# HŐSÖK-E A HEKKEREK?

*The New York Review of Books, 2012. szeptember 27.*

MISHA GLENNY:
DARK MARKET
Cyberthieves, Cybercops and You
Knopf, 296 old., $26.95

KEVIN MITNICK:
GHOST IN THE WIRES
My Adventures as the World's Most Wanted Hacker
(társszerző: William L. Simon)
Little, Brown, 413 old., $25.99

PARMY OLSON:
WE ARE ANONYMOUS
Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency
Little, Brown, 498 old., $26.99

DAVID E. SANGER:
CONFRONT AND CONCEAL
Obama's Secret Wars and Surprising Use of American Power
Crown, 476 old., $28.00

Ez év júniusának utolsó napján a *Redmond Pie* nevezetű technológiai internetes lapon gyors egymásutánban jelent meg két cikk, s látszólag semmi közük nem volt egymáshoz. Az első *Root Nexus 7 on Android 4.1 Jelly Bean, Unlock Bootloader, And Flash ClockworkMod Recovery* főcímmel végső soron használati utasítás ahhoz, mit tegyen, aki módosítani akarja Nexus 7-jének a software-jét, hogy belenyúlhasson az operációs rendszerébe. A Nexus 7 a Google vadonatúj táblagépe. Annyira új, hogy még el se jutott a megrendelőkhöz.

A másik főcím valamivel érthetőbb a nem szakmabeli olvasónak: *Itt az új OS X Tibet Malware, amely személyes információkat küld a felhasználóról a távoli szerverhez.* Maga a történet a „trójainak" nevezett komputervírus felfedezéséről szólt, amely először bizonyos tibeti gépeken bukkant fel. E vírus példáján hívta fel a figyelmet a szerző egyrészt arra, hogy immár az Apple komputerek sem bevehetetlenek a rosszindulatú vírusok és férgek számára, másrészt arra, hogy ez a vírus a kínai rezsimmel szembeforduló tibeti aktivistákat vette célba, vagyis nem esetleges, hanem kifejezetten politikai rendeltetése van. Ha egy tibeti aktivista letölti a fertőzött fájlt, akkor az titokban összeköti komputerét egy kínai szerverrel, amely ily módon nyomon követheti az aktivisták tevékenységét, és hozzáférhet a gépeikben megjelenő tartalmakhoz. (A *Redmond Pie* szerzője még azt is megkockáztatta, hogy szerinte azért épp az Apple gépek ellen indult a támadás, mert a dalai láma ezt a márkát kedveli.)

Valójában a Nexus 7 története és a tibeti trójai faló története ugyanarról szólt – a hekkelésről és a hekkerekről, bár a Nexus 7 meghekkelői – mellesleg a *Rootzwiki* nevű honlap szerzői – egészen mást csináltak, mint azok, akik a tibeti aktivistákat vették célba. A hekkelés és a hekker mára már annyira általános és átfogó megjelölés, hogy e szavak szándékolt jelentése most már mindig csak a szövegösszefüggésből hámozható ki. Mindazonáltal az utóbbi néhány évben mindinkább a hekkelés romboló oldalára esett a hangsúly – a brit telefonhekkelési botrány, az Anonymous és a LulzSec fellépése, illetve a Stuxnet óta, amelyben az amerikaiak és az izraeliek, az iráni atomprogram megvalósítását késleltetve, egy komputervírus segítségével tették tönkre az iráni gyorsítókat, de saját magunk is számtalan esetben voltunk tanúi a mások azonosságával való visszaélésnek.

Éppen ezért, amikor ez év februárjában Mark Zuckerberg, a Facebook vezérigazgatója, mielőtt a tőzsdére vitte volna a céget, levélben fordult a potenciális részvényesekhez, és azt írta, hogy a Facebook a „hekkervilág" filozófiájának híve, nem provokálni akarta őket, csak próbálta megteremteni a negatív közfelfogás ellensúlyát. (Egyben felidézte Steven Levy, a veterán technikai tudósító szavait is, aki elsőként tett komoly erőfeszítést *Hackers: Heroes of the Computer Revolution [A hekkerek – a komputerforradalom hősei]* címmel 1984-ben kiadott könyvében arra, hogy megértse azt a szubkultúrát, amelyből Steve Jobs, Steve Wozniak és Bill Gates érkezett.)

Zuckerberg azt írta, hogy „a hekkelés valójában valaminek a gyors megépítését jelenti, vagy pedig a cselekvési mozgástér határainak kitapogatását. Mint annyi mindent, ezt is lehet jó és rossz célra használni, de az általam ismert hekkerek zöme rendszerint idealista, aki valamilyen kedvező hatást kíván elérni a világban. […] A hekkerek meggyőződése, hogy minden lehet egy kicsit jobb is, és hogy soha semmi sem tökéletes. Egyszerűen javítani kell rajtuk – szembeszállva mindazokkal, akik szerint a dolog lehetetlen, vagy pedig kénytelenek beérni az adott állapottal."

