*Brányi Bence**

Szemelvények a kiberhadviselés jelenéből

Az informatika uralta haderők sebezhetőségének érzékeltetése öt példán keresztül I. rész

Bevezető

A tudás átörökítése terén (az írás megalkotása után) valószínűleg az emberiség második legfontosabb találmánya a számítógépek hálózatba kapcsolása, amely néhány évtized alatt világszerte az élet majdnem minden területén elterjedt, korábban elképzelhetetlen lehetőségeket teremtve.

Az internet és az eléréséhez használt számítógépek három legfontosabb jellemzője a rendkívül alacsony belépési küszöb (használatukhoz nincs szükség extra drága, speciális eszközökre vagy szaktudásra), az azonnali hozzáférés az adatokhoz (a hálózat tagjai a távolságtól gyakorlatilag függetlenül kapcsolódhatnak) és a nagyon komoly számítási kapacitás.

Az internet azonban nem csak lehetőségeket, de egyben nagyon komoly biztonsági kockázatokat is rejt. Ma már az érzékeny, védelmet igénylő adatok (személyek egészségügyi és pénzügyi adatai, de a cégek, állami szervezetek és a hadsereg adatainak) túlnyomó többségét is hálózatba kapcsolt számítógépen tárolják. Ez viszont azt jelenti, hogy – éppen a fenti jellemzők miatt – az adatok megszerzése és a velük való visszaélés is minden korábbinál egyszerűbb: az összes hálózatba kapcsolt gép potenciális célpont és akár egyetlen támadó is több tucat erős fizikai védelemmel rendelkező intézménybe törhet be úgy, hogy azt a károsultak csak jóval később, vagy egyáltalán nem fedezik fel.

A számítógépes hálózatok, programok sebezhetőségét, a hibákat, kiskapukat, illetve a felhasználók manipulálhatóságát kihasználó károkozást kibertámadásnak is nevezik; néhány pénzügyi bűncselekményt (pl.: sikkasztást) leszámítva a nagy értékű bűncselekmények többségét ma már a kiberbűnözés számlájára írják, és ezen az analógián haladva létrejött a kiberterrorizmus, és államok közötti kiberhadviselés is.

A kiberhadviselés végrehajtói, formái, céljai

A kiberhadviselésnek nincs egyértelmű definíciója, de általában azon tevékenységek összességét sorolják ide, amelyek célja egy másik nemzet számítógépes eszközeinek vagy hálózatának támadása, az azokba való behatolás, adatszerzés és károkozás, ugyanakkor maga a forgalom rendkívül szerteágazó, számos potenciális elkövetővel, motivációval, változatos elkövetési móddal és eredménnyel.

A kiberhadviselés elkövetői lehetnek teljesen amatőr végfelhasználók, akik már létező keretrendszereket[1] használnak, amatőr programozók (Script Kiddie-k), de haderők, állami ügynökségek és nagyvállalatok szakemberei is.

A lehetséges motivációk között szerepelhet a morális elhivatottság (pl.: katonák, állami alkalmazottak, de önkényesen cselekvő civilek is), pénz (felbérelt elkövető vagy értékesíthető információk megszerzése), de valamilyen sérelem megtorlása (bosszú) is. Emellett motivációként azonban jelen van a pusztítási vágy, a szórakozásból elkövetett bűncselekmény, a könnyelműség vagy akár a hírnév hajszolása is – utóbbira jelentenek példát a számítógépes játékok komoly másolásvédelmét (pl.: Denuvo) minél gyorsabban feltörni próbáló profi (részben kínai és orosz) csoportok.

A kibertámadásokban a fizikai támadás ritka, de nem ismeretlen, például a szélessávú internetkapcsolatot biztosító optikai kábelekbe és adótornyokba történő behatolás formájában. A támadásnak ezen kívül többféle módja ismert: különböző kártékony programok használata, több száz géppel vérhajtott túlterheléses támadás, de egy rendszerbe akár egy fegyelmezetlen vagy túlzottan segítőkész alkalmazotton keresztül is be lehet jutni (utóbbi esetekben gyakran teljesen kikerülve a biztonsági programokat).

