5. fejezet

A proxycsoportok alkalmazásának taktikája: a hacktivisták

Krasznay Csaba

Bevezetés

A 2007-es Észtország ellen végrehajtott kibertámadás sok tekintetben egészen új helyzetet teremtett a kibertéri műveletek világában. Jelen fejezet szempontjából talán az attribúció körüli polémiát érdemes kiemelni. A nemzetközi sajtó és a politika ugyanis szinte azonnal Oroszországot mint államot vélte felfedezni a támadás mögött, az orosz kormányzat viszont akkor és azóta is folyamatosan tagadja a részvételét a műveletben. Rain Ottis, Észtország egyik legismertebb kiberbiztonsági szakértője 2008-ban így foglalta össze a rendelkezésre álló tényeket:

> „Az orosz kormány folyamatosan tagadta direkt részvételét a kibertámadásban, amely kiütötte Észtországot 2007 tavaszán. A szerző tudomása szerint ez az állítás igaz. De meg kell jegyezni, hogy semmilyen bizonyíték nem áll rendelkezésre arra vonatkozóan, hogy az orosz kormányzat bármit is tett volna a helyzet megoldása érdekében. Az észt nyomozással kapcsolatos együttműködés hiánya arra utal, hogy az orosz kormány nem volt érdekelt a támadók kilétének felfedésében, így röviden szólva védte őket. Más szavakkal a politikai elit által alkalmazott ellenséges retorika arra ösztönözte az embereket, hogy támadják Észtországot, és semmit nem tettek annak érdekében, hogy ezt a támadást leállítsák. Ez a csendes támogatás pedig úgy értelmezhető mint egyfajta implicit állami támogatás, mivel a retorziótól való félelem hiányában szabadon lehetett támadni az észtországi célpontokat."[1]

Ottis azt is hozzáteszi, hogy a támadás végrehajtásával kapcsolatos információkat orosz nyelvű fórumokon osztották meg egymás között a résztvevők. Ezeken pontosan meg volt határozva a célpont, az időzítés, a végrehajtás módja, valamint az ideológiai motiváció is. A támadást végül a Nasi („Mieink") ifjúsági

[1] Rain Ottis: *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective*. Cooperative Cyber Defence Centre of Excellence, 2008. március 2.

https://doi.org/10.36250/01079_05

https://orcid.org/0000-0003-3216-2592

mozgalom aktivistája, Konsztantyin Goloskokov vállalta magára, tagadva, hogy bármilyen utasítást kapott volna az orosz hivatalos szervektől.[2] Érdekesség, hogy 2016-ban az ukrán biztonsági szervek már mint az orosz katonai titkosszolgálat, a GRU, azaz az Oroszországi Föderáció Fegyveres Erői Vezérkarának Felderítő Főcsoportfőnöksége tisztjeként hivatkoznak Goloskokovra.[3]

A *Meduza* nevű orosz oknyomozó portál tényfeltáró riportja a támadás végrehajtásának koordinátoraként Pjotr Levasovot nevezi meg, aki „főállásban" az egyik legnagyobb kéretlen levélküldő szolgáltatást, a Kelihost üzemeltette, amíg 2017-ben az FBI nyomozása után le nem tartóztatták Barcelonában. A *Meduza* forrásai szerint Levasov legalább 2005 óta együttműködött az orosz állami szervekkel, és aktívan támogatta bizonyos műveleteit a Kelihos infrastruktúráját felhasználva.[4] Ezért cserébe érinthetetlen volt, így bár az amerikai nyomozóhatóság már 2007-ben vádat emelt ellene, 10 éven keresztül lehetetlen volt elfogni.[5]

Érdemes még megemlíteni Danyiil Turovszkij, a *Meduza* újságírójának orosz hackerekről szóló könyvének egy bekezdését, ahol a 2000-es évek közepének történéseit dolgozza fel, beleértve a 2007-es incidenst is. Ebben az időben egy Anton Moszkal nevű szentpétervári programozót keresett fel a belbiztonsági és kémelhárítási feladatokat ellátó Szövetségi Biztonsági Szolgálat, az FSZB munkatársa, és arról beszélt neki, hogyan lehetne küzdeni a „terrorista-weboldalak ellen", illetve mit jelent számára a patriotizmus. Bár a megkeresés félrement, a fentiek egyértelműen jelzik, hogy a 2000-es évek közepétől az orosz biztonsági szervek aktívan keresték a kapcsolatot a hazafias érzelmeket tápláló hackerekkel és kiberbűnözőkkel.[6]

[2] Christian Lowe: Kremlin Loyalist Says Launched Estonia Cyber-Attack. *Reuters,* 2009. március 13.

[3] UCMC Press Center: Security Service of Ukraine Possesses Audio Records of Krasnov's Conversations With His Russian Supervisor. 2016. március 3.

[4] Daniil Turovsky: "It's Our Time to Serve the Motherland." How Russia's War in Georgia Sparked Moscow's Modern-Day Recruitment of Criminal Hackers. *Meduza,* 2018. augusztus 7.; Department of Justice of Public Affairs: *Russian National Who Operated Kelihos Botnet Pleads Guilty to Fraud, Conspiracy, Computer Crime and Identity Theft Offenses* (2018. szeptember 12.).

[5] United States District Court: *United States Versus Peter Yuryevich Levashov* (2017. április 4.).

[6] Danyiil Turovszkij: *Orosz hekkerek.* Budapest, Athenaeum, 2020. 143.

A hacktivizmus alapvető fogalmai

Játsszunk el egy pillanatra azzal a gondolattal, hogy ismerve az események utáni közel 15 év történetét és az orosz kibertéri műveletek fejlődését talán a 2007-es esemény mégis egyfajta offenzív katonai kiberművelet volt, és nem tisztán az állampolgári elégedetlenség szülte azt! Tételezzük fel, hogy az orosz katonai vezetés már a korai 2000-es években felismerte annak lehetőségét, hogy az ország stratégiai érdeke megkívánja az információs műveletek során azokat az akciókat, amelyeket nem lehet közvetlenül összekötni a kormányzattal, hanem azokat látszólag független személyekre és csoportokra bízza! Amennyiben így történt, Oroszország sikerrel alkalmazta a fizikai hadviselésből jól ismert proxycsoportok taktikáját. Ráadásul nem is elsőként tette ezt, ahogy látni fogjuk, de a téma megértéséhez tisztázni szükséges néhány alapfogalmat!

