Gál István – Bartkó Róbert

A kibertérben megjelenő kihívások és fenyegetések büntetőjogi kezelésének tendenciái

Military and Intelligence CyberSecurity Research Paper
2022/12.

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROGRAM


UNIVERSITY OF PUBLIC SERVICE
LUDOVIKA

A kibertérben megjelenő kihívások és fenyegetések büntetőjogi kezelésének tendenciái[1] témakörön belül elsősorban a terrorizmussal, illetve a terrorizmus finanszírozásával foglalkozunk e tanulmány keretein beül; valamennyi kihívás és fenyegetés büntetőjogi vonatkozásainak bemutatására egy kismonográfia terjedelmi keretei sem lennének elegendők.

A terrorizmusnak mind a hagyományos, mind az online térben terjedő formái számos biztonságpolitikai kérdést vetnek fel, egyúttal azonban a büntetőjog számára is generálnak szinte feloldhatatlannak tűnő dilemmákat. Ezek közül egyet megemlítve, a terrorizmus egyik legveszélyesebb fajtája, az öngyilkos merénylet a hagyományos büntetőjogot megoldhatatlan probléma elé állítja napjainkban. A büntetőjognak ugyanis az egyik kiindulópontja az, hogy a kilátásba helyezett szankciónak van – több vagy kevesebb – visszatartó hatása. A visszatartó hatás egészen pontosan két tényezőtől függ egy adott bűncselekmény elkövetője tekintetében: a kilátásba helyezett szankció súlyosságától és az adott bűncselekmény felderítési mutatójától. (Rögtön hozzá is tehetnénk, hogy Beccaria szerint a második tényező a hangsúlyosabb, azaz a visszatartó hatás nem a büntetés súlyosságától, hanem annak elmaradhatatlanságától várható, de ez a kérdés a vizsgált téma szempontjából nem sok relevanciával bír.)

A nagy probléma az, hogy az öngyilkos merénylőt hogyan tartsuk vissza? Még ha a legsúlyosabb büntetést helyeznénk is kilátásba, lenne-e visszatartó ereje annak, ha kijelentjük: az elfogott öngyilkos merénylők halálbüntetésre számíthatnak? Van-e visszatartó ereje annak, ha az öngyilkos merénylő ezzel számolhat? Vagy ha esetleg azt is be kell kalkulálnia, hogy az akció végrehajtása közben lelövik? Véleményem szerint egyáltalán nincs! *Az öngyilkos merénylőt a büntetőjog jelenlegi eszköztárával nem lehet visszatartani, egyszerűen azért, mert neki nincs veszítenivalója.* A legtöbb, amit veszíthet, hogy nem a tervezett helyen és időben, hanem pár kilométerrel arrébb és kicsit korábban vagy később hal meg.

A büntetőjog tehát egyszerűen csődöt mond az egyik legsúlyosabb modern bűnözési formával szemben! Ezzel a szituációval bizonyos értelemben analógiát mutat a kibertérben elkövetett terrorizmus és a terrorizmus finanszírozása elleni büntetőjogi és büntetőjogon kívüli jogszabályok hatékonyságának a problémaköre.

A múlt század végén a terrorizmus alapvető motivációja az anarchizmus és a nacionalizmus volt - s noha a jelenkor terrorizmusa számára ez csak történelem, eszmeviláguk több alkotóeleme is felbukkan a későbbi korszak terrorcselekményeinek indoklásában, illetve szolgált motivációként. Más volt az

[1] A mű a Katonai Nemzetbiztonsági Szolgálat TKP2021-NVA-24 azonosító számú „A mesterséges intelligencia alkalmazásának kutatása a katonai nemzetbiztonsági célú adatszerző, adatfeldolgozó és vizualizációs eljárásokban, és kapcsolódó fejlesztések elvégzése” elnevezésű projektje keretében, az Innovációs és Technológiai Minisztérium Nemzeti Kutatási Fejlesztési és Innovációs Alapból nyújtott támogatásával valósult meg.

eszközrendszerük is- tőr, méreg, pokolgép – a századfordulón merényletek sorozatát követték el, államfők és uralkodók ellen-kezdve a sort Carnot francia elnökkel, folytatva egészen Erzsébet királynééig.[2]

Ettől függetlenül kijelenthetjük, hogy maga a terrorizmus jellegzetesen huszadik századi jelenség, és komolyabb problémaként először csak a második világháborút követő időszakban jelentkezett, főként három földrajzi térségben: Nyugat-Európában, Közel-Keleten és Latin-Amerikában.

„A terrorizmus eltérő eszmerendszerekből merítő, sajátos logikának engedelmeskedő, változatos formákat öltő módszeres erőszak-alkalmazás, vagy ezzel való fenyegetés, melynek célja politikai törekvések elérése azáltal, hogy az áldozatban, a nézőközönségben, az államban, a társadalomban megalkuvó magatartás alakuljon ki. A meghirdetett cél általában politikai, ideológiai, vallási, etniaki stb. tartalmú radikális változás kikényszerítése, a cél elérésére alkalmazott cselekménysor. Az eszköz viszont jogi lényegét tekintve köztörvényes, erőszakos bűncselekmény."[3]

A jövő legfontosabb kihívásai a nukleáris terrorizmus, az ökoterrorizmus, a biológiai terrorizmus, a kibertérben elkövetett terrorizmus, és egyre komolyabb problémaként kell számolni a vallási alapon szerveződött radikális terrorcsoportok tevékenységével.

A terrorizmussal foglalkozó tanulmányok megegyeznek abban, hogy a terrorizmus alapvetően politikai jelenség, amely mögött strukturális és pszichológiai tényezők egyaránt vannak. Általános vélekedés, hogy a modernizáció, a demokrácia és a kezeletlen szociális feszültségek teremthetnek olyan feltételeket, amelyek életre hívják a terrorizmust.

A terrorcselekmények veszélyessége a váratlanságban, a kiszámíthatatlanságban és a gyors, mobil csapásmérő képességben rejlik. A régi korok klasszikus és jelenkor terrorizmusa között elsősorban minőségi a változás, de a legfontosabb különbségek mégis a történelmi fejlődésből alakultak ki.[4]

Ahogy a terrorizmus mai modern formájának sincsenek évszázados gyökerei, még erőltetettebb a terrorizmus elleni küzdelem jogtörténetéről beszélni. Ennek előrebocsátása után idézünk egy száztíz éves jogesetet, amelyet a saját korában állam elleni bűncselekménynek minősítettek, de talán a terrorizmus finanszírozása kriminológiai értelemben vett fogalmának egyik korai megnyilvánulási formájának is tekinthetjük:

„M. I. félrevezettetvén a szoczialisták izgatásaitól, és a megtévesztett munkás-elemek általános elégületlenségétől, és félreismerve az állami és társadalmi rend fenntartó s éltető intézményeit, arra a gondolatra jutott, hogy a munkásosztálybeliek helyzete a jobb sorsban levőkkel szemben visszás, a minek a jelenlegi állami rend az oka: ezt megváltoztatni, vagy megbosszulhatni vélte azzal, ha a koronás király élete ellen

[2] Szövényi György: A terrorizmus jellegzetességei az ezredfordulón. *Európai Tükör*, 1998/3. szám, 92. o.
[3] Korinek László: A terrorizmus. Gönczöl Katalin – Kerezsi Klára – Korinek László – Lévay Miklós (szerk.): *Kriminológia-Szakkriminológia*. Budapest, CompLex kiadó, 2006, 447. o.
[4] Gergely Attila: A terrorizmus természetrajza. *Kapu*, 1994/10-11. szám, 92. o.

merényletet tervez és merényletét sikerrel követi el. Elhatározta tehát, hogy a királyt megöli. Miután azonban e tervhez társra volt szüksége, ilyent keresett és talált is a hozzá hasonló H. L. személyében. M. I. és H. L. együtt megbeszélték a tervet, hogy a királyt dinamitrobbantással kellene elpusztítani, amire alkalmas a Margit-körúti csatornavonal, melyet mindketten ismertek. A dinamitot keresetükből kívánták beszerezni. Mivel azonban annyi keresetük nem volt, hogy e czélra megfelelő összeget fordíthattak volna, M. I. egy olyan embert keresett, a ki a szükséges pénzt vagy a robbantó szert megszerezheti. K. Gy.-t mindketten a közvágóhídnál folyt csatornamunkálatok idejéből ismerték: tudták, hogy ez híve V. I.-nek, kinek izgatásairól hallottak; azt is tudták, hogy V. I. gazdag ember, és gondolták, hogy bűnös czéljukra K. Gy útján a szükséges anyagi eszközöket megszerezhetik. Közölték tehát a tervet K. Gy-val, aki azt helyeselte és 500 frtnak szerzését helyezte kilátásba. Így szövetkeztek M. I., H. L. és K. Gy. mindhárman együtt 1898. évnek elején arra, hogy Ő Felségét, a királyt életétől megfosszák. A tervet mindhárman megbeszélték, annak dinamitrobbantás útján történő keresztülvitelét tárgyalták egy oly vonalon, amelyen a király Budapesten időzése alkalmával elhaladni fog. A terv azonban a részletes megvalósítás stádiumába nem került: vádlottak előkészületeket nem tettek, pusztán szövetségre léptek egymással a király élete elleni merénylet czéljából."[5]

A XIX. század végén Sztálin és társai oroszországi akcióikhoz bankrablásokból teremtették elő a szükséges pénzt, a XX. század második felében a Baader-Meinhof csoport[6] tagjai is hasonló módszerekkel jutottak anyagi eszközökhöz. Mára ez a fajta finanszírozás kivételnek számít, ahogy erre Korinek László is rámutat.[7] Napjaink terroristái szívesebben nyúlnak a szervezett bűnözés kipróbált megoldásaihoz, valamint a kibertérben is keresnek finanszírozási forrásokat.