Sok esetben a támadók szoftverhibákat használnak ki, amely ellen az átlagos végfelhasználó érdemben nem tud tenni[2] – a programok biztonsági hibáit nem egy esetben csak évekkel később fedezik fel, és a rendszerek komplexitásának növekedésével a veszélyességük is nő. Katonai (de polgári szempontból is) komoly biztonsági kockázatot jelent a globalizáció: a használt programokat a szervezet már nem maga írja, hanem vásárolja, annak fejlesztésébe nincs beleszólása, az mások számára is könnyen beszerezhető (esetenként nyílt forráskódú), lehetővé téve az adott program hibáinak könnyebb megtalálását, majd kihasználását.

A nagyközönségnek gyártott programok katonai felhasználása ma már általános: az amerikai F–22 „Raptor” va-

ÖSSZEFOGLALÁS: Az elmúlt években a számítógépes hálózatok az élet minden területén, köztük a hadseregnél is széles körben elterjedtek. Az új lehetőségek mellett azonban e technológia rendkívüli veszélyekkel is jár: ellenséges haderők támadhatják a harcjárművek rendszereit, információt szerezhetnek vagy akár jelentős gazdasági károkat is okozhatnak.

KULCSSZAVAK: kiberhadviselés, informatika, DDoS, NSA, Stuxnet, RQ-170, Észak-Korea

ABSTRACT: In recent years, computer networks have been spread in all areas of life, including the military. However, in addition to the new possibilities, this technology also poses extreme threats: hostile forces may attack the systems of combat vehicles, obtain information or even cause significant economic damage.

KEY WORDS: cyber warfare, IT, DDoS, NSA, Stuxnet, RQ-170, North Korea

* ORCID: 0000-0001-6025-1547

DOI: 10.23713/HT.52.4.03

dászrepülőgép központi számítógépét például még Ada programozási nyelven írták, amely egy zárt, rendkívül biztonságosnak tartott programozási nyelv. Az Egyesült Államokkal szövetséges országok számára is értékesített F–35 „Lightning II” típuson ezzel szemben (költségcsökkentési okokból) már kereskedelmi forgalomban kapható részegységeket használtak, a programokat pedig C, valamint C++ programozási nyelven írták, ez utóbbiak elterjedtsége miatt hozzáértő programozók széles köre áll rendelkezésre az egész világon, ami egyben előny, de potenciális biztonsági kockázat is. A szoftverek erejét nem szabad lebecsülni – az F–35-ös még 2018 elején sem volt teljes mértékben bevethető, mivel a központi rendszer és egyes részprogramok (köztük a radar és a HUD szoftvere) súlyos problémákkal küzdött, korábban pedig előfordult, hogy repülés közben összeomlott és újraindítást igényelt a teljes rendszer (ez a Block 3i mellett az újabb Block 3F verzió esetében is előfordult).

A kibertámadások célpontjai az elkövetési módhoz hasonlóan igen széles kört ölelnek fel. Gyakorlatilag az összes értékes információt tároló vagy használó állami létesítmény (nem kizárólag katonaiak), de az alapvető infrastruktúra, pénzintézetek és polgári vállalatok (köztük katonai cégek beszállítói) is támadás áldozataivá válhatnak, hatalmas anyagi és erkölcsi károkat szenvedve el, sőt, a számítógép által vezérelt jármű vagy más eszköz akár emberéletet is követelhet.[3]

A kiberhadviselés több cél érdekében történhet. Az elkövetők az általuk megszerzett információkkal visszaélve megvalósíthatnak kémkedést (információlopást), titkos adatokat nyilvánosságra hozva kompromittálhatnak, felhasználhatják propaganda célokra, illetve ennek részeként lejárathatnak, vezérlőrendszerek módosításával fizikai pusztítást is okozhatnak (szabotázs), de a támadás irányulhat az ellenséges országot, vagy cégeit, lakosait megkárosító pénzszerzésre is.

