Kovács László – Illési Zsolt

Cyberhadviselés[1]

A cyberhadviseléssel[2] kapcsolatosan nagyon sok értelmezés látott napvilágot az elmúlt években, ugyanakkor hivatalos definíciót, illetve letisztult eszköz- és eljárásrendszert mind a mai napig nem fogalmaztak meg. Ennek megfelelően nagyon sokszor a cyberhadviseléssel kapcsolatban az éppen nyilatkozó álláspontja, illetve szakterülete kapta és kapja ma is a legnagyobb hangsúlyt. Így azt nagyon sokan az interneten folyó különböző tevékenységekkel azonosítják, és informatikai problémának tekintik a kérdést. Tovább nehezíti a terület áttekintését, hogy magára a cybertér fogalmára sem találunk egyértelmű hivatalos megfogalmazást. Itt is javarészt az internetet, vagy szerencsésebb esetben a különböző számítógép-hálózatokat is magába foglaló virtuális teret szokták még a szakértők is emlegetni, mint a cybertér dimenzióját.

E terület tudományos igényű megfogalmazása tehát még várat magára, hiszen a szakmai közösség különböző szereplői is attól függően határozzák meg a cyberhadviselést, hogy milyen szerepet töltenek be az információtechnológia felhasználásában vagy alkalmazásában. Ugyanakkor a napjainkra nélkülözhetetlen információs infrastruktúrák, a mind szélesebb körű internet-penetráció, a vezeték nélküli technológiák, az okostelefonok robbanásszerű elterjedése egyre égetőbbé teszik a kérdés megtárgyalását és elemzését. Ezen eszközökkel és rendszerekkel szemben ugyanis olyan fokú függőség alakult ki napjaink társadalmában, amely komoly biztonsági kihívást és kockázatot is jelent. Ezekre a kihívásokra az elmúlt években bekövetkezett számos olyan esemény is felhívta a figyelmet, amelyek során megjelentek a hagyományos hadviseléssel párhuzamosan a cybertámadások is.

Jelen írás célja, hogy nagyon röviden bemutassa a cyberhadviselés elemeit, valamint értelmezze területeit, illetve az azok közötti kapcsolatot. Mindezeken túl

1 Jelen írás a Magyar Tudományos Akadémia Bolyai János Kutatási Ösztöndíj támogatásával valósult meg.

2 A hazai terminológia a *cyber* szót értelemszerűen magyarul a *kiber* szóval igyekszik kifejezni. Véleményünk szerint azonban a kiber szó számos alkalommal nem teljes mértékben fedi le azt a tartalmat, amelyet szakmai körökben túlnyomó részben a cyber szó alkalmazásával egyesítünk. Ezért jelen írásban a szerzők is a cyber szó használata mellett döntöttek.

bemutatja azt az egyik legnagyobb problémát, amely nem más, mint a cybertérben történő bizonyítás nehézsége.

A cybertér és a cyberhadviselés fogalmi meghatározása

William Gibson 1984-ben megjelent Neuromancer című, mára már a cyberpunk egyik alapművének számító novellájában használta elsőként a cybertér kifejezést. Azóta a köznapi értelmezés szerint a cybertér az elektronikus kommunikációs eszközök és rendszerek, valamint az azokon található szolgáltatások, információk által alkotott virtuális tér összefoglaló neve. Ugyanakkor napjainkban –, ahogy egyre több és több hálózatba kötött elektronikai eszközt és rendszert használunk – a cybertér értelmezése is egyre bővül. Ebben a térben helyet kell kapniuk azon a rendszereknek is, amelyek a hálózatba kötött, vezeték nélküli elektronikai eszközöket, így az elektromágneses spektrumot használják fel a kapcsolat kialakítására.[3] [1] Ugyanez igaz a cybertér katonai értelmezésére is. A hadseregek ugyanis már jóval a vezeték nélküli hálózati technológiák megjelenése előtt használták az elektromágneses spektrumot, mint fizikai réteget, a számítógép-hálózatok kialakítására, hiszen a rádió alkalmazása kézenfekvő volt e célra is. [2]

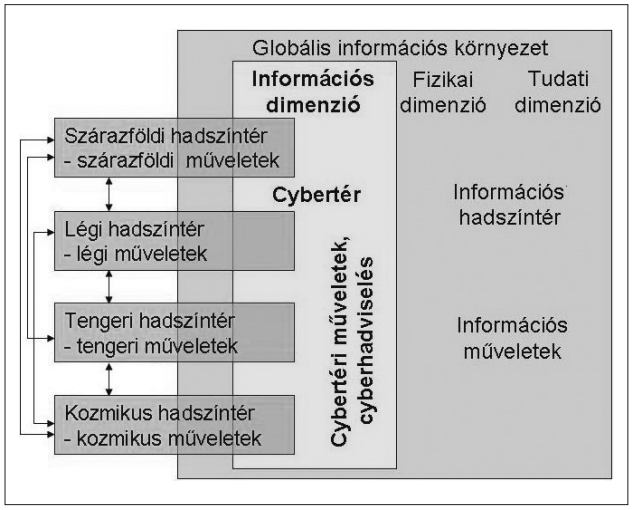
A cybertér értelmezésében és dimenzióinak meghatározásában ugyanakkor továbbra is helyet kell, hogy kapjanak a vezetékes hálózatok, mert a hálózatban lévő különböző elektronikai eszközök továbbra is csatlakozhatnak egymáshoz vezetékes kapcsolatokon keresztül is. Mindezt azok az egyre inkább elterjedő optikai vezetékes hálózatok is alátámasztják, amelyek a különböző, nagy sávszélességet igénylő multimédiás (hang, kép, mozgókép, szöveg) tartalmak átviteléhez nyújtanak elengedhetetlen fizikai kapcsolatot. Ennek megfelelően a cybertér katonai értelmezésében helyet kap az elektromágneses spektrum, és ezzel párhuzamosan a vezetékes hálózatok jelentette virtuális tér is. [2] A cybertér értelmezését mutatja be az 1. ábra.

