DORNFELD LÁSZLÓ

KIBERTERRORIZMUS – A JÖVŐ TERRORIZMUSA?

1. Bevezetés

A terrorizmus, amely a '80-as évek vége óta egyre kevésbé volt jelentős Európában, napjainkban újra egyre nagyobb fenyegetést jelent a kontinensre. A közelmúltban végrehajtott párizsi és brüsszeli támadások megmutatták a lakosság sebezhetőségét az ilyen támadásokkal szemben. A hagyományos terrorizmus ismételt megjelenését látva nő az azzal kapcsolatos félelem is, hogy a terroristák az informatikai rendszerek felhasználásával is képesek lehetnek csapást mérni. Ez igen jelentős biztonsági kockázatot jelentene, hiszen ezen új technológiai vívmányok lassan minden európai lakos mindennapi életének részévé váltak. Ráadásul az internetes környezet jóval ideálisabb körülményeket teremt a terrorcselekmények elkövetésére.

Habár a kiberterrorizmus kifejezés már 1979-ben megjelent egy svéd számítógépes bűnözésről szóló jelentésben,[1] széles körben csak a 9/11-i terrortámadásokat követően terjedt el a büntetőjogi szakirodalomban.[2] Érdemes megjegyezni, hogy politikai célú támadásokat már ezt megelőzően is indítottak az interneten keresztül, így például az 1999-es koszovói konfliktus során. A Jugoszláviát ért bombázásokat követően túlterheléses, ún. DDoS-támadások (Distributed Denial of Service)[3] indultak a NATO weboldalaival szemben,[4] és jugoszláv honlapok működését is megpróbálták ellehetetleníteni vagy tartalmukat módosítani. A NATO szándékosan nem pusztította el az ország internetelérést biztosító fizikai infrastruktúráját, abban bízva, hogy az interneten keresztül szerzett információk a jugoszláv kormány ellen fordíthatják a lakosságot.[5]

---

[1] Oleksiewicz, Izabela: Dilemmas and Challenges for EU Anti-Cyberterrorism Policy: The Example of the United Kingdom. Teka Kom. Politol. Stos. Międzynar. 2016/3. 136. o.

[2] Parti Katalin: Kerekasztal-beszélgetés az online terrorizmusról. Ügyészek Lapja, 2010/2. 43. o.

[3] Lásd bővebben Mezei Kitti: A DDoS-támadások büntetőjogi szabályozása az Egyesült Államokban, Európában és Magyarországon. Pro Futuro 2018/1. 66-83. o

[4] Sipos Zoltán: A kibertér biztonságával kapcsolatos alapvető kérdések áttekintése. Honvédségi Szemle, 2016/1. 28. o. (Denning (2001): i.m. 252. o.)

[5] Denning, D. E. : Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing

Fontos kérdés ugyanakkor, hogy ezek az akciók tekinthetők-e kiberterrorizmusnak. A jogi szakirodalom közel sem egységes abban a kérdésben, hogy hol húzódik a határ az internetes polgári engedetlenség és a terrorizmus között. Tovább nehezíti az elhatárolást, hogy napjainkban a terrorszervezetek egyre gyakrabban élnek a kibertér adta lehetőségekkel saját üzeneteik terjesztésére, a követők toborzására és pénzügyi támogatás szerzésére. Ez a folyamat szintén az 1990-es években kezdődött meg, amikor az egyes csoportok elkezdték létrehozni saját honlapjaikat.[6] Ezek száma alig párról 2007-re már 4300-ra nőtt,[7] és napjainkra a terrorszervezetek aktívan használják az internetet. Jó példa erre, ahogyan az Iszlám Állam a közösségi média aktív és profi felhasználásával gyorsan hírhedté vált, és viszonylag széles online támogatói kört tudott kiépíteni.

E fejezetben áttekintem a jogirodalomban jelen lévő álláspontokat, valamint elhatárolási kísérleteket. A fogalom meghatározás és elhatárolás mellett a kiberterrorizmus jellemzőit is bemutatom, valamint azt, hogy az egyes államok milyen módszerekkel igyekeznek az ilyen támadásokat megelőzni, illetve a mögötte állókat felderíteni. Ezek mellett arra is választ keresek, hogy napjainkban mennyire jelent aktuális biztonsági fenyegetést az internetes terrorizmus, és várható-e ennek változása a jövőben.

2. A kiberterrorizmus meghatározása

A kiberterrorizmus szó nyelvtani értelemben vizsgálva a kibertérben elkövetett terrortámadásokat jelöli. Ennek megértéséhez meg kell vizsgálnunk a két fogalom jelentését. A kiber a görög kübernétészből (κυβερνήτης) ered, amely kormányost jelent. Az angolban ismertté William Gibson tette, aki 1982-ben használta először a kibertér fogalmát a fizikai világtól elkülönülő digitális térre.[8] A terrorizmus a latin terrere (megrémít) szóból ered, amelyet a francia -isme toldalékkal ellátva megkapjuk a terrorisme-et. Ez már a „rémületet okozni" jelentéssel bír.[9]

Foreign Policy. In: J. Arguilla, D. Ronfeldt (ed.) = Networks and Netwars: The Future of Terror, Crime, and Militancy. 2001. 239-241. o.

[6] Denning: i. m. 252. o.

[7] Hummel, Michael L.: Internet Terrorism. Homeland Security Review 2008/2. 117. o.

[8] Wall, David S.: Cybercrime: The Transformation of Crime in the Information Age. Polity, 2007. 10–11. o. Megjegyzendő ugyanakkor, hogy sok helyen tévesen Gibsont jelölik meg, mint a fogalom megalkotóját. http://www.kunstkritikk.dk/kommentar/the-reinvention-of-cyberspace/ [2018.06.23.]

[9] Matusitz, Jonathan: Terrorism & Communication. A Critical Introduction. Thousand Oaks, SAGE Publications, 2013. 1. o.

Ezen fogalmak egyikének sincs egységes meghatározása a jogirodalomban. A kibertér leginkább a mai internet keretei között értelmezhető, de tágabb annál. Fogalmát Frédérick Douzet úgy próbálta megragadni, hogy az „emberek, adatok és számítógépek hálózata… információs tér, területhez nem kötött információcsere, amelyet nehéz megérteni. Materiális infrastruktúrából áll, amelyet fizikai területre építenek, ideértve a világűrben megtalálható műholdakat is."[10]

A terrorizmus szabályozásával 14 ENSZ egyezmény és 4 kiegészítő jegyzőkönyv is foglalkozik, ezek mindegyike megkerüli azonban az egységes fogalom kérdését, ehelyett egy-egy elkövetési módozat fogalmát megadva csupán. Ennek következtében napjainkra mintegy ötven különböző cselekményt rendelnek üldözni a releváns nemzetközi egyezmények, ami nagyfokú bizonytalanságot okoz.[11] Hosszú ideje sikertelenül próbálják elfogadni a Nemzetközi Terrorizmusról szóló Átfogó Egyezmény Tervezetet, amely szerint a terrorcselekmények olyan „másik állammal szemben végrehajtott, személy vagy dolog elleni erőszakos cselekmények, amelyek természetükből adódóan a közéleti szereplőkben, személyek csoportjában, a közvéleményben vagy a lakosságban rémületet, félelmet vagy bizonytalanságot keltenek".[12]