TERRORIZMUS A KIBERTÉRBEN

Az elmúlt század '60-as éveitől kezdődő modernizációs és globalizációs törekvések egy egységes térré törekedtek formálni az addig bipoláris módon felépített világrendünket. Az említett folyamatok a terrorizmus történetében is meghatározó jelentőségűek, hiszen azok kölcsönhatásában[8] a terrorizmus úgy vált posztmodern korunk szerves részévé, hogy idomulva ahhoz, az transznacionálissá és sok esetben virtuálissá is vált.[9] Ezáltal pedig kihasználhatta az indusztriális és információs társadalomban rejlő lehetőségeket. Ebben a formálódásban, „fejlődésben" jelentős szerepet játszott az informatika, fejlődése, a technológia új vívmányainak megjelenése, az internet

[5] Edvi Illés Károly: *Az anyagi büntető törvények és a sajtótörvény.* Budapest, Grill Károly Könyvkiadó Vállalata, 1907, 217. o.
[6] Ld. részletesen: Gerhard Wisnewski – Wolfgang Landgraeber – Ekkehard Sieker: *Das RAF-Phantom Neue Ermittlungen in Sachen Terror.* München, Knaur Taschenbuch Verlag, 2008, 512. o.
[7] Korinek: i. m. (2006), 455. o.
[8] A terrorizmus és a globalizáció kapcsolatára vonatkozóan lásd bővebben: Bartkó Róbert: *A terrorizmus elleni küzdelem kriminálpolitikai kérdései.* Győr, UNIVERSITAS-Győr Nonprofit Kft, 2011, 70–79. o.
[9] Rostoványi Zsolt: Terrorizmus és szabadság. Fundamentum, 2001/4. szám, 56. o.

világméretűvé válása is, mely a terrorista hadviselés számára egyértelműen új távlatokat nyitott. Az ún. konvencionális terrorizmus mellett „a paletta színesedett" a tömegpusztító fegyvereket alkalmazó, valamint a számítógépes terrorizmussal is[10] (összefoglaló nevén: „ABC - Terrorizmus"), utóbbi pedig a kibertérben rejlő lehetőségeket is kiaknázta.

Az információ áramlásának új, az internetnek is köszönhetően felgyorsult módja egyrészt gyökeresen alakította át, és vélhetően a jövőben tovább is fogja formálni a biztonságpolitikai kihívásokat, és az azokra adott válaszokat,[11] ideértve természetesen a jogi természetű válaszokat is,[12] másrészt erősítette a nemzetközi terrorizmus egyik fő ismertetőjegyét, a láthatatlanságot[13] is.

A terrorizmus a maga „régi, hagyományos formájában" közvetlenül a minket körülvevő társadalom feszültségeire reagált, a kriminalitás ezen természete pedig nem változott semmit a technológiai fejlődéssel sem. A technológia, amely – *Kelemen Roland* álláspontját osztva - alapvetően egy olyan szociális konstrukció, mely révén a hagyományos tér folyamatai összefonódnak a kibertér folyamataival, fejlődésének eredményeként a hagyományos társadalmi konfliktusok a kibertér belső rendszerében is megjelentek,[14] lehetőséget és teret adott és ad mind a mai napig a büntetőjog terrénumához tartozó extrémitásoknak, azok térnyerésének.

Más kriminalitáshoz hasonlóan a technológia innovációi, az internet, az okos eszközök, az információs hálózatok használatának fejlődése,[15] a digitális kommunikáció egyre változatosabb csatornái[16] a terrorizmus tekintetében is új elkövetési módokat alakítottak ki, és bővült azoknak a cselekményeknek a köre, mellyel szemben az anyagi büntetőjognak is szükséges fellépnie.

Elfogadva a szakirodalmi álláspontot, a terrorizmus megjelenése a kibertérben alapvetően két síkon értelmezhető. Egyrészt a tulajdonképpeni, szűkebb értelemben vett kiberterrorizmus, vagy számítógépes terrorizmus síkján, másrészt a terroristák, terrorista szervezetek egyéb internetes tevékenysége[17]

[10] Ld erről a kérdésről bővebben: Korinek László: *Kriminológia.* Budapest, Magyar Közlöny Lap- és Könyvkiadó Kft, 2010, 413. o.

[11] A XXI. századi biztonsági kihívásokról lásd bővebben Farkas Ádám: Gondolatok a 21. századi biztonságról, államról, védelemről. *Hadtudomány*, 2018/elektronikus szám, 241–256. o.

[12] A modern technológiai vívmányok jogi kihívásai tekintetében lásd: Nagy Zoltán András: A jövő tegnap óta tart. A modern technikai-technológiai folyamatok kihívásai a jog területén. *Belügyi Szemle*, 2018/10. szám, 36–55.o.

[13] A modern kori terrorizmus főbb ismérvei tekintetében lásd: Bartkó: i. m. (2011), 67. o.

[14] Kelemen Roland: A kibertérből érkező fenyegetések jelentősége a hibrid konfliktusokban és azok várható fejlődése. *Honvédségi Szemle*, 2020/4. szám, 70. o.

[15] Mezei Kitti: A modern technológiák kihívásai a büntetőjogban, különös tekintettel a kiberbűnözésre. *Állam-és Jogtudomány*, 2020/4. szám, 66. o.

[16] Mezei Kitti – Szentgáli-Tóth Boldizsár: Az online platformok használatában rejlő veszélyek: a dezinformáció és a kibertámadások jogi kockázatai. In. Chronowski Nóra – Szentgáli-Tóth Boldizsár – Szilágyi Emese (szerk.): *Demokrácia – Dilemmák. Alkotmányjogi elemzések a demokráciaelv értelmezéséről az Európai Unióban és Magyarországon.* Budapest, ELTE Eötvös Kiadó, 2022, 241. o.; Kelemen Roland: Radikalizálás, dezinformálás és tömegpszichózis modern köntösben: a hibrid konfliktus kibertérben. *Jog Állam Politika,* 2021/3. szám, 75–77. o.

[17] Neparáczki Anna Viktória az előbbit az információtechnológia „hard" típusú, míg a második az ún. „soft" típusú felhasználásaként jelöli meg

vonatkozásában.[18] Előbbi a kibertérben, annak felhasználásával elkövetett terrorista akciókra utal, míg utóbbi olyan célokra fókuszál, melyek részben konkrét törvényi tényállások szintjén is értékelt a jogalkotók által, részben pedig olyan „büntetlen cselekmények", melyek akár a szervezet létezéséhez, működéséhez, akár későbbi akciók végrehajtásához kapcsolódhatnak. *Alisdar A. Gillespie nyomán Dornfeld László* ezeket a célokat az alábbiakban foglalja össze:[19] a terrorista propaganda térnyerésének biztosítása; a pénzgyűjtés; az információ-terjesztés, valamint a biztonságos kommunikáció és hírszerzés.[20]

A nemzetközi terrorizmus ezen megváltozott, összetett jellege nemcsak a katonai, biztonságpolitikai, de a (büntető) jogi válaszok terén is újabb kihívást jelentett a demokratikus jogállamok számára, az egységes fellépés szándéka azonban az utóbbi évtized jogalkotási fejlődésében – főként az Európai Unió szintjén – egyértelműen tetten érhető. A kibertérben megvalósuló terrorista aktivitásokkal szembeni fellépés szükségességét a közelmúlt migrációs eseményei, és az annak nyomán megvalósult terrorista akciók, a támadások legitim voltát igazoló elvek, azaz a propaganda szélesebb körben történő terjesztése is indokolták. Ezek a folyamatok rámutattak arra az európai integráción belül is, hogy a nagyrészt liberálisnak tekinthető migrációs politika komoly biztonsági deficitet okozhat.[21] Az említett migrációs nyomás okozta megingott biztonsági környezet a kibertér, az internet adta lehetőségek mellett az egyes terrorszervezetek számára komoly hálózatépítési, hálózatfejlesztési lehetőségeket teremtett.[22]

A tanulmány jelen szerkezeti egységének ezért az a célja, hogy bemutassa, hogy a hazai büntetőjog – figyelemmel az Európai Unió által is támasztott elvárásokra - hogyan próbál fellépni a kibertérben megjelenő terrorizmussal szemben. Azaz célunk nem a fogalomalkotás, hiszen ennek a kérdésnek hazánkban alapvetően kiforrott szakirodalma van.[23] Elemzésünk során inkább a kiberterrorizmushoz kapcsolódó

munkájában. Ld ezzel kapcsolatban: Neparáczki Anna Viktória: A kiberterrorizmus büntető anyagi jogi megítélése. *Ügyészek Lapja,* 2020/1. szám, 71–85. o.

[18] Dornfeld László: Kiberterrorizmus – a jövő terrorizmusa? In. Mezei Kitti (szerk.): *A bűnügyi tudományok és az informatika.* Pécs, Budapest, PTE ÁJK – MTA Társadalomtudományi Kutatóközpont, 2019, 53. o.

[19] Dornfeld: i. m. (2019), 53. o.

[20] Ha megvizsgáljuk az egyes célokat, könnyen belátható a tézis igazolt volta. A propaganda rendkívül fontos a terroristák és a terrorszervezetek szempontjából, hiszen személyi bázisuk fejlesztésére és a megfélemlítési célzat hatékonyabb közvetítésére is alkalmas. Ugyanez mondható el a pénz-, és információgyűjtési célzatról is, melyek szintén fontos a terrorszervezetek és csoportok létrehozása, működtetése, az egyes akciók előkészítése szempontjából. A biztonságos kommunikáció és a hírszerzés pedig annak záloga, hogy ezen szervezetek a hatóságok előtt észrevétlenek tudjanak maradni, akár konspiratív jellegüket is erősíthetik.

[21] Böröcz Miklós: Az Európai Unió közös kül-, és biztonságpolitikájának néhány főbb kihívása napjainkban. *Terror & Elhárítás*, 2013/2. szám, 81. o.

[22] Migráció és terrorizmus kapcsolata tekintetében lásd bővebben: Bartkó Róbert: *Az irreguláris migráció elleni küzdelem eszközei a hazai büntetőjogban.* Budapest, Gondolat Kiadó, 2019, 128–147. o.

