6. ábra. Az Eikonal hadművelet keretében az NSA és német megfelelője, a Bundesnachrichtendienst (BND) felderítőközpontot üzemeltetett Bajorországban (Bad Aibling Station, Németország), de ezt az együttműködést az adatgyűjtéssel kapcsolatos nézeteltérések miatt 2016-ban a németek leépítették

*Bányi Bence**

Szemelvények a kiberhadviselés jelenéből

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

Adatgyűjtés (USA)

A második világháború végére az Amerikai Egyesült Államok vált a világ legnagyobb demokratikus nagyhatalmává, akkor alakult ki az Amerikai Egyesült Államokban a „világrendőrség" mentalitás, a fejlett világot védelmező ország képe, amely az egész világot védi a diktatúráktól. A német Harmadik Birodalom legyőzését követően azonban az amerikaiak volt szövetségesükkel, a Szovjetunióval és Kínával kerültek szembe, és kritikussá vált az információszerzés kérdése. Amíg a németek által megszállt országokban a helyi ellenálló csoportok a saját életük kockáztatásával folyamatosan szállították az információt a németek minden mozdulatáról, addig az amerikaiak sohasem tudtak jelentős számban titkos ügynököt beépíteni, illetve helyi vezetőket lefizetve vagy megzsarolva elegendő információhoz jutni a mélyen a Szovjetunióban és az általa megszállt országokban található katonai létesítményekről.

A hagyományos, terepen végzett kémkedést ezért mindinkább a technológiára támaszkodó információszerzés vette át. Ezek közé tartoztak a Project Genetrix és Project Moby Dick kémballonok, az U-2-es és SR-71-es kémrepülőgép vagy a Key Hole kémműhold-rendszerek. A hidegháború után a mobiltelefonok és az internet térnyerésével a magasan képzett ügynökök mellett a pilóták helyét is számítógépes szakemberek vették át, akik távoli hozzáféréssel, szoftveres segítséggel végeztek és végeznek adatelemzéseket, szereznek meg értékes információkat.

E nézőpontváltás részeként a Központi Hírszerző Ügynökség (CIA) mellett rendkívüli mértékben megerősödött a Nemzetbiztonsági Ügynökség (NSA), amely a rádióelektronikai jelhírszerzésre (SIGINT) szakosodott, de kriptográfiával és az internetes adatforgalom felügyeletével is foglalkozik (a szervezet létszáma mára egyes adatok szerint a CIA kétszeresére duzzadt).

Az NSA-t 1952-ben alapították, és elsősorban az új elektronikus eszközöket kihasználó, korábban elképzelhetetlennek tartott volumenű adatgyűjtéssel és adatfeldolgozással foglalkozott. Ezek közé tartozott a már közvetlenül a második világháborút követően elindított SHAMROCK program, amelyben elődje, az AFSA (később pedig az NSA) mikrofilmen rögzítette az összes, az Amerikai Egyesült Államokban a Western Union cég rendszerén keresztül érkező táviratot, majd a hírszerzés által fontosnak vélteket más titkosszolgálatoknak továbbították.

Az NSA gyakran jogellenesen hajtott végre akciókat. 1975-ben a sorozatos jogsértések miatt a SHAMROCK műveletet le kellett állítani, és ma már ismert, hogy a hidegháború alatt több ezer, a nemzetbiztonságra veszélytelen amerikai és külföldi személyt (köztük emberi jogi aktivistá-

* ORCID: 0000-0001-6025-1547

DOI: 10.23713/HT.52.5.02

7. ábra. Az RNO NROL–39 (US–247) jelű rakétaindítás logója. (A felirat: Nothing is beyond our reach – Számunkra semmi sem elérhetetlen.) A 2013-as küldetés során egy Atlas V rakéta a hattagú Future Imagery Architecture kémműhold-program harmadik példányát állította Föld körüli pályára. A legutóbbi rakétaindításra 2018. január 12-én került sor

kat) is megfigyeltek (a sorozatos jogsértések csak a Watergate-botrányt követő vizsgálatok során derültek ki).