Ebből a meghatározásból máris kitűnik a legnagyobb probléma a kiberterrorizmus koncepciójával kapcsolatban: személy vagy dolog elleni erőszakos cselekmények szerepelnek benne. Eltérő megközelítést alkalmaz az Európai Unió 2017/541 irányelve[13] és az ezt megelőző 2002/475/IB tanácsi kerethatározat fogalmát a 2012. évi C. törvénybe (a továbbiakban Btk.) építő hazánk, ahol a tényállás előbb meghatározza a célzatot, majd az eszközcselekményeket. Ezek jelentős része is csak a fizikai világban megvalósítható cselekmény, azonban itt már számos olyat találhatunk, amely a kibertérben is megvalósítható. Így például a 3. cikk g) pontja szerinti „veszélyes anyag kiengedése, vagy tűzvész, árvíz vagy robbanás előidézése, amely emberi életet veszélyeztet". 2000-ben Ausztráliában egy hacker 800 ezer liter szennyvizet engedett a környező vizekbe, súlyos károkat okozva az élővilágnak.[14] A cikk h)

[10] Pintér István: A virtuális tér geopolitikája. In: Pintér István (szerk.) A virtuális tér geopolitikája. Geopolitikai Tanács, 2016. 312. o.

[11] Dornfeld László – Sántha Ferenc: A terrorizmus és a terrorcselekmény, mint nemzetközi bűncselekmény aktuális kérdései. Jog Állam Politika 2017/3. 73–75. o.

[12] Dornfeld – Sántha: i. m. 79–80. o.

[13] Az Európai Parlament és a Tanács 2017/541 irányelve a terrorizmus elleni küzdelemről. HL 2017 L 88, 31.3.2017. Elfogadták 2017. március 15-én, átültetés határideje 2018. szeptember 8.

[14] Environmental Risks: Cyber Security and Critical Industries. 5. o. Nevezett támadás ugyan más okból (politikai célzat hiánya) nem tekinthető terrorcselekménynek, de rámutat arra, hogy a terroristák is végrehajthatnak hasonló támadásokat.

pontjában szereplő „a víz- vagy áramellátásnak, illetve más létfontosságú természeti erőforrás ellátásának olyan megzavarása vagy megszakítása, ami emberi életet veszélyeztet" szintén végrehajtható a kibertérben. Az irányelv i) pontja és a Btk. a 314. § (4) bekezdés i) pontja egyaránt az eszközcselekmények közé sorolja a 2013/40/EU irányelvben szabályozott „rendszert érintő jogellenes beavatkozás" (a Btk. terminológiája szerint „információs rendszer vagy adat megsértése") bűncselekményét is.[15]

A kiberterrorizmus angolszász területen egyik népszerű meghatározása szerint „kiber rendszerek elleni erőszak, zavarás vagy működésébe történő beavatkozás vagy ezzel való fenyegetés, mikor valószínűsíthető, hogy ennek eredménye halál vagy sérülés, vagyontárgy súlyos károsodás vagy a társadalmi rend megzavarása."[16] Látható, hogy a fogalom alapvetően a terrorizmus megjelenési formáit és a kibertérben történő elkövetést vonja össze, és bizonyos elemeinél kiütközik az angolszász jogrendszer dogmatikai kötetlensége, például az erőszak szerepeltetésénél. Más fogalmak, így például Denningé szintén tartalmazzák az „erőszakos támadás" fogalmát.[17] Ugyanakkor, mint az a fentiekből is látható, a kontinentális jogrendszerekben a terrorcselekmény már létező tényállásának részeként szabályozzák a jelenséget, és így új fogalmat sem alkotnak rá.

3. Elhatárolása más kiberfenyegetésektől

A kibertérben jelen lévő fenyegetések között már régóta próbálnak a kutatók és az azok elhárításában részt vevő szervezetek különbséget tenni. Ez a kérdés nem csak elméleti jellegű, hiszen két hasonló kibertámadás esetén is előfordulhat, hogy más állami szerv fellépése szükséges. Egy bűncselekmény esetén ugyanis elegendő lehet a nyomozó hatóság fellépése, de ha a cél kémkedés vagy kiberháborús támadás végrehajtása volt, akkor a titkosszolgálat és a hadsereg válaszlépése szükséges. A szakirodalom alapvetően eltérő számú típusát határozza meg a kiberfenyegetéseknek,[18] én ezek közül a következőket gondolom relevánsnak a téma szempontjából: hacktivizmus, kiberbűnözés, kiberterrorizmus és kiberhadviselés. A fogalmaknagyon hasonlóak egymáshoz, hiszen mind valamilyen tevékenység kibertérben történő megvalósítását jelöli, így szükséges ezeket elhatárolni egymástól.

[15] Lukácsi Tamás: A terrorizmus elleni küzdelemről szóló (EU) 2017/541 európai parlamenti és tanácsi irányelv. Európai Jog 2017/6. 23. o.

[16] Gillespie, Alisdair A.: Cybercrime – Key Issues and Debates. Routledge, 2016. 107. o.

[17] Mezey Nándor Lajos: Kiberterrorizmus: valós veszély? Belügyi Szemle, 2011/2. 23. o.

[18] Maras, Marie-Helen: Cybercriminology. Oxford University Press. New York, 2017. 378. o.

3.1. Hacktivizmus

A hacktivizmus kifejezés a hackelés és aktivizmus szavak összerántásából született meg. Jellegét nézve tekinthetjük a hackermozgalom politikai kifejeződésének, politikai célzatú hackelésnek vagy politikai célok hackereszközökkel való elérésnek.[19] Az internet közvéleményt formáló ereje – mint arra már a bevezetőben is utaltam – már hosszabb ideje, legalább a koszovói konfliktus óta ismert. A háború során mindegyik harcban álló fél igyekezett az internetet a saját üzenetének terjesztésére hasznosítani, de e tevékenységek többsége egyszerű internetes aktivizmus volt.[20] Az egyik első komolyabb politikai célú támadásra azonban már egy évtizeddel korábban, 1989-ben sor került, amikor a NASA és az Egyesült Államok Energiaügyi Hivatalának számítógépeit törték fel, és a bejelentkező képernyőt nukleáris energia elleni üzenetekre módosították.[21] Szemben az aktivizmussal, amely az internet nyújtotta legális lehetőségeket – például online petíciók írása, figyelemfelkeltő honlapok és blogok létrehozása – használja fel valamely vélemény szélesebb körű terjesztésére, a hacktivizmus már illegális vagy jogilag aggályos eszközök igénybevételét jelenti. Ez tipikusan az ellenkező véleményen lévő weboldalak vagy kormányzati portálok feltörését, elérésének megakadályozását jelenti, jellemzően minimális károkozással.[22] Példaként hozható az az eset, amikor 2012-ben a magukat az Anonymous hackerideológia követőiként azonosító elkövetők meghackelték az Alkotmánybíróság honlapját és megváltoztatták rajta az Alaptörvény szövegét.[23]

