Berki Gábor
(berkigabor@uni-nke.hu)

Kiberháborúk, kiberkonfliktusok

Lektorálta: Dr. Botz László PhD.

Absztrakt

Az utóbbi néhány évben egyre több hírt hallunk számítógéphálózati támadásokról. A célpontok között szerepelnek nemzetközi nagyvállalatok, kormányzati szervek, pénzügyi vállalatok és kritikus infrastruktúrák is. Az ártó szándékú támadók, kihasználva a sebezhetőségeket, a saját – legyen az ideológiai, vallási, pénzszerzési vagy akár katonai – céljaik elérése érdekében korlátozni, bénítani igyekeznek az információs társadalom részegységeinek működését. Jelen tanulmány célja, hogy bemutassa, milyen konfliktusok voltak az elmúlt időben a kibertérben, milyen fenyegetésekre kell számítani a kibertérből, és hogy milyen kiberhadviselési potenciállal rendelkeznek a világ vezető hatalmai.

Kulcsszavak: kibertér, kiberbűnözés, kiberhadviselés, kiberháború

Abstract

In recent years there have been growing reports of attacks on computer network. Targets include international corporations, government agencies, financial firms and critical infrastuctures. Through the exploitation of this vulnerability attackers directed by malice intend to restrain and paralyze components of information society in order to achieve their personal – either ideological, religious, financial or military – goals. The author would like to examine, what kind of conflicts were the last time in cyberspace, what kind of threats shall be counted in it and what extent cyber warfare potential of the world leaders have.

Keywords: cyberspace, cybercrime, cyber warfare, cyberwar

1. Bevezetés

Napjainkra az információtechnológia olyan mélyen átszőtte a társadalmakat, hogy számítógépek nélkül elképzelhetetlenné vált nemcsak az ipari, a pénzügyi vagy a kormányzati munka, hanem a polgárok mindennapi élete is. Ezt bizonyítja az az adat is, mely szerint 2015 novemberében a Föld lakosságának 46,4%-a, több, mint 3,3 milliárd ember használt internetet. (Internet World Stats, 2015) Bátran kijelenthetjük, hogy a modern kori ember komoly függőségbe került az informatikai rendszerekkel. A mindennapokat megkönnyítő informatikai eszközök és szolgáltatások azonban komoly biztonsági kockázatokat is rejtenek. Egyre-másra jelennek meg azok a hírek, melyek különböző kibertámadásokról, kiberbűnözésről és kiberhadviselésről szólnak. Ahhoz, hogy megérthessük, hogy milyen fenyegetések érhetik a kibertérből eszközeinket és adatainkat, meg kell ismerkednünk néhány alapvető fogalommal.

2. A kibertér fogalma

Első és legfontosabb, hogy tisztázzuk a kibertér mibenlétét. Magát a fogalmat William Gibson tudományos-fantasztikus szerző alkotta meg 1984-es *Neurománc* című regényében. Úgy írta le, mint egy számítógép-hálózatok által teremtett világot, tele mesterséges intelligens lényekkel és felhasználók milliárdjaival. A Enciklopédia Britannica megfogalmazása szerint *„a kibertér egy alaktalan, vélhetően „virtuális" világ, amely számítógépek, internetképes eszközök, szerverek, routerek és az internet-infrastruktúra egyéb elemeinek összekapcsolása révén jön létre."* (Bussell, 1995) Hétköznapi megfogalmazásban számítógépek, számítógép-hálózatok, az ezeket összekötő kommunikációs csatornák, az itt futó alkalmazások és az itt tárolt adatok alkotta virtuális világ összefoglaló neveként hivatkozhatunk rá. Nagyon sok kutató, szervezet próbálta már meghatározni a kiberteret, ennek megfelelően nagyon sok definíció is született rá. Az Egyesült Államok Védelmi Minisztériuma által kiadott és 2016 februárjában pontosított katonai terminológiai szótárban meghatározottak szerint a kibertér *„az információs környezet egy globális tartománya, amely tartalmazza az informatikai infrastruktúrák, a bennük tárolt adatok*

egymással összefüggő hálózatát, beleértve az internetet, a távközlési hálózatokat, a számítógép rendszereket, valamint a beágyazott feldolgozó és vezérlő elemeket". (JP 1-02, 2016)

Hazánkban a kibertér hivatalos megfogalmazására a 2013-ban megjelent, a Magyarország Nemzeti Kiberbiztonsági Stratégiája nevet viselő 1139/2013. számú kormányhatározatban került sor. Eszerint „a *kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti. Magyarország kibertere a globális kibertér elektronikus információs rendszereinek azon része, amelyek Magyarországon találhatóak, valamint a globális kibertér elektronikus rendszerein keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok közül azok, amelyek Magyarországon történnek vagy Magyarországra irányulnak, illetve amelyekben Magyarország érintett.*"

A fenti meghatározásokból leszűrhető, hogy a kibertér az összekapcsolt elektronikus információs rendszerek és hálózatok összessége. Így a hálózatba nem kötött, önálló számítógépek nem részei a kibertérnek. Ha az összekapcsolás módját tekintjük, amely nemcsak vezetékes lehet, hanem vezeték nélküli is, a kibertér részének kell tekintenünk az elektromágneses spektrumot is, amelyen keresztül a kommunikáció történik. A vezeték nélküli kommunikáció legközismertebb formája a Wi-Fi, amely már szinte mindenhol elérhető, de ide kell sorolnunk a mobilhálózatokon keresztül igénybe vehető adatforgalmat is.

3. A kibertérből érkező fenyegetések

A következőkben vizsgáljuk meg, hogy milyen fenyegetések érkezhetnek a kibertérből. Alapvetően a támadások az informatikai rendszereken tárolt és kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, illetve a rendszerelemek rendelkezésre állása és funkcionalitása ellen irányulhatnak. Az adatok bizalmasságán azt értjük, hogy azt csak az arra jogosultak és csak a jogosultsági szintjüknek megfelelő mértékben ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról. A sértetlenség az

adat azon tulajdonsága, mely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyezik, nem történt benne illetéktelen változtatás. Ebbe beleértjük a hitelességét is, hogy a megfelelő forrásból származik-e. A rendelkezésre állás arra vonatkozik, hogy az adatot az arra jogosultak a szükséges helyen és időben elérhessék, használhassák. A rendszerelemek rendelkezésre állása pedig a rendeltetésszerű használat lehetőségét jelentik. (Muha, Krasznay, 2014 p10)

Ha megvizsgáljuk a támadások indítékait, csoportosíthatjuk a támadók körét, akiknek a szándékai, rendelkezésre álló erőforrásai és szaktudásuk eltérő lehet. A szakirodalmakban a fenyegetések többféle csoportosításával is találkozhatunk, de úgy gondolom, hogy jelen tanulmányban az általam legfontosabbnak tartott fenyegetéseket vizsgálom meg. Véleményem szerint ezek a

- kiberbűnözés,
- kiberkémkedés,
- hactivizmus,
- kiberterrorizmus,
- kiberhadviselés.

3.1. A kiberbűnözés

A kiberbűnözés tulajdonképpen számítógépek és számítógépes rendszerek segítségével, vagy számítógépek és hálózatok kárára elkövetett bűncselekmények gyűjtőfogalma. Motivációjáról az esetek többségében bátran kijelenthetjük, hogy az az anyagi haszonszerzés.

2001. november 23-án Budapesten 30 ország írta alá a Számítástechnikai Bűnözés Elleni Egyezményt, melyben részletesen leírták az ilyen típusú bűncselekményeket, az államok jogharmonizációjához szükséges lépéseket és az együttműködés kereteit. Három fő részre osztották a számítógépes bűncselekményeket.

1. *A számítástechnikai rendszer és a számítástechnikai adatok hozzáférhetősége, sértetlensége és titkossága elleni bűncselekmények*
   Idetartozik például a jogtalan belépés, az adatok vagy rendszerek sértetlensége elleni cselekmények vagy az eszközökkel történő visszaélés.
2. *Számítástechnikai bűncselekmények*
   Ez alatt a számítógépes hamisítás és a csalás fogalmának kifejtésére került sor.

3. *A számítástechnikai adatok tartalmával kapcsolatos bűncselekmények*
   Ez a passzus a gyermekpornográfiával szembeni eredményesebb fellépést lehetővé tévő intézkedéseket tartalmazza. (Számítástechnikai Bűnözés Elleni Egyezmény, 2001)

A szükséges intézkedéseket már minden ország megtette és beiktatta jogrendszerébe a megfelelő paragrafusokat, így könnyebbé vált a fellépés ezekkel a bűncselekményekkel szemben. A sikeres harc azonban így sem egyszerű, hisz ezen bűncselekmények jellemzői közé tartozik a gyorsaság és a nemzetköziség, amely nagyon megnehezíti a felderítést. Ahogy az internetpenetráció növekszik a világban, úgy nő a kiberbűncselekmények száma és az általa okozott anyagi kár is. A Norton Cybercrime Report már 2012-ben 114 milliárd dollárra becsülte a bűnözők okozta kárt, a járulékos költségeket (termeléskiesés, helyreállítás költségei), pedig 274 milliárd dollárra, amely így együtt már meghaladta a kábítószerek illegális forgalmából keletkezett 288 milliárd dollárt. (Norton, 2012) Nem csoda, hogy napjainkra már a szervezett bűnözés is jelen van a számítógépes bűncselekmények elkövetői között. Kis kockázattal nagy hasznot tudnak realizálni.

Népszerű elkövetési módszer az adathalászat, amellyel különféle személyes adatokat, bankszámla-, bankkártyaadatokat szereznek meg és ezekkel élnek vissza. Nagyon kezd elterjedni a különféle titkosítást végző rosszindulatú programok terjesztése, amelyek a fertőzött gépen tárolt anyagokat titkosítják és csak a kért váltságdíj kifizetése után kapják meg a felhasználók a feloldáshoz szükséges kódot. Idén februárban jelent meg a Locky elnevezésű ransomware[1], amely makrók segítségével fertőzte meg a számítógépeket. A csalók kéretlen elektronikus levelekbe Word dokumentumokat helyeztek el. Amikor ezt a felhasználó megnyitotta, akkor az elé táruló dokumentum csak értelmezhetetlen karaktersorozatokat tartalmazott. Egy üzenetben arra kérték, hogy engedélyezze a makrókat a fájl tartalmának megtekintéséhez. Ha ezt is megtette, akkor rögtön megfertőződött a számítógépe és elkezdődött a rombolás. A károkozó dokumentumokat, fotókat, videókat tesz használhatatlanná. Mindössze azokat a könyvtárakat hagyja érintetlenül, amelyek a Windows

1 Olyan rosszindulatú számítógépes program, amely valamilyen fenyegetéssel próbál pénzt kicsikarni a felhasználóból.

működéséhez feltétlenül szükségesek. Ez után üzenetben közli a váltságdíj összegét és a fizetési módot. Sok esetben a kért összeg átutalása után sem küldik el a titkosítás feloldására szolgáló kódot. A zsarolás másik formája, amikor vállalatokat, webáruházakat fenyegetnek meg, hogy amennyiben nem fizetnek, elérhetetlenné teszik az oldalaikat.

A kiberbűnözés elleni harc egyik fő fegyvere lehet a felhasználói tudatosság növelése, nem lehet eleget beszélni a körültekintő internethasználatról, hisz a megkárosított felhasználók jelentős része saját internetes tevékenysége folytán kerül a bűnözők csapdájába.

