Dr. Kovács László mk. őrnagy, főiskolai docens
ZMNE BJKMK Informatikai tanszék
kovacs.laszlo@zmne.hu

AZ INFORMÁCIÓS TERRORIZMUS ESZKÖZTÁRA

Absztrakt

Ahogy nő a mindennapjainkban használt számítógépek száma, úgy nő annak a veszélye, hogy ezeken a számítógépeken keresztül támadás ér minket. Ha ehhez a veszélyhez ráadásul azt is hozzáadjuk, hogy a mindennapi életünket nagyban befolyásoló kritikus információs infrastruktúrák is számítógépek, számítógépes hálózatokon keresztül működnek – és ezért ezek szintén sebezhetőek –, akkor nyilvánvaló, hogy fel kell tárnunk honnan, és milyen veszély fenyeget a hagyományos vagy a cyber terrorizmus oldaláról. Ezt a cél tűzi ki maga elé ez az írás.

Nowadays we use more and more computer in our everyday life. As the number of computers increase the hazard of attacks against our computers also growing. Parallel with this serious danger a new challenge has been appeared: our critical information infrastructures are also based on computers and computer networks which are threatening by terrorism. That's why this paper main goal is to characterize the main points of these threats.

Kulcsszavak: *terrorizmus, információs terrorizmus, cyber terrorizmus, információtechnológia, kritikus információs infrastruktúrák ~ terrorism, information terrorism, cyber terrorism, information technology, critical information infrastructure.*

BEVEZETÉS, avagy MIT és MIÉRT?

Legújabbkori történelmünkben, nevezetesen 2001. szeptember 11-ét követően, ahogy a terrorizmus ismét a figyelem középpontjába robbant, elemzések, írások, szakértői jelentések tucatjai születtek a témakörben. Mindezek jelentős része a hagyományos terrorizmust[1], mint a 21. század elejének legfőbb kihívását elemzik és vizsgálják. A hagyományos terrorizmus mellett azonban meglehetősen kevés szó esik egy másik dimenzióból leselkedő hasonló veszélyről. Ez a dimenzió a mindennapjainkat átszövő információs rendszerek dimenzióját jelenti, amelynek egyik része az internet megformálta cyber-tér. Az elmúlt években a terrorizmussal foglalkozó szakemberek jelentős része még nagyon gyakran egy kézlegyintéssel elintézte ezt a fajta veszélyt, mondván rendkívül kicsi a valószínűsége egy a cyber-térből érkező terroristatámadásnak. Azonban ahogy nő az információtechnológia dominanciája a mindennapokban, úgy erősödnek azok a szakértői figyelmeztetések, amelyek e veszélyek fokozódására próbálják meg felhívni a figyelmet.

[1] A hagyományos terrorizmus alatt az olyan eszközöket, eljárásokat és akciókat, illetve az ezek mögött álló embereket vagy csoportokat értem, amelyek a már „megszokott" módon – emberrablásokkal, robbantásokkal, öngyilkos merényletekkel, illetve az ezekhez hasonlatos módszerekkel – kívánják céljaikat elérni.

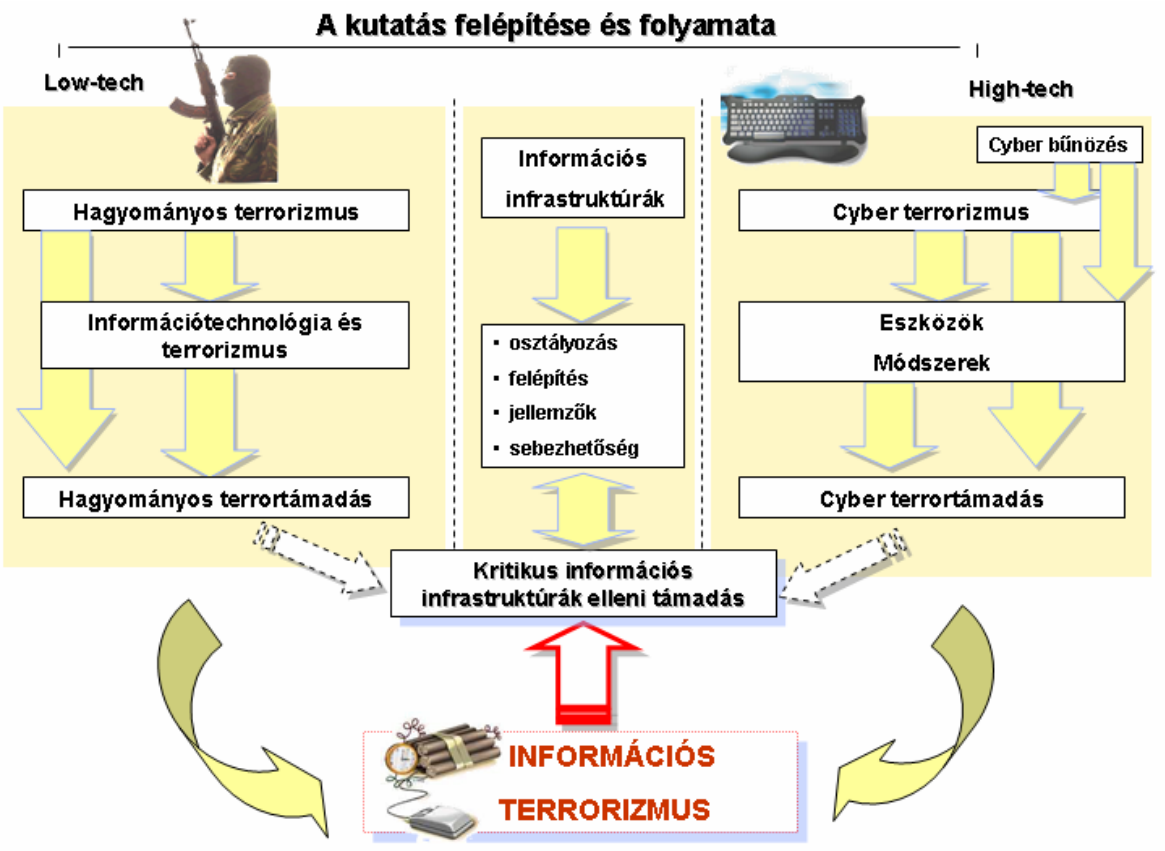
Ennek oka elsősorban az, hogy ahogy nő a számítógépek száma úgy nő annak a veszélye, hogy a számítógépeinket megtámadják, illetve a megtámadott gépeket – akár azok tulajdonosainak tudta nélkül[2] – további támadásokra felhasználják.

Számítógépek természetesen nem csak otthonainkban vannak. Azokat az infrastruktúrákat, amelyek a mindennapi életünket kiszolgálják, segítik, vagy támogatják szintén számítógépek, illetve számítógépes hálózatok működtetik és irányítják.

Mindezeknek megfelelően meg kell vizsgálni, hogy melyek azok az – akár hagyományos, akár információtechnológiai eszközök és lehetőségek –, amelyekkel számítógépeink, hálózataink, illetve az információs infrastruktúráink támadhatók.

Ehhez a munkához azonban olyan – egymásra épülő – rész-kutatásokra van szükség, amelyek kiterjednek a hagyományos terrorizmus rövid elemzésére, bemutatják a legsebezhetőbb infrastruktúrákat, megkeresik azokat az eszközöket, amelyekkel ezek támadhatók, és természetesen e feltáró és elemző munka után megpróbálnak valamilyen védelmi elgondolást is kidolgozni a feltárt veszélyek, támadási módszerek és sebezhető pontok függvényében. A látszólag szerteágazó kutatások dinamikusan kiegészítik egymást és így abba az irányba haladnak, hogy a definiált információs terrorizmust megértsük és felkészüljünk annak potenciális támadásaira.

E kutatómunka tervezett folyamatát mutatja be az 1. sz. ábra.



1. számú ábra

[2] Az ilyen számítógépeket zombi-nak nevezik. A felhasználó tudta nélkül különböző rosszindulatú, pl. trójai programok telepítődnek a gépre, amelyek azután részlegesen vagy teljes egészében átveszik az irányítást a gép felett, és onnan különböző támadásokat és egyéb tevékenységeket végeznek. Részletesebben jelen írás Malwares (rosszindulatú szoftverek) című fejezetében kerül ismertetésre ez, illetve az ehhez kapcsolódó egyéb támadási formák..