Proxycsoportok a kibertérben. Michael N. Schmitt és Liis Vihul, a kiberhadviselés legismertebb nemzetközi jogi szakértői szerint akkor beszélhetünk proxycsoportokról a kibertérben, ha egy nem állami szereplő az adott állam utasításai szerint cselekszik, vagy az adott állam kontrollálja, illetve irányítja a nem állami szereplő cselekedeteit, kivéve akkor, ha az állami szereplő túllépi a hatáskörét, és úgy befolyásolja a nem állami szereplőket. Ha tehát „rendes ügymenet" szerint egy állami titkosszolgálat hatással van egy hackerre, kiberbűnözői csoportra, laza, informális csoportra, vállalatra vagy akár egy terrorista-, felkelőcsoportosulásra proxyműveletről beszélhetünk. A lényeg, hogy bár mindezt esetileg kell megítélni, legyen egyértelmű irányítási kapcsolat az állam és a nem állami szereplő között.[7]

Hacktivizmus. A fogalom magyarázatára számos forrást lehet találni, de érdemes visszamenni az ősforrásig, amely így határozza meg a hacktivizmust: „Az emberek felhatalmazásának célként való kitűzése, hogy a világ tudomást szerezzen az igazságtalanságokról, az emberi jogok megsértéséről. Más szóval, az információáramlás megszervezése világszerte, korlátozások és cenzúra nélkül. Ez a hacktivizmus." A hacktivizmus szó Omegától származik, a fogalmat pedig Count Zero írta le. Oxblood Ruffin így egészítette ezt ki: „a technológia használata az elektronikus médián keresztül az emberi jogok fejlesztése érdekében." Mindhárman a *Cult of the Dead Cow* (cDc) nevű hackercsapat tagjai

[7] Michael N. Schmitt – Liis Vihul: Proxy Wars in Cyberspace. *Fletcher Security Review,* 1. (2014), 2. 54–73.

voltak, a fogalom maga pedig az 1990-es évek közepén alakult ki, amikor a cDc igen aktív közéleti tevékenységet is folytatott.[8]

Hacktivista. Az előző gondolatmenet alapján következik, hogy a hacktivista az, aki részt vesz a hacktivizmusban. A 90-es évek óta viszont annyiféle megjelenését láttuk a hacktivistamozgalmaknak, hogy érdemes tágabban értelmezni a résztvevőket! Tim Jordan és Paul Taylor hacktivizmust feldolgozó könyvében így írja le a jelenséget:

> „A hacktivizmus a népszerű politikai akciók továbbfejlődése, embercsoportok saját akciói a kibertérben. A politikai tiltakozások és a számítógépes hackelés kombinációja. A hacktivisták a kibertér keretein belül működnek, küzdenek a virtuális életben technikailag lehetséges dolgokért, és kinyúlnak a kibertérből, a virtuális erők felhasználásával alakítják az offline életet. A társadalmi mozgalmak és a népi tiltakozás a 21. századi társadalmak szerves részét képezik. A hacktivizmus tulajdonképpen az aktivizmus elektronikussá válása."[9]

Hacktivista tehát az, aki egy politikai ideológia mentén szervezett kibertéri akcióban vesz részt, amelynek hatása van a fizikai világra is.

Patrióta vagy hazafias hacker. A katonai kiberműveletek szempontjából nagyon fontos csoportot alkotnak a hacktivistákon belül a patrióta vagy hazafias hackerek. Athina Karatzogianni hacktivizmusról szóló könyvében úgy írja körbe a patrióta hackereket, mint akik a nemzetük tisztaságáért küzdenek az online média ügyes felhasználásával. Paradox módon tehát a nacionalizmus mint politikai ideológia jelenik meg a klasszikus hacktivista akciók mögött, kihasználva az internetet mint globális médiát.[10]

Hacktivistacselekmény. A hacktivistaakciók eszköztára közel sem annyira összetett, mint amilyet egy kiváló műveleti tervező képességekkel rendelkező állami szereplő kivitelezni tudna. A hacktivistacsoportok ereje ráadásul a láthatóságban van, így nem érdekeltek abban, hogy a művelet rejtve legyen, illetve tipikusan csoportosan követik el a cselekményt, sokszor egymást nem is ismerve, akár nagyon eltérő földrajzi helyekről. A konspiráció tehát nem feltétlen cél. Romagna összefoglalója alapján így egy hacktivistacselekmény jellemzően az elosztott túlterheléses támadásokra (DDoS), a weboldalak átírására *(defacement)*

[8] Oxblood Ruffin: Hacktivism: From Here to There. *Threatpost,* 2010. december 9.

[9] Tim Jordan – Paul A. Taylor: *Hacktivism and Cyberwars. Rebels with a cause?* New York, Routledge, 2004. 1.

[10] Athina Karatzogianni: *Firebrand Waves of Digital Activism 1994–2014: The Rise and Spread of Hacktivism and Cyberconflict*. Basingstoke, Palgrave Macmillan, 2015. 22.

és az adatlopásra korlátozódik. Időnként előfordulhat kártékony kódok alkalmazása, de ennek meglehetősen negatív visszhangja van a közösségben.[11]

Hacktivizmus a *Tallinni kézikönyv* szerint

A proxycsoportok alkalmazásának tilalma a kibertéri műveletek során egyértelműen megjelenik az ENSZ 2012–2013 között működő Group of Governmental Experts (GGE) csoportjának zárójelentésében. A GGE feladata a tagállamok konszenzusát elérni bizonyos alapvető kibertéri szabályok és normák tekintetében. Az A/68/98 számú ENSZ-határozat 23. pontja világosan megfogalmazza ezt az elvárást:

> „Az államoknak teljesíteniük kell azon nemzetközi kötelezettségüket, hogy a nemzetközi jogot sértő cselekmények nekik legyenek tulajdoníthatók. Az államok nem használhatnak proxykat a nemzetközi jogot sértő cselekmények elkövetése során. Az államoknak biztosítaniuk kell azt, hogy a területüket ne használhassák olyan nem állami szereplők, akik jogtalanul használják az infokommunikációs technológiákat."[12]

Természetesen a fenti követelmény esetén is az ördög a részletekben rejlik. Egyrészt, nem egyértelmű, hogy hol is van a határa a nemzetközi jogot sértő cselekményeknek. Másrészt, igen nehezen bizonyítható, hogy az állam ténylegesen kontrollálta-e a nem állami szereplőt a cselekmény végrehajtása során. Harmadrészt, az internet határtalan, tehát a proxycsoportoknak nem feltétlenül kell abban az országban működnie, ahonnan az utasításokat kapják, a fogadó ország pedig nem biztos, hogy rendelkezik olyan képességekkel, amelyekkel meg tudja akadályozni a nemzetközi jogba ütköző cselekmény végrehajtását.