3.2. A kiberkémkedés

Azt tartják, hogy a kémkedés az egyik legősibb mesterség a földön. Nemcsak katonai titkok megszerzése jelent előnyt az ellenséggel szemben, hanem az ipari, pénzügyi, diplomáciai információk is az esetleges vetélytársakkal szemben. Az informatikai eszközök térnyerése és az internet elterjedése kifejezetten hasznos volt a kémek számára, hiszen egy jó felkészült támadó képes akár a világ másik végén lévő informatikai rendszerbe is behatolni és onnan adatokat letölteni. Az Egyesült Államok kiberbiztonsággal foglalkozó hatóságai 2002-től észleltek olyan informatikai behatolás sorozatokat, amelyek a katonai, a kormányzati és a vállalati szektor informatikai hálózatait érintette. A vizsgálatok szerint Kínához köthető hackerek hosszú időn keresztül precízen megtervezett és kivitelezett támadásokon keresztül 10-20 terrabájtnyi anyagot töltöttek le a megtámadott rendszerekről. Összehasonlításképpen, az amerikai Kongresszusi Könyvtár, amely a legnagyobb a világon, összes könyve kb. 10 terrabájt adatot tárol. Az akcióban, amely a Titan Rain nevet kapta, érintett volt a NASA, a Lockheed Martin és a Pentagon is. (Kovács, 2009)

2012 augusztusában tűnt fel egy új, kémkedésre kifejlesztett rosszindulatú program. A Gauss névre keresztelt vírus elsősorban banki és egyéb hozzáférési adatokat gyűjtött a fertőzött rendszerből, majd továbbította azokat a C&C[2] szerverek felé. Egy biztonsági cég szerint a Gauss elsősorban Libanonban, Izraelben és a Palesztin területeken volt aktív, de az Egyesült Államokból is jelentettek fertőzést. (CERT, 2012)

2 Command and Control – Irányító és vezérlő szerver

2013 januárjában a Kaspersky jelentette be, hogy leleplezett egy nagyarányú online kémkedési akciót. A vírusirtó cég által *Vörös októbe*rnek nevezett kártékony kód már 2007 óta volt aktív, főképp Kelet-Európában, a volt szovjet tagköztársaságokban, illetve Kelet-Ázsiában, de találtak fertőzött gépeket szerte a világon kormányszervezetekben, nagykövetségeken, kutatóközpontokban is. A vírus fő célja titkos dokumentumok megszerzése volt, de ezen kívül információkat gyűjtött a megfertőzött hálózatokról is. Ez a vírus is, akárcsak az előzőekben ismertetett kártevők, igen kifinomult volt és több, eddig ismeretlen metódust alkalmazott működése során. A terjedéséhez viszont régi, bevált módszereket, adathalász e-maileket, fertőzött weboldalakat, a Word- és Excel-sérülékenységeket használt. A program moduláris felépítésű, több mint ezer modult fejtettek vissza. Az egyik érdekes modul például a fertőzött számítógépre csatlakoztatott okostelefonokról, illetve a gépre dugott pendrive-okról le tudta menteni az érdekesnek tűnő tartalmat, még a törölt fájlokat is vissza tudta állítani ezekről. A forráskód, illetve az ahhoz fűzött megjegyzések orosz programozók munkájára engedtek következtetni. Persze az is elképzelhető, hogy ez csak az álcázás része volt és az orosz, illetve a programozói szlengben elterjedt kifejezésekkel csak félrevezetésből szórták meg az angol nyelvű megjegyzéseket a programsorok mellett. (Securelist, 2013)

Ezeknek az igen kifinomult kémprogramoknak a kifejlesztése nagyon nagy szakértelmet, anyagi és szellemi ráfordítást igényelt, minden ok megvan azt feltételezni, hogy kifejlesztésük mögött állami támogatás állhat.

3.3. A hacktivizmus

A következő fenyegetés, amelyet be kell mutatnom, a hacktivizmus. A szó a hacker és az aktivista szavakból alakult ki. Leghírhedtebb képviselőjük az Anonymous csoport. Ez a laza szerveződésű internetes közösség vélt vagy valós sérelmek megtorlásául vagy egyszerűen valamely ügyet felkarolva indít támadásokat internetes tartalmak, cégek, kormányzatok ellen.

Az Anonymous logója egy fej nélküli, babérkoszorúba foglalt öltönyös figura, tagjai pedig, ha utcára mennek vagy képet tesznek ki magukról a netre, akkor a *V mint vérbosszú* című filmből ismert mosolygó Guy Fawkes maszkot viselik, amelyet annak főhőse hordott.

Az Anonymous logója

(forrás: http://en.wikipedia.org/wiki/Anonymous_(group) letöltve: 2016. február 14.)

A közösség a 2003-ban alakult 4chan nevű képmegosztó oldal felhasználóiból verbuválódott. A kezdetben a japán képregények rajongóinak szóló oldal hamar nagy népszerűségre tett szert, tartalmában és stílusában azonban az internet sötét oldalához tartozik. A beszélgetések úgy általában a tizen-huszonéves internet, online pornó és videojáték-mániás amerikai fiatalok szellemi színvonalán zajlik, akik ebből ítélve az oldal törzsközönségét alkotják. Az obszcén tartalmairól és féktelen szabadosságáról ismert fórum, vagyis képes üzenő fala már kevesebb látogató számára érdekes és vállalható, de így is az internet egyik legnagyobb hatású oldala. Jellemző, hogy felhasználói a kortárs online popkultúra rengeteg fontos elemét termelték, termelik ki és dolgozzák fel újra folyamatosan. A 4chan mindezek ellenére, vagy talán épp ezért, az online tömegkultúra egyik termékeny alkotóműhelyévé vált, amelynek látogatói saját elvetemült humoruk és a Photoshop segítségével rengeteg internetes mémet, vagyis egy adott témára épülő, továbbküldés útján terjedő, folyamatosan remixelt műalkotást dobnak be a köztudatba. A 4chanról származnak például a lolmacskák, vagyis az internetes szlengben feliratozott vicces macskás képek. (Vámosi, 2010)

Ebből a közegből származik tehát az Anonymous, melynek fontos eszköze a weboldalakat automatikus lekérdezésekkel megbénító túlterheléses támadás, amire magasztos hangnemben megfogalmazott webes szórólapjain tobo-

rozza a résztvevőket, rendszerint nem csak a 4chanon, hanem más csevegő szobákban és fórumokon is. A szaknyelven dosolásnak[3] nevezett támadásokban való részvételhez nem is kell más, csak pár ingyenesen letölthető szoftver, amelyek beszerzéséhez, használatához a felhasználók rendszerint már a szórólapokon megkapják a szükséges instrukciókat. 2007-ben először így bénították meg a rasszista kijelentéseiről elhíresült amerikai rádiós, Hal Turner műsorát, noha a 4chanon mindennapos dolog a niggerezés vagy más népek, országok alpári stílusú pocskondiázása. A következő nagy támadás a szcientológiai egyház ellen indult 2008-ban. Tiltakozásul az egyház által véleményük szerint elkövetett csalások, illetve az egyház által állítólag végzett agymosások miatt, kiterjedt támadásba kezdtek ellenük. A szolgáltatásmegtagadásos támadásokon kívül, amellyel elérhetetlenné tették az egyház honlapját, nyilvánosságra hoztak több száz iratot és dokumentumot, amelyeket számítógépes betörések útján szereztek. (Nemes, 2008)

Saját meghatározásuk alapján tiltakoznak és fellépnek minden olyan jelenség ellen, amely a szólásszabadságot és az internet szabadságát veszélyeztetik.

Ebbe belefért a Sony ellen indított támadás is, mely során több millió felhasználó adatait, köztük bankkártyaszámait lopták el és tették nyilvánossá azért, mert a Sony perbe fogta azt a hackert, aki feltörte a PlayStation védelmét.

A legnagyobb port felvert támadássorozatuk a Wikileaks támogatását megakadályozó amerikai intézkedések miatt következett be. Mint az ismeretes, 2010-ben a Wikileaks több ezer titkos amerikai diplomáciai és katonai iratot jelentetett meg az interneten a szólásszabadság jegyében. Ez komoly diplomáciai feszültséget és még komolyabb biztonsági problémákat okozott, elsősorban az amerikai hadsereg műveleti területein. Az amerikai kormány erős politikai nyomást fejtett ki az oldal ellehetetlenítésére, többek között a finanszírozásával kapcsolatban. A PayPal, a Visa vagy a MasterCard e nyomás hatására nem engedélyezte a Wikileaks számláira történő utalásokat. Ennek hatására hirdette meg az Anonymous a fenti pénzintézetek elleni támadássorozatát, amelyben sikerült is kisebb fennakadásokat okozni. Ezekért a támadásokért 2013-ban 13 embert el is ítélt egy amerikai szövetségi bíróság. (Rawlings, 2013) 2015-ben a párizsi Charlie Hebdo szerkesztőségét ért táma-

3 DOS – Denial of Service – szolgáltatásmegtagadással járó támadás

dás, majd a novemberi 129 emberéletet követelő merénylet után háborút hirdettek az Iszlám Állam ellen. (Dubuis, 2015) Feltörték a terrorszervezet több szerverét, hozzájuk köthető Twitter és Facebook fiókokat és adataikat nyilvánosságra hozták.

Létezik az Anonymous csoportnak magyar szárnya is, Facebook oldaluk is van, ahol a hitvallásukat is közzétették:

> *„Anonymous vagyunk. Egy eszme vagyunk. A pénzügyi és politikai zsarnokság ellen küzdünk itthon és globális szinten, Egy emberibb világot akarunk, ahol nem a profit, a hatalom, az erőszak számít, hanem az igazság, a szabadság, az egyenlőség. Változást szeretnénk elérni: a tudás, az információ nyílt áramlását, a cenzúra eltörlését, a szúk, kapzsi elit uralmának a végét és a 99% valódi hatalmát. Közvetlen demokráciát, igazi beleszólást akarunk. A jelenlegi rendszer igazságtalan, embertelen és végpusztulás felé sodorja a civilizációt. Nincsenek vezetőink, nincsenek rendszabályaink, nincsenek bombáink, Sokan vagyunk, napról-napra egyre többen vagyunk. Légiót alkotunk. Nem felejtünk, nem bocsájtunk meg. Számolj velünk és számíts ránk! Csatlakozz hozzánk és legyél részese egy győztes forradalomnak!" (Anon, 2012)*

Magyarországi tevékenységük weboldalak feltörésével kezdődött; 2012. március 4-én feltörték az Alkotmánybíróság honlapját és átírták az Alaptörvény szövegét, április 8-án a Nemzeti Rehabilitációs és Szociális Hivatal következett. Augusztus 28-án túlterheléses támadást intéztek a Közgép Zrt. honlapja ellen, amelyet sikerült is egy rövid időre megbénítani. A magyar Anonymous saját csoportjának méretét 50-60 aktív főre tesz, akik állandóan akcióra készek, valamint további 150-200 fő elkötelezett követőre. Legutóbb 2016. február 23-án a Nemzeti Választási Irodánál történt incidens kopasz résztvevőit fenyegették meg személyes adataik nyilvánosságra hozatalával.

Hosszan sorolhatnánk a csoport által elkövetett támadásokat, a világ szerzői jogvédő hivatalaitól az arab tavasz támogatásán át a világméretű pedofilhálózat feltöréséig.

Céljaik néhány esetben támogathatók ugyan, de a módszereik veszélyesek és egyértelműen törvénytelenek. Nincsenek nevesített vezetőik, szervezetük

decentralizált és tagjaik a világ minden részén megtalálhatók. Az, hogy milyen célpontot támadnak sikeresen, attól is függ, hogy mennyi támogatót tudnak megnyerni maguknak.

Nagyon sok politikus, újságíró jelentette már ki, hogy az Anonymous csoport tagjai kiberterroristák. Én ezzel a véleménnyel nem értek egyet, szerintem a hacktivizmust nem lehet összemosni a terrorizmussal, mert nekik nem céljuk a pánikkeltés és az erőszak.