Az eddigieket összefoglalva katonai értelmezésben a cybertér a hadviselésnek a földi-, légi-, tengeri- és kozmikus színterekkel hasonlatos, azzal egyenértékű tartománya. Ahogy a légi hadszíntér a levegőben folytatott műveletekkel, a szárazföldi hadszíntér a földön végrehajtott akciókkal, ugyanúgy jellemezhető a cybertér is a hálózatba kötött elektronikai rendszerekkel és a teljes frekvencia spektrum használatával. [2]

Ugyanakkor a hadviselésben, a különböző katonai tevékenységek során, számos helyen alkalmazunk szeizmikus és akusztikus szenzorokat, amelyek tovább bővítik a cybertér fogalmát, hiszen ezekkel az eszközökkel megjelenik a szeizmikus, illetve az akusztikus rezgések tartománya is. Mindezek mellett az irányított energiájú fegyverek, amelyek jelentős része (például az infrahangfegyverek, a hallható tartományú lökéshullám-generátorok, a nagy energiájú részecske sugárzók stb.) szintén a fizikai tartományokban működik, még tovább bővíthetik a cybertér értelmezését. Mindezeknek megfelelően a cybertér kibővített értelmezésében az elektromágneses spektrum helyett a teljes frekvenciatartományt kell értelmeznünk. [2]

---

3 Ez a kapcsolat az ISO OSI (Open Systems Interconnection) modell alapján az a fizikai réteg, amelyet az elektromágneses hullámok segítségével hozunk létre.



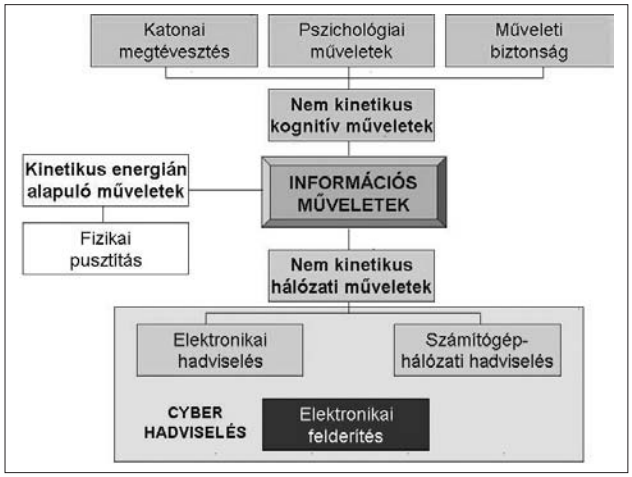
1. ábra. A cybertér értelmezése [1]

A cybertér definiálása után meg kell vizsgálnunk, mit is értünk a cyberhadviselés fogalmán. Az 1980-as évek közepén jelent meg az információs hadviselés fogalma, amely az 1991-es Öböl-háborút is meghatározta. Az azóta eltelt időszakban azt a tevékenységet, amelynek elsődleges célja az információs fölény és az információs uralom megszerzése, majd ennek vezetési, illetve hadműveleti fölénnyé váltása, információs hadviselés helyett – főleg a katonai terminológiában – információs műveleteknek nevezzük. Az információs műveletek három alapvető területre oszthatók: a nem kinetikus kognitív műveletekre, a hagyományos kinetikus energián alapuló műveletekre és a nem kinetikus hálózati műveletekre. [3]

Ez utóbbi területen, azaz a hálózati műveleteken belül értelmezzük a cyberhadviselést úgy, hogy párhuzamosan a hagyományos műveletekkel, az információs dimenzióban (és bizonyos értelemben a kognitív dimenzióban is) megjelenik a cyberhadviselés is. E területek összefüggéseit mutatja be a 2. ábra.

Definíciószerűen megfogalmazva cyberhadviselésnek nevezhetjük mindazon tevékenységeket, amelyekben a számítógép-hálózati hadviselés, a számítógép-hálózati műveletek, az elektronikai hadviselés, bizonyos esetekben a rádióelektronikai felderítés (Signals Intelligence – SIGINT),[4] valamint a cyberterrorizmus, illetve az ellene folyatott tevékenységek közösen jelennek meg. [2]

4 SIGINT: Signals Intelligence, azaz rádióelektronikai felderítés. A SIGINT két alapvető részre osztható: a COMINT-re (Communication Intelligence), azaz rádiófelderítésre, és az ELINT-re (Electronic Intelligence), azaz a hagyományos magyar katonai terminológiával élve rádiótechnikai felderítésre.



2. ábra. A cyberhadviselés értelmezése [3]

A cyberhadviselés szélsőséges megnyilvánulása: a cyberterrorizmus

Minden számítógépes hálózat sérülékeny. Ha ezt egy terroristacsoport kihasználja, akkor beszélhetünk a cyberterrorizmusról.

