles hangú kritika jelent meg a 22 évvel korábbi csernobili atomerőmű katasztrófájáról. Majd az éjjel nagy erejű terheléses támadás érte a Rádió nyolc országnak szóló web-oldalait (Fehéroroszország, Koszovó, Azerbajdzsán, Taát-Baskír Föld, Tadzsikisztán, és más oldalak). A támadás intenzitását jól jellemzi, hogy 50000 ping/másodperc terhelte a szervert. A támadás vagy fehérorosz vagy orosz támadóktól származhatott.[27]

2009-ben a kazahsztáni ellenzék web-oldalát („forum.msk"), amelyen kritikus vélemények jelentek meg a kazah elnök politikájáról terheléses támadás érte. Az adatözön beazonosított egyik forrása egy oroszországi szerver a „sexiland.ru" volt.[28]

Az orosz ellenzék internetes oldalai ellen jellemzővé vált a terheléses támadás (2007-ben Gari Kaszparov és híveinek oldalai, elérhetőségei ellen, 2008. március 14-én a Kommemersant Daily című újság web-oldalát, majd év végén a „grani.ru", „ikd.ru", „nazbol.ru" orosz ellenzéki oldalakat ért terheléses támadás).[29]

2009. január közepén a négy kirgiz internetszolgáltató közül három leállt, mert terheléses támadás bénította meg. Mivel orosz hackerek akciója volt, a támadás politikai motivációjú volt, mivel Kirgizisztán a

[27] NAZARIO 2009, 168.
[28] NAZARIO 2009, 169.
[29] https://asert.arbornetworks.com/political-ddos-ukraine-kasparov/ [A letöltés dátuma: 2018.10.20.]

területén levő manasi légibázist az Egyesült Államok rendelkezésére bocsátotta az afganisztáni hadműveletekhez. Az oroszok pénzt is ajánlottak a kirgizeknek a bázis bezárásáért.[30]

Ugyanezen év júniusában az iráni ellenzékiek kézi beállítású „page reboot" szkriptekkel próbálta lehetetleníti a kormányzati - hivatalos web-oldalakat.

Nagy visszhangot váltott ki a júliusi észak-koreai kibertámadás az Egyesült Államok kormány és kereskedelmi oldalai ellen. Negyvenezer egyesült államokbeli szervert fertőzött meg a 2004-ben felfedezett MyDoom e-mail-worm változata. A támadás hatékonyságát jelzi az, hogy több kormányzati komputerhálózat 4-5 napig működésképtelen volt. A támadás pontos hátterének tisztázását nehezítette az, hogy tucatnyi észak-koreai szerver is megfertőződött. Nyilván az Észak-Koreán belüli szerverek üzemeltetői nem tudtak a támadásról vagy a nemzetközi botrányról ezzel a manőverrel kívánták elterelni a figyelmet vagy ezek a számítógépek fertőzött amerikai kereskedelmi oldalakat látogattak (már, ha ezt az észak-koreai cenzúra engedte).

A július 4-re időzített támadás időpontja jelképes, hiszen egyfelől az Egyesült Államok szövetségi ünnepén, a Függetlenség Napján történt, másfelől Kim Ir Szen (Kim Il Sung – az angolszász nyelvekben) halálának 15. évfordulójára időzítették a támadássorozatot.

Ugyanebben az évben Izrael és a Hamas között – nyilván nem először és nem is utoljára – zajlott egy kiberháború. Egy ismert web-oldal a „Help Israel Win" szerveiről indították a „Patriot DDoS" Vélhetően izraeli hazafiak hajtották végre támadásaikat (vagy jól leplezték az izraeli hivatalos támadásokat).

