PATAKI MÁRTA – KELEMEN ROLAND

TERRORIZMUS 2.0

ELŐSZÓ

„A civilizáció hajnalán az erő volt a legértékesebb és leghasznosabb tényező. Az erősebb győzött. Pár ezer évvel később a pénz vált a legfontosabbá – akinél a több pénz volt, az több mindent elérhetett. Mára a pénz elvesztette vezető szerepét – napjainkban az első és legértékesebb tényező, az információ. Aki birtokolja az információt, az nyert. És a hacker minden információhoz hozzáfér…"[1]

A terror főnév latinul ijedtséget, rémületet jelent. Bruce Schneier amerikai biztonsági szakértői is úgy véli, hogy *„[…] a terrorizmus valódi lényege nem maga a cselekmény, hanem az arra adott reakció."*[2] A terrorizmus, mint politikai, társadalmi jelenség végigkísérte az emberiség történelmét. A XIX. századig legtöbb esetben állami terrorról, királygyilkosságról beszélhetünk. A király gyilkosságok kiemelkedő példái III. és IV. Henrik francia királyok ellen elkövetett merényletek. III. Henriket, aki szövetkezett a protestánsokkal és börtönbe vetette a francia főpapság egy részét, egy paraszti sorból származó dominikánus szerzetes – a 23 éves Jacques Clement – hason szúrta egy, egy láb hosszú késsel (1589. augusztus 1.). IV. Henrikkel egy magányos megszállott, Francois Ravaillac végzett 1610. május 14-én. A merényletekre kitűnő példa a londoni parlament épültének felrobbantására irányuló kísérlet (1604). Guy Fawkes és társai a királyt és a walesi herceget, valamint a királyság politikai vezetőit, vagyis további félezer embert kívántak felrobbantani. A XIX. században az anarchizmus és a nacionalizmus voltak az ideológiai alapjai egy-egy terrorcselekménynek vagy terrorszervezetnek. Az anarchista mozgalmak áldozata lett Erzsébet osztrák császárné, magyar királyné Genfben 1898-ban, szintén anarchisták követtek el több merényletet II. Sándor orosz cár ellen is. A nacionalista mozgalmak közül a legismertebb az ír nacionalisták szabadságküzdelme a Brit Birodalom ellen, csoportjukat Ír Republikánus Körnek nevezték el.

1948. május 14-én David Ben-Gurion kikiáltotta Izrael állam függetlenségét, ezzel új irányt adva az addig ismert terrorizmusnak. Az arab államok Szent háborút (dzsihádot) hirdettek Izrael ellen, azonban az arab-izraeli háborúban (1948-1975) mindannyiszor Izrael győzött. A háborúk idején már jelentős terrorcselekményeket követtek el. Ezek közül kiemelendő az 1970. szeptember 6-án történt eset mikor palesztin terroristák három utasszállító repülőgépet térítettek el, ebből két gépet – egyet pedig az utasok leszállítását követően Kairóban felrobbantottak – utasokkal együtt Jordániába irányították majd bebörtönzött társaikra cserélték a túszokat. Ekkor merült fel először az a kérdés, hogy szabad-e tárgyalni terroristákkal. Erre a kérdésre az államok egyre inkább nemleges választ adtak.

Ezen eseményeket követően a terrorizmus a XX. század végére teljesen új formát öltött, egyfelől a „tradicionális" terrorizmus célja már csak a pusztítás lett, másfelől pedig a számítógép, az internet világméretű elterjedésével új típusú cselekmény a kiberterrorizmus is megjelent. Dennis C. Blair az Amerikai Egyesült Államok Nemzeti Hírszerzésének[3] igazgatója jelentésében hangsúlyozta, hogy *„a növekvő információs rendszerek közötti kapcsolat, az internet illetve egyéb infrastruktúrák lehetőséget teremtenek a támadóknak, hogy megzavarják a távközlési, villamos energia, a pénzügyi hálózatokat, finomítókat, valamint más létfontosságú hálózatokat."*[4] Véleménye szerint az ezeket ért kiber támadás hetekre képes megzavarni az állam működését. A hivatal becslése szerint a kiberbűnözés évente az USA-nak 42 milliárd, világszerte pedig 140 milliárd dollár kárt okoz. Az Európai Unió véleménye is azonos, legújabb irányelvében úgy fogalmaz, hogy

[1] BlueBird (magyar hacker) – KAZÁRI CSABA: *Hacker, cracker, warez. A számítógépes alvilág titkai*, 2003, Computer Panoráma, Budapest, 97. o.
[2] SCHNEIER BRUCE: *Schneier a biztonságról*, 2010, HVG Kiadó, Budapest, 14. o.
[3] 16 hírszerző tevékenységet végző szervezet munkáját kontrollálja. Többek között a CIA-t is.
[4] BLAIR C. DENNIS: *Annal Treat Assessment of the Intelligence Community for the Senate Select Committe on Intelligence (2009. február 12.)*, 38. o. http://archive.org/stream/AnnualThreatAssessmentOfTheIntelligenceCommunityForTheSenateSelect/20090212_testimony#page/n0/mode/2up (2013.09.30.).

„bizonyított az olyan, egyre veszélyesebb, ismétlődő és átfogó támadások előfordulása, amelyeket a tagállamok szempontjából, vagy a köz- és magánszféra bizonyos feladatai tekintetében gyakran kulcsfontossággal bíró információs rendszerek ellen intéznek."[5] Ezek okán úgy véljük a kiberterrorizmus a XXI. század potenciálisan egyik legveszélyesebb bűncselekménye. Tanulmányunkban bemutatjuk a kiberterrorizmusnak és eszközcselekményének jogi szabályozását, majd megkíséreljük csoportosítani az elkövetők körét, hiszen az általánosan használt hacker kategóriánál jóval árnyaltabb, hogy mely tudású és szándékú kiber szakember[6] képes megvalósítani ilyen cselekményt. A harmadik fejezetben a kiberterroristák által használt eszközöket kívánjuk ismertetni, az eszközök köre nem taxatív felsorolás mivel ezen terület gyorsan változik új eszközök jelennek meg és régiek válnak elavulttá, tehát ez az éppen aktuális állapotot tükrözi. A fejezetben próbáltunk megoldási lehetőséget vázolni ezen eszközök ártalmatlanítására. Munkánk során tételes jogi szabályokat (magyar és nemzetközi), és kiber szakemberek munkáit használtuk fel.

1. A TERRORIZMUS, KIBERTERRORIZMUS JOGI HÁTTERE

> *„A terrorizmus – vagy legalábbis annak végletekig sarkított változata – teljesen új és ijesztő arcot vett fel […] új típusú ellenféllel kerültünk szembe, amely folyamatosan bővíti instrumentumainak tárházát, megnehezítve ezzel az ellene folyó küzdelmet."*[7]

A terrorizmus, mint társadalmi jelenség az 1970-es években jelentősen felerősödött, állításunk igazolásaként kiemelnénk, hogy ebben az időszakban több mint kétszáz új terrorszervezet jött létre a világon, valamint – a nagyszámú terrorcselekmények közül – az 1972-es müncheni olimpián az izraeli delegációt ért támadást. Ennek okán nem meglepő, hogy a magyar büntetőjogban először az 1978. évi IV. törvény volt az, amely szabályozta a terrorcselekmény tényállását. Ez a tényállás *„… lényegében az emberrablás, illetve a zsarolás egy speciális esetéről rendelkezett, amikor a követelést állami szervhez vagy társadalmi szervezethez intézték és a követelés kikényszerítése a személyi szabadság korlátozása vagy jelentős anyagi javak hatalomba kerítése révén történt."*[8]

A század végére azonban a terrorcselekmények jelege teljesen megváltozott, fő motívuma a pusztítás lett. Eme jelenséggel szemben kívántak az államok egységes szabályozással fellépni, ezen szándékok nemzetközi egyezmények[9] formájában tárgyiasultak. Bartkó Róbert véleménye szerint ezen egyezmények által megalkotott meghatározások közös pontjai a következők:

„a.) a terrorizmus keretében megvalósított és az egyes egyezmények által részletesen is felsorolt bűncselekmények elkövetése valamennyi állam belső joga szerint békeidőben is büntetendő;

b.) az terrorizmus céljai között szerepel a lakosság megfélemlítése, valamint az állam vagy nemzetközi szervezet valamilyen magatartásra történő kényszerítése;

c.) a terrorista megnyilvánulások kivétel nélkül vagy politikai, vagy valamilyen ideológiai megfontolás által motiváltak."[10]

Az Európai Unió már a Maastrichti Szerződésben közös érdeknek jelölte meg a terrorizmus elleni együttes fellépést. Ezt erősítette meg az Európai Unió Tanácsa által 1995-ben elfogadott ún. *La Gomera nyilatkozat*, mely szerint *„[…] a demokrácia, az emberi jogok szabad gyakorlása, illetve a gazdasági-társadalmi fejlődés számára egyaránt fenyegetést jelentő terrorizmus tekintetében az Európai Unió egyetlen tagállama sem te-*

---

[5] Európai Parlament és Tanács 2013/40/EU irányelv az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról Preambulum (5) bekezdés.

[6] Szakember jelző nem véletlen mivel – mint ahogy az a későbbi csoportosításból is ki fog tűnni – tudásuk okán saját területük legképzettebb személyei képesek csak megvalósítani kiberterrorizmust, más kiberbűncselekményt már gyengébb tudású elkövető is véghez tud vinni.

[7] BARTKÓ RÓBERT: Gondolatok a terrorizmus fogalmáról, in *Belügyi szemle*, 2005/6. szám, 75. o

[8] BELOVICS ERVIN – MOLNÁR GÁBOR MIKLÓS – SINKU PÁL: *Büntetőjog II. – Különös rész,* 2012, HVGorac Lap- és Könyvkiadó, Budapest, 471. o.

[9] Arab Liga 1998. április 22-i egyezménye a terrorizmus visszaszorításáról; Afrikai Unió 1999. július 14-i egyezménye a terrorizmus megelőzéséről és a terrorizmus elleni küzdelemről; Iszlám Államok Konferenciája 1999. július 1-jei egyezménye a nemzetközi terrorizmus elleni küzdelemről; ENSZ-egyezmény a terrorizmus pénzügyi támogatásának visszaszorításáról 2000. február 25.

[10] BARTKÓ RÓBERT: A terrorcselekmény, mint nemzetközi bűncselekmény, in *Rendészeti Szemle,* 2010/5. szám, 79. o.

kinthető védettnek,"[11] és az ilyen transznacionális bűncselekményekkel szemben csak a közös fellépés lehet eredményes. Az Amszterdami Szerződés volt az, amely lehetővé tette, hogy *„… az eredményes fellépés érdekében megtegyék a szükséges intézkedéseket az Unió szervei a tagállamok büntetőjogi szabályainak harmonizálása érdekében."*[12]

A büntetőjogi szabályozás egységesítésére azonban csak az Amerikai Egyesült Államokat ért 2001-es terrortámadást követően került sor. Magyarország első körben a nemzeti jog részévé tette két nemzetközi egyezmény rendelkezéseit is: az 1997. december 15-én New York-ban elfogadott ENSZ Egyezményt a robbantásos terrorizmus visszaszorításáról a 2002. évi XXV. törvénnyel, és az 1999. december 9-én New Yorkban elfogadott ENSZ Egyezményt a terrorizmus finanszírozásának visszaszorításáról a 2002. évi LIX. törvénnyel. Ugyanezen évben az Európai Unió Tanácsa elfogadott egy kerethatározatot (2002/475/IB) a terrorizmus elleni küzdelemről, melyben többek között meghatározták az elkövetési módokat, a terrorista csoport fogalmát, valamint olyan szabályozási célokat is, hogy a terrorizmus finanszírozója, támogatója és a részesek cselekménye is büntetendő legyen.[13] A fent említett kerethatározatba foglaltakat a magyar jogalkotó a 2003. évi II. törvénnyel implementálta a magyar jogba, ezzel egy teljesen új terrorcselekmény tényállást megfogalmazva. A tényállás a kerethatározatba foglaltak átvételének köszönhetően jóval árnyaltabb és összetettebb lett, mely nagyban tükrözi a korábban bemutatott nemzetközi egyezményekben felvázolt metszéspontokat. A célcselekmények taxációjával *„[…] elkészült a köztörvényes bűncselekményeknek azon tételes listája, melyet a terroristák legitimnek hitt céljaik elérése érdekében elkövetnek. Dogmatikailag egy új típusú delictum complexum került ezzel megalkotásra, ahol az eszközcselekmény nem önmagában egy elkövetési magatartás, hanem egyenesen egy önálló bűncselekmény."*[14] A jogalkotó azonban a terrorizmus finanszírozására vonatkozó kriminalizációs kötelezettségének nem tett eleget, ezen hiányosságot csak a 2007. évi XXVII. törvénnyel orvosolta. Az új büntető törvénykönyv jelentős változásokat nem hozott a terrorizmus tényállásának szabályozásában. A jogalkotó annyi változást eszközölt csupán, hogy a terrorizmus finanszírozása önálló tényállás lett.

A kiberterrorizmus eszközcselekménye a 2003. II. törvény szerint a számítástechnikai rendszer és adatok elleni bűncselekmény volt. Ezen tényállás quasi elődje a számítógépes csalás 1994-ben került be a büntető törvénykönyvbe. Igényként merült fel azonban újabb számítógéppel elkövethető cselekmények pönalizálása, mint például a számítógépes adatok megszerzése. Az Európa Tanács 2001-ben Budapesten fogadta el az Informatikai bűnözésről szóló Egyezményt (Cybercrime Egyezmény), mely büntetőjogi rendelkezéseinek megfelelően a 2001. évi CXXI. törvénnyel a jogalkotó új tényállásokat alkotott meg. Ezen bűncselekmények voltak a számítástechnikai rendszer és adatok elleni bűncselekmény, valamint a számítástechnikai rendszer védelmét biztosító technikai intézkedés kijátszása.[15] A törvénymódosítás orvosolta a számítógépes rendszer fogalmának[16] büntető törvénykönyvi hiányát is.*„Az új tényállás – az új formában megjelenő számítógépes csalás mellett – büntetni rendelte a számítástechnikai rendszerbe történő jogosulatlan belépést, valamint a számítástechnikai rendszer és az abban tárolt, feldolgozott, kezelt vagy továbbított adatok sértetlensége elleni cselekményeket is."*[17]A Cybercrime Egyezményt csak a 2004. évi LXXIX. törvénnyel implementálta a jogalkotó. Fontos előrelépést jelentet a számítástechnikai adat fogalmi meghatározása. Majd a 2004-es év története, hogy az Európai Parlament és Tanács közös rendeletével[18] életre hívta az Európai Hálózat- és Információbiztonsági Ügynökséget, melynek feladatait általánosan a következők szerint fogalmazta meg a rendelet: *„hozzájáruljon a magas szintű hálózat- és információbiztonság megteremtéséhez a Közösségen belül, valamint, hogy kifejlessze a hálózat- és információbiztonság kultúráját az európai unióbeli polgárok, fogyasztók, vállalkozások és a közszektor szervezetei érdekében, elősegítve ezáltal a belső piac zavarta-*

[11] Európai Unió Tanácsa ún. La Gomera nyilatkozata a terrorizmusról. (Az 1995. december 15-16.)
[12] BARTKÓ RÓBERT: *A terrorizmus elleni küzdelem kriminálpolitikai kérdései,* 2011, Universitas-Győr, Győr, 142-143. o.
[13] Európai Unió Tanácsának 2002/475/IB kerethatározata a terrorizmus elleni küzdelemről (2002. június 13.) 1-6. cikk.
[14] BARTKÓ: i. m. (2011) 216. o
[15] 2001. évi CXXI. törvény a Büntető Törvénykönyvről szóló 1978. évi IV. törvény módosításáról 57-58. §.
[16] „Számítástechnikai rendszer az adatok automatikus feldolgozását, kezelését, tárolását, továbbítását biztosító berendezés vagy az egymással kapcsolatban lévő ilyen berendezések összessége"– 1978. évi IV. törvény a Büntető törvénykönyvről 300/F. §.
[17] BELOVICS ERVIN – MOLNÁR GÁBOR MIKLÓS – SINKU PÁL: *Büntetőjog – Különös rész,* 2009, HVGorac Lap- és Könyvkiadó, Budapest, 591. o.
[18] Európai Parlament és Tanács 460/2004/EK Rendelete az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról.

lan működését."[19] Feladatainak részletezéséből kiderül, hogy ezen Ügynökség jóval inkább tanácsadó, az együttműködést elősegítő és nem egy folyamatos védelmet biztosító szerv.

A tényállás fejlődésében előképet jelentett az Unió 2005/222/IB Kerethatározata, melyből jól kitűnt, hogy a kodifikáció jövőbeli iránya a számítógépes rendszerrel elkövetett csalás és számítástechnikai rendszer és adatok elleni bűncselekmény szétválasztása. Ennek magyarázata, hogy az utóbbi alá egyre több típusú elkövetési magatartás tartozhat, és ezek szükségessé teszik önálló tényállásként való szabályozását. Hiszen ekkor a tényállás még csak a számítógépes rendszerben tárolt adatokkal kapcsolatos tényállási elemeket tartalmazott, míg a kerethatározat már információs rendszerhez való jogsértő hozzáférést, a rendszerben való jogsértő beavatkozást is büntetendő cselekményként kezelte.[20] Meg kell jegyezni, hogy ezen tényállások tartalmilag megegyeznek a Cybercrime Egyezmény tényállásaival, mivel azonban a kerethatározat Uniós jogforrás, ezért ez kötelező minden tagállamra nézve, így jobban segítette az egységes fellépés lehetőségét. A két bűncselekmény különválasztása a 2012. évi C. törvényben, vagyis az új Büntető törvénykönyvben történt meg. A terrorizmus új kiber eszközcselekménye az információs rendszer vagy adat megsértése elnevezésű tényállást lett. Mely teljes egészében megfelel az Uniós szabályozási kritériumainak. Az Európai Unió és Tanács 2013 nyarán új irányelvet fogadott el – amely felváltotta 2005-ös kerethatározatot – amelyben az Unió újraszabályozta a kiberbűnözés típusait és azokhoz kapcsolódó tényállásokat. A magyar szabályozásban tényállási szinten biztosan változást eredményez a jogellenes adatszerzés kiberbűnözésként való megjelenése. Az irányelv kimondja, hogy *„… az információs rendszeren belülre, kívülre vagy azon belül továbbított, nem nyilvános számítógépes adatok – többek között az információs rendszerekből érkező, ilyen adatokat hordozó elektromágneses sugárzás – technikai eszközökkel történő, szándékos és jogosulatlan megszerzése, legalább a súlyosabb esetekben bűncselekménynek minősüljön."*[21] Az már a jogalkotó saját hatásköre, hogy új tényállást alkot vagy a 423. § részévé teszi, mint új elkövetési magatartást. Az irányelv kimondja még, hogy az ezen bűncselekmények elkövetési eszközeinek előállítóit, forgalomba hozóit szintén büntetni kell. A magyar jog ezt már a jelenlegi szabályozással is megteszi, így itt nincsen feladata a törvényhozásnak. Általánosságban elmondható, hogy az irányelv szabályai szigorodtak a kerethatározathoz képest, ami jól lemérhető az általa nyújtott szankciónálási lehetőségben. Mivel a 2005-ös kerethatározat a büntetés maximumaként 3 évet jelölte meg, addig a 2013-as irányelv már 5 évben maximál. Az irányelvből kitűnik az információs rendszerek fontossága, hiszen ezek, mint fogalmaz *„…a politikai, a társadalmi és a gazdasági interakció kulcstényezői az Unióban."*[22] Ezen infrastruktúrák védelme alapvető Uniós érdek és ezt a nemzeti büntetőjogi szabályoknak is tükrözniük kell. Úgy véljük, ez anyagi jogi területen meg is valósul Magyarországon.

Kiberterrorimusról szóló szabályozás keretében célszerű megemlíteni azt a 2013-ban elfogadott törvényt, amely Magyarország állami és önkormányzati szervei által használt információs rendszerek hatásosabb védelmét hivatott biztosítani. A törvény célként fogalmazza meg, hogy *„a nemzet érdekében kiemelten fontos – napjaink információs társadalmát érő fenyegetések miatt – a nemzeti vagyon részét képező nemzeti elektronikus adatvagyon, valamint az ezt kezelő információs rendszerek, illetve a létfontosságú információs rendszerek és rendszerelemek biztonsága."*[23] Ezzel a jogalkotó kifejezi elhivatottságát a kiberterrorizmussal szemben, a másik oldalról pedig láttatja, hogy ez valódi veszélyforrás bármely állam számára. A törvény felállította a Nemzeti Biztonsági Felügyeletet, melynek feladata sérülékenységi vizsgálatok elvégzése, és az észlelt hiányosságok kijavítása, információs rendszerek működésének ellenőrzése, támadás esetén azonnali intézkedést javasol (működés korlátozása, leállítása), tájékoztatót kérhet az adott szerv vezetőjétől, dolgozójától. Felügyeleti jogkörének gyakorlása során megbírságolhatja azon szervezet vezetőjét, aki írásbeli felszólítás ellenére nem teljesíti az abban meghatározottakat. A bírság 50 ezertől 5millió forintig terjedhet.[24] A hatóság jogköreit tekintve kibertámadás esetén valós hatáskörrel nem rendelkezik, hiszen a rendszer leállítása vagy a működés korlátozása csak felületi kezelés, a problémát nem orvosolja. Támadás esetén hatékonyan csak a Terrorelhárítási Központ tudna fellépni, azonban az ő lehetőségeik is korlátozottak, ezen lehetősége-

[19] Európai Parlament és Tanács 460/2004/EK Rendelete az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról. Preambulum (15) bekezdés.
[20] Európai Unió Tanácsának 2005/222/IB Kerethatározat az információs rendszerek elleni támadásokról 2-3. cikk.
[21] Európai Parlament és Tanács 2013/40/EU irányelv az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról 6. cikk.
[22] Európai Parlament és Tanács 2013/40/EU irányelv az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról (2) bekezdés.
[23] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról preambuluma.
[24] A Nemzeti Elektronikus Információbiztonsági Hatóság és az információbiztonsági felügyelő feladat- és hatásköréről, valamint a Nemzeti Biztonsági Felügyelet szakhatósági eljárásáról szóló 301/2013. (VII.29.) Korm. rendelet.

ket kellene kiszélesítenie a jogalkotónak. Ennek lehetőségeit kívánjuk bemutatni a következő fejezetekben egyfelől a potenciális elkövetői csoportok megjelölésével és az általuk használt eszközök ismertetésével, másfelől pedig olyan eszközök alkalmazásnak bemutatásával, amelyeket más országokban már jogszerűen alkalmazhatnak a terrorelhárító hatóságok.

2. KIBERBŰNÖZŐK

„A biztonság gyakran összefügg a technológiával, de mindig rólunk szól. A biztonság mindenekelőtt az emberek érdekében létezik, és bármilyen biztonsági törés hátterében is ők állnak."[25]

A számítógépek és az általuk működtetett információs rendszerek a modern társadalom és a modern állam alapköveivé váltak. Sem a hétköznapi ember élete, sem az állam szerveinek működése nem képzelhető el ma már információs rendszerek nélkül. Ilyen rendszerek üzemeltetik többek között az elektromos áramellátást, a tömegközlekedés egyes eszközeit, állami szinten az ingatlan-nyilvántartást, a társadalombiztosítást, továbbá számos katonai eszközt is. Azonban ezek a rendszerek, amelyek számos esetben összefogják, megkönnyítik a hétköznapokat számtalan kockázatot rejtenek, amelyeket a bűnözök egy speciálisan képzett rétege kíván kihasználni, őket nevezzük kiberbűnözőknek. A veszély valódiságát mutatja, hogy *„becslések szerint egy-egy érdekesebb szervert naponta 100-150 hacker próbál feltörni […]"*[26]. Ezen fejezetben a kiberbűnözők különböző típusait kívánjuk bemutatni, hiszen jelenleg több kategóriáját tudjuk elkülöníteni, attól függően, milyen szándék vezérli az adott bűnözőt illetve, hogy milyen tudással rendelkezik az adott egyén.

Az első ilyen típus a hacker: *„Az elnevezés az 50-es évekből származik, a MIT nagygépeket programozó végzős diákok és szakemberek kezdték magukra alkalmazni ezt a kifejezést, mégpedig azért, mert az akkori gépek korlátaival találkozva (nagyon kevés memória volt a számítógépekben akkoriban), megpróbálták minél kisebbre „összenyomni" a programokat és az operációs rendszereket, tehát belenyúltak a programokba, rendszerekbe, illetve átírták azokat."*[27] Mára ennek a fogalomnak a jelentéstartalma teljesen átalakult, a legkisebb mértékben sem egyeztethető össze a ma használt elnevezés az ötvenes évekbelivel, mivel a számítógépek térhódításával a kép jóval árnyaltabb lett, melynek köszönhetően már egy általános hacker definíció nem határozható meg. Tudásuk erősorrendjében a hackereket a következőképpen rangsorolhatjuk: (1) valódi hacker, (2) dark-hacker, (3) light-hacker, (4) wannabe-hacker, (5) drifter, (6) troll.[28]

A következőkben ezen a sorrendben kívánjuk bemutatni az egyes típusokat:

1) ***valódi hacker:*** *„olyan „kimagasló számítástechnikai tudással bíró személy", aki szigorúan segítő jelleggel […] feltárja a számítógépes rendszerek/alkalmazások előnyeit és hibáit, illetőleg javít azokon."*[29] A valódi hacker kiválóan ért a számítógépekhez, fontos számára az internet biztonsága, ebből következőleg ez a csoport ritkán követ el információs rendszer elleni bűncselekményeket, inkább rendszergazdaként dolgozik a biztonsági rendszerek hibáinak tesztelésével foglalkozó cégeknél vagy esetlegesen kormányhivataloknál.
2) ***dark-hacker:*** a számítástechnikai tudása jelentős, de őt a nyereségvágy vagy éppen a bosszú motiválja, megállapítható hogy mindenféleképpen valamilyen ártó szándékkal tevékenykedik. Az internetes vírusok legtöbbje e kategória képviselőitől származik. Gyakran valósítják meg a Btk. 375. §-a szerinti információs rendszer felhasználásával elkövetett csalás (5) bekezdésében meghatározott bűncselekményt.[30] A dark-hacker szakértelme és szándéka is megvan terrorcselekmény elkövetéséhez.

[25] SCHNEIER: i. m. 11. o
[26] FORREST DAVE: *Barát vagy ellenség? – A totális kontroll forgatókönyve,* 2005, Focus Kiadó, Budapest 202. o.
[27] KAZÁRI: i. m. 18. o.
[28] A valódi hacker és a dark-hacker között tudásbeli differencia nem fedezhető fel csak szándékbeli különbségről beszélhetünk.
[29] KAZÁRI: i. m. 18. o.
[30] Btk. 375. § (5) *„Az (1)-(4) bekezdés szerint büntetendő, aki hamis, hamisított vagy jogosulatlanul megszerzett elektronikus készpénz-helyettesítő fizetési eszköz felhasználásával vagy az ilyen eszközzel történő fizetés elfogadásával okoz kárt."*

3) ***light-hacker:*** számítástechnikai tudása jóval elmarad a valódi hackerétől, tudásukat gyakorolgatva keresik a hibás és támadható felületeket a világhálón. A hírnévre vágyakozva főleg *defacementeket*[31] követnek el, melyek a Btk. 423. § (1) bekezdés c) pontjába ütköznek.[32] Egyes vélemények szerint nem is tartoznak az igazi hackerek közé, ugyanis a hackerek nem követnek el bűncselekményeket, ők az internet biztonságáért dolgoznak, míg a „light-hackerek" honlapokat törnek fel. A hacker társadalom e csoportot *script-kiddiesnek* nevezte el.
4) ***wannabe-hacker:*** e kör tagjai még nem valódi hackerek, de arra törekednek, hogy azzá váljanak. Tudásuk jóval elmarad az előzőekéhez, ebből kifolyólag más hackerek által kitalált úgynevezett hack-programokkal, és exploitokkal[33] munkálkodnak, főként az információs rendszer vagy adat megsértése bűncselekményt követik el e kategória képviselői.
5) ***drifter:*** ők általában csak valamilyen információt vagy adatot keresnek az adott egyén gépén és ha megtalálják a keresett adatot lemásolják saját gépükre és tovább állnak. Az ő tevékenységük kiterjed a személyes adatokra, üzleti titkokra stb., ezért a drifter a tiltott adatszerzés bűncselekményének az (1) bekezdés d) pontjában meghatározott bűntettét követi el.[34] A gépen való jelenlétük legtöbbször észrevétlen, csupán csak néhány jel utalhat egy drifter jelenlétére számítógépünkön.
6) ***troll:*** *„A trollok előképzettség nélkül gyakorlatilag céltalanul ténferegnek a világhálón, és tönkretesznek minden elébük kerülő és támadható dolgot a neten."*[35] Ők a legfiatalabb „hacker" generáció, ezen csoport is előre mások által kitalált hack-programokkal dolgozik, de legtöbbször nem is nagyon tudják, mit is csinálnak. A próbálkozások sikerességétől és annak milyenségétől függ a büntetőjogi felelősségük megállapítása.

A kiber bűnözők második csoportját a *crackereket* a köznyelv sokszor összekeveri a hackerekkel, pedig két különböző fogalomról beszélhetünk, ezért elkülönülten kell őket elemezni. Az első és legfontosabb különbség köztük, hogy *„a cracker feltör, a hacker betör."*[36], azonban további különbségek is kimutathatók a két típus között, miszerint *„tapasztalatuk és szakértelmük az internet, az Unix vagy más több felhasználós rendszerek területén sem éri el a hackerekét."*[37] A cracker fogalmának *„[…] elsődleges jelentése szerint olyan kárt okozó személy, aki számítógépes rendszereket rongál, illetve adatokat tulajdonít el, vagy bármilyen egyéb módon kárt okoz."*[38] A cracker a saját gépén lévő anyaggal dolgozik, munkássága népszerű, mivel tevékenykedéseinek eredményei az olcsó kalózmásolatok. *„A cracker által okozott kár igazán csak a szoftvergyártóknak érdekes, tehát a kár inkább relatív jellegű […]"*[39]. A *crackerek* mindig ártó szándékkal törnek fel egy adott rendszert, szoftvert. *„Másodlagos jelentése szerint […] a cracker olyan valaki, aki megváltoztatja a kereskedelmi forgalomban lévő szoftverek kódját (ez már önmagában illegális tevékenység) annak érdekében, hogy a szóban forgó szoftver szabadon másolható, használható és terjeszthető legyen."*[40] A programfeltörés sokkal korábban létezett, a Commodor 64-es számítógépek magalkotásával párhuzamosan fejlődött, míg a mai értelemben vett *cracker* jelentése csak 1986-87-ben alakult ki. A *crackerek* igen összetartó közösség, amely nem csak *crackerekből* áll, hanem a velük együtt dolgozó olyan egyénekből, akik beszerzik az eredeti programokat, amelyek majd a *cracker* által feltörésre kerülnek, illetve a már feltört program ter-

[31] Defacement: honlapok feltörése és megváltoztatása. *„Hacker nyelven egy adott weboldal/weboldalak kicserélését jelenti, ezáltal „szégyenítve" meg az adott oldalt üzemeltető céget, magánszemélyt. A deface egyfajta üzenőfelület is: a hackerek egyik kommunikációs csatornája; a megváltoztatott oldalakon adnak hangot véleményüknek, nemtetszésüknek."* – KAZÁRI: i. m. 154. o.

[32] Btk. 423. § (1) *c*):*" információs rendszerben lévő adatot jogosulatlanul vagy jogosultsága kereteit megsértve megváltoztat, töröl vagy hozzáférhetetlenné tesz vétség miatt két évig terjedő szabadságvesztéssel büntetendő."*

[33] Exploit: védelmi hibát, biztonsági rést, illetve ezek kihasználását jelenti, kiválóan használhatók honlap feltörésekre.

[34] Btk. 422. §(1) *„Aki személyes adat, magántitok, gazdasági titok vagy üzleti titok jogosulatlan megismerése céljából, d) elektronikus hírközlő hálózat – ideértve az információs rendszert is – útján másnak továbbított vagy azon tárolt adatot kifürkész, és az észlelteket technikai eszközzel rögzíti, bűntett miatt három évig terjedő szabadságvesztéssel büntetendő."*

[35] FORREST: i. m. 205. o.

[36] Uo. 206. o.

[37] RAYMOND ERIC S.: *The new hacker's dictionary,* 1996, MIT Press, Cambridge, 22. o.

[38] KAZÁRI: i. m. 19. o.

[39] FORREST: i. m. 206. o.

[40] KAZÁRI: i. m. 19. o.

jesztői is e csoport tagjainak minősülnek. Maga a *cracker* a védelmet biztosító műszaki intézkedés kijátszása vétségét követi el, amely az *„aki a szerzői jogról szóló törvényben meghatározott hatásos műszaki intézkedést*[41] *haszonszerzés végett megkerüli”*[42] került meghatározásra.

A következő típusa a kiber bűnözőknek a *phreaker*: a „*phonephreaker*” kifejezésből ered. *„A phreaker-ek a telekommunikáció szakértői, „átprogramoznak” távközlési berendezéseket, ingyen mobiloznak és interneteznek (vonalat „lopnak”), értenek a lehallgatáshoz, és mindenféle mobiltelefont képesek kikódolni, átprogramozni, titkosítani stb.”*[43]. Magyarországon ez a tevékenység még kialakulóban van. A telekommunikációs hálózat átprogramozásához tökéletes 2600 Hz-es hang kiadására van szükség, mely az úgynevezett in-band jelzés, mellyel elérhető az ingyen távolsági hívás, ugyanis a gép az in-band jelzés hatására kezdeményezi a hívást. Ma ennek a hangnak az előállítására a blue box szerkezetet használják.

Ezen csoportosítás utolsó típusa a HPAV: mely a *Hacking, Phreaking, Anarchy, Virus* szavakból tevődik össze. *„A HAPV csapatok a létező legkártékonyabbak – vírusokat írnak, állami szervek munkáját teszik tönkre, magánszámítógépekbe törnek be, mindezt csak azért, hogy másoknak gondot okozzanak.”*[44] Ilyen csoportosulás jelenleg Európa területén gyakorlatilag alig létezik. Magyarországon egy ilyen ismert csapat található a Lukundo-féle HPAV. *„A HPAV scene tagjai a szó szoros értelmében vett számítógépes bűnözők […]. Legismertebb képviselőik a vírusokat író programozók és csapatok.”*[45] Egy HPAV tevékenykedése során bármely információs rendszer elleni bűncselekményt képes elkövetni. Sőt olykor még a terrorcselekmények elkövetésétől sem riadnak vissza.

Összegezve tehát a témánk szerinti terrorcselekmény tényállás elkövetéséhez három típusú szakember rendelkezik megfelelő tudással. A valódi hacker bár szakértelme megvan hozzá, de szándéka nincs ilyen bűncselekmények megvalósítására, azonban véleményünk szerint potenciális elkövetők a dark-hackerek illetve a HPAV-k lehetnek. Szakmai tudásuk és tapasztalataik alapján kijelenthető, bármilyen információs rendszerre valós veszélyt jelentenek.

3. A KIBERTERRORIZMUS ESZKÖZEI, MÓDSZEREI, ELLENÜK VALÓ VÉDEKEZÉSI TECHNIKÁK

> *„A sikeres támadás mindig a meglepetés erejével hat. Ha tudnánk, mikor jön, mely rendszerek válnak célpontjává, hogyan indul, mekkora lesz a veszteség, minden bizonnyal képesek lennénk megelőzni.”*[46]

Az alábbiakban tárgyalandó fejezet célja, hogy bemutassa a kiberterrorizmus eszközeit és az azokra vonatkozó esetleges védekezési technikákat, illetve részletes képet kíván adni, arról hogy a kiberbűnözők milyen módszerekkel követhetik el a terrorcselekmény tényállásába eső, az információs rendszer vagy adat megsértésével megvalósított elkövetési magatartásokat. Itt kell megjegyezni, hogy az elkövető szándékától függ milyen információs rendszerbe tör be, milyen adatot szerezz meg és azt milyen módon használja fel, melynek egyik felhasználási módozata a terrorcselekmény elkövetése.

Az első támadási módszer, mellyel a hacker betörhet egy információs rendszerbe a helyi hálózatok ellen irányuló veszélyek csoportjába sorolható. Az Ethernet- és a Token Ring helyi hálózat elleni támadás: az Ethernet egy üzenetszórásos helyi hálózat, melynek lényege, hogy *„ha az ügyfél állomás a kiszolgálótól adatot kér, adatcsomagot állít össze, amelyhez hozzácsatolja a megfelelő fejlécet, megcímzi a kiszolgálónak, majd útjára indítja a vonalon, ahol eljut a címzetthez.”*[47] A más állomásnak szánt adatcsomagot tovább engedi, fontos itt megemlíteni, hogy az állomások csak a csomag fejlécét olvassák és abból észlelik, hogy a csomagot nekik címezték-e, ezt a technikát alkalmazza a Token Ring vezérjelgyűrűs hálózat is. Mindkét

[41] 1999. évi LXXVI. törvény a szerzői jogról 95. § (3) :*„műszaki intézkedés minden olyan eszköz, alkatrész vagy technológiai eljárás, illetve módszer, amely arra szolgál, hogy a szerzői jog jogosultja által nem engedélyezett cselekményeket – rendeltetésszerű működése révén – megelőzze, illetve megakadályozza. A műszaki intézkedést akkor kell hatásosnak tekinteni, ha a mű felhasználását a jogosultak a hozzáférést ellenőrző vagy védelmet nyújtó olyan eljárás – különösen kódolás vagy a mű egyéb átalakítása, vagy másolatkészítést ellenőrző mechanizmus – útján ellenőrzik, amely alkalmas a védelem céljának elérésére.”*

[42] Btk. 386. § (1)

[43] KAZÁRI: i. m. 20. o.

[44] Uo. 21. o.

[45] Uo. 21. o.

[46] CRUME JEFF: *Az internetes biztonság belülről- ...amit a hekkerek titkolnak,* 2003, Szak Kiadó, Bicske, 74. o.

[47] Uo. 138.

technológia esetén a hacker[48] a hálózatba hatolva az állomásokat promiszkuitív módba kapcsolva képes megszerezni az összes adatcsomagot. A Lan-csatoló ugyanis promiszkuitív módban nem csak az adatcsomag fejléce alapján rá vonatkozó adatcsomagokat menti le, hanem egy mappában rendszerezve az összes a helyi hálózat által továbbított üzenetet. Ezzel ideális körülményeket teremtve a hackernek, hogy a tiltott adatszerzés bűncselekményét elkövesse, amely a Btk. 422.§ (1) bekezdés d) pontjába ütközik,[49] illetve az információs rendszer vagy adat megsértése tényállás a pontjában meghatározott elkövetési magatartását tanúsítsa. Egy ilyen támadás esetében a hálózat összes adatcsomagjának birtokában a terrorcselekmény információs rendszer vagy adat megsértésével bűncselekmény elkövetését is megalapozhatja, melynél jelentősége van annak, hogy az információs rendszer vagy adat megsértése bűncselekmény alap, illetve minősített esetét valósítja meg az elkövető. A hacker jelen esetben a hálózatba való betöréshez ugyanazt a követőprogramot (*sniffert*) használja, amelyet a teljes helyi hálózat megfigyelésére alkalmaznak a hálózati szakemberek. A támadás ellen kifejlesztettek egy *AntiSniff* elnevezésű programot. *„Az AntiSniff különböző szaglászótechnikákat ötvöz egy programban, és így teszteli a gyanítottan promiszkuitív módban futó rendszereket.”*[50]

Jelszavak feltörése: a jelszavak kinyeréséhez és feltöréséhez a leghatékonyabb eszköz *„a L0phtCrack hálózatfigyelő program beépített Server Message Block (kiszolgáló-üzenetblokkoló) csomag elfogó funkciója, amely megfigyel a helyi hálózaton átmenő minden csomagot, a kiszolgálóra történő belépési információt tartalmazó csomagokról másolatot készít, a többit pedig törli.”*[51] Ezzel a programmal a hacker listát kap a felhasználói azonosítókhoz tartozó titkosított jelszavakról, melyeket a hálózat figyelő programmal egyúttal fel is tud törni. A jelszavak feltörésére további módszerek is alkalmazhatók, ilyen például a *Social Engineering*. *„A social enginering a befolyásolás és rábeszélés eszközével megtéveszti az embereket, manipulálja vagy meggyőzi őket, hogy a social engineer tényleg az, akinek mondja magát. Ennek eredményeként a social engineer – technológia használatával vagy anélkül – képes az embereket információszerzés érdekében kihasználni.”*[52] Tehát a *social engineer* (azaz a hacker) miután megszerezte tőlünk a legfontosabb személyes adatainkat egy kódfeltörő programba beírva azokat könnyedén megszerezheti titkos jelszavainkat. Mivel megfelelően akarunk védekezni egy ilyen támadás ellen, fontos, hogy véletlenszerű jelszót válasszunk, mely véletlenül sem kapcsolódik hozzánk. *„[…] Ha azt akarjuk, hogy nehéz legyen feltörni a jelszavainkat (nem lehetetlen, mivel mindent fel lehet törni – de legalább ne legyen egyszerű…), akkor válasszunk valami teljesen eszement, „véletlenszerű” kódsort, variálva a kis- és nagybetűket és számokat”*[53] Továbbá figyeljünk oda arra, hogy ne értelmes szót válasszunk, mert az úgynevezett *Dictionary Hack* eljárás azon alapul, hogy értelmes szavak variációit próbálgatja a kódfeltörés közben. Amennyiben nem értelmes szót választottunk, a hacker csak a *Brute Force* eljárással[54] járhat sikerrel jelszavunk megfejtésében. A jelszó feltörés esetében a Btk. 423.§ (1) bekezdésének a pontban meghatározott az információs rendszer vagy adat megsértése bűncselekmény alapesetét követi el a hacker, mely a jelszóval védett információs rendszer fontosabb tulajdonságai határozzák meg, hogy alkalmas-e a terrorcselekmény megfelelő fordulatának elkövetéséhez.

Szintén e fejezetben kell szólnunk a puffertúlcsordításos támadásról: *„A hekker egyszerűen több adatot küld, mint amennyit a vevő vár, és ha a vevő rendszere nem végez elegendő hibaellenőrzést, váratlan helyzet állhat elő. Néhány esetben a vevő programja egyszerűen összeomlik. Más esetekben a jogosult felhasználók nem tudják elérni a rendszert.”*[55] Ezeket a támadásokat könnyű észrevenni és nem is nehéz védekezni ellenük, csak egy biztonsági frissítésre van szükségünk. Véleményünk szerint könnyű felfedezhetősége miatt ugyan elkövethető a terrorcselekmény, de rövid ideje miatt nem célszerű. Így jobbára az információs rendszer vagy adat megsértése bűncselekmény alap esetének a), b) és c) pontjában foglaltak kerülhetnek megvalósításra.

---

[48] E fejezetben összefoglalóan a hacker fogalma alatt a dark-hackert és HPAV-t kell érteni.

[49] Btk.422. § (1) Aki személyes adat, magántitok, gazdasági titok vagy üzleti titok jogosulatlan megismerése céljából … *d)* elektronikus hírközlő hálózat – ideértve az információs rendszert is – útján másnak továbbított vagy azon tárolt adatot kifürkész, és az észlelteket technikai eszközzel rögzíti, bűntett miatt három évig terjedő szabadságvesztéssel büntetendő.

[50] CRUME: i. m. 142. o.

[51] Uo. 140. o.

[52] MITNICK, D. KEVIN – WILLIAM, SIMON L.: *A biztonság emberi tényezőinek irányítása, A legendás hacker – A megtévesztés művészete*, 2003, Perfact – Pro, Budapest, 1. o.

[53] KAZÁRI: i. m. 61. o.

[54] Brute Force eljárás: *„Ennek a lényege, hogy a kódtörő program minden variációt kipróbál – de ez nagyon időigényes, és a jelszavak tekintetében nem is az a cél, hogy ne lehessen feltörni, hanem, hogy sokáig tartson!” – Kazári*: i. m. 61. o.

[55] CRUME: i. m. 153. o.

DoS támadások: e támadások egyfajta szolgálatmegtagadásos támadások. *„ A DoS- támadó nem fér hozzá fontos rendszerhez, nem lop el bizalmas információkat […]”*,[56] hanem valós vagy vélt sérelmének hangot adva rongálja meg az adott webhelyet. A támadás eredménye, hogy a rendszer megtagadja a felhasználóktól a hozzáférést a különböző szolgáltatásokhoz, amelyekre egyébként jogosultak lennének. Tehát a kritikus erőforrás lefoglalásával gátolja a webhely tevékenységét. Álláspontunk szerint a hírközlési hálózat ellen indított DoS támadás indokolttá teheti a terrorcselekmény elkövetése miatti felelősségre vonást.

A *Back Orifice* (hátsó nyílás) támadás: a hacker a *back orifice* nevű rosszindulatú programot az elnevezéséből is adódóan a „hátsó ajtón” juttatja be az információs rendszerbe, melyet egy jóindulatú programba rejtve juttat el a felhasználóhoz, amit gyanútlanul feltelepít a gépére abban a hiszemben, hogy valamilyen hasznos, jóindulatú programot telepít. A telepítés után a rosszindulatú program létezésének minden látható jele eltűnik, közben a hacker teljes mértékben átveheti és távolról irányíthatja a számítógépet. Ebben az esetben a terrorcselekmény elkövetése teljes mértékben megvalósítható és a támadás azon tulajdonsága, miszerint a feltelepítés után a program létezésének látható nyomait eltűnteti, nagyon hatékony a kiberterrorizmus területén. Sőt, ha a hálózathoz mikrofon és videokamera is van csatlakoztatva, a hacker az eszközök bekapcsolásával figyelheti meg a felhasználót.

A levél bomba támadás: a támadó e-mailek sokasságát küldi el egy program segítségével a felhasználónak, mellyel túlterheli a levelezőrendszert, mert rákényszeríti, hogy az összes tárhelyet felhasználja a nem fontos adatok, üzenetek tárolására, így a fontos üzenetek nem tudnak bejutni. A támadás elkerülésére a levelezőrendszert úgy kell beállítani, hogy felismerje a levél bombát és azonnal szüntesse meg a kezdeményező fiókot. Az olvasottak alapján kijelenthetjük, hogy a levél bomba támadás nem lehet eredményes terrorcselekmény elkövetése esetén.

A Vírus támadás: *„a számítógépes vírus olyan program, amely a futtatáskor lemásolja magát(vagy egy részét). Kapcsolódhat a felhasználó merevlemezén lévő más futtatható állományokhoz, de akár az indítórekordhoz is, amely a számítógép indításakor betölti az operációs rendszert.”*[57] A lassabb lefolyású vírusok óriási területet fertőzhetnek meg, nem úgy, mint a gyorsabb lefolyású társaik, mert a gyors lefolyás miatt a gazdagép hamar megsemmisül. *„A vírusnak valamihez hozzá kell kapcsolódnia, egy programhoz, egy dokumentumhoz vagy a merevlemez boot szektorához.”*[58]A terrorcselekmény elkövetéséhez az egyik legideálisabb módszer, mivel a lassabb lefolyású vírus esetén fokozatosan nagy kárt lehet elérni vele, míg a gyorsabb lefolyású vírus esetén elemi csapás mérhető az adott információs rendszerre, amellyel könnyedén kényszerítheti a hacker az államot vagy a nemzetközi szervezetet. [423. § (1)-(4) eszközcselekménnyel elkövetett 314.§ (1) a)].

A trójai faló támadást a vírusok után kell megemlítenünk, mivel technikailag nem vírus ugyan, de hasonló károkat okoz az információs rendszerben. A vírustól való megkülönböztetést viszont az indokolja, hogy a trójai falovak nem feltétlenül másolják le önmagukat, mégis rosszindulatú programok, melyek hatalmas károkat tudnak okozni. Az információs rendszerbe jóindulatú programba rejtve kerülhetnek be. *„A trójai faló a felszínen hasznos, sőt mi több, szórakoztató funkciókat mutat, így teljesen ártalmatlannak tűnhet – pedig valójában a velejéig romlott.”*[59] A vírusokhoz való hasonlósága miatt, úgy véljük, a második legideálisabb módszer lehet a trójai faló a kiberterrorizmus eszköztárában a terrorcselekmény információs rendszer vagy adat megsértésével bűncselekmény elkövetéséhez.

A számítógépféreg: a féregnek a vírushoz hasonlóan nem kell valamihez kapcsolódnia, egymaga egy kész, egész program. A férget törléssel el lehet távolítani a számítógépről. *„ A számítógépféreg olyan szoftverparazita, amely tulajdonképpen mindent felfal, ami az útjába kerül. Időről időre újra meg újra lemásolja magát, ezáltal a folyamat során felemésztheti a memóriát, a lemezterületet, vagy a sávszélességet.”*[60] A terrorcselekmény harmadik legideálisabb elkövetési módszere, hiszen egy gyorsan ható féreg jelentős kárt tud okozni az információs rendszerben, melynek kényszerítő hatása is legalább ilyen jelentős lehet.

A zombihálózatokat, azaz boot hálózatokat azért kell itt megemlíteni, mert ezen hálózatok számítógépek sokasságát foglalhatják magukba, melyek segítségével nagyobb támadásokat lehet indítani. A zombihálózatba kapcsolt gépeket valaki más távolról irányítja. Többnyire személyes adatok, illetve titkos információk lopásához használják, de használható gyorsan terjedő férgek szétküldésre is, mely megbéníthatja

[56] CRUME: i. m. 174. o.
[57] Uo. 188. o.
[58] WARREN, PETER – STREETER, MICHAEL: *Az internet sötét oldala – Vírusírók, adatrablók, hackerek – és amit tehetünk ellenük, 2005,* HVG kiadó, Budapest 137. o.
[59] CRUME: i. m. 189. o.
[60] Uo. 189. o.

az adott információs rendszert. A boot hálózatok kiválóan alkalmasak terrorcselekmények elkövetésére, hiszen csak egy ártó szándékú nagy tudású hacker és annak zombihálózata szükséges hozzá. A zombihálózat adathalász támadása ellen a leghatékonyabban úgy védekezhetünk, ha a kommunikációnkat titkosítjuk a kriptográfia segítségével. A titkosításhoz egy titkosító algoritmusra van szükségünk, mely véletlenszerű kulcsot generál, amelyet hackerünk nem tud visszafejteni. Az így kapott kulcsot célszerű nem a számítógép merevlemezén tárolni, mert ehhez a hacker könnyen hozzá férhet, hanem inkább intelligens kártyán helyezzük el, amelynek tartalmát PIN-kóddal védjük. *„Minél hosszabb a kulcs, annál nagyobb az adott üzenet lehetséges rejtjeles változatainak száma. Az 1 bit hosszú kulcs esetében csak 2 lehetőség áll fenn."*[61] Ahogy növeljük a bitek számát, a lehetőségek úgy növekednek a 2^n képlet szerint, melyben az „n" a kulcs bitben számított hossza, tehát 3 bitnél már 8 lehetőségről beszélhetünk. Sajnos a titkosított kommunikációt nem csak a magánszemélyek, esetlegesen a köztisztviselők használják, hanem a kiberterroristák is gyakran élnek ezzel a módszerrel kommunikációjuk során. Így az esetleges kibertámadások elkerülése végett egyes államok (úgy, mint Amerikai Egyesült Államok vagy Nagy-Britannia) azon a véleményen vannak, hogy a magánszemélyek személyes adatok védelméhez való joga korlátozható, hiszen az állam és a köz érdekében figyelik meg a magánszemélyek titkosított üzenet váltásait is, ugyanis például az FBI által kifejlesztett üzenet megfigyelő program egyelőre nem képes hitelt érdemlően elkülöníteni a privát, magán titok körébe eső üzeneteket a kiberterroristák kommunikációjától. Az FBI által alkalmazott Carnivore-program az *„IP adatforgalom hasznos adatait elemzi […]"*[62] A programot egy megfigyelő rendszerrel egészítik ki, mely a *Cyber Knight* fedőnevet kapta. Ennek a megfigyelő rendszernek a fő feladata, hogy az *„e-maileket, a megfigyelt chatszobák logjait, üzenetküldő programok szóváltásait rögzítse, rendszerezze és tárolja"*,[63] majd a *Magic Lantern* elnevezésű program segítségével, – mely egy keyloger és trójai faló kombinációja – elemzi a titkosítást és feltöri az adott titkosított üzenetet. Nagy-Britanniában 2002-ig a nyomozati jogkörökről szóló törvény (*Regulation of Investigatory Powers Act*) hasonló módon szabályozta az Egyesült Államokéhoz, miszerint átnézhették bárki elektronikus levelezését, de a titkosított üzeneteket nem törhették fel, majd 2002-ben a szabályozás akképp változott, hogy azon személyek, akik kriptográfiai programokat használnak a kommunikációjuk során kötelesek a titkosító kulcsot átadni a hatóságoknak. A titkosító kulcs át nem adása súlyos jogkövetkezményeket von maga után, a felhasználó jogtalanul használja az adott programot, amelynek börtönbüntetés a szankciója.

Összegezve tehát véleményünk szerint a kiberterroristák számtalan, a felsoroltakon kívül, talán még nem is ismert újabb és újabb eszközökkel és módszerrel képesek terrorcselekményeket elkövetni, ezért fontos egy államnak felkészülni egy ilyen támadás ellen, akár a személyes adatok védelméhez való jog szükséges mértékű korlátozásával és a magánszemélyek kommunikációjának megfigyelésével. A kibertámadások elleni védekezési rendszer megfelelő szintre emelése jelentős stratégiai lépés lehet, hiszen egy ártó szándékú hacker bármilyen rendszerbe képes betörni, csak az nem mindegy milyen gyorsan és nekünk mennyi időnk van erre reagálni.

ZÁRÓ GONDOLATOK

A XX. század végére az internet révén az egyes információs rendszerek globális hálót alkotnak. Ezen hálózat részét képezik a civil személyeken és gazdasági társaságokon túl az államok létfontosságú rendszerei is. Az 1990-es évek végére a terrorizmus új arcát mutatta – azon túl, hogy a „tradicionális" terrorizmus célja már csak a rombolás – azon számítógépes szakemberek révén, akiket ma már kiberterrorista elnevezéssel illetünk. A számítógépek fejlődésével egy ütemben nő azon szakemberek száma, akik képesek az állam alapvető rendszereiben a kiber téren keresztül kárt tenni. A köznyelv ezen elkövetőket *hackereknek* hívja. Hibásan, hiszen ezen elnevezés igen tág kategória, magába foglalja a valódi hackert, a *dark-hackert,* a *light-hackert,* a *wannabe hackert* és így tovább. Ezen személyek szakmai tudása és szándéka között igen jelentős eltérések vannak. Kiberterrorizmus elkövetésére a valódi és a *dark-hacker* képes. A valódi hackernek viszont nincs szándékában ilyen cselekmény elkövetése, sőt célja annak megakadályozása. A *dark-hacker* az, akinek szándéka és tudása is megvan ilyen cselekmények elkövetéséhez, ezen személyeken túl még a HPAV csoportja képes ilyen „akciók" végrehajtására.

A XXI. század első évtizedének elejére már a jogalkotó számára is világossá vált, hogy a fent említett személyek cselekménye ellen fel kell lépni. Az Európa Tanács 2001-ben Budapesten fogadta el a

[61] CRUME: i. m. 219. o.
[62] FORREST: i. m. 178. o.
[63] Uo. 179. o.

Cybercrime Egyezményét, amely az elfogadó országok számára kötelezővé tette egyes cselekmények kriminalizálását. Az Európai Unió közös fellépést sürgette, ennek eredményeként 2004-ben felállították a Hálózat- és Információbiztonsági Ügynökséget. A 2005-ös kerethatározattal pedig meghatározták azon cselekmények körét, amelyet a nemzeti jogban pönalizálni kell. 2013-ban irányelvet fogadtak el, amely a 2005-ös kerethatározathoz képest szigorítaná a kiberbűnözökkel szembeni szankciókat, továbbá figyelmeztet arra, hogy óriási veszélyforrást jelentenek ezek a támadások az Európai Unióra nézve. A magyar szabályozás mindvégig követte az Unió irányvonalát, véleményünk szerint az anyagi jogi szabályozás megfelelő, a lehető legteljesebben lefedi a kiberbűnözés egyes cselekményeit.

A 2013-ban elfogadott új, az állami és önkormányzati szervek információ biztonságát szabályozó törvény előrelépést mutat, követve a nemzetközi szabályozást[64] felállítja a Nemzeti Biztonsági Felügyeletet, amelynek feladata többek között a megelőzés, a szükséges védelem kiépítése, ennek ellenőrzése és utasítási lehetőség támadás esetére, azonban a magyar szabályozás nem biztosít lehetőséget arra, hogy támadás közben aktív védekezést tanúsítson bármely magyar szervezet. Álláspontunk szerint a szabályozást úgy kellene alakítani, hogy a TEK vagy a Felügyelet támadás esetén viszonttámadást indíthasson a támadó rendszer ellen. Az Egyesült Államokban e tervezetet elvetette a Szenátus – bár ott a filmgyártók szövetsége kérte ezt – arra hivatkozva, hogy ez sérti az ártatlanság vélelmét. Véleményünk szerint a támadás pillanatát úgy kellene kezelni, mintha jogos védelmi helyzetről lenne szó, ahol a támadó ártalmatlanná tétele megengedett. Tipikusan alkalmas eszköz lenne erre a szolgáltatás megtagadásos támadás és túlterheléses támadás, amely kárt nem okozna, de alkalmas arra, hogy a támadó rendszer ne férjen hozzá a hálózathoz, ezzel meghiúsítva annak eredményességét. Az internetes levelezés megfigyelése kulcsszavas kereséssel szintén gátat szabhat az egyes támadások lehetőségét, viszont a megfigyelést nehezíti a kriptográfiai programok használata. Ezen nehézségek leküzdésére nyújt mintát az angol *Regulation of Investigatory Powers Act*, mely kimondja, aki ilyen programot használ, az köteles annak kulcsát átadni az illetékes hatóságnak, amennyiben ezt nem teszi meg szabadságvesztéssel is büntethető.

Véleményünk szerint e két lehetőség sok esetben megkönnyítené a hatóságok feladatát a támadás megelőzése és megakadályozása területén.

FORRÁSJEGYZÉK

[1.] BARTKÓ RÓBERT: A terrorcselekmény, mint nemzetközi bűncselekmény, in *Rendészeti Szemle,* 2010/5. szám, 73-87. o.

[2.] BARTKÓ RÓBERT: Gondolatok a terrorizmus fogalmáról, in *Belügyi szemle,* 2005/6. szám, 75-89. o.

[3.] BARTKÓ RÓBERT: *A terrorizmus elleni küzdelem kriminálpolitikai kérdései,* 2011, Universitas-Győr, Győr.

[4.] BELOVICS ERVIN – MOLNÁR GÁBOR MIKLÓS – SINKU PÁL: *Büntetőjog – Különös rész,* 2009, HVGorac Lap- és Könyvkiadó, Budapest.

[5.] BELOVICS ERVIN – MOLNÁR GÁBOR MIKLÓS – SINKU PÁL: *Büntetőjog II. – Különös rész,* 2012, HVGorac Lap- és Könyvkiadó, Budapest.

[6.] BLAIR, C. DENNIS: *Annal Treat Assessment of the Intelligence Community for the Senate Select Committe on Intelligence (2009. február 12.)* http://archive.org/stream/AnnualThreatAssessmentOfTheIntelligenceCommunityForTheSenateSelect/20090212_testimony#page/n0/mode/2up (2013.09.30.).

[7.] CRUME, JEFF: *Az internetes biztonság belülről- …amit a hekkerek titkolnak,* 2003, Szak Kiadó, Bicske.

[8.] FORREST, DAVE: *Barát vagy ellenség? – A totális kontroll forgatókönyve,* 2005, Focus Kiadó, Budapest.

[9.] KAZÁRI CSABA: *Hacker, cracker, warez. A számítógépes alvilág titkai*, 2003, Computer Panoráma, Budapest.

[10.] MITNICK, D. KEVIN – WILLIAM, SIMON L.: *A biztonság emberi tényezőinek irányítása, A legendás hacker – A megtévesztés művészete,* 2003, Perfact – Pro, Budapest.

[64] Például: EU fent ismertetett Ügynöksége, USA Comprehensive National Cybersecurity Initiative, India Indian Computer Emergency Response Team.

[11.] RAYMOND ERIC S.: *The new hacker's dictionary,* 1996, MIT Press, Cambridge.
[12.] SCHNEIER, BRUCE: *Schneier a biztonságról,* 2010, HVG Kiadó, Budapest.
[13.] WARREN, PETER – STREETER, MICHAEL: *Az internet sötét oldala – Vírusírók, adatrablók, hackerek – és amit tehetünk ellenük,* 2005, HVG kiadó, Budapest.

Jogforrások:

[1.] A Büntető Törvénykönyvről szóló 1978. évi IV. törvény.
[2.] A szerzői jogról szóló 1999. évi LXXVI. törvény.
[3.] A Büntető Törvénykönyvről szóló 1978. évi IV. törvény módosításáról szóló 2001. évi CXXI. törvény.
[4.] A Büntető Törvénykönyvről szóló 2012. C. törvény.
[5.] Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény.
[6.] A Nemzeti Elektronikus Információbiztonsági Hatóság és az információbiztonsági felügyelő feladat- és hatásköréről, valamint a Nemzeti Biztonsági Felügyelet szakhatósági eljárásáról szóló 301/2013. (VII.29.) Korm. rendelet.
[7.] Európai Parlament és Tanács 2013/40/EU irányelv az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról.
[8.] Európai Parlament és Tanács 460/2004/EK Rendelete az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról.
[9.] Európai Unió Tanácsának 2002/475/IB kerethatározata a terrorizmus elleni küzdelemről (2002. június 13.)
[10.] Európai Unió Tanácsának 2005/222/IB Kerethatározat az információs rendszerek elleni támadásokról.