DOI:10.38146/bsz-ajia.2011.v59.i2.pp21-48

MEZEY NÁNDOR LAJOS

Kiberterrorizmus: valós veszély?

Ha napjainkban meghalljuk a terrorizmus kifejezést, mindannyian öngyilkos merénylőkre, autókba rejtett pokolgépekre, emberrablásokra és hasonló, általában sok emberi életet követelő, jobbára politikai, vallási indíttatású cselekedetekre gondolunk, amelyekhez, mondhatni a terroristák legnagyobb örömére, kellő nyilvánosságot teremt mind a hagyományos, mind az elektronikus sajtó.

A terrorizmus hagyományos megjelenése mellett a számítástechnika előretörése a terroristáknak is rengeteg új elkövetési lehetőséget, célpontot kínálhat, ezáltal új feladatokat adhat a bűnüldöző szerveknek.

Az említett lehetőség ellenére, ha megállítanánk tíz embert az utcán, és megkérdeznénk, mit takar a kiberterrorizmus kifejezés, félő, hogy tíz egymástól jelentősen különböző választ kapnánk.

Ezen az arányon akkor sem tudnánk jelentősen javítani, ha a számítástechnika terén jártas embereknek tennénk fel a kérdést!

Márpedig ameddig a jelenségnek nincsen egységes fogalmi meghatározása, vagyis míg nincsen konszenzus a téren, pontosan mit is takar a jelenség, addig igen nehézzé válik a hatékony fellépés megszervezése.

A többféle értelmezés oka leginkább újdonságában keresendő. E jelenség, ellentétben a hagyományos terrorizmussal, nem a való világban zajlik, hanem virtuális számítógépes hálózatokon – jóllehet a hálózatok is valóságosak, mégis egy virtuális teret alkotnak.

Mondani sem kell, a politikusok, (biztonsági és informatikai) szakemberek és főként a média figyelmét gyorsan felkeltette e jelenség.

E tény nem is meglepő, hiszen ahogy a számítástechnika és a számítógépes hálózatok egyre inkább életünk és társadalmaink alapvető részévé válnak, továbbá egyre több információt tárolunk rajtuk, kiszolgáltatottabbá válunk hibátlan működésüknek.

Az előbbiekre tekintettel valóban ijesztőnek tűnhet a lehetőség, hogy egyes egyének, vagy csoportok a névtelenség és a nehezen azonosíthatóság védőernyője mögé bújva, meghatározott motívumok szerint, támadást indítanak az egyre komplexebbé – így egyre sebezhetőbbé – váló számítástechnikai rendszerek és alapvető, kritikus infrastruktúrák ellen, számítógépek és virtuális információk felhasználása révén.

Jóllehet a veszély mértéke semmiképpen sem elhanyagolandó, mindazonáltal ez eddig egyetlen nagyobb támadást sem jelentettek!

E tény felveti a kérdést: *egyáltalán, mennyire kell komolyan venni e jelenséget?*

Jelen cikkben a kiberterrorizmus jelenségét kívánom bemutatni, rávilágítva jellemzőire, elkövetőire, az elkövetés módszereire, a terroristák eszköztárára, a jelenség veszélyességére.

Fogalma

A kiberterrorizmus fogalmának meghatározása előtt szükségesnek tartom meghatározni a terrorizmus fogalmát is, hiszen a kiberterrorizmus a terrorizmus egyik megjelenési formája!

A *terrorizmus* az erőszak alkalmazásának vagy az azzal való fenyegetésnek olyan stratégiája, amelynek elsődleges célja félelem, zavar keltése és ennek révén meghatározott politikai eredmények elérése, vagy a hatalom megtartása.[1]

Az iménti definíciónak három lényegi eleme

– az erőszak alkalmazása, vagy azzal fenyegetés,
– politikai célok,
– félelem-, zavarkeltés.

A két jelenség közötti kapcsolat miatt nyilvánvalóan a kiberterrorizmusnak is bírnia kell e három jellemzővel.

Az egyes fogalomalkotási kísérletek bemutatása előtt ki kell emelni, hogy a jelenség pontos definiálását főként két tényező nehezíti.

– *Egyrészt* a média kiemelt figyelmet fordít e jelenségre, az újságírók azonban a pontos meghatározás helyett a jelenség felnagyításában, minél drámaibb színben feltüntetésében érdekeltek, megtévesztve az olvasókat.
– *Másrészt* gyakori, hogy a számítógépekhez kapcsolható jelenségek elnevezése során pusztán a „cyber", „computer", „information" stb. kifejezéseket illesztik egy már meglévő kifejezés elé, anélkül hogy pontosan meghatároznák azok lényegét.

1 http://hu.wikipedia.org/wiki/Terrorizmus

Jó példa erre a kiberterrorizmus is, hiszen e jelenséget rengeteg kifejezéssel illetik: *infowar, netwar, cyberterrorism, virtual warfare, digital terrorism, computer warfare* stb.[2]

Az iménti kitérő után, a teljesség igénye nélkül, íme, néhány meghatározás.

Az *FBI* a következő fogalmat alakította ki: *A kiberterrorizmus olyan bűncselekmény, amelyet számítógépes rendszerek, programok, adatok – polgári célpontok – ellen a nemzetnél kisebb csoportok vagy egyének intéznek politikai célok elérése érdekében.*[3]

Az amerikai nemzetiinfrastruktúra-védelmi központ (National Infrastructure Protection Center; NIPC) meghatározása a következőképpen hangzik: a kiberterrorizmus *olyan bűncselekmény, amelyeket számítógépekkel és telekommunikációs eszközökkel úgy hajtanak végre, hogy azok rombolják és/vagy megzavarják a szolgáltatások működését, zavart és bizonytalanságot keltve ezzel a lakosságban. Ezen akciók célja a kormányzat vagy a lakosság erőszakos befolyásolása a szervezet egyéni politikai, társadalmi vagy ideológiai céljai érdekében.*

Dorothy Denning a következőket érti kiberterrorizmuson: *Olyan jogellenes támadás, vagy azzal fenyegetés, amely számítógépek, hálózatok és az azokban tárolt adatok, információk ellen irányul, és célja a kormányzat vagy a lakosság megfélemlítése, vagy kényszerítése politikai, társadalmi célok elérése érdekében. Továbbá elengedhetetlen feltétel, hogy az erőszakos támadás személyek vagy tárgyak ellen irányuljon, de legalább kellő fenyegetést jelentsen ahhoz, hogy megfelelő mértékű félelmet keltsen.*[4]

Elhatárolása más hasonló jelenségektől

Hactivizmus – kiberterrorizmus

Az előbbi néhány meghatározás számbavétele után elengedhetetlen megkülönböztetni a kiberterrorizmust a *hacktivizmus* néven ismert jelenségtől. E megkülönböztetés két ok miatt is lényeges: egyrészt hasonló jelenségekről van szó; másrészt egyesek kifejezetten tagadják a kiberterrorizmus létezését, és csupán hackerkedésnek, hactivizmusnak tekintik.

2 Gabriel Weimann: Terror on the Internet. United State of Peace Press, Washington D.C., 2006, pp. 151–152.

3 Kathryn Kerr: Putting cyberterrorism into context. Computer Crime Research Center, October 9, 2004, http://www.crime-research.org/articles/putting_cyberterrorism/

4 Uo.

Az hactivizmus nem más, mint a hackerkedés és a politikai tevékenység, mozgalmak egyvelege. A hacktivisták (a hacker és az aktivista keveréke) és az „egyszerű" hackerek közötti legnagyobb különbség, hogy a hackerek tevékenységét nem politikai célok motiválják.

Ellentétben a kiberterrorizmussal, a hacktivizmus fegyvertára „mindösszesze" négy elemből áll:

– virtuális blokádok létrehozása,
– e-mail támadások, bombázás,
– hackelés és elektronikus betörés,
– vírusok és egyéb kártékony programok alkalmazása.

A *virtuális blokád* a valóságban is létesíthető blokádok, akadályok elektronikus megfelelője. Ennek keretében politikai aktivisták ellátogatnak a céloldalra, és megpróbálják – folyamatos forgalom létesítése révén – oly mértékben túlterhelni az oldalt, hogy az összeomoljon, mások számára elérhetetlenné váljon.

Az *e-mail bombázás* keretében a támadók több megoldás közül is választhatnak. Elsőként a célpont elektronikus levelezési címére egyszerre több száz vagy több ezer üzenetet, illetve annál kevesebb, de nagyméretű csatolmányokkal ellátott levelet küldenek, igen rövid időn belül *(Mass mailing).*

A második megoldás, amikor a célpont elektronikuslevél-címét bejegyzik több levelezési listára is, így a célpont hatalmas mennyiségben kap leveleket, ráadásul ebben az esetben nehezebb védekezni is, mivel sok helyről érkeznek üzenetek *(List linking).*

A levélbombázás e két esete egyrészt leterheli vagy megbénítja a levelezési fiókot, másrészt megtölti, így a fontos üzenetek nem feltétlenül érnek célba.