Még ez év nyarán a legnagyobb burmai ellenzéki tömörülés, a Burma Demokratikus Hangja és más Burmában vagy azon kívül élő ellenzékiek web-oldalait terheléses támadás érte. A támadássorozatot megelőzte az, hogy májusban az észak-koreai diktatúrához hasonlóan működő burmai kormány – kínai nyomásra (is) - imázsát átformálni szándékozva új alkotmányt szavaztatott meg Burma lakosságával. Az ellenzék és több ország, köztük az Egyesült Államok szerint a népszavazást csalárd módon bonyolították le. Mivel a nemzetközi környezet meglehetősen rideg volt, - vélhetően - a burmai kormány az ellenzék elhallgatásának módszeréül nem az 1988-ban, majd a 2007-ben a lakos-

[30] NAZARIO 2009, 170.

ság ellen alkalmazott durva erőszakot választotta, hanem a kibertérbeli támadásokat. A támadások része volt web-oldalak defacelése is.[31]

2011. júliusában feltörték a holland DigiNotar hitelesítés szolgáltatót, és ezáltal a Google-ban hamis tanúsítványok jelentek meg (Digi Notar – case). A hacker iráni volt, aki a Hezbollah által uralt Dél-Bejrút peremvárosából, Haret Hreikből indította a támadást. A támadás oka egyértelműen bosszú volt, amiért az 1995-ben a boszniai Srebrenica városában szerbek által elkövetett muszlim lakosság elleni népirtást holland katonák „nézték végig". Azóta kiderült, hogy nemcsak ők, hanem az amerikaiak is a CIA bécsi bázisán, a felderítőgépeken levő kamerákon keresztül „élőben" az ott történteket.[32] A Hezbollah infrastruktúrája jelenti Irán számára a kitörés lehetőségét a nemzetközi elszigeteltségből.

2012 augusztusában a szaúd-arábiai Aramco olajcég 30 ezer számítógépes munkaállomását árasztották el malware-ekkel .A támadást több szervezet is magára vállalta, de két szervezetre esett a gyanú. Az egyik a Cutting Sword of Justice, míg a másik Youth Arabiannak nevezte (nevezi?) magát. Mindkettő iráni szervezet lehet, Iránhoz vagy síitákhoz köthető. Önkéntes vallási fanatikusok akciója nem biztos, hogy a valódi választ adja. A támadást muszlim vallási megosztottságot mutat, hiszen a szunnita államvallású Szaúd-Arábiát a síita államvallású Irán provokálta.

4. A legkülönösebb kibertámadás, amely a kiberháborúk új dimenzióját jelentik

A 2009-2010. években egy ismeretlen malware, a Stuxnet[33] bénította meg az iráni natanzi atomerőmű dúsítóját. A Stuxnetet és (klónját?) DuQut azért kell külön kezelnünk, mert eltér az eddigi malware-ek tulajdonságaitól, és ez veszélyességüket rendkívül megnöveli.

Egyfelől, míg az ún. nulladik napi támadást követően a malware-ek hatásmechanizmusa ismert lesz, így az ellenük kifejlesztett vírusirtó programok is hamarosan megjelennek - és legálisan vagy illegálisan –

[31] http://www.bbc.com/news/technology-11693214 [A letöltés dátuma: 2018.10.20.]
[32] http://index.hu/nagykep/2015/07/11/srebrenica/ [A letöltés dátuma: 2018.10.20.]
[33] GYEBROVSZKY T. (2014): Stuxnet – mint az első alkalmazott kiberfegyver a tallini kézikönyv szabályrendszere szempontjából, *Hadmérnök,* IX. évfolyam 1. sz., 164–172.; http://hadmernok.hu/141_16_gyebrovszkyt.pdf [A letöltés dátuma: 2018.10.20.]

hozzáférhetők. Egy „macska - egér harc” folyik, ismertté válik egy általános jellemzőkkel bíró (valamennyi fertőzött számítógépen ugyanazon károkat okozó) malware, majd megjelenik ennek az ellenszere.

A Stuxnet és a DuQu egyedi, célzott hatása miatt nem valószínű, hogy lesz általános ellenszere (víruskeresés, és -irtás). Másfelől, míg a kommersz malware-ek hatása ismert, addig ennek a két új malware csak egyetlen célba vett technikai - technológiai vagy más művelet megbénítására alkalmas.