2001 szeptembere után az USA-ban is megkezdődött a cyberterrorizmus definíciójának megfogalmazása. Az elsők között megjelent ilyen fogalom a következő volt: *„a cyberterrorizmus számítógép-alapú támadást vagy fenyegetést jelent, amelynek célja, hogy megfélemlítsék, vagy kikényszerítsék a kormányok vagy a társadalmak részéről az adott terror szervezet politikai, vallási, vagy ideológiai céljainak elérését".* [4]

A különböző, hagyományos terrorista szervezetek és csoportok is ugyanúgy használják és kihasználják a csúcstechnika nyújtotta lehetőségeket, mint a hétköznapok többi szereplője. A mobil és a műholdas kommunikációs eszközökön kívül az internet is azon eszközök közé tartozik, amelyeket a kapcsolattartástól kezdve, az akciók szervezésén át, a tagok toborzásáig felhasználnak a terrorszervezetek. Az terroristacélú információtechnológia-felhasználás a következő területeken jelenhet meg:

– tervezés;
– kommunikáció;
– titkos kapcsolattartás;
– szervezés;
– toborzás;
– propaganda;
– pénzügyi támogatás;
– adat- és információszerzés.

A különböző terrorista csoportok – 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. (E tevékenységet gyakran *soft,* azaz puha

típusú cyberterrorizmus névvel is illetik.) A másik – és nyugodtan kijelenthetjük: hatványozottan veszélyesebb – csoportba azok a terroristák tartoznak, akik nemcsak ilyen úgynevezett *soft*-tevékenységre kívánják használni a hálózatokat és az internetet, hanem ezeket felhasználva, illetve ezeken keresztül, rombolni vagy egyéb erőszakos, *hard*-cselekményeket is végre akarnak hajtani. Célpontjaik között nemcsak az internet szerepel, hanem minden olyan kritikus információs infrastruktúra is, amelyek információtechnológiai eszközökkel, vagy fizikai támadásokkal pusztíthatók.

Le kell szögeznünk: a cyberterrorizmus veszélye reális! Ezt a veszélyt nem lehet túldimenzionálni, hiszen függőségünk a kritikus információs rendszereinktől rendkívül nagy. Ez a függőség olyan mértékű, hogy amennyiben e rendszerek – akár időlégesen is, vagy akár csak részlegesen is – kiesnek a működésből, az nemcsak anyagi, de emberéletekben mérhető károkat okoz gyakorlatilag a nyugati világ bármelyik országában. Tovább növeli a veszélyt (és ezzel a sérülékenységet is), miszerint ezek a rendszerek olyan kölcsönös függőségben (interdependenciában) állnak egymással, hogy egy rendszer vagy rendszerelem meghibásodása számtalan más – nagyon gyakran előre nem is definiálható számú – rendszer működését is megbénítja. [2]

A hagyományos terrorista szervezetek cybertérben történő megjelenését bizonyítja, hogy 2001-ben még csak alig néhány, az al-Kaidához köthető vagy azzal szimpatizáns weboldalt tartottak számon. Ezek száma 2001. szeptember 11-ét követően azonban gyors növekedésnek indult. *Khaled al-Faram*, szaudi kutató 2007-ben publikált adatai alapján már 5600-ra tette az ilyen weboldalak számát. [5] [2]

Az al-Kaida ezt a tevékenységet saját honlapjain nagyon gyakran digitális dzsihádnak hívja. *Oszama Bin Laden* számos alkalommal szólította fel híveit a digitális dzsihád minél szélesebb körű kiterjesztésére a nyugati országokkal, különösen az Egyesült Államokkal szemben.

A digitális dzsihád egyik élharcosa és leghírhedtebb tagja az *Irhabi 007* felhasználói nevet használó, marokkói származású fiatal számítógépes zseni, *Junisz Tszuli* volt. (Az irhabi szó arabul terroristát jelent, a 007 pedig James Bond-ra utal, hiszen Tszuli Londonban élt egészen 2006-os letartóztatásáig.) Irhabi az Egyesült Államokban bérelt szervereket és tárhelyeket fórumainak, amelyeket természetesen lopott vagy mesterien hamisított hitelkártyákkal, online fizetett ki.

Irhabi tevékenysége időben ugyanakkorra tehető, mint amikor al-Kaida vezetői felfedezték az internet által nyújtott előnyöket. Az iraki terrorakcióival hírhedté vált *Abu Muszab al-Zarkavi* és Irhabi közös tevékenységére csak találgatások vannak, ugyanakkor Zarkavi szóvivője, *Abu Maiszara al-Iraki* egyik fórumukon elismerte, hogy Irhabi a szervezetnek dolgozott. [2]

Irhabi közel két évig adott arab és angol nyelvű, dzsihádot hirdető, csak meghatározott felhasználók számára elérhető, jelszóval védett fórumokon szakértői tanácsokat esetenként több ezer látogatónak az internetes sérülékenységekkel, azok kihasználásával, valamint a saját – hálózaton folytatott – tevékenységük minél tökéletesebb titkosításával kapcsolatban. Számos multimédiás anyagot készített és ezek segítségével online oktatásokat is tartott a dzsihádban résztvevőknek. A bérelt szervereken tárhelyet biztosított dzsihádistáknak, hogy olyan anyagokat és szoftvereket töltsenek fel, amelyek különböző internetes támadásokban felhasználhatóak. Így a

fórumozók naprakész listákhoz jutottak hozzá, amelyben a különböző legújabb webes és egyéb sérülékenységeket mutatták be. [2]

2005-ben Irhabi magát már az internetről legtöbbet tudó, és az ott alkalmazott technikák legfőbb dzsihádistájaként jellemezte. Mivel számos amerikai szervert használt fórumai fenntartására (amelyek között például az arkansasi állam egyik hivatalos szervere, valamint a George Washington Egyetem gépei is megtalálhatóak voltak), Irhabit nagyon sokáig amerikainak gondolták, és ott is keresték. [2]

Irhabit Angliában, 2007 májusában 22 évre ítélték számos bűncselekményéért, többek között gyilkosságért, robbantásban való előkészületekért és pénzmosásért. A vádak között – érdekes módon – nem szerepelt internetes bűncselekmény. [2]

Cybertámadások

Az elmúlt években számos, a cybertérben bekövetkezett támadás tanúi lehettünk. E támadások közül kettőt emelünk ki.