Az e-mail bombázás harmadik eseteként is felfogható, amikor a címzett számszakilag nem kap sok üzenetet, de azokhoz kártékony programokat kapcsolnak (sok esetben, a vírusirtók kijátszása céljából, tömörített állapotban) *(Zip bombing).*[5]

A sokak által jól ismert *spammelés* az e-mail bombázás egyik típusa, mégis jelentős különbséggel bír az ismertetett esetekhez képest.

A spam (kéretlen üzenet) küldése esetén egy vagy több e-mailt küldenek szét több (általában több száz) címzett részére, tehát a spammelésnél a cím-

5 http://en.wikipedia.org/wiki/E-mail_bomb

zettek száma a lényeges, ellentétben az említett esetkörrel, ahol a leveleket egy címzett kapja!

A *hackelés és elektronikus betörés* általánosságban engedély nélküli behatolást jelent számítástechnikai rendszerekbe, különböző célok elérése érdekében.

A hactivisták konkrétan az informatikai rendszereken tárolt olyan adatok (pénzügyi, üzleti, politika információk stb.) megszerzése érdekében törnek fel számítógépeket, számítógépes hálózatokat, amiket a későbbiekben felhasználhatnak politikai céljaik elérése érdekében.

A *vírusok és egyéb kártékony* programok működésük során – a valós vírusokhoz hasonlóan – folyamatosan többszörözik magukat, és megfertőzik a célszámítógépet, a tulajdonos tudta nélkül.

A vírusok különféle, akár jelentős károkat okozhatnak – például: adatvesztés, adatmódosítás, a rendszer lassítása vagy tönkretétele, politikai üzenetek továbbítása stb.

Az iménti ismertetésből is egyértelműen látszik, hogy a hactivizmus eszköztára széles körű, továbbá nagyobb szakismeret és nehézség nélkül alkalmazható.

Mint már korábban is kiemeltem, a hacktivizmus – akárcsak a vizsgált jelenség – politikailag motivált cselekedeteket takar, a két jelenség mégsem keverendő össze. A hacktivisták célja lehet figyelemfelhívás, az ellenfél ellehetetlenítése, megzavarása, de semmilyen körülmények között sem emberölés, megfélemlítés. Az előbbieken túl hangsúlyozni kell, hogy a két jelenség közötti határ elég keskeny, és könnyen elmosható, különösen akkor, ha a terrorista csoportok hackereket bérelnek fel, vagy saját maguk képeznek ki, illetve ha a hacktivisták kulcsfontosságú (kritikus) ellátórendszereket kezdenek támadni.[6]

A kiberterrorizmus lényege

Az átlagember – már csak a jelenséggel kapcsolatos véleménykülönbségek miatt is – a ténylegesnél több mindent sorolhat a kiberterrorizmus körébe, így célszerű tisztázni, mi *nem* kiberterrorizmus.

Nem tekintendő kiberterrorizmusnak:

– az ismert terrorista csoportok tagjai, támogatói közötti kommunikáció és adatátvitel biztonsága céljából *titkosítási technológiák alkalmazása,*

6 Gabriel Weimann: i. m. 157. o.

– az ismert terrorista szervezetek által különféle *kommunikációs megoldások alkalmazása* toborzási, támogatószerzési, szervezési, valamint propagandaterjesztési célból,
– egyes kibertámadási *technikák terroristák általi esetleges használata*, ami nem okoz jelentős károkat vagy félelmet a lakosság körében,
– olyan országból érkező *port-*[7] *szkennelés*[8], amely feltehetően támogat terrorista szervezeteket.[9]

Az előbbi negatív és leíró definíciókon, valamint csoportosításon túl a jelenség pontos megértéséhez fel kell tenni két lényeges kérdést:
– Léteznek-e olyan célpontok, amelyek támadása révén a terroristák elérhetik céljaikat?
– Ha léteznek alkalmas célpontok, vannak-e olyan személyek, akik képesek végrehajtani a támadásokat?[10]

Támadható rendszerek

Az első kérdést szinte fölösleges feltennünk, hiszen a válasz csakis igen lehet. A terroristák rengeteg célpont közül választhatnak, túlságosan is sok közül.

Mielőtt azonban átlépnénk a második és egyben lényegesebb kérdésre, célszerű alaposabban megvizsgálni a célpontokat, mivel azok vizsgálata révén, legalábbis részben, választ kapunk a második kérdésre is.

A célpontok számbavételekor mindenképp ki kell emelni, hogy napjaink társadalmai jelentős mértékben függenek az információs technológiai eszközök megbízható működésétől, ami jelentős veszélyeket rejt magában.

Gondoljunk csak arra, hogy az egyes társadalmak különböző területein (gazdaság, állami szektor, pénzügyi világ stb.) nélkülözhetetlenné váltak eme eszközök, mindamellett a számítástechnikai eszközök jelentős mértékű használata magával hozta az egyes rendszerek sebezhetőségét és támadhatóságát.

Általánosságban elmondhatjuk tehát, hogy minden olyan rendszer, amely valamilyen formában kapcsolódik a kibertérhez, potenciális célpontnak tekinthető a kiberterroristák számára (is).

7 *Port:* hálózatba kötött számítógépek, számítástechnikai eszközök egymás közötti kommunikációját lehetővé tevő csatlakozási pont. Lényegében az egyes eszközök közötti adatforgalom lehetőségét megteremtő kapu.
8 *Portszkennelés:* hálózati helyek portjainak vizsgálta, meghatározott cél érdekében.
9 Kathryn Kerr: i. m.
10 Gabriel Weimann: Cyberterrorism: How Real Is the Threat? United States Institute of Peace, May 2004, http://www.usip.org/pubs/specialreports/sr119.html

Értelemszerűen a terroristák kizárólag olyan célpontokat fognak támadni, amelyek egyrészt kellően sebezhetők, másrészt a támadás révén elérhetik céljaikat. E két feltételnek leginkább a *kritikus infrastruktúrák* felelnek meg.

Célkeresztben a kritikus infrastruktúrák

A kiberterrorizmus elsődleges célpontjai tehát az úgynevezett kritikus infrastruktúrák, számbavételük előtt szükségesnek tartom röviden kitérni az infrastruktúra fogalmának meghatározására.

Általánosságban infrastruktúrán azon eszközök és intézmények összességét értjük, amelyek bár nem részei a közvetlen termelési folyamatnak, viszont annak nélkülözhetetlen feltételei.

Az infrastruktúrákat sokféleképpen lehet csoportosítani, ezek bemutatása nélkül néhány példával szemléltetve, infrastruktúrának minősül: a közlekedés, hírközlés, kereskedelem, vízgazdálkodás, jogrend, adórendszer, szervezetek, állami apparátus, honvédelem, rend- és tűzvédelem, igazságszolgáltatás stb.[11]

Az egyes infrastruktúrák között meg kell különböztetnünk azokat, amelyek leállítása vagy működésük megzavarása súlyos következményekkel járhat, vagyis a kritikus infrastruktúrákat. E fogalmat is sokféleképpen lehet definiálni, de itt csak kettőt említek.

E speciális infrastruktúrák egyik lehetséges megfogalmazás szerint: „*a nemzeti, szövetségi és uniós infrastruktúra azon létfontosságú elemei, melyek jelentős károsodása, üzemzavara vagy megsemmisülése súlyos következményekkel járna a nemzet vagy a nemzetek biztonságára, a gazdaságra, a környezetre és közegészségre, illetve az egyes kormányok, az állam hatékony működésére*”.[12]

Egy általánosabb meghatározás szerint: *kritikus infrastruktúrák alatt olyan, egymással összekapcsolódó, interaktív és egymástól kölcsönös függésben lévő infrastruktúra elemek, létesítmények, szolgáltatások, rendszerek és folyamatok hálózatát értjük, amelyek az ország (lakosság, gazdaság és kormányzat) működése szempontjából létfontosságúak és érdemi szerepük van egy társadalmilag elvárt minimális szintű jogbiztonság, közbiztonság, nem-*

11 Kovács Ferenc: A kritikus infrastruktúra elméleti alapjai. IVB Innovációs Klubnap, 2008. december 11. http://www.ivb.org.hu/documents/INNOVACIOSklub/200812ho/KIelmeletia.ppt

12 Uo.

zetbiztonság, gazdasági működőképesség, közegészségügyi és környezeti állapot fenntartásában.[13]

A teljesség igénye nélkül a legfontosabb kritikus infrastruktúrák:

– energiatermelő és -elosztó infrastruktúrák (különböző típusú erőművek, energiahordozó-kitermelő, -feldolgozó egységek, energiahordozókat szállító vezetékek stb.);
– banki és pénzügyi infrastruktúrák (banki hálózatok, kereskedelmi központok, egyéb pénzügyi szervezetek stb.);
– vízellátó, közmű-infrastruktúrák (víztisztítók, víztározók, vízvezetékek és csatornák stb.);
– távközlési és kommunikációs infrastruktúrák (távközlési és kommunikációs eszközök, számítógép-alapú hálózatok stb.);
– szállító infrastruktúrák (nemzeti légitársaságok, repülőterek, személy- és teherszállítás, út- és autópálya-hálózatok, vasúti hálózatok, vízi szállítóeszközök stb.);
– katasztrófavédelmi infrastruktúrák (rendőrség, tűzoltóság, kórházak és egyéb egészségügyi intézetek, katasztrófaelhárító szolgálatok stb.);
– honvédelmi, katonai infrastruktúrák;
– élelmiszer-ellátási infrastruktúrák.