A nyilvánosságra került adatok alapján az NSA később is folytatott jogsértő programokat, de a 2001. szeptember 11-ei terrortámadást követően az amerikai politikai vezetés elnézőbbé vált a szervezettel szemben, mert a műholdak és internetes kommunikáció megfigyelése és feldolgozása részeként a szervezet információkkal segítette a terrorizmus elleni harcot. A 2010-es évekre az NSA ismét kikerült a köztudatból, amikor 2013-ban kirobbant a Snowden-ügy.

Edward Joseph Snowden (1983–) egy, a CIA-nak dolgozó informatikus volt, aki saját bevallása szerint – miután látta, hogy a kampányában kommunikált ígéreteivel szemben, az újonnan megválasztott amerikai elnök, Barack Obama republikánus elődjéhez hasonlóan elnéző az NSA jogsértő programjaival –, több újságíróval tárgyalva nyilvánosságra hozott számos NSA dokumentumot. Ezekből kiderült, hogy az NSA több mint egy milliárd ember telefonos beszélgetéseit és teljes információ-áramlását figyelte; a túlnyomórészt a hírszerzés számára érdektelen magánszemélyek és cégek kommunikációját vizsgálva számos gazdasági és ipari titkot, illetve kompromittáló anyagot szerezhetett meg.

A Snowden által nyilvánosságra hozott iratokból kiderült, hogy az NSA gyakorlatilag az egész világon bárki azonosítására és megfigyelésére képes volt. A legtöbb ismert számítógépes vállalat (köztük a Google, az Apple és a Microsoft) rendszereit és eszközeit fel tudta törni (amit az erre feljogosító bírósági végzés nélkül is több esetben megtett), vagy azokat lefizetve, rájuk nyomást gyakorolva együtt tudott működni, hozzáférve az összes általuk tárolt adathoz. Hasonlóképpen naponta több száz millió mobiltelefon mozgását dokumentálta és a megszerzett adatokat felhasználva az adott személy ismerőseinek listáját is megszerezte, tovább bővítve a megfigyeltek körét, akár valós időben is.

A hihetetlen mennyiségű információ megszerzését, feldolgozását és esetleges felhasználását az NSA a terrorizmus elleni harc szlogenje jegyében, részben az amerikai jogszabályokat megszegve végezte. Az Amerikai Egyesült Államokban széleskörű felháborodást keltett, hogy az NSA – hozzáférve a teljes amerikai internetes forgalomhoz – akár az amerikai lakosság negyedét is folyamatosan megfigyelés alatt tarthatta.

Az NSA a világ majdnem összes országban végzett ilyen kémtevékenységet (Kínában több lehallgató állomást is felállítottak, egyet a pekingi ausztrál nagykövetségen). Egyes, potenciális ellenségnek tartott országok, pl.: Oroszország, ez ellen igyekezett fellépni (pl.: az oroszok az NSA-tól saját módszereivel szereztek meg adatokat, Kína pedig néhány év alatt számos amerikaiaknak dolgozó ügynököt fogott el), nemzetközi szinten viszont az váltott ki széles körű felháborodást, hogy kiderült, az NSA adatlopásainak egy része kifejezetten szövetséges országok ellen irányult.

A nyilvánosságra hozott információk szerint egyetlen akció során mintegy 200 fő, ebből 35 ország vezetőjének beszélgetéseit hallgatták le, köztük a német kancellár, Angela Merkel telefonját (2002 óta) és az Egyesült Királyságban is több millió főt figyeltek meg, annak ellenére, hogy a szigetországgal az Amerikai Egyesült Államok külön megfigyelési megállapodást kötött (Five Eyes).

Az amerikai kémkedés ezen listában egyedülálló abból a szempontból, hogy egyértelmű bizonyítékokra épül, ezek egy részének valóságtartalmát az Amerikai Egyesült Államok külön is elismerte. A rendkívüli amerikai és külföldi negatív visszhang hatására 2015-ben az Amerikai Egyesült Államokban életbe lépett a USA Freedom Act, amelyben részben korlátozták az NSA adatgyűjtését (pl.: az amerikai megfigyelés bírói engedélyhez, a külföldi a hírszerzési döntőbíróság, a FISC engedélyéhez kötött, az engedélyt 180 naponta meg kell újítani).

Mindez azonban nem garancia a tömeges és általános megfigyelések végére, lévén az NSA és más szervezetek eddig is végeztek akciókat illegálisan, az amerikai törvényeket megkerülve, a hírszerző szolgálatok pedig értelemszerűen igyekeznek minél jobban kihasználni az adatszerzési lehetőségeket.