Ha megnézzük történetüket, akkor megértjük veszélyességüket. 2010. szeptember 25-én Irán beismerte, hogy natanzi atomerőműjében technikai problémák felmerültek. Az erőmű nukleáris centrifugáiban mechanikai hibák keletkeztek. Az irániak a centrifugákat kicserélték, és felfedezték azt a malware-t, annak mutálódott formáját, amely a centrifugák abnormális működését előidézte. Ma már – nem megerősített, de nem is cáfolt forrásból - tudjuk, hogy Bush és Obama elnökök utasítására amerikai és izraeli szakemberek alkották meg ezt a malware-t.[34] A cél az iráni atomprogram akadályozása, megbénítása.[35] Az akció fedőneve: „Olympic Games” (olimpiai játékok). Mivel az atomerőművet állig felfegyverzett katonák védik, kérdésessé vált, hogy egy fegyveres, katonai akció meghozza-e a kívánt eredményt. Kockázatok sorával kellett és kell számolnia az izraeli hadvezetésnek az iráni atomerőművek megtámadásával pl. 1800 km-es távolság áthidalása, katonai veszteségek, nemzetközi közvélemény negatív viszonyulása, gondoljunk arra, hogy az Európai Unió is óvatosabb az iráni atomkísérletek megítélésében, továbbá egy azonnali, nyílt bosszú Iránról vagy Irán-barát terrorista csoportoktól a világ bármely pontján, bármikor izraeli, egyesült államokbeli polgárok (turisták, sportolók) ellen. Megoldandó feladat volt, hogy az atomerőmű belső informatikai hálózata off-line üzemmódban működött, működik, azaz nincs kapcsolata az Internettel. Bármilyen malware feltöltése csak a helyszínen lehetséges.

Mint, minden támadás első lépése: a cél felderítése volt, azaz annak megismerése, hogy a natanzi atomerőmű milyen technológiával

[34] http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyber attacks-against-iran.html?_r=1&pagewanted=all [A letöltés dátuma: 2018.10.27.]

[35] Többféle módon kívánták az iráni atomprogramot lassítani, bénítani, pl. az Irán által rendelt alkatrészeket harmadik országban titokban „átalakították”, sőt 2008-ban egy malware-rel is próbálkoztak. Talán ez a próbálkozás „altatta el” az irániakat, hogy kétszer nem lépnek ugyanabba a folyóba. De léptek, sőt sokkal agyafúrtabban.

működik, milyen hardver és szoftver erőforrásokkal rendelkezik. Ez hagyományos hírszerzői feladat volt. A megszerzett információk birtokában a cél eldöntetett, azokat a centrifugákat kellett tönkretenni, amelyek gyors és folyamatos forgásuk révén az uránban levő 235 jelű hasadó izotóp részarányát növelik. (Egy atombomba elkészítéséhez 1000 centrifuga működése szükséges egy éven át.) Natanzban 8000 centrifuga dúsította az uránt.

Az „Olympic Games" hadművelet már ismert (vagy kikövetkeztethető) elemei:

a) A malware bejuttatását a számítógépes rendszerbe megkönnyítette a Windows akkori felhasználóbarát, kényelmi funkciója, ami a számítógéphez csatlakoztatott adattárolókat automatikusan betöltötte. [36] A feltöltés a fenti források szerint egy USB pendrive-on keresztül történhetett.[37]

b) A Stuxnetnek egy Windows operációs rendszerbe kellett települni. Az operációs rendszer – természetesen - „nem enged beépülni" bármilyen programot, csak azokat, amely a Microsoft által elismert digitális aláírással rendelkeznek. Tehát olyan digitális aláírással kellett ellátnia Stuxnetet, amit a Windows elismer. Állítólag Tajvanon és állítólag lopással szerezték meg a Microsoft által is elismert JMicron és a Realtek cégek digitális aláírását. Mára egyébként ezeket a digitális jeleket érvénytelenítették. (Mondhatott volna-e mást a tajvani cég, mint azt, hogy lopás történt?)

c) A natanzi atomerőmű centrifuga vezérlőit egy Siemens WinCC program irányította, irányítja. Ehhez szoftverhez a villanymotort vezérlő eszközök csatlakoztak. Az ezek közötti kapcsolatot biztosító Step-7 nevű illesztőprogramba a Stuxnet „adminjogokkal" beépítette saját moduljait. A Stuxnet villanymotort és a centrifugavezérlők közötti

[36] A külső adathordozó behelyezésével az azon levő programok „azonnal" indulnak. A Windows az adathordozón észleli az autorun.inf fájlt, amely tartalmazza azt a következő lépést, amelyet a számítógépnek végre kell hajtania.