HAGYOMÁNYOS TERRORIZMUS

Bár jelen írás célja – mint ahogy címéből nyilvánvalóan kiderül – nem a hagyományos terrorizmus (öngyilkos merénylők, nemzetközi terrorszervezetek, illetve az általuk végrehajtott terrortámadások) kutatása és vizsgálata. Mindazonáltal azonban – még ha nagyon röviden és tárgyilagosan is –, szükséges a terrorizmus főbb fogalmainak, szereplőinek és mozgatórugóinak az áttekintése, mivel számos azonosság tételezhető fel a hagyományos és az információs terrorizmus különböző formái között. Mindezeken túl, amennyiben sikerül felvázolni néhány jelentős tényezőt a hagyományos terrorizmus kapcsán, akkor talán sikerül az információs terrorizmus néhány hasonló jellemzőjét – az erre a tevékenységre, illetve az ebben szereplők esetében – megvizsgálni. Néhány ilyen jellemző lehet:

- okok;
- szereplők;
- cél;
- a végrehajtás módszerei.

Természetesen ezt a rövid bemutatást az is indokolttá teszi, hogy első megközelítésben is látszik az a tény, hogy a hagyományos terrorizmus és a cyber térből érkező terrorizmus egymásra találása, párhuzamosan elkövetett, egymást mintegy kiegészítő akcióik hatványozottan nagyobb károkat okozhatnak, mint a külön külön-külön elkövetett hagyományos-, illetőleg cyber terrortámadások.

A terror és a terrorizmus fogalma

A mai értelemben vett hagyományos terrorizmus az 1970-es években történt számos terror-akció kapcsán került ismét a figyelem középpontjába. Talán még sokak emlékezetében élénken él az olyan terrorcsoportok neve, mint például a Fekete Szeptember[3]; IRA[4]; Baader-

[3] 1972. augusztus 26. és szeptember 11. között Münchenben rendezték meg a XX. nyári olimpiát. Szeptember 5-én a Fekete Szeptember nevű terrorista csoport nyolc tagja az olimpiai faluban behatolt az izraeli csapat szálláshelyére, ahol két izraeli sportolót megöltek és kilencet túszul ejtettek. Miután az izraeli kormány megtagadta a követelt 200 palesztin fogoly szabadon bocsátását, a terroristák a német kormánytól repülőgépet követeltek a túszok elszállítására. A terroristákat és a kilenc túszt két helikopteren átszállították a fürstenfeldbrucki katonai repülőtérre, ahol egy Boing repülőgép már várakozott, hogy elszállítsa őket valamelyik arab országba. A repülőtéren a német rendőrség túszmentési akciót kezdeményezett, amely olyan szerencsétlenül végződött, hogy a terroristák megölték túszaikat, illetve a tűzharcban öt terrorista és egy rendőr is meghalt. A három további terroristát elfogták. [1]

[4] 1972. január 30-án – amit azóta „véres vasárnapként" emlegetnek – a brit katonák az internálás ellen tüntető tömegbe lőttek, és 13 embert megöltek. Egyes vélemények szerint ez az esemény járult a leginkább hozzá ahhoz, hogy az IRA terrorista szervezetté váljon. Az IRA 1972 februárjában kezdte meg terrorhadjáratát a protestáns és a brit célpontok ellen. Az erőszak megfékezésére a brit kormány felfüggesztette az észak-ír parlamentet és átvette az országrész irányítását, ahol már tizenötezer brit katona állomásozott. Az IRA bomba-merényletekkel és gyilkosságokkal válaszolt erre a lépésre. [2]

Meinhof Csoport[5] vagy Vörös Brigádok[6], amelyek abban az időben a napi hírek meghatározói voltak a különböző akcióikkal.

2001. szeptember 11. azonban újra a mindennapok részéve tette a terrorizmust. A Pentagon és a Világkereskedelmi Központ elleni merényletek rádöbbentették a világot arra, hogy a hidegháború elmúltával már nem a nagyhatalmi szembenállás a legfőbb veszélyforrás, hanem a terrorizmus, illetve ennek egyik legveszélyesebb formája: a nemzetközi terrorizmus. Szeptember 11-ét követően írások, elemzések és szakértői magyarázatok tucatjai születtek a terrorizmust, mint a XXI. század új és egyik meghatározó veszélyforrását elemezve. Ezek közül számosat tanulmányozva választ kaphatunk a következő kérdésekre, amelyek további tanulmányozása, illetve az azokból levont következtetések segíthetik a cyber terrorizmus megértését. Ilyen megvizsgálandó kérdések lehetnek:

- a háború és a terrorizmus fogalmi és tartalmi elkülönítése;
- az állami terror és a (nem állami) terrorista csoportok vizsgálata;
- a terrorizmus mozgatórugójának (motiváció) vizsgálata.

Mielőtt ezeket nagyon röviden megvizsgálnánk, szükségessé válik a terrorizmus fogalmának meghatározása. Ez azonban meglehetősen nehéz feladat, hiszen egyrészt nem létezik egységesen elfogadott definíció, másrészt pedig akárhány megfogalmazást is nézünk azok számos ponton eltérnek egymástól. Ennek oka elsősorban talán abban keresendő, hogy a fogalom megalkotói más és más szemszögből vizsgálják a kérdést, és így természetszerűleg más és más álláspontot is képviselnek. Mindezek ellenére – vagy talán éppen az előbb említett okok miatt –, álljon itt egyetlen megfogalmazás a terrorizmus leírására, amelyet a Magyar Hadtudományi Társaság határozott meg a Hadtudományi lexikonban:

> **„***Terror, megkülönböztetés nélküli támadás: minden olyan erőszakos cselekmény, vagy azzal való fenyegetés, amelynek elsődleges célja, hogy rettegést keltsen a polgári lakosság körében."* [3]

Háború és terrorizmus

Amióta az emberiség „feltalálta" a háborúskodást és háborúkat vív egymással, azóta minden háború természetszerűleg erőszakos cselekményeket tartalmaz és félelmet kelt az emberekben. Amiben a háború mégis különbözik a terrorizmustól az az, hogy itt nem elsődleges cél a terrorizálás, a félelemkeltés, hanem az csak egy járulékos tény, hiszen Clausewitzel élve a háború nem más, mint a politika folytatása erőszakos eszközökkel; két élőerő nyíltösszeütközése. Egy másik meghatározó különbség a háború és a terrorizmus között az lehet, hogy a háborúkat alapvetően államok vívják, míg a terrorizmus az állammal

---

[5] Andreas Baader és Ulrike Meinhof vezette csoport nevéhez számos – az 1970-es évek elején elkövetett – merénylet és gyilkosság fűződik. Csoportjukat később átnevezték a RAF–Rote Armee Fraktion, azaz a Vörös Hadsereg Frakció névre.

[6] Vörös Brigádok – *Brigate Rosse*, olasz terroristacsoport, amely a 60-as évek végén Renato Curcio vezetésével szerveződött a Trentói Egyetem szélsőbaloldali köreiben. Tagjai lelkesedtek a forradalom eszméjéért, a parlamentáris demokráciát csak álarcnak tartották, amely mögött zavartalanul folyik a kizsákmányolás és az elnyomás. Céljuk az állam meggyengítése és a proletárforradalom kirobbantása volt. Ezt gyújtogatások, robbantások, emberrablások, gyilkosságok útján akarták elérni. Aldo Moro volt olasz miniszterelnök, a baloldallal történelmi kiegyezést kereső kereszténydemokrata politikus 1978. március 16-i elrablásával, majd megölésével politikai válságot idéztek elő. Ők a felelősek a bolognai pályaudvar felrobbantásáért is. Bár a csoport tagjait már a 70-es évek közepétől kezdték letartóztatni és elítélni, aktivitásuk a 80-as évek végéig tartott. A megszűntnek hitt szervezet 2003 őszén ismét hallatott magáról. Az olasz rendőrség ekkor tartóztatott le hat embert, akit Massimo D'Antona kormányzati tisztviselő négy évvel azelőtti, és Marco Biagi tanácsadó 2002-es megölésével vádoltak. [4]

(vagy több állammal) szembenálló nem állami csoportok, szervezetek jelenítik meg. Ehhez még az a jellemző is hozzájárul, hogy *„a terrorizmus lényege egyértelműen a nyílt ütközet tagadása.”* [5]

Állami terror vagy terrorista csoportok

Természetesen a történelemben nagyon sok példát láthatunk arra, hogy az állam, vagy az állami hatalmat gyakorlók lépnek fel a terror eszközeivel az ország állampolgáraival szemben. Ez a fajta terror azonban inkább elnyomó, sokszor brutálisan totális befolyása miatt érdemli ki ezt a jelzőt, ellentétben az általunk tárgyalt hagyományos terrorizmus figyelemfelkeltő, demonstráló jellegével.