2007 áprilisában és májusában *elosztott szolgáltatás-megtagadással járó támadások* (Distributed Denial of Service – DdoS) érték Észtország számítógépes hálózatait. Az egyébként igen fejlett információs infrastruktúrával rendelkező, és az e-kormányzat területén komoly sikereket elért Észtország a több mint kéthetes támadás során komoly anyagi károkat szenvedett. A támadások következtében számos kormányzati, minisztériumi és pénzintézeti internetes oldal vált elérhetetlenné. A támadások a tallinni orosz emlékmű elmozdítása után kezdődtek, és nagy részük többé-kevésbé beazonosíthatóan Oroszországban működtetett szerverekről indult. Az észt miniszterelnök az orosz kormányt tette felelőssé a támadások miatt. (Oroszországot korábban Ukrajna és az Egyesült Államok is megvádolta hasonló támadások végrehajtásával, de Moszkva minden alkalommal határozottan tagadta részvételét az akciókban.)

Az online támadások alatt összesen 128 túlterheléses támadás történt. A legkomolyabbak öt-tíz órán át, több száz megabitnyi sávszélességen bombázták folyamatos adatlekérésekkel a megtámadott szervereket addig, amíg azok össze nem omlottak. Az észt hálózaton az adatforgalom esetenként órákon át a normális ezerszerese volt. (Ehhez – egyes források szerint – valószínűleg az internetes alvilágtól kellett erőforrásokat bérelnie a támadóknak.) Érdemes megjegyezni, hogy közel fél évvel a támadások után csak egyetlen támadót sikerült bizonyíthatóan azonosítani. Meglepő módon azonban ez a támadó egy észt fiatalember volt, akit a bizonyítékok alapján pénzbüntetésre ítéltek. [7] [8]

A másik cybertámadás, amelyet jelen írásban ismertetünk, 3 évvel a klasszikussá vált orosz–észt cyberkonfliktus után következett be. Ez a támadás egy rosszindulatú speciális szoftverhez: a Stuxnet nevű féreghez köthető, amely hatalmas riadalmat okozott 2010 nyarán, illetve kora őszén. A riadalom oka elsősorban az volt, hogy ez volt az első olyan rosszindulatú program, amely ipari létesítmények vezérlő szoftvereit támadta meg. [9]

A *Stuxnet*et 2010 nyarán egy fehérorosz vírusirtó cég fedezte fel. Már a felfedezés utáni első elemzések során kiderült, hogy azt elsősorban ipari folyamatirányító rendszerek ellen fejlesztették ki. A féreg programozása olyan zseniális volt, amely feltételezte, hogy azt profi programozók, nem kevés anyagi források birtokában készítet-

ték. A program négy olyan biztonsági hiányosságot is kihasznált, amelyeket mindaddig még csak nem is publikáltak. [9]

A féreggel kapcsolatosan a felfedezését követően nagyon sok találgatás látott napvilágot. E találgatások oka elsősorban a program újdonságában keresendő. A rosszindulatú programok több évtizedes történetében ez volt első olyan szoftver, amely nagy tömegben támadta ipari létesítmények vezérlő-szoftvereinek működését.

A találgatások politikai felhangoktól sem voltak mentesek, hiszen a féreg előfordulási gyakorisága és észlelése Iránban volt a legmagasabb. Ez rögtön szemet szúrt a különböző médiumoknak, és rögtön hírül is adták: a féreg célpontja az iráni atomlétesítmények, konkrétan azok működésének leállítása. Ezeket a találgatásokat az informatikai biztonsági cégek elemzései még részben alá is támasztották, hiszen nagyon gyorsan kiderült: valóban olyan ipari vezérlő szoftverek ellen készült a Stuxnet, amelyeket Irán is használ például a bushehri atomerőműben, vagy a natanzi centrifugáinál. [9]

2011 januárjában a New York Times (NYT) adott elsőként hivatalosan hírt arról, hogy a Stuxnet mögött Izrael áll (a féreg forrásáról mindaddig csak feltételezések és találgatások léteztek). A NYT cikke összhangban állt információbiztonsági szakértők véleményével, hiszen a cikk szakértőkre hivatkozva szintén megemlíti, hogy a férget olyan ipari létesítményben kellett tesztelni, mint a későbbi célpontok. Ez a létesítmény pedig nem más, mint az izraeli Negev-sivatagban lévő Dimona-komplexum, amely köztudottan az izraeli nukleáris kutatás központja. Itt tesztelték és próbálták ki az urándúsítás elengedhetetlen kellékein, az izotópcentrifugákon, illetve ezek irányító szoftverein a Stuxnetet. A cikk kitér arra is, hogy *Hillary Clinton* és a nemrég nyugdíjba vonult Moszad vezető, *Meir Dagan*, egymástól függetlenül, de nagyjából azonos időben kijelentették: remélik az események az iráni atomprogramot akár több évvel is visszavetik. Ez természetesen arra is következtetni enged, hogy az akció nemcsak Izrael magánakciója volt, hanem az USA is hathatósan közreműködött. [9] [10]