[37] A feltöltésnek még számos megoldása lehetett volna, pl. a kábelrendszer megcsapolása vagy akár a világban „keringtetve", a célzott személyekhez eljuttatva, akik majd adathordozóikon eljuttatják a végcélhoz. Ne feledjük, hogy a Stuxnet csak az adott környezetben, azt felismerve funkcionált, más környezetben passzív maradt.
Érdekeség kedvéért: egy kereskedelmi forgalomban kapható K…n márkanevű mini pendrive mérete: mindössze 3,9 cm x 1,235 cm x 0,455 cm és 3 gramm. Speciális célra nyilván kisebbek is alkothatók, amelyek beépíthetők golyóstollba, karórába, kulcstartóra rögzített kabalatárgyba, emblémába, sőt akár lemezes öv csatjába stb.

kapcsolatba épült be. (Honnan szereztek az amerikai - izraeli szoftverírók a német Siemenshez rendszergazda jogokat?)

d) A Stuxnetet úgy kellett megírni, hogy más rendszerekben, funkciókban nem tehessen kárt, hiszen, ha felfedezik, akkor az a főcélt veszélyeztette volna, másrészt felfedezését megkönnyítette volna. Célzottan a centrifugák működésének megzavarására alkották meg. A vírus hatása (feladata) a centrifugák rotorjai forgási sebességének lelassítása majd felgyorsítása volt. Először 86400 fordulat/perc-re gyorsította fel, amely olyan komoly rezonanciát keltett, ami tönkretette a centrifugát, majd a rotorokat lelassította, 120 fordulat/percre, amitől a centrifuga szinte leállt, aminek következtében a szétválasztott gáz ismét összekeveredett benne. Majd ismét felgyorsította, aztán ismét lelassította, és így tovább.

Mire felfedezték a vírust, addigra mutálódása révén három különböző verzió futott az atomerőmű számítógépein. 2009-2010-ben kétezer centrifugát kellett kicserélni az irániaknak. 2010 szeptemberére sikerült a vírust kiirtani az erőmű számítógépéről. Hogy mennyi késedelmet szenvedett a dúsítás? Legfeljebb bennfentesek ismerhetik a bizonytalan választ.

Az hogy, folytatódott-e, folytatódik-e kiberháború az iráni atomlétesítmények ellen nem tudjuk, nem tudhatjuk. Később felröppent egy hír, miszerint Irán leleplezett egy kiber-támadást, amelyet az USA, Izrael és Nagy-Britannia együttesen intézett iráni létesítmények ellen. De, hogy van-e alapja vagy nincs a bejelentésnek, indok-e egy későbbi megtorló akcióhoz, azt csak az érintettek ismerhetik.[38]

A perzsa atomprogramot nem lehetett leállítani, sem ilyen, sem más diplomáciai eszközökkel. Nemzetközi kontrollját a 2015-ös amerikai - iráni szerződéssel törekedtek, törekednek megteremteni. A kompromisszumok nehézségét jelzi, hogy Izrael és más államok ellenezték, ellenzik a szerződést.

---

[38] http://www.hirado.hu/Hirek/2012/06/21/21/Teheran_azt_allitja_hogy_sulyos_informatikai_tamadast_leplezett.aspx [A letöltés dátuma: 2018.10.20.]
Talán a 2012.júliusi Burgaszban izraeli turisták ellen elkövetett robbantásos merénylet volt a bosszú. Talán…. http://hvg.hu/vilag/20120718_bulgaria_izraeli_autobusz [A letöltés dátuma: 2018.10.20.]

