Kovács László

Kiberháború? Internetes támadások a Wikileaks ellen és mellett

A jelen írás nyomdába adásakor a Wikileaks portál csupán 2890-et dokumentumot tett közzé abból a több mint 251 ezer diplomáciai iratból, melyek kiszivárogtatását 2010. november 28-án kezdte meg a Julian Assange nevével fémjelzett társaság. Az eddig közzétett iratmennyiség – az összes dokumentum alig több mint egy százaléka – nem teszi lehetővé, hogy messzemenő és megalapozott következtetéseket vonjunk le az „évszázad kiszivárogtatásának" nevezett akció tényleges nemzetközi hatásairól. Éppen ezért – jóllehet a Nemzet és Biztonság vissza kíván majd térni a kiszivárogtatás hatásának kérdésére – itt és most csupán a közzétételt kísérő internetes támadások tanulságait vonja meg a ZMNE egyetemi tanára.

1999-es megjelenése óta a Wikileaks dokumentumok százezreit hozta nyilvánosságra internetes oldalán. Julian Assange szervezete tudatosan épített az internetre, azokra a szolgáltatásokra és előnyökre, amelyek a gyorsaságban, a viszonylagos kis anyagi befektetésben, és a széles tömegek elérésében kézenfekvőek az új médium megjelenése óta. Ugyanakkor az is nyilvánvalóvá vált, hogy ez az internetes weboldal hamar támadások kereszttüzébe kerülhet. Az már sokkal meglepőbb, hogy a mindazok a pénzügyi szolgáltatások is támadások célpontjaivá váltak, amelyek a botrány hatására nagyon gyorsan felfüggesztették a szervezet számára küldött pénzügyi adományok átutalását.

2010 decemberében Julian Assange számláját befagyasztotta az azt kezelő PostFinance svájci bank, valamint a Visa és a Mastercard is blokkolta a szervezet számára érkező utalásokat. Ezt követően az internetes pénzügyi tranzakciókat végző Paypal cég is felfüggesztette az Assange-nak és a szervezetnek szánt pénzek továbbítását. A cég honlapján hivatalos közleményben tudatta a tranzakciók felfüggesztésének okát, mely szerint szabályzatuk tartalmazza azt a kitételt, hogy illegális tevékenységet folytató személy vagy szervezet nem használhatja a cég szolgáltatásait.

Mindezek után szabályos bosszúhadjárat kezdődött e pénzügyi szervezetek ellen. Internetes aktivisták támadásokat indítottak minden olyan pénzügyi szolgáltató ellen, amely nem fogadta a Wikileaks számláira érkező adományokat. Egyes források szerint több ezer hekker napokon keresztül támadta őket. Ezek a hekkerek egy 4chan nevű internetes fórumhoz köthetők, akik a csoport hagyományait hűen követve Anonymousnak nevezik magukat. A 4chan 2003 őszén indult olyan fórum, ahol a felhasználók többek között képeket és – a Japánban igen népszerű – manga történeteket tesznek közzé, alapvetően angolul. A fórum egy olyan internetes szubkultúra megnyilvánulása, amely a különböző nemzetközi internetes tiltakozó akciók egyik melegágya és kiinduló pontja volt a közelmúltban. A csoport egyik elhíresült tiltakozó akciója az úgynevezett

Project Chanology (vagy *Operation Chanology*) volt, amely a Szcientiológiai Egyház ellen irányult 2008-ban. Az Anonymous megnevezés nem egy személyt takar, hanem – a 4chan meghatározása szerint – a csoport kollektívájának összessége.

