Fekete Csanád

A kiberhadviselés fejlődése és az ukrán válság

Rezümé

A Krím félsziget kapcsán kirobbant válság során aktivizálták magukat az orosz és ukrán hackercsoportok, melynek hatására a konfliktus átterjedt a kibertérre. Célom, hogy röviden ismertessem a kibertér konfliktusokban játszott szerepének felértékelődéséhez vezető folyamatokat, különös hangsúlyt fektetve Oroszország e téren folytatott törekvéseire. Írásom második felében bemutatom az ukrán válságot kísérő „kiberháború" főbb mozzanatait és annak jellemző vonásait.

Kulcsszavak: krími-válság, kiberhadviselés, információs műveletek

Resume

During the crisis in the Crimean peninsula, Russian and Ukrainian hacker groups appeared, causing the conflict to spread to cyberspace. My aim is to briefly describe the processes leading to the increased role of cyberspace under conflicts, with particular emphasis on Russia's efforts. In the second half of my paper, I will detail the key elements and features of the "cyberwar" that accompanied the Ukrainian crisis.

Keywords: crimean crisis, cyber-warfare, information operations

Bevezetés

A kibertérben elkövetett támadások gyakorisága az elmúlt évek során dinamikusan növekedett,[1] így a kiberbiztonság napjaink legfontosabb biztonsági kihívásai közé tartozik. Az elmúlt évtizedben számos nemzetközi szervezet és kormány felismerve a kibertér sebezhetőségét, lépéseket tett a fenyegetések kezelése érdekében. Az utóbbi években a kritikus információs infrastruktúra (KII), és a kibertér biztonságának védelmében az egyes országok és szervezetek létrehozták kiberstratégiáikat, megteremtették a szükséges

[1]A 2013 végére a beazonosított malware-k száma 170 millióra nőtt, melyek közül minden egyes példány akár támadások százezreiért lehet felelős. Csak 2013 szeptemberében a kéretlen üzenetek (spamok) száma elérte a 4 trilliót. Lásd: Andrzej Kozłowski, Kacper Rękawek, Marcin Terlikowski: Cyberterrorism: The Threat That Never Was. PISM Strategic Files, No. 4. (40). p. 1-2. in: http://www.pism.pl/files/?id_plik=16470, Letöltve: 2014.06.07.

intézményi hátteret.[2] Az egyes kormányzatok, a kibervédelmi képességek fejlesztése terén tett erőfeszítések ellenére, továbbra is ki vannak téve a kibertérből származó fenyegetéseknek, köszönhetően az egyre kiterjedtebbé váló rosszindulatú tevékenységeknek.[3] Az utóbbi időben jelentősen megugrott a különböző kormányszerveket és globális vállalatokat érintő, nagy szakértelemmel végrehajtott célzott támadások száma.[4] Ezek a támadások főként az érzékeny adatok megszerzésére és a fontos rendszerek megbénítására irányulnak, továbbá megfigyelhető az is, hogy a támadók egyre nagyobb figyelmet fordítanak az új technikák és módszerek alkalmazására.

Az utóbbi években kifejlesztésre kerültek olyan komplex felépítésű kártevők, mint a 2010-ben felfedezett Stuxnet, melynek feladata a szakértők szerint Irán nukleáris létesítményeinek megbénítása volt.[5] Mindez arra a növekvő tendenciára hívja fel a figyelmet, hogy a kibertérben zajló rosszindulatú tevékenységek ma már nem csak magányos hackerekhez és egyéb bűnözői csoportokhoz köthetők. Az utóbbi időben a támadások mögött rejlő motivációk, valamint az alkalmazott eszközök és módszerek jelentős változáson mentek keresztül, szakértők szerint az olyan szintű programok megírása, mint amilyen a Stuxnet is volt szinte lehetetlen állami támogatás nélkül.[6] A különböző kormányok felismerték a hacker csoportokban rejlő potenciált és felhasználják őket az állami, katonai és egyéb gazdasági érdekek elérése céljából.[7] Ezen folyamat tetten érhető az utóbbi évtized minden jelentősebb konfliktusában, természetesen ez alól a jelenleg is zajló ukrán válság sem kivétel. E tendencia többek között azt vonja maga után, hogy az utóbbi időben megszületett kibervédelmi stratégiák máris felülvizsgálatra szorulnak.

---

[2]E folyamatba illeszkedik, hogy 2013-ban kiadták Magyarország Nemzeti Kiberbiztonsági Stratégiáját. Lásd: A Kormány 1139/2013. (III. 21.) Korm. határozata Magyarország Nemzeti Kiberbiztonsági Stratégiájáról. in: http://www.mysec.hu/download/MK2013_47_M_N_Kiberbiztonsagi_Stratagiaja.pdf, Letöltve: 2014.06. 12.

[3]Tiffany Kaiser: DHS: Cyber Attacks Against U.S. Infrastructure Increased by 52 Percent in 2012. in: http://www.dailytech.com/DHS+Cyber+Attacks+Against+US+Infrastructure+Increased+by+52+Percent+in+2012/article29632.htm, Letötve: 2014. 06. 07.

[4]2012-ben 42%-al nőtt az ilyen támadások száma. Lásd: Andrzej Kozłowski, Kacper Rękawek, Marcin Terlikowski: Cyberterrorism: The Threat That Never Was. PISM Strategic Files, No. 4. (40). p. 2. in: http://www.pism.pl/files/?id_plik=16470, Letöltve: 2014.06.07.

[5]Cserháti András: A Stuxnet vírus és az iráni atomprogram. Nukleon on-line folyóirat, Magyar Nukleáris Társaság, 2011. április 5. in: mnt.kfki.hu/Nukleon/index.php?action=abstract&cikk=155, Letöltve: 2014.07. 27.

[6]Jaikumar Vijayan: Government role in Stuxnet could increase attacks against U.S. firms. Computerworld, 2012. 06.02.In:http://www.computerworld.com/s/article/9227696/Government_role_in_Stuxnet_could_increase_attacks_against_U.S._firms,Letöltve: 2014. 06. 08.

[7]Feltételezhetően ilyen magasan képzett hackerekből toborozhatták a Kínai Népi Felszabadító Hadsereg 61398-as számú egységét. A csoport tevékenységéről részletesebben itt: William Knowles: U.S. Department of Justice Indicts Five Members of the Chinese PLA 'Unit 61398' for Cyber Espionage. Infosec News, 2014. 05. 20. in: http://www.infosecnews.org/u-s-department-of-justice-indicts-five-members-of-the-chinese-pla-unit-61398-for-cyber-espionage/, Letöltve: 2014.06. 27.

Az információs műveletek és az információs hadszíntér

Az információs társadalmak kialakulását követően, megnőtt az információs műveletek konfliktusokban[8] játszott jelentősége, melyek a hagyományos hadszíntereken folyó katonai tevékenységekkel párhuzamosan, az információs hadszíntéren folynak. Az információs korszak, információs környezet, információs társadalom és a digitális, precíziós és hálózatos hadseregek megjelenése következtében, a katonai műveletek által érintett területek és tartományok tovább bővültek. A szárazföldi, tengeri, légi és kozmikus hadszíntér mellett a hadviselés egy újabb tartománya jelent meg, melyet információs hadszíntérnek nevezünk.[9] A hadviselés ezen tartományában a többi hadszíntérrel szoros összhangban folyó katonai tevékenység az információ megszerzéséért, megtartásáért, és hatékony használatáért folyik. Az információs hadszíntér magába foglalja az összes valós és virtuális teret, helyet, eszközt és rendszert, amely az információ megszerzésével, előállításával, feldolgozásával, felhasználásával, tárolásával és védelmével foglalkozik. Az információs hadszíntér a globális információs környezet része, a valódi hadszíntéren túlnőve magába foglalja a hátországban működő katonai és polgári szervek infokommunikációs rendszereit és szervezeteit, melyek támogatják, biztosítják vagy jelentősen befolyásolják a katonai műveleteket.[10] Az információs műveletek működési környezetében, az információs hadszíntéren a tevékenységek, fizikai, információs és tudati dimenziókban egyaránt folyhatnak. A fizikai dimenzióban, az információs rendszerek és infrastruktúrák ellen végrehajtott fizikai támadások és az azok védelmére irányuló tevékenységek zajlanak. Az információs dimenzióban folytatott információs műveletek, az elektronikus információs folyamatok – adatszerzés, adattárolás, feldolgozás, kommunikáció – elektronikai úton történő támadása, annak érdekében, hogy a célpontokat és azok működését fizikai romboló ráhatás nélkül lehessen befolyásolni. A tudati dimenzióban az emberi gondolkodást veszik célba, – az észlelést, érzékelést, értelmezést,

[8] A szakértők szerint a történelem első információs háborúja az 1991-es, első Öböl-háború, az első hálózatos-vezetésű háborúja a 2003-as, második Öböl-háború volt. In: Dr. Haig Zsolt, Dr.Várhegyi István: Hadviselés az információs hadszíntéren, p. 181.