A terrorizmus mozgatórugója - motiváció

Későbbi vizsgálataink előtt – amelyek a cyber térben potenciálisan meglévő terrorizmusra irányulnak –, fontos tisztázni, hogy mi, vagy mik azok a motivációk és mozgatórugók, amelyek a hagyományos terrorizmus esetében tapasztalhatók. Fontos ennek kiderítése illetve feltérképezése, hiszen amennyiben ebben az esetben találunk egyértelmű és kézzelfogható indítékot, akkor ennek analógiáján megkereshető a cyber terror esetében az a kiinduló ok, amely az ottani akciókat mozgathatja és motiválhatja.

A probléma azonban összetett. Annál is inkább, hiszen láttuk, hogy még egységes terrorizmus definícióval sem tudunk szolgálni, mert ahány vizsgálat, illetve ahány szempontrendszert felállító van annyi oldalról közelíthetjük meg a fogalmat. Ráadásul a szereplők is saját szemszögből viszonyulnak a terrorizmus kérdéséhez, hiszen aki az egyik oldalon terrorista az a másik oldalon gyakran szabadságharcos.

Megvizsgálva számos terrorakciót az azonban közös tényként értékelhető, hogy minden terrorakció egyik kulcseleme a *nyilvánosság.* Ez az egyik, nagyon sok esetben – eltekintve a hasonló kivitelezési módoktól –, az egyetlen közös a különböző terrorakciók között. Függetlenül az indítéktól minden terrorszervezet számára létfontosságú a nyilvánosság különböző fokú biztosítása, hiszen csak ezen keresztül lehetséges, hogy a társadalom szélesebb rétegei is kapjanak információt magáról az akcióról, illetve a szervezet céljairól. A terrorszervezet csak így tudja biztosítana, hogy az erőszakos eszközökkel elkövetett akciók a megfélemlítésen, a bizonytalanságon keresztül befolyásolják a közvéleményt, illetve a kormányzatot. Így tehát a terrorakciók a nyilvánosság számára és a nyilvánosság befolyásolására születnek. Ennek hiányában a terrorizmus értelmetlen és céltalan!

TERRORIZMUS ÉS INFORMÁCIÓTECHNOLÓGIA

A 20. század végének és a 21. század elejének társadalmában az információtechnológia és az erre épülő technika rohamos térhódítása már-már mindennapos ténynek számít.

Természetesen a különböző terrorista szervezetek és csoportok is ugyanúgy – hacsak nem jobban! – használják, és kihasználják a csúcstechnika nyújtotta lehetőségeket mint a hétköznapok többi szereplője. A következőkben néhány olyan tevékenység felsorolása és rövid elemzése történik, amelyek során a hagyományos terrorszervezetek az információtechnológiával kapcsolatba kerülhetnek.

Tervezés

Természetesen a hagyományos terrorista szervezetek tagjai is használják az információtechnológia nyújtotta lehetőségeket, hiszen őket sem hagyja érintetlenül a 21. század.

Az internet segítségével kommunikálhatnak, szervezhetik akcióikat. Az internetről letölthető és viszonylag könnyen kezelhető titkosító programok segítségével még annak a veszélye is igen kicsi, hogy kommunikációs, kapcsolattartó tevékenységüket „lehallgassák".[7] A titkos üzenetváltás egy másik módszere lehet az úgynevezett szteganográfia[8]. Ez azt jelenti, hogy látszólag érdektelen és ártalmatlan hordozókba építenek be a kívülállók számára láthatatlan módon információkat. Ilyenek hordózók lehetnek például különböző formátumú képek, ahol a kép digitális jelei közé vannak elrejtve az információk, vagy ilyen lehet akár egy hang fájl is, amely esetében a háttérzaj tartalmazhatja az információt. Mivel ezekben az esetekben nincs semmi, ami a titkos információtovábbításra utalna ezért legtöbbször nem is kerülnek a „felderítők" látókörébe.

Toborzás, propaganda, pénzügyi támogatás

Új tagok verbuválása, toborzása terén szintén hatalmas lehetőségeket nyújt az internet a hagyományos terrorista szervezetek számára. A különböző terrorista szervezetek által fenntartott weboldalakon nyíltan is történik új tagok toborzása. Ezeken az oldalakon a potenciális új tagok meggyőzésére számos megoldás kínálkozik. A webes technikának köszönhetően egy weboldalon lehetőség van felhívni az érdeklődők figyelmét az „ügyre" különböző írásokkal, publikációkkal, a szervezet történetének és vezetőinek bemutatásával, az eddigi akciókról készített videók, pedig sokszor le is tölthetők. Lehetőség van továbbá pénzbeli adományok[9] gyűjtésére is e lapok segítségével. Ehhez hasonló weboldal például a Hezbollah (http://www.hizbollah.org) oldala.

A toborzás terén olyannyira követik a trendeket, hogy a hagyományos propagandafilmek helyett, amelyek hosszúak, unalmasak, nehezen követhetőek voltak, olyan új médiumokat láthatunk, mint például a rövid, színes mozgalmas flash animációk, vagy a gyerekeknek szánt vicces képek. Ezek sokkal jobban megragadják a figyelmet, mint a már említett hagyományos egy kamerával rögzített, a vezető (pl. Oszama Bin Laden) beszédeit több tízpercen keresztül mutató videók. Az új médiumtípusokkal elsősorban a fiatalokat célozzák meg.

Érdemes megemlíteni, hogy röviddel az újfajta figyelemfelkeltő terrorista szervezetek, vagy azokhoz közel álló internetes médiumok után a CIA is levonta a tanulságokat. A CIA megújult honlapján már nyíltan toboroz munkatársakat, elsősorban a fiatalabb generációt megcélozva. Ennek egyik ötletes megoldása, egy olyan ötlépéses, on-line kitölthető játékos teszt,[10] amely végén a jelentkező megtudhatja, milyen állásra is lenne alkalmas. Persze a figyelemfelkeltés és a toborzás mellett nem elhanyagolható cél, hogy a Cég így is megpróbálja megváltoztatni a CIA-ról – az elmúlt időben cseppet sem pozitív – kialakult képet.

---

[7] Meg kell azonban jegyezni, hogy gyakran hangoztatott szakértői vélemények szerint a kódolt adatcsomagok megfejtése, és ezáltal az információtartalom visszanyerése az esetek jelentős részében az elektronikus felderítésre szakosodott NSA-nek (National Sacurity Agency) nem jelent különösebb gondot.

[8] A szteganográfia nem a 21. század találmánya. Már az ókorban is használtak olyan eszközöket és eljárásokat, amelyek segítségével titkos üzeneteket lehetett küldeni valamely nyílt üzenetbe rejtve. Ilyen volt például a „láthatatlan" tinta, amely alkalmazásával az üzenet csak akkor vált láthatóvá, ha megfelelő hőmérsékletűre melegítették. Napjainkban a szteganográfia a digitális technika alkalmazásával újra fénykorát éli.

[9] Ezt a fajta tevékenységet *donation* –nak nevezik, amely közvetett pénzügyi támogatást jelent. A szervezetet támogatni szándékozónak nincs más dolga, mint egy meglehetősen egyszerű elektronikus űrlapot kitölteni, megadni az adatait, bankkártyája számát, a kívánt összeget, és már kész is.