3.4. A kiberterrorizmus

Ma már közhelynek számító kifejezés, hogy a világ megváltozott 2001. szeptember 11-e óta, amikor is az Al Kaida terrorcsoport lerombolta New Yorkban a World Trade Center ikertornyait. Több milliárd ember nézte a Földön élőben, ahogy a füstölgő épületek összeomlanak. Kétségtelen, hogy ez volt a legnagyobb szabású terrortámadás, ami eddig történt. Oszama Bin Laden és társai örülhettek, hisz sikerült megleckéztetni az Egyesült Államokat, az amerikaiak mindennapjaiba becsempészni a rettegést. Végül is ez a terrorizmus célja, a fenyegetés, a félelemkeltés, a társadalombefolyásolás. A Hadtudományi Lexikonban található definíció szerint:

„Terror, megkülönböztetés nélküli támadás: minden olyan erőszakos cselekmény, vagy azzal való fenyegetés, amelynek elsődleges célja, hogy rettegést keltsen a polgári lakosság körében." (Hadtudományi Lexikon, 1995 p1324)

Míg a 70-es évek terrorcselekményei elszigetelt jelenségek voltak és csupán néhány országot érintettek, mára már világméretűvé vált a fenyegetettség, gondoljunk csak az Iszlám Állam vagy a Boko Haram rémtetteire.

A terroristacsoportok is kihasználják a korszerű technológiák adta lehetőségeket, melyek segítségével gyorsabban, hatékonyabban tudják a számukra fontos információt megszerezni, illetve célközönségük irányába eljuttatni.

Ha az információtechnológia terrorista célú alkalmazását vizsgáljuk, akkor több területet is kiemelhetünk, a teljesség igénye nélkül:

3.4.1. Kapcsolattartás

Mivel a hagyományos vezetékes és mobiltelefonok könnyedén lehallgathatók a hatóságok által, ezért az internet nyújtotta kommunikáció nagyon népszerű a terrorista szervezetekben. A sok helyről letölthető és könnyen kezelhető

titkosító programok segítségével kódolhatják az üzeneteiket, így nehezítve meg a felderítésüket. Az utóbbi időben előszeretettel használják a különböző játékkonzolok játékainak azon funkcióit is, amelyek segítségével a játékosok kommunikálhatnak egymással.

3.4.2. Információszerzés

Közhelynek hangzik, de valóban igaz, hogy amit nem lehet megtalálni az interneten, az nem is létezik. Tudják ezt a terrorista szervezetek is, és ki is használják az akcióik tervezéséhez. Ha beírjuk a Google keresőjébe a „How to make a bomb" mondatot, 153 000 000 találatot kapunk 0,66 másodperc alatt. Itt videók tömkelegét is megtaláljuk, amelyek lépésről lépésre mutatják be a bombakészítés módszereit. De a terrorakciók szervezéséhez jó szolgálatot tehet a Google Earth vagy a StreetWiev is, melyeken nagyszerűen fel lehet térképezni akár egy potenciális támadás környezetét is. Számos épület 3D-s látványképei és alaprajzai is megtalálhatók a neten. A lehetőségek széles tárházát támasztja alá egy al-Kaida kézikönyv, ami szerint nyilvános forrásokból, többnyire az internetről a szükséges információk 80%-a megszerezhető. (Timothy, 2003.) Nem véletlen, hogy 2003 januárjában Donald Rumsfeld akkori amerikai védelmi miniszter kiadott egy utasítást, mely szerint azonnal radikálisan csökkenteni kell az Amerikai Védelmi Minisztérium és egyéb USA-intézmények olyan weboldalainak a számát, illetve tartalmát, amelyeken keresztül különböző terrorszervezetek szenzitív információkra tehetnek szert, vagy a különböző honlapokon különkülön meglévő adatok felhasználásával juthatnak értékes – az USA számára pedig hihetetlenül veszélyes – következtetésekre. (Kovács, 2006.)

3.4.3. Propaganda

Az internet nagyon lényeges eszköz a terroristáknak az eszméik, szervezeteik, hőseik és tevékenységük bemutatására, hiszen a hagyományos médiákat nem használhatják propagandacélokra. Ezért saját weboldalakat üzemeltetnek itt számolva be tetteikről, céljaikról. Mindig hangsúlyozzák, hogy az ellenségeik hajthatatlansága miatt, céljaik elérésére nincs más lehetőségük, mint az erőszak. Saját magukat szabadságharcosnak állítják be, és így próbálnak szimpátiát ébreszteni maguk és az ügyük iránt. A könnyen befolyásolható embereket akár terrorcselekmények elkövetésére is ösztönözhetik az ilyen oldalak. Ez

a fajta propaganda sajnos nem hatástalan, az utóbbi idők magányos terroristái, mint például **Mohamed Merah, a toulouse-i merényletek elkövetője** 2012-ben **vagy a 2009-ben** az amerikai Fort Hood támaszponton 16 katona életét kioltó *Nidal Malik Hasszán* is lelkes olvasója volt ezeknek az oldalaknak. (Hess, 2009) Az Iszlám Állam is előszeretettel használja toborzásra, merényletek végrehajtására történő felbujtásra.

3.4.4. Adománygyűjtés

A terrorista szervezetek működésük finanszírozásához is felhasználják az internetet, weboldalaikon, fórumokon gyűjtenek adományokat. Az al-Kaida, függetlenül Oszama bin Laden jelentős magánvagyonától, mindig is függött a különböző adományoktól. Globális adománygyűjtő hálózatokat építettek ki, amelyek különböző alapítványokon, államoktól független szervezeteken és pénzintézeteken alapultak. Egy szunnita szélsőséges csoport, a Hizb al-Tahrir Európától Afrikáig terjedő internetes hálózatot használ erőfeszítései pénzbeli és elvi támogatására. Az IRA weboldalán pedig a látogatók hitelkártyával tudnak támogatást nyújtani. (Haig, 2007.)

Figyelemmel kísérik a közösségi oldalakat is, ahol azokat a felhasználókat, akik pozitívan nyilatkoznak hozzászólásaikban róluk, e-mailben keresik meg, hogy támogatást kérjenek tőlük. Az iszlám vallás öt alappillérének egyike a zakat, amely a muszlim vallású emberek számára kötelezővé teszi az anyagilag nehéz helyzetben lévő hittestvérek segélyezését. Ezt kihasználva számos olyan iszlám jótékonysági szervezet működik a világban, amely valójában terrorszervezetek finanszírozásában érdekelt. Természetesen nem terrorcselekmények támogatását kérik az olvasóktól, hanem árvaházak, gyermekek támogatását. Ez sok esetben hatásos érvelésnek bizonyul.

3.4.5. Pszichológiai hadviselés

Mint azt már említettem, a terrorizmus célja a fenyegetés, a félelemkeltés, a társadalombefolyásolás. Ennek nagyszerű eszköze az internet, ahol számos módja van a pszichológiai hadviselésnek, mint pl. félretájékoztatások, fenyegetések kézbesítése, félelem elültetése képek, videófelvételek bemutatásával stb. A legjobb példa erre az Iszlám Állam, amely professzionális szintre fejlesztette ezt a tevékenységet. Nap-nap után töltötték fel a különböző videó-

megosztó helyekre a hatásosan megvágott, HD minőségben felvett videóikat, elrabolt emberek lefejezéséről, elfogott katonák tömeges kivégzéséről. Ezekkel a felvételekkel nemcsak a keresztény világnak üzentek, hanem az ellenük harcoló muszlimoknak is. A módszer működött is, hisz katonai sikereiket nem egyszer az iraki vagy a szír hadsereg megfutamodásának köszönhették.

3.4.6. Kibertámadások

Ne legyenek illúzióink, mert ha egy terrorszervezetnek lenne lehetősége kritikus infrastruktúrák elleni kibertámadásra, amellyel emberéleteket is veszélyeztetne, habozás nélkül megtennék. Szerencsére azonban még nincsenek birtokában annak a tudásnak, mely ilyen támadás kivitelezéséhez szükséges. Már törtek be rendszerekbe, loptak el adatokat, cseréltek le honlapokat, de komolyabb támadást még nem sikerült véghezvinniük. Az nyilvánvaló, hogy ha egy hagyományos terrortámadást össze tudnának vonni egy kibertámadással, amely egymással összefügg, komoly károkat okoznának.

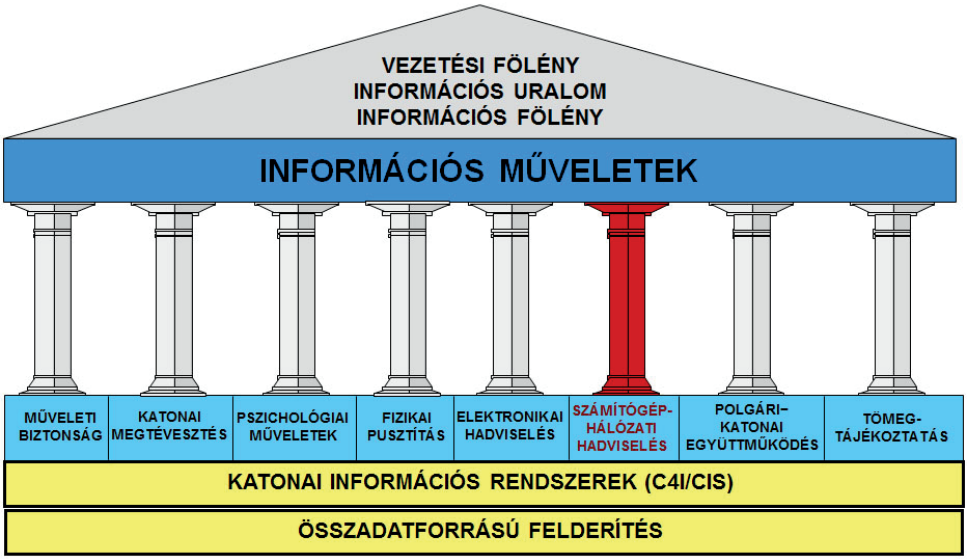
A hagyományos fegyverekkel végrehajtott támadások kibertámadásokkal való ötvözése már a kiberhadviselés témaköréhez tartozik.

4. Kiberhadviselés

A kiberhadviselés részletes ismertetése előtt meg kell ismerkednünk a katonai műveletekben elfoglalt helyével. A magyar terminológiában számítógéphálózati hadviselésként definiált tevékenység az információs műveletek szerves részét képezi. A NATO-ban az információs műveleteket az AJP 3.10-es doktrína taglalja, míg a Magyar Honvédségben a 2014-ben kiadott Információs Műveletek Doktrína foglalkozik vele. Az információs műveletek keretében egymással szorosan összefüggő tevékenységeket integrálunk annak érdekében, hogy a katonai műveletekben elérhessük az információs fölényt, ennek következtében kivívjuk az információs uralmat, majd a vezetési fölényt azáltal, hogy a saját oldali vezetési ciklus számára időcsökkentést, a szemben álló félnél pedig időnövekedést érünk el. Ez biztosíthatja, hogy elérjük a hadműveleti fölényt is. Ezen tevékenységek a fizikai, az információs és a tudati dimen-

ziókban fejtik ki hatásunkat. Részét képezi az elektronikai hadviselés, a pszichológiai műveletek, a műveleti biztonság, a katonai megtévesztés és a fizikai pusztítás is. (Haig, Várhegyi, 2005 p185) Az alábbi ábra mutatja be a számítógéphálózati hadviselés helyét az információs műveletekben.

2. ábra Számítógéphálózati műveletek helye az információs műveletekben



(forrás: Haig, Várhegyi, 2005 p198)

Az Egyesült Államokban egy kicsit másfajta megközelítést használnak a katonai szakértők. Egy új műveleti elgondolást dolgoztak ki, amelyet a 2014-ben elfogadott FM 3-38 Kiber-elektromágneses tevékenységek (Cyber Elecromagnetic Activities) nevet viselő doktrínában jelent meg. Lényege, hogy integrálják és szinkronizálják az elektronikai hadviselést, a kiberműveleteket és a frekvenciamenedzsment-műveleteket annak érdekében, hogy egymást kiegészítő és erősítő hatásokat érjenek el. Könnyen belátható, hogy a fenti tevékenységek közötti együttműködés hiánya csökkentené a műveletek hatékonyságát, az elektromágneses spektrumot használó eszközök és rendszerek között nem kívánt ütközéseket és interferenciákat hozhatna létre. (Haig, 2015 p122) A doktrína meghatározása szerint „ *A kiber-elektromágneses tevékenységek azok a tevékenységek, melyek biztosítják a szemben álló féllel és az ellenséggel*

szembeni előny megszerzését, megtartását és kihasználását a kibertérben és az elektromágneses spektrumban egyaránt, miközben akadályozzák és csökkentik a szemben álló fél és az ellenség lehetőségeit ugyanerre és megóvják a saját vezetésirányítási rendszert."(FM 3-38, 2014)

Ezt a koncepciót az alábbi ábra szemlélteti:

3. ábra Kiber-elektromágneses tevékenységek

(forrás: Kovács Z. 2014)

A számítógéphálózati hadviselést két fő csoportra oszthatjuk. A támadó jellegű műveletekre, melynek célja az ellenség hálózatba kötött informatikai rendszereinek feltérképezése, működésük befolyásolása, lerontása, megbénítása és a védelmi jellegű tevékenységekre, amely a saját számítógép-hálózataink megóvását jelenti a szemben álló fél információs támadásaival szemben.