Az Anonymous csoport Wikileaks melletti szimpátiaakciója az *Operation Payback* nevet kapta. A szólásszabadságot és a transzparenciát zászlajukra tűzve honlapjukon megjelent közleményükben kijelentették, hogy ugyanazokért a célokért küzdenek, mint a Wikileaks. Ennek megfelelően minden olyan szervezetet potenciális célpontnak tekintenek, amelyek részt vesznek a – főleg internetes – cenzúrában. Mivel a szervezet a Wikileaks pénzeit záró pénzügyi szolgáltatókat is a cenzúra kiszolgálóiként azonosította, ezért a támadásaikat elsősorban ezek ellen intézték.

A hekkerek DoS (*Denial of Service* – szolgáltatásmegtagadás) támadásokat irányítottak a pénzügyi szolgáltatók internetes rendszerei ellen. A Visa és a Mastercard is rögtön sietett közölni, hogy bár valóban támadják rendszereiket, de azok nem okoznak fennakadásokat a hitelkártyák használatában. Ugyanakkor biztonsági cégek elemzései azt mutatták, hogy a Visa rendszereit, amelyeket egyébként sokkal védettebbnek tartanak a konkurensénél, mintegy kétezer, amíg a Mastercardot közel négyszáz hekker támadta. Bár a két hitelkártya-óriás tranzakciós szolgáltatásaiban nem volt komoly fennakadás, internetes oldalaikat több órán keresztül nem lehetett elérni. December 6-án az Anonymous csoport újra aktivizálta tagjait, és a Paypal szolgáltatót vették célba. A támadások ebben az esetben jóval hatékonyabbak voltak, hiszen a Paypal szolgáltatásai, amelyeket például csak az E-bay aukciós szájton folytatott kereskedések esetében több százezer ügyfél használ naponta, közel egy napig szüneteltek.

Ugyanakkor ezek a támadások egyáltalán nem számítanak túl kifinomult hekkerakcióknak. Többségüket a *Low Orbit Ion Cannon* szoftver segítségével követték el. Ez a program tömeges DDoS-támadást idéz elő, azaz a nyers erőt használja a briliáns programozói megoldások helyett. Maga a program nyilvánosan elérhető és bárki által letölthető az internetről, azóta hogy megalkotója – a Praetox Technologies – 2008 év végén a már említett Project Chanology akció után közzétette. 2010 év végén a programot több mint 80 ezer alkalommal töltötték le.

Denial of Service – DoS; Distributed Denial of Service– DDoS. A DoS-támadás a szolgáltatás teljes vagy részleges megbénítása, amely történhet megosztva is, több forrásból (Distributed Denial of Service– DDoS). A DDoS-támadások összetettek, amelyek a támadón és támadotton kívüli számítógépek kapacitásait, illetve a külső számítógépek nagy mennyiségét használja a támadáshoz. Az egyszerű DoS-támadás szemtől szembeni támadás, ahol egy nagyon erős támadó állomás és a célállomás van csak kapcsolatban, nincsenek közbeiktatott gépek.

A DDoS-támadásokhoz szükségeltetnek úgynevezett zombik, korábban valamilyen úton megfertőzött olyan számítógépek, amelyek így távvezérelhetőek. A támadás során a mesterállomás jelt ad a zombigépnek vagy gépeknek, hogy kezdjék meg a támadást a kiszemelt célpont, vagy célpontok ellen. Ekkor az összes zombi egyszerre elindítja a támadást, és bár egyenként kis mennyiségű adattal dolgoznak, mégis több száz, vagy akár százezer támadó gép esetén a sok kis adatcsomag eredménye hatalmas adatáramlás, mely a megtámadott gép ellen irányul. A támadás során olyan nagy mennyiségű adat érkezik a megtámadott gépre, hogy az arra már nem képes válaszolni (vagy akár eleve már nem is képes azt fogadni). Ez komoly fennakadást okoz a gép működésében, akár teljesen le is állítja annak operációs rendszerét. E támadási forma veszélye abban rejlik, hogy nagyon-nagyon nehéz ellene hatékonyan védekezni. A védelem sokszor csak a megtámadott gépek lekapcsolásával valósítható meg.