[9]Haig Zsolt, Várhegyi István: A cybertér és a cyberhadviselés értelmezése. HADTUDOMÁNY XVIII. Évf, p. 2. in: http://mhtt.eu/hadtudomany/2008/2008_elektronikus/2008_e_2.pdf, Letöltve: 2014.06.08.

[10]Haig Zsolt, Várhegyi István: Hadviselés az információs hadszíntéren p. 157.

véleményt, vélekedést – csúsztatott, hamis vagy valós információkkal, amit elektronikus és nyomtatott média útján, vagy közvetlenül beszéd formájában terjesztenek.[11]

A harc-hadműveleti támogatás (Combat Support) körébe tartozó információs műveletek tehát három dimenzióban folyó, koordinált tevékenységek, amelyek a szemben álló fél információira, információalapú folyamataira és infokommunikációs rendszereire gyakorolt ráhatások útján képesek befolyásolni a döntéshozókat, a politikai és katonai célkitűzéseik elérésében. Az információs műveletek célja a hadműveleti előny elősegítése, az információs fölény, információs uralom és vezetési fölény kivívása által.[12] Ezen tevékenységnek két azonos fontosságú oldala van, megvédeni és kihasználni a saját, gyengíteni és befolyásolni a szemben álló fél információs képességeit. Mindezek elérése érdekében az adott szervezetek a béke és konfliktusok időszakában egyaránt hajtanak végre információs műveleteket. Amíg a hagyományos katonai műveletek általában az ellenség erőinek és eszközeinek a tűzzel való pusztítására irányulnak, addig az információs műveletek az ellenség információinak, és információs képességeinek, vezetés-irányítási rendszereinek felderítésére, befolyásolására, és a saját hasonló rendszerek és képességek alkalmazására és védelmére törekszenek. Az információs műveletek alkalmazása kevesebb erőforrás bevonásával, és a veszteségek csökkentésével teszi lehetővé a győzelem kivívását.[13]

Az információs műveletek mellett további információs tevékenységi formák is léteznek, melyek az egymással szemben álló felek közötti információalapú folyamatok befolyásolásával foglalkoznak. Ezek közé tartozik az információs hadviselés (Information Warfare) és a vezetési hadviselés (Command and Control Warfare). Az Egyesült Államok összhaderőnemi információs műveleti doktrínája (JP 3-13) az információs hadviselés alatt azon információs műveleteket érti, melyeket válság vagy háborús konfliktusok során alkalmaznak az ellenséggel szemben, a különböző célok elérése vagy elősegítse érdekében. A vezetési hadviselés a pszichológiai műveletek, katonai megtévesztés, műveleti biztonság, fizikai megsemmisítés és elektronikai hadviselés összehangolt alkalmazása az ellenség vezetési lehetőségeinek csökkentése, befolyásolása, rombolása, illetve a saját oldali vezetési

[11]Haig Zsolt: Az információbiztonság komplex értelmezése. Robotadviselés tudományos konferencia kiadványa. Hadmérnök különszám 2006. nov. 22. in:http://www.zmne.hu/hadmernok/kulonszamok/robothadviseles6/haig_rw6.html, Letöltve: 2014.06. 27.
[12]Haig Zsolt, Várhegyi István: Hadviselés az információs hadszíntéren, p. 185.
[13]Ibid., p. 186.

képességek védelme érdekében.[14] A konfliktusok szintje alapvetően befolyásolja az infokommunikációs rendszerek elleni ellenséges tevékenységek körét és mértékét. Békeidőben az információs tevékenységek a számítógép-hálózatokba történő illetéktelen behatolásra és a különböző passzív eszközökkel végzett elektronikai felderítésre terjednek ki. Ezek a rendszer gyenge pontjainak és sebezhetőségének felmérésére irányulnak. A válság elmélyülésével számítani lehet az infokommunikációs rendszerek ellen végrehajtott közvetlen támadásokra. A katonai műveletek kezdetét napjainkban rendszerint összehangolt információs támadások előzik meg, ahogy az a 2008-as orosz-grúz háborúban is történt.[15]

A kibertér megjelenése a közelmúlt konfliktusaiban

A kibertér, konfliktusokban játszott szerepének felértékelődését Jason Healey – a Fehér Ház korábbi kiberbiztonsági tanácsadója, és az Atlanti Tanács kiberpolitikai kezdeményezésének jelenlegi igazgatója – 2013-ban megjelent könyvében három szakaszra bontja.[16] Healey szerint a kiberkonfliktusok első periódusa az 1980-as évek közepén kezdődött. Ebben a korszakban történt az 1986-os "Cuckoo's Egg" néven ismertté vált eset, mely során a KGB két német hackert bérelt fel, hogy törjenek be és szerezzenek bizalmas információkat az Egyesült Államokban található Lawrence Berkeley Nemzeti Laboratóriumból. Fontos megemlíteni, hogy ekkor jelent meg az első számítógépes féreg, a Morris Worm, mely az 1988-ban történt incidens során képes volt napokig lebénítani a világhálót.[17] Ez az időszak Healey szerint fontos tanulságokkal szolgált, ráirányítva a szakemberek figyelmét a kiberkonfliktusok által jelentett fenyegetésekre. Ennek következtében az 1990-es években kidolgozásra kerültek a kiberhadviselésre vonatkozó doktrínák és megalakultak az első kiberparancsnokságok.[18] Az ezen időszakban zajló orosz-csecsen konfliktus során mindkét fél kiterjedt „háborút" vívott a kibertérben, a szárazföldön zajló katonai műveletekkel párhuzamosan. A csecsen szeparatisták az elsők közt voltak, akik a webet eszközként használták politikai céljaik elérése érdekében. Politikai üzeneteik és más

[14]Ibid., p. 186-187.
[15]Haig Zsolt: Az információbiztonság komplex értelmezése. Robotadviselés tudományos konferencia kiadványa. Hadmérnök különszám 2006. nov. 22. in: http://www.zmne.hu/hadmernok/kulonszamok/robothadviseles6/haig_rw6.html, Letöltve: 2014.06. 27.
[16]Jason Healey: A Fierce Domain: Conflict in Cyberspace, 1986 to 2012. CCSA/Atlantic Council, 2013.
[17]William Marmon: A Fierce Domain: Conflict in Cyberspace, 1986 to 2012," by Jason Healey (Review). European Affairs, 2013 july. in: http://www.europeaninstitute.org/index.php/180-european-affairs/ea-july-2013/1769-a-fierce-domain-conflict-in-cyberspace-1986-to-2012-by-jason-healey Letöltve: 2014. 06. 08.
[18]Chris Carroll : Should cyber warfare be elevated to highest command structure?, Stars and Stripes, 2013. 04. 29. in:http://www.stripes.com/news/should-cyber-warfare-be-elevated-to-highest-command-structure-1.218776, Letöltve: 2014.07. 27.

információk – többek között a háborús kiadások fedezésére létrehozott sacramentói bankszámla száma – közzététele a világhálón segítette a csecsen diaszpóra egységbe kovácsolását.[19] A csecsenek oroszok ellen folytatott további tevékenységei is igen hatékonyak voltak, értve ez alatt a harcok áldozatairól készült képek közzétételét, amely az orosz hadsereg túlkapásaira hívta fel a közvélemény figyelmét. A technika fejlődésével lehetővé vált a harcokról készült videók megosztása, amiket többek között az orosz katonai konvojokon történt rajtaütésekről készítettek. Mindez a kibertér szerepének átértékelésére késztette az orosz kormányt, amit az Oroszországi Föderáció elnöke, Vlagyimir Putyin 1999-ben megfogalmazott kijelentése is bizonyít: „*A közelmúltban feladtuk ezt a területet… de most újra beszállunk a játékba*.”[20] Az elnök szavait tettek követték, így a második csecsen háború idején orosz hackerek csecsen honlapokat törtek fel, ezen akciók időzítése és kifinomultsága arra utalt, hogy a támadók állami háttérrel rendelkeztek.