A számítógéphálózati támadás szoftveres vagy hardveres úton történő behatolást jelent a megtámadott fél informatikai rendszerébe, annak érdekében, hogy az ott tárolt adatokat megsemmisítsük, módosítsuk vagy hozzáférhetetlenné tegyük, illetve magának a rendszernek a működését ellehetetlenítsük. Ezeket a támadásokat jól felkészült informatikai szakemberek, úgynevezett hackerek végzik, akik az informatikai rendszereket a mindenki által elérhető szint felett ismerik, képesek a hálózatok gyenge pontjain keresztül illegálisan belépni, ott jogosultságokat szerezve, különféle műveleteket végezni. (Haig, Várhegyi, 2005 p228) Fontos megjegyezni, hogy ezek a szakemberek nem mindig rosszindulatú céllal használják szaktudásukat, a rendszerek gyenge pontjainak kijavítása érdekében is dolgozhatnak, ekkor etikus hackelésről beszélünk.

A számítógépes támadások eszközei közül ki kell emelnünk a rosszindulatú programokat, amelyeknek számos alfaja létezik. A mindenki által ismert vírusok olyan programok, amelyek saját programkódjukat hozzáfűzik egy másik programhoz, így szaporodnak, terjednek. Általában két fő részük van, az egyik a terjedésért felelős, a másik pedig a mag, amelyben a végrehajtandó tevékenység található. A programférgek önálló programok, akik képesek a szaporodásra, önmaguk terjesztésére. A felépítésük hasonló, mint a vírusoké, általában pluszban külön programrész felel az álcázásért, hogy nehezebben lehessen felfedezni őket. A trójai típusú programok látszólag hasznos funkciókkal bíró alkalmazások, azonban eredeti funkciójuk mellett nem kívánt műveleteket is végrehajtanak. Ezeken kívül léteznek még különböző kémprogramok, billentyűzetfigyelő programok és ezek kombinációi. (Haig, 2015. p131) Egy másik gyakran használt módszer a botnetek vagy zombi hálózatok használata. A zombi számítógép olyan számítógép, amelyet valamilyen trójai szoftverrel irányítása alá vesz egy rosszindulatú támadó. A számítógép erőforrásait ezután a saját céljára, sokszor DDoS-támadások[4] lebonyolítására

4 Distributed Denial of Service – elosztott szolgáltatásmegtagadással járó támadás

használja. Botnetnek ezeknek a zombi gépeknek a hálózatát nevezzük. Ha elegendő mennyiségű zombi számítógép áll a támadó rendelkezésére, képessé válhat a kiválasztott célpont túlterhelésére és ezáltali működésképtelenné tételére. (Orbók, 2015) Az ilyen irányított gépeket használják egyébként spamek, azaz kéretlen levelek tömeges küldésére is. Fontos megjegyezni, hogy ezen eszközök nem csak a kiberhadviselés eszköztárában vannak jelen, ezt használják a kiberbűnözők és az egyéb rossz szándékú támadók is.

A védelmi jellegű műveletek értelemszerűen a saját informatikai rendszereink megvédése az ellenség támadó tevékenységével szemben. Ezek eszközei például a tűzfalak, amelyek az illegális hálózati forgalmakat szűrik ki, a különböző vírusvédelmi szoftverek, amelyek a rosszindulatú kódokat ismerik fel és semmisítik meg.

Nagyon lényeges kiemelni, hogy kiberhadviselésről csak abban az esetben beszélhetünk, ha egy ország egy másik ország számítógépes hálózatai, kritikus informatikai infrastruktúrái ellen indít támadást informatikai és fizikai eszközökkel saját nevében vagy egy harmadik fél bevonásával. E harmadik fél lehet állam, valamilyen szervezet vagy csoport. Ezt azonban az elmúlt évek kibertámadásaiban még egyszer sem sikerült bizonyítani, hiszen minden, hírbe hozott ország határozottan tagadta a vádakat.

A következőkben bemutatom az elmúlt időszak nagyobb kibertámadásait.

Habár a szakirodalom szerint a legelső dokumentált kibertámadást 1997-ben egy Srí Lanka-i terrorszervezet, a *Tamil Tigrisek* követték el (Haig, Kovács, 2008), úgy gondolom, nem mehetünk el szó nélkül az 1982-es szibériai gázvezeték-robbanás mellett sem. Thomas C. Reed, az amerikai Nemzetbiztonsági Hivatal egykori munkatársa 2004-ben megjelent könyvében leírja, hogy a robbanás nem a véletlen műve volt, hanem a szovjetek elleni gazdasági hadviselés része. A Szovjetunió megpróbált embargós nyugati technológiához jutni, az Egyesült Államok viszont meg akarta akadályozni, hogy a szovjetek valutabevételhez jussanak a nyersanyagszállításokból.

Egy, a KGB-be beépült ügynök juttatta el a CIA-hoz azt a listát, amelyen a szovjetek által beszerezni kívánt technológia szerepelt. Ezen találták azt a bizonyos szoftvert, amelyet a nyersanyagvezetékek irányítási rendszereihez használtak volna. Egy kanadai vállalaton keresztül a CIA adta el a szovjeteknek a szoftvert, amelybe azonban olyan hibákat építettek, hogy néhány hónapos

kifogástalan működés után összezavarta a szállítási folyamatokat. Ezt a vezeték irányítószelepeinek precízen megtervezett fals működtetésével érték el. Ennek eredménye volt az eddigi legnagyobb, nem nukleáris eredetű robbanás, amely a szovjet gazdaságot is megrázta 1982 nyarán.

Ez az emberéletet nem követelő, de hatalmas kárt okozó robbanás indította el a hidegháború utolsó felvonását – állítja a könyv szerzője. Mert noha a szovjetek rájöttek, hogy manipulált technológiát vettek, innentől kezdve nem bízhattak meg egyetlen beszállítójukban sem. (Kettmann, 2004)

Ebben a történetben az a furcsa, hogy mind a szovjet, mind az amerikai kormány hevesen tagadta a szerző állításait. A szovjetek a hanyag munka rovására írták a robbanást, az amerikaiak pedig nem ismertek el semmilyen szoftvermódosítást. Technikailag elképzelhető a kivitelezés, de mivel csak egyetlen forrás áll rendelkezésünkre, ezért kezeljük fenntartással a történetet annak ellenére, hogy a Wikipédia „Cyberwarfare in the United States" szócikkében szerepel az esemény mint kibertámadás más nemzet ellen.[5] Mindenesetre jól mutatja, hogy a számítógép-vezérlésű eszközök sebezhetősége és támadhatósága nem napjainkban keltette fel a potenciális támadók figyelmét.

1999-ben szerb hackerek – a NATO szerbiai bombázásaira válaszul – támadták meg a szövetség szervereit és néhányat DDoS módszerrel tettek átmenetileg elérhetetlenné, valamint feltörtek néhány weboldalt és propagandaüzeneteket helyeztek el rajtuk.

Az első kibertámadás, amelyet egy ország ellen indítottak, 2007-ben következett be. Az igen fejlett informatikai kultúrával rendelkező Észtországban 2007. április 27-én zavargások törtek ki a tallinni szovjet hősi emlékmű eltávolítása miatt. Az első túlterheléses támadások jelei néhány nappal az első tüntetések után jelentkeztek a parlament, kormányhivatalok, minisztériumok, bankok, telefontársaságok és médiacégek szerverei ellen. A célpontok kiválasztása, a támadások összehangoltsága, precíz kivitelezése és hatékonysága arra mutatott, hogy e támadások hátterében szervezett erők állnak. Néhány esetben szakértők megállapították, hogy a támadások orosz szerverektől indultak, amit az orosz hatóságok természetesen tagadtak. Ugyanakkor a megtámadott szerverek jellegéből adódóan nyilvánvaló, hogy a támadások célja

5 Kiberhadviselés az Egyesült Államokban – https://en.wikipedia.org/wiki/Cyberwarfare_in_the_United_States

egyértelműen a balti állam kritikus információs infrastruktúrájának bénítása volt. Az ország online adatforgalmát irányító kulcsfontosságú szerverek naponta omlottak össze, sok állami intézmény hálózatát kénytelenek voltak ideiglenesen leválasztani az internetről. Az elektronikus banki forgalom és kereskedelem részint megszűnt, részint erősen akadozott. Egyes szakértők szerint a kibertámadás sokkal súlyosabb gazdasági károkat okozott Észtországnak, mint amit azok a kereskedelmi szankciók okoztak volna, amikkel Oroszország a krízis első heteiben fenyegetőzött.

Bár kezdetben NATO-szakértők is részt vettek a támadások felderítésében, azok jellegéből adódóan a támadók azonosítása szinte lehetetlen volt. Számos támadót lehetett ugyan azonosítani orosz területen, de annak egyértelmű igazolása, hogy kormányzati szerverek voltak, sikertelennek bizonyult. Általánosan elterjedt nézet szerint orosz hazafias érzelmű hackerek olyan botnet-hálózatot hoztak létre, amelybe orosz gépeken kívül még 178 ország területén lévő számítógépeket is beszerveztek a tudtuk nélkül (zombi gépek), és ezeken keresztül hajtották végre a támadásokat. (Haig, Kovács, 2008)

A 2008 augusztusában kitört orosz-grúz háborúnak is volt kiberaspektusa. Mint az köztudott, a hosszú évek óta tartó grúz-oszét és a grúz-abház konfliktust a grúz elnök 2008. augusztus 8-án katonai úton próbálta megoldani az említett területek megtámadásával. Rosszul mérte fel azonban az erőviszonyokat, amikor nem számolt azzal, hogy Oroszország nem fogja szó nélkül hagyni a támadást, már csak azért sem, mivel csapatai ENSZ-felhatalmazással békefenntartó missziót teljesítettek Dél-Oszétiában. Az orosz csapatok erőteljes válaszcsapásokat mértek a grúz erőkre, és öt napig tartó heves harcok után a grúzok kénytelenek voltak fegyverszünetet kérni. (Németh, Hajzer, 2008)

A fegyveres konfliktussal egy időben megindult Grúzia ellen egy kiberhadjárat is. Az internetforgalmat ellenőrzése alá vonta Oroszország – vagy legalábbis valakik Oroszországból, állította a grúz kormány, amely valóságos kiberemigrációba kényszerült, és a hadi jelentések mellett sorra jelentette meg a virtuális támadásokról szóló közleményeit.[6]

6 http://georgiamfa.blogspot.hu/2008/08/cyber-attacks-disable-georgian-websites.html

A leglátványosabb hacker-akciók ugyanis az ország kormányzati weboldalai ellen indultak, amelyeket kívülről megbénítottak, illetve a tartalmukat kicserélték[7]. Az orosz földről érkezett hackerek Mihail Szakasvili elnök portréjával vandálkodtak. Az államfő képére Hitler-bajuszt rajzoltak, és egy sor olyan képet tettek ki róla az oldalra, ahol a náci diktátor pózaiban ábrázolták, vagy a történelem nagy gonosztevői közé kopírozták be az arcmását.