Noha a „javítás" szó semlegesen cseng, valójában nagyon sokféle értelmezést enged meg. Vajon az új Google Nexus 7 már tönkrement, mielőtt becsomagolták és postázták volna? A Google szerint egyáltalán nem, és a megrendelők túlnyomó többsége szerint sem, ám azok, akik szemügyre vették a műszaki adatait, nyomban hibásnak minősítették, mert észrevették, hogy viszonylag kicsi a beépített memóriája. Ezért akarták úgy átalakítani a gépet, hogy külső adathordozót lehessen csatlakoztatni hozzá, ami hatalmasan megnövelné a memóriakapacitását. S ugyanez történt az eredeti iPhone-nal is: kiválóan működött, de nem azok szemében, akik esetleg nem az Apple-től származó vagy általa jóváhagyott programokat akartak rá feltölteni, akik nem fogadták el, hogy csak egy bizonyos szolgáltatóhoz (nevezetesen az AT&T-hez) kapcsolódhatnak, vagy egyszerűen szeretnek barkácsolni, és úgy gondolják, hogy erre mint tulajdonosoknak minden joguk megvan. A hekkerek megtalálták a módját, hogy megkerüljék ezeket a korlátozásokat – ezt nevezték „börtönkitörésnek", avagy Zuckerberg szavaival: a gépek „feljavításának".[1]

Az Apple azonban más álláspontot képviselt, és úgy érvelt az USA Szerzői Jogi Hivatalában, hogy az iPhone operációs rendszerének módosítása szerzői jogot sért, s mint ilyen törvénytelen. 2010-es döntésében a Szerzői Jogi Hivatal viszont leszögezte: „Semmi sem indokolja, hogy a szerzői jogi törvény segítsen az Apple-nek meg-

1 ■ Vannak olyan, a Google által az Androiddal együtt forgalmazott, a tulajdonoshoz rendelt alkalmazások, például a Gmail, amelyekbe nem lehet belenyúlni.

védeni korlátozó üzleti gyakorlatát." A szerzői jog azonban országonként más és más, és csak idén már három embert tartóztattak le Japánban a tisztességtelen verseny megakadályozására szolgáló, nemrégiben korszerűsített törvény alapján azért, mert a Nintendo játék konzoljait módosították – azaz meghekkelték. Viszont a Nexus 7 meghekkelőinek semmi okuk az aggodalomra: a Google Androidja „nyitott forráskódú", azaz a közönség rendelkezésére áll, mely – egy bizonyos mértékig – szabadon babrálhat rajta.

A döntő mozzanat Mark Zuckerberg hekker-himnuszában, amiért is kapott az alkalmon, hogy ezt a leendő részvényeseknek is tudtára adja, az, hogy a hekkelés valóban javíthatja, s gyakran fel is javítja a termékeket: feltárja a sebezhető pontokat, újításokat javasol, jelzi azt is, mit lehet, és azt is, mit kívánnak a vevők. Zuckerberg nem titkolta, hogy van a hekkelésnek sötét oldala is, amely – különösen a köztudatban – homályba borítja a játékos, szórakoztató, kreatív oldalát, és egyáltalán nem indokolatlanul. A hekkelés ugyanis egy bizonyos lopási mód kedvelt eszköze lett, azoké a tolvajoké, akik leemelik a pénzt az ember számlájáról, és a személyes adataival – mindenekelőtt a hitelkártyáival és a jelszavaival – kereskednek az internet virágzó nemzetközi alvilágában. Továbbá zsarolásra, nyilvános megszégyenítésre, üzleti megkárosításra, szellemi tulajdon elbirtoklására, kémkedésre s akár még háborúra is bevált a hekkelés módszere.

Az FBI nemrégiben két ügyet is felgöngyölített, amelyek jól szemléltetik, hogyan hekkelték meg lényegében a hekkelést rossz célokra. Az első a Szellemkattintás *(Ghost Click)* művelet volt tavaly novemberben, amely hat észt nemzetiségű személy letartóztatásához vezetett, akik mintegy száz országban több mint 4 millió komputert fertőztek meg egy olyan vírussal, amely lehetővé tette, hogy 14 millió dollárt keressenek tiltott internetes reklámból szerzett bevételekkel. A vírust olyan programnak álcázták, amellyel online videókat lehet nézni. Aki egyszer letöltötte, akaratlanul is a hekkerek által kézben tartott lapokra irányította fertőzött komputere keresőgépét. Amikor az FBI lecsapott a hekkerek szervereire, szándékolatlanul is óriási kárt okozott: számítógépek tízezreiről nem lehetett hozzáférni az internethez, ha gyanútlan tulajdonosaik már korábban nem „fertőtlenítették" őket.