[23] Ld ebben a körben az alábbi fontosabb hazai munkákat: Neparáczki: i. m. (2020); Nagy Zoltán András: Kiberbűncselekmények, kiberháború, kiberterrorizmus – avagy ébresztő Magyarország! *Magyar Jog*, 2016/1. szám, 17–24. o.; Szádeczky Tamás: Terrorizmus a kibertérben. *Infokommunikáció és Jog,* 2008/5. szám, 200–205. o.; Mezei Kitti: *A kiberbűnözés aktuális kihívásai a büntetőjogban.* Budapest, TKJTI, L'Hartmann, 2020.; Lajtár István: A kiberbűnözésről.

jelenségek büntető anyagi jogi vetületeire koncentrálunk majd, illetve kitérünk azokra a területekre, magatartásokra is, melyek „szürke foltként" értékelhetők a kriminalizáció folyamatában. Nem célunk ugyanakkor a kiberbűnözéssel általános, elméleti szinten foglalkozni, hiszen az, annak számtalan területe révén, szétfeszítené a tanulmány e részének célját és kereteit, ezért kifejezetten csak anyagi büntetőjogi kérdésekre fókuszálunk. Az elemzés során külön értékeljük hazánk anyagi jogi fellépését a tulajdonképpeni kiberterrorista cselekmények, valamint a terroristák egyéb internet-használati cselekményei esetében.

A KIBERTERRORIZMUS KRIMINALIZÁLÁSA A HAZAI BÜNTETŐJOGBAN

Az Európai Parlament 2017. február 16. napján fogadta el a terrorizmus elleni uniós szintű küzdelem módosított jogi kereteit megfogalmazó 2017/541 számú Irányelvet (a továbbiakban: Irányelv), mely jelenleg az Európai Unió valamennyi tagállama számára – felváltva a korábbi kerethatározati szabályozási rendszert – a fellépés fundamentális kereteit rögzíti. Az Irányelv célja, hogy szélesítse a büntetendővé nyilvánítandó cselekmények körét, külön kiemelve annak a követelményét, hogy a tagállamoknak az interneten történő elkövetéssel szemben is biztosítaniuk kell az anyagi büntetőjogi fellépés lehetőségét.[24]

Az Európai Unió ezen jogalkotási lépése illeszkedik ahhoz a folyamathoz is, amely a terrorizmus elleni tagállami fellépésben a büntetőjogi eszközök mellett a közjogi és védelmi jellegű eszközök megerősítését is célozta.[25]

Az Európai Unió már több jogi dokumentumában, így az irányelvben is rögzítette, hogy a terrorcselekmények jelentik a legsúlyosabb támadást az Unió alapértékeinek tekinthető jogállamiság és demokrácia ellen.[26] Mint hogy a terrorizmus súlyos fokban veszélyezteti az Unió által képviselt demokratikus értékeket,

Ügyészek Lapja 2019/1. szám, 47–52. o.; Ambrus István: *Digitalizáció és büntetőjog*. Budapest, Wolters Kluwer Hungary Kft, 2021.; Mezei Kitti: Cyberterrorism – How real is the threat? In.: Szőke Gergely László (szerk.): *Studia Iuridica Auctoritate Universitatis Pécs Publicata. Essays of Faculty of Law University of Pécs Yearbook of 2017-2018*. Pécs, Pécsi Tudományegyetem, 2020, 59–75. o.

[24] Az Irányelv a Preambulum (6) bekezdésében utal arra, hogy a büntetendővé nyilvánítandó magatartások büntetni rendeltségét akkor is biztosítani kell, ha az interneten keresztül, vagy a közösségi média felületek közbeiktatásával kerülnek elkövetésre, míg a (11) bekezdés a toborzás, kiképzés, a (22) bekezdés pedig a nyilvános uszítást megformáló online tartalmakkal szembeni fellépések körében támaszt ilyen követelményeket.

[25] Lásd ezzel kapcsolatban a hazai szakirodalomban: Simicskó István (2016): A terrorizmus elleni védelem fokozása a különleges jogrendi kategóriák bővítésével. *Hadtudomány*, 3-4. szám, 100–113. o.; Farkas Ádám: A terrorizmus elleni harc, mint kiemelt ágazatközi fegyveres védelmi feladat. *Szakmai Szemle*, 2017/3. szám, 5–20. o.; Farkas Ádám: Gondolatok a terrorveszélyhelyzetről. *Szakmai Szemle*, 2016/3. szám, 174–189. o.; Kelemen Roland – Németh Richárd: A kibertér fogalmának és jellemzőinek multidiszciplináris megközelítése. In: Farkas Ádám (szerk.): *Védelmi alkotmányosság az új típusú biztonsági kihívások erőterében*. Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2018, 147–169. o.; Kelemen Roland: Pillanatképek a kivételes állapot elméleti kérdéseinek köréből. *Katonai Jogi és Hadijogi Szemle*, 2016/1-2. szám, 65–80. o.

[26] Az Európai Parlament és a Tanács 2017/541 számú Irányelve, Preambulum (2) bekezdés.

az Irányelv a büntetendővé nyilvánítandó magatartások körének bővítésével törekedett elérni a fellépés hatékonyságának fokozását. Ennek megfelelően a terrorcselekmény tényállása mellett külön szabályozásra kerülnek a terrorizmussal összefüggő bűncselekmények, melyek révén az Unió azt reméli, hogy a terrorista gyanús személyek még egy adott akció végrehajtása előtt – az előkészítő fázisban, vagy akár még azt megelőzően - kiemelhetők lesznek a társadalomból. Az Irányelv egyebekben az Unió átfogó terrorizmus-ellenes politikájának fontos, jogi részét képezi, mely politikát egyebekben további más elemek – így az EUROPOL és az EUROJUST munkája, a különféle cselekvési tervek és politikai szinten megfogalmazott stratégiák, az Unió külső határainak ellenőrzésére irányuló tevékenység is kiegészítenek.[27]

A tulajdonképpeni kiberterrorizmus elleni fellépés anyagi büntetőjogi eszközei

A szakirodalom a kiberterrorizmus fogalmához kétféleképpen közelít. Az egyik álláspont szerint kifejezetten a kiberbűncselekmény terrorista célzatú elkövetése értendő ezen kategória alatt. *Dornfeld László* véleménye szerint azonban a jelenség azokkal a terrortámadásokkal azonosítható, melyek a kibertérben kerülnek elkövetésre[28]. A szerző – nézetem szerint – helyes kiindulópontot választ, hiszen ilyen értelemben a kiberterrorizmus nem azonos egy kiberbűncselekmény terrorista célzatú elkövetésével, annál jóval tágabb kategória. Egy ettől eltérő értelmezés ugyanis jelentősen szűkítené a terrorcselekmény összetett tényállási konstrukciójában részletesen szabályozott eszközcselekmények körét.[29] Azaz a tulajdonképpeni kiberterrorizmus esetén az elkövető nemcsak önmagában egy terrorista célzatú hacker-támadást követhet el információs rendszer ellen – ezzel megvalósítva az információs rendszer vagy adat megsértése eszközcselekményét -, hanem azon keresztül egyben egy másik, a Btk. 314.§ (4) bekezdés i) pontjában értékelt eszközcselekmény elkövetési magatartását is meg tudja valósítani. Ezáltal pedig cselekménye egy másik eszközcselekmény elkövetési magatartásaként, maga a számítógépes rendszer pedig a bűncselekmény elkövetésének eszközeként is minősülhet. Ilyen értelemben tehát egy terrorista akció végrehajtásának kriminalizálása egységes függetlenül attól, hogy az a kibertér

[27] Cian C. Murphy: Counter-Terrorism Law and Policy: Operationalisation and Normalisation of Exceptional Law after the 'War on Terror. Diego Acosta Arcarazo –Cian C. Murphy: *EU Security and Justice Law: After Lisbon and Stockholm*. London, Hart Publishing Ltd., 2014,168–169. o.

[28] Dornfeld: i. m. (2019), 47. o.

[29] Neparáczki Anna Viktória ettől eltérő álláspontot fogalmaz meg a tanulmányban már idézett 2020-ban publikált munkájában, amennyiben az ún. „hard" típusú elkövetést tisztán a kiberbűncselekmény terrorista célzatú elkövetésével azonosítja, és törvényi szabályozottságát a Btk. 314.§ (4) bekezdés i) pontja szerinti eszközcselekményben látja azzal, hogy természetesen ilyen esetben a minősítés differencia specifikája a terrorista célzat. Ugyanakkor – ahogyan arra Dornfeld László példákban is rámutat – nézetem szerint a számítógépes rendszerekkel szemben megvalósított terrorista célzatú támadás más eszközcselekményhez, pl. közveszélyokozáshoz, radioaktív anyaggal visszaéléshez, vagy éppen közérdekű üzem működésének megzavarásához, jármű hatalomba kerítéséhez is kapcsolódhat.

felhasználásával kerül-e elkövetésre vagy sem.

Az irányadó szakirodalom is megerősíti a fenti álláspontot, amikor az internetes, vagy kiberterrorizmusnak alapvetően megkülönbözteti a tömeges pusztításra, a tömeges zavarkeltésre, valamint a társadalmi rend destabilizálására irányuló formáját. Az első kategóriában tartozhatnak tipikusan a kritikus infrastruktúrák elleni – számítógépes rendszer felhasználása révén megvalósított – terrorista célzatú támadások, míg a második alapvetően a pánikkeltésre, a lakosság megfélemlítésére, az utolsó pedig a társadalmi élet működésének ellehetetlenítésére (pl. közérdekű üzemekkel szembeni támadások) irányul.[30]

Amennyiben tehát a fentiekben hangsúlyozott jogi érvek mentén elfogadjuk, hogy a terrorcselekmény tényállását egységesen kell megítélni, és nem lehet tényállástani szempontból különbséget tenni aközött, hogy a kibertér felhasználásával kerül-e sor az elkövetésre, kijelenthető, hogy a magyar Btk. összhangban van az uniós Irányelvben foglalt elvi kereteknek. A terrorcselekmény Btk-ban szabályozott esetkörei, az egyes cél-, és eszközcselekmények, valamint a tényállásokhoz kapcsolt szankciókeret is megfelel az uniós elvárásoknak, követelményeknek, azokkal kapcsolatban alapvetően módosítási igény, vagy szükség nem merül fel, mely egyebekben uralkodó álláspont a hazai szakirodalomban is.