Az Észak-atlanti Szerződés Szervezetét (NATO) 1999-ben érte történetének első jelentősebb kibertámadása. A koszovói válság idején szerb, majd később kínai és orosz hackerek támadásokat indítottak a NATO és a szervezet tagállamainak hálózatai ellen.[21] A bombázások ellen tiltakozó hackerek deface[22] és elosztott túlterheléses (Distributed Denial of Service- DDoS) támadásokat hajtottak végre, melynek következtében ideiglenesen elérhetetlenné vált a NATO honlapja valamint több más szolgáltatás is leállt, ennek ellenére mindez nem gyakorolt jelentős hatást a katonai műveletek menetére.[23] Az incidens meghatározó szerepet játszott abban, hogy a 2002-es prágai csúcson elfogadták a NATO kibervédelmi programját.[24] Healey szerint 2003-at követően megtörtént a kibertér militarizálása, ennek révén a kibertér mindinkább az államok közötti konfliktusok

[19]Kenneth Geers: Cyberspace and the Changing Nature of Warfare. Hakin9 E-Book 19(3). P. 5. in: http://www.carlisle.army.mil/DIME/documents/Cyberspace%20and%20the%20Changing%20Nature%20of%20Warfare.pdf, Letöltve: 2014.07. 28.
[20]Kenneth Geers: Cyberspace and the Changing Nature of Warfare. Hakin9 E-Book 19(3). P. 5. in: http://www.carlisle.army.mil/DIME/documents/Cyberspace%20and%20the%20Changing%20Nature%20of%20Warfare.pdf, Letöltve: 2014.07. 28.
[21] Uo p. 8.
[22]A deface típusú támadás által a támadó le tudja cserélni a weboldal nyitó oldalát és így megjelenítheti saját üzenetét.
[23]Jason Healey: Cyber Attacks Against NATO, Then and Now. Atlantic Council, 2011. 09. 6. in: http://www.atlanticcouncil.org/blogs/new-atlanticist/cyber-attacks-against-nato-then-and-now, Letöltve: 2014.06. 17.
[24]Jason Healey: NATO's Cyber Capabilities: Yesterday,Today, and Tomorrow. Atlantic Council, 2012. 02. p. 2. in:http://www.atlanticcouncil.org/images/files/publication_pdfs/403/022712_ACUS_NATOSmarter_IBM.pdf, Letöltve: 2014.07. 17.

hadszínterévé változott.[25] Mindez tetten érhető a Közel-Kelet ezredfordulót követő konfliktusaiban, vagy az utóbbi időben egyre inkább eszkalálódó kínai-amerikai kiberháborúban.[26]

Az Észtország ellen, 2007 tavaszán folytatott kiterjedt támadássorozat új megvilágításba helyezte a kibervédelem kérdéskörét. A támadás hátterében egy második világháborús szovjet emlékmű eltávolítása állt. A parlament, kormányhivatalok, minisztériumok, bankok, telefontársaságok és médiacégek szerverei ellen végrehajtott tömeges támadások eredményeként az internet szolgáltatás akadozott, egyes esetekben hosszabb-rövidebb időre leállt. A támadás érzékenyen érintette az észteket, mivel az ország internet-penetrációja az egyik legmagasabbnak számít a világon.[27] A célpontok kiválasztása, a támadások összehangoltsága, precíz kivitelezése és hatékonysága arra mutatott, hogy e támadások hátterében szervezett erők állnak. Az orosz kormány érintettsége nyilvánvaló, még akkor is, ha ennek bizonyítására nem állnak rendelkezésre konkrét bizonyítékok.[28] Annak ellenére, hogy az oroszok végül nem tudták térdre kényszeríteni Észtországot, a támadás felkészületlenül érte mind az észteket mind pedig a NATO-t. Az eset jelentős hatást gyakorolt a NATO kibervédelmi politikájára.

A 2008-as orosz-grúz háború során az oroszok kibertérben folytatott tevékenysége még kiterjedtebbé vált. Szakértők szerint az orosz hírszerző szolgálatoknak sikerült megbénítania a grúz információs infrastruktúrát és a kormány weboldalait.[29]A rendelkezésre álló bizonyítékok szerint az orosz kormányerők ekkor már a katonai műveletekkel összhangban szervezett keretek között koordinálták az akciókat. Ezt bizonyítja az is, hogy a tűzszünet megkötése után a grúz weblapok – kormányoldalak, hírportálok és a bankok – ellen végrehajtott DDoS támadások szinte azonnal leálltak. Fontos megjegyezni, hogy a

[25]Cryptome.org: A Fierce Domain: Conflict in Cyberspace 1986 to 2012 by Jason Healey (Review). Cryptome.org, 2013. november 11. in: http://cryptome.org/2013/11/fierce-domain.htm, Letöltve: 2014. 06. 05.
[26]Az Egyesült Államok és Kína között zajló kiberháború az utóbbi időben egyre fokozódik. A két ország kapcsolatairól részletesebben itt: Kenneth Lieberthal, Peter W. Singer: Cybersecurity and U.S.-China Relations. The Brookings Institution, 2012. 02. 23. in: http://www.brookings.edu/~/media/research/files/papers/2012/2/23%20cybersecurity%20china%20us%20singer%20lieberthal/0223_cybersecurity_china_us_lieberthal_singer_pdf_english.pdf, Letöltve: 2014.07. 23.
[27]Az 1,34 millió észt 75%-a internethasználó, ezenkívül Észtország az e-kormányzás éllovasának számít.
[28]Kertu Ruus: Cyber War I: Estonia Attacked from Russia. European Affairs, Volume number 9, Issue number 1-2/2008.In:http://www.europeaninstitute.org/index.php/component/content/article?id=67:cyber-war-i-estonia-attacked-from-russia, Letöltve: 2014. 06. 08.
[29]Ward Carroll: Cyber War 2.0 — Russia v. Georgia. Defense Tech, 2008. 08. 13. in: defensetech.org/2008/08/13/cyber-war-2-0-russia-v-georgia/, Letöltve: 2014.07. 12.

támadásokért feltételezhetően civilek a felelősek, akiknek tevékenységét különböző kormányzati és katonai szervezetek koordinálták.[30]

Ezen esetekből jól látszik, hogy az adott államok stratégiai céljaik elérése érdekében egyre nagyobb szerepet szánnak a kibertérben folytatott műveleteknek. Az akciók esetenként már a szárazföldi műveletek előkészítő szakaszában megindulnak, majd ezt követően a konfliktus egész időtartama alatt tovább folytatódnak az információs műveletek részeként, mint ahogy az a 2008-as orosz-grúz háború során is történt. Megállapítható, hogy az orosz kormány eleinte csak közvetve támogatta a különböző hacker csoportokat, de az utóbbi időben, a katonai műveletek részeként, az információs tevékenységek keretei között szervezetten hajtják végre a célzott támadásokat, bénítva ezzel az ellenséges állam információs rendszereit és hírközlési hálózatait.

Kiberműveletek az ukrán válság alatt

A 2014 elején, Viktor Janukovics bukását követően kirobbant krími válság a kiberhadviselés tekintetében is új mérföldkőnek tekinthető. A két ország közötti konfliktus azt követően kezdett fokozódni a kibertérben, hogy az orosz parlament felsőháza március 1-jén felhatalmazta az elnököt a katonai erő Ukrajna területén történő alkalmazására. A válság kirobbanását megelőzően még szoros kapcsolatban álló orosz és ukrán hacker közösségek gyors ütemben aktivizálták magukat. Az #OpUkraine és az #OpRussia elnevezésű kampányok során végrehajtott több száz támadás, a különböző minisztériumokhoz és államszervekhez köthető weboldalak, valamint sok e-mail és banki szolgáltatás ideiglenes lebénulásához vezetett. A támadások mértékét jól jelzik a FireEye Inc., kiberbiztonsági vállalat által közzétett vizsgálat eredményei.[31] A FireEye Inc. napi szinten, több millió callback-et észlel és elemez, melyekből kimutathatóak a kibertérben folytatott ellenséges tevékenységek.[32] Az általuk készített elemzésben 2013 januárját követően vizsgálták a callback aktivitást, a szakértők kimutatták, hogy a válság eszkalálódásával jelentősen megemelkedett az

[30]Mark Rutherford: Report: Russian mob aided cyberattacks on Georgia. CNET, 2009. 08. 18., in: http://www.cnet.com/news/report-russian-mob-aided-cyberattacks-on-georgia/, Letöltve: 2014.07. 22.
[31]Kenneth Geers: Strategic Analysis: As Russia-Ukraine Conflict Continues, Malware Activity Rises. FireEye, 2014. 05. 28., in:http://www.fireeye.com/blog/technical/2014/05/strategic-analysis-as-russia-ukraine-conflict-continues-malware-activity-rises.html, Letöltve: 2014.07. 25.
[32]A legmegbízhatóbb módja a számítógépes-hálózati műveletek felderítésérnek, ha figyeljük a fertőzött számítógépen található malware „callback"-jét, amit titkosított kapcsolaton keresztül küld a támadó C&C szervere felé.