A megtámadott oldalak között volt az elnök saját weblapja mellett a grúz külügy- és hadügyminisztérium is. Szakasvili elnök erre válaszul a hazája ügyét nyíltan támogató Lengyelország vezetőjétől kért és kapott segítséget: az államfő, illetve stábja Lech Kaczynski hivatalos, angol nyelvű oldalán is lehetőséget kapott arra, hogy tájékoztatást adjon a háborús eseményekről. Még ezt a hivatalos, nagyban gesztusértékű lépést megelőzően a honlap nélkül maradt grúz külügyminisztérium blogot indított a Google által birtokolt Blogspot blogszolgáltatónál.

Mindezekkel egy időben megindultak az ország lejáratását célzó, dezinformációs céllal indított weboldalak is – a hiteles forrásokat a konfliktusról percről percre beszámoló blog a linkek között listázta. A kaukázusi országban a .ru végződésű webcímek is elérhetetlenné váltak, amelyeket egyes források szerint maga a grúz kormányzat tilttatott le, hogy útját állja az orosz propagandának, és a Tbilisziben lévő orosz nagykövetség munkatársai szerint a mobil- és vezetékes telefonszolgáltatásban is fennakadások voltak a túlterhelés miatt (igaz, ennek inkább a katonai offenzívához lehetett köze). (Vámosi, Szedlák, 2008)

Véleményem szerint a grúz kormány erősen eltúlozta az ellene indított kibertámadásokat, hisz korántsem rendelkezett olyan infrastruktúrával, mint például Észtország, így a támadásoknak sem volt olyan hatása, nem bénult meg a bankrendszer, illetve a kormányzat. Az interneten keresztül zajló nagyszabású támadások akkor különösen hatékonyak, ha egy olyan ország ellen irányulnak, amely erőteljesen támaszkodik információs technológiára és annak infrastruktúrájára. Grúzia esetében ez nem mondható el: az interneten keresztül a támadók nem tudtak nagyobb károkat okozni, mint az or-

7 Ezt nevezi az internetes szaknyelv defacementnek.

ság földjére lépő orosz katonák. Hétköznapi ésszel érthetetlen, hogy a kormány miért foglalkozott olyan erőteljesen a kiber-támadásokkal, miközben városait, infrastruktúráját lőtte és bombázta az orosz hadsereg. Mindazonáltal ennél a konfliktusnál mutatható ki először, hogy a hagyományos katonai műveletek támogatására kiberműveleteket is alkalmaztak.

Mind az orosz-észt, mind az orosz-grúz konfliktus vonatkozásában elmondhatjuk, az orosz hivatalos szervek kategorikusan tagadták, hogy közük lenne a támadásokhoz. A konfliktusok lezárulta utáni elemzések csupán azt tudták kimutatni, hogy orosz nacionalista érzések vezérelték a támadókat, ám az orosz állam közreműködését nem sikerült bebizonyítani.

Nem szabad figyelmen kívül hagyni azokat a támadásokat sem, amelyek célzottan valamely kritikus infrastruktúra ellen irányulnak. Ezek lehetnek áramszolgáltatók, erőművek vagy más létfontosságú rendszerek. Több olyan támadás is volt már a világon (Brazília, Törökország), ahol kibertámadás következtében állt le az áramszolgáltatás. Legutóbb 2015 decemberében regisztráltak ilyen jellegű támadást Ukrajnában, melynek következtében egy, hétszázezer embert érintő áramszünet következett be. Idén januárban a kijevi repülőtér számítógépes rendszerében találtak rosszindulatú kódokat, amelyek akár a repülés biztonságát is veszélyeztethették volna.

A kritikus infrastruktúrák, ipari folyamatirányító rendszerek támadásának eszközéül használt rosszindulatú kódok egyre fejlettebbek és kifinomultabbá váltak az utóbbi években. Ezen kódok készítői nagy hangsúlyt helyeznek programjaik rejtőzködő képességének fejlesztésére, ezáltal nehezítve a felderítésüket. Tipikus és hírhedt példája ezeknek a programoknak a fehérorosz VirusBlokAda cég által 2010 júniusában felfedezett új rosszindulatú kód, amelyet Stuxnetnek neveztek el.

Az új féreg Microsoft operációs rendszereken terjedt és kizárólag ipari folyamatirányító rendszerek ellen lett kifejlesztve. A Stuxnet kivételes mivoltát és specializáltságát erősíti az a tény is, hogy az említett ipari felügyeleti, vezérlő és adatgyűjtő rendszereket egyetlen cég, a **német Siemens gyártja (SIMATIC WinCC HMI és WIMATIC STEP 7)** és alapvetően a nehézipari szektorban, illetve az energiatermelés és szállítás területén használják, azaz fenyegetést alapvetően csak olyan létesítményekre jelent, melyek egy része kritikus infrastruktúrának minősül. (Berzsenyi, Szentgáli, 2010)

A Stuxnet végső célja ipari vezérlő rendszerek automatikus folyamatainak újraprogramozása volt. Elsősorban PLC[8] szoftvereket támadott. A WinCC/Step 7 szoftver volt mindezek közül az elsődleges, amelyet a Stuxnet megcélzott. Ez a szoftver adatkábelen keresztül kapcsolódik a PLC-hez és eléri a memóriatartalmat, képes folyamatokat újrakonfigurálni, programokat feltölteni és a végrehajtás során rendelkezik bizonyos nyomkövetési funkciókkal is. Ha a PLC már programozásra került, akkor lekapcsolható róla, és a PLC már önmagában is képes a működésre. A Stuxnet e szoftver segítségével juttatta be kódblokkjait a PLC-be, majd ezeket el is rejtette.

A Stuxnet a PLC-ken bizonyos konkrét ipari eszközök, nevezetesen nagy sebességű motorok frekvenciaátalakítói után kutatott és csak akkor lépett akcióba, ha a finn Vacon és az iráni Fararo Paya készülékeire talált, valamint a felügyelt eszköz 807 és 1210 Hz között működött. Ilyen frekvenciaátalakítók és motorok szinte kizárólag az iráni urándúsítókban használatosak. (Cserháti, 2011)

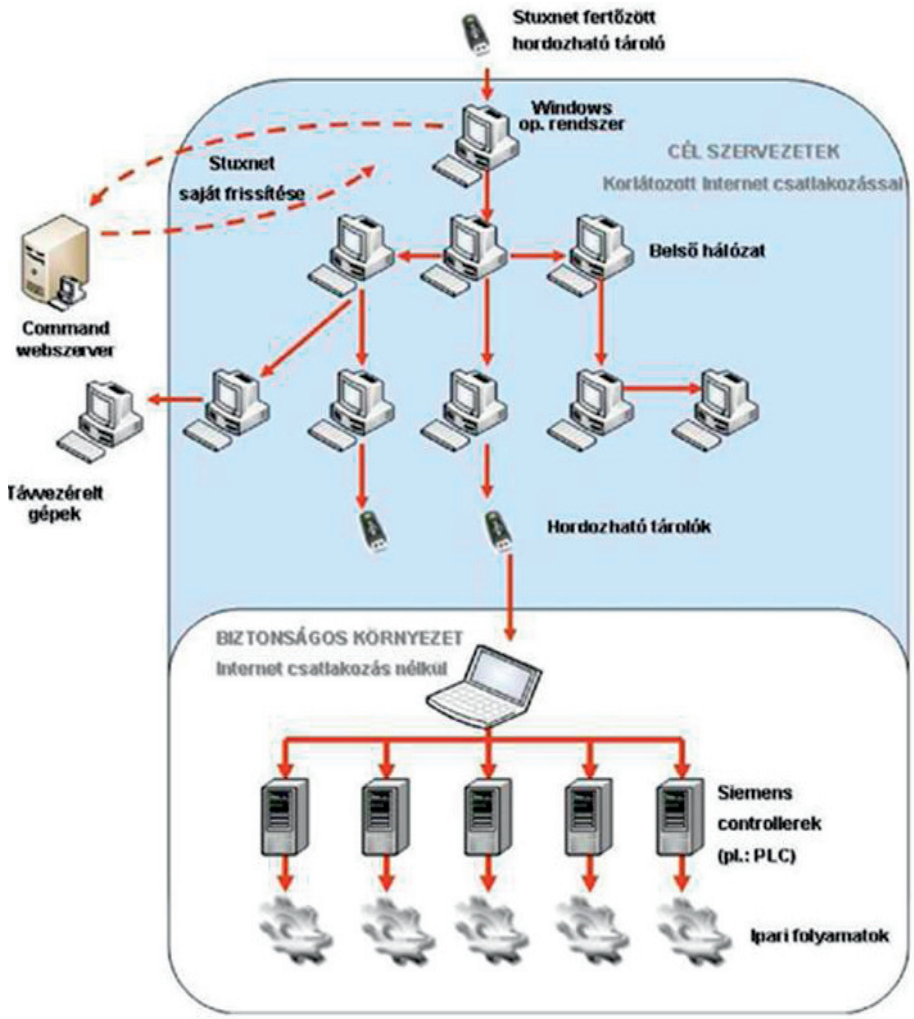
A vírus egyértelmű célja az urándúsító centrifugák észrevétlen tönkretétele és a dúsítási folyamat megzavarása volt. Ezt a célt sikeresen el is érte, hisz legalább 1000 centrifugát tett használhatatlanná a Natanzban lévő dúsítóban és mértékadó vélekedések szerint legalább két évvel vetette vissza az iráni atomprogramot.

A támadó kód megírásának profizmusára utal, hogy egyszerre négy zero-day[9] fenyegetést is kihasznált a terjedéséhez és két lopott digitális aláírással is tudta igazolni legitimitását.

Terjedését a következő ábra mutatja be.

8 A PLC – Programmable Logic Controller, azaz programozható logikai vezérlő. PLC-ket nagy számban az ipari szabályozástechnikában, a különböző villamos, illetve az ilyen módon működtetett folyamatok irányításában használják.

9 A zero-day/zero-hour, vagyis nulladik napi támadás kifejezést azokra a számítógépes biztonsági fenyegetésekre használják a szakemberek, amelyek egy adott számítógépes alkalmazás még felfedezetlen, nem publikált sebezhetőségét használják ki. A támadó a sebezhetőség felfedezését követően úgynevezett zero-day exploitot készít, amely az a tényleges számítógépes kód, ami képes a sérülékenység kiaknázására. Azonban a sérülékenységek nehéz és bonyolult detektálhatósága miatt a kártékony programok készítői számára jelentős értéket képvisel egy újonnan felfedezett sérülékenység, ezért egy program általában csak egy sérülékenység kihasználására épül. Ezen támadások idején a megtámadott alkalmazás fejlesztőjének még többnyire nincs tudomása a sérülékenységről, vagy még nem tudott javítást készíteni hozzá.