A kiberhadviselés előnyös tulajdonsága, hogy a világhálón keresztül távoli, fizikailag erősen őrzött célpontok is támadhatók (például minden nap számos támadási kísérlet történik a Pentagon rendszerei ellen) és bár egy hatékony kiberalakulat fenntartása dollármilliókba kerülhet, ez így is eltörpül a harcjárművek megvásárlásának és fenntartásának nagyságrendekkel magasabb összege mellett. Mindezek (és a potenciális anonimitás) miatt, a nagyhatalmak mellett több korlátozott méretű haderő, valamint szakadár (köztük terroristának tartott) szervezet is preferálja az internetes hálózatokon történő támadásokat.

Ezt a folyamatot az is elősegíti, hogy a hagyományos (két hadsereg közötti) harcok részaránya mára minimálisra csökkent, helyét az aszimmetrikus hadviselés vette át. Ezek többségében hosszú ideig tartó konfliktusok, amelyekben a jelentős erőfölénnyel rendelkező hagyományos haderő csak korlátozottan használható, mert a gyengébb fél (pl.: lázadók, terroristák) nem rendelkezik klasszikus célpontokkal (pl.: gyárakkal), amelyeket elpusztítva kivívható lenne az egyértelmű győzelem és a decentralizált felépítésük miatt még a vezetők likvidálása sem feltétlenül okoz megsemmisítő vereséget.

Ahogy a hadseregek által használt eszközökben is elterjedtek az összekapcsolt számítógépes rendszerek, a támadható informatikai célok száma a korábbi sokszorosára nőtt. A célpont nem feltétlenül egy rendszeresített haditechnikai eszköz (pl.: harckocsi), értékes információk nyerhetők például egy hazautazó katona okostelefonjának (szoftveres) lehallgatása során, de akár egy elektromos bojler vezérlőrendszerének módosításával is (pl.: egy afganisztáni tábor számítógép-vezérelte légkondicionáló berendezéseit tönkretéve a katonák komfortérzete, ezáltal harckészsége csökkenthető).

A kiberhadviselés tehát hihetetlenül szerteágazó téma, teljes körű bemutatását pedig tovább nehezíti, hogy az esetek túlnyomó részében az érintett államok és cégek (az elkövető és az elszenvedő is) tagadja a behatolást, a támadást elkövető személyek ellen a megrendelő ország értelemszerűen nem indít eljárást, sőt, magát a támadás tényét is titokban tartja, mivel így a sebezhető területet a későbbiekben is kihasználhatja.

Jelen írás ezért nem is egy felületes átfogó ismertetésre törekszik – ehelyett néhány (a főbb támadási profilokat lefedő) példán keresztül mutatja be az elmúlt évek néhány nagy horderejű, a kiberhadviselés témakörébe tartozó támadásait, az elkövetés módját, az okozott kárt, a feltételezett elkövetőket és ennek okait, érzékeltetve a téma sokszínűségét.