A másik a Kártyabolt *(Card Shop)* művelet, egy beépített FBI-ügynök segítségével megvalósított lebuktatás volt, amely 4 földrész 8 országában összesen 24 személyt csalt csapdába, akik hitelkártyák ellopott adataival kereskedtek a „kártyás", azaz egy, csak meghívottaknak hozzáférhető, privát internetes portálon, amelyet valójában az FBI működtetett. A felhasználók lopott hitelkártyaszámokkal és egyéb személyes adatokkal kereskedhettek, kicserélhették ötleteiket arról, hogyan lehet megszerezni és felhasználni ilyen adatokat. Az FBI becslése szerint ez a 24 letartóztatás nagyjából 400 000 potenciális áldozatnak mintegy 205 millió dollárját mentette meg. (Az FBI a lopott adatokat visszajuttatta a bankoknak, s úgy tűnik, ezzel elkerülhető lett a kár.)

A Kártyabolt-műveletben letartóztatott tizenegy amerikai jellemrajzával zárul a *Dark Market (Sötét piac),* Misha Glenny felkavaró ábrázolása a bűnöző hekkerekről – pontosabban feltörőknek nevezhetjük őket –, akik egy korábbi kártyás ügyben vettek részt, amely ugyancsak egy személyes adatokkal kereskedő internetes portál körül szerveződött. A Kártyabolt-műveletben érintett hekkerek – akárcsak Glenny könyvének szereplői – fiatal férfiak voltak, még egyikük sem töltötte be a 25 évet. Michael Hogue például, egy 21 éves fiú az arizonai Tucsonból, olyan „csaló programot" árult, amellyel a felhasználó megfertőzhette – a legkülönbözőbb módszerekkel, kelepceként működő hivatkozásokkal, levelekkel és programokkal –, majd távirányítással szabályozhatta a „foglyul ejtett" komputert. Például bekapcsolta a webkamerát, és megleste az áldozatot, rögzítette a billentyűk minden egyes leütését, amivel aztán könnyen ellophatta az áldozat jelszavait, és hozzáférhetett a számláihoz.

S aztán ott volt a 19 éves Christian Cangeopol a georgiai Lawrencevilleből, az „áruházas", aki az interneten lopott hitelkártyákkal drága elektronikus berendezéseket vásárolt valamelyik boltban (innen az „áruházas" ragadványnév), amelyeket azután készpénzért adott tovább. Ha ezek a fiatalemberek a bűnöző alvilág kishalainak tűnnek, csak azon mód miatt, amellyel az FBI elfogta őket: kivetett egy hálót, aztán nézte, ki úszik bele. Ám tipikus esetben a nagy internetes bűnözés bűnszövetkezetek műve, amelyek közül sok a volt Szovjetunióból – már ha egyáltalán valahonnan – „kiindulva" működik.

Körülbelül ugyanakkor, amikor az FBI beszámolt a Kártyabolt-műveletről, két biztonsági cég, a McAfee és a Guardian Analytics fehér könyvet adott ki egy trükkös hekkelő rendszer dokumentumaival, amely a hálózaton át elérhető, nagy összegű céges és egyéni bankszámlákat vette célba. A hekkerek megszerezték a jelszavakat és a banki adatokat, amelyek segítségével azután a saját számláikra utaltak át nagy összegeket. Ez a Nagy hengerként emlegetett lopássorozat Olaszországból indult el, végigment Európán, majd átugrott Latin-Amerikába, onnan az Egyesült Államokba – valahogyan úgy, ahogy a csapatokat buzdító szurkolók kiabálása hullámzik végig a stadion lelátóján.

Igen figyelemre méltó, hogy ezt az egész műveletet Oroszországból irányította és hangolta össze 60 nagy teljesítményű komputer. A hekkelő rendszer, ha egyszer már beüzemelték, önműködővé vált. „Nincs szükség emberi beavatkozásra, minden támadás gyors és gördülékeny – állapították meg a fehér könyv szerzői. – Ezt a műveletet, amely a banki ügyletek rendszerének beható szakmai ismeretét párosítja az egyedi megoldású vagy tucatáruként hozzáférhető kártevő kóddal, joggal lehet »szervezett bűnözésnek« nevezni." Becslésük szerint a lopások mögött tucatnyi bűnszövetkezet állt, az okozott kár összértéke pedig 78 millió dollár volt. S ha a művelet teljes sikerrel jár, a kár elérhette volna a 2 milliárd eurót is.

Kétmilliárd euró vagy 2,5 milliárd USA-dollár sok pénz, de 78 millió dollár sem csekélység. E számok közzétételével a McAfee és a Guardian Analytics ugyanúgy a nagyközönséggel próbálta megértetni, mekkora ve-

szélyt jelentenek az internetes bűnözők, mint az FBI, amikor beszámolt arról, hogy mintegy 205 millió dollár veszteséget jelentett volna a Kártyabolt-művelet, ha a bűnözők kezében lett volna. Csakhogy mindhárman spekulatív számokat közöltek, becslést arról, ami megtörténhetett volna, de nem történt meg.