Emellett a 2001. szeptember 11-i amerikai pánik időszakában született, ma már nem érvényes Patriot Act záradéka alapján a már megkezdett megfigyelések tetszőleges ideig folytathatóak, továbbá az NSA számára engedélyezték, hogy megtartsa az összes eddig megszerzett adatot és szakértők szerint például a jelenleg is folyamatban lévő PRISM (US–984XN) program minden korábbinál szélesebb körben gyűjt adatokat. (Az utóbbi években további kémműholdakat állítottak pályára).

Szolgáltatás-megtagadásos támadás (Oroszország)

A Szovjetunió összeomlását követően az orosz gazdaság rendkívül nehéz helyzetbe került, miközben a kétes körülmények között privatizált állami vagyon jelentős részét egy szűk csoport, az ún. oligarchák szerezték meg.

Oroszországot az utóbbi két évtizedben Vlagyimir Putyin irányította (elnökként, illetve kormányfőként). Az ultrakonzervatív politikus és körének elsődleges célja az ország (a szovjet, illetve a cári időkbeli) világhatalmi státuszának visszaállítása.

A Szovjetunió összeomlását követően Oroszország elsősorban a kőolaj- és földgázexportra támaszkodott, de a bevételekből nem sikerült hosszú távon stabilizálni a gaz-

daságot, amelyre komoly csapást jelentett az energiahordozók OPEC által diktált árainak összeomlása.

A gazdasági és társadalmi nehézségek ellenére az orosz vezetés gyakran alkalmaz (jelentős költségű) katonai erőket politikai céljainak eléréséhez és erejének demonstrálásához. Ide sorolható az önállóságát kikiáltó Csecsen Köztársaság elleni első csecsen háború (1994–1996), illetve azt ezt követő második csecsen háború (1999–2000), a 2008-as Grúzia elleni dél-oszétiai háború (Haditechnika 2011/5.), illetve a Krím-félsziget 2014-től máig tartó megszállása. Az ilyen katonai akciók (pl.: a szíriai katonai jelenlét) több tekintetben párhuzamba állíthatók a Szovjetunió 1979–1989 közötti afganisztáni háborújával. A stagnáló gazdaságú, szövetséges nagyhatalommal nem rendelkező, amerikai és európai embargó alatt álló Oroszország hatalmas összegeket költ a harcok folytatására, de kérdéses, hogy ezzel sikerül-e elérniük a vélelmezett hatást, illetve képesek-e a harcokhoz szükséges, korábban kifejlesztett új eszközök széles körű rendszeresítésére.

Ezek helyett, illetve mellett, Oroszország jelentős energiát fektet a lényegesen olcsóbb kiberhadviselésbe, amelyet többek között DDoS támadások képében használ ki, ám ennek megértéséhez érdemes néhány szót szólni a DoS támadásokról is. Az interneten keresztül elérhető honlapokat (és közvetve az általuk biztosított szolgáltatásokat) háromféleképpen lehet elérhetetlenné tenni: fizikai támadással (pl.: a szerverterem felrobbantásával), egy célzott támadással, amely lekapcsolja a rendszert, illetve a célpont túlterhelésével. Az első lehetőség rendkívül ritka, akárcsak a második mód. A média (különösen az akciófilmek) sugallta kép ellenére a kibertámadásokat végrehajtó hackerek rendkívül ritkán koncentrálnak arra, hogy lekapcsoljanak egy szervert, hiszen az üzemeltető rövid idő alatt helyreállíthatja a szolgáltatást, ezért a belefektetett idő, energia és pénz nem térülne meg.

A támadók lényegesen kisebb szakértelmet igénylő módja a Denial of Service (DoS), magyarul szolgáltatásmegtagadásos vagy túlterheléses támadás, amelynek lényege, hogy a támadó, valamilyen kiskaput kihasználva, blokkolja a hozzáférést egy weboldalhoz.