A hacktivizmus a kiberterrorizmushoz hasonlóan szintén a politikai célok elérését szolgálja, ám mégis szükséges külön kezelni a két jelenséget. Különösen azért, mert – mint arra Mezey Nándor is rámutat – vannak, akik tagadják az utóbbi létezését.[24] Denning szerint az utóbbit elkövetők céljaikat valamilyen súlyos veszteség, például halálozások vagy jelentős gazdasági kár előidézésével kívánják megvalósítani. Ezzel szemben a hacktivizmust a polgári elégedetlenség kibertérben történő megjelenéseként értelmezi.[25] Illig szintén hasonlóképp vélekedik a hacktivizmus szerepéről. Szerinte a hacktivisták legfőbb célja az internetes szólás- és információszabadság biztosítása, és módszerükben az különbözteti meg őket a kiberterroristáktól, hogy

[19] Simon Béla: Hacktivism and Its Status in Hungary. Magyar Rendészet 2016/2. 161. o.
[20] Denning: i. m. 246–250. o.
[21] Illig, A. T.: Computer Age Protesting: Why Hacktivism is a Viable Option for Modem Social Activists. Penn State Law Review, ?/2015. 1035–1036. o.
[22] Denning: i. m. 240–242. o.
[23] http://index.hu/tech/2012/03/04/az_anonymous_atirta_az_alaptorvenyt/ [2018. 06. 23.]
[24] Mezey: i. m. 23. o.
[25] Denning: i. m. 263. o.

elkötelezettek az erőszakmentes aktivizmus mellett.[26] WALL szerint a fő különbség a két besorolás között abban áll, hogy a kiberterrorizmus valamilyen kritikus infrastruktúrát vesz célba.[27] A kritikus infrastruktúra fogalmát a 2008/114/EK irányelvet átültető 2012. évi CLXVI. törvény 1. § tartalmazza: ez alapján ide tartozik minden olyan rendszerelem és létesítmény, amely elengedhetetlen a létfontosságú társadalmi feladatok ellátásához, és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna. Egy példán keresztül szemléltetve: míg a magyarországi Anonymous korábban említett oldalfeltörése elhanyagolható anyagi kárt okozott, addig az Észtország online infrastruktúráját 2007-ben három hétig támadó orosz hackerek szinte teljesen megbénították az állam működését.[28]

3.2. Kiberbűnözés

Fontos kérdésként merül fel, hogy a kiberterrorizmus a kiberbűnözés részeként értelmezhető-e vagy pedig elkülönül attól. Egyes szerzők annak pártján állnak, hogy a jelenség a kiberbűnözés egyik megjelenési formája.[29] A kettő eszköztára ugyanis jelentős átfedést mutat, így például kártékony programok, elosztott szolgáltatásmegtagadással járó, avagy DDoS-támadás, információs rendszerbe történő jogosulatlan belépés mindkettőnél megfigyelhető.[30] Ugyanígy megegyeznek a támadások módszerei, amelyek arra irányulnak, hogy a rendszerek gyengepontjait használva adjanak hozzáférést a támadónak a rendszerhez. A legtöbb államban a két bűncselekményi körrel foglalkozó szervek is azonosak vagy legalábbis igen jelentős átfedést mutatnak.

A fő különbség az elkövetés mögötti motivációban lelhető fel. Míg a bűnözők elsősorban vagyoni vagy más előny eléréséért, esetleg szórakozásból követnek el bűncselekményeket a kibertérben, addig a kiberterrorizmus mögött valamilyen politikai, vallási indíttatású cél húzódik meg. További különbség még, hogy a terroristák sokkal szélesebb körben határozzák meg célpontjaikat, mint a bűnözők. A célok terén a fő különbség, hogy a terroristák a megkülönböztetés nélküli fizikai károkozást kívánják elérni, míg a bűnözők esetén ez nem kifejezetten cél.[31]

---

[26] ILLIG: i. m. 1036–1037. o.

[27] WALL: i. m. 9. o.

[28] BUONO, Laviero: Gearing Up the Fight Against Cybercrime in the European Union: A New Set of Rules and Establishment of the European Cybercrime Centre (EC3). New Journal of European Criminal Law, 2012/3. 336. o.

[29] CASSIM, F.: Addressing The Spectre of Cyber Terrorism: A Comparative Perspective. Potchefstroom Electronic Law Journal, 2012. 381. o.

[30] Az egyes eszközök részletesebb leírásáért lásd: PATAKI Márta – KELEMEN Roland: Kiberterrorizmus. A terrorizmus új arca. Magyar Rendészet 2014/5. 106–109. o.

[31] BRENNER, W. Susan: Cybercrime, Cyberterrorism and Cyberwarfare. Revue internationale de droit pénal, 2006/3. 453–471. o.

Véleményem szerint ugyanakkor ez a különbségtétel legfeljebb elméleti szinten tehető meg, hiszen a gyakorlatban szinte lehetetlen teljesen egyértelműen eldönteni, hogy egy támadás mögött ki áll. Az eszközök és módszerek nagymértékű hasonlósága, a támadás mögötti cél homályossága folytán az éles elkülönítés esetén komoly hatásköri viták állhatnának elő, pontosan akkor, amikor gyors reakció szükséges a kiberbiztonság helyreállítása érdekében. Ebből kifolyólag én nem látom előnyét a kiberbűnözés és a kiberterrorizmus közötti éles határvonal meghúzásának, amely a jövőben is valószínűleg inkább akadémiai, semmint gyakorlati jellegű vizsgálati kérdés marad.

3.3. Kiberhadviselés

A kiberhadviselés az államok által indított kibertámadásokra alkotott fogalom, amelynek alapját képezi az, hogy a technológiai fejlődést az államok egyre gyakrabban a politikai és katonai erőfölény biztosítása érdekében használják fel.[32] Hadtudományi szempontból a NATO az információs műveletek részeként kezeli, amelyek célja az információs fölény elérése. Jellegét tekintve lehet támadó, amely az ellenség hálózatait célozza, valamint védekező, amely a saját rendszerek megóvására irányul. Lényeges az is, hogy kiberhadviselésről nemzetközi jogi értelemben akkor beszélhetünk, ha ismert a támadó állam kiléte.[33]

A fő különbség éppen ezért könnyedén megállapítható a kiberterrorizmus és a kiberhadviselés között: előbbinek nem állami szereplők, utóbbinak államok a végrehajtói. Ugyanakkor az állami érintettség kérdése az, amelyet igen nehéz bizonyítani, az államok ugyanis nem vállalják fel nyíltan a békeidőben végrehajtott kibertámadásaikat. Jó példa erre az, hogy a Snowden-botrány révénkiderült, az Egyesült Államok 2011-ben 231 alkalommal indított titokban támadást Oroszország, Kína, Irán és Észak-Korea ellen.[34] De ugyanígy nem bizonyítható az, hogy az Egyesült Államok és Izrael hajtotta végre az iráni atomlétesítmények elleni támadást a Stuxnet kártevővel,[35] annak ellenére, hogy a jelek egyértelműen rájuk mutatnak.[36]

---

[32] Szathmáry Zoltán: Bűnözés az információs társadalomban – Alkotmányos büntetőjogi dilemmák az információs társadalomban. PhD értekezés. Budapest, 2012. 43. o.