A terrorista célzatú információs rendszer-használat egyéb vetületei

Követve a korábbiakban, a szakirodalom alapján hivatkozott felsorolást, a téma kapcsán elsődlegesen *az ún. propaganda-tevékenység* anyagi büntetőjogi értékelésével szükséges foglalkozunk. Ez alapvetően kapcsolódhat általában a terrorizmusnak legitimációt adó eszmék, indokok szélesebb körben történő sugárzásához, akár egy-egy konkrét már megvalósított akció indokainak utólagos igazolásához, de természetesen az egyének gondolkodásának befolyásolásához is, melynek eredményeként ezen személyek utóbb vagy csatlakozhatnak egy terrorszervezethez, terrorista csoporthoz, vagy „saját elhatározásból", formális hűségesküt téve „a magasztosnak hitt céloknak" maguk követnek el eseti akciókat. A fenti esetkörök vizsgálata alapján teljesen nyilvánvaló, hogy büntetőjogi fellépés azon magatartásokkal szemben indokolt, melyek közvetve, vagy akár közvetlenül is hozzá tudnak járulni ezen extrémitás eszkalálásához.[31]

Az Irányelv – figyelemmel az elmúlt időszak terrorista akcióira és az egyes szervezetek azzal kapcsolatosan kifejtett „propagandakampányára" – rögzíti, hogy a

[30] Brenner, W. Susan 2006-ban „Cybercrime, Cyberterrorism, Cyberwarfare" c. a Revue internationale de droit pénal 3. számában megjelent tanulmányára ehelyütt Dornfeld László hivatkozik már hivatkozott tanulmányának 55-57. oldalain.

[31] Az azonban fontos, hogy itt olyan propaganda tevékenységről van szó, amely nem egy már konkrét és körvonalazható terrorista akció végrehajtására keres elkövetőket, szólít fel embereket, hiszen amennyiben ez a magatartás már egy konkrét terrorcselekmény elkövetési szándéka által vezérelt, akkor a klasszikus értelemben vett terrorcselekmény sui generis jelleggel szabályozott valamely előkészületi magatartásért felel az elkövető.

tagállamoknak minden olyan magatartást is büntetniük kell, amely terrorcselekmény elkövetésére irányuló nyílt felhívás céljából nagy nyilvánosság előtt közvetve vagy közvetlenül magasztalja, illetve szorgalmazza a terrorcselekmények megvalósítását.[32] Azaz ebben az esetben az elkövető a cselekmény kifejtésekor nem egy konkrét terrorcselekményhez kapcsolódik büntetendő magatartásával,[33] hanem azt, mint eszközt „reklámozza" a nyilvánosság felé, azaz az uszító magatartás hatására fennáll a terrorista bűncselekmény elkövetésének, a terrorista szándék kialakulásának veszélye.

A hazai jogalkotás ezzel kapcsolatban megelőzte az Európai Uniót, hiszen a 2016. évi LXIX. tv-el 2016. július 17. napjától kezdődő hatállyal egy szubszidiárius bűncselekményi alakzattal is kiegészítette a Btk.-t, azonban immáron annak nem a közbiztonság elleni bűncselekményeket tartalmazó fejezetében, hanem a köznyugalom elleni kriminalitásokat taglaló szerkezeti egységben. A Btk. fent nevezett módosítása a nagy nyilvánosság előtt elkövetett terrorizmus támogatására való uszítást, erre irányuló hírverés folytatását immáron önállóan is büntetni rendelte.[34] Ezen tényállás az elmúlt időszak terrorista akcióit, valamint azok elkövetőit tekintve különösen is indokolt. Több esetben is előfordult ugyanis, hogy a merénylő nem tartozott konkrétan valamely terrorszervezethez, azonban az elektronikus tömegtájékoztatási eszközök segítségével sugárzott propagandával egyetértve, a radikalizálódás irányába fordult, „hűségesküt téve" a szervezetnek.[35]

Fontos tehát leszögezni, hogy az ebben a tényállásban értékelt uszítás vagy hírverés folytatása nem egy konkrét terrorista támadáshoz, terrorcselekményhez kapcsolódik, de ilyen vagy ehhez hasonló szélsőséges magatartások megvalósításának a veszélyét egyértelműen magában hordozza. Azaz büntetendőségének nem feltétele, hogy ennek nyomán harmadik személyek ténylegesen is terrorista akciókat hajtsanak végre.[36] A tényállásban értékelt magatartás

[32] Természetesen az Irányelv 5. cikke helyesen mutat rá, hogy csak azon szándékos magatartások lehetnek relevánsak e körben, melyek közvetve, vagy közvetlenül szorgalmazzák terrorista cselekmények elkövetését, vagy annak veszélyét hordozzák magukban, hogy ilyen akciók kerülhetnek elkövetésre. Az ezen következmény kiváltására objektíve alkalmatlan propaganda kívül marad a büntető anyagi jogi fellépés terrénumán.

[33] Erre maga az Irányelv is utal a 13. cikkben, amikor kimondja, hogy a büntetendőséget attól függetlenül biztosítani kell, hogy fennáll-e a kapcsolat az uszító magatartás és a terrorista bűncselekmény között.

[34] Lásd Btk. 331. § (2) bekezdés.

[35] Ilyenek voltak például a teljesség igénye nélkül az alábbi merényletek. 2017. április 7-én Stockholmban egy 39 éves férfi kerített a hatalmába egy teherautót, amit aztán a gyalogosforgalom felé irányított. 9 ember meghalt, és további 14 megsérült. Ez az elkövetési mód hasonló volt a 2017. március 22-i londoni merénylethez, ahol egy 52 éves férfi vezette az autóját a Westminster hídon a gyalogosok felé. A merényletben 5 ember meghalt, és legkevesebb 50-en megsérültek. Londonban ugyanebben az évben június 3-án volt hasonló akció a London hídon, ahol 8 ember meghalt, és további 48-an sérültek meg. A gyalogosforgalom ilyen formában történő veszélyeztetésével megvalósított merényletek közül 2017-ben a Barcelonában elkövetett volt a legsúlyosabb, amikor a merénylő augusztus 17-én a La Rambla sétányra hajtott be 15 ember halálát és további 131 ember sérülését okozva. (Europol TE-SAT 2018. 23–24. o.)

[36] Neparáczki Anna Viktória: *A terrorizmus elleni fellépés eszközei a magyar és a német anyagi büntetőjogban. PhD értekezés*, Pécs, 2017, 206. o.

büntetni rendeltsége azért fontos, mert a radikalizálódás egyik eszköze lehet, ezért elengedhetetlen az ilyen magatartásokkal szembeni fellépés.

Éppen ezért az ilyen uszító cselekmények elsősorban a közbiztonságot és csak másodlagosan sértik a köznyugalmat. Véleményem szerint ezért az elsődleges jogi tárgy okán indokoltabb lenne ezen tényállást a terrorcselekményhez kapcsolva egy önálló tényállásban a Btk. 318. §-a szerinti „Terrorizmus finanszírozása", valamint a Btk. 319. § szerinti „Értelmező rendelkezés" között elhelyezni „Terrorcselekmény elkövetésére irányuló uszítás" cím alatt. A cselekmény egyértelműen a terrorizmushoz kapcsolódó cselekmény, így a háborús uszítás tényállásán belüli szabályozásának nincs dogmatikai alapja.

Másodikként a nemzetközi szakirodalom alapján *Dornfeld* a *pénzgyűjtést* említi meg. A pénzgyűjtés természetesen a terrorszervezetek működése, a terrorizmus dinamikája szempontjából is nélkülözhetetlen eszköz. Ugyanakkor a terrorista célzatú forrásgyűjtés már régóta bűncselekménynek számít. Ezzel összefüggésben az Irányelv 11. cikke is leszögezi, hogy a terrorizmus finanszírozása alatt az olyan pénzgyűjtési tevékenységet érti, melynek célja valamely terrorista bűncselekmény, vagy ehhez kapcsolódó büntetendő magatartás elkövetése, vagy az abban való bármilyen formájú közreműködés biztosítása. A terrorizmus pénzügyi támogatása a hatályos büntető anyagi jogunkban is kriminalizált magatartás, a cselekmény büntetendőségét a Btk. 318-318/A.§§-ai biztosítják.[37]

Ugyanakkor kérdésként merül fel, hogy szükséges-e büntetőjogi eszközökkel reagálni az olyan magatartásokra, melyek a legális és illegális szálak összefűzött rendszerében egy-egy szervezet működését, fennmaradását általános szinten támogatják, ahhoz generális jelleggel járulnak hozzá. Másként feltéve a kérdést, szükséges-e a büntetni az olyan magatartásokat, melyek egy-egy szervezetet azok különféle „fedő-szervezetein", „fedő-vállalkozásain" keresztül, a törvényes működés látszatának fenntartása érdekében támogatják? Hiszen ezekben az esetekben formálisan a „támogató" törvényesen folytatott tevékenységhez kapcsolódik.

Mivel mind az Irányelv, mind pedig a Btk. a finanszírozói magatartások esetében azok terrorcselekményhez, vagy terrorista jellegű cselekményhez való kapcsolódását tényállási elemként határozzák meg – így a fentebb említett esetet alapvetően nem fedik le büntetőjogi válasszal, reakcióval -, a kérdés feltétele korántsem teoretikus. Az természetesen nyilvánvaló, hogy ha a támogató – pl. egy, az adott szervezethez kapcsolódó vállalkozás által nyújtott szolgáltatás igénybe vevő – személy nem tud arról, hogy az adott gazdálkodási tevékenység milyen mögöttes célokat szolgál, a bűnösségen alapuló felelősség elvéből is következően nem vonható felelősségre semmilyen bűncselekményért.