[10] https://www.cia.gov/careers/CIAMyths.html

Adat- és információszerzés

Gyakran ismételgetett, és már-már szállóigévé vált meghatározás az internettel kapcsolatban: „ami nincs az interneten az nincs is”. Ez a kissé vicces kijelentés arra utal, hogy ma már gyakorlatilag nincs az életnek olyan területe, amelyről ne találnánk legalább egy kicsinyke információmorzsát az interneten.

Napjainkban az internet népszerűségének egyik oka abban rejlik, hogy ki sem kell mozdulnunk a szobánkból, vagy irodánkból, ahhoz hogy információkat gyűjtsünk a legváltozatosabb témákban. Napilapokat olvashatunk, digitalizált könyveket lapozhatunk, bármilyen kérdésre is keressük a választ, azt – kevés kivételtől eltekintve – meg is találjuk az interneten. Sőt, az esetek jelentős részében „konyhakész” választ kapunk a keresett kérdésre vagy problémára.

A terrorista szervezetek számára is adott hát a lehetőség, hogy a számukra szükséges információkat megkeressék, és ami ennél sokkal rosszabb – meg is találják. A „házkészítésű bomba” (homemade bomb) szavakat begépelve az egyik legismertebb internetes keresőbe 0,17 másodperc alatt kb. 17 millió találatot kapunk. Ezeknek a találatoknak a jelentős része természetesen esetünkben (a terroristák esetében) irreleváns. De a sokmilliónyi találat között van olyan, amely kész recepttel szolgál az otthon, akár a kereskedelemben szabadon megvásárolható alapanyagokból való bombák előállításához („konyhakész bomba”). A találatok között nagyon sokáig keresnünk sem kell, hogy akár kész videofilmeket is találjunk a témában.

A nyugati társadalmak információszabadsága a különböző terrorszervezetek számára tehát nagyon hasznos, hiszen az internet révén olyan adatokhoz és információhoz is hozzáférhetnek, amelyek megszerzése szinte elképzelhetetlen lett volna 15-20 évvel ezelőtt, nem beszélve arról, hogy maga az információszerzés is hallatlan kockázattal járt volna. A nyílt csatornákon történő információszerzésre az egyik legjobb példa, hogy 2003. januárjában Donald Rumsfeld akkori amerikai védelmi miniszter kiadott egy utasítás, mely szerint azonnal radikálisan csökkenteni kell a DoD és egyéb USA intézmények olyan weboldalainak a számát, illetve tartalmát, amelyeken keresztül különböző terrorszervezetek szenzitív információkra tehetnek szert, vagy a különböző honlapokon külön-külön meglévő adatok felhasználásával juthatnak értékes – az USA számára pedig hihetetlenül veszélyes – következtetésekre. Ennek az utasításnak az apropója az az Afganisztánban talált terrorista kézikönyv volt, amelyben a felhasznált információk több mint 80%-a nyílt – DoD – weboldalról származott. [6]

INFORMÁCIÓS INFRASTRUKTÚRÁK

Nagyon röviden be kell mutatnunk, hogy melyek azok a – főleg – információs infrastruktúrák, amelyek nélkülözhetetlenek a nyugati társadalmak részére, és amelyek ugyanakkor roppant módon ki is vannak téve a cyber térből érkező veszélyeknek, hiszen ezen rendszerek jelentős része valamilyen formában kapcsolódik a cyber térhez.

Infrastruktúrán azoknak a rendszereknek, illetve ezek elemeinek az összességét értjük, amelyek biztosítják az adott szervezet rendeltetésszerű működését. A fontosság, feladat, rendeltetés és felépítés alapján számtalan infrastruktúrát különböztethetünk meg. Ezek közül azonban ki kell emelni azokat, amelyek részleges, időleges, vagy teljes leállása olyan következményekkel jár, amelyek más infrastruktúrák működésképtelenségét is magukkal vonzzák. Azokat az infrastruktúrákat, amelyek ezek alapján a legfontosabbak, a legsebezhetőbbek, folyamatos és rendeltetésszerű működésük elengedhetetlen a többi infrastruktúra működéséhez *kritikus infrastruktúráknak* nevezhetjük. [7]

A teljesség igénye nélkül néhány e kritikus infrastruktúrák közül: [8]

- *az energiatermelő, -tároló és -szállító infrastruktúrák:* a szén- és olajtüzelésű, gázüzemű, vízi-, szél-, nap-, biogáz- és atomerőművek, földgáz és kőolajtermelő és -finomító vállalatok, szénbányák, villamos energia átalakítók, távvezetékek, kőolaj- és földgázszállító vezetékek, stb.;
- *a banki és pénzügyi infrastruktúrák:* banki hálózatok, kereskedelmi központok, érték- és árutőzsdék, egyéb pénzügyi szervezetek;
- *a vízellátó rendszerek:* víztisztítók, víztározók, vízvezeték- és csatornahálózat, stb.;
- *a távközlési és kommunikációs rendszerek:* távközlési és kommunikációs eszközök, amelyek számítógép alapú hálózatokat, szoftvereket, stb., is magukba foglalnak;
- *a szállító infrastruktúrák:* nemzeti légitársaság, repülőterek, közúti személy- és teherszállító vállalatok, út- és autópálya hálózatok, vasúti társaságok, vasúthálózatok, vízi szállító eszközök stb.;
- *a vészhelyzeti és katasztrófavédelmi infrastruktúrák:* mentőszolgálatok, rendőrség, tűzoltóság, egészségügyi intézetek, katasztrófa elhárító szolgálatok, stb.;
- *a kormányzati és önkormányzati szervek.*

Napjainkban ezek az infrastruktúrák mindegyike jórészt számítógépes hálózatra, vagy ezek egyes elemeire épül. Ezek önmagukban is sérülékenyek, de mivel ezek a számítógépes hálózatok nagyon sok esetben természetszerűleg – pont az általuk elvégzendő feladatok miatt – nem zártak, nem a külvilágtól hermetikusan elzárt hálózatok, hanem számos helyen kapcsolódnak más hálózatokhoz. Mivel vannak külső kapcsolódási pontjaik – az esetek jelentős részében ezek számának a meghatározása, illetve a kapcsolódási pontok behatárolása is komoly nehézségekbe ütközik (komplexitás, feladatok sokrétűsége, fizikai kialakítás, területi lefedettség, stb. miatt) –, így az egyébként is sérülékeny hálózatok kívülről is támadhatóvá válnak.

A Magyar Köztársaság nemzeti biztonsági stratégiájában (2073/2004. (IV. 15.) Korm. Határozat) II.1.6. pontban tárgyalja *Az információs társadalom kihívásai* címmel ezt a veszélyt: *„A hosszú távú lemaradás hátrányos következményeinek elkerülése érdekében Magyarország számára kiemelt feladat a felzárkózás a fejlett világ információs és telekommunikációs színvonalához. Az információs forradalom vívmányainak mind szélesebb körű megismertetése, az oktatás színvonalának emelése kulcsfontosságú érdek, ami közvetve pozitív hatással van a gazdaságra, a társadalom életére és az ország érdekérvényesítő képességére. Az informatikai infrastruktúra technikai és szellemi feltételeinek biztosítása mellett ügyelni kell e rendszerek védelmére és a megfelelő tartalékok képzésére is. Az informatika számtalan lehetőséget teremtett a társadalom számára, de fokozta annak*

veszélyeztetettségét. A számítógépes hálózatok és rendszerek sebezhetősége, túlterhelése, az információlopás, a vírusterjesztés és a dezinformáció kockázati tényezőt jelent az ország számára." [9]

A magyar kormány meghatározta azokat az infrastruktúrákat, amelyekre elsősorban – a terrorizmus elleni harcban – a civil lakosság védelme érdekében különös gondot kell fordítani. Ezek a következők [10]
:

- energiaellátás;
- közművesítés;
- közlekedés;
- szállítás;
- távközlés;
- elektronikus adatforgalom;
- informatikai hálózat;
- bankrendszer;
- szolgáltatások;
- média;
- ivóvíz;
- élelmiszer alapellátás;
- egészségügyi biztosítás.