A *Tallinni kézikönyv* azért kísérletet tesz arra, hogy pontosítsa a proxycsoportok, ezen belül is a hacktivisták alkalmazásának szabályait. Legpontosabban a 17. szabály fogalmazza meg azt a követelményt, amelyet korábban már ismertettünk, egyben a GGE-határozat lényegét is tartalmazza. Eszerint tehát a kiberműveleteket végrehajtó nem állami szereplők tevékenysége akkor tulajdonítható egy államnak, amikor azok az állami szereplő utasításai szerint

[11] Marco Romagna: Hacktivism: Conceptualization, Techniques, and Historical View. In Thomas J. Holt – Adam M. Bossler (szerk.): *The Palgrave Handbook of International Cybercrime and Cyberdeviance*. London, Palgrave Macmillan, 2020.

[12] ENSZ: Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Document A/68/98 (2013. június 24.).

cselekszenek, illetve irányítása és kontrollja alatt állnak, valamint az állami szereplő tudomásul veszi és felhasználja a műveletet saját céljai érdekében.[13]

A 69. szabály próbálja meghatározni, hol kezdődik a nemzetközi jogot sértő cselekmények határa. Eszerint a kiberműveletek erőszakos cselekménynek minősülnek, amennyiben azok mértéke és hatása összehasonlítható az erőszakos cselekménynek minősülő nem kibertéri műveletekkel. A magyarázatban az szerepel, hogy például egy hacktivistacsoportnak pusztán a finanszírozása nem minősül erőszakos cselekménynek, abban az esetben, ha az adott csoport egy felkelés részese egy másik ország ellen.[14] Ez magyarázatot ad arra, hogy miért lehet hasznos az olyan országon belüli hacktivistacsoportok támogatása, mint például a CyberBerkut, egy Ukrajnán belül működő oroszbarát csoportosulás, amely aktívan kivette a részét a Kelet-Ukrajnában zajló fegyveres konfliktus kibertéri részéből.[15]

A 82. szabály tovább pontosítja, hogy egy kibertéri művelet milyen esetben minősül fegyveres konfliktusnak, és hol van a helye mindebben a hacktivistacsoportoknak. Fegyveres konfliktusról akkor beszélünk, amikor ellenséges cselekmények történnek két állam között, beleértve ebbe akár a pusztán kiberműveleteket alkalmazó akciókat is. A szabály magyarázata szerint az Észtországgal szemben végrehajtott művelet nem minősül fegyveres cselekménynek, mivel nincsen bizonyíték arra, hogy az abban részt vevő személyek valamely állam iránymutatása szerint cselekedtek volna, illetve valamely állam szervezte vagy jóváhagyta volna a műveletet. Ráadásul kérdéses, hogy egyáltalán volt-e fegyverhasználat, tehát a bevetett eszközök kiberfegyvernek minősülnek-e. A magyarázatból látszódik tehát, hogy bár számos jel utal titkosszolgálat által összehangolt műveletre, bizonyítékok hiányában a nemzetközi jog alapján nem lehetett eszkalálni a válaszadást.[16]

A 95. szabály szerint ráadásul egy fegyveres konfliktusban mindaddig civilnek kellene tekinteni egy személyt, ameddig egyértelműen be nem bizonyosodik, hogy az illető nem civil. Egy hacktivista esetében éppen ezért különösen nehéz bármilyen ellenintézkedést foganatosítani mindaddig, amíg direkt módon részt

[13] Michael N. Schmitt (szerk.): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge, Cambridge University Press, 2017. 94.

[14] Schmitt (2017): i. m. 330.

[15] Nikolay Koval: Revolution Hacking. In Kenneth Geers (szerk.): *Cyber War in Perspective: Russian Aggression against Ukraine*. Tallinn, NATO CCD COE Publications, 2015. 55–58.

[16] Schmitt (2017): i. m. 379.

nem vesz az ellenséges tevékenységben.[17] A 97. szabály szerint viszont a direkt részvétel megfosztja őt a civil státusztól. A magyarázat szerint, ha például egy hacktivista többször egymás után is megpróbál megtámadni egy vezetési pontot, mindaddig támadható marad, ameddig a támadásokat elköveti, tehát nemcsak a konkrét támadás idején, hanem a támadások között is. Sőt, amennyiben fennáll a lehetősége annak, hogy támadásait folytatni fogja hosszabb kihagyás után is, mindaddig célpont maradhat, ameddig a műveleti képessége fennmarad.[18]

A hacktivizmus gyökerei

Ahogy láthattuk, a *Tallinni kézikönyv* már tényként kezeli a hacktivistacsoportok offenzív kibertéri felhasználását, hosszú volt azonban az út, amíg idejutottunk. Érdemes tehát röviden áttekinteni, hogyan alakult ki a hackerszcéna, milyen fázisokon ment át a hacktivizmus, és hogyan kapcsolódtak ezek a csoportok az állami szereplőkhöz! Ahogy a történelmi áttekintésben látni fogjuk, Oroszország katonai szervei egyáltalán nem véletlenül kerültek közel ezekhez a csoportokhoz, de nem elsőként használták ki a bennük rejlő potenciált.