Az Anonymous csoport más eszközökkel is fel kívánta venni a harcot céljai elérése érdekében. Az újabb eszközök között az egyik például ingyenes internetes faxszolgáltatások igénybevétele volt, amelyek segítségével napokon keresztül számtalan faxszámra a Wikileaks logójával ellátott kiszivárogtatott dokumentumok tömegeit küldték szét Angliában.

A Wikileaks mellett demonstráló támadásokkal egy időben brit hivatalos források arra figyelmeztettek, hogy kormányzati számítógépes rendszerek lehetnek a Wikileaks mellett álló hekkerek következő célpontjai. Ezek a figyelmeztetések az olyan weboldalakat és az azokon elérhető szolgáltatásokat hozták fel példának, mint az online adóbevallás oldala. Amennyiben ezeket a publikus weboldalakat érik támadások, akkor azok – bár hosszú távon nem okoznak komoly károkat – mégis nagyon látványosak lehetnek, sok ember figyelmét ráirányíthatják a tiltakozás igazai okára.

Mindezekkel az akciókkal párhuzamosan a Wikileaks szervereit is támadások érték. Információbiztonsági elemzések szerint a támadásokat egy th3j35t3r kódnevű hekker kezdte meg november 30-án. A Wikileaks szervereit ért támadások mellett a szimpátiaakciókat folytató Anonymous csoport számítógépeinek is támadásokkal kellett szembenézniük, azaz a támadások pro és kontra folytak.

Érdemes megjegyezni, hogy a Wikileaks elsődleges szervereinek az Amazon.com adott helyet, amely a hirtelen kialakult nemzetközi botrány hatására egyébként december 2-án magától is leállította azok működését. Ezt követően az EveryDNS nevű domain szolgáltató a wikileaks.org domain elérését is leállította. Ennek köszönhetően a Wikileaks még ma is csak egy svájci domain alatt érhető el a http://wikileaks.ch címen.

A demokrata elkötelezettségű Joe Lieberman szenátornak a Wikileaks online rendszerei ellen tett intézkedéseket üdvözlő közleményét sok helyen idézték, és a fentieket látva az abban foglaltakat valószínűleg sok helyen meg is fogadták. Lieberman szerint: „Ma reggel az Amazon értesítette kollégáimat, hogy megszüntette a Wikileaks weboldalának elérését. … Úgy gondolom, hogy ez a helyes döntés példa lehet a többi olyan vállalat számára is, amelyek a Wikileaks által megszerzett anyagok közzétételében részt vesznek. … Felhívom bármely más cég vagy szervezet figyelmét, amely a Wikileaks dokumentumainak közzétételében közreműködik, hogy azonnali hatállyal szüntesse meg a kapcsolatot a szervezettel. A Wikileaks jogellenes, felháborító és meggondolatlan cselekményei komolyan befolyásolhatják a nemzetbiztonságot, és életeket veszélyeztetnek világszerte.”

A hétköznapi emberek azonban – köszönhetően talán a média kiemelt figyelmének – egyre fokozódó érdeklődést tanúsítottak a Wikileaks által közzétett dokumentumok iránt, és hatalmas igény mutatkozott a friss hírekre. Ennek köszönhetően december közepén az egyik legnépszerűbb okostelefonra hamar el is készült az az alkalmazás, amellyel meg lehetett nézni a legfrissebb Wikileaks-híreket, illetve online nyomon lehetett követni a szervezet twitteroldalát. A szoftver megjelenését követő három nap után azonban az Apple cég eltávolította internetes boltjából az alkalmazást, mondván, hogy az ellentétes a cég szabályzatával.