Mindkét bemutatott támadás esetén világosan látszik: számos bizonytalan tényező van a támadások körül. Egyrészt a támadók, illetve az elkövetők személye bizonytalan. Még ma sem bizonyítható teljesen egyértelműen az orosz–észt konfliktus esetében, hogy valóban oroszok voltak a támadók. A Stuxnet esetében szintén nem bizonyítható, hogy Izrael vagy az USA az ötletgazda, vagy esetleg a támadó. Mindezeken túl sok egyéb kérdés is felmerül: hol kezdődik a hagyományos hadviselésen túl a cyberhadviselés? Vannak-e ennek szabályai? Lehet-e atomerőműveket, kórházakat, iskolákat támadni, amelyeket egyébként a hágai vagy a genfi egyezmények tiltanak? Kik a szembenálló felek egy cybertámadás során, amikor az elkövetők személye sem bizonyítható?

Különösen fontos tehát a bizonyíthatóság kérdése (azaz ki a támadó, és mi a cél) abban az esetben, ha egy NATO-országot ér cybertámadás (mint ahogy azt Észtország esetében láthattuk), hiszen a Szövetség alapokmányának 5. cikkelye egyértelművé teszi a kollektív védelmet. Ugyanakkor a bizonyíthatóságon túl annak eldöntése, hogy egy adott cybertámadás fegyveres támadással egyenértékű-e, szintén olyan kérdés, amely komoly kihívás elé állítja az a különböző országokat, vagy akár a NATO-t.

Bizonyíthatóság a cybertérben

A bizonyítás jogi értelemben egy sajátos megismerési folyamat, ami főleg – az egyedi ügyek tényállásával kapcsolatos – jogilag releváns múltbeli eseményeknek a valóságnak megfelelő és megállapítására, utólagos rekonstrukciójára irányul és bizonyítékok összegyűjtésével, vizsgálatával és azok mérlegelésével kapcsolatos tevékenységekből áll. A tényállás valósággal adekvát megállapítására a bíróság jogosult, azonban a bizonyítékok összegyűjtése, vizsgálata és előzetese mérlegelése a nyomozóhatóságok feladata. Amennyiben a tények megállapításához, vagy mérlegeléséhez különleges szakértelem szükséges, úgy a hatóságok szakértői vizsgálatokat rendelnek el, illetve szakértőt bíznak meg szakértői vélemény adásával. [11]

Az eljáró hatóság a bizonyítás során arra keresi a választ, hogy:

– Ki vagy kik az elkövetők?
– Milyen cselekmények valósultak meg?
– Hol követték el a cselekményt?
– Az események milyen sorrendben követték egymást?
– Mik voltak az esemény hátterében álló motivációs tényezők?
– Hogyan és milyen eszközzel, eszközökkel hajtották végre a cselekményt? [12]

A fenti kérdések megválaszolása elengedhetetlen az elkövetett cselekmények jogi megítéléséhez. Az objektív tényállási elemek (az elkövető személye, az elkövetés helye és ideje) alapozzák meg magát a (büntető, polgári stb.) jogi tényállást, a szubjektív (az emberi akarattal kapcsolatos) tényállási elemek (jó- és rosszhiszeműség, szándékosság, gondatlanság, aljas indok stb.) pedig főleg a minősítést meghatározó tényező. A cyberhadviselés vagy a cyberterrorizmus vizsgálatakor azonban valamennyi fenti kérdés megválaszolása sajátos problémákat rejt. A következőkben ezeket a kérdéseket járjuk körül.

Az elkövető személye

Az informatikai rendszerek vizsgálatakor az adatok között a szakértők számítógép-azonosítókat (IP/MAC-cím stb.), felhasználói azonosítókat (USER ID) találnak. Büntetőjogi felelősségre azonban csak természetes személyeket lehet vonni. A felhasználó-név vagy számítógép azonosító viszont nem egyértelműen és nem minden kétséget kizáróan kapcsolódik egy-egy természetes személyhez. A jelszavakat illetéktelenek is használhatják, a speciális hardverkulcsokat ellophatják, a biometriai azonosítókat pedig esetenként meghamisíthatják vagy becsaphatják az érzékelőket az elkövetők. A nyomozás során sajátos technikákat kell alkalmazni, hogy a számítógépek, felhasználói nevek mögött rejtőző személyeket egyértelműen össze lehessen kapcsolni.

További probléma az, hogy az azonosított természetes személyek mögött álló szervezeteket, államokat még nehezebb összefüggésbe hozni az elkövetőkkel. Így pedig a cselekmény minősítése (terrortámadás, katonai művelet), és a szükséges válaszlépések meghatározása is, szerteágazó és hosszadalmas folyamat.

Az internetes támadásoknál jellemző az érintett informatikai eszközök és infrastruktúra-elemek nagy száma, azoknak a cselekményekben betöltött szerepéből

pedig nehéz következtetni a szerepükre. Az informatikai eszközök lehetnek a támadás forrásai (például DDoS-támadás esetén egy támadó „zombi számítógép"), a támadások útvonala (például az internetszolgáltatók által működtetett hálózatok), illetve támadások célpontjai. Az egyes szerepek esetenként összekeverednek (például a nagymama által levelezésre és böngészésre használt, védetlen otthoni számítógépet megtámadva jutnak egy másik támadás aktív zombi számítógéphez az elkövetők).