[33] Berki Gábor: Kiberháborúk, kiberkonfliktusok. In: Pintér István (szerk.) A virtuális tér geopolitikája. Geopolitikai Tanács, 2016. 260–264. o.

[34] Eichensehr, Kristen E.: The Cyber-Law of Nations. Georgetown Law Journal, 2015/2. 319. o.

[35] Lásd részletesen: Nagy Zoltán András: A kiber-háború új dimenzió – a veszélyeztett állambiztonság (Stuxnet, DuQu, Flame – a Police malware). In: Gaál Gyula – Hautzinger Zoltán: Pécsi Határőr Tudományos Közlemények XIII. 2012. 225-228. o.

[36] Lásd ehhez Holt, Thomas J. – Bossler, Adam M. – Seigfried-Spellar, Kathryn C.: Cybercrime and digital forensics: An introduction. Routledge, 2018. 411-415. o.

Szemben a kiberbűncselekménytől való elhatárolástól, itt gyakorlati jelentősége is lenne a különbségtételnek, hiszen teljesen más következményekkel járnak, és más szerveknek kell érintetté válnia. Kiberhadviselés esetén a diplomáciai-katonai válaszok foganatosításának kell megtörténnie, így például az Egyesült Államok kibertérre vonatkozó nemzetközi stratégiája leszögezi, hogy kibertérből érkező állami támadásra bármely eszközzel – legyen az diplomáciai, információs, katonai vagy gazdasági – válaszolhatnak.

4. Terroristák és az internet

A továbbiakban szükséges még egy elhatárolást megtennünk, méghozzá a kiberterrorizmus és a terroristák egyéb internetes tevékenysége között. Mint arra már a bevezetőben is utaltam, a terroristák és terrorszervezetek napjainkra már előszeretettel veszik igénybe az internet nyújtotta lehetőségeket, hiszen olcsón tudnak nagy közönséghez eljutni üzeneteik. Alapvetően ötféle célt különböztethetünk meg: propaganda, pénzgyűjtés, információterjesztés, biztonságos kommunikáció és hírszerzés.[37] Ezek a szervezet rendes működéséhez kapcsolódó tevékenységek, amelyeknél az új technológia igénybevétele könnyebbé vagy biztonságosabbá teszik addigi tevékenységeiket.

A propaganda a terrorszervezet online történő kommunikációját takarja, aminek célja a befolyásolás, és jelentheti céljaik, akcióik bemutatását és a toborzást is. Például csecsen terroristák weboldalukon közzétették egy lelőtt orosz gép képét, mivel Moszkva azt megelőzően tagadta ezt.[38] Érezhető a jelentős előrelépés, hiszen alig pár évtizede még csak otthon másolt kazettákon terjedhetett csak egy-egy szervezet ideológiája. A kommunikáció az internet igénybevételével nemcsak felgyorsult, de többirányúvá is vált, a magánkézben lévő nagy közösségi médiák pedig csak lassan reagáltak a terrorszervezetek megjelenésére. Az Iszlám Állam elsősorban a Twitter lehetőségeit használta ki, például a hashtagek használatával (#), amiknek a lényege, hogy az ezzel ellátott tartalmak együtt megtalálhatók és könnyen kereshetők, és így az aktuálisan felkapott témák közé a szervezet terrortámadásainak, lefejezéseinek képeit vegyítették. Ez annyira sikeresnek bizonyult, hogy 2014-ben a szervezet saját Twitter applikációt készített, amellyel ki tudták játszani a Twitter algoritmusait, és az azt telepítő felhasználók nevében üzeneteket küldeni.[39]

[37] Gillespie: i. m. 110. o.

[38] Warren, M. J.: Terrorism and the Internet. In: Janczewski, Lech J. – Colarik, Andrew M. (ed.): Cyber Warfare and Cyber Terrorism. Information Science Reference, 2008. 43. o.

[39] Besenyő János: Az Iszlám Állam. Terrorizmus 2.0. Kossuth Kiadó, Budapest, 2016. 157–161. o.

A pénzgyűjtés a terrorszervezetek működéséhez elengedhetetlen tevékenység, és már régóta bűncselekménynek számít a terrorizmus finanszírozása. Az internet számos lehetőséget kínál arra, hogy ezek a tevékenységek rejtve maradjanak a bűnüldöző hatóságok elől. Így például az Azzam Publications nevű oldal dzsihád témájú kiadványok árusításából juttatott összeget az Al-Kaida számára.[40] A terroristák számára más, a kiberpénzmosásban is használt eszközök is rendelkezésre állnak. Ilyenek például az online banki átutalások, a közvetítőkön, mint a PayPal keresztüli átutalások, a mobil fizetések és a különböző digitális pénzek, mint például a Bitcoin.[41] Ezeknél különösen nehéz ellenőrizni a tranzakciók végső címzettjét, és a több szereplőn keresztülfutó átutalások összege könnyedén számos kisebb összegre bontható, amelyek nem keltenek feltűnést.[42] A szervezetek adománygyűjtő számláira mutató elérhetőségeket pedig a közösségi médiában lehet könnyedén terjeszteni. Az online kaszinók szintén használhatók a terrorizmus finanszírozására.[43] Egy másik megoldás lehet, ha különböző kiberbűncselekmények elkövetéséből szereznek pénzt a szervezet működéséhez,[44] például zsarolóvírusok révén.[45]

Az információterjesztés abban különbözik a propagandától, hogy nem az embereket igyekszik megszólítani, hanem a terrorszervezet tagjai és szimpatizánsai számára közöl fontos tudnivalókat. Így például katonai mozgásokról, hogy elkerülhessék őket vagy a bombakészítés lépéseiről.[46] A már említett Azzam nevű weboldalon számos útmutató elérhető volt a dzsihád folytatásának módjaival kapcsolatosan.[47] A 87 halálos áldozattal járó 2016-os nizzai támadás elkövetője, Lahouaiej-Bouhlel is ilyen internetes forrásokból vette az ötletet az elkövetés módjához, a kamionnal történő tömegbe hajtáshoz.