Maga a hackelés fogalma több évtizedre tekint vissza. A *hacking* szó eredeti jelentése valaminek a véletlenszerű levágását jelenti nehéz ütésekkel, és már az 1200-as évek Angliájában használták. Modern értelmében először 1955-ben írták le a Massachusetts Institute of Technology (MIT) modellvasútklubjának jegyzőkönyvében: „Mr. Eccles kéri, hogy bárki, aki az elektromos rendszeren dolgozik, vagy azt hackeli, legyen szíves lekapcsolni az áramot, hogy a biztosíték ne égjen le."[19] A „hackelés" ezen az egyetemen ettől kezdve azt jelentette, hogy valaki egy technikai problémán dolgozik szokatlan, kreatív megoldásokat keresve. Magyarul talán a buherálás, berhelés szavakkal lehetne a legjobban lefordítani. Nem meglepő módon a kifejezést elsősorban a *signals and power subcommitte*-ban, azaz az irányítástechnikai csoportban használták, innen ered az, hogy a *hackinget* a modellvasút minél hatékonyabb irányításának kifejezésére használták. Mivel a számítógépek civil környezetben elsők között az MIT-n jelentek meg, és ezekhez elsősorban azok a diákok fértek hozzá, akik szabadidejükben a modellvasutakat „programozták", törvényszerűen a hackelés kifejezés tőlük

[17] Schmitt (2017): i. m. 424.
[18] Schmitt (2017): i. m. 428.
[19] Ben Yagoda: A Short History of "Hack". *The New Yorker,* 2014. március 6.

ragadt át az informatika világára is. Nekik köszönhetjük egyébként a hackeretikát és az egész „cyber életérzést" is. Mivel az MIT diákjai között kialakult sajátos nyelvezetet kívülálló nem igazán érthette, megírták a *The Jargon File*-t, amely az általuk használt kifejezések magyarázatát tartalmazta. Ebben találhatjuk a hacker definícióját is.

1. Olyan személy, aki élvezi a programozható rendszerek részleteinek feltárását és a képességei kibővítését, szemben a legtöbb felhasználóval, akik inkább csak a szükséges minimumot tanulják meg. Az RFC1392 szerint olyan személy, aki örömmel ismeri meg a rendszer, különösen a számítógépek és a számítógépes hálózatok belső működését.
2. Aki lelkesen (akár rögeszmésen) programoz, vagy aki sokkal inkább élvezi magát a programozást, mint a programozásról való elmélkedést.
3. Olyan személy, aki képes értékelni a *hack* értékét.
4. Olyan ember, aki jól tud gyorsan programozni.
5. Egy adott program szakértője, vagy aki gyakran dolgozik a programon vagy annak segítségével (lásd a „Unix hacker" definícióját).
6. Bármilyen szakértő vagy rajongó. Lehet valaki például csillagász hacker is.
7. Aki élvezi a korlátok kreatív legyőzésének vagy megkerülésének intellektuális kihívását.
8. [elavult] Rosszindulatú beavatkozó, aki kényes információkat próbál felfedezni próbálkozással. Ezek a jelszóhackerek vagy hálózati hackerek. Ma már a helyes kifejezés ezekre a cracker.[20]

Az 1970-es években a hackerszubkultúra folyamatosan terjedt, elsősorban a Szilícium-völgyben és a nagy amerikai műszaki egyetemeken. Ennek folyamatát és történetét Steven Levy 1984-es könyve írja le, egyben itt található meg a hackeretika leírása is, amely szerint az ősi hackerek a világhoz viszonyultak.

1. A számítógépekhez való hozzáférésnek – és bárminek, ami megtaníthat valamit arról, hogy a világ hogyan működik – korlátlannak és totálisnak kellene lennie.
2. Minden információnak hozzáférhetőnek kellene lennie.
3. Ne bízz a hatóságban – támogasd a decentralizációt!
4. A hackereket az általuk elkövetett tettek alapján kellene megítélni, nem pedig iskolai végzettség, kor, faj vagy pozíció alapján.

[20] Eric S. Raymond: The Jargon File, version 4.4.8. *Eric S. Raymond's Home Page,* 2004. október 1.

5. Művészetet és szépséget kreálhatsz a számítógépeden.
6. A számítógépek jobbá tehetik az életedet.[21]

Érdemes kiemelni, hogy a negyedik pont szerint a hatóságokkal való együttműködés nemkívánatos, ami annak is köszönhető, hogy ekkoriban jelent meg az amerikai büntetőjogban az első olyan passzus, amely szankcionálta a számítógépes bűncselekményeket. Ezután a hackerközösség tagjai egyre gyakrabban kerültek szembe a törvénnyel és a bűnüldöző szervekkel. Ennek tragédiáját fogalmazza meg Loyd Blankenship, a Legion of Doom tagjának nagy hatású írása, *A hacker kiáltványa,* amelynek utolsó sorai így hangzanak Voyager2 fordításában:

> „Igen, bűnöző vagyok. A bűnöm a kíváncsiság. A bűnöm az, hogy azután ítélem meg az embereket, amit mondanak és gondolnak, és nem a külsejük alapján. A bűnöm, hogy okosabb vagyok, mint ti, ez olyan dolog, amit soha nem fogtok nekem megbocsátani. Hacker vagyok, és ez a kiáltványom. Megállíthatjátok az egyént, de nem állíthattok meg minket… végül is, mind egyformák vagyunk."[22]

Nem tett jót az állam és a hackerek közötti kapcsolatnak az sem, hogy a hatósági érdeklődés pont 1984-ben erősödött fel. George Orwell világhírű regényének címe és tartalma, valamint az aktuális évszám és a közösséget érő csapások közötti látszólagos összefüggések ugyanis nagy hatást tettek az arra érzékeny közönségre, és nem javították az USA kormányával szembeni bizalmat. Lassan 30 éves távlatból viszont úgy látszódik, hogy sokkal inkább véletlen egybeesések alakították ezt a viszonyt. Az 1980-as évek elejétől az amerikai háztartásokban is széles körben elérhetővé váltak a számítógépek, fiatalok százezrei ismerkedtek meg a programozás alapjaival. 1983-ban vetítették a *Háborús játékok* című amerikai filmet, amely széles körben ismertté tette a hackerizmust. 1984-ben megtartották az első hackerkonferenciát, a Hackers Conference-t, elindult az első hackermagazin, a *2600,* illetve ehhez kapcsolódóan megjelent Steven Levy már említett könyve. A hacker tehát bekerült az amerikai közbeszédbe, aminek a hatására létrejöttek az első szervezett hackercsoportok, amire viszont már lépnie kellett a jogalkotónak, és meg kellett szabnia azokat a határokat,

[21] Steven Levy: *Hackers: Heroes of the Computer Revolution*. Garden City, Anchor Press/Doubleday, 1984. 458.