A különböző pénzügyi szervezetek, valamint a Wikileaks szervereit kezelő internetszolgáltatók után természetesen a hivatalos adminisztráció is megtette az online hírek elérését megnehezítő lépéseit. A Fehér Ház megtiltotta az összes szövetségi alkalmazottnak, hogy a Wikileaks – még esetleg el-

érhető – weboldalait megtekintsék, és arra utasítottak minden minisztériumot, illetve szövetségi hatóságot, hogy akadályozzák meg az internetes hozzáférést a Wikileaks dokumentumaihoz. Ez az utasítás a Kongresszusi Könyvtárra is vonatkozott, amelynek szóvivője ugyanakkor természetesen igyekezett nyilatkozatában cáfolni, hogy ezzel cenzúrát vezetnének be. Indoklásként a kormánydokumentumok védelmének szükségességét jelölte meg, amely a többi szövetségi intézményhez hasonlóan kiemelt feladatuk. (Ezen intézkedés vonatkozásában az mindenesetre érdekes tény, hogy a Wikilaks rájött: Sarah Palin volt alaszkai kormányzó korábban nyilvános e-mail címről intézte hivatalos levelezését is. A Wikileaks programozói az elfogott leveleket természetesen közzétették).

A Wikileaks hivatalos twitteroldalán 2011. január 9-én este megjelent egy bejegyzés, amely a Gabrielle Giffords képviselő elleni merénylet és a Julian Assange ellen folytatott médiakampány között von érdekes párhuzamot. A bejegyzés azt az igen veszélyes retorikát említi fel, hogy több közszereplő – például tévériporterek és -kommentátorok, illetve számos újságíró – Assange egyszerű meggyilkolásában látta a megoldást. Assange és csapata létrehozott egy weboldalt PeopleOKwithmurderingAssange.com címen, ahol ma is megtekintetők azok a nyilatkozatok, amelyek Assange likvidálására szólítanak fel. A twitterbejegyzés szerint egyenes út vezetett oda, hogy többen, nagy nyilvánosság előtt Assange halálát kívánták, majd pedig egy fiatalember fényes nappal megsebesítette Giffords képviselőnőt, környezetében pedig több embert meg is ölt.

A Wikileaks melletti és elleni internetes támadások – különösen a pénzügyi szolgáltatások elleni akciók – felhívják a figyelmet arra, hogy minden olyan ország, amely fejlett informatikai rendszereket használ, igen komoly mértékben ki van téve ezeknek a veszélyeknek. Amennyiben mindezeket továbbgondoljuk, akkor felmerül, hogy számos olyan infrastruktúrával rendelkezünk, amelyek működése és rendelkezésre állása elengedhetetlenül szükséges a mindennapi életben, és amelyek támadhatóak az interneten. Ráadásul számtalan helyen informatikai rendszereket találunk a vezérlés, az ellenőrzés, vagy a működtetés biztosítására az olyan rendszereinkben, mint például az energiaszolgáltatók. Önmagukban ezek a vezérlő rendszerek kritikus információs infrastruktúrák. Tovább növeli a kockázatot az, hogy ezek a rendszerek nagyon sok helyen kapcsolódnak egymáshoz, egymást átfedő alrendszereik vannak, azaz komoly intra- és interdependencia van közöttük.

E rendszerek fontosságát, illetve az említett igen komoly veszélyforrásokat jelzi az Európai Unió 2005-ben kiadott úgynevezett Zöld Könyve is. Ez a dokumentum meghatározta azokat a lépéseket, amelyeket uniós vagy akár nemzeti szinten meg kell tenni a kritikus infrastruktúrák és a kritikus információs infrastruktúrák védelme érdekében. Ezt követően az Európa Tanács 2008 decemberében a kritikus infrastruktúrák azonosításáról szóló irányelvet adott ki, amely talán az egyik legnehezebb terület, hiszen nagyon nehéz eldönteni még nemzeti vagy akár regionális szinten is, hogy milyen infrastruktúrák minősülnek kritikusnak. A kérdést tovább bonyolítja, hogy ezek az infrastruktúrák jelentős részben nem állami tulajdonban és nem állami működtetésben vannak. Hazánkban 2008-ban született meg az első komoly terv egy kormányhatározat formájában, amely a Nemzeti kritikus infrastruktúra védelméről címet kapta. 2010 év végén pedig megjelent az a kormányhatározat is, amely a kritikus infrastruktúrák azonosítására és a védelem fokozására határoz meg feladatokat és ütemtervet.