Ebből a felsorolásból is világosan látszik, hogy bár különálló rendszerekről van szó, azok mégis nagyon sokszor feltételezik egymást. Így például az energiaellátás számos egyéb – szintén nagyon fontos - infrastruktúra működésének feltétele. Ebből következően, ha nem is célunk semmiféle prioritás, vagy sorrend felállítása a felsorolt hazai infrastruktúrák vonatkozásában, azt mégis nyugodtan kijelenthetjük, hogy az *energiaellátó rendszerek* hosszabb-rövidebb ideig történő, részleges vagy teljes üzemképtelensége igen komoly hatást gyakorolhat a többi infrastruktúrára.

CYBER BŰNÖZÉS ÉS CYBER TERRORIZMUS

Mielőtt megvizsgálnánk, hogy kik is azok, akik potenciálisan szóba jöhetnek, mint cyber terroristák, meg kell vizsgálnunk, hogy kik is azok, akik a cyber térben olyan tevékenységeket folytatnak, amelyek adott esetben akár terrorista – esetünkben cyber terrorista – akciók végrehajtására is alkalmasak lehetnek. A vizsgálatot természetesen a cyber tér szereplőivel kell kezdenünk:

- **Hackerek:**
  A hacker olyan személy, aki internet segítségével hozzá tud férni védett adatokhoz a számítógépeken. Kezdetben külön fogalmat alkottak a hackerek, akik azért törtek fel rendszereket, weboldalakat, illetve programokat, hogy bizonyítsák azok gyenge pontjait, azonban ezeket a hiányosságokat a rendszergazdák tudomására hozták, azaz általában jóindulatúan jártak el. Ők voltak az úgynevezett fehérkalaposok, azaz a „white hat" csoport tagjai. Az ellentábort azok a fekete kalaposok, „black hat" alkották, akik sokszor rosszindulatból, vagy valamilyen haszonszerzés reményében hatoltak be egy-egy rendszerbe. Ma már általában gyűjtőnévként csak a hackert használják, függetlenül a behatolás okától. Korábban igen elterjedt volt az úgynevezett phreak-ek, akik csoportjai telefonvonalat lopva jutottak anyagi előnyökhöz. A phreak-

ek a telefonközpontok vezérlő számítógépeinek, a távközlési vonalak ingyenes igénybevételének és általában a telekommunikációnak a szakértői voltak. Rendelkeztek azzal a tudással, ami a központok átprogramozásához szükséges. Emellett a mobil telefonhálózat forgalmának, belső adatainak lehallgatásához is voltak (vannak) megfelelő eszközük.
A SANS Institute (https://www.sans.org) immár hat éve ad ki egy olyan tízes toplistát, amely az interneten keresztül leggyakrabban kihasznált sebezhetőségeket tartalmazza, valamint bemutatja melyek a hackerek legnépszerűbb célpontjai.. A lista olyan nagy érdeklődésre tett szert, hogy azóta az már húsz eleműre bővült és minden évben megjelenik. A lista több kategóriát tartalmaz. Az első ilyen kategória az operációs rendszerek, illetve ezek összetevőinek a csoportja, amely első három helyezettje, azaz azok az alkalmazások, amelyeket a legtöbb támadás érte 2006-ban: 1. Internet Explorer, 2. Windows könyvtárak (DLL-ek), 3. Microsoft Office alkalmazások. [11]

- **Hacktivisták (Hactivists):**
  A hackerek és az aktivisták tulajdonságait, illetve céljait közösen vallók társasága. Rendszerint valamilyen politikai motivációval rendelkeznek. Számos olyan akciót hajthatnak végre, amelyek során valamilyen – számunkra fontos – ügy érdekében internetes oldalakat törnek fel, átalakítják azok kinézetét, adatokat lopnak el onnan, illetve akadályozhatják az oldal működését pl. virtuális ülősztrájkkal (flood vagy DoS támadással.) Számos esetben támogatnak olyan terrorista szervezeteket, amelyek céljai vagy akciói partikulárisan egybe esnek az övékével. Az egyik ilyen hactivista megmozdulás volt 1999-ben, amikor az Egyesült Államok illetve a NATO csapatok Szerbiát bombázták és találat érte a belgrádi kínai nagykövetséget, amely után kínai hackerek tucatjával intéztek támadásokat amerikai szerverek ellen.

- **Számítógépes bűnözők:**
  Azok a gyakran igen magas szintű hálózati és számítógépes ismeretekkel rendelkező elkövetők, akik elsődleges célja a pénzszerzés. A később tárgyalt rosszindulatú szoftverek, illetve eljárások alkalmazásával – pl. phishing – hajtják végre akcióikat. Az elmúlt években a számítógépes bűnözők által elkövetett bűncselekmények, illetve az ezekkel okozott károk nagysága nagyságrendekkel nőtt.
  Trendként értékelhető az elmúlt években, hogy míg korábban a jó képességű és sikeres betöréseket végrehajtó hackerek közzétették tapasztalataikat, pl. egy adott rendszerben hol található gyenge, vagy behatolásra alkalmas pont, addig ma már ezt megtartják maguknak, illetve megpróbálnak ezekből az információkból pénzt kinyerni. Azaz felajánlják az általuk feltört rendszerek tulajdonosainak vagy üzemeltetőinek mintegy megvételre ezeket a kulcsfontosságú adatokat. Más esetekben pedig megbízásból, anyagi ellenszolgáltatás fejében – pl.: a behatoláshoz, vagy információszerzéshez tudással, eszközökkel és módszerekkel nem rendelkező hagyományos bűnözői körök számára –, adatokat, információkat szereznek, törölnek vagy módosítanak. Mindazonáltal a hagyományos bűnözésre szakosodott – sok esetben szervezett – bűnözői körök is felismerték a pénzszerzés új módszereit ezen a téren. Más esetekben nem a közvetlen pénzszerzés a cél, hanem a más módszerekkel megszerzett illegális jövedelmek nyomainak eltüntetése, vagy e jövedelmek tisztára mosása jelenik meg elsődleges motivációként.

- **Ipari kémek:**
  Természetesen az iparban elkövetett illegális információszerzés nem napjaink találmánya, hiszen amióta elkezdődött az iparosodás azóta ez a jelenség állandóan jelen van. Ami mégis új dolog az a módszerekben és a kivitelben keresendő. A számítógépes tervezés, irányítás és rendszerfelügyelet magában hordozza azt a lehetőséget, hogy a számítógépeken tárolt, vagy a hálózatokon áramoltatott adatokat és információkat illetéktelenek – ebben az esetben ipari kémek: konkurens cégek alkalmazottai, vagy éppen az előbb említett számítógépes bűnözők, akik a megszerzett adatok piacra dobásával üzletelnek – szerzik meg. Megjelent tehát egy új, elektronikus csatorna az illegális adatszerzők kezében, amelyen keresztül hatalmas mennyiségű adatot képesek szerezni, amely ráadásul nemcsak polgári cégek adataiban merülhet ki, hanem katonai technológiák adatainak a megszerzésére is irányulhatnak, amelyek esetenként sokkal több pénzt is érnek bizonyos piacokon.

- **Belső szakértők és külső szerződők:**
  Egy adott vállalat életében óriási szerepet játszanak a szakértők, akik sok esetben számos helyen – akár több telephelyen – is végzik munkájukat. A szakértők munkájuk elvégzése érdekében általában magas szintű hálózati hozzáféréssel rendelkeznek. Ebből következően adott esetben – pl.: munkahelyi konfliktusok, zsarolás, stb. – igen értékes adatokat tud eltulajdonítani, illetve akár különböző rosszindulatú programok bevitelére is lehetősége van, hiszen a hálózathoz belülről fér hozzá.
  A külső szerződők szintén kaphatnak hozzáférési jogokat a hálózathoz, és természetesen szintén számos igen értékes adathoz férhetnek hozzá, amelyekkel később visszaéléseket követhetnek el.

- **Terroristák:**
  Az előzőekben bemutatott szereplők mellett meg kell említenünk a terroristákat is, hiszen ők is használhatják az internetet. Attól függően, hogy milyen célból használják az információtechnológiát, két csoportra oszthatóak. Az első csoportba, azok a terrorista szervezetek tartoznak, amelyek a már említett célokra – propaganda, toborzás, adatszerzés – használják e rendszereket. A másik – sokkal veszélyesebb – csoportba azok a terroristák tartoznak, akik nemcsak ilyen úgynevezett „soft” tevékenységre kívánják használni a rendszereket, hanem azt, illetve azon keresztül rombolni vagy egyéb erőszakos, „hard” cselekményeket is végre akarnak hajtani.