[22] The Mentor: The Conscience of a Hacker. *Phrack Inc.,* 1. (1986), 7. Phile 3 of 10.

amelyeket a számítógépes tevékenységek nem léphetnek át. Ez viszont érdekellentétet és meglehetős bizalmatlanságot szült.

Az első hacktivistacsoportok

Az amerikai hackercsoportok gondolkodásában eközben egyre inkább megjelentek az ideológiai vonások is. Ez egyenesen következik a keleti és nyugati parti amerikai egyetemek klasszikus szabadelvűségéből és a korszellemből, amely előbb a vietnámi háborúval, majd később a Ronald Reagan nevével fémjelzett mély konzervatív gondolkodással való szembenállásban manifesztálódott az amerikai fiataloknál. A hacker nem bízott az államban, és meg akarta mutatni, hogy az állam hazudik. Éppen ezért, ahogy a hackeretika második pontjában olvashatjuk is, az információt sokan hozzáférhetővé akarták tenni. Beleértve ebbe az állam titkait is. Ezt a mozgalmat az „Information wants to be free", azaz az információ szabad akar lenni mottóval indították el, eredete az MIT modellvasútklubjának két tagjához, Jack Dennishez és Peter Samsonhoz nyúlik vissza. A kifejezést viszont Stewart Brand alkotta meg, aki 1984-ben, a Hackers Conference-en ezt mondta:

> „Egyrészt az információ drága akar lenni, mert nagyon értékes. A megfelelő információk a megfelelő helyen egyszerűen megváltoztatják az életedet. Másrészt az információ ingyenes akar lenni, mert a kinyerésének költsége folyamatosan csökken. Tehát ez a kettő harcol egymás ellen."[23]

Az 1980-as évek közepén, 1990-es évek elején számos hackercsoport jött létre, így volt táptalaja ennek a gondolkodásnak. A legnagyobb ilyen csoportok: a Cult of the Dead Cow 1984-ben, Texasban alakult meg; a Legion of Doom, szintén 1984-es alapítással, szerte az USA-ban rendelkezett tagokkal; a Masters of Deception az 1980-as évek végétől New Yorkban működött; és ott volt még a bostoni L0pht Heavy Industries, 1992-es indulással. Ahogy korábban olvasható volt, a cDc tagjai megalkották a hacktivizmus kifejezést, a hackercsoportok pedig egyre többször szerepeltek a nyilvánosság előtt. Talán a legemlékezetesebb ebből az időszakból a L0pht kongresszusi meghallgatása volt 1998-ban, amelyet

[23] Cory Doctorow: Saying Information Wants to Be Free Does More Harm Than Good. *The Guardian,* 2010. május 18.

az első, széles körben ismertté vált kiberbiztonsági ülésként tartanak számon. Ennek témája az USA kibertéri kitettsége volt. A hackerek segítettek rávilágítani arra, hogy milyen súlyos sebezhetőségek vannak az interneten és a kritikus infrastruktúrákban.[24] Érdekesség, hogy a meghallgatáson fontos szerepet játszott Peiter „Mudge" Zatko, a L0pht tagja, aki 2004-től kezdve hosszabb ideig a DARPA-nak dolgozott, katonai kibervédelmi projekteken.

A hacktivizmus ekkoriban találkozott a digitális aktivizmussal, és nagyon hasonló eszköztárral ugyan, de nagyon különböző háttérrel két irányzat erősödött meg. Az egyiket tömegmozgalmi hacktivizmusnak nevezték, és sokkal inkább a politikai aktivizmus jegyeit mutatta, de már kihasználta az internetben rejlő lehetőségeket. Az első ilyen mozgalmat Ricardo Dominguez alapította, aki művész és író volt. Mozgalmának neve The Electronic Disturbance Theater volt, és 1997-ben indította el. Ez volt az első olyan polgárjogi mozgalom, amely számítógépeket használt aktivistatevékenysége során. Legismertebb akciója a FloodNet volt, amelynek segítségével DDoS-t indítottak a mexikói zapatista felkelők támogatása érdekében. A célpontok között volt a mexikói és az amerikai elnök weboldala is.[25]

A másik irányzatot digitálisan korrekt hacktivizmusnak hívták. Ez a Cult of the Dead Cow-ból indult mozgalom volt, Oxblood Ruffin vezetésével.[26] Elsődleges célkitűzése az információhoz való hozzáférés és a szólásszabadság biztosítása volt az interneten. 2001. július 4-én, a függetlenség napján adták ki a *Hacktivismo Declarationt,* amelyben az internet szabadságának máig ható alapértékeit fogalmazták meg. Ebben többek között foglalkoznak az internethozzáférés szabadságával, az elektronikus információ cenzúrájának kérdésével és a szólásszabadsággal is.[27] Ők kezdik el propagálni az anonim kommunikációs megoldások használatát az információ szabad áramlása érdekében, ami a 2020-as évek elejére annyira általánossá vált, hogy már a nemzetbiztonságot fenyegeti ezen platformok lehallgathatatlansága.

A 90-es évek végén az amerikai hacktivistacsoportok már a globális biztonságpolitikába is belekeveredtek, valószínűleg nem is sejtve, hogy ezzel elindítják a proxycsoportok alkalmazásának taktikáját a 2000-es években. Az egyik nagy visszhangot kiváltó akciót az utókor Blondie Wong és a Hong Kong Blondes

[24] Rosemary Tropeano: Landmark Senate Hearings Exposed Risks and Threats That Are Still Being Confronted. *National Security Archive,* 2019. január 9.

[25] Jordan–Taylor (2004): i. m. 69.

[26] Jordan–Taylor (2004): i. m. 98.