A felsorolásból is látszik, hogy egymástól különálló rendszerekről van szó, azok mégis legtöbbször feltételezik egymást, és alapjaiban befolyásolják egy egész társadalom működését.

Jelentőségük mellett tovább növeli e rendszerek sebezhetőségét, hogy szinte valamennyi teljesen vagy jórészt számítógépes hálózatokra, vagy ezek egyes elemeire, de mindenképp számítástechnikai eszközökre épül – e rendszerek irányítását és felügyeletét külön számítógépes rendszerek végzik.

Ki kell emelni, hogy a számítógépes hálózatok legtöbb esetben nem zártak, hanem – a minél nagyobb hatékonyság és a kooperáció kiaknázása céljából – kapcsolatban állnak egymással.

Nem nehéz belátni, hogy minél több kapcsolódási pontja van egy rendszernek, annál könnyebben támadható, illetve annál nehezebben védhető, hiszen a nagyszámú kapcsolódási pont felderítése és folyamatos levédése rengeteg erőforrást köthet le.

A nagyszámú kapcsolódási lehetőség mellett a számítógépes rendszerek, illetve a használt programok tökéletlensége is további problémákat vet fel.

13 Uo.

Hiába javítják folyamatosan a programokat, azok sosem lesznek tökéletesek, mindig lesznek kiskapuk, amelyeket felderítve be lehet törni a rendszerekbe!

Mindenképpen hangsúlyoznom kell, hogy e rendszerek nemcsak elektronikus úton, hanem fizikailag – mondhatni a „hagyományos" módszerekkel – is támadhatók, így a védelem megszervezésekor több irányú, különböző típusú (hagyományos, elektronikus) támadással is számolni kell.

A két támadási mód közötti jelentős különbségek igencsak megnehezíthetik a védelem megszervezését.

Az előbbi általános megállapítások mellett ki kell emelni, hogy a legtöbb állam nagy hangsúlyt helyez a kritikus infrastruktúrák, azon belül különösen a haditechnikai, honvédelmi rendszer védelmére, így a kritikus infrastruktúrákon belül meg lehet különböztetni jobban és kevésbé védett rendszereket. Példaként felhozható a fegyverraktárak és a kőolajvezetékek helyzete, mindkettő vitathatatlanul kritikus infrastruktúra, mégis egyértelműen az előbbit védik jobban, már csak lokalizálhatósága miatt is.

Az erősebben védett kritikus infrastruktúrák fizikailag gyakran nagyon nehezen támadhatók, így az elektronikus támadás lehetősége roppant kecsegtető lehet a terroristák számára.

Természetesen az egyes államok gyorsan felismerték e veszélyt, és megfelelő védelmi megoldásokat iktattak be.

E rendszerek többségénél egyedi – kifejezetten a rendszer adottságaihoz igazodó – programokat használnak (amelyek a telepítés előtt esetleg még külön állami hivatal általi ellenőrzésen esnek át), amelyek mellé erős, nehezen feltörhető védelmi megoldásokat párosítottak, nem beszélve arról, hogy a legtöbb ilyen rendszer nem is kapcsolódik közvetlenül az internetre (a kiberterroristák fő mozgási és vadászterülete), így azok kívülről elérhetetlenek a támadók számára.

Az említett megoldások alkalmazása miatt igen kicsi az esélye az erősen védett kritikus infrastruktúrákat érő támadásnak, így a kiberterroristák kénytelenek a kevésbé védett kritikus infrastruktúrák között válogatni, ezek jó része a magánszférában helyezkedik el.

Az alacsonyabb szintű védelem mellé az internet nagymértékű használta is társulhat, ami tovább növeli támadhatóságuk lehetőségét.

A kevésbé védett kritikus rendszerek támadása (például vízvezetékek, elektromos hálózatok stb.) nem feltétlenül fenyeget olyan hatalmas és azonnali pusztítással, mint például a katonai fegyvereket érő támadás, de mégis e

rendszerek megzavarása vagy tönkretétele jelentősen képes megzavarni a lakosság vagy az adott közösség életét.[14]

A kritikus infrastruktúrák mellett mindenképpen számolni kell az előbbi csoportba nem sorolható infrastruktúrák, rendszerek támadásának lehetőségével is.

Vegyünk például egy nagyszámú személyi adatot tartalmazó rendszert, amely ellen intézett támadással a kiberterroristák megszereznek több ezer személyi adatot.

Önmagában e cselekedet veszélyessége messze a kritikus infrastruktúrák ellen intézett támadás szintje alatt marad, mindamellett a megszerzett adatokat felhasználva a terroristák egy későbbi támadás vagy egyéb tevékenykedésük (például bizonyos termékek beszerzése interneten keresztül stb.) során elfedhetik valódi személyazonosságukat, nehéz helyzetbe hozva a hatóságokat, no meg persze azt, akinek ellopták az adatait.

A mai világban az iménti eset alapján számolni lehet a virtuális személyi adatok ellopásával is (közismert és adott személyhez köthető becenevek, belépési adatok, jelszavak stb.), amelyeket a kiberterroristák szintén fel tudnak használni támadásaik előkészítése, végrehajtása során.[15]

Alkalmas elkövetők

A lehetséges célpontok számbavétele után feltehetjük a fontosabb kérdést. Láthattuk, hogy a számítástechnika széles körű használata miatt rengeteg potenciális célponttal kell számolnunk, de vajon létezik olyan megfelelően képzett és főleg motivált elkövetői csoport, amely a számítástechnikai rendszerek tökéletlenségét kihasználva képes terrorcselekményeket végrehajtani a korábban bemutatott rendszerek ellen?

Mielőtt választ keresnénk a feltett kérdésre, szükségesnek tartom megvizsgálni, egyáltalán kik jöhetnek szóba lehetséges elkövetőként.

Akárcsak a számítógépes bűnözés egyéb megjelenési formáinál, a lehetséges elkövetőknek két konjunktív feltételnek kell megfelelniük:

– egyrészt olyan helyzetben kell lenniük, amely lehetővé teszi számukra a számítógép vagy egyéb számítástechnikai berendezés használatát,

14 Joshua Green: The Myth of Cyberterrorism, There are many ways terrorists can kill you—computers aren't one of them. Washington Monthly, November 2002 http://www.washingtonmonthly.com/features/2001/0211.green.html

15 Sarah Gordon: Cyberterrorism? Symantec Security Response. http://www.symantec.com/avcenter/reference/cyberterrorism.pdf, p. 7.

– másrészt megfelelő szinten kell érteniük a technikai eszközökhöz, azok kezeléséhez.

Ezek után vegyük számba, kiknek lehet megfelelő képzettségük ahhoz, hogy terrorcselekményt hajtsanak végre.

Talán nem meglepő módon a sort a *hackerek* nyitják! A hacker – általánosságban – olyan számítástechnikai szakember, aki az átlagosat messze meghaladó szinten ismeri az informatikai rendszerek működését (az ötvenes, de különösen a hatvanas években elsősorban azokat nevezték így, akik a szokásostól eltérő módon használták az új technológiát és kiemelkedő szintű szaktudásukat).

E szakemberek komoly szakismeretük segítségével képesek (lehetnek) egy adott rendszerbe „betörni" (azt engedély nélkül használni), és azon belül különféle módosításokat végrehajtani, avagy információt eltulajdonítani, megváltoztatni. Céljuk szerint a hackerek négy plusz egy csoportját különböztetjük meg:

Az *első* csoportot az úgynevezett „jó vagy etikus hackerek", más néven fehér kalapos hackerek *(white hat hacker)* alkotják. Ők károkozási cél nélkül törnek be rendszerekbe, és a sikeres műveletek után felhívják a rendszergazdák figyelmét a védelmi hiányosságokra, gyenge pontokra, vagyis segítő szándék vezérli őket. E csoporton belül külön kategória, akik eseti vagy állandó megbízás alapján végzik munkájukat, ők a szakértő rendszertesztelők.