A Wikileaks-botrány után természetes módon azonnal megkezdődtek a szakértők és a diplomácia vezetői között az egyeztetések. Ezeken olyan alternatívákkal próbáltak meg előállni, amelyek megakadályozhatják egy ilyen botrányos eset megismétlődését. Ugyanakkor tisztában kell lenni azzal, hogy Assange maga is hekker volt, aki ráadásul húszas éveinek elején komoly hírnevet is szerzett ezzel magának Ausztráliában. Nagyon korán felismerte az internet és az ezzel megjelenő, soha addig nem tapasztalt szabad információáramlás hatalmas lehetőségét és nagyon komoly közvélemény-formáló erejét. A Wikileaks létrehozása, valamint a számtalan forrásból számukra eljutatott dokumentumok ellenőrzése szintén a hálózat segítségével, alapvetően internetes technikák alkalmazásával történt. Assange egyik – szintén az interneten látható – nyilatkozatában utal arra, hogy bár a dokumentumok nyilvánosságra hozatala, illetve ezt megelőzően ezek zömének ellenőrzése számítógépes eszközökkel történt, ez egy idő után már nem bizonyult elegendőnek. A véges emberi kapacitás miatt kénytelen volt a hagyományos média segítségét kérni, hiszen nekik évtizedek óta megvannak azok az eszközeik, amelyek például az oknyomozó újságírásban beváltak. (Az eszközök mellett természetesen az oknyomozó újságírás jogszabályi környezete is fontos: Belgiumban, Franciaországban, vagy akár az Egyesült Államokban alkotmányos garanciákat találunk az újságírók védelmére). Ennek köszönhető, hogy a Wikileaks egyik partnere a *The Guardian* lett.

A csak néhány éves múltra visszatekintő, úgynevezett webkettes szolgáltatások, azaz például az olyan közösségi portálok, mint a Facebook (vagy akár a hazai Iwiw) hatalmas lehetőségeket rejtenek. Ezek a lehetőségek nemcsak az emberek egymás közötti kapcsolatának alakításában jelentkeznek, hanem akár abban is, hogy a világban bekövetkezett eseményekről szóló hírek hihetetlen sebességgel terjednek ezeken a hálózatokon, amelyekhez a vélemények hozzáadása teljesen szabadon működik. Azaz megjelenik a véleményformálás közösségi ereje. A közösségi erő az önszerveződést is támogatja. Ez igaz még az olyan országokban is, mint például Irán, ahol – noha igen erős a hagyományos és az internetes média cenzúrázása – működik az internetes önszerveződés, hiszen a 2009 nyarán, Teherán utcáin folyó tüntetések megszervezése, illetve az azokról szóló tudósítások nagyban köszönhetőek az internetes közösségi oldalaknak.

A Wikileaks és az általa képviselt eszme folyamatosan vonzotta azokat a szintén önszerveződés útján létrejött – alapvetően internetes – csoportokat, amelyek hasonló értékrendet vallottak. Az egyik ilyen csoport a németországi Chaos Computer Club, amely saját meghatározása szerint „galaktikus életformák közössége, függetlenül kortól, nemtől, fajtól vagy társadalmi orientációtól", és amely a határokon átívelő információszabadságra törekszik. Ezt a nagyon tehetséges programozókból álló csoportot egy másik – szintén a Wikileaks értékrendjéhez hasonló elveket valló – társaság csatlakozása követte. Ez a svéd Pirate Bay, amely folyamatos harcot vív a szabad fájlcserék érdekében. Így létrejött egy magas szintű informatikai tudással rendelkező társaság, amelyben a vélemény- és az információszabadság igénye nagyon erős. Ez a tudás, illetve a hozzá kapcsolódó informatikai eszközök és technikák színvonala igen figyelemre méltó. Ugyanakkor az a tény sem elhanyagolható, hogy Svédországban nagy hagyományai vannak az internetes tartalmak cenzúra elleni védelmének. A PRQ nevű svéd internetszolgáltató cég,