4.1. A Stuxnet reális fenyegetése

Az első és legveszélyesebb az, hogy ismertté válásával „közkinccsé vált". Elemei kikerültek a „szabadpiacra". Ilyen a Stuxnethez hasonlító mechanizmusokat tartalmazó malware, pl. a DuQu, amelyet a Budapesti Műszaki és Gazdaságtudományi Egyetem CrySyS Adat- és Rendszerbiztonsági Laboratóriumának kiváló csapata fedezte fel és publikálta először az Interneten.[39] A hasonlóságukból adódik a kérdés, hogy melyik volt előbb? Stuxnetből ett DuQu, vagy vica versa? A DuQu eredetije tényleg a Stuxnet volt, vagy a hatásmechanizmus volt az ötlet a DuQu megírásához? Aki a DuQU-t megírta ismerte-e a Stuxnetet, ha igen, hogyan jutott az ismeretek birtokába? Ugyanazok voltak a készítők mindkét programnak? Hipotetikus kérdés továbbá az, hogy a DuQu volt a 2008-as első sikertelen Irán elleni támadáskor alkalmazott malware kísérleti példánya, amelynek továbbfejlesztett változata lett a Stuxnet?

5. Összegzésként

Néhány tanulság a kiberháború eddigi történetéből összefoglalásképpen:

1. A kibertér a hadviselésnek, a terrorcselekménynek, a földi, a légi, a tengeri és a kozmikus színterekkel egyenértékű tartománya.[40]

2. A kibertéri támadás gyakorlatilag olyan, mintegy precíziós bomba vagy rakéta.

3. A támadás célja az informatikai rendszer elleni támadás módszerét, eszközét is meghatározza. Az informatikai rendszer védelmének szintjét, miléntjét pedig a kezelt adatok tartalma, minősége szabja meg.

4. Az *államok által és más állam ellen alkalmazott számítógépes hadviselés* eszköztára, sőt sokszor elkövetői is ugyanazok, mint bármely bűncselekménynek továbbá terrorcselekménynek. Ez utóbbi utalás talán meglepő lehet, ám az államok a kibertámadások végrehajtásához a szaktudást tekintik elsődleges szempontnak, saját „white hat" elkövetői mellé szerződtethetnek ismert jó képességű hackereket. Továbbá az államok közvetlenül vagy közvetítőkön keresztül kereshetnek, „bérelhetnek, illetőleg „vásárolhatnak" (finanszírozhatnak) botnetet, vehetnek rend-

[39] http://www.crysys.hu/skywiper/skywiper.pdf [A letöltés dátuma: 2018.10.20.]
[40] HAIG – KOVÁCS – VÁNYA 2011, 196.

szer vagy szoftver loophole-okat, „zéró-napi sérülékenységről” ismeretet vagy más eszközt, tudást, például tipikusan a tor-szerverekről, ahol, az alvilág teljes eszköztára elérhető bitcoinért, vagy valós dollárért, botnetért cserébe stb.. „Bérmunkaként” hacking[41] (elektronikus betörés) is igénybe vehető.

5. Az államok által kezdeményezett kibertámadások ma már lehetnek önálló harci cselekmények (provokációk, a valós térbeli hadműveleteket megelőző, megalapozó támadások), illetőleg a valós térbeli hadműveletekhez kapcsolódnak, céljuktól függően (propaganda, dezinformáció, kommunikáció megbénítása, félelemkeltés további potenciális akciókkal stb.).

A kiberhadászati tevékenység vonatkozásában a mai katonapolitika doktrínában elfogadott megelőző csapás illetőleg az agresszió között – csupán elvi – politikai distinkció tehető –, ám a kibertámadás módszerei, céljai között nincs.

6. Új harcmodort jelentek ezek a támadások. Még inkább felértékelődnek az informatikai felkészültség, hardver- és szoftverfejlesztések.

A támadástechnikák igazolják azt axiómát, hogy a technikai – technológiai fölény békében és háborúban, akár valóstérben-, akár a kibertérben egyaránt döntő tényező. Más fogalmakkal élve az információalapú hadviselési módok a végső sikert jelentősen befolyásoló tényezők.[42]

A kibertéri hadműveletek esetében tökéletesen igaz az megállapítás, hogy „elég egyetlen évtizednyi lemaradás a csúcstechnikától és a vereség elkerülhetetlen.”[43] Konvencionális háborúkban más tényezők is