A vírusirtó programokat előállító Norton software-cég is megjelentette 2011. évi *Jelentését a számítógépes bűnözésről (Cybercrime Report),* és az internetalapú globális bűnözés felmérése alapján azt a becslést adta, hogy a károsultak évente 114 milliárd dollár veszteséget szenvednek. Erre ráharapott a sajtó is, és rögtön felállította az egyenlőséget: pénzügyi tekintetben az internetes bűnözés ma már semmiben sem marad el a globális drogkereskedelemtől. Íme, az internetkorszak újabb, döbbenetes ténye, amely kétségkívül sokakat arra késztetett, hogy jelszóval védjék komputerüket, és vírusirtó programokat töltsenek le. Talán épp ez volt a cél, hiszen ebben a játékban a vírusirtó programok gyártói és az internetbiztonsági cégek is érdekeltek. A kiberbűnözés kiterjedésével párhuzamosan a vállalatok kiberbiztonsági kiadásai egyre nőttek. Egyes becslések szerint 2006. óta évi 10 százalékkal, s ma már ez az összeg évi 80 milliárd felett jár.

E csillagászati számokra adható még egy magyarázat: nem is igaz, hogy ennyibe kerül a számítógépes bűnözés. A Norton jelentése például egy olyan felmérésre támaszkodik, amelyben 12 704 felnőttet, 4553 gyermeket és 2379 tanárt kérdeztek meg 2011. február–márciusában. Az ő válaszaikat extrapolálva jutott el a Norton a 114 milliárd dolláros becsléshez, amelyet még azzal a kijelentéssel is megtoldott, hogy a kérdéses évben 431 millió embert károsított meg az internetes bűnözés. Csakhogy a Microsoft két kutatója, Dinei Florencio és Cormac Herley bebizonyította, hogy a Norton az exit-poll közvéleménykutatásban alkalmazott statisztikai elemzéssel állította elő ezeket a számokat. Míg ott a minta egyszerű felszorzásával lehet állításokat tenni a populáció egészéről, ez a módszer itt nem használható, tekintve, hogy a szavazói döntésekkel és a pénzbeli veszteségekkel nem lehet ugyanúgy számolni. „Tegyük fel, hogy megkérünk 5000 embert, mondják meg, mennyivel károsították meg őket a számítógépes bűnözők, majd ezt az adatot extrapoláljuk a 200 milliós lakosságra – írta Florencio és Herley tavaly tavasszal a *New York Times*ban. – Azaz minden állítólag elvesztett dollárt megszorzunk 40 000-rel. Ha csak egy ember is hamisan állítja, hogy 25 000 dollárt veszített, az már 1 milliárddal torzítja felfelé a becslésünket. S mivel senki sem számolhat be negatív veszteségekről, a hiba nem oltódik ki."

A számokat nemcsak a túlbecslés torzítja, hanem az elhallgatás is. Ma már igazolható, hogy a nagyvállalatok és egyéb intézmények nem szívesen vallják be ilyen típusú veszteségeiket és biztonsági rendszerük feltörését abbeli félelmükben, hogy ezzel elidegenítik a vevőiket, részvényeik ára zuhanni kezd, és az érintettek kártérítési pert kezdenek ellenük. A hekkerek az elmúlt négy évben háromszor is betörtek a Wyndham szállodalánc számítógépes rendszerébe, és több százezer hitelkártyaszámot szereztek meg, a cég mégsem ismerte el ezt a lopást a részvényeseknek írott éves beszámolójában. Ugyanígy tett az Amazon is, amely elmulasztott beszámolni arról, hogy rengeteg vásárló adatait lopták el két ruházati részlegétől (az egyik a *Zappos,* a másik a *6pm* volt). Feledékenységét a Tőzsde- és Értékpapírfelügyelet *(Securities and Exchange Commission)* is kifogásolta, amely szeretné, ha a cégek maguktól közölnék az efféle információkat. (A bizottság annál többet nem tehet, mint hogy kifejezi reményeit – szabályozó jogköre e téren nincs.)

A nagyvállalatok vonakodása ellenére, vagy esetleg épp amiatt, a bíróságok is bekapcsolódtak. Miután egy orosz bűnszövetkezet idén tavasszal mintegy hat és fél millió jelszót szedett le a LinkedIn közösségi média lapjáról, a károsultak egyike pertársaságot szervezett, azzal vádolva a Linekdlnt, hogy nemcsak nem védte megfelelően a személyes információkat, de értesíteni is tudatosan elmulasztotta azokat, akiknek az adatait a támadás érintette. Az ellopott jelszavakkal hozzá lehetett férni a felhasználók személyes adataihoz – a telefonszámukhoz, címükhöz, szakmai előmenetelük történetéhez –, sőt gyakran egyéb elektronikus számláikhoz is – e-mailjükhöz, bankszámlájukhoz –, mivel nagyon sokan az összes internetes tevékenységükhöz ugyanazt a jelszót használják. Időközben a Szövetségi Kereskedelmi Felügyelet *(Federal Trade Commission)* beperelte a Wyndham World Wide céget, az állítva, hogy az nem védte meg a vendégeit. Arra kérte az Egyesült Államok illetékes bíróságát, „utasítsa a Wyndham céget, hogy információbiztonsági gyakorlatában hagyjon fel a vendégek megtévesztésével, és kötelezze arra, hogy térítse meg a vendégek pénzbeli kárát".