[27] Cult of the Dead Cow: *Hacktivismo Declaration* (2001. július 4.).

néven ismeri. Az 1995–1998 között zajló történet lényege, hogy állítólag Oxblood Ruffin kapcsolatba került egy kínai disszidens csoporttal, amely a kínai triádok segítségével csempészett nyugatra olyan másként gondolkodókat, akik szembekerültek a kínai kormánnyal. A Blondie Wong néven ismert kapcsolattartó és a Hong Kong Blondes-nak nevezett csoportja Ruffin segítségével kapcsolatba került a cDc-vel és más hackercsoportokkal is, amelyek segítségével egyrészt sajtónyilvánosságot kaptak, másrészt elsajátítottak hackertechnikákat, és hozzáfértek olyan támadóeszközökhöz, mint például a Back Orifice 2000 nevű, távoli hozzáférést lehetővé tevő szoftver, amelynek segítségével sikeresen támadtak kínai célpontokat. A részletek nem ismertek, de Ruffin évekkel későbbi beszámolója arra enged következtetni, hogy a művelet nem nélkülözte a titkosszolgálati jelleget.[28] Már ha megtörtént egyáltalán, és nem a cDc hatalmas médiahackje volt, a kínai szakirodalomban ugyanis nyoma sincsen a sztorinak.[29] Az amerikai média mindenesetre felkapta a történetet, és széles körben ismertté vált a hacktivizmus.

A másik ilyen akcióra 1998 végén került sor, amikor a Legions of the Underground nevű csoport kiberháborút hirdetett Kína és Irak ellen, az emberi jogok megsértése miatt. A felhívás lényege az volt, hogy néhány napon keresztül a közösség tagjai célzottan támadják a két ország informatikai infrastruktúráját, ezzel ellehetetlenítve az országok normális működését. Ez hatalmas vihart kavart, a legjelentősebb hackercsoportok, mint a cDc, a L0pht vagy a német Chaos Computer Club, közös közleményben határolódtak el a felhívástól, jelezve azt, hogy elfogadhatatlannak tartják az ilyen beavatkozást más országok működésébe.[30] A beszámolók szerint egyébként a Legions of the Underground is tagadta, hogy köze lenne a felhíváshoz. A felhívást a csoport egyik tagjának, Staktonnak tulajdonították, viszont ő saját bevallása szerint a felhívás idején két hétig nem volt online, a nevében nyilatkozott valaki, akit utána soha többet nem láttak.[31] A támadást végül nem hajtották végre, a történeti visszatekintésekben viszont egyre többször merül fel, hogy az érintett titkosszolgálatok beépültek ezekbe a közösségekbe. Ezt erősíti meg az FBI-tól kikért akták sokasága is, amelyek szerint legkésőbb az 1995-ös DefCon hackerkonferencián már műveleti célból

[28] Oxblood Ruffin: Blondie Wong And The Hong Kong Blondes. *Medium,* 2015. március 23.

[29] Wei Honker: cDc Created Hong Kong Blondes and ‚Hacktivism' as a Media Hack. *Seclist.org,* 2012. május 3.

[30] International Coalition of Hackers: „Hackers Don't Go To War" (1999. január 7.).

[31] James Glave: Confusion Over 'Cyberwar'. *Wired,* 1999. január 12.

vettek részt FBI-ügynökök.[32] Ezen a rendezvényen azóta is rendszeres esemény a „Spot the Fed", azaz a „Szúrd ki az ügynököt" játék.

Hacktivizmus a keleti nagyhatalmakban

Turovszkij orosz hackerekről szóló könyvéből az olvasható ki, hogy nagyon más fejlődési úton ugyan, de a 2000-es évek elejére Oroszországban is kialakult a hacktivizmus útját járó közösség. Az orosz hackerszcéna a számítógépekhez való szabad hozzáféréssel kezdődött a 90-es évek elején, majd az IRC-csatornák, az orosz nyelvű *Hacker* magazin és nem utolsósorban a kiváló matematikaoktatás folyamatosan kitermelte az erre fogékonyak közül az első generációs hackereket. Az orosz vadkapitalizmus során ezek a fiatalok elsősorban klasszikus kiberbűncselekményeket követtek el, nyugati, elsősorban amerikai áldozatok bankszámláit és kártyáit csapolták meg. Az orosz hatóságok egy ideig képtelenek voltak ellenük bármit is tenni, majd megszületett az a hallgatólagos megállapodás, hogy ameddig nem hazai célpontokat támadnak, addig nem is tesznek hatalmas erőfeszítéseket az elkövetők kézre kerítése érdekében. Ami rossz Amerikának, de nem fáj Oroszországnak, az elfogadható, azaz az ellenségem ellensége a barátom. Ez az évtizedek során azt eredményezte, hogy a külföldön elkövetett gazdasági bűncselekmények „elnézése" fejében ezeket a kiberbűnözői csoportokat és a támadó infrastruktúráikat egyre gyakrabban használták fel proxyként az Oroszország érdekében álló műveletek végrehajtása során, ahogy azt az észtországi példában is láthattuk.[33]

Az orosz állampolgár és az orosz államhatalom közötti, évszázadok alatt kialakult sajátos kapcsolat miatt a hacktivizmus itt nem a liberális, szólásszabadságot és állami túlhatalmat ellenző irányban jelent meg hangsúlyosan – bár ilyen irányzatokkal is lehet találkozni –, hanem kitermelte a hazafias hackerek irányzatát. Ez hangsúlyosan a második csecsen háborútól érződik, amikor önszerveződő csoportok kaukázusi internetes célpontok ellen hajtottak végre támadásokat, majd 2005-től egyértelműen megjelentek azok a szervező erők a fórumokon, amelyekre 2007-ben már támaszkodni lehetett.

[32] JPat Brown: FBI Files on Def Con Show "Spot the Fed" Contest a Sore Spot for Feds. *Muckrock,* 2015. május 6.

[33] Turovszkij (2020): i. m. 27–59.

A nyugati olvasók számára talán kevésbé ismert, de a kínai hacktivista-csoportok létrejötte és politikai célok mentén történő aktivizálódása megelőzte orosz társaikét. Scott J. Henderson könyvében részletesen feldolgozta a kínai hackerközösség történetének első évtizedét; kiderül, hogy a kínai internet 1994-es indulása után szinte azonnal megjelentek azok a fórumok, ahol a téma iránt érdeklődő tízezrek egymásra tudtak találni. Az első szervezettebb csoport a Zöld Hadsereg (Green Army) volt, amelyet az első kommunista katonai akadémia, a Whampoa Academy után neveztek el. Nem sokkal ezután indult a Kínai Sasszövetség (China Eagle Union). Mindkét csoport indulása 1997-re datálható.