A biztonságos kommunikáció azt az igényt szolgálja ki, hogy a terrorszervezetek tagjai a hatóságok számára láthatatlanul maradva tudják egymással a kapcsolatot fenn-

[40] Warren, M. J.: i. m. 43–44. o.
[41] Nagy Zoltán – Mezei Kitti: Pénzmosás a kibertérben. Infokommunikáció és jog. 2018/70. 27-28. o.
[42] Tropina, Tatiana: Fighting money laundering in the age of online banking, virtual currencies and internet gambling. ERA Forum, 2014/1. 73–77. o.
[43] Nagy Zoltán András – Mezei Kitti: The organised criminal phenomenon on the Internet. Journal of Eastern-European Criminal Law. 2016/2. 143. o.
[44] Hummel: i. m. 120–121. o.
[45] Lásd Nagy Zoltán András – Mezei Kitti: A zsarolóvírus és a botnet vírus, mint napjaink két legveszélyesebb számítógépes vírusa. In: Gaál Gyula – Hautzinger Zoltán (szerk.): Pécsi Határőr Közlemények XIX. Pécs, 2017.
[46] Gillespie: i. m. 111. o.
[47] Bozonelos, Dino – Stocking, Galen: The Effects of Counter-Terrorism on Cyberspace: A Case Study of Azzam.com. Journal of the Institute Of Justice & International Studies, 2003/3. 94. o.

tartani.[48] A CIA terrorelhárításért felelős vezetője szerint az internetes kommunikáció alapvetővé vált az Al-Kaida tagjai között, mivel ez nagyobb anonimitást biztosít nekik. Ebben igen fontos szerepe van a titkosításnak, amelyet az ezredforduló óta használnak egyre inkább.[49] Nagy segítséget nyújtanak számukra a kiberbűnözők által is előszeretettel használt „privát szférát erősítő technológiák".[50] Ilyenek például a virtuális magánhálózatok (VPN), amelyek segítségével a felhasználó könnyedén kaphat a világ bármely más országába mutató IP címet, illetve az Amerikai Egyesült Államok által katonai célokra kifejlesztett TOR (The Onion Router), amely igen nehezen feltörhető titkosítási módszerrel védi a kommunikáció tartalmát. A titkosításnak nemcsak a kommunikációban, hanem az adatok titkos tárolásában is szerepe lehet, így például a World Trade Center elleni 1993-as bombamerénylet kitervelője is ezzel a módszerrel élt.[51]

5. A kiberterrorizmus jellemzői

A kibertér sajátosságai jelentősen megkönnyítik a kiberbűnözők dolgát, és ilyenformán a potenciális kiberterroristákét is. Így például az internet globális jellege, amely nem teszi szükségessé, hogy személyesen is jelen legyenek az elkövetésnél. Hasonlóan fontos szempont az anonimitás is, hiszen lehetővé teszi, hogy maguk az elkövetők nehezen beazonosíthatók legyenek. Ráadásul az itteni működés sokkal olcsóbb, mint a tradicionális terror eszközei, és a lebukás esélye is jóval kisebb a támadást megelőzően. A támadáshoz nagyszámú célpont közül választhatnak, és ezek potenciálisan nagyobb számú ember életét képesek befolyásolni, mint egy hagyományos terrorcselekmény. Ebből eredő további előny az is, hogy jóval nehezebb védekezni a kibertámadásokkal szemben.[52] Ugyanakkor akadnak ellenérvek is az eszköz használata kapcsán, így például az, hogy megfelelő informatikai szaktudásra van szükség hozzá. Vagy a terroristák maguk szerzik meg ezt évek alatt vagy pedig már képzett hackerek segítségét veszik igénybe, de erősen kérdéses, hogy ők egyáltalán dolgoznának-e egy terrorszervezetnek.[53]

[48] MEZEY: i. m. 23. o.
[49] HUMMEL: i. m. 118. o.
[50] KISS Attila: A privátszférát erősítő technológiák. Infokommunikáció és jog 2013/56. 113–119. o.
[51] CASSIM: i. m. 385. o.
[52] MEZEY: i. m. 36–37. o.; OLEKSIEWICZ: i.m. 138–139. o.; valamint GYARAKI Réka: A számítógépes környezetben elkövetett gazdasági bűncselekmények. In: Gaál Gyula – Hautzinger Zoltán: Tanulmányok „A biztonság rendészettudományi dimenziói – változások és hatások" című tudományos konferenciáról. Pécsi Határőr Tudományos Közlemények XIII. Pécs, 2012. 235-236. o.
[53] GILLESPIE: i. m. 109. o.

A témával foglalkozó szakirodalom három fő fejlődési irányát különbözteti meg az informatikai terrorizmusnak: a tömeges pusztítást (weapon of mass destruction), a tömeges zavarkeltést (weapon of mass distraction) és a társadalmi rend szétzilálását (weapon of mass disruption).

A tömeges pusztítás a kritikus infrastruktúrát célzó támadásokat jelenti, amelyeknek célja a súlyos károkozás, például egy erőmű felrobbantása a rendszereinek a túlterhelésével. Ez Brenner megfogalmazásában csak elvi, és nem gyakorlati lehetőség, ami abból a téves feltételezésből ered, hogy a számítógépek képesek a 9/11-i terrortámadáshoz hasonló károkat okozni. Maguk a számítógépek ebben az esetben nem közvetlenül okoznak kárt, hanem csak elindítják az ahhoz vezető eseményeket. Brenner szerint azonban egy atomerőmű felrobbantására senki sem számítógépes terrorizmusként, hanem inkább nukleáris terrorizmusként emlékezne.[54]

A tömeges zavarkeltés fő célja a lakosság biztonságérzetének aláásása a kormányzatba vetett bizalom lerombolásának segítségével. Brenner szerint ilyen eredménnyel járhat, ha például egy hagyományos terrorcselekmény elkövetésének időpontjában mértékadó médiák weboldalait feltörik és azokon hamis információkat terjesztenek, vagy hamis közleményeket tesznek közzé kormányzati oldalakon. Ugyan ennek a pánikkeltő hatása erősen korlátozott, mégis növelheti a zavart a hagyományos támadás miatt egyébként is pszichológiai nyomás alatt lévő lakosság körében.[55] Ezzel a felhasználással kapcsolatban aggodalomra adnak okot az elmúlt évek álhírekkel kapcsolatos fejleményei, különösen például a 2016-os amerikai elnökválasztás tapasztalatai. Ugyan az álhírek terjesztése alapvetően a korábban már érintett propagandatevékenységet jelenti, az így elterjesztett hamis információknak súlyosabb társadalmi következményei is lehetnek, például abban az esetben, amikor egy amerikai férfi lövöldözni kezdett egy helyi pizzériában, mivel elhitte, hogy az valójában egy titkos gyerekmolesztáló hálózat része.[56]

A társadalmi rend szétzilálása esetén az elkövetők fő célja, hogy a civil lakosság társadalom működésébe vetett hitét rombolja, például közműszolgáltatások vagy más kritikus infrastruktúrák leállításával. Ebben az esetben nem a rendszerekben történő közvetlen károkozás a cél, hanem a társadalmi bizalom lerombolása.[57] Ugyanakkor ennek a gyakorlati hasznossága annyiban kérdéses, hogy például áramkimaradások terrorcselekményektől függetlenül is történnek, például 2005-ben öt-

[54] Brenner: i. m. 453–471. o.
[55] Brenner: i. m. 453–471. o.
[56] https://www.reuters.com/article/us-washingtondc-gunman/man-pleads-guilty-in-washington-pizzeria-shooting-over-fake-news-idUSKBN16V1XC [2018.06.23.]
[57] Brenner: i. m. 453–471. o.