Ez többféleképpen megvalósítható. A legegyszerűbb módszer a teljes sávszélesség lefogása, ám ez igen ritka[6], mivel a támadáshoz jelentős erőket kell összevonni, ezért az elkövetők általában valamilyen hibát kihasználva terhelik le a célszervereket olyan mértékben, hogy az üzemeltetett honlaphoz történő hozzáférés rendkívül lassúvá válik, jelentős túlterhelésnél pedig akár össze is omolhat, elérhetetlenné téve a weboldalt.[7]

Egy DoS támadás során a támadó nagyszámú, de egyenként kis méretű csomagot küld a megtámadott szervernek gyakran úgy, hogy egyetlen csomag elküldésével – a hálózat sajátosságait kihasználva – a fogadónak 2-3 csomagot kelljen feldolgoznia. Mindezek ellenére a nagyobb célpontok elleni DoS támadások mára gyakorlatilag eltűntek, mert a komolyabb szerverek feladatspecifikus kialakításuk miatt lényegesen erősebbek egyetlen számítógépnél, így egyszerre akár több DoS támadás mellett is működőképesek maradhatnak.

A támadók ezért a DDoS (Distributed Denial of Service), magyarul: az elosztott szolgáltatás-megtagadással járó akciókat preferálják. Ez a DoS támadásokkal azonos technikákat használ, azonban egy támadásban nem egyetlen gép, hanem akár több száz vagy több ezer gépből álló géppark vesz részt. A DDoS támadások lényege, hogy egy központi számítógép által megadott jelre az összes résztvevő bombázni kezdi a szervert, az általuk küldött adattengert pedig a célpont képtelen feldolgozni.

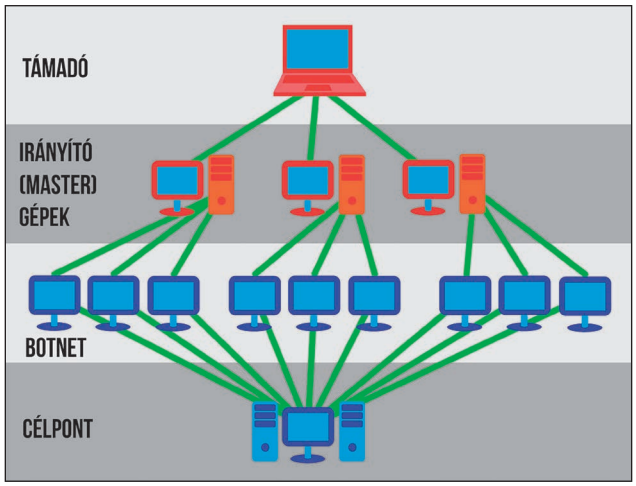
A DDoS további előnye, hogy amíg egyetlen támadó IP címét letiltva a támadás megállítható, nagyszámú támadó esetén több tucat számítógép blokkolása sincs érdemi hatással a támadásra. Természetesen a támadás értelmetlenné válik, ha a szervert lekapcsolják, de a támadóknak éppen az a célja, hogy a szolgáltatás elérhetetlenné váljon. Ugyanezen okból nem tiltható ki minden, a szerverhez kapcsolódni próbáló számítógép, mivel így a felhasználók szintén nem érnék el az adott weboldalt.

A DDoS támadások végrehajtásához a támadónak nincs feltétlenül szüksége hatalmas saját gépparkra. Ha a felhasználó egy kéretlen e-mail fertőzött mellékletét megnyitja, számítógépére települhet egy kis méretű program vagy végrehajtódik egy parancssor, amely közkeletű elnevezéssel „zombivá” teszi az adott gépet (bot). A támadás megkezdésekor, a központi gép jelzésére a zombigép is részt vesz a támadásban (általában a felhasználó tudta nélkül), a támadást így a botokból álló botnet hajtja végre. A felhasználó sok esetben arról sem tud, hogy a számítógépe éppen egy támadásban vesz részt, mindössze annyit érzékel, hogy gépe a megszokottnál lassabb. A támadás során vagy azt követően csak a támadó és master gépeket, illetve az azokat használó személyeket kell elrejteni.

DoS és DDoS eseményre már 2000 előtt is volt példa, az elmúlt években pedig számos célpontot ért szolgáltatásmegtagadással járó támadás, gyakran ismert cégeket támadva, de az elkövetők általában magánszemélyek voltak, akiket a szórakozás, eltérő vallási/politikai nézet vagy a bosszú motivált.