A *második* csoportba, a mondhatni „kevésbé jóindulatú szakértők", a fekete kalapos hackerek *(black hat hacker)*, más néven *cracker*ek tartoznak. A köznyelvben általában a hacker kifejezésen kizárólag ezeket a szaktudásukkal visszaélő szakembereket értik, akik fehér kalapos társaikhoz hasonlóan szintén idegen számítógépes rendszerekbe az őket védő védelmi programok kijátszása, feltörése révén jutnak be, de gyökeresen más célokból. A fekete kalapos hackerek céljai igen sokfélék lehetnek: károkozás, haszonszerzés, képességeik tesztelése, erőfitogtatás, kíváncsiság, tapasztalatszerzés, de előfordul, hogy egyfajta sportként tekintenek saját tevékenységükre.

A *harmadik* csoportot az előbbi kettő keresztezését jelentő szürke kalapos hackerek *(grey hat hacker)* alkotják, akik hol legálisan, hol illegálisan tevékenykednek. Ki kell emelni, hogy általában nem önös érdekből vagy károkozási célból tevékenykednek, pusztán illegális cselekedeteket *is* elkövetnek legális munkájuk közben. E csoport egyfajta szürke zónát alkot.

A *negyedik* csoportot a hacktivisták alkotják, akik, mint korábban kiemeltem, olyan hackerek, akik technikai eszközöket használnak politikai, ideoló-

giai, vallási üzeneteik közvetítésére, általában weboldalak feltörése, átalakítása, túlterhelése (például DoS, flood) révén.[16]

A hacktivisták megmozdulására jó példa az 1999-ben amerikai szervereket érő kínai támadás, amely a belgrádi kínai nagykövetséget érő NATO-találat hatására történt.[17]

Végül az *ötödik* csoportba az úgynevezett *script kiddie*-k tartoznak, vagyis a képzetlen, mélyebb számítástechnikai ismeretekkel nem bíró crackerek. Ők a profi hackerek által készített és internetre feltöltött segédprogramok (scriptek) segítségével törnek fel szervereket, vagyis e csoport a szakértő hackerek nélkül nem is létezne. Tekintettel arra, hogy e személyek, magas szintű képzettség hiányában, kilógnak a valódi hackerek sorából, így nem tekinthetjük őket teljes értékű, ötödik csoportnak.

A lehetséges elkövetők sorában a következő csoport a *phreak*ek. A phreak olyan személy, aki telekommunikációs rendszereket – elsősorban telefonhálózatot és ahhoz kapcsolódó eszközöket – tanulmányoz, illetéktelenül igénybe vesz, felhasznál céljai elérése érdekében.

A phreakek tulajdonképpen telekommunikációs szakemberek, szaktudásuk segítségével akár telefonközpontok működését is manipulálhatják. Értelemszerűen a mobiltelefon-hálózatok sem menekülhettek el e csoport elől, különösen a hálózat illetéktelen lehallgatására kell gondolni. A telekommunikációs rendszerek komputerizálása után a phreakek és a hackerek közel kerültek egymáshoz, hiszen mindkét csoport tagjai a számítógépes hálózatok feltörésével, manipulálásával foglalkoznak.

Az említett változás következtében átalakuló *phreaking* jelenségre esetenként H/P (H = Hacking; P = Phreaking) kultúraként hivatkoznak.[18]

Az előbbi csoportok mellett az *ipari kémeket* is fel kell venni a lehetséges elkövetők listájára. Az egyes iparágakban folytatott illegális információszerzés régóta fennálló jelenség, az idők folyamán csupán az elkövetési módszerek változtak. A számítógépek és a számítástechnika elterjedése az iparban mind a tervezés, irányítás és rendszerfelügyelet terén magával hozta annak veszélyét, hogy a számítógépeken és hálózatokon tárolt hatalmas mennyiségű adatokat és információkat illetéktelenek (ipari kémek, konkurens cégek alkalmazottai) megszerezhetik és értékesíthetik.[19]

16 http://en.wikipedia.org/wiki/Hacker_(computer_security)

17 Kovács László: Az információs terrorizmus eszköztára. Robothadviselés 6. Konferencia. Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2006. november 22. Hadmérnök, Különszám, 2007. január http://hadmernok.hu/kulonszamok/robothadviseles6/kovacs_rw6.html

18 http://en.wikipedia.org/wiki/Phreaking

19 Kovács László: i. m.

Hangsúlyozni kell, hogy e kémek nem kizárólag a magánszférában tevékenykedhetnek, a katonai adatok megszerzése és értékesítése révén szintén jelentős bevételre lehet szert tenni.

Tulajdonképpen az ipari kémek – amennyiben a számítógépes hálózatokat használják eszközként a kívánt adatok megszerzésére – is hackerek, de speciális céljaik miatt célszerű külön csoportba sorolni őket. Talán a legveszélyesebb potenciális elkövetők – szemben az előbbi külső támadókkal – éppen a *belső szakértők* és a rendszer működésébe bevont *külső személyek*.[20]

Egy komputerizált szervezet vagy rendszer működtetésében, amelyik rengeteg, esetleg rendkívül fontos adatot tárol, óriási szerep és felelősség hárul a szakértőkre. Szükségesnek tartom kiemelni, hogy nemcsak számítástechnikai szakértőkre kell gondolni, bár kétségtelen, hogy a vizsgált jelenség feltételezi a számítástechnika terén jártas elkövetők létét, de a belső szakértők, a bűnsegéd szerepét betöltve, más végzettségűek is lehetnek. A szakértők több szempontból is veszélyt jelentenek egy rendszerre.

Egyrészt magas szintű hálózati hozzáférésük van, illetve nem számítástechnikai szakember esetén, hozzáférnek a rendszer egyes elemeihez, még akkor is, ha megosztják a jogosultságokat az egyes szakértők között. *Másrészt* szakképzettségük folytán. *Harmadrészt* rendszerismeretük miatt, hiszen leginkább a belső szakértők ismerik a rendszer működését, annak gyengéit, hiányosságait.

A bemutatott veszélyességi tényezők miatt a belső szakértők szinte az ideális elkövetők, hiszen amellett, hogy hatékonyan képesek végrehajtani tettüket, jogosultságuk folytán az összes árulkodó nyomot is eltüntethetik.

Mindezeken túl a belső emberek akkor is veszélyt jelenthetnek, ha maguk nem követnek el semmilyen cselekményt, de kulcsfontosságú adatokat adnak ki harmadik személyeknek, akik aztán a megszerzett adatok birtokában támadhatják és esetleg működésképtelenné tehetik a rendszer kulcspontjait. A külső személyek szintén kaphatnak jelentős mértékű hozzáférési jogokat a teljes rendszerhez vagy egyes elemeihez. Ráadásul a külső személyek esetében még a munkavállalói hűségre sem lehet építeni, hiszen míg egy több éve a szervezetben dolgozó belső szakértő esetén számolni lehet e tényezővel, egy rövid ideig a szervezet keretében dolgozó külső személynél aligha.

A lehetséges elkövetők számbavétele után rátérhetünk a tényleges kérdésre: *A potenciális elkövetők, bár elméletileg képesek végrehajtani (kiber)ter-*

20 Uo.

rorcselekményeket, vajon ténylegesen is végrehajthatnak támadásokat a korábban bemutatott rendszerek ellen?

Mindenképp le kell szögezni, hogy – mivel nincsen feltörhetetlen rendszer – a potenciális elkövetők fel tudják törni a korábban nevesített rendszereket, de nem elegendő feltörni őket, mondhatni, ez a könnyebbik fele! A kívánt eredmény elérése érdekében a rendszer feltörése után megfelelő módosításokat kell végrehajtani.

A mai rendszerek többsége egyszerűen túl bonyolult ahhoz, hogy valódi rendszerismeret nélkül jelentős károkat, vagy akár csak jelentős üzemzavart lehessen előidézni bennük.

Az IBM Global Security Analysis Lab 2002-es jelentése szerint a hackerek csaknem kilencven százalékának nincsen kellő szakismerete, mondhatni amatőrök, így a kritikus rendszereket sem tudnák feltörni, kilenc százalékuk már elég képzett a rendszerek feltöréséhez, de a behatolás ellenére nem lennének képesek jelentős károkat okozni, végül mindössze egy százalékuk kellően képzett és motivált ahhoz, hogy feltört rendszerekben súlyos károkat okozzon, vagy akár megbénítsa őket.

A jelentést alátámasztja *Douglas Thomas*nak, a Dél-kaliforniai Egyetem professzorának vizsgálata is. Thomas több száz hackert hallgatott meg tevékenységük jobb megértése érdekében. Kutatása eredményét a következőképpen összegezte: *„A hackerek túlnyomó többsége, legalább 99 százalékuk részéről elhanyagolható a kiber-terrortámadás veszélye, azon egyszerű ok miatt, mivel az említetteknek egyszerűen nincsen kellő szakismeretük vagy lehetőségük egy olyan támadás végrehajtásához, mely egy kisebb zavarnál többet tudna okozni."*[21]

A külső támadók próbálkozásai mellett, mint már hangsúlyoztam, nagyobb veszélyt jelentenek a belső alkalmazottak, akiknek ráadásul kellő rendszerismeretük is van, így sokkal nagyobb eséllyel okoznak súlyos károkat.