Ukrajnában és Oroszországban észlelt callback-ek száma.[33] A támadók kilétének megállapítása sok esetben nehézségekbe ütközött, mivel a különböző hacker csoportok támadásai gyakran ugyanarról az IP-címről indultak ki. Szakértők szerint a krími válság elmélyülését követően az orosz katonai hírszerző szolgálat (GRU) által, az információs műveletek részeként indított támadások következtében lebénult a Krím félsziget telekommunikációs hálózata. Az ukrán biztonsági szolgálat vezetője Valentin Nalivajcsenko egy március 4-én tartott sajtótájékoztatón közölte: „*az ukrán telekommunikációs infrastruktúrát nagyarányú támadás érte, ami a Krím félszigetről indult ki.*"[34] Nalivajcsenko szerint mindez annak érdekében történt, hogy megzavarják az ukrán parlament tagjai közötti összeköttetést.[35] A támadás alatt álló Ukrtelecom nevű ukrán telekommunikációs vállalat bejelentette, hogy jelzés nélküli fegyveresek hatoltak be a Krím félszigeten található létesítményükbe, akik a szolgáltató hálózatába telepített berendezéseik segítségével sikeresen blokkolták az ukrán politikusok telefonjait. Ezen túlmenően ismeretlen fegyveresek a Krím félsziget több pontján behatoltak a szolgáltató telephelyeire és megrongálták az ott található eszközöket. Szakértők szerint a szevasztopoli kikötőben állomásozó orosz hajókon olyan zavaró berendezések lehettek, amelyek segítségével az oroszok blokkolni tudták a rádiókommunikációt, továbbá szabotálták a város környezetében található ukrán haditengerészeti kommunikációs állomásokat és villamosvezetékeket.[36]A fizikai és kibertérben végrehajtott támadások hatására a Krím félsziget telekommunikációja megbénult. Ezen akciók kiegészülve a katonai műveletekkel azt a stratégiai célt szolgálták, hogy elvágják a félszigetet Ukrajna többi részétől. Az a tény, hogy a ezen a területen csak egy internetes forgalomcsere pont (*Internet Exchange Point-IXP*) épült, nagyban megkönnyítette az orosz kiberegységek dolgát. Megállapítható tehát, hogy a támadók elsődleges célpontja az ország kritikus infrastruktúrájának egyik eleme volt, melyet az információs műveletek részeként változatos módszerekkel, egyszerre támadtak az információs és a fizikai dimenzióban.

---

[33]Lásd 1. ábra

[34]Pavel Polityuk, Jim Finkle: Ukraine says communications hit, MPs phones blocked, Reuters, 2014. 05. 04., in:http://www.reuters.com/article/2014/03/04/us-ukraine-crisis-cybersecurity-idUSBREA231R220140304, Letöltve: 2014.07. 26.

[35]Pierluigi Paganini: Crimea – The Russian Cyber Strategy to Hit Ukraine, Infosec Institute, 2014. 03. 11., in:http://resources.infosecinstitute.com/crimea-russian-cyber-strategy-hit-ukraine/, Letöltve: 2014.07. 25.

[36]Pierluigi Paganini: Crimea – Is Russia adopting the same cyber strategy used in Georgia?. Security Affairs, 2014. 03. 05. in: http://securityaffairs.co/wordpress/22781/cyber-warfare-2/crimea-russia-cyber-strategy.html, Letöltve: 2014. 06. 05.

Egyes nyugati szakértők szerint az oroszok által végrehajtott akciók meglehetősen visszafogottnak tekinthetőek, mivel szerintük ennél sokkal átfogóbb támadásokra is képesek lettek volna. A CIA Különleges Műveleti Osztályának korábbi magas rangú tisztjének, Marty Martinnak a véleménye szerint nagyobb mértékű támadásokra a konfliktus további eszkalációja esetén került volna sor. „*Néha hasznos pár kommunikációs csatornát meghagyni annak érdekében, hogy képesek legyünk a rajtuk keresztülfutó információkat ellenőrizni és nyomon követni, mintsem azokat teljesen elvágva megfosszuk magunkat a hírszerzői forrásoktól.*”[37]

Az oroszok által alkalmazott módszerek és azok háttere

Jason Healey véleménye szerint, a krími válság alatt az oroszok információs műveleteik végrehajtása során más módszereket alkalmaztak, mint a 2007-es észt vagy a 2008-as orosz-grúz konfliktus idején.[38] Moszkva ezúttal több fizikai támadást hajtott végre, ami visszatérést jelent a régimódi hidegháborús taktikákhoz. Az ellenséges területen, infokommunikációs rendszerekre gyakorolt fizikai ráhatás egy régi, nem túl kifinomult módszer, amit a múltban gyakran alkalmaztak az orosz titkosszolgálatok. Ezt egészítették ki a kibertérben kifejtett támadó jellegű tevékenységek, melyek így meghozták a kívánt eredményt. Ezek során alkalmazásra kerülhetnek olyan, az oroszok által kémkedésre kifejlesztett kifinomult és összetett kártevők, mint az Uroburos, ami a görög mitológia saját farkába harapó kígyójáról kapta a nevét. A kártevőt még februárban fedezte fel a német G Data Security, ami a cég szakértői szerint képes az önálló működésre, és a megfertőzött hálózaton keresztül terjeszti magát. Az Uroburos felépítését tekintve egy úgynevezett rootkit, amely két fájlból tevődik össze, egy driverből és egy titkosított virtuális fájlrendszerből. A rootkit képes átvenni a megfertőzött számítógép feletti irányítást, tetszőleges parancsokat végrehajtani és a rendszerfolyamatokat elrejteni. Moduláris felépítése révén könnyedén továbbfejleszthető új funkciókkal, amely különösen hatékonnyá teszi. A driver fájl rendkívül komplex és tervezésének köszönhetően képes észrevétlenül működni, ami jelentős mértékben megnehezíti a rootkit azonosítását. A G Data szakértői szerint a kártevő komplex felépítése és egyéb

[37]Defense Update: The Ukrainian crisis – a cyber warfare battlefield. Defense Update, 2014. 04. 05. in: http://defense-update.com/20140405_ukrainian-crisis-cyber-warfare-battlefield.html#.U3SZDKL8eW8, Letöltve: 2014.07. 21.
[38] Uo.

tulajdonságai azt sugallják, hogy kifejlesztése mögött az orosz kormány állhat.[39] Az olyan kártevők alkalmazása, mint a kígyó ötvözve a klasszikus fizikai támadásokkal igen hatékony technikának számít. Ezek integrált alkalmazásának köszönhetően az oroszok képesek voltak lebénítani a Krím félsziget telekommunikációját, ezzel segítve a katonai műveleteket.

Szakértők szerint az Ukrajna ellen végrehajtott kibertámadások tekintetében az egyik legfontosabb változás abban mutatható ki, hogy az orosz hacker csoportok nem támogatták olyan mértékben a kormányt, mint ahogy azt az Észtország és Grúzia ellen végrehajtott akciók során tették. Ez részben arra vezethető vissza, hogy Oroszország az utóbbi időben jelentős erőfeszítéseket tett kiberképességeinek fejlesztése terén. Ennek szellemében született meg az a 2013-as döntés, amely rendelkezett az orosz kiberparancsnokság felállításáról, továbbá az átfogó kiberstratégiai koncepció kidolgozásáról. E folyamatban fontos lépcsőfok volt a 2010-ben közzétett orosz katonai doktrína,[40] melyben az információs műveletek jelentős mértékben felértékelődtek. Ezt egészíti ki az orosz védelmi minisztérium által 2012-ben közzétett stratégiai koncepció, ami az Oroszországi Föderáció fegyveres erőinek kibertérben folytatott tevékenységeiről szól.[41]

Összességében elmondható, hogy Oroszország Kínához és az Egyesült Államokhoz hasonlóan egyre nagyobb hangsúlyt fektet kiberképességeinek fejlesztésére, melyeket a különböző konfliktusok során aktívan alkalmaz céljai elérése érdekében. Oroszország minderre egyre nagyobb forrást biztosít, melynek köszönhetően mára az orosz fegyveres erők és biztonsági szolgálatok kiberképességei jelentősen meghaladják a 2008-as szintet. Ennek is köszönhető, hogy a jelenlegi ukrán válság során már a különböző állami szervek szervezett keretek között végrehajtott információs műveleteit láthatjuk, míg az észtországi és grúziai támadásokat főként államilag támogatott aktivisták és egyéb civil csoportok hajtották végre.