Eszközök

Az előzőekben megvizsgáltuk, hogy kik azok valamiféle támadást képesek végrehajtani a hálózatokon keresztül, azokat felhasználva, vagy pont azokat támadva. Természetesen azt le kell szögezni, hogy a felsorolt személyeken kívül gyakorlatilag bárki végre tud hajtani egy információs támadást, akinek van megfelelő szaktudása, amely lehet akár rész-tudás is, azaz csak az adott támadási mód kivitelezéséhez, illetve az adott cél támadásához elegendő, illetve rendelkezi hálózati hozzáféréssel és eszközökkel. Rögtön adódik persze a kérdés, hogy számtalan ember van, aki mindezekkel rendelkezik, és mégsem követ el ilyen támadásokat. Szerencsére csak nagyon kevesekben van ott az a bizonyos motiváció, ami elindíthatja magát a támadást vagy annak kísérletét.

A következőkben megvizsgáljuk azokat az eszközöket és módszereket, amelyekkel, a kellő szaktudással, felszereléssel és nem utolsósorban motivációval rendelkező emberek a támadásokat végre is tudják hajtani.

Ezek a módszerek alapvetően két nagy kategóriába lehet sorolni: a rosszindulatú szoftverekre, mint eszközökre, illetve a többnyire ezeket is felhasználó támadási módszerekre.

Rosszindulatú szoftverek - Malwarek (Malicious Software):

Malware-eknek általában azokat a programokat hívjuk, amelyek anélkül lépnek a számítógépbe, hogy arra a felhasználó engedélyt adott volna (vagy ennek az engedélynek a tudatában lenne), ott végrehajtó objektumokat – programokat – módosít, illetve a gépben kárt okoz, vagy ennek potenciális volta fennáll. Potenciálisan a következő károkat okozhatják:

- erőforrásokat foglalnak le (memória, lemezterület, processzorteljesítmény);
- adatvesztést, adatmódosítást, hardver hibát okozhatnak;
- eltávolításuk időt és energiát igényel.

Abban az esetben, ha nem csak anyagi haszonszerzés (cyber crime), vagy esetleg csak a „szakértelem" bizonyítása a cél ezekkel a rosszindulatú szoftverekkel, hanem akár ideológiai, akár vallási vagy politikai okok is munkálnak a háttérben, akkor hatványozottabban jelentkezhetnek a károk.

Havonta több rosszindulatú szoftver, illetve eljárás jelenik meg. A következőkben néhányat mutatunk be, vizsgálva annak potenciális – cyber terror – veszélyét.

Program típusú malware: [12]

- számítógépvírusok és programférgek:
  a vírusok technikai értelemben olyan rosszindulatú programok, amelyek saját programkódjukat egy másik programhoz hozzáfűzik és így szaporodnak. A kapcsolódás módjai különbözőek lehetnek, például a vírus saját programkódját beleírja a gazdaprogram kódjába, azaz módosítja azt. Az egyik rendkívül veszélyes fajtája a vírusoknak a makrovírusok. Ezek célpontjai a dokumentumfájlok és ezeken keresztül is érkeznek, illetve szaporodnak.
  A programférgek (worms) olyan önállóan futó, gazdaprogramot nem igénylő programok, amelyek képesek saját maguk megsokszorosítására. Másolataikat részben a megtámadott számítógép merevlemezén készítik el, részint pedig a hálózaton keresztül juttatják el.

- vírusfejlesztő kitek:
  a vírusfejlesztő kitek olyan szoftverek, amelyek vírus program megírását és fejlesztését szolgálják. Ezek segítségével komolyabb szoftverfejlesztői vagy programozói tudás nélkül is lehetőség van vírusok megírására és előállítására.

- trójai és backdoor programok:
  *a trójai programo*k látszólag, vagy akár valóságosan is hasznos funkciókat látnak el, de emellett olyan nem kívánt műveleteket is végrehajtanak, amelyek adatvesztéssel járnak. Például adatokat módosítanak, könyvtárakat, adatállományokat törölnek, stb. A backdoor programok eredetileg a rendszeradminisztrátorok, vagy rendszer felügyeleti jogokkal rendelkező személyek részére nyitottak olyan lehetőségeket, hogy a kívánt számítógépet távolról is elérjék, és azon különböző javításokat illetve beállításokat végezzenek. A rosszindulatú backdoor programok azonban jogosulatlanul próbálnak meg „hátsó ajtókat" nyitni a rendszerhez. Többségük e-mail

mellékletként, vagy egyéb letöltés „mellékleteként” érkezik. Az igazi veszélye backdoor programoknak az, hogy ezek remek megoldásokat nyújtanak a rendszeradminisztrációs jogok megszerzésére.

- dropperek:
  a dropperek a trójai programok speciális fajtájának tekinthetőek, mivel hasonló elven kerülnek a számítógépbe. Ott azonban legyártanak kettő vagy több, az operációs rendszer által futtatható vírust, majd elindítják azokat. Mivel nem saját magát másolja a program, hanem új programot állít elő, ezért ezeket nem lehet a klasszikus vírus kategóriába sorolni.

- kémprogramok:
  a kémprogramok a rendszerbe juttatva, ott elrejtőzve, a háttérből figyelik a rendszer eseményeit és ezekről jelentéseket, illetve adatokat küldenek.

- keyloggerek:
  a keyloggerek a háttérben települve a billentyűleütéseket – így akár a jelszavakat, bankkártyaszámokat, azonosítókat is - rögzítik és juttatják ki ezeket az információkat a hálózaton keresztül.

- egyéb kártékony programok.

Vannak azonban olyan malwarek, amely nem programként tipizálhatóak, hiszen ezek nem konkrét szoftverek, hanem valamilyen szövegként jelentkeznek, és így jelentenek veszélyt. Néhány szöveg típusú malware:

- spam:
  a spam kéretlen leveleket jelent, amelyek igen változatos témában, ráadásul időnként rendkívül nagy számban érkeznek egy-egy számítógépre. A nagy szám miatt sávszélességet és tárhelyet foglalnak, illetve kiválogatásuk a többi – várt és számunkra hasznos – elektronikus levél közül idő- és energiaigényes.

- Hoax:
  a spam egyik speciális csoportja, amelyekben vagy valamilyen veszélyre (vírus, spam, csatolt file) figyelmeztetnek, vagy valamilyen nyereményt (szerencsét) helyez kilátásba, ha x helyre továbbítjuk őket. Több veszélyt rejt magában, hiszen amennyiben x helyre továbbítjuk ezeket akkor sávszélességet és tárhelyet foglalunk le, ugyanakkor lehetnek ezek önmagukban például trójait tartalmazó melléklettel ellátottak is.

- Holland és spanyol lottónyeremény levelek, nigériai csalások:
  az emberek naivitására és gyanútlanságára építő e-mail alapú malwerek. Vagy valamilyen lottónyereményt ígérnek, amely átvételéhez csak be kell fizetnünk néhány tíz dollárt, vagy valamilyen nigériai (olaj) üzletember zárolt bankszámlájának a feloldásához kérnek tőlünk segítséget, természetesen részesedés fejében, amelyhez szintén csak át kell utalunk néhány száz dollárt.

- Phishing:
  az utóbbi idők egyik legelterjedtebb csalásra, illetve az emberek hiszékenységére és megtévesztésére épülő eljárása. A phising, azaz az „adathalászat” eljárása roppant

egyszerű. Látszólag a bankunktól érkezik egy e-mail, amelyben arra szólítanak fel, hogy valamilyen banki átalakítás után legyünk kedvesek adatot egyeztetni. Ehhez előzékenyen meg is adnak egy linket, amely látszólag a bank oldalára mutat. Rákattintva erre a hivatkozásra a bankéhoz látszólag tökéletesen megegyező honlapra kerülünk, ahol kérik a login nevünket, jelszavunkat és elektronikus azonosítónkat is. A honlap azonban csak látszólag a banké. A csalók az eredeti banki oldalhoz a megtévesztésig hasonló oldalra navigálták így a felhasználókat, akik közül sokan bedőlnek és meg is adják adataikat. Ezeket az adatokat azután a csalók elektronikus vásárláshoz, vagy pénzátutaláshoz használják a saját céljaikra. A bankok és a média tömeges és látványos, a veszélyre figyelmeztető felhívásokat tesznek közre időről-időre, de ennek ellenére még mindig euró milliárdokra tehető a phishing-el okozott veszteség Európában.