S nemcsak bevett gyakorlattá kezd válni, hogy a cégek eltitkolják az internetes támadásokat, hanem ráadásul olyan sok és alattomos támadásra kerül sor, hogy a vállalatok és egyéb szervezetek gyakran nem is tudják, hogy a rendszerüket kikezdték. Az egyik internetes technológiai cégnek, a Juniper Networksnek a *Homeland Security News Wire* című kiadványban közzétett tanulmánya szerint „tavaly a cégek 90 százalékának sértették meg a biztonsági rendszerét". S amikor a Mandiant nevű amerikai számítógép-biztonsági cég biztonsági főnöke, Richard Bejtlich érdeklődött a cég ügyfeleinél, akkor kiderült, 94 százalékuk nem is tudott arról, hogy vállalkozásának számítógépes rendszerébe betörtek – méghozzá ez esetben, úgy tűnik, kínai hekkerek, akik üzleti titkok s egyéb olyan információk után kutattak, amelyek számukra üzleti előnyökkel járhatnak. „Sok esetben az ellenfél annyira ügyes – nyilatkozta Shawn Henry az FBI-tól a *Wall Street Journal*nek –, hogy lazán átugorja a kerítést, és még a riasztó sem szólal meg."

Bejtlichet és cégét a hekkervilág a „fehérkalaposok", avagy „etikus hekkerek" közé sorolja, mivel a hekkelés eszközeit arra használják, hogy a számítógépes rendszerekbe behatolva észrevegyék és – ideális esetben – be is foltozzák a biztonsági lyukakat. A fehérkalapos jófiúknak annyira fontos, hogy össze ne tévesszék őket a feketekalapos rosszfiúkkal, hogy az elektronikus kereskedelmi tanácsadók nemzetközi tanácsa már tanfolyamot is szervezett, ahol etikai

igazolást kaphatnak. Ez részben azért is fontos, mert sok fehérkalapos feketekalaposként kezdte, majd követték Kevin Mitnick példáját, akit egy nemzedékkel korábban a világ leghírhedtebb feketekalapos hekkereként, az FBI átkaként emlegettek, és öt év börtönbüntetésre ítéltek, mert betört telekommunikációs cégek, kormányhivatalok (valószínűleg köztük volt a National Security Agency is) és tudományos intézmények rendszerébe. Mitnick ma a saját fehérkalapos számítógép-biztonsági cégét irányítja, s most komoly pénzekért végzi ugyanazt, amit egykor szórakozásból, egy csíkos kezeslábas városmányosaként csinált.

Mitnick most megjelentette emlékiratait *Ghost in the Wires (Szellem a vezetékekben)* címmel, melynek lélegzetelállító kezdőlapjain megtudjuk, hogyan tört be *Mission Impossible* stílusban egy nagyvállalat számítógépes hálózatába. Először hamis igazolvánnyal bejut a vállalat székházába, aztán egyik segítője a plafonon átmászva beengedi a hálózati adminisztrátor irodájába, akinek a számítógépét feltöri. Jó időbe telik, míg tudatja olvasóival, hogy ezek az adrenalinpumpáló mulatságok halálkomoly dolgok. Ám hiába bizonygatja, ezzel nem igazán sikerül eloszlatni a közvéleményben élő képet, hogy minden hekker egyforma.

Hogy miért olyan nehéz megkülönböztetni, mondjuk, az Anonymous hekkereit a kínai hadseregéitől, s mindkét csoportot egy 19 éves georgiai kamasztól, annak egyik oka, hogy a hekkereknek ez így jó. Jelmondatuk – akárcsak a természetvédő túrázóké: „ne hagyj nyomokat". A saját gépük és a célgépek között közvetítő proxyszerverek mögé bújva dolgoznak, elrejtve saját gépük azonosítóit, úgyhogy szinte lehetetlen megállapítani, a világ mely pontján találhatók. Külön hálózati személyiséget alakítanak ki, amely rendszerint inkább a vágyott, semmint a valóságos személyiségre emlékeztet, és becsapós ragadványnéven jelentkeznek be. (Az Anonymous nevű hekkercsoport egyik igen aktív tagja Kayla nevű amerikai tinilányként azonosította magát, pedig valójában egy húszas éveiben járó brit férfi volt, aki előzőleg négy évet szolgált le a hadseregben.) Mint Parmy Olson is megjegyzi kimerítő, fekete humorú krónikájában, amelynek a *We Are Anonymous (Névtelenek vagyunk)* címet adta, „felbukkanhatnak ugyan személyiségek, de az embereknek még sincs igazi, való világbeli azonossága".