A következő, gyakran hivatkozott eset 2000 márciusában történt az ausztrál Queenslandben, a Maroochy Water Services szennyvízkezelő üzemben. *Vitek Boden*, miután elbocsátották munkahelyéről, egy laptop és egy rádió adóvevő segítségével behatolt az üzem számítógépes rendszerébe, és több pumpa átállításával egymillió liter szennyvizet engedett a Queensland menti vizekbe. Az elkövető előállítása után derült fény arra, hogy Boden a szennyvízkezelő üzem biztonsági rendszerét tervező vállalat dolgozója volt.[22]

21 Gabriel Weimann (2006): i. m. 165. o.

22 http://csrc.nist.gov/groups/SMA/fisma/ics/documents/Maroochy-Water-Services-Case-Study_report.pdf

A kritikus infrastruktúrákat irányító számítógépes rendszerek nem megfelelő védettsége esetén kialakuló veszélyhelyzetek lehetőségének igazolására többször is felhozták a szennyvízkezelő üzemben történteket.

Jóllehet a hasonló esetek súlyos veszélyeket hordoznak magukban, az eset mégis speciális, hiszen a támadást olyasvalaki hajtotta végre, aki jól ismerte a rendszer működését, ráadásul a bosszú vezérelte, és nem politikai, vallási célok, így a hasonló eseteket semmiképpen sem lehet kibertámadásnak minősíteni.

Tekintettel arra, hogy a kritikus infrastruktúrák a külső és a rendszert nem ismerő személyek számára nehezen támadhatók, így elméletben lehetséges, hogy a terroristák – saját dolguk megkönnyítése érdekében – belső embereket szerveznek be. A károkozás mértéke ebben az esetben is csupán korlátozott lehet, egyrészt a rendszerek – jobb esetben a személyzet által kiiktathatatlan – védelmi megoldásai miatt, másrészt a személyzet többi tagja miatt, akik megpróbálnák elhárítani társuk károkozását.[23]

Összegezve az eddigieket, a lehetséges elkövetők többségének lehet megfelelő szintű szaktudása és eszköze ahhoz, hogy számítógépes rendszereket támadjanak, mindazonáltal hiányzik a kellő motivációjuk a súlyos következményekkel járó támadások végrehajtásához.

Az igazi veszélyt tehát nem az említett lehetséges elkövetők jelentik. Jóllehet fejtörést okozhatnak a biztonsági szakembereknek, és mindenképp szükséges velük számolni, mint lehetséges veszélyforrással, a legnagyobb veszélyt pontosan azok a csoportok jelentik, amelyek a való világban is terrorcselekményeket hajtanak végre.

A kiberterrorizmus struktúrája

1999 augusztusában a kaliforniai Montereyben található Terrorizmus- és irregulárishadviselés-vizsgáló központ (Naval Postgraduate School Center for the Study of Terrorism and Irregular Warfare) jelentése *(Cyberterror: Prospects and Implications)* a következőképpen rendszerezi a kiberterrorizmus struktúráját:

a) Egyszerű, szervezetlen: e szervezetek képesek a mások által készített programokkal egyszerűbb támadásokat végrehajtani egyéni rendszerek ellen. Az ilyen szervezeteknek általában semmilyen célpontelemzési, irányítási és vezetési, valamint önfejlesztési képességük nincs.

23 Joshua Green: i. m.

b) Fejlett, szervezett: elméletileg már több és nagyobb rendszerek, illetve hálózatok ellen is végrehajthatnak sikeres támadásokat, valamint egyszerűbb programokat is készíthetnek. Az ilyen szervezetnek alapvető célpontelemzési, irányítási, vezetési és fejlődési képessége van.

c) Összetett, koordinált: e szervezet már összehangolt, súlyos zavart és esetleges károkat okozó támadások végrehajtására is képes. A szervezet tagjai már valódi hackeléshez használt programokat is készíthetnek. Magas szintű célpontelemzés, irányítás, vezetés és önfejlesztő képesség jellemzi e csoportokat.

A vizsgálat összegzése szerint egy az alapoktól induló csoportnak legalább kettő-négy év kell a szervezett, és hat-tíz év az összetett szint eléréséhez. Természetesen külső források bevonásával erősen csökkenthető ez az időintervallum.[24]

Miért használnák a kiberterroristák az internetet, mik a céljaik?

Az internet előnyei a kiberterroristáknak

Feltehetjük a kérdést: a számítástechnika felhasználásával elkövetett terrorcselekmények vajon miért lehetnek vonzóbbak a terroristák számára a hagyományosnak nevezhető módszereknél akkor, amikor több évet kell tölteniük a kellő szakismeret megszerzésével, programokat és számítástechnikai eszközöket kell beszerezniük, és a siker, az egyre fejlettebb védelmi megoldások következtében, messze nem garantált?

Ráadásul a hagyományos elkövetési módszerek esetében jóval rövidebb idő alatt hozzá lehet jutni a szükséges eszközökhöz.

Több előnye is van az elektronikus útnak:

– *Egyrészt* messze olcsóbb, mint a hagyományos módszerek, hiszen a támadás megvalósításához csupán számítógépre és internetkapcsolatra van szükség, ezek, ellentétben például a robbanóanyagokkal, fegyverekkel, könnyedén, bármely számítástechnikai üzletben, jogszerűen beszerezhetők, ezzel is csökkentve a lelepleződés veszélyét.

24 Dorothy E. Denning: Cyberterrorism. Testimony before the Special Oversight Panel on Terrorism Committee on Armed Services U.S. House of Representatives by Georgetown University May 23, 2000 http://www.cs.georgetown.edu/~denning/infosec/cyberterror.html

– *Másrészt* a kiberterrorizmus személytelenebb, mint a hagyományos módszerek. Ez esetben ugyanis a terroristáknak nem szükséges fizikailag is jelen lenniük az elkövetés helyszínén (vagy annak közelében), ez pedig szintén a lelepleződés veszélyét csökkenti. Nem is beszélve a célpontig és vissza vezető utazás közben fennálló lelepleződés veszélyéről (ellenőrző pontok, rendőrségi útzárak, határok stb.). Hagyományos társával ellentétben a kiberterrorista fantomnév, vagy korábban megszerzett létező személy valós vagy interneten használt adataival beléphet weboldalakra, rendszerekbe, ezáltal jelentősen megnehezítve valódi személyazonosságának kiderítését, ráadásul más személyre terelhetik a gyanút.
– *Harmadrészt* a célpontok nagy száma is pozitív tényezőként esik latba. A korábban bemutatott célpontok igen széles körén is látszik, hogy a kiberterroristák szabadon válogathatnak kormányzati, illetve magánszférában lévő célpontok (számítógépes rendszerek, kritikus infrastruktúrák) között. A célpontok nagy száma szinte garantálja, hogy előbb-utóbb még a kevésbé képzett elkövetők is találnak olyan célpontot, amely nem kellően védett, vagy olyan gyenge pontot, amelyen keresztül kellő mértékű zavart kelthetnek egyes rendszerekben. További előnyt jelentenek a kiberterroristák számára a számítógépes hálózatok és elsősorban az internet felépítéséből és jellemzőiből következő támadási és adatszerzési lehetőségek. Példának okáért egy jelentős károkkal fenyegető kártékony program szétküldése, amely gyorsan terjed az interneten, tökéletes „elterelő hadművelet" is lehet a támadások előtt.
– *Negyedrészt* a kibertámadásokat számítógépekkel hajtják végre, így, ellentétben a hagyományos terroristákkal, nem szükséges felkészíteni őket, sem testileg, sem lelkileg. Az emberveszteség lehetősége szinte kizárt, a lelepleződésé pedig jóval alacsonyabb, mint a hagyományos támadások esetén. A kiképzés kiiktatása idő és leginkább jelentős költségek megtakarítását jelenti. Jóllehet egyfajta kiképzésre a kiberterroristáknak is szükségük van, mégpedig kellő számítástechnikai jártasságot kell szerezniük, de ez könyvekből is elsajátítható. Esetükben nincs szükség külön táborra és kiképzőhelyre, a testi kiképzéshez szükséges felszerelések beszerzésére stb.
– *Ötödrészt* a kibertámadásokkal jóval több ember életét befolyásolhatják, gondoljunk például a víztisztító rendszerekre. A nagyobb veszély – még ha csak lehetőség is – nagyobb visszhangot és nagyobb médiaérdeklődést vált ki, így az adott terrorszervezet nagyobb nyilvánossághoz juthat.[25]

25 Gabriel Weimann (2004): i. m.

Az előbbi felsorolásból is kitűnik, hogy jó néhány igen jelentős előnnyel kecsegtet a számítástechnika alkalmazása mind a hagyományos, mind a kiberterroristák számára, de e csúcstechnika nyújtotta lehetőségeket nemcsak a konkrét támadások végrehajtásakor használhatják ki, hanem egyéb területeken is.