- Pharming:
  szofisztikáltabb megoldás az adathalászatra, amely a számítógépen található *hosts* fájlba írja bele a meghamisított banki oldalak címét. Ennek megfelelően a megtámadott számítógépen a felhasználó hiába írja be böngésző címsorába bankja URL címét, a címfeloldás nem a megszokott DNS-szerveren történik, hanem helyben, az átírt hosts fájl segítségével, és az ügyfél a hamis banki oldalon találja magát, ahol gyanútlanul megadja adatait.

- Egyéb, szöveges típusú kártékony tartalmak.

A rosszindulatú programokon kívül – egyrészt azokat felhasználva, másrészt azokat kiegészítve számos egyéb eljárást találunk, amelyekkel támadható egy hálózat, és amelyekkel kár okozható azokban. Mivel az esetek túlnyomó többségében a hálózatok egymástól nem függetlenek, hanem egymásra épülnek, kapcsolódnak egymáshoz, sokszor feltételezik egymás szolgáltatásait vagy megoldásait, ezért egy-egy hálózati támadás nagyon sok esetben más – kapcsolódó – hálózat működésére is hatással van. Gyakran az is előfordul, hogy nem is közvetlenül az a hálózat a célpont, ahol a beavatkozás történik, hanem egy másik – ehhez a hálózathoz –, kapcsolódó egyéb hálózat, illetve annak egyik számítógépe.

Néhány e támadási módszerek közül:

- denial of service,
- distributed denial of service, (CodeRed,nimda) –
- spamming, viral ~ (ld. love-letter),
- flooding (TCP SYN packet),
- man-in-the-middle attack,
- 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)
- és még sok más...

Ezek közül itt csak a Denial of Service-t (DoS), azaz a működésképtelenség elérését szolgáló túlterheléses támadásokat, vagy más néven a *szolgáltatás-megtagadással járó támadást*, illetve a distributed denial of service-t (DDoS), azaz a több helyről érkező, vagy elosztott

működésképtelenség elérését szolgáló túlterheléses támadásokat (más néven megosztott *szolgáltatás-megtagadással járó támadás)* vizsgáljuk meg röviden. Ennek oka egyrészt jelen írás terjedelmi korlátaiban keresendő, másrészt ezek a támadási formák ma a leggyakoribbak egy hálózat vagy egy rendszer ellen.

A DoS támadás a szolgáltatás teljes vagy részleges megbénítása, helyes működési módjától való eltérítése, amely történhet megosztva is, több forrásból (*DDoS)*.

A DDoS támadások összetettetek, amelyek a támadón és támadotton kívüli számítógépek kapacitásait, illetve a külső számítógépek nagy mennyiségét használja a támadáshoz. Az egyszerű DoS támadás szemtől-szembeni támadás, ahol egy nagyon erős „támadó" állomás és a célállomás van csak kapcsolatban, nincsenek közbeiktatott gépek. DoS támadó gép kialakítása kétféle módon lehetséges:

- egy automatizált eszköz (szoftver) felkutatja a hálózatra kapcsolódó, sebezhető számítógépeket. Amikor talál egyet, és képes megfertőzni azt, feltelepít egy rejtett támadóprogramot, amitől a megtámadott gép zombivá alakul;
- másik lehetőség, hogy a rejtett program telepítése számítógépes vírusokkal vagy trójai programokkal történik.

A támadás menete során a zombi gépek távolról vezérelhetőek egy mester gépről (a támadó gépéről). Ha elég gépet fertőzött meg a támadóprogrammal a mester állomás jelt ad a zombi gépnek vagy gépeknek, hogy kezdjék meg a támadást a kiszemelt célpont vagy célpontok ellen. Ekkor az összes zombi egyszerre elindítja a támadást, és bár egyenként kis mennyiségű adattal dolgoznak, mégis több száz, vagy akár százezer támadó gép esetén a sok kis adatcsomag eredménye hatalmas adatáramlás, mely a megtámadott gép ellen irányul.

A támadás során a támadó vagy támadók megpingelik a célba vett számítógépet. A pingelést általában számítógépes hálózatok hibakeresésére szokták használni. Pingeléskor néhány rövid kérést (csomagot) küldenek egy másik számítógép felé, amelynek válaszolnia kell erre a csomagra. Ezt használják ki a DDoS támadás során, ugyanis ha nagyobb mennyiségű csomag érkezik a megtámadott gépre, mint az arra képes lenne válaszolni (vagy már eleve fogadni), akkor az képes komoly fennakadást okozni a gép működésében, vagy akár teljesen össze is omlaszthatja annak operációs rendszerét, például Windows esetén kék halált[11] vagy Linux esetén kernel pánikot[12] is okozhat.[13]

Az eddig felsorolt – elsősorban informatikai – támadási eszközök és módokon kívül létezik még egy igen gyakran használt támadási mód. Ez nem más, mint a *Social Engineering*-nek nevezett módszer. Magyarul meglehetősen nehezen lehet visszaadni a fogalom megfelelőjét, ezért célszerű azt inkább körül írni azt. A social engineering azt a módszert, vagy módszereket jelenti, amelyekkel a hálózatba behatolni kívánó, vagy onnan adatokat megszerezni akarók úgy jutnak belépési kódokhoz, nevekhez, jelszavakhoz, hogy azokat a jogosult felhasználóktól ellopják, kicsalják, kizsarolják, vagy csak egyszerűen megtévesztik őket, ezzel kényszerítve a fontos adatok átadására őket.

Egy amerikai fiatalembert – Kevin D. Mitnicket – tartják az egyik legsikeresebb hackernek. Azonban Mitnick magyarul is megjelent könyvében[13] világosan rámutat, hogy a hackerek számára rendelkezésre álló számtalan eszköz közül a social engineering az egyik, és nagyon sok esetben az egyetlen, lehetőség a hálózatba való behatolásra. Az elmúlt két-három

[11] Windows operációs rendszer esetében a hibaüzenetet megjelenítő képernyőkép színére utaló elnevezés, amely akkor jelenik meg, amikor az operációs rendszer nem tud helyreállni egy rendszerhibából.

[12] Linux operaciós rendszer esetében, amikor a kernel olyan hibával találkozik, amelyet nem tud lekezelni, meghívja a *panic* (pánik) függvényt.

[13] Kevin D. Mitnick – William L. Simon: A legendás hacker [14]

év egyre erősödő tendenciái azt mutatják, hogy a támadások már nem elsősorban a különböző szervereket érik, hiszen azok védelme egyre inkább felveszi a versenyt a potenciális támadókkal, hanem a felhasználókat. Egyre inkább a felhasználó lesz a leggyengébb láncszem, hiszen annak naivitása, hiszékenysége, vagy csak egyszerűen nemtörődömsége az igazi támadható pont.

A hagyományos- és a cyber terrorizmus kapcsolata

Napjainkig mindezidáig egyetlen cyber terrorista, vagy annak nevezhető akció került napvilágra, amely az LTTE (Tamil Eelam Felszabadító Tigrisei) nevéhez fűződik. A szervezet aktivistái 1997-ben spamekkel árasztották el a világ különböző országaiban működő srí lankai követségek e-mail postaládáit. Az akció nagy kárt nem okozott, de felhívta a figyelmet az információs rendszerek sebezhetőségére. [15]

Az LTTE akciójából azonban látszik, hogy ez nem az a „valódi" cyber terrorista akció, inkább egy hagyományos terrorszervezet új dimenzióban, azaz a cyber térben elkövetett akciója.