A könyvéhez végzett kutatásai során Misha Glenny is azt tapasztalta, hogy „lehetetlen teljes képet kapni arról, mi zajlik a játékosok között, s végül is ki kivel dolgozik együtt". Ez nemcsak a magafajta kívülállóknak okoz fejtörést. Olson szerint még az Anonymousban dolgozó Anonok sem tudták, kivel működnek együtt. A bizalom esetleges és múlékony: amikor a Sabu néven futó hekker az Anonymous csoportban elkezdett személyes információkat közölni magáról, feltárva, mi a valódi neve és lakhelye, Topiary nevű kollégája rögtön gyanút fogott. Feje tetejére állított logika, mégis telitalálat. Amikor az FBI márciusban bejelentette, hogy elfogta Sabut, azt is közölte róla, hogy nyolc hónapon át volt az FBI informátora, aki kiadta munkatársait.

Parmy Olson azt is elbeszéli, hogy Sabu – valójában Hector Monsegur a New York-i Jacob Riis lakótelepről (Lower East Side) – annyira azonosult kettős szerepével, hogy szövetségi ügynökként mutatkozott be egy rendőrnek, amivel csak súlyosbította börtönbüntetését. Miközben információkkal látta el az FBI-t, továbbra is együttműködött a többi Anonnal olyan támadások kitervelésében, amelyek lehetővé tették, hogy a „barátairól" az FBI elegendő terhelő bizonyítékot gyűjtsön. Az Anonymous az FBI éber figyelmétől kísérve hekkelhetett tovább, a leghírhedtebb támadását a Strategic Forecasting (Stratfor) nevű „globális hírszerző" cég ellen indította, amely Olson szerint „egy austini székhelyű hírszerző vállalkozás volt, hírlevele árából élt, amelyet kiküldött előfizetőinek, köztük a Belbiztonsági Minisztériumnak *(Department of Homeland Security*) is". Az FBI nyugodtan végignézte, hogyan szerez meg az Anonymous 60 000 hitelkártyaszámot a jelszavával együtt, hogy azután közel egymillió dollárt adományozzon a Vöröskeresztnek, a Gyermekmentő Szolgálatnak és egyéb jótékonysági szervezeteknek. Megszerezték továbbá a Stratfor ötmillió tételből álló elektronikus levelezését, amelyet viszont a WikiLeaksnek „adományoztak".

A Stratfor-e-mailek között voltak például olyan, a Stratfor munkatársaitól származó kijelentések, amelyek szerint a kormány megfigyeltet amerikai állampolgárokat, a nagyvállalatok pedig szakszervezeti vezetőket és egyéb aktivistákat. Arra is célozgattak, hogy az Egyesült Államok titkos vádemelést készít elő a WikiLeaks alapítója, Julian Assange ellen. Ezek után nem alaptalanul vetődik fel a kérdés: kik voltak itt a fehérkalapos és kik a feketekalapos hekkerek?

Az Anonymous és a belőle szétágazó csoportok különböző akciói közül megemlíthetjük, hogy kétszer is blokkolták a Sony honlapjait (először bosszúból azért, mert a Sony beperelt egy fiatal hekkert, aki feltörte a Sony PlayStation játékkonzol „börtönét"; másodszor pedig azért, mert a Sony támogatta az akkoriban a kongresszusnak benyújtott törvényjavaslatot az internetes kalózkodás ellen *(Stop Online Privacy Act),*[2] egy rövid időre kiiktatták mind a MasterCard, mind a PayPal internetes működését, miután azok blokkolták a WikiLeaksnek és Julian Assange-nek címzett adományokat,[3] és a Szcientológia honlapját is kiiktatták, így próbálva meg kiűzését az internetről. A vezérelv, amely összeköti, ha egyáltalán, ezeket az akciókat, az, hogy „az információ szabadságot érdemel". Nem annyira információszabadságról van itt szó, mint inkább az információ kiszabadításáról azokból a szervezetekből, amelyek rendelkeznek vele.

Nemcsak botorság volna, ha megpróbálnánk valamilyen összefüggő politikai elgondolást tulajdonítani egy csomó embernek, akik konokul viszszautasítanak mindenféle koheren-

2 ■ Tudni kell azonban, hogy George Hotz, az a fiatal hekker, akire hivatkoztak, elutasította a nevében végrehajtott támadást. David Kushnernek, a *New Yorker* riporterének így nyilatkozott (2012. május 7.): „Én épp az ellentéte vagyok az Anonymousnak. Én George Hotz vagyok. Minden, amit teszek, nyílt és törvényes."