hasonlóan a svájci banktitok fogalmához, teljes névtelenséget ad a nála működtetett szerverek üzemeltetőinek, és nem ad ki semmilyen információt a szerverek forgalmáról, valamint az azt látogató felhasználókról sem. Valószínűleg ez az egyik legfontosabb oka, hogy ma már a Wikileaks gépei a PRQ-nak egy Stockholmhoz közeli szerverparkjában működnek.

Ugyanakkor azt mindenképpen meg kell jegyeznünk, hogy az internet létrehozói az információ szabad áramlásáról beszéltek anno, amely persze napjainkban országonként, politikai berendezkedéstől függően nagyon sok helyen csak utópia lehet, hiszen Kína, az említett Irán vagy Észak-Korea nem feltétlenül az információhoz való szabad hozzáférésről híres. A cenzúra – és ebben az internetes cenzúra – kiválóan működik nagyon sok országban. Abban az esetben azonban, ha az internet bölcsőjének tekintett Amerikai Egyesült Államokban kerül sor az interneten közzétenni kívánt információk szűrésére, akkor ez a régi-régi alapelv sérülhet. Sokan párhuzamot vonnak a demokrácia csorbítása, a szabadságjogok lábbal tiprása, valamint az internetes vagy akár a hagyományos média cenzúrázása között. Ebben nyilván van is némi igazság, hiszen épp az angolszász országok a legjobb példái a sajtónyilvánosság, illetve a civil kontroll közötti szoros összefüggésnek.

Az információs technika és technológia rohamos változásával együtt – nem kis részben talán éppen ennek köszönhetően – nemcsak az emberek egymással való kapcsolata alakul át, hanem megjelenik egy olyan új médium is, amely komoly kihívás lehet a kormányok számára. Nagyon nehéz a szabad véleményalkotás, a nyitottság és a nemzetbiztonsági szempontból fontos dokumentumok, tények nyilvánosságra hozatalának szabályozása mint elemi érdek közötti – sokszor nagyon keskeny – mezsgyéjén maradni.

Mindezek mellett azonban nem szabad elfelejtkezni arról a talán még komolyabb dilemmáról sem, ami napjainkban a szabadságjogokat, a szabad véleménynyilvánítás jogát, és a nemzetbiztonsági érdekeket teszi a mérleg két serpenyőjébe. A kérdés tehát továbbra is marad (vagy talán az eddigieknél még komolyabban jelentkezik): meddig mehetünk el a nyilvános adatok és információk nyilvánosságra hozatalában, és hol kezdődnek a valóban nemzetbiztonsági érdekek miatt nem nyilvánosságra hozható információk? ■

Irodalom

http://www.reuters.com/article/idUSL3E6N80HH20101208
http://wikileaks.ch
http://www.4chan.org/faq#anonymous
http://www.informationweek.com/news/security/cybercrime/
http://index.hu/tech/2010/12/15/kormanyzati_weboldalak_lehetnek_a_wikileaks-barat_hekkerek_uj_celpontjai/
http://www.readwriteweb.com/cloud/2010/12/amazon-drops-wikileaks.php
http://www.readwriteweb.com/archives/wikileaks_calls_for_sarah_palins_arrest.php
http://www.peopleokwithmurderingassange.com/
http://www.wired.com/threatlevel/2010/12/wikileaks-app/
http://www.msnbc.msn.com/id/40610611/ns/us_news-wikileaks_in_security/