Az orosz–észt cíberkonfliktus során 178 országból – köztük hazánkból is – érkeztek támadások észt rendszerek ellen. A támadásokat elemző Arbor Networks cég 128 túlterheléses támadást észlelt az incidens során, amelyeknek a zöme egy órán belül véget ért. Volt azonban 15 olyan támadás, amely öt óráig, illetve néhány, ami több mint tíz órán át tartott. A legsúlyosabb támadások 100 Mbps feletti (a normális forgalom akár ezerszerese) összesített sávszélességen zajlottak, ami óriási zombipécéhálózatok meglétét valószínűsíti a háttérben. [13] [14] [15]

Az események valós természete

A bizonyítékszerzés során a legjobb forrás egy hiteles naplóállomány-rendszer lenne valamennyi érintett számítógépről és infrastrukturális elemről. A probléma azonban az, hogy ezeknek az állományoknak a rendelkezésre állása esetleges (a rendszergazdák, szervezetek, felhasználók maguk döntik el, hogy bekapcsolják-e ezen a naplózási funkciót vagy sem; a programok alapbeállítása is teljesen véletlenszerű). Amennyiben rendelkezésre állnak naplóállományok, akkor azok szerkezete egyedi: a legtöbb programozót nem képezték ki ugyanis arra, hogy szabványos formában tárolja a naplóadatokat, illetve nincs fogalma arról, hogy milyen adatokat kell (vagy kellene) tartalmaznia egy használható naplónak. Az eltérő szerkezetű és adattartalmú naplók adatait pedig sokszor nem, vagy csak nagyon körülményesen lehet összevetni.

Naplóállományok híján a nyomokat rekonstruáló szakértőknek a fájlrendszerek, adatbázisok mélyén megbújó, sokszor implicit információmorzsák alapján – nyomkereső módjára – kell rekonstruálnia az eseményeket. Ez sokszor nem biztosít elegendő támpontot a bizonyításhoz, legfeljebb a további nyomozati cselekményekhez ad némi muníciót.

A Microsoft-cég összeállított egy programcsomagot (COFEE, [16]) a Windows rendszer segédprogramjaiból. Ezt a helyszínen talált vagy az ügyben érintett MS Windows operációsrendszerű gép vizsgálatakor a szakértő csak egy USB-eszközre másolva csatlakoztatja a számítógéphez és viszonylag egyszerűen le tudja menteni a lényeges adatokat. A támadók erre válaszul kifejlesztettek egy olyan programot (DECAF, [17]), amely érzékeli a COFEE jelenlétét és mindenféle válaszlépés megtételére képes (törli a naplókat és/vagy lezárja a számítógépet, és/vagy véletlen időadatokkal írja felül a fájl MAC-adatait, és/vagy törli a fájlokat stb.). Megállapítható tehát, hogy az elkövetők is felkészültek a szakértői vizsgálatokra: mindent megtesznek azért, hogy ellehetetlenítsék azokat. A vizsgálat során tehát különös figyelmet kell fordítani a szándékosan vagy véletlenül módosított (inkonzisztens) adatok kiszűrésére és elemzésére.

Az események helyszíne

Súlyos nehézséget okoz a cyberterrorizmus és cyberhadviselés vizsgálatakor annak megállapítása, hogy pontosan mi is a cselekmény helyszíne. Amíg egy gyilkosságnál jól látható módon „körbekeríthető" a helyszín, „körberajzolható" az áldozat és az elkövetés eszköze, addig a cybertérben ez a kérdés sokszor egyértelműen meg se válaszolható. A virtuális helyszíneléskor – a fizikaihoz hasonlóan – a kérdés az, hogy ott van-e a helyszín

– az ahol az elkövető van;
– az ahol a felhasznált rendszerek vannak;
– az ahol a célpont van;
– ahol ezek együtt vannak?

A cybertámadásokra jellemző a nemzetközi jelleg. Nem csak az orosz–észt konfliktus során „vett részt" több ország (pontosabban több országban működő számítógép) a támadásban, de szinte lehetetlen olyan internetes támadást indítani, hogy a támadó csak egy országban működő számítógépeket használjon fel és támadjon meg. A technológia fejlődésével (például a cloud-computing terjedésével) pedig már azt is nehéz lesz megmondani, hogy pontosan melyik számítógép (számítógépfelhő) tárol, továbbít, dolgoz fel. (Például egy Google-levelezés, dokumentumok, naptár, csoportok felhasználásával megszervezett és elkövetett támadás esetén az is komoly szakmai kérdés, hogy hol is van [ti. a cloud mely számítógépén, szerverparkjában] tulajdonképpen az adathalmaz.)

A nemzetközi jelleg nem csupán a helyszín fizikai méretét tágítja ki kezelhetetlenül nagyra, hanem gátja a hatékony felderítésnek. A külföldön tárolt adatokhoz, az ott tartózkodó elkövetőkhöz a hazai hatóságok csak nemzetközi jogsegély útján tudnak hozzáférni. Ehhez az szükséges, hogy a hazai jogban bűncselekménynek minősülő magatartás büntetendő legyen a célországban is, mivel bűncselekmény hiányában általában a felkéréseknek nem tesznek eleget a külföldi hatóságok. Az országok jogharmonizációs hiányosságai miatt előfordulhat ugyanis, hogy ami az egyik országban bűncselekmény, az egy másik országban tűrt vagy éppen megengedett.