A legjelentősebb csoportosulás azonban a 90-es évek végén, különböző csoportok egyesülése után jött létre. Az önmagát Vörös Hackerek Szövetségének (Red Hacker Alliance) nevező csoport több tízezer tagot számlált, és kimondottan a patrióta hackerek jellemzőit viselte magán. A csoport első komoly hacktivistatevékenysége 1998-ra tehető, amikor tömeges *deface* támadásokat intéztek indonéz kormányzati célpontok ellen, mivel ebben az időben a kínai kisebbséget jelentős támadás érte az indonéz többség részéről. Később célponttá vált Tajvan és Japán is, minden esetben a kínai nacionalizmust sértő lépések miatt.

A Vörös Hackerek Szövetsége valószínűleg a kínai kormányzattól függetlenül jött létre, ráadásul az is valószínű, hogy a kínai kultúra sajátossága miatt a kínai titkosszolgálatok nem vettek részt aktívan az első hacktivistaakciók szervezésében, azt a kínai hackerek ténylegesen saját patrióta beállítottságuk miatt hajtották végre. Az azonban Henderson kutatásai szerint biztosnak tűnik, hogy a csoport felbomlásának idején, 2005-ben a kínai hadsereg már aktívan toborzott a tagok között, illetve a 2000-es évek elején már létezett olyan kiberhadviseléssel foglalkozó csoport a Kínai Népi Felszabadító Hadseregen belül, amely az amerikai és izraeli példa alapján szerveződött.[34] Ezzel véget is ért a kínai hacktivizmus első generációjának aktivitása, de jöttek a következő generációk, amelyeknek egyre inkább a kontrollált kínai interneten kellett működniük, az érdeklődés azonban nem csökkent, éppen ellenkezőleg, nőtt a hackerizmus iránt.[35]

[34] Scott J. Henderson: *The Dark Visitor. Inside the World of Chinese Hackers.* Scott Henderson, 2007.

[35] Craig Webber – Michael Yip: The Rise of Chinese Cyber Warriors: Towards a Theoretical Model of Online Hacktivism. *International Journal of Cyber Criminology,* 12. (2018), 1. 230–254.

Következtetések

Jelen fejezet a 2000-es évek első felében hagyja abba a hacktivistacsoportok történetének bemutatását, nem foglalkozik az Anonymous vagy a LulzSec csoporttal, nem részletezi a WikiLeaks tevékenységét és Edward Snowden vagy Bradley (ma már Chelsea) Manning szerepét sem elemzi. A 2007-es észtországi események ugyanis teljesen új világot teremtettek a kiberhadviselésben, és a nagyhatalmak inkább az ilyen proxycsoportok integrálására törekedtek. Ennek oka egyrészt a nemzetközi kapcsolatokban keresendő, de valószínűleg nagyobb súllyal esett latba az, hogy a hackerek kevéssé kontrollálhatóak, egyáltalán nem biztos, hogy egy titkos művelet nem kerül napvilágra egy sértett hacker miatt. Ha ugyanezek az emberek fegyveres testületen belül, annak szabályait követve dolgoznak, valószínűleg sokkal hatékonyabbak is.

Ha megnézzük a nagyhatalmak hozzáállását a hacktivistacsoportokhoz, ugyanazt az utat látjuk. Az Egyesült Államokban az első generációs hacktivisták eltűntek, sokan közülük valószínűleg, Mudge-hoz hasonlóan, kormányzati szolgálatba álltak. Az biztos, hogy az Anonymous csoportra már rendvédelmi problémaként tekintettek az amerikai rendvédelmi szervek, a szétzüllesztésére és felszámolására törekedtek. Az USA-ra egyébként sem volt jellemző a hacktivisták proxyként való felhasználása. Oroszország hibrid hadviselése során továbbra is széles körben alkalmaz proxykat, de ezek ma már szinte kizárólag magánbiztonsági cégek. Ezek közül talán a legismertebb az Internet Research Agency, amelyet a 2016-os amerikai elnökválasztás befolyásolási kísérlete során használtak, de számos más, hasonló cég megtalálható az amerikai embargós listán, amelyet az őket ért kiberincidensek nyomán bővítenek. Emellett természetesen minden lehetőséget kihasználnak, így Julian Assange, a WikiLeaks vezetőjének gyakori szereplése az orosz RT nevű propagandatévében sem véletlen. Kína esetében pedig a hacktivisták és az állam motivációi sosem álltak egymástól távol, így aránylag könnyen integrálták és integrálják jelenleg is a hackerizmus iránt érdeklődő fiatalokat a hadseregbe.

A hacktivisták proxyként való felhasználása offenzív kiberműveletekben tehát inkább a 2000-es évekre jellemző. De hacktivizmus mindig lesz. Egészen pontosan mindig lesznek olyan lánglelkű fiatalok, akik rendszerkritikusságukat vagy éppen hazafiságukat a hackerizmus eszközeivel élik meg. Amennyiben egy ország tudatosan törekszik ezen fiatalok honvédelembe való integrálására – hasonlóan a nagyhatalmakhoz –, akár rövid távon is megvalósítható az offenzív kiberképességek létrehozása. Egy 2012-es felmérés szerint

Magyarországon az információbiztonságban dolgozó vagy az iránt érdeklődő személyek 59%-a akár ingyen is szolgálná a hazáját, míg 27%-uk pénzt kérne ezért. Csupán 14% válaszolt úgy, hogy nem venne részt a honvédelemben.[36] Bár a felmérés régi, feltehetően továbbra is sikerrel lehetne meríteni a magyar hackerek közül, ami tudatos tervezéssel a magyar kiberhadviselési képességek fejlesztésének egyik fontos eleme lehet.