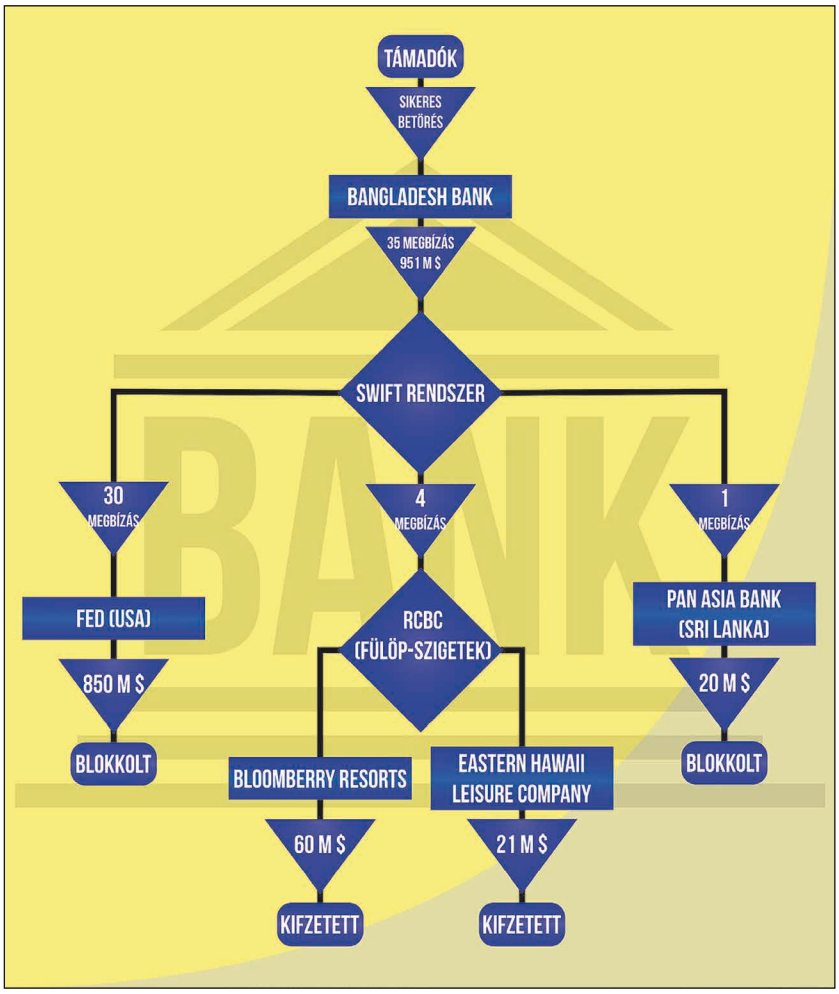
Pénzlopás (Észak-Korea)

A Koreai Népi Demokratikus Köztársaság, közkeletű nevén Észak-Korea a világ egyik leginkább elzárt, kommunista országa. Észak-Korea meghatározó ideológiája a dzsucse, amelynek lényege a teljes mértékű önfenntartás, a globalizáció tagadása, a bezárkózás és a kommunista mintára történő folyamatos ellenségkeresés.

Észak-Korea gazdaságilag gyakorlatilag életképtelen állam, túlélését utolsó támogatójának, a szintén kommunista Kínai Népköztársaságnak köszönheti, amely számára rendkívül fontos, hogy határa és a demokratikus, Amerikabarát Dél-Korea között pufferzónát tartson fent. Észak-Korea valamivel egymillió fő feletti aktív állományú hadsereggel rendelkezik, és folyamatosan készül egy (elsősorban az Amerikai Egyesült Államok és Dél-Korea elleni) inváziórа[4], de az állandó fegyverkezés a gazdaságilag fejletlen országnak rendkívüli megterhelést jelent.

Az ország számára az egyik legnagyobb problémát a valutahiány jelenti. Észak-Korea gyakorlatilag hermetikusan elzárkózott a világ többi részétől, ami a lakosságtól hatalmas áldozatokat kíván, de a hadsereg fejlesztéséhez szükséges bizonyos mennyiségű import fenntartása. A problémát az okozza, hogy az emberiesség elleni bűncselekmények, nukleáris- és ballisztikusrakéta-programjai miatt Észak-Korea nemzetközi embargók hatálya alá esik, ezért csak közbenső cégek beiktatásával, magas áron juthat a szükséges anyagokhoz. A helyzetet tovább súlyosbítja, hogy pénzneme, az észak-koreai von nemzetközi szinten értéktelen, és (mivel nem enged be befektetőket) teljes mértékben tervutasításos gazdasága a lehetséges potenciáljától messze elmarad,

1. ábra. Észak-koreai kadétok informatika-oktatásban részesülnek (számítógépeik monitorát a német Belinea, illetve a Fujitsu Siemens Computers gyártotta)



2. ábra. A támadás vázlata, illetve az egyes megbízások értéke és sorsa

gyakorlatilag az ország csak nyersanyagokat értékesíthet, amely iránt minimális a kereslet.