Az események sorrendje

Az események idejének megállapításakor a legtöbb esetben nem áll rendelkezésre hiteles időadat. Bár a számítógépek rendszerint egy-egy atomórához kapcsolódva szinkronizálják az órájukat, erre nem lehet alapozni. Az órákat a rendszergazdák, felhasználók időnként elállítják (például hogy lefusson egy korábban lejárt próbaidejű program), a szinkronizálást kikapcsolják, vagy nem kapcsolják be. A rosszindulatú támadók pedig (a DECAF-nál leírtakkal analóg módon) automatizálják a rendszer időadatainak összekavarását, hogy megnehezítsék vagy ellehetetlenítsék a bizonyítást.

A hiteles időadatok meglétének hiánya mellett felmerül a dátum- és időábrázolások sokféleségének a problémája. A *y2k* (2000. év) problémája már rámutatott arra, hogy az évszámok nem megfelelő tárolása normál körülmények között is működési problémát jelent. A helytelen/bizonytalan adatstruktúra a bizonyítás során azonban

egyenesen ellehetetlenítheti a dátumadatok helyes értékelését. (Milyen dátum lehet például a 01/02/03 vagy a 09/10/11?)

A cybertámadások során problémát jelent a felhasználók és a számítógépes rendszerek eltérő „időléptéke" is. A támadások több tényezője akár hosszú ideig működhet látens módon, miközben a sértett nem is tud arról, hogy a rendszere felett külső erők részben vagy egészében már átvették az uralmat. A Stuxnet-féreg például hónapokon keresztül kompromittálta az iráni atomprogramban résztvevő számítógépeket és ipari rendszereit, miközben a célország informatikai biztonsági szakemberei nem tudtak arról, hogy mi folyik az általuk biztonságosnak vélt rendszerekben. A látens támadások alatt a támadó nemcsak a közvetlen céljait tudja elérni, hanem lehetősége van a nyomainak eltüntetésére, módosítására – az időadatok és a valódi bizonyítékok manipulálása mellett álbizonyítékok elhelyezésére.

A motivációs tényezők

A számítógépek sok információt tárolhatnak a cselekmény elkövetésének okairól, az elkövető motivációs tényezőjéről. A társ-elkövetőkkel folyatott levelezés, a személyes naplók, az elkövető számítógépén tárolt könyvek, a meglátogatott weboldalak mind hozzájárulhatnak az elkövető személyiségprofiljának, motivációs tényezőinek feltárásához. Azonban egy támadás értékelésekor külön figyelmet kell annak szentelni, hogy az így nyert adatoknak – a teljes kép szempontjából – van-e értelmük, és nem csak egy elterelő művelet részét képezik.

A cybertámadás felhasználható ürügyként is, hogy két állam viszonyát megrontsa, vagy kirobbantson egy fegyveres konfliktust. Külön vizsgálandó tehát a célország és a feltételezett támadó ország, illetve a támadásban résztvevő, „eszközként felhasznált" országok egymáshoz való viszonya is. A vizsgálat során az indítékok feltárásához sokszor szükséges (lenne), hogy az ügyben érintett országok (állam- és/vagy szolgálati) titkaiba is betekintsenek a vizsgálatot végzők. Ez viszont – a titokvédelem okán/ürügyén – sokszor teljesen ellehetetleníti az objektív és teljes körű elemzést és értékelést.

Az elkövetés módja és eszköze

Az összetett és áttételes támadási módszerek miatt sokszor nehézkes annak megállapítása, hogy pontosan mit és hogyan használ fel a cybertámadó. A támadó és a célszámítógép közé beékelődnek ún. kontrollgépek is, amelyek tovább hátráltatják a támadás részleteinek feltárását. A támadási rendszer komplex struktúrája mellett a támadók egyre hatékonyabban használják a kriptográfiai eszközöket: titkosítják az adatátviteli csatornát, az üzeneteket, a támadás során felhasznált számítógépek merevlemezét.

A titkosítás jelentősen szűkíti a vizsgálatot végző szakemberek lehetőségeit. A kriptográfia ellen a nyomozóhatóságok eredményesen tudnak fellépni a titkos felderítés és adatszerzés eszközeivel; ezeket azonban célzottan kell végrehajtaniuk (például billentyűzetfigyelő programok telepítésével), hogy az informatikai szakértők a kriptoanalízishez elegendő és megfelelő adatokhoz jussanak.

A hatékony felderítésben és elemzésben – az általános bizonyítási kérdések mellett – problémát okoz a hazai szakértők szűkös eszközrendszere, illetve az igazságügyi szakértők és a hatóságok közötti kommunikáció és együttműködés sekélyessége. Az informatikai szakértői vizsgálatok – amelyeket csak speciálisan képzett szakemberek tudnak elvégezni – a többi szakértői vizsgálathoz hasonlóan költségesek, azok elvégzéséhez speciális hardver- és szoftver-eszközök kellenek.

Az igazságszolgáltatás hazai rendszerére jellemző, hogy a speciális szaktudást igénylő kérdésekben igazságügyi szakértőt kell igénybe venni. Nincs meghatározva azonban a *sajátos szakértelem* tartalma, továbbá nagyon esetleges az, hogy a hatóság mikor rendel ki szakértőt, illetve mikor oldja meg a problémát saját hatáskörben.