Irodalomjegyzék

Brown, JPat: FBI Files on Def Con Show "Spot the Fed" Contest a Sore Spot for Feds. *Muckrock,* 2015. május 6. Online: www.muckrock.com/news/archives/2015/may/06/def-cons-spot-fed-contest-sore-spot-feds/

Cult of the Dead Cow: *Hacktivismo Declaration* (2001. július 4.). Online: https://blog.9while9.com/manifesto-anthology/2001.html

Department of Justice Office of Public Affairs: *Russian National Who Operated Kelihos Botnet Pleads Guilty to Fraud, Conspiracy, Computer Crime and Identity Theft Offenses* (2018. szeptember 12.). Online: www.justice.gov/opa/pr/russian-national-who-operated-kelihos-botnet-pleads-guilty-fraud-conspiracy-computer-crime

Doctorow, Cory: Saying Information Wants to Be Free Does More Harm Than Good. *The Guardian,* 2010. május 18. Online: www.theguardian.com/technology/2010/may/18/information-wants-to-be-free

ENSZ: *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. Document A/68/98* (2013. június 24.). Online: https://undocs.org/A/68/98

Glave, James: Confusion Over ‚Cyberwar'. *Wired,* 1999. január 12. Online: www.wired.com/1999/01/confusion-over-cyberwar/

Henderson, Scott J.: *The Dark Visitor. Inside the World of Chinese Hackers*. Scott Henderson, 2007.

International Coalition of Hackers: „Hackers Don't Go To War" (1999. január 7.). Online: http://lists.jammed.com/ISN/1999/01/0019.html

Jordan, Tim – Paul A. Taylor: *Hacktivism and Cyberwars. Rebels with a Cause?* New York, Routledge, 2004.

[36] Krasznay Csaba – Varga-Perke Bálint: Ifjúságvédelem a hacker szubkultúrában. In Bíró A. Zoltán – Gergely Orsolya (szerk.): *Ártalmas vagy hasznos internet? A média hatása a gyermekekre és fiatalokra*. Csíkszereda, Státus, 2013. 179–202.

Karatzogianni, Athina: *Firebrand Waves of Digital Activism 1994–2014: The Rise and Spread of Hacktivism and Cyberconflict*. Basingstoke, Palgrave Macmillan, 2015.

Koval, Nikolay: Revolution Hacking. In Kenneth Geers (szerk.): *Cyber War in Perspective: Russian Aggression against Ukraine*. Tallinn, NATO CCD COE Publications, 2015. 55–58.

Krasznay Csaba – Varga-Perke Bálint: Ifjúságvédelem a hacker szubkultúrában. In Bíró A. Zoltán – Gergely Orsolya (szerk.): *Ártalmas vagy hasznos internet? A média hatása a gyermekekre és fiatalokra.* Csíkszereda, Státus, 2013. 179–202.

Levy, Steven: *Hackers: Heroes of the Computer Revolution.* Garden City, Anchor Press/ Doubleday, 1984.

Lowe, Christian: Kremlin Loyalist Says Launched Estonia Cyber-Attack. *Reuters*, 2009. március 13. Online: www.reuters.com/article/us-russia-estonia-cyberspace-idUSTRE52B4D820090313

Ottis, Rain: *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective.* Cooperative Cyber Defence Centre of Excellence, 2008. március 2. Online: https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf

Raymond, Eric S.: The Jargon File, version 4.4.8. *Eric S. Raymond's Home Page,* 2004. október 1. Online: http://catb.org/jargon/

Romagna, Marco: Hacktivism: Conceptualization, Techniques, and Historical View. In Thomas J. Holt – Adam M. Bossler (szerk.): *The Palgrave Handbook of International Cybercrime and Cyberdeviance*. London, Palgrave Macmillan, 2020. Online: https://doi.org/10.1007/978-3-319-90307-1_34-1

Ruffin, Oxblood: Hacktivism: From Here to There. *Threatpost,* 2010. december 9. Online: https://threatpost.com/hacktivism-here-there-120910/74759/

Ruffin, Oxblood: Blondie Wong And The Hong Kong Blondes. *Medium,* 2015. március 23. Online: https://medium.com/emerging-networks/blondie-wong-and-the-hong-kong-blondes-9886609dd34b

Schmitt, Michael N. (szerk.): *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge, Cambridge University Press, 2017.

Schmitt, Michael N. – Liis Vihul: Proxy Wars in Cyberspace. *Fletcher Security Review,* 1. (2014), 2. 2014. 54–73. Online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2388202

The Mentor: The Conscience of a Hacker. *Phrack Inc.,* 1. (1986), 7. Phile 3 of 10. Online: http://phrack.org/issues/7/3.html

Tropeano, Rosemary: Landmark Senate Hearings Exposed Risks and Threats That Are Still Being Confronted. *National Security Archive,* 2019. január 9. Online: https://bit.ly/3I1jNKh

Turovsky, Daniil: "It's Our Time to Serve the Motherland." How Russia's War in Georgia Sparked Moscow's Modern-Day Recruitment of Criminal Hackers. *Meduza*, 2018. augusztus 7. Online: https://meduza.io/en/feature/2018/08/07/it-s-our-time-to-serve-the-motherland

Turovszkij, Danyiil: *Orosz hekkerek*. Budapest, Athenaeum, 2020.

UCMC Press Center: Security Service of Ukraine Possesses Audio Records of Krasnov's Conversations With His Russian Supervisor. 2016. március 3. Online: https://uacrisis.org/en/40837-sbu-3

United States District Court: *United States Versus Peter Yuryevich Levashov* (2017. április 4.). Online: www.justice.gov/opa/press-release/file/956511/download

Webber, Craig – Michael Yip: The Rise of Chinese Cyber Warriors: Towards a Theoretical Model of Online Hacktivism. *International Journal of Cyber Criminology,* 12. (2018), 1. 230–254. Online: http://cybercrimejournal.com/Webber&YipVol12Issue1IJCC2018.pdf

Wei Honker: cDc Created Hong Kong Blondes and ‚Hacktivism' as a Media Hack. *Seclist.org,* 2012. május 3. Online: https://seclists.org/fulldisclosure/2012/May/30

Yagoda, Ben: A Short History of "Hack". *The New Yorker,* 2014. március 6. Online: www.newyorker.com/tech/annals-of-technology/a-short-history-of-hack