Az érdemi export, bankrendszer és turizmus nélküli ország a valuta (elsősorban amerikai dollár) megszerzésének módját a fegyver- és kábítószer-csempészetben, valamint a kiberhadviselésben vélte megtalálni. 1994-ben még a jelenlegi pártfőtitkár, Kim Dzsong Un apja, Kim Dzsong Il alapította a 121-es irodát, amelynek célja kibertámadások végrehajtása az Amerikai Egyesült Államok, Dél-Korea és Japán célpontok ellen. Dél-Koreát 2009-ben, 2011-ben és 2013-ban is széles körű támadások érték, amelyek elsősorban banki szolgáltatásokat (pénzkiadó automatákat és mobil fizetési rendszereket), valamint TV-állomásokat céloztak. Egyesek a Sony Pictures 2014-es adatlopását is Észak-Koreának tulajdonítják, igaz, ennek ellentmondó információk is napvilágot láttak.

Ezek „hagyományos" támadások voltak, céljuk elsősorban káosz és pénzveszteség okozása volt, az utóbbi években viszont az észak-koreai kibertámadások prioritása megváltozott, elsődleges céllá a pénzszerzés vált. 2016 februárjában ismeretlen tettesek betörtek a Bangladesh Bank rendszerébe (Banglades állam központi bankjába), ahonnan átutalási megbízásokat adtak összesen 951 millió dollár átutalására. Az akciót február 4-5-re időzítették, amikor a bankfiókok zárva tartottak (az átutalási rendszer folyamatosan üzemel). A támadók a kifejezetten banki adatok ellopására kifejlesztett Dridex trójait használták (egy, a felhasználó tudta nélkül tevékenykedő programot), amelyel ismeretlen elkövetők már 2014-ben is összesen több millió dollárt szereztek meg, és amelyet 2015-ben az IT-szakma egyszer már legyőzöttnek ítélt.

A program a Microsoft Office makróit kihasználva működik, a gépekre fertőzött Word és Excel fájlokkal került. A behatolást követően a támadóknak rálátása nyílt a bank által használt kifizetések rendszerére és hozzáférést szereztek a SWIFT-hez, a bankok közötti átutalási rendszerhez, majd ezt kihasználva 35 megbízást adtak ki amerikai, Srí Lanka-i és Fülöp-szigeteki bankoknak.

A bank és a befektetők szerencséje az volt, hogy a támadók a teljes rendszert nem ismerték. A pénz nagy részét az Amerikai Egyesült Államokon keresztül próbálták átutalni, de az ország központi bankrendszere, a Federal Reserve System (röviden FED) a beérkezett 30 átutalást kérdésesnek tartotta, ezeket banki alkalmazottak megvizsgálták, majd az átutalást leállították (mintegy 850 millió dollár összértékben). A fennmaradó pénzből 81 millió dollár a Fülöp-szigeteki Rizal Commercial Banking Corporation (röviden RCBC) bankrendszeren keresztül három Hong Kong-i kaszinóba került, a pénzmosást követő sorsuk ismeretlen (feltételezhetően a támadók kezébe került), míg egy 20 millió dolláros Srí Lanka-i tranzakció az elkövetők figyelmetlensége miatt hiúsult meg. Utóbbi esetben az elkövetők a helyi Shalika Foundation (Shalika alapítvány) számlájára utalták a pénzt, de az alapítvány nevét elírták, „Shalika Fundation"-t tüntetve fel, ami feltűnt az átutalásban résztvevő Deutsche Bank alkalmazottjának, aki – miután megkereste a Bangladesh Bank-ot – blokkolta az átutalást.

Korábban, 2015-ben, majd 2016-ban már több kísérlet is történt a SWIFT-rendszeren keresztüli pénzlopásra, de ezek lényegesen kisebb összegekről szóltak és sikertelenek voltak. A célok között vietnami, ecuadori és közel-keleti bankok szerepeltek. A támadások lehetséges elkövetői között szerepelt a Lazarus Csoport nevű, valószínűleg észak-koreai kötődésű hacker-csoport. Amennyiben bebizonyosodna Észak-Korea érintettsége, ez lenne a világ első, egy állam által megrendelt, pénzlopásra irányuló kibertámadása.