ven millió amerikai maradt áram nélkül, így csak az igazán kirívó eseteknek lehet érezhető társadalmi hatása.[58]

6. Valós a fenyegetés?

Mint CONWAY nyomán GILLESPIE is rámutat, a kiberterrorizmus koncepciója a terrorizmustól és a technológiától való félelmet testesíti meg. A múltban a hackertámadásoktól való félelem volt képes hasonló reakció kiváltására, és néhányan odáig merészkednek, hogy „ítéletnapi forgatókönyveket" vázoljanak fel. A legsebezhetőbb kritikus infrastruktúrák – mint például a bankrendszer vagy az áramellátás – azonban nem kapcsolódnak az internethez, és így jóval nehezebb ezeket célzó kibertámadást indítani.[59] Azonban nem lehetetlen, mint azt a Stuxnet példája is mutatja, hiszen az iráni urándúsító üzem is internetkapcsolat nélkül működött, amit a beszállítók megfertőzésével tudtak megkerülni. Ugyanakkor a problémát hajlamosak sokan túlbecsülni, és az érzelemtől fűtött retorikát összekeverni a valóságos lehetőségekkel, ami egyébként is komoly probléma a kiberbűnözéssel kapcsolatos kommunikáció terén.[60] STOHL véleménye szerint a kiberterrorizmussal kapcsolatos fő aggályok a félelemből és tudatlanságból erednek.[61] MEZEY véleménye szerint a félelem mellett a bizonytalanság, a média szenzációhajhászása is a veszély túlbecsüléséhez vezettek.[62]

Csakugyan tény, hogy napjainkig egyetlen olyan jelentős kibertámadásra sem került sor, amit terrorszervezetek hajtottak volna végre. GILLESPIE abban látja a kiberterrorizmus elterjedésének fő gátját, hogy az egyszerűen nem elég „látványos" ahhoz, hogy a megfelelő hatást kiváltsa. Például egy áramkimaradás okozása nem jár olyan tömeglélektani hatásokkal, mint egy robbantás egy forgalmas helyen. Ráadásul a fizikai világban, még ha nem is sikerül egy támadás, úgy is képes zavart okozni, például egy forgalmas pályaudvar lezárásával. Ezzel szemben egy sikertelen kibertámadásnak aligha lehet ilyen hatása, sőt a célpont talán meg sem tudja, hogy támadást kíséreltek meg ellene.[63]

[58] GILLESPIE: i. m. 109. o.
[59] GILLESPIE: i. m. 108. o.
[60] WALL: i. m. 26–27. o.
[61] CASSIM: i. m. 387. o.
[62] MEZEY: i. m. 46. o.
[63] GILLESPIE: i. m. 109. o.

7. Válaszok a kihívásra

A kiberterrorizmussal kapcsolatos nemzetközi és állami válaszok szorosan összefüggnek a terrorizmusra adott válaszokkal, és azok nehézkes és kiforratlan rendszerével. Az ott meglévő problémák ennél a jelenségnél még élesebben kiütköznek, a kiber elemből fakadó jellemzőknek köszönhetően. A terrorizmussal nemzetközi egyezmények rendszere meglehetősen kusza, és szinte teljes egészében nemzeti hatáskörbe utalja a terrorizmus elleni fellépést, amely igen sok esetben nem vezet eredményre (politikai akarat hiánya, bukott államok), így pedig a szankció sem bír olyan elrettentő erővel.[64] A terrorizmus elleni küzdelem jelenlegi nemzetközi rendszere tehát nem olyan, amire támaszkodni lehetne a kiberterrorizmussal szemben. Ígéretesebb azonban a kiberbűncselekményekkel kapcsolatos szabályozás: a legszélesebb körben elfogadott egyezmény az Európa Tanács 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezménye, amely számos minimumszabályt tartalmaz a büntető anyagi és eljárási jog területén.

Anyagi jogi szempontból – mint arra már a fogalom kapcsán is kitértem – az EU terrorizmus elleni küzdelemről szóló 2017/541 irányelve már előírja a tagállamok számára, hogy a terrorizmus részeként kriminalizálják a kiberterrorizmust. Az Egyesült Királyságban a 2000. évi terrorizmusról szóló törvény bünteti az olyan támadásokat, amelyek az elektronikus rendszerekbe történő súlyos beavatkozásra vagy zavarásra irányulnak.[65] Ettől eltérő módon az Egyesült Államokban 2001-ben elfogadott hazafias törvény (PATRIOT Act) a kiberbűncselekmények között szabályozta a kiberterrorizmust. Ugyanígy a kiberterrorizmus elleni fellépést szolgálta az Obama elnök által 2015. április 1-jén aláírt 13694. számú elnöki rendelete, amelynek hármas célja volt, így a „rosszindulatú kiberszereplők" vagyonának zárolása; megakadályozni, hogy pénzhez jussanak; illetve belépésüket az Egyesült Államok területére. Azonban alkalmazására egyetlen alkalommal került csak sor, Oroszországgal szemben a 2016-os elnökválasztás befolyásolása miatt, ami alapvetően megkérdőjelezi, mennyire hasznos a kiberterrorizmus visszaszorításában.[66]

Eljárásjogi szempontból[67] a legkomolyabb problémák egyike az internet globális jellegéből fakad, és az ebből eredő joghatósági kérdésekből. A jelenlegi terrorizmus

[64] Dornfeld – Sántha: i. m. 99–100. o.

[65] Cassim: i. m. 390. o.

[66] Brunner, Jordan A.: The (Cyber) New Normal: Dissecting President Obama's Cyber National Emergeny. Jurimetrics, 2017/3. 398. o.

[67] Lásd kriminalisztikai aspektusok vizsgálatát Fenyvesi Csaba: Az új generációs bizonyítékok a kriminalisztika történeti mérföldköveinek tükrében. Magyar Jog 2014/7-8. 441-443. o.

elleni egyezmények az aut dedere aut judicare elvet vallják a magukénak, ám a hagyományos terrorizmussal szemben itt nem ismert az elkövető személye, így szintén nem alkalmazható. A kiberbűnözéssel kapcsolatos joghatósági kérdések vonatkozásában szupranacionális szinten, az EU-s joganyagban találunk iránymutatást. Az információs rendszerek elleni támadásokról szóló 2013/40/EU irányelv[68] 12. cikke az elkövetés helyét, illetve az állampolgárságot határozza meg, mint joghatósági okok, de lehetőséget ad a tagállamoknak, hogy megállapítsák joghatóságukat, ha a területükön található jogi személy javára történt az elkövetés, vagy pedig az elkövető szokásos tartózkodási helye a területükön van. Komoly hiányosság azonban, hogy az irányelv nem állapít meg sorrendiséget ezen joghatósági okok között, így lényegében a tagállami szerveknek kell erről megegyezniük. Akárcsak a terrorcselekményeknél, a kiberterrorizmusnál is az egyik legjelentősebb előrelépés az univerzális joghatóság megállapítása lenne.