(forrás: Kovács, Sipos 2010)

4. ábra A Stuxnet terjedése a belső hálózaton

Származásáról sokáig nem voltak pontos adatok, de mindenki rögtön az Egyesült Államokra és Izraelre gondolt mint olyan országokra, amelyeknek érdekében és módjában is állhatott az iráni atomprogram elleni akció. Ralph Langner hamburgi vírusbiztonsági szakértő blogjában mélyrehatóan foglalkozott a Stuxnettel és a 2010. december 31-i bejegyzésében az alábbiakat írta:

„Egy ilyen nagy horderejű támadás mögött feszülő hatalmas erőket elég könnyű érzékelni. A Stuxnet kártevő kifejlesztéséhez extrém mennyiségű hírszerzési adat kellett a natanzi dúsító mű elrendezéséről, teljesen meg kellett érteni az IR-1[10] működését (amihez feltehetően rendelkezésre állt egy üzemképes tesztelő rendszer is), valamint a Siemens érintett termékeiről rengeteg bennfentes tudásra volt szükség. Mindez igen kevés szervezetre szűkíti le a világon azt a kört, amely a feladat megoldására vállalkozhatott." (Langner, 2010)

2016 februárjában mutatták be a Berlini Nemzetközi Filmfesztiválon Alex Gibney dokumentumfilmjét, Zero Days címmel, amely ezzel a témával foglalkozott. A filmben megszólal Michael Hayden tábornok is, aki a CIA[11] és az NSA[12] vezetője is volt. Itt elismeri, hogy a Stuxnetet Izraellel együttműködve fejlesztették ki, célzottan Irán atomprogramja ellen. (Magyar Nemzet Online, 2016)

Ám a Stuxnet csak a kezdet volt az új generációs kártevők sorában. A Budapesti Műszaki Egyetem Híradástechnikai Tanszékén működő CrySyS Adat- és Rendszerbiztonság Laboratórium munkatársai fedezték fel 2011-ben a Duqu és 2012-ben a sKyWiper kódokat, amelyek szintén nagyon fejlett, kifinomult eszközök, voltak és kifejlesztésükben szinte biztosra vehető volt az állami segítség. 2015 elején a Kaspersky Lab talált egy új kártékony kódot, amelyet Duqu 2 néven vált ismerté. Az új kód a legkifinomultabb, amivel eddig találkoztak, készítőinek gondolkodásmódja és filozófiája teljesen újszerű. A cég vezető kutatója szerint a kémprogrammal mintegy száz célpontot támadtak meg, köztük olyan luxusszállodákat is, amelyekben az iráni atomfegyverprogram megfékezését célzó nagyhatalmi tárgyalások folytak. (SG1, 2015)

Ezek az adatok is azt támasztják alá, hogy a világ számos katonai és kormányzati szerve törekszik arra, hogy a kibertérben is meghatározó befolyást szerezzen, ott nem csak a támadások elhárítására törekedjen, hanem támadó kapacitással is rendelkezzen.

10 A pakisztáni P-1 urándúsító centrifuga iráni változatának a külvilág által adott neve.
11 Central Intelligence Agency – Központi Hírszerző Ügynökség
12 National Security Agency – Nemzetbiztonsági Ügynökség

Az informatikai támadások elhárítása mára elsőrendű problémává lépett elő a világban. Mindenhol felismerték, hogy a kiberbiztonság fejlesztése elengedhetetlen, és a kulcsfontosságú információs rendszereket meg kell tudni védeni a kibertámadásoktól. Ezzel összhangban 2008 májusában alakult meg a Kooperatív Kibervédelmi Kiválósági Központ (NATO Cooperative Cyber Defence Centre of Excellence (CCDCoE)). Május 14-én írták alá az Együttműködési Nyilatkozatot az alapító országok, a balti államok, valamint Németország, Spanyolország, Olaszország és Szlovákia. A Központot az Északatlanti Tanács döntése alapján 2008. október 28-án jogi értelemben is nemzetközi katonai szervezetté nyilvánították. Jelzésértékkel bír, hogy a Központ Tallinnban, Észtország fővárosában jött létre. A Központ feladatai közé tartozik többek között a tagállami kiberképességek kialakításának, tagállami doktrínák, koncepciók és stratégiák kidolgozásának támogatása, az információbiztonság oktatása, folyamatos képzések és gyakorlatok lebonyolítása és a kiberhadviselés jogi vonatkozásainak elemzése. Vagyis a szervezet nem a NATO kiber támadóerejét jeleníti meg, hanem mint kutatási és oktatási központ működik. Hazánk 2010. június 23-án csatlakozott a Központ munkájához.

2013-ban jelent meg az a kiadvány, melyet nemzetközi hírű jogászok, technikai szakemberek és kutatók segítségével állítottak össze és a „Tallinn Manual on the International Law Applicable to Cyber Warfare[13]" címet viseli. Ez a kézikönyv több mint 300 oldalon, 2 részben, 95 fő szabályra lebontva részletesen tárgyalja a kiberhadviselés szabályait. Az első rész a „Nemzetközi kiberbiztonsági jog", a második a „Kiberhadijog" címet viseli. Az első részben határozzák meg, hogy a kibertámadás fegyveres támadásnak minősíthető, így a megtámadott állam jogosan használhat önvédelemből akár hagyományos fegyvereket is. Azonban nem tekinthető fegyveres támadásnak a kiberkémkedés, az információlopás és a honlapok feltörése. Az államok felelősséggel tartoznak ugyan ha a fennhatósági területeiről az ellenőrzésük alatt álló szervezetek más ország ellen kibertámadást hajtanak végre, az azonban, hogy egy támadást egy adott országból indítottak, még nem bizonyítja az adott ország felelősségét. Elképzelhető ugyanis, hogy más államok használták az adott ország kiberterét a támadás lebonyolítására.

13 Tallini kézikönyv a nemzetközi jog alkalmazásáról a kiberhadviselésben.

A második részben többek között kitérnek arra, hogy a hagyományos fegyveres konfliktusokhoz hasonlóan el kell kerülni a civil áldozatokat, tehát például tilos a civil célpontok, kórházak, atomerőművek, vízierőművek vagy gátak támadása – ezt egyébként a genfi egyezmények most is tiltják a hadviselő felek számára. Védekező és támadó kiberhadműveletekkel kapcsolatban megállapítják, hogy akkor minősül egy művelet a kibertérben elkövetett támadásnak, ha annak hatására személyek sérülnek vagy halnak meg, illetve vagyontárgyak rongálódnak, illetve semmisülnek meg. A támadások célszemélyei lehetnek a fegyveres erők és szervezetek tagjai. A hadviselés eszközei és módszerei kapcsán ügyelni kell arra, hogy nem szabad felesleges sérülést és szükségtelen szenvedést okozni ellenfélnek. A kiberhadviselésre is vonatkozik az arányosság elve, amelynek alapján a megtámadott fél nem okozhat sokkal nagyobb veszteséget a támadónak, mint amennyit elszenvedett.

Elmondhatjuk, hogy kiemelkedő jelentőségű mű született a kiberhadviselés szabályozásáról, amely ugyan nem tartalmaz kötelező jellegű ajánlásokat, de a széles körben történt egyeztetések során olyan elveket fektettek le, amelyet az egyes országok jól hasznosíthatnak jogalkotásukban. (Gyebrovszki, 2014)

Azt, hogy a NATO komoly kihívásnak tekinti a kibertérből érkező támadásokat, jól bizonyítja, hogy a 2016. július 8-án és 9-én Varsóban megrendezett csúcstalálkozón az állam- és kormányfők kiemelt figyelmet szenteltek a kiberbiztonságnak. A tagállamok a kiberteret új műveleti környezetként ismerték el, melyben a NATO-nak ugyanolyan hatékonyan kell védekeznie, mint a szárazföldön, a tengeren vagy a levegőben. Célul tűzték ki a kibervédelem fejlesztését, a tervezési folyamatokba történő nagyobb fokú integrálását, a nemzeti és szövetséges hálózatok fokozott védelmét a legmodernebb technológiák felhasználásával. A 2014-es walesi csúcstalálkozó után ismét deklarálták a kollektív védelem kibertérre történő kiterjesztését is. (Warsaw Summit Communiqué. 2016)

Mint említettem, a tallinni Központ nem a NATO kibertámadási képességeit fejleszti, ilyen típusú programja nincs is a szervezetnek, azonban egyes tagországok foglalkoznak a támadókapacitások fejlesztésével is, még ha ez nem is a nyilvánosság előtt zajlik. A világ sok országában indult kutatás a kibervédelem minél nagyobb szintre fejlesztése mellett arról is, hogy a támadási képességeket is kiterjesszék.

5. Kiberképességek a világban

Az Egyesült Államok, úgyis mint az internet szülőhazája és mint a világ vezető hatalma, igen nagy erőfeszítéseket tesz a kibertérben elfoglalt pozíciójának megőrzésére. Erre való tekintettel a Védelmi Minisztérium elhatározta egy katonai parancsnokság létrehozását, amely összefogja a kibertér védelmét az országban. A USCYBERCOM[14] az Egyesült Államok Stratégiai Parancsnokságának alárendeltségében, a Maryland állambeli Fort Mead-ben kezdte meg tevékenységét 2010-ben. Küldetésnyilatkozatuk szerint:

„*A USCYBERCOM tervezi, koordinálja, irányítja és vezeti azon tevékenységeket, amelyekkel megvédheti a Védelmi Minisztérium információs hálózatait, felkészülhet a kibertérben végrehajtott katonai műveletek végrehajtására, valamint minden területen biztosítja az Amerikai Egyesült Államok és szövetségesei számára a cselekvési szabadságot a kibertérben és megakadályozza a szemben álló felet annak használatában.*" (DoD, 2010)

A Parancsnokság fennhatósága alá került valamennyi fegyvernem kiberműveletekkel foglalkozó egysége: a Hadsereg Kiberműveleti Parancsnoksága (U.S Army Forces Cyber Command), a Légierő Kiberműveleti Parancsnoksága (24th USAF), a Haditengerészet Kiberműveleti Parancsnoksága (Fleet Cyber Command) és a Tengerészgyalogság Kiberműveleti Parancsnoksága (Marine Forces Cyber Command). Várhatóan a létszámát 2016-ra töltik fel teljesen, így 6200 fő fog itt szolgálatot teljesíteni. Tevékenységét az elektronikai felderítéssel foglalkozó NSA-vel összhangban végzi. Az egység mindenkori parancsnoka egyben az NSA főigazgatója is. (NSA, 2016) A kiberműveleti képességek fejlesztését az Egyesült Államok katonai és polgári informatikai hálózatainak egyre növekvő veszélyeztetettsége indokolta. A Parancsnokságnak az országot ért hagyományos és informatikai támadások esetén is képesnek kell lennie a megfelelő válaszcsapás végrehajtására a kibertérben. Kibertámadást az Amerikai Egyesült Államok elnöke rendelhet el, az ország katonai vagy civil számítógépes hálózatai elleni támadásra válaszul vagy ilyen támadás megelőzésére. Az Amerikai Egyesült Államok elleni kibertámadások elleni védekezés és a válaszcsapás módjai a 2011-ben megjelent Nemzetközi Kiberbiztonsági Stratégiában kerültek rögzítésre.

14 United States Cyber Command – Az Egyesült Államok Kiberernetikai Parancsnoksága

A stratégia szerint az amerikai kibervédelem a megelőzésre és az elrettentésre épít. A megelőzés alapja a nemzetközi együttműködés. Olyan nemzetközi rendészeti együttműködés kialakítását szorgalmazza, amely lehetőséget teremt a kiberbűnözés és a kiberterrorizmus elleni küzdelem továbbfejlesztésére. Az Amerikai Egyesült Államok elleni, egy nemzetállam által indított kibertámadást követő ellencsapás jogi megalapozásaként a stratégia megállapítja, hogy az kibertérben zajló tevékenységek is a nemzetközi közösséget alkotó szuverén nemzetállamok felelősségi körébe tartoznak. A stratégia szerint az Amerikai Egyesült Államok vagy szövetségesei elleni kibertámadás esetén az Amerikai Egyesült Államok minden szükséges diplomáciai, gazdasági és katonai ellenlépést megtehet. A stratégia alapján az Amerikai Egyesült Államok kibertámadásra akár hagyományos katonai válaszcsapással is felelhet. (International Strategy for Cyberspace, 2011)

Feltétlenül ki kell térnünk az NSA szerepére az amerikai kibertevékenységek kapcsán. A szervezet a Védelmi Minisztérium alárendeltségében működik, Alapvetően rádióelektronikai felderítésre hozták létre 1952. november 4-én. Tevékenységi körébe tartozik a külföldre irányuló rádiófelderítés, a kriptográfia, azaz a külföldi rejtjelfejtés és az amerikai rejtjelzés biztonságának védelme, valamint mindennemű elektronikai felderítés. (NSA2, 2016)

Az NSA volt az egyik főszereplője a még a hidegháborúban indult, de utána is évtizedeken át folytatott ECHELON műveletnek is, amelyben az Egyesült Államok, Nagy-Britannia, Ausztrália, Kanada és Új-Zéland vett részt, és amelynek fő tevékenysége a kereskedelmi távközlési műholdak adatforgalmának ellenőrzése volt. Ez a szoros együttműködés az öt ország között a mai napig fennáll (a szakirodalom csak „Big Five"-ként emlegeti őket). Edward Snowden, az NSA korábbi szerződéses munkatársa 2013 nyarán számos dokumentumot hozott nyilvánosságra, amelyek fényt derítettek az NSA globális lehallgató tevékenységének méreteire. A leleplezések óriási világvisszhangot váltottak ki.