---

[41]A *hacker* olyan mesterember, aki faipari munkát végez, fát fúr-farag stb. Az 50-es évek végén az MIT nagygépek programozói nevezték így magukat. Az akkori nagygépek szűk memóriakapacitásával küszködtek. A programokból törekedtek "faragni", hogy minél több hely maradjon a számítógép memóriájában feldolgozni kívánt adatok számára. Ebben gyökerezett a 2000. év számítástechnikai problémája az ún. Y2K-probléma (a "milleneumi bomba"). A 2000-es számot, mint évet takarékossági megfontolásból 00-nak ábrázolták. Ezáltal az évszám a számítógép számára bármely 00-ra végződő évszámmal összekeverhető, ezáltal a számítógép számára értelmezhetetlen volt, vagy legalábbis annak vélték a számítástechnikai szakemberek. A probléma feloldására pótlólagosan programokat készítettek, amelyek a szoftveriparnak jól jövedelmező üzlet, biztos piacot jelentettek. Bár vitathatatlan veszélyt rejtett volna egy - egy számítógépes rendszer (energia-, pénzügyi stb.) leállása.

[42] HAIG Zs. (2007): Információs műveletek. SIGINT és az elektronikai hadviselés kapcsolatrendszere. *Felderítő Szemle. Budapest,* MK KFH, 2. sz., 27–48.

[43] PETRUSKA F. (2012): Három elfeledett háború (1. rész) – *Hadmérnök*, VII. évf. 1.

(helyismeret, lakosság támogatása, bizalma) rendkívül lényegesek, nem egyszer döntőek.

7. A kibertámadások váratlansága okoz(hat) zavart. A különböző támadástípusokra, illetve a számítástechnikai rendszer gyors helyreállítására, cseréjére is fel kell készülni.

8. Léteztek, és minden bizonnyal íródnak olyan malware-ek, melyek feltöltése off-line módon, azaz a helyszínen történik. Erre volt példa a Stuxnet, amelyet az natanzi atomerőműben töltöttek fel, vagy a civil szférából említhető, a banki automatákból a pénzkiadás „végtelenítésére" írott a bank épületében feltöltendő Tyupkin-malware. Azoknál a támadásoknál, amelyek off-line hajtanak végre, a támadót olyan személyek között kell keresnünk (és megtalálnunk), akik a hálózathoz hozzáférhetnek legálisan, akár illegálisan. Ez pedig egy fontos biztonsági tényezőre kell, hogy felhívja a figyelmet!

9. A kibertámadások kiválthatják a hagyományos fegyverek bevetését. Elkerülhetők a politikailag mindig kínos és magyarázatot kívánó emberi élet veszteségeket.

10. A kibertámadások jól leplezhetők. Az államok (tkp. hackerei) akár anonimek is maradhatnak akcióik során.

11. Magasan képzett, elméleti és szakmai-technikai ismeretekkel felvértezett kiberhadsereg lehet csak eredményes.

13. A kibertámadások tehát ugyanúgy veszélyeztetik egy-egy ország békéjét, mint a valós térben végrehajtott katonai akciók, terrorcselekmények.

14. A kibertámadások költségei minimálisak, hatásuk nagyon jelentős is lehet. A kibertámadások elleni védekezés az adott ország kiberstratégiája alapján szükséges megtervezni és létrehozni, amelyben a feladatokat, felelősségi köröket világosan meg kell fogalmazni, a humán és a technikai erőre áldozni kell, de a védekezés elsősorban az egyéni felhasználóknál kezdődik, de az országokban az állami és a magánszervezetek szervereinek védelme, e szervezetek együttműködése – ellentétes érdekeik ellenére is – elengedhetetlen. A most megszülető Nemzeti Kiberstratégia minden bizonnyal kijelöli a megteendő feladatokat.

---

szám 2012. VII. évf. 1. sz., 259.

Felhasznált irodalom:

BALLA P. (1995): Adalékok a terrorizmus fogalmához, *Belügyi Szemle*, XXXIII., 10. sz.

CHAWKI, M. – A. DARWISH, A. – KHAN, M. – TYAGI, S (2015.): Cybercrime, Digital Forensics and Jurisdiction. Springer International Publishing, Switzerland.