Kommunikáció, koordináció, tervezés, információszerzés – könnyen belátható, hogy a terroristák – akár a hagyományos, akár a modern módszereket választók – kezében az internet nagy segítséget nyújthat mind a kommunikáció, mind a szervezés területén. Az interneten több kapcsolattartási mód közül is válogathatnak az elkövetők (például chatszobák, weboldal-üzenőfal, azonnali üzenet küldésére alkalmas programok), ezek segítségével személyes kapcsolat nélkül szervezhetik akcióikat. A személyes kapcsolat hiánya tovább nehezíti a nyomozó hatóságok munkáját is, hiszen egy sikeres rajtaütéskor egyszerre csak egy terroristát foghatnak el, aki ráadásul nem is ismeri társai valódi személyét, így információkat sem adhat róluk.

Az internet viszonylagos névtelensége, illetve esetlegesen lopott adatok segítségével valós személyazonosságuk tekintetében a terrorista szervezet tagjai egymást is megtéveszthetik.

Akárcsak a való világban, az interneten és egyéb számítógépes hálózatokon alkalmazhatók különféle titkosítások. A könnyedén beszerezhető titkosító programok akár erős titkosítással is kódolhatják a kívánt dokumentumot, és segítségükkel a terroristák ilyen formában is eljuttathatják társaiknak különösen fontos adataikat.

Az erős titkosítások a világ titkosszolgálatainak rémálmai, így nem csoda, hogy igyekeznek kiskapukat beépíttetni a kereskedelmi forgalomba kerülő titkosító eszközökbe, az ezek által generált kódot, egyéb támpont hiányában, kizárólag „nyers erővel" *(brute force)* – vagyis az összes létező kombináció végigpróbálása révén – lehet feltörni. Mindazonáltal a terrorista szervezetek könnyen toborozhatnak programozókat is, ők pedig olyan algoritmust készítenek, amelyben nincsenek kiskapuk…

A titkos üzenetváltás kevésbé egyértelmű, de a történelemben és a terroristák által is széles körben alkalmazott változata a *szteganográfia*, vagyis az üzenet elrejtésének tudománya. E megoldás során látszólag érdektelen hordozókba építenek be a külső személyek számára láthatatlan vagy értelmezhetetlen titkosítani kívánt információkat. Néhány példa: üzenetek „zajos" kép- vagy hangfájl legkisebb bitjeibe rejtése; futtatható programokban való elrej-

tés; kódolatlan üzenetek, amelyekből adott rendszer alapján olvasható ki az információ.[26]

Az interneten keresztüli kommunikáció nemcsak az adott szervezet tagjai között, hanem terrorszervezetek egymás közötti viszonyában is elképzelhető, ez szintén jelentős információforrás lehet.

A tervezés terén is támaszkodhatnak az internetre, hiszen információkat, programokat, adatokat szerezhetnek, sok esetben teljesen legálisan, segítségükkel megszervezhetik támadásaikat.

Az információk megszerzése kapcsán hangsúlyozni kell, hogy az interneten található elképesztő adatmennyiség miatt megfelelő keresőszavak segítségével, vagy megfelelő weboldalak látogatásával könnyedén hozzá lehet jutni szinte bármilyen, az internet előtt csak jelentősebb nehézségek árán megszerezhető információhoz. Ráadásul nem pusztán leírásokat találhatunk, hanem akár szemléltető videókat, interaktív térképeket, műholdfelvételeket is.

Toborzás, propaganda terjesztése, források szerzése – a kommunikáció és szervezés mellett az új tagok toborzása, nézetek terjesztése terén szintén hatalmas lehetőségeket nyújt az internet mind a hagyományos, mind a kiberterrorista szervezeteknek. Tekintettel arra, hogy a terroristák nem férnek hozzá a televíziók és rádiók műsorszórásához – hacsak támadásaik révén közvetetten nem –, így nézeteik terjesztésének egyetlen útja az internet. A különböző terrorista szervezetek weboldalaikon, illetve a követőik által létesített további oldalakon (például *Hizbullah: The Party of God*[27]) nyíltan toborozhatnak tagokat, hirdethetik nézeteiket. A weboldalakon a lehetséges új tagok toborzásának számos módszerét is bevethetik. A céljaikat bemutató írások mellett eddigi akcióikról, vezetőikről, ellenségükről készített képeket, videofelvételeket helyezhetnek el, adományokat gyűjthetnek.[28]

Az internet hivatkozási lehetőségeit kihasználva más oldalakon elhelyezhetnek olyan hivatkozásokat, figyelemfelkeltő animációkat, amelyek megragadják az emberek figyelmét, és elvezetik őket a kívánt oldalakra.

A kiberterroristák fegyvertára

E fejezetet akár egyetlen szóban is össze lehetne foglalni, hiszen a kiberterroristák alapvető fegyvere – és célpontja is – maga a számítógép. Persze

26 http://hu.wikipedia.org/wiki/Szteganográfia
27 http://almashriq.hiof.no/lebanon/300/320/324/324.2/hizballah
28 Kovács László: i. m.

utóbbi rengeteg elkövetési módszert és további támadási eszközöket foglal magában.

Mielőtt rátérnénk az egyes eszközökre, általánosságban elmondható, hogy egy új technológiai eszköz kifejlesztése után számolni kell az új eszköz bűnözők általi felhasználásával is – ez a kiberterrorizmus terén sincs másként. Másképp fogalmazva, a kiberterrorizmus – akárcsak a számítógépes bűnözés – fejlődése szorosan összefügg a számítástechnika fejlődésével. A számítástechnika terén kevésbé jártas egyének feltehetik a kérdést: *egy olyan robusztus hálózat, mint az internet, illetve egyéb hálózatok, hogyan támadható hatékonyan?*

Az elkövetők elég széles eszköztárból válogathatnak!

Az eszközök alapvetően két csoportba sorolhatók: az elsőt a rosszindulatú szoftverek mint eszközök, a másodikat a részben ezeket felhasználó támadási módszerek alkotják.[29]

Hangsúlyozni kell, hogy a kiberterroristák által felhasználható eszközök legnagyobb veszélyei, hogy az elkövetéskor nem kell a támadás helyszínén tartózkodniuk; akár több ezer kilométer távolságból is csapást mérhetnek, mégpedig nehezen felderíthető módon. Így könnyen előfordulhat, hogy az esetleges üzemzavart a támadás után nem is kapcsolják külső támadáshoz, hanem belső meghibásodásnak tulajdonítják.[30]

Eszközök: a rosszindulatú szoftverek (malware)

A *malware*-ek az olyan rosszindulatú számítógépes programok összefoglaló elnevezése, amelyek a felhasználók engedélye nélkül hatolnak be számítógépekbe, és azokban nem kívánt változásokat idéznek elő, egyebek között: erőforrásokat kötnek le; adatokat módosítanak, törölnek; egyéb jellegű kárt okoznak, vagy ennek veszélyét hordozzák magukban. A malware-ek nem összekeverendők a hibás programokkal, amelyek céljukat tekintve hasznos programok, de valamilyen programozási hiba maradt a szoftverkódban.[31]

A malware-ek két csoportját különböztethetjük meg, előbbibe a programalapú (különösen: vírusok, programférgek, trójai programok, keyloggerek stb.), utóbbiba a szöveges malware-ek (spam, hoax, phishing, pharming stb.) tartoznak. Ezek közül csak a legjelentősebbeket veszem számba.

29 Uo.
30 http://ntrg.cs.tcd.ie/undergrad/4ba2.02/infowar/terrorism.html
31 http://en.wikipedia.org/wiki/Malware

Programalapú malware-ek

A számítógépes *vírusok* olyan kisméretű, rosszindulatú programok, amelyeket arra terveztek, hogy saját másolataikat más végrehajtható programokban vagy dokumentumokban elhelyezve megfertőzzenek számítógépeket.[32] A számítógépes vírusok működése megfelel a biológiai értelemben vett vírusok viselkedésének, így általában használhatatlanná teszik vagy törlik a megfertőzött állományokat, de előfordul, hogy „csak" túlterhelik a rendszert, és egyéb kárt nem okoznak. Veszélyességük különösen abban áll, hogy a számítógép bármely részét megfertőzhetik (alkalmazások, dokumentumok, rendszervírus stb.), mégpedig minden előjel nélkül, és a felhasználó már csak a vírus tevékenykedésének következményével szembesül.

A programférgek (worm) olyan rosszindulatú programok, amelyek programkódjaikat nem más programok belsejébe építik be (vagyis nincs szükségük gazdaprogramra), hanem azt önálló fájlban tartalmazzák, és ezt másolva sokszorozódnak. A sokszorosítás közben módosítják azokat a fájlokat is, amelyekkel a programindítás lehetséges. A programférgek észlelése és működésük megakadályozása nehezebb feladat, mint a vírusoké. A vírusok esetén a vírusirtó programok az egyes programanomáliák alapján könnyen felderítik a vírusokat, a programférgek azonban nem módosítják a programfájlok kódjait, így az észlelésük is nehézkesebb.[33] A wormok saját másolataikat a megtámadott számítógép merevlemezén készítik el, és hálózati kapcsolódási pont esetén a hálózaton keresztül továbbítják is más gépeknek.