Amennyiben viszont szándékosan és abban a tudatban veszi igénybe és fizet egy szolgáltatásért, vagy fejt ki egyéb módon,

[37] A terrorizmus finanszírozása elleni fellépés szükségessége az Irányelv 11. cikkén alapszik. A hazai Btk. hatályos szövegét 2018. január 01-i hatályba lépési időponttal a 2017. évi XXXIX. törvény alakította ki.

támogatásként értékelhető magatartást, hogy az ő közreműködése révén keletkezett bevétel a későbbiekben milyen célokra kerülhet felhasználásra, közvetve alapvetően a terrorista szervezet fennmaradásához járul hozzá. Viszont mivel nincs kapcsolata, ismerete konkrét terrorista támadásról, vagy terrorista jellegű bűncselekményről, és ahhoz kapcsolódó személyről, így magatartása nem illeszthető be a Btk. említett rendelkezéseibe. Ez tehát egy szürke folt. Egy olyan határvonal a terrorizmus elleni fellépés anyagi jogi szabályozásában, mely mindenképpen megoldandó feladat, ugyanakkor belátom, hogy egy ilyen tényállás absztrakciója korántsem egyszerű jogalkotói munka.[38]

A harmadik, fentiekben említett terület az *információ terjesztése.* Természetes, hogy a terjesztett információ sokféle lehet, több mindenre is vonatkozhat, ugyanakkor *Dornfeld* hivatkozott tanulmánya nyomán egy dologban mindenképpen különbözik a propagandától. Nevezetesen ebben az esetben a terroristák saját, már meglévő szimpatizánsaikkal kívánnak információkat megosztani,[39] pl. egy konkrét terrorista akcióról, annak végrehajtásáról, következményeiről. Ebben az esetben az internet tehát egyfajta hírforrás a szervezet tagjaira számára. Ez a tömegtájékoztatás mindaddig, amíg már nem fordul át propagandává, álláspontom szerint nem éri el azt a küszöböt, amelyet a büntetendőség körében akár az Irányelv, akár a hazai Btk. felállított. Az pedig, hogy a híradások átfordulnak-e propagandává, azt minden esetben az adott híradás tartalma, kimutatható hatásai alapján kell és lehet is megítélni, eseti jelleggel, az eset összes körülményének mérlegelése révén.

A terjesztett információ ugyanakkor akár ismeretterjesztő célokat is szolgálhat, mely nemcsak a terrorista szervezetek követőinek számaránybeli növekedéséhez, de akár a terrorista akciók végrehajtásához szükséges ismeretek megszerzéséhez, azok elmélyítéséhez is hozzájárulhat. Az Irányelv éppen ennek megakadályozása céljából mind a toborzói, mind pedig a kiképzéshez közreműködőként kapcsolódó magatartásokkal szemben a szükséges büntetőjogi válaszok megfogalmazására hívta fel az egyes tagállamokat.[40] A dogmatikai problémát ugyanakkor az olyan információk, ismeretek közvetítése,

---

[38] Belátható ugyanis dogmatikai szempontból, hogy egy ilyen magatartás a jelzett indokok miatt nemcsak a terrorizmus finanszírozása, sem pedig a bűnszervezetben részvétel, mint sui generis előkészületszerű bűncselekmény törvényi tényállásába nem illeszthető. Utóbbi esetében a terrorista csoport és a bűnszervezet legál-definíciójában rejlő különbségek is minősítési problémát jelenthetnek.

[39] Dornfeld: i. m. (2019), 54. o.

[40] Az Irányelv 6. cikke, valamint 15. cikk (4) bekezdése előírja, hogy a tagállamok nyilvánítsák büntetendő magatartásnak a terrorista bűncselekmény elkövetésére, vagy az abban való közreműködésre történő felhívást, kiemelten akkor is, ha a célszemélyek gyermekkorúak. A kiképzéssel kapcsolatos 7. cikk tekintetében ugyanezt az elvárást fogalmazza meg az Irányelv. Bár az Irányelv és annak magyar fordítása is a 6. cikk tekintetében a„felhívás"-ban jelöli meg az elkövetési magatartást, látva a preambulumban is rögzített célokat nyilvánvalóan az eredményes és az eredménytelen felbujtás is egyaránt üldözni kívánt magatartás az Irányelv szellemiségét tekintve. Ld ezzel kapcsolatban: Bartkó Róbert: Az Unió 2017/541. sz. Irányelvének hatása a V4 országainak büntető anyagi jogszabályalkotására. In: Bartkó Róbert (szerk.): *A terrorizmus elleni küzdelem aktuális kérdései a XXI. században.* Budapest, Gondolat Kiadó, 2019, 145. o.

átadása jelenti, melyek esetében azok nem kapcsolódnak egy konkrét terrorista bűncselekményhez.[41] Ez ismételten egy olyan „szürke folt", ahol a jogalkotásnak igazodnia kellene az uniós követelményekhez. A problémát jelentő esetek ugyanis pont az olyan ismeretterjesztésre vonatkoznak, melyek közép, vagy akár rövidtávon is terrorista akciók megjelenéséhez, elkövetéséhez vezethetnek, azonban közvetlen terrorista célzatuk hiányában nem illeszthetők be egyik terrorizmushoz kapcsolódó tényállásba sem. Hasonlóan a pénzgyűjtési célzatnál említettekhez, egy ilyen tényállás absztrakciója is komoly kihívás nemcsak a jogalkotás, de a jogalkalmazás számára is, hiszen számtalan bizonyítási nehézséget hordoz magában.

A negyedik és egyben utolsó terrorista internet-használati cél *a biztonságos kommunikáció és a hírszerzés.* A terrorizmus dinamikája szempontjából nemcsak a folyamatos pénzügyi ellátottságnak, de természetesen – minthogy a bűnözés egyik formájáról van szó – az információkkal való rendelkezésnek is jelentős szerepe van. A terroristák igyekeznek az internet olyan felületeit használni, ahol az egymás közötti kommunikáció, a társadalom adott szegmensébe alvó sejtként beépült alegységek tagjai által megszerzett információk titkosan, a bűnüldöző hatóságok előtt láthatatlan módon tudnak gazdát cserélni.

Az anonimitás ezen a területen különösen is fontos, melyet a terroristák is – más bűnözői csoportokhoz hasonlóan – a különféle információ-technológiai megoldások használatával tudnak elérni. Így például nagy segítséget jelentenek a terroristák számmára is a kiberbűnözők által is igénybe vett privát szférát erősítő technológiák, mint például „a virtuális magánhálózatok (VPN), melyek segítségével a felhasználó könnyedén kaphat a világ bármely más országába mutató IP címet"[42] is.

Ezeknek a csatornáknak tehát elsődlegesen az adott terrorista akció előkészítése során van komoly szerepe, melyek az Irányelvvel való összhangban sui generis tényállásban értékelt büntetendő magatartások a hatályos Btk-ban. Amennyiben a terroristák közötti kommunikáció tartalma szerint nem kapcsolható konkrét akcióhoz, a büntetőjog által értékelési körön kívül marad, ugyanakkor az egyes szervezetek, vagy azok sejtjei, illetve az egyes elkövetőkkel szembeni titkosszolgálati eszközöket is igénybe vevő felderítési munkában fontos szerepük van, hiszen ezek feltérképezése révén lehetnek képesek a hatóságok egy-egy akciót meghiúsítani, egy-egy szervezetet, csoportot, vagy alvó ügynököt kézre keríteni.

[41] Az Irányelv 13. cikke értelmében: „a terrorista bűncselekmény tényleges elkövetése nem szükséges feltétele annak, hogy a 4. cikkben vagy a III. címben említett bűncselekmények büntetendőnek minősüljenek, az 5-10. és a 12. cikkben említett bűncselekmények büntetendővé minősítésének szempontjából pedig szintén nem tekinthető szükséges feltételnek az ebben az irányelvben meghatározott valamely más konkrét bűncselekmény vonatkozásában fennálló kapcsolat megállapítása."

[42] Dornfeld: i. m. (2019), 55. o.

TERRORIZMUS FINANSZÍROZÁSA A KIBERTÉRBEN

A terrorista csoportok akkor tudnak hatékony romboló tevékenységet kifejteni, ha létrehoznak bizonyos szervezeti struktúrákat. Ezek a szervezeti keretek egyébként kísértetiesen hasonlítanak az üzleti szervezetek által kialakított szervezeti és működési formákhoz.
Két ideális szervezeti forma létezik, amelyet a terroristák használhatnak:

1. a parancsnok-beosztott típusú, vagyis *hierarchikus szervezet*
2. *a hálózati típus*.

Napjainkban a terrorszervezeteknek aktív adaptációs mechanizmussal kell reagálnia a környezeti változásokra, vagyis arra, hogy a jogi szabályozás következtében folyamatos külső nyomás nehezedik rájuk. Emiatt *a hálózati típusú szervezeti forma a hatékonyabb*. A terroristák virtuális hálózatokat hoznak létre, ahol a résztvevő terrorista sejtek legtöbbször a saját maguk által biztosított forrásokból finanszírozzák a működésüket, kapcsolatuk a központtal nagyon laza. A vezető feladata csak az, hogy világképet és ideológiát szolgáltat, és stratégiákat javasol. ezt azonban soha nem konkrét csoporttagoknak, hanem csak úgy általánosságban. A vezető feladata inkább az ösztönzés, nem a parancsolás. A virtuális hálózat előnyei a terroristák számára:

a) a funkciók megtöbbszöröződése, vagyis a redundancia (így erősebbé válnak a külső behatásokkal szemben, és egy sejt vagy csoport kiesése esetén nem omlik össze az egész hálózat, hasonlóan az Internet felépítésének alapfilozófiájához[43])
b) az Internet szerepe: virtuális terrorista közösségek alakulhatnak
c) a tagok, az egyes terroristák és terrorista sejtek személyes találkozás nélkül kommunikálhatnak egymással a kibertéren keresztül
d) a minimális kommunikáció rendkívül nehéz az ilyen szervezetekbe beépülni.

A virtuális hálózat azonban egy komoly hátrányt is rejt magában: az ilyen terrorszervezetek nem vagy csak nagyon nehezen képesek komplex feladatok megoldására. Erre a célra inkább a hierarchikus, parancsnok-beosztott típusú szervezet alkalmas. A hierarchikus felépítésű terrorszervezetek azonban sebezhetőbbek, ezért szinte kizárólag csak olyan államokban tudnak működni, amelyiknek a központi kormányzata gyenge. A CIA becslése szerint jelenleg hozzávetőlegesen 50 ilyen államot találunk, ezek közel felében működnek hierarchikus szervezeti struktúrával rendelkező terrorista csoportok. (Az al-Kaida hierarchikus felépítésű központi magja vélhetően Pakisztán törzsi uralom alatt álló területein rejtőzik.)[44]

[43] A hatvanas évek végén felmerült föl az USA-ban egy kevéssé sebezhető számítógép-hálózat szükségessége, amelynek egy esetleges atomtámadás után megmaradó részei működőképesek maradnak. Ezen az elven kezdett működni 1969-ben az ARPANET, amelyből a polgári változat, az Internet 1983-ban kiválva megszületett.

[44] Thomas J. Bierstecker – Sue E. Eckert (szerk.): *Countering th Financing of Terrorism*. London, New York, 2008, 23–27. o.