A vizsgálódást a terroristák egyéb internetes tevékenységével kapcsolatos reakciókra is kiterjesztve megállapítható, hogy ezen a téren is szigorításokra került sor. Így például a Twitter a felületén az Iszlám Állam által kifejtett jelentős propagandatevékenységének visszaszorítására szigorított az addigi politikáján, ami komoly felületvesztéssel járt a szervezet számára.[69] Szabályozási szinten is számos törekvés született azzal kapcsolatban, hogy felléphessenek a terrorista tartalmat terjesztőkkel szemben. Számos államban, így például az Egyesült Királyságban, Spanyolország és Franciaországban bűncselekménnyé vált a „terrorizmus dicsőítése". A magyar jogrend a Btk. 331. § (2) bekezdés alapján háborús uszításként kriminalizálja a „nagy nyilvánosság előtt a terrorizmus támogatására uszítást, vagy egyébként a terrorizmust támogató hírverés folytatását". Hasonló úton jár az EU terrorizmus elleni küzdelemről szóló 2017/541 irányelve, amelynek 5. cikke szintén előírja a tagállamoknak a terrorcselekmények elkövetésére buzdító magatartások, így például a terrorizmus dicsőítésének kriminalizációját. Sokan azonban a gyakorlattal szemben foglalnak állást, például Ben Emmerson ENSZ különmegbízott is, aki a homályos megfogalmazásból eredő, és a szólásszabadságot potenciálisan korlátozó problémákra helyezi a hangsúlyt.[70]

Komoly erőfeszítések figyelhetők meg a titkosítás szabályozása terén is. Számos államban bűncselekménnyé vált megtagadni a titkosítást feloldó kulcs átadását a hatóságok számára.[71] A belga büntetőtörvénykönyv egy, míg a francia 434-15-2. szakasza három, illetve minősített esetben öt évig terjedő szabadságvesztéssel rendeli büntetni azt, aki meg-

[68] Az Európai Parlament és a Tanács 2013/40/EU irányelve (2013. augusztus 12.) az információs rendszerek elleni támadásokról és a 2005/222/IB tanácsi kerethatározat felváltásáról. HL 2013 L 218., 2013.8.14.
[69] Besenyő: i. m. 161. o.
[70] https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=17229 [2018.06.23.]
[71] Gillespie: i. m. 111. o.

tagadja a feloldáshoz szükséges kulcs átadását a hatóságoknak. Nagy-Britanniában a 2000. évi vizsgálati hatáskörök szabályozásáról szóló törvény 53. szakasza nemzetbiztonsági és gyermekeket érintő ügyekben 5 évig, egyéb estekben 2 évig terjedő szabadságvesztést helyez kilátásba, ha valaki megtagadja a titkosítást feloldó kulcs átadását. Ez azonban elég komoly aggályokat vet fel, és az önvádra kötelezés tilalmába ütköző lehet. Támogatói úgy érvelnek, hogy nem maga kulcs a terhelő, hanem az azzal védett információk, ilyenformán ez egy semleges adatnak tekintendő, akárcsak a vér vagy DNS minta.

Hazánkban a terrorellenes intézkedések részeként született meg a titkosított kommunikációt biztosító alkalmazásszolgáltatók és a titkos információgyűjtésre feljogosított szervezetek együttműködésének rendjéről szóló 185/2016. (VII. 13.) Kormányrendelet, amely előírja az alkalmazásszolgáltatóknak, hogy nem hajthatnak végre olyan fejlesztéseket, amelyek a titkos információgyűjtést kizárják vagy ellehetetlenítik. Ennek hatásai ugyanakkor kétségesek, hiszen az elkövetők számos külföldi fejlesztésű eszközt beszerezhetnek, amelyek fejlesztőire ezek a rendelkezések nem vonatkoznak. Elég csak egy egyszerű iPhone-ra gondolni, amelyen hamarosan bezárják az eddigi biztonsági réseket a fejlesztők, így a bűnüldöző és terrorelhárítási szervek sem ismerhetik meg a rajtuk tárolt adatok tartalmát.[72]

Összefoglalás

A kiberterrorizmus kapcsán igen élénk diskurzus folyt nemcsak a jogtudományban, de a médiában és a társadalomban is az elmúlt évtizedekben. A 2001-es terrortámadásokat követően sokan tartottak attól, hogy a terrorizmus könnyedén új erőt meríthet a kibertér kiaknázásából, és a terroristák ezen keresztül indíthatnak újabb és még pusztítóbb támadásokat. A jelenséggel kapcsolatban hamar a pesszimista hangok váltak uralkodóvá, például az Egyesült Államok 2002-es kiberbiztonsági gyakorlatát „digitális Pearl Harbor" névre keresztelte, míg hazai vonatkozásban a „digitális Mohács" kifejezés jelent meg.[73] Az új technológia jelentette veszélyek már régóta mozgatják az emberek fantáziáját, és az ezektől való félelem számos film, könyv, videojáték témájává is vált.

A 2001. szeptember 11. óta eltelt években mind a mai napig nem került sor jelentős kiberterrorista támadásra sehol a világon, ami véleményem szerint azt mutatja, hogy a jelenséggel kapcsolatos félelmek túlzóak voltak. Ugyan képes lehet egy

[72] https://apnews.com/8b23b35b73684c3d90f739c90949146f/Apple-closing-iPhone-security-gap-used-by-law-enforcement [2018.06.23.]

[73] Kovács László – Krasznay Csaba: Digitális Mohács. Egy kibertámadási forgatókönyv Magyarország ellen. 2010/2.

csoport egy állam digitális működésében súlyos fennakadásokat okozni, mint Észtország esetén 2007-ben az orosz hackerek, ennek lélektani hatása korántsem azonos egy terrorcselekményével. Észtország esete korántsem vált ki olyan erős érzelmi reakciót, mint a New York-i ikertornyok leomlását bemutató képek, hiszen előbbi jóval megfoghatatlanabb, mint a fizikai rombolás. Így bár elméletben a kiberterrorizmus sokkal jelentősebb veszély a hagyományos terrorizmusnál, a valóság egyelőre látványosan nem kíván igazodni ehhez a felvetéshez. A terrorizmus jövőbeli tendenciáit vizsgáló kutatások is elsősorban a hagyományos eszközökkel elkövetett terrortámadások számának további növekedésével számolnak.[74]

A kiberterrorizmus kapcsán alkalmazható az a régi mondás, hogy „jobb félni, mint megijedni", vagyis az államoknak készen kell állniuk arra, hogy megvédjék polgáraikat a kibertérből érkező terrorfenyegetésekkel szemben. Napjainkra egyre több jogrendszer kriminalizálta a kiberterrorizmust – vagy a kiberbűnözés vagy a terrorizmus részeként –, és a kibervédelmet ellátó szervek és incidenskezelő központok is egyre hatékonyabban működnek. Jelenleg az állami támadások a leginkább jellemzők, amelyek célja vagy a kémkedés vagy az ellenfél védelmének tesztelése.