A trójai falovak olyan programok, amelyek működése a felhasználó megtévesztésén alapul. E programok látszólag hasznosnak tűnnek, de a valóságban nem kívánt műveleteket hajtanak végre, általában terhelik a rendszert, adatvesztést okoznak. Lényeges tulajdonságuk a vírusokhoz képest, hogy általában nem többszörözik önmagukat, terjedésük egyéni támadások következménye. Előfordulhat, hogy nem tartalmaznak rosszindulatú programkódot, de ettől függetlenül többségük úgynevezett hátsó ajtó telepítését is elvégzi, amely a fertőzés után hozzáférést enged a célszámítógéphez.[34]

A hátsóajtó- (backdoor) programok szoftverekbe épített, a felhasználók számára láthatatlan kiegészítések, amelyek bizonyos kiválasztott személyek részére (illetéktelen) hozzáférést engednek a programokhoz, számítógéphez, vagy az azokon tárolt adatokhoz. A backdoor terjesztője vagy használója a

32 http://hu.wikipedia.org/wiki/Számítógépes_vírus
33 http://www.antivirus.hu/virved/displayer.php?site=antivirus&page=40.10
34 http://hu.wikipedia.org/wiki/Trójai_faló_(számítástechnika)

hátsó ajtó segítségével az interneten keresztül a megtámadott gépen tárolt adatokat megtekintheti, módosíthatja, törölheti, vagy megfigyelheti a felhasználót.[35]

A pottyantók (dropper) olyan programok, amelyek önállóan szaporodó vírusokat, trójai programokat, programférgeket vagy egyéb rosszindulatú programokat juttatnak be a megtámadott rendszerekbe oly módon, hogy miután beférkőztek a számítógépekbe, legyártanak meghatározott számú, az operációs rendszer által futtatható vírust vagy egyéb ártó programot, majd futtatják őket.[36]

Szöveges malware-ek

Az előbbi programokkal ellentétben léteznek szöveges, nem programalapú malware-ek is, amelyek szintén veszélyt jelenthetnek. A leggyakoribbak: kéretlen üzenetek (spam, hoax), adathalászás (phishing, pharming).

Kéretlen üzenetek (spam) – a spamek a fogadó által nem kért, elektronikusan (jobbára: e-mailben) tömegesen küldött hirdetések, felhívások, igen változatos témákban. A nagy számban szétküldött kéretlen levelek hátrányos következményei egyrészt a lefoglalt tárhelyben, másrészt a lekötött sávszélességben nyilvánulnak meg.

Hoax – a kéretlen levelek egyik típusa, általában szintén e-mailben terjesztett álhír-lánclevelek különféle változata. A megtévesztés gyakran kiegészül honlapokkal, illetve esetenként a hagyományos média is hajlamos átvenni. Fontos hangsúlyozni, hogy a hoax célja a célközönség megtréfálása, nagyon ritkán irányul illegális célokra.[37]

Célja ellenére hatásai a spaméivel azonosak, mivel a hoax annál hatásosabb, minél több ember tudomást szerez róla, így sok szétküldés esetén szintén sávszélességet és tárhelyet köt le. Nem is beszélve arról, hogy mellékletként egyéb rosszindulatú programot lehet csatolni hozzá.

Adathalászat (phishing) – az emberek hiszékenységére építő csalási módszer, amelynek során egy csaló egy ismert cég (általában pénzintézet) nevében e-mailt vagy azonnali üzenetet küld a címzettnek, és például üzemzavarra vagy adategyeztetésre hivatkozva megpróbálja – válaszlevél keretében vagy a cég weboldalához nagyon hasonlító weboldal segítségével – kicsalni

35 http://www.virushirado.hu/lexikon.php?l=b
36 http://www.antivirus.hu/virved/index.php?CN=40.4&CIE=0
37 http://hu.wikipedia.org/wiki/Hoax

a felhasználó személyi adatait (azonosítók, jelszavak, bankkártyaszámok stb.). A másik jellemző levéltípus esetén hatalmas összegű internetes lottónyeremény átutalásához kérik a fogadó adatait. Fontos kiemelni, hogy a levelek minden esetben hivatalos megkeresés látszatát keltik.

Pharming – a phishing fejlettebb változataként, ugyancsak csalárd eljárásról van szó. A kétfajta csalási módszer között két jelentős különbség van. Egyrészt az utóbbi esetben kizárólag az áloldalon lehet megadni a kért adatokat, másrészt egy rosszindulatú szoftver segítségével a csaló az eredeti lapról a saját hamisított weboldalára téríti a felhasználót; vagyis a felhasználó hiába írja be helyesen a cég weboldalcímét, a böngésző az áloldalra vezeti.[38] A megszerzett adatokkal pedig már könnyedén visszaélhetnek a csalók.

Eszközök: greyware-ek

A *greyware* kifejezés olyan programokat takar, amelyek nem okoznak olyan károkat, mint a malware-ek, de jelenlétük bosszantó, zavaró. E programok főként a hálózatba kapcsolt számítógépek teljesítményét befolyásolják, illetve lehetőséget adnak károkozó cselekmények végrehajtására. Ahogy nevük is jelzi, egyfajta szürke zónát jelentenek a normális programok és a malware-ek között. A greyware-ek közé sorolható programok különösen a kémprogramok *(spyware)*, reklámprogramok *(adware)*, a *trackware*.

Kém- és reklámprogramok

A *kémprogramok* olyan főként az interneten terjedő rosszindulatú programok, amelyek célja, hogy megszerezzék a megfertőzött számítógép felhasználójának személyes adatait (egyebek között felhasználói nevek, belépési jelszavak, bankkártyaszám stb.), és elküldjék a kémprogram felhasználójának, és később akár jogszerűtlen cselekményekhez is felhasználhatják. A kémprogramok feltelepülése észrevétlenül történik, a felhasználó figyelmetlenségének és a számítógép böngészőprogramja biztonsági hiányosságainak kiaknázásával. Kizárólag többféle védelmi program kombinációjával lehet ellenük hatékonyan védekezni (víruskereső programok, intelligens tűzfalprogramok, illetve spyware-ek felismerésére készített programok használata).[39] A *reklámprogramok* olyan szintén az interneten terjedő programok, amelyek célja, hogy egy termé-

38 http://www.cert.hu/index.php?option=com_content&task=view&id=378&Itemid=155
39 http://hu.wikipedia.org/wiki/Spyware

ket és annak készítőjét vagy egy céget reklámozzanak. Jóllehet több reklámprogram egyben kémprogram is, mégis jelentős különbség van a kettő között. Amíg a kémprogramok mindig rejtetten működnek és szerzik meg a felhasználó adatait, addig a reklámprogramok, érthető módon, jól láthatóan, általában a böngészőprogramban jelenítenek meg hirdetéseket, amelyek sávszélességet vonnak el a felhasználótól, adott esetben közvetetten okozva kárt.[40]

Kiberterrorista módszertan

Számos olyan eljárási módszer létezik, amelyekkel – a rosszindulatú programok felhasználásával, illetve kiegészítésükkel – károkat lehet okozni egy hálózatban. Tekintettel arra, hogy a hálózatok általában kapcsolatban állnak más hálózatokkal, a károk tovább növelhetők, hiszen egy hálózat kiesése más hálózatokban is károkat okozhat, de legalábbis hatással lehet annak működésére.
A legjelentősebb támadási módszerek:

– Denial of service.
– Distributed denial of service.
– Flooding.
– SMTP backdoor command attack.
– IP address Spoofing attack.
– IP fragmentation attack.
– TCP Session High jacking.
– Information leakage attack.
– JavaScript, applet attack.
– Cross site scripting (XSS).

A felsorolásban szereplő módszerek közül csupán az első kettőre térek ki, egyrészt gyakoriságuk miatt, másrészt terjedelmi okokból.

A *szolgáltatásmegtagadással járó támadás (Denial of Service; DoS)* lényege, hogy a támadás következében egy adott szolgáltatás – az azt biztosító hardver vagy szoftver megbénítása vagy működésének zavarása révén – részben vagy egészben elérhetetlenné válik. A támadók az elérni kívánt céljukat a korlátolt erőforrások kimerítésével vagy a kommunikációban és a kiszolgálásban részt vevő egységek működésének zavarásával érik el.