Oroszország különböző módszerekkel már több alkalommal végrehajtott DDoS támadásokat. 2007-ben, miután Észtországban áthelyezték a Tallinnban található szovjet emlékművet, orosz támadók átmenetileg elérhetetlenné tették a kormánypárt és több észt hírcsatorna honlapját. A támadást követően Észtország az Oroszországgal kötött rendőrségi együttműködésre hivatkozva kérte, hogy az orosz fél állítsa bíróság elé az elkövetőket, de miután a támadást orosz szerverekig, illetve orosz kormányzati számítógépekig követték vissza, az orosz legfelsőbb ügyészség az észtek kérését elutasította. A támadás valószínűleg (ha nem is feltétlenül közvetlenül a hadsereg vagy a titkosszolgálat által, de) állami, illetve orosz hálózat-üzemeltetői segítséggel zajlott.

8. ábra. A DDoS elvi működése: az egyetlen támadó master gépeken keresztül irányítja a felhasználók megfertőzött gépeit, amelyek parancsra mind egy-egy DoS támadást hajtanak végre a célpont ellen



A támadás rávilágított a NATO felkészületlenségére, ezért még 2007-ben az észt államfő találkozott George Bush akkori amerikai elnökkel, majd a találkozót követően, 2008-ban a támadásra reagálva létrehozták a NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) szervezetét, jelzésértékű, Tallinni központtal (Magyarország nyolcadikként, 2010-ben csatlakozott a szervezethez).

9. ábra. A CCDCOE logója: a szervezetet ma már több mint egy tucat ország alkotja (túlnyomórészt Európai Uniós tagországok, valamint az Amerikai Egyesült Államok és Törökország), ennek ellenére a CCDCOE jelképében máig szerepel Tallinn

2008-ban, a korábban említett dél-oszétiai háború előtt és alatt Oroszország DDoS támadást mért számos grúz weboldalra is, köztük az államfő honlapjára és több grúz híroldalra. A támadásokra reagálva az amerikai The New York Times napilap szakértőkre hivatkozva jelezte, hogy ez volt a világon az első olyan ismert kibertámadás, amelyet egy fizikai háborúban, a pszichológiai hadviselés részeként alkalmaztak. A támadások csak a tűzszünetet követően haltak el, és a grúz internet egyes részeit csak jóval később sikerült helyreállítani. Oroszországban a háború alatt nyíltan terjesztettek olyan programokat, amelyeket a felhasználók tudatosan telepítve, részt vehetnek a támadásban, növelve azok hatását (ezek hatékonysága nem ismert).

A DDoS támadások elsődleges céljai a bizonytalanság és félelem keltése, erőfitogtatás, illetve a felhasználók boszszantása. Ezen okokból kifolyólag a támadásoknak leginkább kitett oldalak az állami honlapok, a híroldalak és a pénzügyi szolgáltatást nyújtó oldalak (természetesen bármilyen honlap célba vehető, de egy néhány fő által látogatott statikus oldal leállítása erőforrás-pazarlás).

A DDoS támadások más műveletekhez képest rendkívül olcsók, ám hatásuk és hosszabb távú következményük megkérdőjelezhető. A világ legnagyobb honlapjait, köztük a Google-t és a Facebookot gyakorlatilag lehetetlen hatékonyan blokkolni, mert ezen cégek gépparkja kisebb országok együttes kapacitásával vetekszik és gyakran házon belül tervezett, saját programozási nyelven írt programokat használnak (a Google például a Go, a Facebook pedig a Hack programozási nyelvet). A DDoS támadások időtartama általában néhány óra vagy 1-2 nap, nem célja pénz vagy információszerzés, a leállított honlapok felhasználói pedig más oldalakon (pl.: Facebook, Twitter) tájékozódhatnak.

A nagyszámú DDoS támadás miatt mára több módszer született ezek semlegesítésére, de a DoS támadok rendkívül olcsók, az interneten található részletes útmutatók és specializált, ingyenes programok segítségével bárki képes a kivitelezésükre, miközben jól használható a tájékozatlanabb felhasználók befolyásolására, a fenyegetettség érzésének fenntartására. Részben emiatt Oroszország máig folytatja a DDoS támadásokat, 2018 januárjában például dán és holland bankokat, híroldalakat és állami szervezeteket (köztük a dán adóhatóságot) is ért Oroszországból indított elosztott szolgáltatás-megtagadásos támadás.