Nyilvánosságra került, hogy az NSA világszerte több mint egymilliárd ember telefonos és internetes kommunikációját követi figyelemmel, és nem csak a terrorizmusról, hanem külpolitikai, gazdasági, konkrét kereskedelmi témákról is adatokat gyűjt. 2012 közepén az ügynökség naponta több mint 20 milliárd kommunikációs eseményt, úgynevezett metaadatokat (internet és telefon) rögzített.

Az NSA kiterjedt kémtevékenységet folytatott az Európai Unió, az Egyesült Nemzetek Szervezete és számos olyan kormányzat ellen is, amelyek egyébként az Egyesült Államok szoros szövetségese. A szervezet képességeiről a teljesség igénye nélkül csak annyit, hogy hozzáfér a legnagyobb online szolgáltatók szervereihez, be tudja kapcsolni a mobiltelefonok kameráját és mikrofonját távolról, titokban megcsapolja a tenger alatti adatkábelek forgalmát, távolról le tudja hallgatni a wi-fi forgalmat. A szervezet egyik legfontosabb egysége a TAO[15], melynek tagjai jól képzett hackerek. Feladatuk a külföldi szervezetek által működtetett számítógépes hálózatok azonosítása, megfigyelése, az azokba való behatolás és azokból információszerzés. A TAO együttműködik más hírszerzési szervekkel, mint a CIA és az FBI, ha szükség van rá, be is segít. A helyszínre juttatják, akár repülővel a hackereket, hogy a helyi hálózatokhoz vagy akár az internetről elzárt hálózatokhoz is hozzáférjenek. (Greenwald, 2014)

Tehát, mint láthatjuk az Egyesült Államok deklaráltan is képes támadóműveletek végrehajtására a kibertérben.

Kína az elmúlt évtizedek szédületes fejlődése után mára a világ második legnagyobb gazdaságává vált. Habár a 2008-as válság nem hagyta érintetlenül a kínai gazdaságot sem, a növekedés nem állt meg. Természetes, hogy a katonai képességek terén is töretlen a fejlesztés. 2016-ban a GDP növekedését meghaladó mértékben, 7,6 %-kal növelik a katonai kiadásokat, amely így eléri a 135 milliárd dollárt. Folyamatosan fejlesztik a kiberhadviselési képességeiket is. Az internetet potenciális háborús eszköznek tekintik, beleértve szakértők, hackerek kiképzését és felszerelését, hogy behatoljanak az ellenfél katonai információs hálózatába. Egyetemi kurzusokat indítottak a kibertámadásokra és azok kivédésére való felkészítés céljából, tanulmányozzák a hackerek módszereit, a számítógépvírusok tervezését és alkalmazását, a hálózati biztonság problémáit. (Jordán, 2011)

A világ vezető hálózatbiztonsági cégeinek jelentéseiből kitűnik, hogy a kibertámadások jelentős része kínai támadókra vezethető vissza. Több jelentés is említi a Sanghajban állomásozó 61398-as számú katonai egységet, melynek munkáját Kína államtitokká nyilvánította. Az egység bázisa Pudongban, a sanghaji pénzügyi központban van, és több ezer tagja lehet, akik

15 Tailored Access Operations (magyarul kb. „Testre szabott hozzáférési műveletek")

jól beszélnek angolul, illetve kiváló számítógépes ismeretekkel rendelkeznek. A jelentések szerint 2006 óta több száz terabyte adatot loptak el 141 szervezet számítógépeiről. (Mandiant, 2013 p3) A kínai védelmi minisztérium természetesen kategorikusan cáfolta, hogy Peking valaha is támogatott volna hackertevékenységet. Az azonban elgondolkodtató, hogy ekkora mennyiségű és ilyen típusú adatokkal egyszerű hackerek vagy kiberbűnözők mit kezdtek volna.

A kibertér harmadik nagy szereplője Oroszország, amely bevallása szerint szintén nem rendelkezik kiberhadsereggel. Ennek ellenére ők voltak az első számú gyanúsítottjai az észtországi incidensnek és a grúziai támadásoknak. Egyes vélemények szerint Oroszország kiberműveleti képességeinek alapjait kiberbűnözői csoportok képezik. Ezek a csoportok az orosz kormány hallgatólagos engedélyével végzik tevékenységüket, bevételeiket klasszikus kiberbűnözéssel szerzik. Képességeiket pedig szükség szerint az orosz vezetés által kijelölt célpontok ellen használják fel. Szakértők szerint az orosz kiberképességek alapját botnetek[16] képezik, emellett az orosz hackerek vezető szerepet töltenek be a számítógépes programok feltörésében is. A legismertebb orosz számítógépes bűnözői csoport a Russian Business Network (RBN), amelynek botnetjei a 2007. évi, Észtország elleni túlterheléses támadásokban is részt vettek. Egyes források szerint az RBN vezetői és az orosz államigazgatás, illetve a titkosszolgálatok között személyi összefonódás mutatható ki. (Flook, 2009) A kiberműveletekben részt vevő orosz titkosszolgálatok – elsősorban a Szövetségi Biztonsági Szolgálat, a Szövetségi Védelmi Szolgálat – számítógépes biztonsági szakértők szerint információs műveleti tevékenységüket fantomcégek létrehozásával, illetve az RBN és más számítógépes bűnözői csoportok működésének utánzásával fedik el. Oroszország – Kínához hasonlóan – rendszeresen támadja az Amerikai Egyesült Államok és más NATO-tagállamok számítógépes rendszereit. A botnetek természetéből adódóan azonban nem bizonyítható, hogy e tevékenységek valóban az orosz kormány irányításával zajlanak. (Nagy, 2012) Propaganda célokra előszeretettel használják a közösségi hálózatokat is. Egy Szentpéterváron működő cég két volt munkatársának beszámolója szerint a váltott műszakban dolgozó bérkommentelők százai,

16 Rosszindulatú kódokkal megfertőzött számítógépek sokasága, amelyeket egy vezérlő számítógép segítségével irányítanak. Tipikusan DDoS-támadásokhoz használják.

szigorúan szabályozott keretek között dolgoznak, hogy nyugatellenes, Kreml-barát híreket osszanak meg hazai és külföldi portálokon. A témákat az adott nap elején jelölik ki, és meghatározott számú kommentet kell meghatározott számú profillal elhelyezni. Ez a tevékenység azonban nem csak Oroszországra jellemző, más országok is használják a közösségi hálózatokat propagandaterjesztésre. Nagy-Britanniában a hadseregen belül hoztak létre egy egységet, 77-es dandár néven, melynek feladata a közösségi hálózatokon történő lélektani műveletek végrehajtása (Bányász, 2016)

A kisebb országok is fejlesztik kiberképességeiket; Irán például az urándúsítóját ért 2010-es kibertámadás után kezdte fejleszteni a Forradalmi Gárdán belül felállított katonai egységét, amely alig egy évre rá, sikeresen átvette az irányítást egy amerikai RQ-170-es pilóta nélküli lopakodó technológiájú gép felett és azt sértetlenül leszállította.

Észak-Korea szintén felállított egy kiberhadviselési egységet a hírszerzésen belül, a 121-es osztagot. Szakértők szerint az egység létszáma már elérte a 6000 főt, ebből több százan külföldön dolgoznak. Fő célpontjuk Dél-Korea, de hozzájuk kötötték a 2014-es Sony elleni támadást is, amelyet állítólag az Interjú című film miatti bosszú motivált.

Meg kell még említeni Izraelt, mely mindig is élen járt az elektronikai fejlesztésekben – hadseregük használt például először frekvenciaugratásos rádiókat – és jelenleg szakértők szerint a világ kiberbiztonsági piacának 10 százalékát tudhatja magáénak. Az Egyesült Államok mellett Izrael is részt vett a Stuxnet kifejlesztésén és bevetésén az iráni urándúsító ellen, habár ezt hivatalosan sosem ismerték el. 2016 elején jelentették be, hogy Beér-Sevában létrehoznak egy technológiai parkot, ahol magáncégek bevonásával nemzetközi kiberbiztonsági központot akarnak kialakítani. A tervek szerint 15000 ember foglalkozik majd itt IT-biztonsággal. Ide fogják áthelyezni a fegyveres erők kibervédelmi egységeit is, illetve itt kap helyet a hadsereg kiberhadviseléssel foglalkozó, most alakuló egysége is. (SG2, 2016)

Németországban 2009-ban alakult a Bonn melletti Rheinbachban lévő Tomburg-kaszárnyában egy 76 fős Információs és Számítógépes Hálózati Műveleti Részleg nevű különleges csoport a Stratégiai Felderítő Parancsnokság alárendeltségében. A részleg tagjait a Bundeswehrrel együttműködő egyetemek informatikai tanszékeiről toborozzák és a legújabb technikákat sajátítják el.

A tervek szerint képesek lesznek észrevétlenül behatolni idegen hálózatokba, ott felderítéseket végezni, információkat szerezni vagy módosítani, illetve szerverek és hálózatok elleni támadásokat végrehajtani. (SG3, 2009) Ursula von der Leyen német védelmi miniszter 2016 áprilisában jelentette be, hogy a német hadseregen belül létrehoznak egy Cyber/IT (CIT) nevű egységet, amelynek fő feladata a kiterjedt kibervédelem megszervezése lesz. A tervek szerint 2021-ig 13500 katonát és civil alkalmazottat vesznek fel az egységhez. (HVG, 2016)

Úgy gondolom, a fent említett országokon túl még jó néhány ország törekszik a kibertámadási képességek kifejlesztésével. Arra már mindenki rájött, hogy a kibervédelem nagyon fontos. Több ország – köztük hazánk is – megteremtette azt a jogszabályi hátteret, amely elősegíti a védelem megszervezését. A NATO-tagállamok nagy része már kidolgozta a kiberbiztonsági stratégiáját, ezeket meg is osztották egymással. A stratégiák nyilvánosak, a Kiber Kiválósági Központ honlapján megtekinthetők, több NATO-tagsággal nem rendelkező ország ilyen típusú dokumentumaival egyetemben. Itt megtalálhatjuk többek között Oroszország, Kína, Japán, Szaúd-Arábia, Új-Zéland, Dél-Afrika nemzeti kiberbiztonságról szóló anyagait. A nemzetközi összefogás azonban elengedhetetlen, hisz a kiberbűnözést és a kiberterrorizmust csak így lehet visszaszorítani. Ennek jegyében született nemrég két nagy horderejű bilaterális szerződés Oroszország és Kína, illetve az Egyesült Államok és Kína között.

Oroszország és Kína 2015. május 8-án írt alá egyezményt, amelyben kifejezték eltökélt szándékukat a kibertérben történő törvénytelen cselekedetek megakadályozására, a kiberbűnözés és a terrorizmus minden formájával szembeni közös fellépés szükségességéről. Megegyeztek abban, hogy nem támadják egymás rendszereit és nem támogatnak semmilyen ilyen törekvést. Rendszeresen informálják egymást a kiberfenyegetésekről és a kutatás-fejlesztés terén közös tudományos, oktatási projekteket indítanak.

Egyes elemzők a szerződés aláírása után aggodalmuknak adtak hangot, mely szerint a két ország e szerződéssel össze kívánja hangolni az Egyesült Államok elleni kibertevékenységét. Remélhetőleg ez a szerződés azonban nem erről szólt. Ezt erősíti, hogy 2015. szeptember 25-én a Fehér Házban Barack Obama amerikai és Hszi Csin-ping kínai elnök is aláírt egy kétoldalú egyezményt, melyben a felek megegyeztek, hogy felgyorsítják a rosszindulatú

támadások esetén az információáramlást és a segítségnyújtást. Egyik fél sem folytat és nem támogat tudatosan szellemi tulajdon eltulajdonítására irányuló, kibertérben végrehajtott műveleteket, amelyek célja üzleti titkok és üzleti előnyszerzésre alkalmas más bizalmas információk megszerzése, valamint javítják a kiberbűnözés elleni együttműködést.