Elmondhatjuk tehát, hogy a XXI. században új típusú terrorfenyegetettséggel kell szembenéznünk: a „war on terror" politikája, amit az USA meghirdetett, aktivált egy kevésbé lazán összekapcsolódó, dzsihádista sejtekből álló, globális terrorista hálózatot… Emellett az is aggodalomra adhat okot, hogy egyes szakértők szerint az elsődleges terrorista célpontok ma már az európai nagyvárosok.[45] Ezt számos terrortámadás támasztja alá az elmúlt évtizedből.

A terrorszervezetek mindkét alaptípusa legalább egy tekintetben megegyezik: anyagi erőforrásokra van szüksége a támadások megszervezéséhez és végrehajtásához. Ez a számukra költségként jelentkezik. Érdemes megvizsgálni a terrorizmus költségeit két oldalról: a terroristák oldaláról (finanszírozási igény) és a társadalom oldaláról (károk és áldozatok).

A terrorizmus finanszírozása azt a tevékenységet jelenti, amelynek során közvetve vagy közvetlenül terrortámadások megvalósításához anyagi eszközöket bocsátanak rendelkezésre. *A terrorizmusnak a témánk szempontjából talán a legfontosabb jellemvonása az, hogy nem szükséges nagy összeg az egyes akciók kivitelezéséhez.*

A költségek három nagy csoportja: a műveleti költségek, az adminisztratív költségek és a merénylők családtagjainak adott dotáció.

Néhány példa a „műveleti költségek"-re:

- 1993. február 26-án a World Trade Center ellen egy gépjárműben elrejtett, 680 kg súlyú bombával követtek el merényletet, ennek költsége 18.000 USD volt, 6-an meghaltak, és több mint 1000 sebesült volt,
- a 2001. szeptember 11-i, a világtörténelem eddigi legnagyobb, csaknem három ezer emberáldozatot követelő terrortámadásának összköltsége a becslések szerint 400-500.000 USD volt, ebből 300.000 USD érkezett banki átutalások formájában,
- a 2002. október 12-én végrehajtott Bali robbantás becsült bekerülési költsége 20-35.000 USD volt, 190 halott és 309 sebesült volt a mérleg másik oldalán,
- a 2003. november 15-én és 20-án Isztambulban végrehajtott pokolgépes akciók 40.000 USD körüli összegbe kerültek, 27 halott és 450 sebesült maradt a helyszínen,
- 2004. március 11-én Madridban robbantak bombák, ezt az akciót 10.000 (spanyol becslések szerint 60.000) USD költségvetéssel tudták a merénylők kivitelezni. A mérleg másik oldalán 191 halott és több mint 1500 sebesült volt.
- 2004. november 2-án megkéselték és lelőtték Theo Van Gogh holland filmrendezőt, akit az iszlámról vallott radikális nézetei miatt korábban már többször megfenyegettek. Ugyan ebben az esetben „csak" 1 halálos áldozattal járt a támadás, de a költsége

[45] Sean S. Costigan – David Gold: *Terronomics ASHGATE*. Printed in Great Britain, 2007, 19. o.

elképesztően alacsony: 100 USD volt!

- 2005. július 7.-én Londont érte támadás, 700-an megsérültek, 38-an életüket vesztették. A támadás teljes költsége mindössze 15.000 USD volt.

Látható tehát, hogy a terrortámadások kivitelezése elképesztően alacsony költségvetéssel is megoldható, az okozott károk viszont óriásiak. Ezekből az összegekből azt a következtetést is levonhatnánk, hogy a terrorizmus finanszírozása elleni küzdelemnek nincs sok értelme. Ez így nem igaz. Nagyon nehéz feladat a terroristákat elvágni a pénzügyi forrásaiktól, de nem lehetetlen, és van értelme az erre irányuló erőfeszítéseknek. Erre két példát hoznék fel igazolásképpen:

1) Az 1993-as WTC elleni merénylet után az egyik elfogott elkövető, Ramzi Yousef bevallotta, hogy nagyobb bombát akartak használni, de nem volt rá pénzük! Ráadásul a nyomozásban az egyik kulcs-elem az volt, hogy a terroristák vissza akartak kapni egy letéti díjat, amit a merényletet megelőzően a robbantáshoz használt furgonért fizettek…[46]
2) A terrorszervezetek működési költsége sokkal nagyobb, mint az egyes műveletek végrehajtási költsége. Az a terrorszervezet, amelyik nem jut kellő mennyiségű anyagi erőforráshoz, lassan elsorvad.

A második költségtényező az adminisztratív, vagyis a működési költség. Az al-Kaida például a bevételeinek kb. 10%-át költi műveleti költségekre, 90%-ot a szervezet adminisztratív és működési költségeire fordít.[47] A finanszírozási igény természetesen függvénye a szervezeti struktúrának. A hierarchikus szervezet magasabb finanszírozási igényével szemben a hálózati struktúra lényegesen kevesebb pénzből is működtethető. Ha ehhez még azt is hozzátesszük, hogy a virtuális hálózat egyes elemeit alkotó terrorista sejtek sokszor önfinanszírozó módon működnek, akkor komoly aggodalmaink támadhatnak. Rögtön meg kell jegyeznünk azonban, hogy egy önfinanszírozó terrorista sejtekből álló virtuális hálózati struktúrában működtetett terrorszervezet lényegesen veszít a hatékonyságából a hierarchikus struktúrához képest, és gyakorlatilag nem tud összehangolt, valamint egyáltalán nem tud nemzetközi méretű műveleteket végrehajtani.

Ennek ellenére – ahogy Donald Rumsfeld fogalmazott – „A költség-haszon arány ellenünk dolgozik! A mi milliárdos költségeink állnak szemben a terroristák milliós költségeivel."[48]

Van a terrorista támadásoknak egy érdekes, új költségtényezője is, ez az öngyilkos merénylők családtagjainak – általában egy összegben – fizetett anyagi dotáció, illetve életjáradék. Ez a Hamasz esetében becslések szerint 5000 USD, de például Szaddam Husszein regnálása során 25.000 USD-t ajánlott az öngyilkos

[46] Bierstecker – Eckert: i. m. (2008), 7. o.
[47] D. Bugg: Speech to IAP Conference 8.12.2003. (http://www.cdpp.gov.au/Media/Speeches/20030812db.aspx).
[48] http://www.globalsecurity.org/military/library/policy/dod/rumsfeld-d20031016sdemo.htm.

merénylőknek „sikerdíjként".[49] Ez azonban nem növeli meg jelentősen a terrorista támadások költségét, mivel:

1) az öngyilkos merénylők egy jelentős része gazdag (vagy legalábbis jó körülmények között élő) családból származik, így ezek esetében nincs jelentős szerepe az anyagi ösztönzésnek,
2) a „sikerdíj" nem minden estben a terrorszervezet vagy terrorista sejt költségvetését terheli, mint ahogy ezt Szaddam Husszein példája is mutatja.

A terrorista támadások kivitelezésének összköltsége tehát napjainkban három alapvető költségtényező nagyságától függ: a terrorszervezet adminisztratív, fenntartási költségei[50], az öngyilkos merénylő családjának juttatott anyagi támogatás[51], valamint a terrortámadás végrehajtásának közvetlen operatív költségei.[52]

A terrorizmus finanszírozásának a legtágabb értelemben négy fő formája ismert[53]: bűncselekmények elkövetése, adományok, törvényes üzleti tevékenység és meghatározott földrajzi területi egységek feletti kontroll.

1. Bűncselekmények elkövetése

A terrorizmus a bűnözés egyik formája, mégpedig az egyik legsúlyosabb és legveszélyesebb formája. Emiatt a terrorszervezetek természetszerűen nem riadnak vissza attól, hogy egyéb bűncselekményeket is elkövessenek. Ennek a kockázata általában kisebb is, mint a terrorcselekményé, hiszen a büntetési tételek rendszerint alacsonyabbak. A terroristák általában olyan bűncselekmény-típusokat kedvelnek, amelyek rövid idő alatt nagy összegű bevételt eredményeznek.

Talán a legkedveltebb ezek közül is *kábítószerrel visszaélés*. A kábítószer-kereskedelem adja a columbiai paramilitáris szervezetek és gerillák bevételeinek a 60-90%-át.[54] Az iszlám terrorista szervezeteket ráadásul néhány fatwa kifejezetten felhatalmazza arra, hogy a dekadens Nyugattal szemben folytatott küzdelmükben a kábítószer-kereskedelmet eszközként használják fel.[55]

Emellett a terroristák jelentős bevételforrása az *emberrablás* is. Az IMU (Üzbég Iszlám Mozgalom) például 5 millió USD bevételhez jutott 4 japán geológus szabadon engedéséért cserébe, miután 1999-ben elrabolták őket Kirgizisztánban.[56]

Az *embercsempészet* is jövedelmező tevékenység a terroristák számára. A világ fejletlen és fejlett régiói közötti életminőség-különbség, illetve a demokratikus államok által nyújtott

[49] Bierstecker – Eckert: i. m. (2008), 102. o.
[50] Ez a szervezet nagyságától függ, sokszor kis terrorista sejtek alacsony működési költségek mellett is képesek nagy károkat okozó merényletek végrehajtására, ugyanakkor a nemzetközi ütőképességük minimális.
[51] Ennek a mértéke különböző, és természetesen (szerencsére) nem minden támadásban vesznek részt öngyilkos merénylők.
[52] Sajnos ez a legkisebb költségtényező, pedig jórészt ezen múlik az akció sikeressége illetve az okozott kár nagysága is.
[53] Ld.: Gál István László: *A terrorizmus finanszírozása. Die Terrorismusfinanzierung,* Pécs, Pécsi Tudományegyetem Állam- és Jogtudományi Kar Gazdasági Büntetőjogi Kutatóintézet Pécs, 2010.
[54] Berry LV – Curtis GE, Hudson RA – Kollars NA: *A Global Overview of Narcotics-Funded Terrorist and Other Extremist Groups*, Library of Congress 2002. 52. o.
[55] Beers R – Taylors FX: Narco-Terror: The Worldwide Connection Between Drugs and Terror. *Terrorsim and Goverment Information*, 2002, 322. o.
[56] Napoleoni L: *Modern Jihad: Tracing the Dollars Behind the Terror Networks*. London, Pluto Press, 2003, 89. o.

biztonság iránti vágy hívta életre a gazdasági és a politikai migrációt. Ahhoz, hogy egy bangladesi vagy egy kínai állampolgár eljusson Nyugat-Európába, 20-25 ezer dollárt is kell áldoznia.[57]

A *pénzmosás* egyrészt jövedelmező tevékenység a terroristák számára, így tehát a terrorizmus finanszírozásának az egyik eszköze is. Másrészt viszont rokon jelenségnek is tekinti a szakirodalom tekintélyes része a terrorizmus finanszírozását és a pénzmosást. A terrorizmus finanszírozása várhatóan rövid időn belül, mint „fordított pénzmosás", vagy „pénzbepiszkítás" (money dirtying) be fog épülni a tágabb értelemben vett pénzmosás-fogalomba is. A terrorizmus finanszírozása viszont a pénzmosással összehasonlítva a következő eltérő jellemvonásokkal rendelkezik:[58]

– A motívum inkább erőszakos (megfélemlítés), mint anyagi (nyereségvágy). A terroristák célja leginkább állami szervek, nemzetközi szervezetek valamire történő kényszerítése, a lakosság megfélemlítése vagy más állam alkotmányos, társadalmi vagy gazdasági rendjének megváltoztatása, illetve megzavarása. Ezeket a nemzetközi dokumentumok által megnevezett célokat a magyar Btk. is tartalmazza a terrorcselekményről szóló 261.§-ban. A terroristák célja tehát csak a legritkább esetben lehet a haszonszerzés, míg a pénzmosók egyértelműen „profitorientáltak".