FARIVAR C.: A Brief Examination of Media Coverage of Cyberattacks, in: NAZARIO (2009)

GRAGIDO, W. – PIRC, J. (2013): *Cybercrime and Espionage*. Amsterdam-Heidelberg-London

GYEBROVSZKY T. (2014): Stuxnet – mint az első alkalmazott kiberfegyver a tallini kézikönyv szabályrendszere szempontjából, *Hadmérnök*, IX. évfolyam 1. sz.

HAIG Zs. – KOVÁCS L. – VÁNYA L. (2011.): Az elektronikai hadviselés, a SIGINT és a cyberhadviselés kapcsolata. *Felderítő Szemle*, X. évfolyam, 1-2. sz.

HAIG Zs. (2007): Információs műveletek. SIGINT és az elektronikai hadviselés kapcsolatrendszere. *Felderítő Szemle. Budapest*, MK KFH, 2. sz. 27-48.

MEZEI K. – NAGY Z. (2017): A zsarolóvírus és a botnet, mint napjaink két legveszélyesebb számítógépes vírusa, *Pécsi Határőr Tudományos Közlemények XIX. kötet*, 155-163

NAGY Z (2009.): *Bűncselekmények számítógépes környezetben*. Budapest

NBH Évkönyv 2006 (2007). Budapest.

NAZARIO, J. (2009): Politically Motivated Denial of Service Attacks, in: : The Virtual Battlefield Perspectives on Cyber Warfare (Editors: C. Czosseck – K. Geers), Amsterdam

NEWSWEEK, May 31. 1999.

PETRUSKA F. (2012): Három elfeledett háború (1. rész) – *Hadmérnök*, VII. évf. 1. szám 2012. VII. évf. 1. sz.

PIERRE-CAPS S. (1997): *Soknemzetiségű világunk*. Budapest.

RADZINSKY, E.(1977): *Stalin. The First In-Depth Biography Based on Explosive New Documents from Russia's Secret Archives*. Anchor.

WILSON, C. (2008): Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress. *CRS Reports for Congress*, updated January, Washington.

https://history.state.gov/milestones/1937-1945/tehran-conf, [A letöltés dátuma: 2018. 10. 20.]

http://kitekinto.hu/europa/2007/04/20/vahhabitak_tzharca_szerbiaban/ [A letöltés dátuma: 2018.10.20.]
https://sg.hu/cikkek/54768/kinanak-nincsenek-katonai-hackerei [A letöltés dátuma: 2018.10.20.]
http://www.zdnet.com/article/cias-cyberwar-is-just-computer-crime/ [A letöltés dátuma: 2016.05. 10.]
http://query.nytimes.com/gst/fullpage.html?res=9C04E4D61E3BF930A25756C0A9679C8B63&partner=rssnyt&emc=rss [A letöltés dátuma: 2018.10.20.]
www.w4rri0r.com/hacker-group-honker-union.html [A letöltés dátuma: 2018.10.20.]
http://tech.transindex.ro/?hir=867 [A letöltés dátuma: 2018.10.20.]
http://www.haaretz.com/hasen/spages/732465.html [A letöltés dátuma: 2018.10.20.]
http://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html [A letöltés dátuma: 2018.10.20.]
https://asert.arbornetworks.com/political-ddos-ukraine-kasparov/ [A letöltés dátuma: 2018.10.20.]
http://www.bbc.com/news/technology-11693214 [A letöltés dátuma: 2018.10.20.]
http://index.hu/nagykep/2015/07/11/srebrenica/ [A letöltés dátuma: 2018.10.20.]
http://hadmernok.hu/141_16_gyebrovszkyt.pdf [A letöltés dátuma: 2018.10.20.]
http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=1&pagewanted=all [A letöltés dátuma: 2018.10.27.]
http://www.hirado.hu/Hirek/2012/06/21/21/Teheran_azt_allitja_hogy_sulyos_informatikai_tamadast_leplezett.aspx [A letöltés dátuma: 2018.10.20.]
http://hvg.hu/vilag/20120718_bulgaria_izraeli_autobusz [A letöltés dátuma: 2018.10.20.]
http://www.crysys.hu/skywiper/skywiper.pdf [A letöltés dátuma: 2018.10.20.]