[39]G Data Security Labs: Uroburos Highly complex espionage software with Russian roots. G DataRed Paper 2014.in:https://public.gdatasoftware.com/Web/Content/INT/Blog/2014/02_2014/documents/GData_Uroburos_RedPaper_EN_v1.pdf, Letöltve: 2014.07. 24.
[40]Carnegie Endowment For International Peace: Russian military doctrine, 2010. 02., in: http://carnegieendowment.org/files/2010russia_military_doctrine.pdf, Letöltve: 2014.07. 27.
[41]NATO CCD COE: Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space (unofficial translation). in: http://www.ccdcoe.org/strategies/Russian_Federation_unofficial_translation.pdf, Letöltve: 2014.06. 20.

Megállapítható, hogy ezen csoportok jelentősége az orosz kiberképességek fejlődésével kezd egyre inkább háttérbe szorulni.[42]

Az oroszok által indított információs műveletek jellege

Az ukrán válság során az információs műveletek mindhárom spektrumában zajló tevékenységek – a dezinformáció és propaganda terjesztésének, a telekommunikációs rendszerek módosításának és pusztításának, valamint a kibertámadások végrehajtásának – összehangolt alkalmazására került sor. Az információs műveletek ilyen szinten történő alkalmazása váratlanul érintette a nyugati országokat, melyek elsősorban annak technikai oldalára fókuszáltak az elmúlt években.[43] Hasonlóan az 1999-es koszovói eseményekhez, a mostani válság során is számos alkalommal érte támadás a NATO szervereit.[44] Oroszország továbbá a Krím félsziget katonai megszállását megelőzően – kevés kivételtől eltekintve – képes volt az összes ukrán kormányzati weboldalt átmenetileg megbénítani, valamint az ország teljes telekommunikációs hálózatát megfigyelése és irányítása alá vonni. Ezeket az akciókat részben az orosz különleges erők hajtották végre, akik fizikai ráhatás útján eltérítették a jelentős kommunikációs rendszereket. A krími válság óta elmúlt időben a kibertérben folytatott ellenséges tevékenységek jelentősen visszaestek.[45] A legnagyobb akcióra a május 25-i elnökválasztáskor került sor, amikor orosz hackerek támadásaikkal megpróbálták szabotálni a választás menetét. A helyzet rendeződéséhez hozzájárult az is, hogy Oroszország végül nem indított átfogó támadást Ukrajna kritikus információs infrastruktúrája ellen. Egy ilyen támadás beláthatatlan következménnyel járna, egyes szakértők szerint a célország társadalmi rendjére döntő mértékű csapást mérne, így az adott konfliktus a támadást követően akár konvencionális háborúvá is alakulhatna. Korunk kiberháborúi ugyanis olyan tartományban zajlanak, amelyet még nem szabályoz a háborús jog, ami arra ösztönözheti a célba vett országot, hogy hatékony nemzetközi jogi és kibervédelmi eszközök hiányában, fizikai úton intézzen megtorlást a támadó ellen. A komoly kiberfegyverek pontos hatását természetükből adódóan nehéz megjósolni, mivel könnyen

[42]Jeffrey Carr: Russian Cyber Warfare Capabilities in 2014 (We aren't in Georgia anymore). Digital Dao, 2014. 03. 08. in:http://jeffreycarr.blogspot.hu/2014/03/russian-cyber-warfare-capabilities-in.html,Letöltve:2014.07. 27.
[43]Jason Healey: Russia vs. Ukraine: The Cyber Front Unfolds. Atlantic Council, 2014. 04. 02. in: www.atlanticcouncil.org/blogs/new-atlanticist/russia-vs-ukraine-the-cyber-front-unfolds, Letöltve: 2014. 06. 04.
[44]Adrian Croft, Peter Apps: NATO websites hit in cyber attack linked to Crimea tension, Reuters, 2014. 03. 16. in:http://www.reuters.com/article/2014/03/16/us-ukraine-nato-idUSBREA2E0T320140316,Letöltve:2014.06. 12.
[45]Jeremy Hsu: Why There's No Real Cyberwar in the Ukraine Conflict. IEEE Spectrum, 2014. 03. 14. in: http://spectrum.ieee.org/tech-talk/computing/networks/why-theres-no-real-cyberwar-in-the-ukraine-conflict, Letöltve: 2014. 06. 08.

kicsúszhatnak az irányítás alól, ez részben magyarázattal szolgálhat arra is, hogy végül miért nem lettek nagy számban bevetve a konfliktus során. Feltételezhetően Oroszország nem akart az első olyan ország lenni, amely egy másik állam kritikus infrastruktúrája ellen átfogó támadást indít, mivel tart attól, hogy ennek következményeként ő is hasonlóan járhat. [46]

Végül az is az átfogó kibertámadás megindítása ellen szólt, hogy Oroszország törekszik rá, hogy kiberképességeinek valódi ereje továbbra is rejtve maradjon. A nyugati hírszerző szolgálatok úgy vélik, hogy az oroszok alvó malwareket telepítettek ellenségeik számítógépes hálózataiba, melyek csak arra várnak, hogy egyszer valaki távolról aktiválja őket. Egyes szakértők mindezek hatására az Egyesült Államokra leselkedő egyik legnagyobb fenyegetést az orosz kiberképességekben vélik felfedezni.[47]

Összegzés

Megállapítható, hogy az ukrán válság során az információs műveletek részeként az orosz erők folyamatosan támadták a Krím félsziget információs infrastruktúráját annak érdekében, hogy elvágják a félszigetet az ország többi részétől. A konfliktus során mindkét fél hacker csoportjai aktivizálták magukat, és ennek köszönhetően mindkét országban észrevehetően megugrott a különböző weboldalak ellen elkövetett deface és DDoS típusú támadások száma. A támadások során az oroszok a szárazföldi műveletekkel párhuzamosan, az információs műveletek minden dimenziójában összehangoltan végezték tevékenységeiket. A műveletek végül nem alakultak át egy, az ukrán kritikus információs infrastruktúrák ellen végrehajtott átfogó támadássá, azaz a konfliktus a kibertérben nem eszkalálódott kiterjedt kiberháborúvá. Az ukrán válság alatti kibertérben folytatott műveletek jellege sok hasonlóságot mutat a 2007-es észtországi és a 2008-as grúziai válságban tapasztaltakkal, azonban markáns különbségek is megmutatkoztak.

Ez nagyrészt az orosz kiberképességek fejlesztése terén tett erőfeszítéseknek köszönhető. Az információs műveletek végrehajtása során megnőtt az állami szervek jelentősége, ami illeszkedik a nemzetközi trendekhez. A támadások során a két fél képességei között megmutatkozó különbségek jól szemléltették, hogy az oroszok jelentős erőt képviselnek a kibertérben. Ezért a konfliktus során többen arra szólították fel a nyugati

[46]Dr. Jarno Limnéll: Why hasn't Russia unleashed a cyber attack on Ukraine?. CBS News, 2014. 07. 02. in:http://www.cbsnews.com/news/why-hasnt-russia-unleashed-a-cyber-attack-on-ukraine/,Letöltve:2014. 07. 08.
[47]Piret Pernik: Is All Quiet on the Cyber Front in the Ukrainian crisis?. RKK ICDS, 2014. 03. 07. in: http://www.icds.ee/et/blogi/artikkel/is-all-quiet-on-the-cyber-front-in-the-ukrainian-crisis/,Letöltve: 2014.06. 08.

országokat, hogy nyújtsanak segítséget Ukrajna számára az orosz kibertámadások elhárításában. A segítség részeként a nyugati országok megosztanák az orosz hackerek tevékenységéről gyűjtött információikat az ukrán kormánnyal, valamint megakadályoznák a kritikus infrastruktúrák ellen indított nagyszabású támadásokat. Végül a szakértők javaslata szerint a támadások súlyosabbá válása esetén kiberszakértők és anyagi támogatás küldésével segíthetnék a védekezést.[48] Véleményem szerint a nyugati országoknak le kell vonnia a történtekből a megfelelő tanulságokat, és fel kell készülniük arra az eshetőségre, hogy a jövőben sor kerülhet egy kiterjedt kiberháborúra. Az események valószínűleg a 2007-es észt és a 2008-as grúz válsághoz hasonlóan jelentős változásokhoz fognak vezetni, arra ösztönözve a NATO-t és a többi nyugati országot, hogy még több erőforrást szánjanak kibervédelmi képességeik fejlesztésére.