3 ■ Amire a csoport a twitteren a MasterCard reklámhadjáratát visszhangozva válaszolt: „A kifejezés szabadsága felbecsülhetetlen érték. Minden másra ott a MasterCard."

ciát pusztán azzal, hogy egy olyan szervezethez kötődnek, amely nem is létezik, hiszen nincsenek tagjai, nem lehet csatlakozni hozzá, hanem szem előtt tévesztenénk azt a nihilista áramlatot is, amely áthatja az Anonymoust, amely elsődlegesen – legalábbis a kezdetekben – röhögés *('lulz'),* vagyis szórakozás, játékok és nevetés – mindegy, kinek a rovására. (Innen ered az Anonymous egyik fő leágazásának, a LulzSecnek a neve: a Laugh Out Loud – hangosan nevess – internetes rövidítésből.) Miért hívják egymást buzinak és niggernek? Miért kényszerítenek embereket szexuális aktusra a webkamera előtt, azzal fenyegetve őket, hogy máskülönben leleplező információkat tesznek közzé róluk, vagy pedig „kiderítik, valójában kicsodák, fenyegetéseket küldenek nekik a Facebookon, vagy megkeresik a családtagjaikat és őket is zaklatni fogják"? Hogy miért? Mert szerintük jó vicc másokat megdöbbenteni és megalázni.

Ugyanakkor viszont közülük kerültek ki azok is, aki „kiszabadították" a Stratfor elektronikus leveleit, akik feltörték egy korrupt, a kormányzatnak dolgozó építkezési beruházónak, H. B. Garynek az internetes fiókjait, és a nyilvánosság elé tárták, hogy ez a cég és még jó néhány a WikiLeaks megtámadásának és lejáratásának tervével jelentkezett a Bank of Americánál. (A *Forbes Magazine* online kiadásában megjelent riport szerint a cégek által javasolt módszerek között szerepelt „a hamis iratok használata, az adományozók megfenyegetése, sőt a WikiLeaks egyik támogatójának megzsarolása" is.) Az Anonymous egyik tagja írta azt a programot is, amely lehetővé tette, hogy a tunéziaiak a kormány ellenőrzését megkerülve használhassák az internetet – az az aprócska parancssor akaratlanul is az arab tavasz egyik katalizátora lett.

Viszont a jó hecc szellemében lopta el az Anonymous nagyjából ugyanebben az időben ártatlan emberek személyes adatait, akik a Fox TV *X Faktor* műsorába szerettek volna bekerülni, és meghallgatásra jelentkeztek; elfoglalta a PBS közszolgálati televízió honlapját, mert nem tetszett az Assangeról sugárzott dokumentumfilm – ennyit az információk szabad áramlásáról. Az utóbbi támadás során feltettek egy kitalált hírt is a PBS híroldalára, amely arról tudósított, hogy Tupac Shakur, a rapsztár valójában él, méghozzá Új-Zélandon; a cég honlapja helyébe pedig egy karikatúrát tettek, amelyen egy dagadt ember eszik egy óriási hamburgert „LOL SZIASZTOK GYEREKEKET ESZEM."

Ha mindez eléggé durvának és gyerekesnek hat, akkor talán azért, mert mint kiderült, az Anonymous sok tagja épphogy csak kinőtt a gyermekkorból. Jake Davis (Topiary) 18 éves volt, amikor letartóztatták; T-flow, aki a tunéziaiaknak a programot írta, mindössze 16. A 28 éves Hector Monsegur majdnem egy nemzedékkel öregebb volt náluk. Amikor kiderült, hogy részt vett a csoportban, a sajtó rögtön a vezetőjévé kiáltotta ki, ami igaz is volt, meg nem is. Noha az Anonymous szándékosan strukturálatlanul és hierarchikus viszonyok nélkül működik, és azt vallja, hogy kizárólag a „kaptármentalitás" parancsait követi, jól tudjuk, hogy egy igazi kaptár, amelyből mézet is nyerünk, valójában egy felvilágosult uralkodó, a méhkirálynő irányítása alatt áll. Ennél cseppfolyósabb a vezetés az Anonymousnál: hol az egyik, hol a másik Anon javasol egy-egy akciót, s a többiek vagy csatlakoznak, vagy sem; mindenesetre Monsegur részvétele idején úgy tűnt, ő az, aki politikusabb irányba terelgeti a többieket.

Megvan az előnye annak is, ha nincs tényleges vezető, formális struktúra és előre kijelölt munkaterv. Amikor az FBI és a többi rendészeti szerv a világ minden táján összefogott, s letartóztatta Monsegurt és még 24 Anont, kivonva őket az internetes forgalomból, az Anonymous nem veszett oda. Továbbra is működik, hol a saját nevén, hol újabb neveken (pl. LulzSecReborn, MalSec, SpexSec). A nevek felcserélhetők, mint ahogy az Anonymous nevet is bárki, bárhol felveheti, és szabadon dolgozhat ebben az álarcban. A LulzSecReborn egyik meg nem nevezett tagja állítólag azt mondta egy ugyancsak névtelenségbe burkolódzó újságírónak abban a beszélgetésben, amelyet a Softpedia nevű román honlap tett közzé, hogy a LulzSecReborn „ott folytatja, ahol a régi LulzSec abbahagyta, katonai és kormányzati honlapokat tör fel, és közzéteszi érzékeny információk sokaságát tartalmazó adatbázisaikat". Mint mondják: „Névtelenek vagyunk. Sokan vagyunk. Nem felejtünk. Nem bocsátunk meg. Ezzel számoljanak." És állják is a szavukat.