Önmagában a 81 millió dollárnyi, sőt, akár a teljes, 951 millió dolláros összeg sem jelent kiheverhetetlen veszteséget, azonban több sikeres támadás alááshatja a globális, valódi alternatíva nélküli SWIFT-rendszerbe vetett bizalmat is.[5]

Teljesen más típusú, kifejezetten a nagyközönséget érintő, de azonos célú támadás volt a 2017 májusában felbukkanó WannaCry zsarolóvírus. Ennek lényege, hogy a felhasználó, miután megnyitotta egy ismeretlen feladótól származó fertőzött e-mail mellékletét, az egy kártékony programot telepített a gépére, amely titkosította a felhasználó egyes adatait; képeit, dokumentumait, banki információt, majd ezek visszaállításáért váltságdíjat kért. A követelt összeget kriptovalutában kellett kifizetni, mivel ezt gyakorlatilag lehetetlen nyomon követni.

3. ábra. A WannaCry vírus felhasználói felülete

4. ábra. A Pentagon, az Amerikai Egyesült Államok Védelmi Minisztériumának Virginia állambeli ikonikus központja. A Védelmi Minisztérium irányítása alá tartozik az amerikai hírszerző ügynökségek többsége, köztük a Nemzetbiztonsági Hivatal (NSA) és a Nemzeti Felderítő Hivatal (NRO), a Központi Hírszerző Ügynökség (CIA) azonban nem

5. ábra. Észak-Korea vezetője, Kim Dzsong Un ismeretlen észak-koreai létesítményben tesz látogatást

A támadásoknak néhány óra alatt kb. 150 ország több mint 200 000 számítógépe esett áldozatul, köztük olyan nagyvállalatok, mint az amerikai FedEx csomagküldő, a német Deutsche Bahn vasúttársaság, de a Telenor magyarországi leányvállalata is. A zsarolóvírus rávilágított a támadás emberéletet veszélyeztető mivoltára is, ugyanis a WannaCry az angol National Health Service központi egészségügyi irányító/finanszírozó szervezet mintegy 70 000 gépét is megfertőzte, ezáltal több ezer orvosi diagnosztikai eszköz átmenetileg használhatatlanná vált.

A vírussal szerzett pénz mennyisége nem ismert, de a gazdaságnak még az óvatosabb becslések szerint is többszáz millió (akár több milliárd) dolláros kárt okozott, mivel több vállalat (köztük a Honda, a Nissan és a Renault autógyártók) komplett gyártósorai bénultak meg vagy a további károkat megelőzendő leállításra kerültek.

2017 decemberében az Amerikai Egyesült Államok, Ausztrália és az Egyesült Királyság közös nyilatkozatában Észak-Koreát vádolta meg a támadással. Az Észak-Koreának tulajdonított, pénzlopásra irányuló támadások egy részét kínai szerverekig sikerült visszakövetni. Ebben az időszakban Észak-Korea egyetlen külföldi gerinc internetvonala Kínához kapcsolódott (ezt ma már egy második, Koreát Oroszországgal összekötő vonal egészíti ki).

A támadást a Windows EternalBlue biztonsági rése tette lehetővé, amelyet az amerikai NSA fejlesztett ki azért, hogy hozzáférjen a Windows operációs rendszereken tárolt adatokhoz, azonban ezt a The Shadow Brokers nevű hackercsoport megszerezte a szervezettől, majd nyilvánosságra hozta. Az NSA kémeszközét nem csak a WannaCry használta ki, de a 2017-ben Ukrajnában megjelent, majd több országban elterjedt NotPetya zsarolóvírus is.