Mindazonáltal annak a veszélye, hogy komoly, nagy károkat okozó, az internetet kihasználó, vagy éppen azt illetve az egyéb hálózatokat támadó valódi cyber terrorista események bekövetkezhetnek igencsak reális. Bizonyítja ezt az is, hogy az FBI (Federal Bureau of Investigation) már konkrét definícióval is rendelkezik, amely elég világosan meghatározza a cyber terrorizmus fogalmát. E szerint: „*a cyber terrorizmus olyan bűncselekmény, amelyeket számítógépekkel és telekommunikációs lehetőségekkel 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*."[16]

A különböző helyi vagy nemzetközi konfliktusok idején gyakran tapasztalható, hogy az adott felek szimpatizánsai az interneten is kifejezik véleményüket különböző támadásokkal, amelyek nagyban hasonlítnak a hacktivisták akcióihoz. Így történt ez az izraeli csapatok Gázába történő újbóli 2006. nyarán történt benyomulása esetén is, amikor palesztinokat támogató hackerek 750 izraeli honlapot törtek fel, és megtámadták az Izrael legnagyobb bankját is.[18]

Bár nem kapcsolható közvetlenül terrorista szervezetekhez az *Electronic Intifada* (EI) – Elektronikus Intifáda[14] weboldal, amely ars poeticája szerint az izraeli-palesztin konfliktust próbálja meg bemutatni egy másik – ebben az esetben palesztin – szemszögből, Izraelnek

[14] Az intifada – Az izraeli megszállás elleni palesztin népfelkelés. Az ún. első intifada 1987 decemberében kezdődött, miután egy izraeli katonai teherautó a Gáza-övezetben – valószínűleg véletlenül – palesztinok közé hajtva négy embert halálra gázolt. A zavargások 6 éven át tartottak a Gáza-övezetben és Ciszjordániában. A felkelés, ill. ellenállás sajátos formájaként palesztin fiatalok rendszeresen kövekkel dobálták az izraeli katonákat, de sor került sztrájkokra és tüntetésekre is. Az izraeli katonák válaszul fegyvert is használtak és több száz embert bebörtönöztek. A válaszlépések közé tartozott a gazdasági szankciók életbe léptetése is, valamint további telepek létesítése a megszállt területeken. Az összetűzéseknek 2000 palesztin és 200 izraeli esett áldozatul. Az első intifadának az 1993-as oslói béke-megállapodás vetett véget. A második intifada, amelyik még jelenleg is tart, 2000. szeptember 29-én kezdődött. Ennek kiváltó oka az volt, hogy Ariel Sharon, akkori ellenzéki Likud-pártvezető megjelent Jeruzsálemben a Templomhegyen és miután ott található az Al-Aksza Nagymecset, a palesztinok provokációnak vették a látogatást. Ugyanakkor vannak olyan vélemények is, hogy mindez csak ürügy volt egy már korábban tervbe vett felkelésre. Az előző intifadához képest jelentős változás, hogy az izraeli katonasággal történő nyílt összecsapás helyett a palesztinok kis fegyveres csoportok, ill. egyéni öngyilkos merénylők bevetésével veszik fel a harcot. [17]

erről biztosan más a véleménye, hiszen láthattuk a terrorista kontra szabadságharcos, illetve az azokat támogatók besorolása igencsak nézőpont kérdése.

2. ábra:
Az EI bemutatkozása [19]

Az világosan látszik az eddig elmondottakból, hogy az igazi, és ki kell mondani – reális – veszélyt az jelenti, amennyiben a hagyományos terrorizmus találkozik a cyber terrorizmussal.

Bár nehéz meghúzni a határt a cyber térben elkövetett bűnözés, amely mint láttuk, bár sokszor rendkívül nagy szakértelmet igényel, mégsem különbözik sokban a köztörvényes bűnözéstől (leszámítva természetesen azt a tényt, hogy ez nem a hagyományos dimenzióban, hanem a cyber térben végzi tevékenységét), valamit a cyber terrorizmus között. A cyber terrorizmust azok a tényezők különböztetik meg a cyber bűnözéstől, amelyeket a hagyományos terrorizmusnál is feltérképeztünk, azaz a motiváció – ideológiai, vallási, vagy politikai –, és természetesen a célok, hiszen a cyber terrorizmusnak nemcsak az anyagi haszonszerzés a célja, hanem a kitűzött politikai célok elérése is terrorista eszközökkel: megfélemlítéssel, terrorral.

Mégis azt kell mondanunk, hogy mindezidáig nem láttunk példákat, amelyek igazi cyber terrortámadásokra utaltak volna. Nem voltak olyan – a cyber térből érkező – támadások, amelyek egyértelmű célpontjai a kritikus információs infrastruktúrák lettek volna. Ez persze, mint ahogy jelen írásból talán ki kis derül, nem jelenti azt, hogy nem is lehetnek ilyen támadások. Sajnálatos módon infrastruktúráink jelentős része igen komoly mértékben sebezhető és támadható, akár azokkal az eszközökkel és módszereket, amelyeket ehelyütt is tárgyaltunk. Az is nyilvánvaló és az eddig elmondottakból szintén következik, hogy a hagyományos terrorizmus, illetve a potenciálisan meglévő cyber terrorizmus közös, esetenként egymást kiegészítő, párhuzamos támadásai a legsebezhetőbb, ráadásul a mindennapi élethez nélkülözhetetlen információs infrastruktúráink ellen, beláthatatlan anyagi és humán károkat okoznának.

Abban az esetben amennyiben egy ilyen közös támadás, vagy az azzal való fenyegetés megjelenik, és azok valóban az információs rendszereinket célozzák, beszélhetünk *információs terrorizmusról*.

Az információs terrorizmus tehát:

> *A cyber-támadásokat és a hagyományos terrortámadásokat egyszerre alkalmazó olyan terrortevékenység, amely az információs infrastruktúrákat felhasználva, a kritikus információs infrastruktúra elleni támadásokkal próbálja meg célját elérni.*

FELHASZNÁLT IRODALOM:

[1] http://www.ezenanapon.hu/main.php?reszletes=414=9=5

[2] http://www.origo.hu/tudomany/tarsadalom/20011106iraes.html

[3] Hadtudományi Lexikon MHTT Budapest, 1995.

[4] http://www.enc.hu/1enciklopedia/fogalmi/poltud/vor_brig.htm

[5] Charles Townshend: A terrorizmus, Magyar Világ kiadó, 2001.

[6] http://www.fas.org/sgp/news/2003/01/dodweb.html

[7] Kovács László: A terrorizmus veszélye és a Magyar Köztársaság kommunikációs infrastruktúrája, Kommunikáció 2005 Budapest, ZMNE2005. 10. 27. ISBN 963 706011 1 p.: 187-198

[8] Haig – Várhegyi: Információs műveletek, Egyetemi jegyzet, ZMNE, Budapest, 2004.

[9] 2073/2004. (IV. 15.) Korm. Határozat: A Magyar Köztársaság nemzeti biztonsági stratégiája

[10] 2112/2004. (V. 7.) Korm. határozat a terrorizmus elleni küzdelem aktuális feladatairól

[11] https://www.sans.org/top20/

[12] Dr. Nagy Gábor: Phishing, pharming - mi jöhet még? http://it.news.hu/cikkek/2005-04-19/phishing_pharming_johet_meg/

[13] http://hu.wikipedia.org/wiki/DDoS

[14] Kevin D. Mitnick – William L. Simon: A legendás hacker – a megtévesztés művészete, Perfact-Pro Kiadó, Budapest, 2003.

[15] http://konfliktus.index.hu/sritigrisek.html

[16] Testimony of Keith Lourdeau, Deputy Assistant Director, Cyber Division, FBI Before the Senate Judiciary Subcommittee on Terrorism, Technology, and Homeland Security February 24, 2004 http://www.fbi.gov/congress/congress04/lourdeau022404.htm

[17] http://www.enc.hu/1enciklopedia/fogalmi/poltud/intifada.htm

[18] http://english.aljazeera.net/news/archive/archive?ArchiveId=24098

[19] http://electronicintifada.net/v2/article1387.shtml

Az előadás és a publikáció a Magyar Tudományos Akadémia Bolyai János Kutatási Ösztöndíjának támogatásával készült.

This paper and presentation was supported by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences