Magyar Rendészet 2014/5. 103–116.

Kiberterrorizmus. A terrorizmus új arca

PATAKI Márta – KELEMEN Roland

A szerzők munkájukban bemutatják a kiberterrorizmus eszközcselekményének jogi szabályozását. Csoportosítják az elkövetők körét, hiszen az általánosan használt „hacker" kategóriájánál jóval árnyaltabb kép alakítható ki, figyelembe véve, hogy mekkora tudású és milyen szándékú kiberszakember képes megvalósítani ilyen cselekményt. Ezt követően pedig a kiberterroristák által használt eszközöket vázolják fel – az eszközök köre nem taxatív, mivel ezen terület gyorsan változik, új eszközök jelennek meg, és régiek válnak elavulttá.

A „terror" főnév latinul ijedtséget, rémületet jelent. Bruce Schneier amerikai biztonsági szakértő is úgy véli, hogy *„a terrorizmus valódi lényege nem maga a cselekmény, hanem az arra adott reakció."*[1] A terrorizmus – mint politikai, társadalmi jelenség – végigkísérte az emberiség történelmét. A 19. századig a legtöbb esetben állami terrorról, királygyilkosságról beszélhettünk. A 19. században az anarchizmus vagy a nacionalizmus volt az ideológiai alapja egy-egy terrorcselekménynek vagy terrorszervezetnek. Az anarchista mozgalmak áldozata lett Erzsébet osztrák császárné, magyar királyné Genfben, 1898-ban, és szintén anarchisták követtek el több merényletet II. Sándor orosz cár ellen. 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, amikor palesztin terroristák három utasszállító repülőgépet térítettek el, ebből két gépet utasokkal együtt Jordániába irányítottak, majd bebörtönzött társaikra cserélték a túszokat, a harmadikat pedig az utasok leszállítását követően Kairóban felrobbantották. Ekkor merült fel először az a kérdés, hogy szabad-e tárgyalni terroristákkal, erre az államok egyre inkább nemleges választ adtak.

Ezen eseményeket követően a terrorizmus a 20. század végére teljesen új formát öltött, egyfelől a „tradicionális" terrorizmus célja már csak a pusztítás lett, másfelől pedig a számítógép, az internet világméretű elterjedésével egy új típusú cselekmény, a kiberterrorizmus is megjelent. Dennis C. Blair, az Amerikai Egyesült Államok nemzeti hírszerzésének igazgatója (Director of National Intelligence)[2] jelentésében hangsúlyozta, hogy „a növekvő információs rendszerek közötti kapcsolat, az internet, illetve egyéb infrastruktúrák lehetőséget teremtenek a támadóknak, hogy megzavarják a távközlé-

1 Schneier (2010) 14.

2 Tizenhat hírszerző tevékenységet végző szervezet munkáját kontrollálja, többek között a CIA-ét is.

si, villamosenergia-, a pénzügyi hálózatokat, finomítókat, valamint más létfontosságú hálózatokat."[3] Véleménye szerint az ezeket ért kibertámadás 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 „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."[4] A fentebb részletezett tényekből is kiolvasható, hogy a kiberbűncselekmények, valamint a kiberterrorizmus az egyre inkább teljessé váló globális térnek köszönhetően a 21. század legnagyobb veszéllyel fenyegető cselekményei.

Kiberbűnözők

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. Ezek a rendszerek, amelyek megkönnyítik a hétköznapokat, számtalan kockázatot rejtenek, amelyeket a bűnözők 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."[5] Ezen fejezetben a kiberbűnözők különböző típusait kívánjuk bemutatni.

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."[6] 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, ennek köszönhetően mar már nem határozható meg a hacker fogalmának egy általános definíciója.

Tudásuk erősorrendjében a hackereket a következőképpen rangsorolhatjuk: 1. valódi hackerek, 2. dark-hackerek, 3. light-hackerek, 4. wannabe-hackerek, 5. drifterek, 6. trollok. A következőkben ezen sorrendben kívánjuk bemutatni az egyes típusokat.

3 Blair (2009) 38.
4 Az Európai Parlament és a Tanács 2013/40/EU irányelve az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról, (5) bekezdés
5 Forrest (2005) 202.
6 Kazári (2003) 18.

1. A *valódi hacker* „olyan kimagasló számítástechnikai tudással bíró személy, aki szigorúan segítő jelleggel feltárja a számítógépes rendszerek/alkalmazások előnyeit és hibáit, illetőleg javít azokon."[7] 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 a biztonsági rendszerek hibáinak tesztelésével foglalkozik cégeknél vagy esetlegesen kormányhivataloknál.
2. A *dark-hacker* 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. A dark-hackernek szakértelme és szándéka is megvan terrorcselekmény elkövetéséhez.
3. A *light-hacker* számítástechnikai tudása jóval elmarad a valódi hackerétől, tudását gyakorolgatva keresi a hibás és támadható felületeket a világhálón. A hírnévre vágyakozva főleg defacementeket[8] követ el. Egyes vélemények szerint a light-hackerek 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 hackertársadalom e csoportot script-kiddie-nek nevezte el.
4. A *wannabe-hackerek* körének tagjai még nem valódi hackerek, de arra törekednek, hogy azzá váljanak. Tudásuk jóval csekélyebb az előzőekéhez képest, ebből kifolyólag más hackerek által kitalált, úgynevezett hackprogramokkal és exploitokkal[9] munkálkodnak.
5. A *drifterek* általában csak valamilyen információt vagy adatot keresnek az adott egyén gépén, és ha megtalálják a keresett adatot, lemásolják azt saját gépükre, majd továbbállnak. A gépen való jelenlétük legtöbbször észrevétlen marad, csupán néhány jel utalhat rá.
6. A *trollok* „előképzettség nélkül, gyakorlatilag céltalanul ténferegnek a világhálón, és tönkretesznek minden elébük kerülő és támadható dolgot a neten."[10] Ők a legfiatalabb „hackergeneráció", ezen csoport tagjai is mások által korábban kitalált hackprogramokkal dolgoznak, de legtöbbször nem is nagyon tudják, mit is csinálnak. A próbálkozások sikerességétől és annak milyenségétől függ a büntetőjogi felelősségük megállapítása.

Homogén csoportot alkotnak a HPAV-k (hacking, phreaking, anarchy, virus). „A HAPV-csapatok a létező legkártékonyabbak – vírusokat írnak, állami szervek munkáját teszik tönkre, magánszámítógépekbe törnek be, mindezt csak azért, hogy másoknak gondot okozzanak."[11] Ilyen csoportosulás jelenleg Európa területén gyakorlatilag alig

7 Kazári (2003) 18.
8 Defacement: honlapok feltörése és megváltoztatása. *„Hackernyelven egy adott weboldal/weboldalak kicserélését jelenti, ezáltal »szégyenítve« meg az adott oldalt üzemeltető céget, magánszemélyt."* Kazári uo. 154.
9 Exploit: védelmi hibát, biztonsági rést, illetve ezek kihasználását jelenti, kiválóan használható honlapfeltörésekre.
10 Forrest (2005) 205.
11 Kazári (2003) 21.

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."[12] Egy HPAV a tevékenykedése során bármely információs rendszer elleni bűncselekményt képes elkövetni. Sőt, olykor még a terrorcselekmények elkövetésétől sem riad vissza. Ezen egyéni vagy tisztán kiberbűnözőkből álló csoportok mellett egyre inkább megfigyelhető jelenség, hogy az egyes terrorszervezetek felbérelnek ilyen típusú szakembereket, vagy azok ideológiai meggyőződésből csatlakoznak ezekhez a csoportokhoz. Ezek fokozottabb veszélyt jelentenek, mivel jóval nagyobb anyagi bázissal bírnak, mint a fentebb felvázolt elkövetői körök.

A kiberterrorizmus eszközei, módszerei, és az ellenük való védekezési technikák

A kibertámadásoknak közvetlen és közvetett formáit különböztetjük meg. „A közvetlen cybertéri támadás során a támadó fél egyrészt a különböző információbiztonsági rendszabályokat kikerülve bejut a kommunikációs rendszerekbe, […] és ezáltal számára hasznosítható információkhoz jut. Másrészt […] rosszindulatú szoftverek bejuttatásával tönkreteszi, módosítja, törli stb. a szembenálló fél számára fontos információkat. A közvetett támadás során a támadó fél hozzáférhetővé teszi a másik fél számára a saját félrevezető információit, […] illetve hamis adatokkal túlterheli a rendszert."[13] Az alábbiakban tárgyalandó fejezet célja, hogy bemutassa a kiberterrorizmus eszközeit, 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 szerez meg, és azt milyen módon használja fel (az egyik felhasználási módozat a terrorcselekmény elkövetése).

Az információs rendszerek elleni támadási módszerek első csoportját azon eszközök képezik, amelyek a *helyi hálózatok ellen irányulnak,* ilyen az ún. Ethernet és a Token Ring helyi hálózat elleni támadás. Az Ethernet egy üzenetszórásos helyi hálózat, melynek lényege, hogy „ha az ügyfélállomás a kiszolgálótól adatot kér, adatcsomagot állít össze, amelyhez hozzácsatolja a megfelelő fejlécet, megcímzi a kiszolgálónak, majd útjára indítja a vonalon, ahol eljut a címzetthez."[14] A más állomásnak szánt adatcsomagot továbbengedi. Fontos itt megjegyezni, 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 technológia esetén a hacker[15] a hálózatba hatolva az állomásokat promiszkuitív módba kapcsolva képes megszerezni az összes adatcsomagot. A LAN-csatoló

12 Kazári (2003) 21.
13 Haig–Várhegyi (2008) 8.
14 Crume (2003) 138.
15 E fejezetben a „hacker" fogalma alatt összefoglalóan a dark-hackert és a HPAV-t kell érteni.

ugyanis promiszkuitív módban nemcsak az adatcsomag fejléce alapján rá vonatkozó adatcsomagokat menti le, hanem egy mappában rendszerezve az összes, helyi hálózat által továbbított üzenetet. Ezzel ideális körülményeket teremt a hackernek, hogy a titott adatszerzés bűncselekményét elkövesse, amely a Btk. 422. § (1) bekezdés d) pontjába ütközik,[16] illetve az információs rendszer vagy adat megsértése tényállás a) pontjában meghatározott elkövetési magatartását tanúsítsa. Egy ilyen támadás esetében a hacker (a hálózat összes adatcsomagjának birtokában) a terrorcselekmény információs rendszer vagy adat megsértésével bűncselekményének elkövetését is megalapozhatja, amelynél jelentőséggel bír, hogy az információs rendszer vagy adat megsértése bűncselekmény alap-, illetve minősített esetét valósítja-e meg. A hacker jelen esetben a hálózatba való betöréshez ugyanazt a követőprogramot (sniffert) használja, amelyet a teljes helyi hálózat megfigyelésére alkalmaznak a hálózati szakemberek.

Gyakori elkövetési mód a *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."[17] Ezzel a programmal a hacker listát kap a felhasználói azonosítókhoz tartozó titkosított jelszavakról, melyeket a hálózatfigyelő programmal egyúttal fel is tud törni. A jelszavak feltörésére további módszerek is alkalmazhatók, ilyen például a social engineering (pszichológiai manipuláció). „A social engineering 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."[18] Tehát a social engineer (azaz a hacker), miután megszerezte tőlünk a legfontosabb személyes adatainkat, feltölti azokat egy kódfeltörő programba, amely könnyedén megszerezheti titkos jelszavainkat. A jelszófeltörés esetében az elkövető a Btk. 423. § (1) bekezdés a) pontjában meghatározott, az információs rendszer vagy adat megsértése bűncselekményének alapesetét követi el, ebben az esetben a jelszóval védett információs rendszer fontosabb tulajdonságai határozzák meg, hogy e cselekmény alkalmas-e arra, hogy terrorcselekmény eszközcselekményéül szolgáljon.

A *DoS típusú támadás* egyfajta szolgálatmegtagadásos támadás, amely „egy számítógép-hálózati szolgáltatás teljes vagy részleges megbénítása, helyes működési módjától való eltérítése ártó, támadó szándékkal, elosztottan, több forrásból."[19] A támadás eredménye, hogy a rendszer megtagadja a felhasználóktól a hozzáférést a különböző szolgáltatásokhoz, amelyekre egyébként jogosultak lennének. Tehát a kritikus erőforrás

16 Btk. 422. § (1) bekezdése szerint: *„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."*

17 Crume (2003) 140.

18 Mitnick–Simon (2003) 1.

19 Haig–Kovács (2008) 66.

lefoglalásával gátolja a webhely tevékenységét. „A DoS-támadó nem fér hozzá fontos rendszerhez, nem lop el bizalmas információkat",[20] hanem valós vagy vélt sérelmének hangot adva rongálja meg az adott webhelyet. Álláspontunk szerint a hírközlési hálózat ellen indított DoS-támadás indokolttá teheti a terrorcselekmény elkövetése miatti felelősségre vonást.

A *Back Orifice (hátsó nyílás) támadás* esetében a hacker a Back Orifice nevű rosszindulatú programot – az elnevezéséből is adódóan – a „hátsó ajtón" juttatja be az információs rendszerbe, egy jóindulatú programba rejtve közvetíti azt a felhasználóhoz, aki gyanútlanul feltelepíti a gépére, abban a hiszemben, hogy valamilyen hasznos, jóindulatú programmal van dolga. A telepítés után a rosszindulatú program létezésének minden látható jele eltűnik, miközben 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 nyomai nincsenek, nagyon hatékony a kiberterrorizmus területén. Sőt, ha a hálózathoz mikrofon és videokamera is csatlakoztatva van, a hacker az eszközök bekapcsolásával figyelheti meg a felhasználót.

A *levélbomba-támadás* során a támadó e-mailek sokaságát küldi el egy program segítségével a felhasználónak, s ezzel 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 levélbombát, és azonnal szüntesse meg a kezdeményező fiókot. Az olvasottak alapján kijelenthetjük, hogy a levélbomba-támadás nem lehet eredményes terrorcselekmény elkövetése esetén.

A *vírustámadás* definíciója szerint: „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",[21] továbbá „a vírus fontos tulajdonsága a fejlődés képessége, tehát az, hogy képes ugyanazt a kódot megváltoztatott formában lemásolni."[22] 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."[23] Terrorcselekmény elkövetéséhez a 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 céljai kiszolgálására az államot vagy a nemzetközi szervezetet.[24]

A *trójai faló támadás*t a vírusok után kell megemlítenünk, mivel technikailag nem vírus ugyan, de hasonló károkat okoz az információs rendszerben. A vírustól való meg-

20 Crume (2003) 174.
21 Crume (2003) 188.
22 Szőr (2010) 15.
23 Warren–Streeter (2005) 137.
24 Btk. 423. § (1)–(4); 314. § (1) *a)* pontja

különböztetést az indokolja, hogy a trójai falovak nem feltétlenül másolják le önmagukat, mégis rosszindulatú programok, amelyek 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."[25] A vírusokkal való hasonlósága miatt, úgy véljük, a második leghatékonyabb módszer lehet a kiberterrorizmus eszköztárában a terrorcselekmény információs rendszer vagy adat megsértésével bűncselekményének elkövetéséhez.

A *számítógépféreg*nek 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."[26] A terrorcselekmény harmadik legjobb elkövetési módszere, hiszen egy gyorsan ható féreg jelentős kárt tud okozni az információs rendszerben, így kényszerítő hatása is legalább ilyen jelentős lehet.

A *zombihálózat*okat, azaz *bothálózat*okat azért kell itt megemlíteni, mert ezen hálózatok számítógépek sokaságát foglalhatják magukban, melyek segítségével nagyobb támadásokat lehet indítani. A zombihálózatba kapcsolt gépeket valaki más távolról irányítja. Többnyire személyes adatok, illetve titkos információk lopásához használják, de alkalmas gyorsan terjedő férgek szétküldésére is, így általa megbénítható az adott információs rendszer. A bothálózatok kiválóan alkalmasak terrorcselekmények elkövetésére, hiszen csak egy ártó szándékú, nagy tudású hacker és a zombihálózata szükséges hozzá.

A terrorizmus, kiberterrorizmus jogi háttere

A terrorizmus mint társadalmi jelenség az 1970-es években jelentősen felerősödött, „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."[27] Kiemelnénk egyrészt azon tényt, hogy ebben az időszakban több mint kétszáz új terrorszervezet jött létre a világon, másrészt – a nagyszámú terrorcselekmény közül – az 1972-es müncheni olimpián az izraeli delegációt ért támadást. Ezek okán nem meglepő, hogy Magyarországon 1978-ban került be először a büntető törvénykönyvbe a terrorcselekmény tényállása. 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."[28]

25 Crume (2003) 189.
26 Crume (2003) 189.
27 Bartkó (2005) 75.
28 Belovics et al. (2012) 471.

A század végére azonban a terrorcselekmények jellege teljesen megváltozott, fő motívuma a pusztítás lett. Eme jelenséggel szemben kívántak az államok egységes szabályozással fellépni, amely szándék nemzetközi egyezmények[29] formájában tárgyiasult. Bartkó Róbert véleménye szerint az 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."[30]

Az Európai Unió már a szervezetet létrehozó maastrichti szerződésben közös érdekként jelölte meg a terrorizmus elleni együttes fellépést. 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."[31] 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 Yorkban 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, amelyben többek között meghatározták az elkövetési módokat, a terroristacsoport fogalmát, valamint olyan szabályozási célokat is, hogy a terrorizmus finanszírozója, támogatója és a részesek cselekménye is büntetendő legyen.[32]

A fent említett kerethatározatba foglaltakat a magyar jogalkotó a büntető jogszabályok és a hozzájuk kapcsolódó egyes törvények módosításáról szóló 2003. évi II. törvénnyel implementálta a magyar jogba, egy teljesen új terrorcselekmény-tényállást megfogalmazva ezzel. A tényállás a kerethatározatba foglaltak átvételének köszönhetően jóval árnyaltabb és összetettebb lett, s nagyban tükrözi a korábban bemutatott nemzetközi egyezményekben felvázolt metszéspontokat. Az új büntető törvénykönyv jelentős változásokat nem hozott a terrorizmus tényállásának szabályozásában. A jogalkotó annyi változást eszközölt, hogy a terrorizmus finanszírozása önálló tényállás

29 Az Arab Liga 1998. április 22-i egyezménye a terrorizmus visszaszorításáról; az Afrikai Unió 1999. július 14-i egyezménye a terrorizmus megelőzéséről és a terrorizmus elleni küzdelemről; az Iszlám Államok Konferenciájának 1999. július 1-jei egyezménye a nemzetközi terrorizmus elleni küzdelemről; ENSZ-egyezmény a terrorizmus pénzügyi támogatásának visszaszorításáról (2000. február 25.)

30 Bartkó (2010) 79.

31 Bartkó (2011) 142–143.

32 Az Európai Unió Tanácsának 2002/475/IB kerethatározata a terrorizmus elleni küzdelemről (2002. június 13.), 1–6. cikk

lett. A kiberterrorizmus eszközcselekménye a 2003. évi II. törvény szerint a számítástechnikai rendszer és adatok elleni bűncselekmény volt. Ezen tényállás kvázi 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 a Számítástechnikai Bűnözésről szóló Egyezményt (Convention on Cybercrime, a továbbiakban: Cybercrime Egyezmény),[33] s ennek büntetőjogi rendelkezéseivel összhangban, a 2001. évi CXXI. törvénnyel a jogalkotó új tényállásokat alkotott meg: a számítástechnikai rendszer és adatok elleni bűncselekményt, valamint a számítástechnikai rendszer védelmét biztosító technikai intézkedés kijátszását.[34] A törvénymódosítás orvosolta a számítógépes rendszer fogalmának 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."[35]

A 2004-es év története, hogy az Európai Parlament és Tanács közös rendeletével[36] életre hívta az Európai Hálózat- és Információbiztonsági Ügynökséget. A rendelet szerint az ügynökség feladata, hogy „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 zavartalan működését."[37] Feladatainak részletezéséből kiderül, hogy az ügynökség jóval inkább egy tanácsadó, az együttműködést elősegítő, nem pedig egy napi védelmet biztosító szerv.

A tényállás fejlődésében előképet jelentett az unió 2005/222/IB kerethatározata, amelyből kitűnt, hogy a kodifikáció jövőbeli iránya a számítógépes rendszerrel elkövetett csalás és a számítástechnikai rendszer és adatok elleni bűncselekmény szétválasztása. Ennek magyarázata, hogy az utóbbi körébe az elkövetési magatartások egyre több típusa tartozhat, és ez szükségessé teszi önálló tényállásként való szabályozását. Hiszen 2005-ig a tényállás csak a számítógépes rendszerben tárolt adatokkal kapcsolatos tényállási elemeket tartalmazott, míg a kerethatározat már az információs rendszerhez való jogsértő hozzáférést, a rendszerben való jogsértő beavatkozást is büntetendő cselekményként kezelte.[38] Meg kell jegyezni, hogy ezen tényállások tartalmilag megegyeznek a Cybercrime Egyezmény tényállásaival, mivel azonban a kerethatározat kötelező uniós jogforrás, ezért a tagállamok tekintetében jobban segítette az egységes fellépés

33 Számítástechnikai Bűnözésről szóló Egyezmény. Kihirdette: 2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről.

34 2001. évi CXXI. törvény a Büntető Törvénykönyvről szóló 1978. évi IV. törvény módosításáról, 57–58. §

35 Belovics et al. (2009) 591.

36 Az Európai Parlament és a Tanács 460/2004/EK rendelete az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról

37 Az Európai Parlament és a Tanács 460/2004/EK rendelete az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról, preambulum (15) bekezdés

38 Az Európai Unió Tanácsának 2005/222/IB kerethatározata az információs rendszerek elleni támadásokról, 2–3. cikk

lehetőségét. A két bűncselekmény különválasztása az új büntető törvénykönyvben történt meg. A terrorizmus új kiber-eszközcselekménye az információs rendszer vagy adat megsértése elnevezésű tényállás lett, mely teljes egészében megfelel az uniós szabályozási kritériumoknak.

Az Európai Unió és Tanács 2013 nyarán új irányelvet fogadott el – amely felváltotta a 2005-ös kerethatározatot –, amelyben az unió újraszabályozta a kiberbűnözés típusait, és az 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."[39] Az már a jogalkotó saját hatásköre, hogy új tényállást alkot, vagy – mint új elkövetési magatartást – a 423. szakasz részévé teszi. 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 nincs feladata a törvényhozásnak. Általánosságban elmondható, hogy az irányelv szabályai szigorodtak a kerethatározathoz képest, s ez jól lemérhető az általa megadott szankcionálási módban: míg a 2005-ös kerethatározat a büntetés maximumát három évben szabta meg, addig a 2013-as irányelv már öt évben állapította meg azt.

Az irányelvből kitűnik az információs rendszerek fontos szerepe, hiszen ezek, mint fogalmaz, „a politikai, a társadalmi és a gazdasági interakció kulcstényezői az Unióban."[40] Ezen infrastruktúrák védelme alapvető uniós érdek, és ezt a nemzeti büntetőjogi szabályoknak is tükrözniük kell. Ezért – véleményünk szerint – a tiltott adatszerzés alapesetei közül az „elektronikus hírközlő hálózat – ideértve az információs rendszert is – útján másnak továbbított vagy azon tárolt adatot kifürkész, és az észlelteket technikai eszközzel rögzíti" fordulat szerinti tényállást is a terrorcselekmény eszközcselekményévé kellene tenni, mivel – mint ahogy arra már korábban is kitértünk – a mai társadalomban az egyik legfontosabb hatalmi forrás az információ, amelynek birtokosa azt akár fegyverként is fel tudja használni a társadalom széles tömegeivel, az állammal és akár nemzetközi szervezetekkel szemben is.

Ez kiemelten igaz az állam- és nemzetbiztonság területén, ezért Magyarország az Európai Unióhoz hasonlóan kidolgozta saját kiberstratégiáját, amelynek részeként az Országgyűlés 2013-ban elfogadta azon törvényt, amely a 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 infor-

39 Az Európai Parlament és Tanács 2013/40/EU irányelve az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról, 6. cikk

40 Az Európai Parlament és Tanács 2013/40/EU irányelve az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról, (2) bekezdés

mációs rendszerek, illetve a létfontosságú információs rendszerek és rendszerelemek biztonsága."[41] Ezzel a jogalkotó kifejezi elhivatottságát a kiberterrorizmussal szemben, más oldalról pedig láttatja, hogy ez valódi veszélyforrás bármely állam számára.

A törvény felállította a Nemzeti Biztonsági Felügyeletet, amelynek feladata sérülékenységi vizsgálatok végzése, az észlelt hiányosságok kijavítása, információs rendszerek működésének ellenőrzése, támadás esetén azonnali intézkedés javaslása (működés korlátozása, leállítása), és tájékoztatást kérhet az adott szerv vezetőjétől, dolgozójától. Felügyeleti jogkörének gyakorlása során megbírságolhatja azon szervezet vezetőjét, aki írásbeli felszólítás ellenére sem teljesíti az abban meghatározottakat. A bírság ötvenezertől ötmillió forintig terjedhet.[42] 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 annak lehetőségei is korlátozottak – a jogalkotónak ezen lehetőségeket kellene kiszélesítenie.

Zárógondolatok

A 20. 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. A 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 a „kiberterrorista" elnevezéssel illetünk. A számítógépek fejlődésével azonos ütemben nő azon szakemberek száma, akik képesek az állam alapvető rendszereiben a kibertéren keresztül kárt tenni. A köznyelv ezen elkövetőket hackereknek nevezi. Hibásan, hiszen ezen elnevezés igen tág kategória, magában foglalja a valódi hackert, a dark-hackert, a light-hackert, a wannabe-hackert és így tovább. Ezen személyek szakmai tudása és szándékai 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-k csoportja képes ilyen „akciók" végrehajtására.

A 21. század első évtizedének elejére már a jogalkotó számára is világossá vált, hogy a fent említett személyek cselekményei ellen fel kell lépni. Az Európa Tanács 2001-ben, Budapesten fogadta el a Cybercrime Egyezményt, amely az elfogadó országok számára kötelezővé tette egyes cselekmények kriminalizálását. Az Európai Unió a 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

41 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról, preambulum

42 301/2013. (VII. 29.) Korm. rendelet a Nemzeti Elektronikus Információbiztonsági Hatóság és az információbiztonsági felügyelő feladat- és hatásköréről, valamint a Nemzeti Biztonsági Felügyelet szakhatósági eljárásáról

fogadtak el, amely a 2005-ös kerethatározathoz képest szigorítja a kiberbűnözőkkel szembeni szankciókat, továbbá figyelmeztet arra, hogy óriási veszélyforrást jelentenek ezek a támadások az Európai Unióra nézve. A magyar szabályozás mindvégig követte az unió által elvártakat, így e területen jelenleg nincs a jogalkotóval szembeni uniós elvárás.

A 2013-ban elfogadott új, az állami és önkormányzati szervek információbiztonságát szabályozó törvény előrelépést jelent, követve a nemzetközi szabályozást[43] felállítja a Nemzeti Biztonsági Felügyeletet, amelynek feladata többek között a megelőzés, a szükséges védelem kiépítése, ennek ellenőrzése és utasítás lehetősége támadás esetében. A magyar szabályozás azonban nem biztosít lehetőséget arra, hogy támadás közben aktív védekezést tanúsítson bármely magyar szervezet. Álláspontunk szerint a szabályozást úgy kellene alakítani, hogy a TEK vagy az NBF támadás esetén viszonttámadást indíthasson a támadó rendszer ellen. Az Egyesült Államokban ezen 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. Nyilvánvalóan a visszatámadás jogával felhatalmazott szervnek diszkrecionális joga volna eldönteni, hogy mely esetekben él ezzel a felhatalmazással, hiszen egyes esetekben e jog gyakorlása hátráltatná a büntetőjogi felelősségre vonás esélyeit, azonban vannak olyan adatok, információs rendszerek, amelyek esetében elsődleges a védelem, a támadás visszaverése (például nemzetbiztonsági adatok, repülésirányítási rendszerek), és csak másodlagos a későbbi hatékony felderítés.

Tipikusan alkalmas eszköz lenne erre a szolgáltatásmegtagadásos támadás és a túlterheléses támadás, amely kárt nem okozna, de alkalmas lenne arra, hogy a támadó rendszer ne férjen hozzá a hálózathoz, meghiúsítva ezzel annak eredményességét. Az internetes levelezés megfigyelése kulcsszavas kereséssel szintén gátat szabhat az egyes támadásoknak, a megfigyelést viszont nehezíti a kriptográfiai programok használata. Ezen nehézségek leküzdésére nyújt mintát az angol Regulation of Investigatory Powers Act, amely kimondja, hogy aki ilyen programot használ, az köteles annak kulcsát átadni az illetékes hatóságnak, amennyiben ezt nem teszi meg, szabadságvesztéssel is büntethető. Véleményünk szerint ezen két lehetőség sok esetben hatékonyabbá tenné a hatóságok védekezését, és az esetek egy részében a megelőzést is lehetővé tenné.

IRODALOMJEGYZÉK

Felhasznált irodalom:

Bartkó Róbert (2005): Gondolatok a terrorizmus fogalmáról. In. *Belügyi Szemle,* 53. évf. 6. sz. 75–88.
Bartkó Róbert (2010): A terrorcselekmény mint nemzetközi bűncselekmény. In: *Rendészeti Szemle,* 58. évf. 5. sz. 73–87.

43 Például: az EU fent ismertetett ügynöksége, USA Comprehensive National Cybersecurity Initiative, India Indian Computer Emergency Response Team.

Bartkó Róbert (2011): *A terrorizmus elleni küzdelem kriminálpolitikai kérdései.* Győr, Universitas-Győr.
Belovics Ervin – Molnár Gábor Miklós – Sinku Pál (2009): *Büntetőjog. Különös rész.* Budapest, HVG-ORAC Lap- és Könyvkiadó Kft.
Belovics Ervin – Molnár Gábor Miklós – Sinku Pál (2012): *Büntetőjog II. Különös rész.* Budapest, HVG-ORAC Lap- és Könyvkiadó Kft.
Blair, C. Dennis (2009): *Annal Treat Assessment of the Intelligence Community for the Senate Select Committeon Intelligence.* Forrás: www.intelligence.senate.gov/090212/blair.pdf (2013. 09. 12.)
Crume, Jeff (2003): *Az internetes biztonság belülről – amit a hekkerek titkolnak.* Bicske, Szak Kiadó.
Forrest, Dave (2005): *Barát vagy ellenség? A totális kontroll forgatókönyve.* Budapest, Focus Kiadó.
Haig Zsolt – Kovács László (2008): Fenyegetések a cybertérből. In: *Nemzet és Biztonság,* 14. évf. 5. sz. 61–69.
Haig Zsolt – Várhegyi István (2008): A cybertér és a cyberhadviselés értelmezése. In: *Hadtudomány,* 18. évf. elektronikus sz. 1–12.
Kazári Csaba (2003): *Hacker, cracker, warez. A számítógépes alvilág titkai.* Budapest, Computer Panoráma.
Mitnick, Kevin D. – Simon, William L. (2003): *A legendás hacker. A megtévesztés művészete.* Budapest, Perfact-Pro Kft.
Raymond, Eric S. (1996): *The newhacker'sdictionary.* Cambridge, MIT Press.
Schneier Bruce (2010): *Schneier a biztonságról.* Budapest, HVG Kiadó Zrt.
Szőr Péter (2010): *A vírusvédelem művészete.* Bicske, Szak Kiadó.
Warren, Peter – Streeter, Michael (2005): *Az internet sötét oldala. Vírusírók, adatrablók, hackerek – és amit tehetünk ellenük.* Budapest, HVG Kiadó Zrt.

Felhasznált források:

301/2013. (VII. 29.) Korm. rendelet a Nemzeti Elektronikus Információbiztonsági Hatóság és az információbiztonsági felügyelő feladat- és hatásköréről, valamint a Nemzeti Biztonsági Felügyelet szakhatósági eljárásáról
1978. évi IV. törvény a Büntető Törvénykönyvről
2001. évi CXXI. törvény a Büntető Törvénykönyvről szóló 1978. évi IV. törvény módosításáról
2004. évi LXXIX. törvény az Európa Tanács Budapesten, 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezményének kihirdetéséről
2012. évi C. törvény a Büntető Törvénykönyvről
2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
Az Európai Parlament és a Tanács 460/2004/EK rendelete az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról
Az Európai Parlament és a Tanács 2013/40/EU irányelve az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról
Az Európai Unió Tanácsának 2002/475/IB kerethatározata a terrorizmus elleni küzdelemről
Az Európai Unió Tanácsának 2005/222/IB kerethatározata az információs rendszerek elleni támadásokról

SUMMARY

Cyberterrorism – The New Face of Terrorism

PATAKI Márta – KELEMEN Roland

The authors present the legal regulation of cyber-terrorism. They classify the perpetrators, as the commonly used term hacker is too wide to differentiate between skilled cyber criminals. Finally, they discuss the tools used by cyberterrorists; the list of tools is incomplete because the IT area is rapidly evolving.