(Folytatjuk)

Források

Akhgar, Babak – Brewster, Ben (szerk.): Combatting Cybercrime and Cyberterrorism: Challenges, Trends and Priorities. Springer, 2016. ISBN 978-3-319-38929-5;

Zetter, Kim: Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon. New York: Broadway Books, 2015. ISBN 978-0-7704-3619-3;

Chawki, Mohamed et al.: Cybercrime, Digital Forensics and Jurisdiction. Springer, 2015. ISBN 978-3-319-15149-6;

Bernik, Igor: Cybercrime and Cyber Warfare. Wiley-ISTE, 2014. ISBN 978-1-84821-671-6;

Kshetri, Nir: Cybercrime and Cybersecurity in the Global South. New York: Palgrave Macmillan, 2013. ISBN 978-1-137-02193-9;

Gragido, Will et al: Blackhatonomics: An Inside Look at the Economics of Cybercrime. Syngress, 2012. ISBN 978-1-59749-740-4;

Gragido, Will; Pirc, John: Cybercrime and Espionage: An Analysis of Subversive Multi-Vector Threats. Syngress, 2011. ISBN 978-1597496131;

McQuade III, Samuel C. (szerk.): Encyclopedia of Cybercrime. Greenwood, 2008 ISBN 978-0313339745;
Interjú Anders Fogh-gal. PC World, 2018.01.15 https://pcworld.hu/pcwpro/meltdown-spectre-serulekenyseg-testkozelbol-interju-242545.html [2018.04.16.];
Lara Seligman: Final Software Load Plagues F-35 Test Jets. Aviation Week Network, 2016 07.11. http://aviationweek.com/defense/final-software-load-plagues-f-35-test-jets [2018.04.16.];
Sam Kim: How North Korea Built An Army of Hackers: Q&A. Bloomber Technology, 2017.10.17. https://www.bloomberg.com/news/articles/2017-10-17/how-north-korea-built-an-army-of-cyber-warriors-quicktake-q-a [2018.04.16.];
David E. Sanger, David D. Kirkpatrick, Nicole Perlroth: The World Once Laughed at North Korean Cyberpower. No More. New York Times, 2017.10.15. https://www.nytimes.com/2017/10/15/world/asia/north-korea-hacking-cyber-sony.html [2018.04.16.];
Paul Mozur, Choe Sang-Hun: North Korea's Rising Ambition Seen in Bid to Breach Global Banks. New York Times, 2017.03.25. https://www.nytimes.com/2017/03/25/technology/north-korea-hackers-global-banks.html [2018.04.16.];
Janene Pieters: Russian servers linked to DDoS attack on Netherlands financial network. nltimes.nl, 2018.01.29. https://nltimes.nl/2018/01/29/russian-servers-linked-ddos-attack-netherlands-financial-network-report [2018.04.16.];
zerocool: DoS, és DDoS támadások (túlterheléses támadások). Ethical hecker tutorials, 2013.12.06. http://backtracktut.blogspot.hu/2013/12/dos-es-ddos-tamadasok-tulterheleses.html [2018.04.16.];
Dömös Zsuzsanna: Mit kellene megbocsátani Edward Snowdennek? Origo, 2016.09.15. http://www.origo.hu/techbazis/20160915-edward-snowden-nsa-lehallgatasi-botrany-kembotrany.html [2018.04.16.];
Bolcsó Dániel: Csatát vesztett az NSA, de a totális megfigyelésnek nincs vége. Index.hu, 2015.12.11. https://index.hu/tech/2015/12/11/nsa_freedom_act_megfigyeles_snowden/ [2018.04.16.];
NSA monitored calls of 35 world leaders after US official handed over contacts. The Guardian, 2013.10.24. https://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls [2018.04.16.];
Exclusive: NSA pays £100m in secret funding for GCHQ. The Guardian, 2013.08.01. https://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden [2018.04.16.];
NSA Prism program taps in to user data of Apple, Google and others. The Guardian, 2013.06.06. https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data [2018.04.16.];
NSA collects millions of e-mail address books globally. The Washington Post, 2013.10.14. https://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html?utm_term=.c720a62d5abf [2018.04.16.];
Beismerték Merkel lehallgatását. Index.hu, 2013.10.30. https://index.hu/tech/2013/10/30/az_nsa_a_google-t_es_a_yahoo-t_is_figyelte/ [2018.04.16.];
Paul Mueller, Babak Yadegar: The Stuxnet Worm https://www2.cs.arizona.edu/~collberg/Teaching/466-566/2012/Resources/presentations/2012/topic9-final/report.pdf [2018.04.16];
Jim Finkle: Researchers say Stuxnet was deployed against Iran in 2007. Reuters, 2013.02.06 https://www.reuters.com/article/us-cyberwar-stuxnet/researchers-say-stuxnet-was-deployed-against-iran-in-2007-idUSBRE91P0PP20130226 [2018.04.16];
David Shepardson: Tesla driver in fatal ‚Autopilot' crash got numerous warnings. Reuters, 2017.06.19 https://www.reuters.com/article/us-tesla-crash/tesla-driver-in-fatal-autopilot-crash-got-numerous-warnings-u-s-government-idUSKBN19A2XC [2018.04.16];
Loveday Morris, Ruth Eglash: The drone shot down by Israel was an Iranian copy of a U.S. craft, Israel says. The Washington Post, 2018.02.11 https://www.washingtonpost.com/world/israel-confirms-downed-jet-was-hit-by-syrian-antiaircraft-fire/2018/02/11/bd42a0b2-0f13-11e8-8ea1-c1d91fcec3fe_story.html?utm_term=.b9c1d24ea8ec [2018.04.16].