Ennek már mutatkoznak jelei, a NATO védelmi minisztereinek június 3-i találkozója során jóváhagyták a NATO továbbfejlesztett kibervédelmi politikáját, ami a kollektív védelemről szóló 5. cikkely hatálya alá tartozó cselekmények közé sorolta a kibertámadást, mivel azok fenyegetést jelentetnek az egész euro-atlanti térség stabilitására.[49] Ezt követően a 2014. szeptember 4-5-én tartott walesi NATO-csúcson a tagállamok képviselői hitet tettek a szövetség kibervédelmi képességeinek további fejlesztése mellett, így a kibervédelem bekerült a NATO védelmi tervezési folyamatába.[50]Látható tehát, hogy a nyugati országok felismerve a kibertérből érkező támadások jelentette fenyegetést a legfontosabb prioritások közé emelték a kibervédelmet, és együttes erővel készülnek azok leküzdésére. A szakértők szerint nem zárható ki, hogy a közeljövőben az ilyen támadások egy átfogó kiberháborúvá szélesedhetnek, amely beláthatatlan pusztítással járna a célország gazdasági és társadalmi életére annak köszönhetően, hogy egyre jobban ki vagyunk szolgáltatva a modern infokommunikációs rendszereknek.

[48]Jason Healey: How to Beat a Russian Cyber Assault on Ukraine. Atlantic Council, 2014. 03. 03. in:http://www.atlanticcouncil.org/blogs/new-atlanticist/how-to-beat-a-russian-cyber-assault-on-ukraine, Letöltve: 2014.07. 20.

[49]NATO.int: NATO steps up collective defence, support for reforms in Ukraine. 2014. 06. 03. in: http://www.nato.int/cps/en/natolive/news_110609.htm?selectedLocale=en, Letöltve: 2014.07. 26.

[50]További részletek itt: Wales Summit Declaration 64., 72., 73., 104. paragrafusai Lásd: NATO.int: Wales Summit Declaration. In: http://www.nato.int/cps/en/natohq/official_texts_112964.htm Letöltve: 2015. 02. 25.

MELLÉKLET

Az ukrán konfliktus legfontosabb kibereseményei

- 2013. december 16: A „KiberBerkut” néven elhíresült ukrán hackercsoport támadást intézett több NATO weboldal ellen. Az akciót az Ukrajna területén állomásozó „NATO megszálló erők” jelenléte miatt indították.[51]

- 2014. február 28: Az Anonymus Ukrajnában működő csoportja „kiberháborút” hirdetett az Ukrajna függetlenségét és szabadságát veszélyeztető államok ellen. Ezt követően támadás érte az ukrán parlament, a jobb szektor és más kormányzati szervek honlapjait. A hackerek között egyaránt megtalálhatóak voltak az ellenzéket és kormánypártot támogató csoportok. [52]

- 2014. március 6: A Russian Cyber Command kiszivárogtatta azt a Rosoboronexport orosz fegyverexportőr vállalattól származó, több mint 1000 darab dokumentumot, amit a Moszkvában működő Indiai Nagykövetségen szereztek meg. Ezzel kívánták tiltakozni Putyin stratégiája ellen, melynek célja szerintük a harmadik világháborúba kirobbantása. Az ukrán csoportok között kiemelkedően aktívnak számított a Cyber-Berkut, amely a a krími válság idején több mint 40 orosz hírportál tört fel.[53]

- 2014. március 7: Ukrán hackercsoportok támadást hajtottak végre több orosz hír- és média oldal ellen. A „Kibersotnya” néven elhíresült csoport ideiglenes elérhetetlenné tette a Russian newspaper nevű oldalt, ezzel párhuzamosan a Lenta.ru hírügynökség weboldala ellen is hasonló akciót hajtottak végre.[54]

- 2014. március 9: Az indiai kormány megerősítette, hogy ismeretlen hackerek megpróbálták megszerezni a harci repülőgépek beszerzése kapcsán tartott, indiai-orosz

[51]Defense Update: The Ukrainian crisis – a cyber warfare battlefield. Defense Update, 2014. 04. 05. in: http://defense-update.com/20140405_ukrainian-crisis-cyber-warfare-battlefield.html#.U3SZDKL8eW8, Letöltve: 2014.07. 21.
[52]Waqas: Anonymous Declares Cyberwar on Countries Found Disturbing Peace in Ukraine. 2014. 03. 28. in:http://hackread.com/anonymous-ukraine-declares-cyberwar/, Letöltve: 2014.06. 27.
[53]Defenseworld.net: Indian Embassy's Systems in Moscow Hacked to Target Rosoboronexport. Defense World, 2014.03.04.in:http://www.defenseworld.net/news/10179/Indian_Embassy_s_Systems_in_Moscow_Hacked_to_Target_Rosoboronexport, Letöltve: 2014.07. 24.
[54]Lenta.ru: Massive Attack перепели Янку Дягилеву и «Гражданскую оборону». Lenta.ru, 2014. 07. 07. In:http://lenta.ru/news/2013/07/07/yanka/, Letöltve: 2015. 02. 15.

tárgyalásokról készült katonai dokumentumokat. A feltételezés szerint ki akarták deríteni az orosz légierő lehetőségeit, ennek céljából más országok légierőinek kevésbé biztonságos rendszereibe hatoltak be, hogy megszerezzék a vonatkozó információkat.[55]

- 2014. Március 14: Az orosz Rostec fegyvergyártó vállalat bejelentette, hogy sikerült leszállásra kényszeríteni a Krím félsziget felett 4000 méter magasságban repülő, MQ-5B típusú pilótanélküli felderítő repülőgépet, amely állításuk szerint a 66. amerikai katonai felderítő dandárhoz tartozott.[56] A vállalat közleménye szerint sikerült megszakítani az operátor és a repülőgép közötti adatkapcsolatot az Avtobaza típusú rádiótechnikai felderítő komplexum segítségével. A hírt később a Pentagon[57] és a Rostec[58] is hivatalosan cáfolta. Az eset – még ha nem is történt meg – jelzi a kiberhadviselés egyre inkább növekvő jelentőségét napjaink fegyveres konfliktusaiban, valamint rávilágít a pilóta nélküli repülőgépek és más hálózatba kötött eszközök sebezhetőségére.[59]

- 2014. március 14: Ukrán hackerek több DDoS támadást hajtottak végre az orosz kormányzati és kereskedelmi honlapok ellen. A támadás érintette Putyin elnöki, Oroszország kormányának hivatalos valamint az orosz központi bank, a külügyminisztérium és a Gazprom weboldalát.[60]

- 2014. március 16: A krími népszavazással párhuzamosan nagyszabású DDoS támadássorozat indult az ukrán kormányhoz köthető weblapok ellen. Erre válaszul

---

[55]US Army Space and Missile Defense Command Army Forces Strategic Command G39, Information Operations Division: Information Operations Newsletter. Vol 14. no. 03/2014, p. 30. in: http://www.phibetaiota.net/wp-content/uploads/2014/05/ARSTRAT_IO_Newsletter_v14_no_03.pdf, Letöltve: 2014. 06. 20.

[56]Voiceofrussia.com: US drone intercepted in Crimean airspace - Russia's state corporation. Voiceofrussia, 2014. 03. 14. in:http://voiceofrussia.com/news/2014_03_14/US-drone-intercepted-in-Crimean-airspace-Russias-state-corporation-2994/, Letöltve: 2014.07. 27.

[57]Mike Hoffman: Pentagon Denies Downed U.S. Drone Report in Crimea, Defense Tech. 2014. 03. 14., in:http://defensetech.org/2014/03/14/pentagon-denies-downed-u-s-drone-report-in-crimea/ Letöltve: 2014.06. 18

[58]Rostec: Rostec official denial, in:http://rostec.ru/en/news/4416, Letöltve: 2014.07. 27.

[59]2011. december 4-én Iránnak sikerült elfognia, egy RQ-170 Sentinel típusú amerikai pilótanélküli repülőgépet. Részletek itt: Ványa László: Kérdések és válaszok a szupertitkos RQ170 iráni kézre kerüléséről. Repüléstudományi Közlemények 2: p. 634-641, 2012., in: http://www.szrfk.hu/rtk/kulonszamok/2012_cikkek/52_Vanya_Laszlo.pdf. Letöltve: 2014.07. 17.