Összefoglalás

Összefoglalásul elmondhatjuk, hogy a technológiák fejlődésével elsőrendű kérdéssé vált a kiberbiztonság témaköre. Ezt mára már minden ország felismerte és lépéseket tett ezirányban. A nemzetközi összefogás elengedhetetlen a kiberbűnözés és a terrorizmus visszaszorítása érdekében. Minden arra mutat, hogy az informatikai rendszerek egyre jobban behálózzák nemcsak a mindennapi életet, hanem a hadseregeket is. A katonai vezetésirányító rendszerek, az intelligens fegyverek mind hálózatos elven fognak működni, így biztonsági kockázatnak lesznek kitéve. Tisztában kell lennünk azzal, hogy az elkövetkezendő évek konfliktusaiban egyre nagyobb szerepet fog játszani az ellenséges országok nemcsak katonai, hanem polgári hálózatos elektronikus információkezelő rendszereinek és létfontosságú információs rendszerelemeinek támadása. Azok az országok, amelyek nem fogják ezen irányú képességeiket kialakítani, jelentős hátrányba kerülhetnek, hiszen csak a kibervédelem kialakítása nem biztos, hogy elég lesz egy konfliktusban. Ezért a jövőben számítani kell arra, hogy egyre több energiát fognak a világ államai a kibertámadó potenciáljaik növelésére fordítani. Véleményem szerint hazánkban is fel kellene állítani egy olyan egységet, amely képes a kibertérben támadó jellegű műveletek végrehajtására is. Ahogy az a fentiekben is látható volt, más országok ezeket az egységeket katonai vezetés alatt állították fel, a fegyveres erők kötelékében. Ez biztosíthatja a komplex katonai műveletekben a kiberhadviselési képességek optimális kihasználását, más műveletekkel történő összehangolását. Ezért hazánkban is a Magyar Honvédség kötelékében kellene integrálni ezt a képességet, szoros együttműködést kialakítva a kibervédelemmel foglalkozó más hazai szervezetekkel.

Felhasznált irodalom

Könyvek

MUHA L., KRASZNAY Cs. (2014) *Az elektronikus információs rendszerek biztonságának menedzselése,* NKE, Budapest

Hadtudományi Lexikon (1995), MHTT, Budapest

GREENWALD G. (2014) A Snowden-ügy, HVG Kiadó, Budapest

HAIG Zs. (2015) Információ, társadalom, biztonság, NKE, Budapest

HAIG Zs., Várhegyi I. (2005) Hadviselés az információs hadszíntéren, Zrinyi Kiadó, Budapest

Publikációk

CSERHÁTI A.: A Stuxnet vírus és az iráni atomprogram

Nukleon IV. évfolyam 1. szám Budapest 2011. p.: 85

HAIG Zs., Kovács L.: Fenyegetések a cybertérből

Nemzet és biztonság I. évfolyam, 5. szám. Budapest, 2008. pp.: 61–69

HAIG Zs.: Internet terrorizmus, *Nemzetvédelmi Egyetemi Közlemények*, XI. évfolyam, 2. szám Budapest, 2007. pp.: 81–93.

GYEBROVSZKI T.: Stuxnet – mint az első alkalmazott kiberfegyver – a Tallini Kézikönyv szabályrendszere szempontjából, *Hadmérnök* XI. évfolyam 1. szám Budapest, 2014 pp.: 164–174

JORDÁN Gy: A kínai katonai modernizáció, *Nemzet és biztonság* IV. évfolyam 2. szám. Budapest, 2011. pp.: 32–49

KOVÁCS L.: Információs hadviselés kínai módra, *Nemzet és biztonság* II. évfolyam 7. szám. Budapest, 2009. pp.: 35–44

KOVÁCS L: Európai országok kiberbiztonsági politikáinak és stratégiáinak összehasonlító elemzése I., *Hadmérnök* VII. évfolyam 2. szám Budapest, 2012 pp.: 302–311

KOVÁCS L: Az információs terrorizmus eszköztára, *Hadmérnök különszám* Budapest, 2006. november 22.

KOVÁCS L., Sipos M.: A stuxnet és ami mögötte van, *Hadmérnök* V. évfolyam 4. szám Budapest, 2010. pp.: 163–172

KOVÁCS Z.: Védett vezetők hordozható infokommunikációs eszközeinek védelme a rádiófrekvenciás tartományban, *Bolyai Szemle* XXIII. évfolyam 4. szám Budapest, 2014. pp.: 58–77

NAGY V.: The geostrategic struggle in cyberspace between the United States, China and Russia, AARMS Vol. 11, No. 1 Budapest 2012. pp.: 13–26

BÁNYÁSZ P.: A közösségi média szerepe a lélektani műveletekben az elmúlt időszak válságainak tükrében, *Szakmai Szemle* 2016. I. szám, Budapest pp.: 61–81

Dokumentumok

JP 1-02 Department of Defense Dictionary of Military and Associated Terms, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf

Tallinn Manual on the International Law Applicable to Cyber Warfare https://ccdcoe.org/tallinn-manual.html

FM 3-38 Cyber Electromagnetic Activities, http://www.fas.org/irp/doddir/army/fm3-38.pdf

Magyarország Nemzeti Kiberbiztonsági Stratégiája, http://www.mysec.hu/download/MK2013_47_M_N_Kiberbiztonsagi_Stratagiaja.pdf

Számítástechnikai Bűnözés Elleni Egyezmény, http://www.jogiforum.hu/publikaciok/50

International Strategy for Cyberspace – Prosperity, Security, and Openness in a Networked World, https://www.whitehouse.gov/sites/default/files/rss_viewer/internationalstrategy_cyberspace.pdf

Warsaw Summit Communiqué, http://www.nato.int/cps/en/natohq/official_texts_133169.htm?selectedLocale=en

Internetes forrás

Internet World Stats, http://www.internetworldstats.com/stats.htm [elolvasva: 2016. február 12.]

BUSSELL, J. (1995) Cyberspace – Enciklopedia Britannica, http://www.britannica.com/topic/cyberspace [elolvasva: 2016. február 12.]

NORTON (2012) Norton Cybercrime Report, http://www.symantec.com/content/en/us/home_homeoffice/html/cybercrimereport/assets/downloads/en-us/NCR-DataSheet.pdf [elolvasva: 2016. február 12.]

Securelist (2013) Red October" Diplomatic Cyber Attacks Investigation, https://securelist.com/analysis/publications/36740/red-october-diplomatic-cyber-attacks-investigation/ [elolvasva: 2016. február 14.]

CERT (2012) Újabb taggal bővült a Stuxnet „család", http://tech.cert-hungary.hu/tech-blog/120810/ujabb-taggal-bovult-a-stuxnet-csalad, [elolvasva: 2016. február 14.]

VÁMOSI, G. (2010) *A kretének háborúja zajlott az Interneten*, http://www.origo.hu/techbazis/20101117-a-4chan-a-tumblr-ellen-a-kretenek-haboruja-zajlott-az.html [elolvasva: 2016. február 14.]

NEMES, D. (2008) *Hackerek a szcientológia ellen*, http://pcworld.hu/kozelet/hackerek-a-szcientologia-ellen-20080128.html, [elolvasva: 2016. február 14.]

RAWLINGS, N. (2013) *Anonymous Hackers Plead Guilty to PayPal Cyber Attack,* http://techland.time.com/2013/12/09/anonymous-hackers-plead-guilty-to-paypal-cyber-attack/ [elolvasva: 2016. február 14.]

DUBUIS, A. (2015) Anonymous declares war on Islamic State after Paris attacks in chilling video: ‚We will hunt you down', http://www.mirror.co.uk/news/world-news/anonymous-declares-war-islamic-state-6839030 [elolvasva: 2016. február 14.]

Anon – *Az Anonymous Operation Hungary adatlapja a Facebook-on,* https://www.facebook.com/OpHunAnon/info [elolvasva: 2016. február 14.]

HESS, P. (2009) *Levin: More e-mails from Ft. Hood suspect possible,* http://townhall.com/news/politics-elections/2009/11/21/levin_more_e-mails_from_ft_hood_suspect_possible [elolvasva: 2016. február 15.]

TIMOTHY, T. (2003) *Al Qaeda and the Internet: The Danger of "Cyberplanning"*, http://strategicstudiesinstitute.army.mil/pubs/parameters/Articles/03spring/thomas.pdf, [elolvasva: 2016. február 15.]

KETTMANN, S.: *Soviets Burned By CIA Hackers?.*, http://archive.wired.com/culture/lifestyle/news/2004/03/62806?currentPage=all, [elolvasva: 2016. február 14.]

NÉMETH J., HAJZER T. (2008): *Az orosz-grúz háború néhány jellemző vonása,* http://old.biztonsagpolitika.hu/?id=16&aid=709&title=az-orosz-gruz-haboru-nehany-jellemz337-vonasa [elolvasva: 2016. február 16.]

Magyar Nemzet Online (2016): *Visszafelé sült el Izrael fegyvere*, http://mno.hu/film/visszafele-sult-el-izrael-fegyvere-1329288, [elolvasva: 2016. március 30.]

SG1 (2015): *Izrael tagadja, hogy köze lenne a Duqu 2 kémprogramhoz*, https://sg.hu/cikkek/112940/izrael-tagadja-hogy-koze-lenne-a-duqu-2-kemprogramhoz, [elolvasva: 2016. március 30.]

BERZSENYI D., SZENTGÁLI G. (2010): *STUXNET: a virtuális háború hajnala*, http://old.biztonsagpolitika.hu/?id=16&aid=932&title=stuxnet-a-virtualis-haboru-hajnala [elolvasva: 2016. február 20.]

VÁMOSI G., SZEDLÁK Á. (2008) : *Az Interneten is zajlik az orosz-grúz összecsapás*, http://www.origo.hu/techbazis/internet/20080811-az-interneten-is-zajlik-az-oroszgruz-osszecsapas.html [elolvasva: 2016. február 20.]

LANGNER R. hamburgi vírusbiztonsági szakértő blogja 2010. december 31., http://www.langner.com/en/blog/page/13/ [elolvasva: 2016. február 20.]

FLOOK. K, (2009): Russia and the Cyber Threat, http://www.criticalthreats.org/russia/russia-and-cyber-threat, [elolvasva: 2016. február 25.]

ORBÓK, Á (2015): *Kibertér, mint hadszíntér,* http://biztonsagpolitika.hu/wp-content/uploads/2015/04/Orbok-Akos-A-kiberter-mint-hadszinter.pdf, [elolvasva: 2016. február 14.]

DoD (2010): *U.S. Department of Defense, Cyber Command Fact Sheet, 21 May 2010*, http://www.stratcom.mil/factsheets/2/Cyber_Command/, [elolvasva: 2016. március 30.]

NSA (2016): Leadership, https://www.nsa.gov/about/leadership/, [elolvasva: 2016. március 30.]

NSA2 (2016): About NSA, https://www.nsa.gov/ faqs/about-nsa-faqs.shtml, [elolvasva: 2016. március 30.]

Mandiant (2013): *APT1 Exposing One of China's Cyber Espionage Units,* http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf, [elolvasva: 2016. március 30.]

SG2 (2016): A Negev-sivatagban lesz Izrael kibervédelmi központja, https://sg.hu/cikkek/117093/a-negev-sivatagba-lesz-izrael-kibervedelmi-kozpontja, [elolvasva: 2016. március 30.]

SG3 (2009): Kiberháborús egységet hoz létre a Bundeswehr, https://sg.hu/cikkek/65536/kiberhaborus-egyseget-hoz-letre-a-bundeswehr, [elolvasva: 2016. március 30.]

HVG (2016): Kisvárosnyi létszámú cyberalakulatot hoz létre a német hadsereg, http://hvg.hu/vilag/20160426_Kisvarosnyi_letszamu_cyberalakulatot_hoz_letre_a_nemet_hadsereg/nyomtatas, [elolvasva: 2016. április 30.]