Az említett állapot két fő módszerrel érhető el. Az elsőnél egy szervert olyan mennyiségű kéréssel bombáznak, hogy a rendszer egyszerűen nem ké-

40 http://hu.wikipedia.org/wiki/Adware

pes ellátni feladatait, és legrosszabb esetben összeomlik. A másodikban a programok és az operációs rendszerek gyenge pontjainak *(bug)* vagy a protokollok szabálytalan alkalmazását használják fel a DoS-támadáskor. A DoS-támadások tehát mindig közvetlen, frontális támadások. A DoS-támadások – a felhasznált programok fejlettsége miatt – felderítése elég nehézkes, mivel a támadás során az érkező adatok útja bizonytalanná válik.[41]

A DoS-támadásoknak, az alkalmazott támadási módszer szerint, több alfajtájuk is létezik, de ezek közül csupán az egyik legjelentősebbre térek ki, az *elosztott szolgáltatásmegtagadással járó támadásra (Distributed Denial of Service; DDoS).*

A szolgáltatás teljes vagy részleges megbénítása, helyes működési módjától való eltérítése történhet megosztva is, több forrásból (DDoS). Ellentétben az egyszerű DoS-támadással, a DDoS esetén a támadó már több irányból is támadja a célpontot. A DDoS-támadások összetettek, a támadón és támadotton kívüli számítógépek kapacitásait, illetve a külső számítógépek nagy mennyiségét használják a támadáshoz.

Külső gép két módon kapcsolható be a támadásba:

– egy automatizált szoftver felkutatja a hálózatra kapcsolódó, sebezhető számítógépeket, amelyekre feltelepít egy rejtett támadóprogramot, ettől a megtámadott gép úgynevezett zombigéppé alakul;
– a másik lehetőség keretében az említett rejtett programot nem egy külön szoftver, hanem vírusok vagy trójai programok segítségével juttatják be a leendő zombigépbe.

A DDoS-támadás folyamata a következőképpen zajlik: a támadáskor a zombigépek távolról vezérelhetők egy mestergépről. Ha elégséges számú gépet sikerült megfertőzni a támadóprogrammal, a mestergép jelet ad a zombigépnek vagy gépeknek a támadás megkezdésére.

A támadás idején mindegyik zombigép kis mennyiségű adatot kér vagy küld a célpontnak, de mivel egyszerre teszik ezt, több száz vagy akár ezer támadó esetén a sok kisméretű adatcsomag hatalmas adatáramlást gerjeszt, ami megbénítja a célpontot.[42]

41 http://www.biztonsagosinternet.hu/node/42
42 http://hu.wikipedia.org/wiki/DDoS

A kiberterrorizmus jelene és jövője

Jelen pillanatban – még – elmondhatjuk, hogy a kiberterrorizmus jelensége túlbecsült. Mint már a cikk elején is jeleztem, eddig egyetlen nagyobb támadást sem észleltek. Az egyetlen kiberterrorista támadásnak nevezhető akciót a Tamil Eelam Felszabadító Tigrisei (Liberation Tigers of Tamil Eelam; LTTE) követte el még 1997-ben.

Akciójuk során kéretlen levelekkel bombázták a világ különböző országaiban működő Srí Lanka-i követségek elektronikus postaládáit. A támadások nem okoztak nagyobb károkat, inkább csak rámutattak az információs rendszerek sebezhetőségére. A helyi vagy nemzetközi konfliktusok közben amúgy is gyakran tapasztalható, hogy az adott felek szimpatizánsai az interneten is hadat üzennek egymásnak, és különféle önmagában jelentős károkat nem okozó támadásokat intéznek egymás ellen.

Ha mindezeket tényként fogadjuk el, adódik a kérdés: *miért került ennyire reflektorfénybe a jelenség?*

A lehetséges okok közül az első helyre a *tömegmédia* helyezhető. A médiában sokféle csúsztatással, a fogalmak egybemosásával találkozhatunk, így nem is meglepő, hogy a kiberterrorizmust gyakran keverik a hackeléssel, ily módon jelentősként feltüntetve a vizsgált bűnözési formát.

A képzeletbeli dobogó második fokára a jelenség *újdonsága* kerül. Mint láthattuk, a kiberterrorizmus lényegében technológiai terrorizmusként is felfogható, technológiai volta miatt azonban sokak számára nehezebben érthető. A kellő fokú ismeretek hiánya közismerten félelemkeltő…

Harmadik okként a *politikusok egyéni érdekei* is felhozható, hiszen érdekükben állhat egy ellenség – jelen esetben: a kiberterrorista – létrehozása, így az ellenük való fellepés hangoztatásával könnyen népszerűvé válhatnak.

Negyedik tényező a jelenség kapcsán észlelhető *bizonytalanság.*[43]

Jó néhány kérdés vár még eldöntésre, illetve több bizonytalan pontot kell tisztázni. Néhány fontosabb kérdést kiragadva:

– Hogyan értelmezhető a virtuális erőszak, mit tekinthetünk az erőszak virtuális megfelelőjének?
– A határok nélküli interneten hogyan értelmezhető a nemzeti jelleg (például nemzeti jelleget hangoztató terrorszervezetek esetén)?
– Vajon teljes bizonyossággal eldönthető-e, mely állam hatósága járjon el adott ügyben, és ha igen, melyik jogrendszer szabályai alapján?

43 Gabriel Weimann (2004): i. m.

– A való világban észlelhető jelenségek, veszélyek és dolgok (például tulajdon) könnyen felfoghatók, de vajon létezik virtuális megfelelőjük is? Ha igen, hogyan illeszthetők be a kiberterrorizmus jelenségvilágába?[44]

Leszögezhetjük, hogy a jövő terroristái feltehetően jóval több lehetőséget fognak látni a számítástechnikában, mint elődeik. A számítástechnika fejlődésével és még gyorsabb elterjedésével nagyobb veszélyt hordoz e jelenség.

Nem zárhatjuk ki annak a lehetőségét sem, hogy a jövőben a kiberterrorizmus – a világ számítástechnikai kiszolgáltatottsága miatt – veszélyesebb lesz, mint a jelenlegi „hagyományos" terrorizmus.

Mindazonáltal az egyik legnagyobb veszélyt a hagyományos és a kiberterrorizmus eszköztárának egyidejű bevetése okozhatja, hiszen ebben az esetben maximalizálható a hagyományos támadások hatása.[45]

Konklúzió

Az eddig leírtakat végigolvasva egyértelmű, hogy a kiberterrorizmus, tűnjön bármilyen veszélyesnek is, jelenleg egyfelől lehetőség a terroristák kezében, másfelől potenciális veszélyforrás a társadalmak számára. Súlyos veszélyforrás, hiszen a társadalmakban létező infrastruktúrák – amelyek pontos működése létfontosságú is lehet – jelentős része nagymértékben támadható. Láthattuk, hogy a kritikus infrastruktúrákban okozott kisebb zavar is súlyos károkat okozhat. A veszélyt csak tovább növeli az információs társadalom egyes elemeinek kiépítése, ami még tovább fokozza a társadalmak számítástechnikai függőségét, így sebezhetőségét. Továbbá nem sok magyarázatot igényel, hogy a társadalmakat leginkább a hagyományos és kiberterrorizmus közös, egymást kiegészítő és erősítő támadásai fenyegetik.

Mindamellett, paradox módon, minél összetettebbé válnak az egyes rendszerek, annál nehezebb jelentős károkat előidézni, mivel az eredményes támadás nagyobb szaktudást igényel.

Bár a társadalmak számára súlyos veszélyt jelent e jelenség, a technika és így a fegyverként használható eszközök fejlődése mellett számolni kell a biztonsági megoldások fejlődésével és terjedésével is.

Láthattuk, hogy a kritikus infrastruktúrák sem sebezhetetlenek, de többségében erősebb védelmet élveznek, mint az egyéb, jobbára magántulajdonban

44 Sarah Gordon: i. m. 10–11. o.
45 Gabriel Weimann (2004): i. m.

lévő infrastruktúrák, így azok támadása is nagyobb próbatétel a kiberterroristák számára. Vagyis olyan személyek számára, akiket néha nem egyszerű megkülönböztetni a hackerektől, különösen azért, mivel a kiberterroristák is alkalmazhatnak olyan eszközöket és módszereket, mint a hackerek, vagy egyszerűen toborozhatnak hackereket.

Mindamellett az is látható volt, hogy motivációik (ideológiai, vallási, vagy politikai) és céljaik (nem a haszonszerzés) szerint mégis kellő biztonsággal elkülöníthetjük a kiberterroristákat az egyéb számítógépes bűnözőktől. E jelenséget, mint kitértem rá, többen túlbecsülik, a kelleténél jóval súlyosabb jelenségként feltüntetve.

Való igaz, hogy a dolog akár már a közeljövőben is sokkal jelentősebbé válhat, mint napjainkban, de úgy tűnik, hogy napjaink terroristái egyelőre megmaradnak a jól bevált módszerek mellett.

Érdekes jelenségként könyvelhetjük el, hogy az Amerikai Egyesült Államok által meghirdetett terrorizmus elleni küzdelem *(war on terror)* hatására beszűkültek a terroristák valós világbeli lehetőségei, így figyelmük várhatóan inkább a virtuális világ felé fordul, ahol kellő szakismerettel jelentős károkat okozhatnak a nem kellően felkészült társadalmaknak.[46]

46 Dorothy E. Denning: i. m.