[60]US Army Space and Missile Defense Command Army Forces Strategic Command G39, Information Operations Division: Information Operations Newsletter. Vol 14. no. 03/2014, p. 30. in: http://www.phibetaiota.net/wp-content/uploads/2014/05/ARSTRAT_IO_Newsletter_v14_no_03.pdf, Letöltve: 2014. 06. 20.

másnap ukrán hackerek megindították az addigi legnagyobb, 132 különálló támadásból álló akciójukat különböző oroszországi weboldalak ellen. A támadások jóval erőteljesebbek voltak, mint amiket az oroszok hajtottak végre a grúz háború során. Erősségüket jól jelzi, hogy a legnagyobb ukrán támadás sávszélessége 124 GB/s-t tett ki, mellyel csaknem 18 percen keresztül bombázták a kijelölt hálózatot. Összevetésképp a grúz háború alatti legnagyobb orosz támadás sávszélessége 843 MB/s volt. [61]

- 2014. március 17: Két nagy oroszországi bank, a VTB és az Alpha ellen hajtottak végre kibertámadást, amelynek következtében leálltak az on-line banki szolgáltatások. A támadásért az anonymus hacker csoport egyik kaukázusi csapata vállalta felelősséget.[62]

	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sep	Oct	Nov	Dec	Jan	Feb	Mar	Apr
1	US	US	US	US	US	US	US	US	US	US	US	US	US	US	US	US
2	DE	KR	DE	DE	DE	KR	KR	KR	DE	DE	KR	KR	KR	KR	KR	KR
3	KR	DE	KR	KR	KR	DE	DE	DE	KR	KR	DE	CN	CN	DE	RU	DE
4	CN	CN	CN	CN	NL	NL	GB	CN	CN	CN	CN	NL	DE	CN	DE	RU
5	RU	RU	HK	HK	RU	GB	NL	GB	GB	NL	NL	DE	FR	FR	CN	GB
6	FR	FR	FR	RU	GB	CN	CN	NL	CA	GB	GB	GB	RU	NL	GB	CN
7	NL	GB	NL	NL	CN	RU	CA	CA	NL	RU	CA	FR	NL	RU	NL	NL
8	GB	TR	RU	GB	CA	CA	RU	RU	RU	CA	RU	RU	GB	GB	FR	UA
9	JP	NL	CA	FR	FR	FR	JP	FR	TR	JP	FR	CA	CA	UA	UA	FR
10	PL	CA	TH	CA	HK	HK	PL	JP	FR	UA	UA	UA	UA	CA	CA	CA
11	CA	ID	GB	IT	IN	TR	FR	PL	UA	TR	JP	RO	PT	PT	HK	PL
12	IN	JP	BG	JP	UA	JP	HK	HK	JP	RO	TR	PL	RO	PL	PT	PT
13	RO	HK	TR	PL	PL	IT	UA	UA	PT	CZ	PT	PT	TR	JP	RO	JP
14	IT	UA	UA	UA	JP	PL	PT	CZ	IT	IE	AU	TR	PL	RO	TR	TR
15	UA	PL	JP	BG	TR	AR	IT	BR	CZ	FR	GE	IN	JP	TR	PL	RO
16	ID	RO	IT	TR	PT	UA	TR	IT	PL	PT	HK	JP	BR	CZ	JP	HK
17	HK	IN	PL	IN	BG	RO	VN	TR	HK	PL	PL	ES	CZ	BR	CZ	CZ
18	TW	PA	ID	TH	IT	IN	RO	PT	ES	IT	RO	AU	IT	IT	ES	IT
19	TR	IT	LT	TW	TH	AU	IN	AU	BR	SE	ES	EU	ES	ES	BR	BR
20	HU	TH	IN	CH	RO	BG	SD	TW	IN	HK	IN	HK	HK	HK	IT	TH
	2013	2013	2013	2013	2013	2013	2013	2013	2013	2013	2013	2013	2014	2014	2014	2014

1. ábra

(*Forrás*: http://www.fireeye.com/blog/wp-content/uploads/2014/05/ru1.jpg, Letöltve: 2014. 06. 24.)

[61]Mark Clayton: Massive cyberattacks slam official sites in Russia, Ukraine. Csmonitor, 2014. 03. 18., in:http://www.csmonitor.com/World/Security-Watch/Cyber-Conflict-Monitor/2014/0318/Massive-cyberattacks-slam-official-sites-in-Russia-Ukraine, Letöltve: 2014.06. 17.

[62]US Army Space and Missile Defense Command Army Forces Strategic Command G39, Information Operations Division: Information Operations Newsletter. Vol 14. no. 03/2014, p. 30. in: http://www.phibetaiota.net/wp-content/uploads/2014/05/ARSTRAT_IO_Newsletter_v14_no_03.pdf, Letöltve: 2014. 06. 20.

Felhasznált Irodalom

Andrzej Kozłowski, Kacper Rękawek, Marcin Terlikowski: Cyberterrorism: The Threat That Never Was. PISM Strategic Files; No. 4. (40). in: http://www.pism.pl/files/?id_plik=16470, Letöltve: 2014.06.07.

Cserháti András: A Stuxnet vírus és az iráni atomprogram. Nukleon on-line folyóirat, Magyar Nukleáris Társaság, 2011. április 5. in: mnt.kfki.hu/Nukleon/index.php?action=abstract&cikk=155, Letöltve: 2014.07. 27.

Haig Zsolt, Várhegyi István: A cybertér és a cyberhadviselés értelmezése. HADTUDOMÁNY XVIII. Évf, p. 1-12. in: http://mhtt.eu/hadtudomany/2008/2008_elektronikus/2008_e_2.pdf, Letöltve: 2014.06.08.

Haig Zsolt, Várhegyi István: Hadviselés az információs hadszíntéren. Zrínyi Kiadó, Budapest, 2005.

Haig Zsolt: Az információbiztonság komplex értelmezése. Robotadviselés tudományos konferencia kiadványa. Hadmérnök különszám 2006. nov. 22. in: http://www.zmne.hu/hadmernok/kulonszamok/robothadviseles6/haig_rw6.html,Letöltve: 2014.06. 27.

Jason Healey: A Fierce Domain: Conflict in Cyberspace, 1986 to 2012. CCSA/Atlantic Council, 2013.

Kenneth Geers: Cyberspace and the Changing Nature of Warfare. Hakin9 E-Book 19(3). in: http://www.carlisle.army.mil/DIME/documents/Cyberspace%20and%20the%20Changing%20Nature%20of%20Warfare.pdf, Letöltve: 2014.07. 28.

Kenneth Lieberthal, Peter W. Singer: Cybersecurity and U.S.-China Relations. The Brookings Institution, 2012. 02. 23. in:http://www.brookings.edu/~/media/research/files/papers/2012/2/23%20cybersecurity%20china%20us%20singer%20lieberthal/0223_cybersecurity_china_us_lieberthal_singer_pdf_english.pdf, Letöltve: 2014.07. 23.

Szabó András: Az információs hadviselés és a hadtudomány. HADTUDOMÁNY VIII. Évf, 4. szám. in: http://www.zmne.hu/kulso/mhtt/hadtudomany/1998/ht-1998-4-5.html, Letöltve: 2014. 06. 18.

Ványa László: Kérdések és válaszok a szupertitkos RQ170 iráni kézre kerüléséről. Repüléstudományi Közlemények 2: p. 634-641, 2012. in: http://www.szrfk.hu/rtk/kulonszamok/2012_cikkek/52_Vanya_Laszlo.pdf. Letöltve: 2014.07. 17.

Egyéb internetes források:

Adrian Croft, Peter Apps: NATO websites hit in cyber attack linked to Crimea tension. Reuters, 2014. 03. 16. in:http://www.reuters.com/article/2014/03/16/us-ukraine-nato-idUSBREA2E0T320140316 Letöltve: 2014.06. 12.

Carnegie Endowment For International Peace: Russian military doctrine. 2010. 02. in:http://carnegieendowment.org/files/2010russia_military_doctrine.pdf, Letöltve: 2014.07. 27.

Chris Carroll : Should cyber warfare be elevated to highest command structure?. Stars and Stripes, 2013. 04. 29. in:http://www.stripes.com/news/should-cyber-warfare-be-elevated-to-highest-command-structure-1.218776, Letöltve: 2014.07. 27.

Cryptome.org: A Fierce Domain: Conflict in Cyberspace 1986 to 2012 by Jason Healey (Review). Cryptome.org, 2013. november 11. in: http://cryptome.org/2013/11/fierce-domain.htm, Letöltve: 2014. 06. 05.

Defense Update: The Ukrainian crisis – a cyber warfare battlefield. Defense Update, 2014. 04. 06. in: http://defense-update.com/20140405_ukrainian-crisis-cyber-warfare-battlefield.html#.U3SZDKL8eW8, Letöltve: 2014.07. 21.

Defenseworld.net: Indian Embassy's Systems in Moscow Hacked to Target Rosoboronexport. Defense World, 2014. 03. 07. in:http://www.defenseworld.net/news/10179/Indian_Embassy_s_Systems_in_Moscow_Hacked_to_Target_Rosoboronexport, Letöltve: 2014.07. 24.