Vannak például a rendőrségnek speciálisan képzett és jól felszerelt munkatársai az ORFK csúcstechnológiai bűnözés elleni osztályán. Ezek a szakértők azonban nem felelnek meg az igazságügyi szakértői törvényben meghatározott követelményeknek, nem tagjai a Magyar Igazságügyi Szakértői Kamarának (MISZK), így a jelenleg hatályos jogszabályok értelmében a büntetőeljárás során nem tekinthetők szakértőnek. A MISZK-en belül közel 200 informatikai vagy az informatikához közel álló szakértő van bejegyezve. Ezeknek a szakértőknek a technikai tudása azonban esetleges, főleg attól függ, hogy ki mikor és hol végezte az egyetemi-főiskolai tanulmányait.

A felderítési, nyomozati módszertanok sincsenek kidolgozva. Sem hazai, sem nemzetközi szinten nincsenek olyan egységes módszertani elvek, eljárásrendek, amelyek sztenderdizálnák a nyomozati munkát, illetve a begyűjtött bizonyítékok elemzését, értékelését. Hazánkban nincs informatikai krimináltechnikai kutatás-fejlesztés, így a hazai szakemberek nem vesznek részt a nemzetközi tudományos életben.

Összefoglalás – következtetések

A cyberhadviselés korunk hadtudományának egyik legújabb, és egyelőre legellentmondásosabb területe. Számos olyan kérdéssel találkozunk e téren, amelyekre jelenleg nem tudunk kielégítő választ adni. Ez annál is inkább elgondolkodtató, mert nemcsak a hadviselésben, hanem mindennapi életünkben is találkozhatunk azokkal a veszélyforrásokkal, amelyeket a cyberhadviselés, vagy akár az ezen belül értelmezett cyberterrotrizmus jelent.

A 21. század társadalma erős függőségben van a mindennapos életben használt infrastruktúráival szemben, ami igen komoly veszélyforrásként jelentkezik. Ezek az infrastruktúrák – legyenek azok polgári vagy katonai rendszerek – sérülékenyek és támadhatóak.

Következtetések helyett azokat a nyitott kérdéseket kell megismételünk, amelyek megválaszolása igen sürgető lenne. Az említett sérülékenységek ugyanis egy adott országban, vagy akár a szövetségen belül is olyan veszélyforrásokat jelentenek, amelyek meghatározóak napjainkban. Ennek megfelelően az általunk vélt nyitott kérdések a következők:

– kinek a feladata a cybertérben a védelem?
– NATO-keretek között értelmezhető-e egy cybertámadás során az 5. cikkely?

– kell-e hazánknak is cybertámadó egységeket vagy képességeket fenntartani? Ha kell, akkor ki (ti. a nemzetbiztonsági szolgálatok, a rendőrség, esetleg a Magyar Honvédség kijelölt erői) fogja ezt végezni?

E kérdésekre együtt kell koordinált választ adnia a tudományos kutatásnak, valamint minden, a területen érintett állami és magánintézmény szereplőjének. Amennyiben nem sikerül megfelelő válaszokat találnunk ezekre a kérdésekre, akkor potenciálisan számolnunk kell olyan cybertámadásokkal, amelyek kivédésére nagyon kevés lehetőségünk lesz.

FELHASZNÁLT IRODALOM

[1] Haig Zsolt – Várhegyi István: A cybertér és a cyberhadviselés értelmezése. Hadtudomány, 2008. elektronikus szám. ISSN 1215-4121

[2] Haig Zsolt – Kovács László – Ványa László: Az elektronikai hadviselés, a SIGINT és a cyberhadviselés kapcsolata. Kézirat, ZMNE, Budapest, 2011.

[3] Haig Zsolt – Várhegyi István: Hadviselés az információs hadszíntéren. Zrínyi Kiadó, Budapest, 2005.

[4] Dorothy E. Denning: Is Cyber Terror Next? http://essays.ssrc.org/sept11/essays/denning.htm

[5] http://news.softpedia.com/news/Al-Qaeda-Threatening-The-World-The-Virtual-One-72876.shtml

[6] Katz, Rita – Kern, Michael: Terrorist 007, Exposed. The Washington Post, 2006. március 26.

[7] http://index.hu/tech/jog/eszt250108

[8] Kovács László: Az információs terrorizmus elleni tevékenység kormányzati feladatai. Hadmérnök, III. Évfolyam 2. szám – 2008. június, ISSN 1788-1919

[9] Kovács László – Sipos Marianna: A Stuxnet és ami mögötte van: tények és a cyberháború hajnala. Hadmérnök, V. Évfolyam 4. szám – 2010. december, ISSN 1788-1919

[10] W. J. Broad, J. Markoff, D. E. Sanger: Israeli Test on Worm Called Crucial in Iran Nuclear Delay. New York Times, 2011. január 15. http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=1&scp=2& sq=stuxnet&st=cse

[11] Tremmel Flórián: Bizonyítékok a büntetőeljárásban. Dialóg Campus, Budapest–Pécs, 2006.

[12] Vayne Jansen – Rick Ayers: Guidelines on Cell Phone Forensics (NIST 800-101). National Institute of Standards and Technology, USA, 2007

[13] http://asert.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/

[14] http://index.hu/tech/net/eszt290507

[15] http://index.hu/tech/net/2009/03/12/ifjuoroszok_inditottak_az_orosz-eszt_kiberhaborut_/

[16] https://www.microsoft.com/industry/government/solutions/cofee/default.aspx

[17] http://www.crunchgear.com/2009/12/15/decaf-the-anti-microsoft-cofee-now-available/