(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

6 De nem ismeretlen – 2013-ban például ismeretlen tettesek világrekordot felállítva, a kéretlen leveleket küldő szerverekről feketelistát készítő Spamhaus nonprofit szervezet 300 Gbps-os sávszélességét blokkolták, 2016-ban pedig a brit BBC-t érte 602 Gbps sávszélességet lefogó támadás.
7 Túlzottan kis kapacitású rendszereknél a felhasználók rohama is előidézhet ilyen helyzetet, Magyarországon például adóbevallási határidők előtt a NAV, az egyetemi tantárgy-felvételeknél pedig a Neptun rendszer évente több alkalommal is időlegesen elérhetetlenné válik.

(Illusztrációk a szerző gyűjteményéből.)

Tőrös István (szerk.)

A magyar légierő 100 éve

2018-ban jelentette meg a Zrínyi Könyvkiadó Tőrös István kreatív szerkesztésével *„A magyar légierő 100 éve – Years of the Hungarian Air Force"* című angol–magyar kétnyelvű díszalbumát. Száz évvel ezelőtt, 1918-ban a Monarchia egyesített osztrák–magyar haderejének repülőgépére először került fel magyar felségjelzés, innen számítja létrejöttét a magyar légierő. Az évfordulós kiadvány a magyar katonai repülés történetét fogja át, betekintést engedve az olvasó számára abba a zárt világba, amelyben a magyar katonai repülők éltek, dolgoztak és teljesítették feladataikat. A repülők számos lebilincselő repülőtörténetet, anekdotát őriznek a velük megtörtént, illetve általuk átélt eseményekről. Ezeknek egy töredékét villantja fel ez a látványos fotókkal illusztrált, igényes kivitelű kötet. A könyv a Magyar Királyi Honvéd Légierő II. világháború harcaiban megedzett állományának, illetve az 1945 utáni katonai repülés gázturbinás harci repülőgépeket meghonosító repülőkatonáinak egyaránt méltó emléket állít. Érdekes, kevésbé ismert repüléstörténeti esemény az 1956-ban – a Fertő-tó térségében – a szovjetekkel vívott MiG–15-ös vadászgép légiharca (amely végén a repülőgép osztrák területre zuhant!), illetve a magyar légierő 1968-as, Csehszlovákia megszállásával kapcsolatos tevékenységét taglaló fejezet is. Feltűnik a könyv hasábjain a hazai gyártású Messerschmitt Me 109-es és Me 210-es vadászrepülőgép, a gázturbinás hőskort jelképező MiG–15-ös, a hangsebesség feletti repülést idéző deltaszárnyú MiG–21-es, a variaszárnyú MiG–23-as vadászrepülőgép, valamint a kiemelkedő teljesítményű MiG–29-es „nagyvas", amellyel magyar vadászpilóták oly sok trófeát elhoztak a fairfordi műrepülőversenyekről. Megjelenik a napjainkat képviselő JAS–39 Gripen vadászrepülőgép, és szó esik a repülőnapok történetéről, a magyar szállítórepülő-csapatnemről, illetve katonai helikoptereink történetéről, a kabuli légi kiképzés-támogató csoport mentorairól, továbbá a repülőképzés intézményeiről, sőt a tököli repülőgépjavító-üzemről és a repülő-roncskutatásról is. A kötethez Sáfár Albert dandártábornok, a Magyar Honvédség Összhaderőnemi Parancsnokság légierő haderőnem főnöke írt méltó köszöntőt. A hiánypótló alkotás mintegy 900 korabeli fotóval és dokumentumfilm-DVD melléklettel illusztrálva, egy légijárművek-poszterrel és a Légierő Zenekar Veszprém repülőindulókat tartalmazó CD-jével kiegészítve jelent meg.

A 380 oldalas, keménytáblás, színes és fekete-fehér fotókkal illusztrált könyv 10 500 Ft-os áron kapható a könyvesboltokban, illetve közvetlenül a Zrínyi Kiadónál is, 25%-os helyszíni kedvezménnyel.
(Cím: 1087 Budapest, Kerepesi út 29/b, Tel.: 06 1 459 5373, e-mail: gyoredina@armedia.hu).