– A terrorizmus finanszírozására ugyanúgy felhasználnak legális forrásból származó pénzt, mint illegálisat. A terroristák a pénzügyi támogatásként kapott összeg jelentős részét olyan legális forrásból kapják, mint például a karitatív szervezetek, jótékony adományozók, illetve törvényesen működő cégek.

– A harmadik megkülönböztető jellemvonás az eltérő összegnagyság. A nagyobb terrortámadások is megszervezhetők és lebonyolíthatók viszonylag kisebb összegekből is. A 2001. évi New York-i repülőgép-eltérítések elkövetői például külföldi diáknak álcázva szerény támogatási összegeket vettek fel rendszeresen, és kivétel nélkül egyik átutalás sem érte el a „bűvös" 10.000 dolláros határt.

Emellett vannak még *egyéb* jövedelmező bűncselekmény-típusok is, amelyeket a terroristák felhasználnak a pénzszerzésre. Ezek taxatív felsorolása lehetetlen. 2002-ben az IRA állítólag 11 millió USD bevételhez jutott különféle bűncselekmények elkövetése révén. A bevételük legnagyobb része Kelet-Európából Angliába irányuló dohánycsempészetből származott.[59] Az al-Kaida európai pénzügyi bevételeinek a nagy része pedig hitelkártya-csalásokból származik, titkosszolgálati becslések szerint ez az összeg eléri az 1 millió USD-t havonta (!).[60]

2. Adományok

Az adomány készpénz, számlapénz, értékpapír, nemesfémek, drágakövek vagy

[57] Korinek: i. m. (2006), 456. o.
[58] Steven Mark Levy: *Federal Money Laundering Regulation (Banking, Corporate, and Securities Compliance)*. New York, 2003, 2. fejezet 18–20. o.
[59] Clarke L – Leppard D: Photos link more IRA Men to Colombia. *Sunday Times*, 2002.
[60] Gunaratna R: *Inside Al Quaeda: Global Network of Terror*. London, Hurst&Company, 2002. 65. o.

egyéb, értékkel rendelkező forgalomképes vagyontárgyak ingyenes, ellenszolgáltatás nélküli átadása terroristák vagy terrorista szervezetek részére. Tipikus formája a pénzbeli támogatás. A terroristák egyébként a legmagasabb likviditási fokkal rendelkező vagyontartási formát, a készpénzt részesítik előnyben.

A terroristákat támogathatják magánszemélyek, szervezetek (akár más terrorszervezetek is) és államok. A tágabb értelemben vett „adomány" tekinthető a terrorizmus finanszírozásának büntetőjogi értelemben, míg közgazdasági értelemben a bűncselekmények elkövetése és a legális üzleti tevékenység is e tevékenység részének tekinthető.

Szűkebb értelemben terrorizmus finanszírozása elleni büntetőjogi szabályozás elsődlegesen a magánszemélyek adományaira fókuszál, ha államok támogatnak terrorista célokat, az sokszor megoldhatatlan probléma elé állítja a büntetőjogot. Nem mindegy ugyanis, hogy az állami dotáció milyen formában (közvetlen vagy közvetett pénzügyi juttatás), milyen fedéssel (kereskedelmi ügylet, humanitárius segítség stb.), és milyen katonai-gazdasági erővel rendelkező államtól (kis ország, nagyobb, esetleg atomfegyverrel is rendelkező állam vagy esetleg egy szuperhatalom) származik.

3. Törvényes üzleti tevékenység

Oszama bin Laden Szudánban 30 céget alapított 1991-1996 között, ezeknek összesen 3000 alkalmazottja volt. Már 1994-1995-ben nyugati és izraeli titkosszolgálati források úgy emlegették bin Ladent, mint a terrorizmus kulcsfinanszírozóját.

A törvényes üzleti tevékenység egyre fontosabb szerepet játszik a terrorizmus finanszírozásában, mint ahogy általános értelemben az is kijelenthető, hogy a terrorizmus finanszírozásában egyre fontosabb szerepe van a legális forrásoknak. Említettük már, hogy főként az európai dzsihádista sejtek egyre inkább támaszkodnak legális bevételeikre, például arra, amit törvényes munkahelyükön keresnek meg. A szeptember 11-i támadás volt az utolsó merénylet, amelyet az al-Kaida finanszírozott teljes egészében, 2002-ben a globális finanszírozás megszűnt! A mai robbantások döntő többsége önfinanszírozó sejtek akciója. Megindult tehát egy olyan folyamat, amelyet a *terrorizmus finanszírozásának privatizációjának* nevezett el a szakirodalom.[61]

A törvényes üzleti tevékenység részének tekinthető tágabb értelemben az is, ha a terroristák munkavállalóként a legális jövedelmük egy részét használják fel terrorista célokra. Ha abból indulunk ki, hogy az elmúlt évek nagyobb terrortámadásainak tapasztalatai alapján 8-10.000 USD összegből már komoly akció kivitelezhető, akkor reális lehet azon félelmünk, hogy egy 4-5 fős terrorista sejt 2-3 év alatt gyakorlatilag bármelyik fejlett vagy közepesen fejlett országban, bármilyen legális munkával meg tud takarítani egy ekkora összeget[62], és képes

[61] Sean S. Costigan – David Gold: *Terronomics ASHGATE*. Printed in Great Britain, 2007, 14. o.

[62] 5 fős sejttel számolva 2 év alatt 10.000 USD megtakarításához elég, ha személyenként egy év alatt 1000 USD a megtakarítás összege. Ez alig több, mint 80 USD havonta.

csapást mérni anélkül, hogy szüksége lenne bármilyen egyéb addicionális forrásra!

4. Meghatározott földrajzi területi egységek feletti kontroll[63]

A terroristák úgy is juthatnak finanszírozási forrásokhoz, ha kvázi államként kezdenek működni egy meghatározott területen, ennek kertében pedig hasonló módon tesznek szert bevételekre, mint a nemzetközi közösség tagjaiként elismert államok. Adót szednek, kereskednek, pénzügyi műveleteket végeznek stb. Erre a legjobb példa az Iszlám Állam néven hírhedtté vált terrorszervezet volt.

A terrorizmus finanszírozása az online térben részben hasonló, részben pedig különbözik a fentebb bemutatott hagyományos finanszírozási formáitól. Az online térben megfigyelhető terrorizmus finanszírozási technikákat Serbakov munkája[64] alapján a következő csoportokra oszthatjuk:

1. *Terrorizmus finanszírozás online kiskereskedők és piacok használatával*
2. *Adománygyűjtés és közösségi finanszírozás a közösségi médián*
2. *1. Új fizetési termékek és szolgáltatások*
2. *2. Virtuális fizetőeszközök*
2. *3. Internetes pénzügyi szolgáltatások*

Ad 1) A terroristák a legnagyobb online kereskedelmi piactereket (például Amazon, eBay, Alibaba) felhasználva is igyekeznek finanszírozási forrásokat előteremteni a közvetlen műveleti költségeik valamint a terrorszervezet működtetésének adminisztratív költségei számára. Több forrás is megerősíti, hogy az Iszlám Állam a működési területén zsákmányolt antik műkincseket online kereskedelmi piactereken értékesítette.[65] Ez gyakorlatilag az Ulrich Sieber által leírt negyedik hagyományos terrorizmusfinanszírozási technika körébe sorolható online módszer.

Ad 2) A terroristák a XXI. században már a közösségi médiát is felhasználják arra, hogy forrásokat gyűjtsenek. Erre akár a Facebook különösen jó lehetőséget jelent, de például a kínai WeChat alkalmazás, ami egyben egyfajta a közösségi médium és üzenetküldő illetve kommunikációs alkalmazás is, fizetőeszközként és pénzátutalási applikációként is használható. Napjainkban a WeChat az egyik legnépszerűbb fizetési csatorna Kínában az Alipay mellett. Ez a Kínában élők és a külföldiek számára is rendelkezésre áll, mivel a WeChat fiók létrehozásához nincs szükség kínai személyi igazolványra. Ezenkívül az útmenti árusoktól a nagy bevásárlóközpontokig mindenki elfogadja a WeChat-tel történő fizetést, megkönnyítve a mindennapi életet. Bárki könnyedén átutalhat pénzt WeChat-fiókjából bármelyik ismerőse fiókjába.[66] Ez a platform tehát a terroristák és más bűnözők számára is alternatívát jelenthet, bár a tranzakciók nem teljesen anonimek, de kisebb összegek

[63] Sieber – Vogel.: *Terrorismusfinanzierung: Prävention im Spannungsfeld von internationalen Vorgaben und nationalem Tatstrafrecht.* Berlin, Duncker & Humblot, 2015, 10. o.

[64] Serbakov Márton Tibor: *Egyes szélsőséges terrorista csoportok internethasználata egyes aspektusainak elemzése PhD értekezés.* Pécs, Pécsi Tudományegyetem, 2022, 84–99. o.