Jegyzetek

1 Pl.: a nyílt forráskódú, ingyenes, hálózatok stressztesztelésére (azaz gyakorlatilag DoS/DDoS támadásra) kifejlesztett Low Orbit Ion Cannon és utóda, a High Orbit Ion Cannon.

2 Az év első ilyen eseményei a Meltdown és Spectre biztonsági hibák voltak, amelyek azonban a megszokottól eltérően hardverhibák, súlyosságuk kiemelkedő. E problémák a világ gyakorlatilag összes számítógépét veszélyeztetik: az AMD és Intel processzorok mellett az ARM-alapú és az IBM processzorokat is, a végleges megoldás ebben az esetben az összes érintett processzor lecserélése.

3 2016. május 7-én az amerikai Joshua Brown életét vesztette, miután félautomata üzemmódban haladó („önvezető") Tesla Model S gépjárműve teljes sebességgel belerohant egy kanyarodó vontatóba. Az önvezető személyautók első halálos balesetét vizsgáló NHTSA (amerikai autópálya-közlekedésbiztonsági hatóság) megállapította, hogy a gyártó Tesla nem vétkes, mert bár a halálos kimenetel a program hibája (a jármű egyáltalán nem fékezett), az önvezető rendszer tökéletlensége miatt az eszköz jelenleg folyamatos emberi felügyeletet igényel.
2018. március 18-án az Uber önvezető terepjárója halálra gázolt egy nőt Arizónában, amikor kivilágítatlanul, egy négysávos úton kelt át biciklijét tolva – feltehetően szabálytalanul.
Másrészről azt is meg kell jegyezni, hogy jelenleg az USA-ban 253 millió gépjármű rója az utakat nap, mint nap, és 2016-ban 40 ezer végzetes kimenetelű baleset ismert. Optimista becslések szerint néhány éven belül az autók 10%-a lehet önjáró, amitől a balesetek számának drasztikus csökkenését várják.

4 A két Korea formálisan a mai napig hadban áll egymással, mivel a háborút csak fegyverszünet zárta le, békekötésre nem került sor. Másrészről 2018 februárjában Mun Dzse In dél-koreai elnök a phjongcsangi téli olimpiai megnyitója alkalmával fogadta a hivatalos észak-koreai küldöttséget.

5 Természetesen léteznek alternatív rendszerek (pl.: az európai SEPA, a VISA B2B vagy a Ripple, emellett Kína és Oroszország is saját rendszert fejleszt), de egyik sem rendelkezik a SWIFT-éhez mérhető lefedettséggel és átláthatósággal, ezért az 1973 óta létező Society for Worldwide Interbank Financial Telecommunication, röviden SWIFT megbízható működése kulcsfontosságú.

(Illusztrációk a szerző gyűjteményéből.)