A kiberterrorizmusról szóló diskurzus kapcsán sokszor kevéssé kap helyet a terroristák egyéb internetes tevékenységének vizsgálata, amely talán a legkomolyabb negatív hozadéka a kiberterrorizmus veszélyessége túlértékelésének. Ezek jóval kevésbé ijesztő tevékenységek, mint például egy erőmű felrobbantása, de véleményem szerint jóval veszélyesebbek. Az elmúlt évek nyugat-európai terrortámadásaiban jelentős szerepet játszott a terroristák internetes kommunikációja, az aktív dzsihadista propaganda és persze azok a pénzügyi támogatások, amelyeket a terrorszervezetek az internet segítségével szereztek meg. Véleményem szerint ez egy olyan téma, amivel szemben a jövőben még keményebben kell fellépnie a nemzetközi közösségnek.

Felhasznált Irodalom

Berki Gábor: Kiberháborúk, kiberkonfliktusok. In: Pintér István (szerk.): A virtuális tér geopolitikája. Geopolitikai Tanács, 2016.

Besenyő János: Az Iszlám Állam. Terrorizmus 2.0. Kossuth Kiadó, Budapest, 2016.

Bozonelos, Dino – Stocking, Galen: The Effects of Counter-Terrorism on Cyberspace: A Case Study of Azzam.com. Journal of the Institute Of Justice & International Studies, 2003/3.

[74] Ritecz György – Sárkány István: A jövő terrorizmusa. Belügyi Szemle, 2013/6. sz. 22. o.

BRENNER, W. Susan: Cybercrime, Cyberterrorism and Cyberwarfare. Revue internationale de droit pénal, 2006/3.
BRUNNER, Jordan A.: The (Cyber) New Normal: Dissecting President Obama's Cyber National Emergeny. Jurimetrics, 2017/3.
BUONO, Laviero: Gearing Up the Fight Against Cybercrime in the European Union: A New Set of Rules and Establishment of the European Cybercrime Centre (EC3). New Journal of European Criminal Law, 2012/3.
CASSIM, F.: Addressing The Spectre of Cyber Terrorism: A Comparative Perspective. Potchefstroom Electronic Law Journal, 2012.
DENNING, D. E. : Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. In: J. Arguilla, D. Ronfeldt (ed.) = Networks and Netwars: The Future of Terror, Crime, and Militancy. 2001.
DORNFELD László – SÁNTHA Ferenc: A terrorizmus és a terrorcselekmény, mint nemzetközi bűncselekmény aktuális kérdései. Jog Állam Politika 2017/3.
EICHENSEHR, Kristen E.: The Cyber-Law of Nations. Georgetown Law Journal, 2015/2.
Environmental Risks: Cyber Security and Critical Industries.
FENYVESI Csaba: Az új generációs bizonyítékok a kriminalisztika történeti mérföldköveinek tükrében. Magyar Jog 2014/7-8.
GILLESPIE, Alisdair A.: Cybercrime – Key Issues and Debates. Routledge, 2016.
GYARAKI Réka: A számítógépes környezetben elkövetett gazdasági bűncselekmények. In: Gaál Gyula – Hautzinger Zoltán: Tanulmányok „A biztonság rendészettudományi dimenziói – változások és hatások" című tudományos konferenciáról. Pécsi Határőr Tudományos Közlemények XIII. Pécs, 2012.
HOLT, Thomas J. – BOSSLER, Adam M. – SEIGFRIED-SPELLAR, Kathryn C.: Cybercrime and digital forensics: An introduction. Routledge, 2018.
HUMMEL, Michael L.: Internet Terrorism. Homeland Security Review 2/2008.
ILLIG, A. T.: Computer Age Protesting: Why Hacktivism is a Viable Option for Modem Social Activists. Penn State Law Review, ?/2015.
KISS Attila: A privátszférát erősítő technológiák. Infokommunikáció és jog 2013/56.
KOVÁCS László – KRASZNAY Csaba: Digitális Mohács. Egy kibertámadási forgatókönyv Magyarország ellen. 2010/2.
LUKÁCSI Tamás: A terrorizmus elleni küzdelemről szóló (EU) 2017/541 európai parlamenti és tanácsi irányelv. Európai Jog 2017/6.
MARAS, Marie-Helen: Cybercriminology. Oxford University Press. New York, 2017.
MATUSITZ, Jonathan: Terrorism & Communication. A Critical Introduction. Thousand Oaks, SAGE Publications, 2013.
MEZEI Kitti: A DDoS-támadások büntetőjogi szabályozása az Egyesült Államokban, Európában és Magyarországon. Pro Futuro 2018/1.

MEZEY Nándor Lajos: Kiberterrorizmus: valós veszély? Belügyi Szemle, 2011/2.
NAGY Zoltán – MEZEI Kitti: Pénzmosás a kibertérben. Infokommunikáció és jog. 2018/70.
NAGY Zoltán András – MEZEI Kitti: A zsarolóvírus és a botnet vírus, mint napjaink két legveszélyesebb számítógépes vírusa. In: Gaál Gyula – Hautzinger Zoltán (szerk.): Pécsi Határőr Közlemények XIX. Pécs, 2017.
NAGY Zoltán András – MEZEI Kitti: The organised criminal phenomenon on the Internet. Journal of Eastern-European Criminal Law. 2016/2.
NAGY Zoltán András: A kiber-háború új dimenzió – a veszélyeztett állambiztonság (Stuxnet, DuQu, Flame – a Police malware). In: Gaál Gyula – Hautzinger Zoltán: Pécsi Határőr Tudományos Közlemények XIII. 2012.
OLEKSIEWICZ, Izabela: Dilemmas and Challenges for EU Anti-Cyberterrorism Policy: The Example of the United Kingdom. Teka Kom. Politol. Stos. Międzynar. 2016/3.
PARTI Katalin: Kerekasztal-beszélgetés az online terrorizmusról. Ügyészek Lapja, 2010/2.
PATAKI Márta – KELEMEN Roland: Kiberterrorizmus. A terrorizmus új arca. Magyar Rendészet 2014/5.
PINTÉR István: A virtuális tér geopolitikája. In: PINTÉR István (szerk.) A virtuális tér geopolitikája. Geopolitikai Tanács, 2016.
RITECZ György – SÁRKÁNY István: A jövő terrorizmusa. Belügyi Szemle, 2013/6. sz.
SIMON Béla: Hacktivism and Its Status in Hungary. Magyar Rendészet 2016/2.
SIPOS Zoltán: A kibertér biztonságával kapcsolatos alapvető kérdések áttekintése. Honvédségi Szemle, 2016/1.
SZATHMÁRY Zoltán: Bűnözés az információs társadalomban – Alkotmányos büntetőjogi dilemmák az információs társadalomban. PhD értekezés. Budapest, 2012.
TROPINA, Tatiana: Fighting money laundering in the age of online banking, virtual currencies and internet gambling. ERA Forum, 2014/1.
WALL, David S.: Cybercrime: The Transformation of Crime in the Information Age. Polity, 2007.
WARREN, M. J.: Terrorism and the Internet. In: JANCZEWSKI, Lech J. – COLARIK, Andrew M. (ed.): Cyber Warfare and Cyber Terrorism. Information Science Reference, 2008.