Amikor e csoportokról (Anonymous, LulzSec, AntiSec, MalSec, DarkMarket, Operation Card Shop, Operation High Roller) olvasunk, továbbá arról, hogy nemrégiben kínai hekkerek betörtek az indiai tengerészet központi adattárába, muzulmán Anonok ellopták és közzétették izraeli állampolgároknak a személyi igazolványukban található adatait, indiai hekkerek eltorzították Pakisztán két hivatalos kormányzati honlapját, megemlékezésül az 1981-ben, Mumbaiban bombáktól elpusztított honfitársaikra, a WikiLeaks a Stratfor-támadásból származó – Szíriával kapcsolatos – dokumentumok millióit tette közzé és így tovább – nos, akkor a Stuxnet vírus jut az ember eszébe. A Stuxnet megszületését és sorsát – a szigorúan titkos ötlettől izraeli és amerikai programozók szigorúan titkos közös művének szigorúan titkos bejuttatásáig egy iráni urándúsító üzem rendszerébe, majd ugyancsak közfigyelmet kiváltó kirajzásáig a számítógépekbe világszerte – David Sanger pontról pontra feltárta mind a *New York Times*nak küldött tudósításaiban, mind pedig kiváló új könyvében (*Confront and Conceal (Szembetámad és elrejt).* A Stuxnet egy hadüzenet nélküli háborúban bevetett fegyver, s ez a háború annyira titkos, hogy Sanger szerint jó ideig még azok sem tudták, akiket a fegyver eltalált, mi érte őket, ha egyáltalán. Most már nem titkos, felépítését és kódolását mindenki megnézheti. A Stuxnettel talán egy újabb szintre léphet a hekkelés.

A hekkelés a korai formákban még a gép átalakítását, aztán a gépet vezérlő program átalakítását jelentette, azaz a hekkelés még lényegében egy zárt univerzumban zajlott. Viszont amint kilépett az internetre, egész életünk egyik eleme lett – legalábbis életünk interneten bonyolódó részének, ide tartozik a munka, a személyes levelezés, a bankolás, a vásárlás és még sok minden egyéb. Függetlenül attól, ténylegesen hány embert érint

az internetes bűnözés, valamennyien sebezhetők lettünk, teljesen mindegy, hány különös jellel, számmal és gügye kifejezéssel bővítjük a jelszavainkat. De nem csak külön-külön vagyunk veszélyben: csak tavaly mintegy kétszáz (megkísérelt vagy sikeres) támadás érte a társadalmunkat fenntartó alapvető infrastruktúrát – víztisztító berendezéseket, az elektromos hálózatot, olaj- és gázfinomítókat, villamos erőműveket és szállító rendszereket.

Ám mindez eltörpül a Stuxnet – és az általa még előállítható vagy általa ösztönzött további vírusok – exponenciálisan növekvő ereje mellett.[4] Ralph Langner, az a német biztonsági szakember, aki elsőként törte fel a Stuxnet kódját, azt írta a *New York Times*ban, hogy a Stuxnetben az az igazi veszély, hogy egy olyan olcsó fegyverré alakul át, amelyhez egyaránt folyamodhatnak a szervezett bűnözők, a bandita nemzetek, a terroristák és a ráérő hekkelő gyerekek, egyáltalán bárki, aki „helyére tenné" a világot. „Sokkal könnyebb internetes támadást intézni az Egyesült Államok bármelyik erőműve – köztük az atomerőművek – ellen, mint bármelyik szigorúan őrzött iráni üzem ellen – írta Langner. Ha a támadónak nem fontos, hogy bonyolultan álcázott, hosszú távú hadjáratot folytasson (s melyik gazember játékosnak volna az?), akkor a Stuxnethez képest csak icipici erőfeszítést kell tennie."

S bár a Szenátus mindezzel tisztában van, és az USA Cyber Command főnöke, Keith Alexander tábornok is figyelmeztette, hogy „csak idő kérdése", mikor éri fizikai kár egy internetes támadásban valamelyik kulcsfontosságú, létszükségleti rendszert, idén augusztusban – az USA Kereskedelmi Kamarája és egyéb üzleti érdekcsoportok nyomására – mégis elvetette azt az internetbiztonsági törvényjavaslatot, amely az infrastruktúra védelmének megerősítését célozta. (Ezen infrastrukturális berendezések jelentős részét olyan nagyvállalatok működtetik, amelyek nem jelentik a támadásokat, nem költenek a rendszer megjavítására, és nem járulnak hozzá autonómiájuk semmiféle kormányzati korlátozásához.)

Így azután, lesz, ami lesz, ballagunk tovább a Hekkerek Útján.

***Wessely Anna fordítása***

4 ■ Egy moszkvai székhelyű biztonsági cég, a Kaspersky Lab három másik vírust is talált, amelyet a Közel-Keleten alkalmaztak, s ezek „államilag támogatottnak" mutatkoztak.