Dr. Jarno Limnéll: Why hasn't Russia unleashed a cyber attack on Ukraine?. CBS News, 2014. 07. 02. in:http://www.cbsnews.com/news/why-hasnt-russia-unleashed-a-cyber-attack-on-ukraine/, Letöltve: 2014. 07. 08.

G Data Security Labs: Uroburos Highly complex espionage software with Russian roots. G Data Red Paper 2014. in: https://public.gdatasoftware.com/Web/Content/INT/Blog/2014/02_2014/documents/GData_Uroburos_RedPaper_EN_v1.pdf, Letöltve: 2014.07. 24.

Jaikumar Vijayan: Government role in Stuxnet could increase attacks against U.S. firms. Computerworld, 2014. 06. 02. In: http://www.computerworld.com/s/article/9227696/Government_role_in_Stuxnet_could_increase_attacks_against_U.S._firms, Letöltve: 2014. 06. 08

Jason Healey: Cyber Attacks Against NATO, Then and Now. Atlantic Council, 2011. 09. 06. in: http://www.atlanticcouncil.org/blogs/new-atlanticist/cyber-attacks-against-nato-then-and-now, Letöltve: 2014.06. 17.

Jason Healey: How to Beat a Russian Cyber Assault on Ukraine. Atlantic Council, 2014. 03. 03. in:http://www.atlanticcouncil.org/blogs/new-atlanticist/how-to-beat-a-russian-cyber-assault-on-ukraine, Letöltve: 2014.07. 20.

Jason Healey: NATO's Cyber Capabilities: Yesterday,Today, and Tomorrow. Atlantic Council, 2012. 02. in:http://www.atlanticcouncil.org/images/files/publication_pdfs/403/022712_ACUS_NATOSmarter_IBM.pdf, Letöltve: 2014.07. 17.

Jason Healey: Russia vs. Ukraine: The Cyber Front Unfolds. Atlantic Council, 2014. 04. 02. in: www.atlanticcouncil.org/blogs/new-atlanticist/russia-vs-ukraine-the-cyber-front-unfolds, Letöltve: 2014. 06. 04

Jeffrey Carr: Russian Cyber Warfare Capabilities in 2014 (We aren't in Georgia anymore). Digital Dao, 2014. 03. 08. in:http://jeffreycarr.blogspot.hu/2014/03/russian-cyber-warfare-capabilities-in.html Letöltve: 2014.07. 27.

Jeremy Hsu: Why There's No Real Cyberwar in the Ukraine Conflict. IEEE Spectrum, 2014. 03. 14. in: http://spectrum.ieee.org/tech-talk/computing/networks/why-theres-no-real-cyberwar-in-the-ukraine-conflict, Letöltve: 2014. 06. 08.

Kenneth Geers: Strategic Analysis: As Russia-Ukraine Conflict Continues, Malware Activity Rises. FireEye, 2014. 05. 28.

in:http://www.fireeye.com/blog/technical/2014/05/strategic-analysis-as-russia-ukraine-conflict-continues-malware-activity-rises.html, Letöltve: 2014.07. 25.

Kertu Ruus: Cyber War I: Estonia Attacked from Russia. European Affairs, Volume number 9, Issue number1 2/2008.In:http://www.europeaninstitute.org/index.php/component/content/article?id=67:cyber-war-i-estonia-attacked-from-russia, Letöltve: 2014. 06. 08.

Lenta.ru: Massive Attack перепели Янку Дягилеву и «Гражданскую оборону». Lenta.ru, 2014. 07. 07. In:http://lenta.ru/news/2013/07/07/yanka/ Letöltve: 2015. 02. 15.

Mark Clayton: Massive cyberattacks slam official sites in Russia, Ukraine. Csmonitor, 2014. 03. 18. in:http://www.csmonitor.com/World/Security-Watch/Cyber-Conflict-Monitor/2014/0318/Massive-cyberattacks-slam-official-sites-in-Russia-Ukraine, Letöltve: 2014.06. 17.

Mark Rutherford: Report: Russian mob aided cyberattacks on Georgia. CNET, 2009. 08. 18. in: http://www.cnet.com/news/report-russian-mob-aided-cyberattacks-on-georgia/, Letöltve: 2014.07. 22.

Mike Hoffman: Pentagon Denies Downed U.S. Drone Report in Crimea. Defense Tech. 2014. 03. 14. in:http://defensetech.org/2014/03/14/pentagon-denies-downed-u-s-drone-report-in-crimea/ Letöltve: 2014.06. 18.

Murray Brewster: NATO scrambles to knit together a cyberwar strategy. Macleans, 2014. 05. 06. in:http://www.macleans.ca/society/technology/nato-scrambles-to-knit-together-a-cyberwar-strategy/, Letöltve: 2014.07. 22.

NATO CCD COE: Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in the Information Space (unofficial translation). in: http://www.ccdcoe.org/strategies/Russian_Federation_unofficial_translation.pdf, Letöltve: 2014.06. 20.

NATO.int: NATO steps up collective defence, support for reforms in Ukraine. 2014. 06. 03.in:http://www.nato.int/cps/en/natolive/news_110609.htm?selectedLocale=en, Letöltve: 2014.07. 26.

NATO.int: Wales Summit Declaration. In: http://www.nato.int/cps/en/natohq/official_texts_112964.htm Letöltve: 2015. 02. 25.

Pavel Polityuk, Jim Finkle: Ukraine says communications hit, MPs phones blocked. Reuters, 2014. 05. 04., in:http://www.reuters.com/article/2014/03/04/us-ukraine-crisis-cybersecurity-idUSBREA231R220140304, Letöltve: 2014.07. 26.

Pierluigi Paganini: Crimea – Is Russia adopting the same cyber strategy used in Georgia?. Security Affairs, 2014. 03. 05. in: http://securityaffairs.co/wordpress/22781/cyber-warfare-2/crimea-russia-cyber-strategy.html, Letöltve: 2014. 06. 05.

Pierluigi Paganini: Crimea – The Russian Cyber Strategy to Hit Ukraine. Infosec Institute, 2014. 03. 11. in:http://resources.infosecinstitute.com/crimea-russian-cyber-strategy-hit-ukraine/, Letöltve: 2014.07. 25.

Piret Pernik: Is All Quiet on the Cyber Front in the Ukrainian crisis?, RKK CDS, 2014. 03. 07. in:http://blog.icds.ee/article/251/is-all-quiet-on-the-cyber-front-in-the-ukrainian-crisis, Letöltve: 2014.07. 27.

Rostec: Rostec official denial, in:http://rostec.ru/en/news/4416, Letöltve: 2014.07. 27.

US Army Space and Missile Defense Command Army Forces Strategic Command G39, Information Operations Division: Information Operations Newsletter. Vol. 14 No. 03. in: http://www.phibetaiota.net/wp-content/uploads/2014/05/ARSTRAT_IO_Newsletter_v14_no_03.pdf Letöltve: 2015. 02. 20.

Voiceofrussia.com: US drone intercepted in Crimean airspace - Russia's state corporation. Voiceofrussia, 2014. 03. 14. in:http://voiceofrussia.com/news/2014_03_14/US-drone-intercepted-in-Crimean-airspace-Russias-state-corporation-2994/, Letöltve: 2014.07. 27.

Waqas: Anonymous Declares Cyberwar on Countries Found Disturbing Peace in Ukraine. Hackread, 2014. 03. 28. in:http://hackread.com/anonymous-ukraine-declares-cyberwar/, Letöltve: 2014.06. 27.

Ward Carroll: Cyber War 2.0 — Russia v. Georgia. Defense Tech, 2008. 08. 13., in: defensetech.org/2008/08/13/cyber-war-2-0-russia-v-georgia/,Letöltve: 2014.07. 12.

William Knowles: U.S. Department of Justice Indicts Five Members of the Chinese PLA 'Unit 61398' for Cyber Espionage. Infosec News, 2014. 05. 20. in:http://www.infosecnews.org/u-s-department-of-justice-indicts-five-members-of-the-chinese-pla-unit-61398-for-cyber-espionage/,Letöltve: 2014.06. 27.

William Marmon: A Fierce Domain: Conflict in Cyberspace, 1986 to 2012," by Jason Healey (Review). European Affairs, 2013 july. in: http://www.europeaninstitute.org/index.php/180-european-affairs/ea-july-2013/1769-a-fierce-domain-conflict-in-cyberspace-1986-to-2012-by-jason-healey, Letöltve: 2014. 06. 08.