[65] Vö.: Jessica Davis: *New Technologies but Old Methods in Terrorism Financing.* London, Royal United Services Institute for Defence and Security Studies, 2020.

[66] https://www.webnots.com/how-to-do-money-transfer-in-wechat-accounts/.

esetén nagy valószínűséggel nehezen felderíthetők a hatalmas volumen miatt. Serbakov egy példát is leír a terrorfinanszírozás ezen változatára: „Példa egy hatóságok előtt ismert terrorizmus finanszírozó és családja megsegítésére indított közösségi finanszírozásra: „A" személyt 2016-ban terrorizmus finanszírozásával vádolták meg. Egy GoFundMe közösségi finanszírozás kampányt hoztak létre e személy és terhes felesége támogatására. A támogatandó ügy leírása a következő volt: „Nemrég egy testvér aseer (fogoly) lett a tawagheet (hitetlenek) kezében. (Recently a brother has become an aseer (prisoner) at the hands of the tawagheet (nonbelievers)." A kampány két nap alatt 3.000 USD összeget hozott."[67]

Mindezek mellett komoly biztonsági kockázatot rejt magában az is, hogy új fizetési termékek és technológiák jelentek meg az Interneten a XXI. században. A kriptovaluták különösen alkalmasak a terrorizmus finanszírozására, pénzmosásra, illegális fegyverkereskedelemre és egyéb bűncselekmények finanszírozására, elkövetésük megkönnyítésére, ugyanis ezek „jogi státusza jellemzően nem eldöntött az egyes jogrendszerek esetében. Azaz álláspont kezd kirajzolódni, hogy amennyiben értékpapírnak minősül a kriptoérme-kibocsátás, akkor kötelező nemcsak az értékpapír-kibocsátásra vonatkozó jogi szabályozás, de tőzsdei bevezetést követően az értékpapírok tőzsdei bevezetésére vonatkozó szabályok betartása is. Így egy értékpapír-minősítés kifejezetten versenyhátrányt jelent a többi kriptovalutához képest azon kriptoérme kibocsátójának, aki ezt a minősítést megkapta, azzal szemben, aki által a kibocsátott kriptovaluta nem értékpapírként kerül meghatározásra."[68] 2021. január 1-től a magyar Btk. egyik módosítása a pénzmosás tényállása mellett annak elkövetési tárgyát is megváltoztatta, pont azért (a jogszabály indokolása szerint is), hogy például a tokenek és más hasonló aktívák bevonhatók legyenek ebbe a körbe, elkövethető legyen rájuk a bűncselekmény. Valamint rámutatnak a szerzők, hogy a „kriptovaluták kibocsátásának és tőzsdei kereskedésének a szabályozása és felügyelete éppen azok határterületi elhelyezkedése miatt jelent komoly kihívást a szabályozó hatóságok számára."[69] Manapság számos „online fizetési rendszer és digitális fizetőeszköz anonim, ami vonzóvá teszi őket a terrorizmus finanszírozása szempontjából, különösen akkor, ha a fizetési rendszer egy viszonylag gyengébb pénzmosás/terrorizmus finanszírozás elleni rezsimű joghatóságban működik. A virtuális fizetőeszközök komoly pénzügyi innovációs lehetőséget jelentenek, de számos bűnözői csoport figyelmét is felkeltették, és terrorizmus finanszírozási kockázatot jelenthetnek."[70]

A kriptovaluták és más virtuális fizetőeszközök lényegében elektronikus pénzként viselkednek, nem derivatív

[67] *Social Media And Terrorism Financing*. APG/MENAFATF, Sydney South, 2019. 12. o. (http://www.apgml.org/methods-and-trends/news/details.aspx?pcPage=1&n=1142); alapján Serbakov: i.m. (2022), 86. o.

[68] Kecskés András – Halász Vendel – Bujtár Zsolt: *Tőzsdeuniverzum*. Budapest, HVGORAC Kiadó, 2019, 220. o.

[69] Kecskés – Halász – Bujtár: i. m. (2019), 224. o.

[70] Serbakov: i. m. (2022), 87. o.

eszközökként. „A derivatív termék olyan pénzügyi szerződés, amelynek értéke az alapul szolgáló piaci tényezők, például kamatlábak, valutaárfolyamok és árucikkek, hitel- és részvényárak teljesítményéből származik. A származékos ügyletek a pénzügyi szerződések széles választékát foglalják magukban, beleértve strukturált adósságkötelezettségeket és betéteket, swapokat, határidős ügyleteket, opciókat, fedezeti ügyleteket és ezek különféle kombinációit."[71] – olvasható The Office of the Comptroller of the Currency (OCC) honlapján, amely a U.S. Department of the Treasury egyik szervezete. Vagyis derivatívák csak olyan pénzügyi szerződések lehetnek, amelyek árfolyama egy másik eszköz árfolyamához kötött. Sem a definícióban, sem a hozzá kapcsolódó egyéb elemzésekben nem szerepel, hogy egy elektronikus pénz derivatív eszköznek tekinthető. A származékos ügyletek (derivatívák) egyik legfontosabb jellemzője a szakirodalom szerint az, hogy jelentős hitelmennyiség található mögöttük, vagyis egyik fő jellemzőjük a tőkeáttétel. „Látható tehát a fentiekből, hogy a származtatott ügyletekben hatalmas mennyiségű hitel található, ami gyakorlatilag a kötvény, részvény, árupiaci termékek piacán kötött ki."[72] A derivatívák fajtái:

- CFD[73] termékek (index, futures, részvény CFD)
- határidős piaci termékek
- opciós termékek
- deviza forward ügyletek
- certifikátok, warrantok.[74]

Az elektronikus pénzek illetve a készpénz-helyettesítő fizetési eszközök mögött értelemszerűen nem áll hitel, a derivatíváknak pedig éppen ez az egyik legfontosabb jellemzője. Az elektronikus pénzek tehát emiatt terrorizmus finanszírozására és bármilyen más illegális tevékenységre (például pénzmosás elkövetésére) könnyebben felhasználhatók, mint a derivatív eszközök vagy egyéb hagyományos pénzügyi termékek, nem is említve az azonosításhoz kötött bankszámlákat.

Végül az internetes pénzügyi szolgáltatások is felhasználhatók online terrorizmus finanszírozására és más bűncselekmények elkövetésére egyaránt. „Az előre feltöltött számlák, melyeket online árverési fizetésekhez használnak, a legdominánsabb internetes pénzügyi szolgáltatásokhoz tartoznak. Előfordulhat, hogy a kedvezményezetteknek regisztrálniuk kell a pénzforgalmi szolgáltatónál, hogy átutalást kapjanak. Néhány olyan online fizetési rendszeren keresztül, mint a PayPal, alacsony értékű tranzakciókkal kapcsolatos terrorizmus finanszírozási ügyeket kapcsoltak össze számos terrorista gyanúsítottal."[75]

***

A 2001. szeptember 11-i terrortámadás után a terrorizmus elleni harc szinte minden

[71] https://www.occ.treas.gov/topics/supervision-and-examination/capital-markets/financial-markets/derivatives/index-derivatives.html.
[72] https://elemzeskozpont.hu/szarmaztatott-ugylet-derivativa-jelentese-fogalma-mik-azok.
[73] A CFD az olyan instrumentumokat foglalja magába, amelyeket a nyitó és záró értékek közti különbséggel kereskednek.
[74] https://elemzeskozpont.hu/szarmaztatott-ugylet-derivativa-jelentese-fogalma-mik-azok.
[75] Serbnakov: i. m. (2022), 98. o.

országban bekerült az elsődleges preferenciák közé.[76] 2002-ben az Európai Unió kerethatározatában ítélte el a terrorizmust, és kimondta: „Az Európai Unió az emberi méltóság, a szabadság, az egyenlőség és a szolidaritás egyetemes értékei, az emberi jogok és alapvető szabadságjogok tiszteletben tartása alapján áll, s a demokrácia és a jogállamiság – tagállamai által közösen vallott – elvein alapul. A terrorizmus ezen elvek egyik legsúlyosabb megsértése."[77] A magyar Országgyűlés a terrorizmus finanszírozásának visszaszorításáról, New Yorkban, az Egyesült Nemzetek Közgyűlésének 54. ülésszakán, 1999. december 9-én elfogadott nemzetközi egyezményt a 2002. évi LIX. törvénnyel hirdette ki. Ennek az Egyezménynek a 18. cikke kimondja, hogy a „Részes Államok együttműködnek a 2. cikkben meghatározott bűncselekmények megelőzésében minden lehetséges intézkedés megtételével, többek között belső jogszabályaik szükség szerinti, arra irányuló módosításával, hogy területükön megelőzzék és elhárítsák az ilyen bűncselekmények területükön vagy területükön kívül történő elkövetését célzó előkészületeket, ideértve […] azokat az intézkedéseket, amelyek előírják pénzintézeteknek és pénzügyi műveletekkel foglalkozó más hivatást gyakorlóknak, hogy a rendelkezésükre álló leghatékonyabb eljárásokat alkalmazzák szokásos vagy alkalmi ügyfeleik, továbbá azon ügyfeleik azonosítására, akiknek az érdekében számlát nyitnak, továbbá hogy fordítsanak különös figyelmet a szokatlan vagy gyanús műveletekre, és jelentsék be a vélhetően bűnöző tevékenységből származó műveleteket."

A terrorizmus elleni küzdelem anyagi büntetőjogi eszközei a 2001-es amerikai terrortámadások óta mind nemzetközi, mind európai, mind pedig hazai szintén jelentős fejlődésen mentek keresztül. A fellépés összetett jellegét mutatja, hogy nemcsak az egyes tényállások, de az egyéb büntetőjogi intézmények is bekapcsolódtak ezen megújulási folyamatba. Kijelenthető, hogy a terület büntetőjogi leszabályozottsága jelenleg sokkal szélesebb, mint korábban bármikor is volt. A büntetőjogi felelősségre vonás előbbre hozatalát célzó sui generis jellegű tényállások révén lehetőséget ad a büntetőjog arra, hogy már egész „korán" kiemelhetők legyenek a terrorgyanús személyek a társadalomból. Az egységesítő szándék pedig hozzásegít bennünket ahhoz, hogy az egyes terrorizmushoz kapcsolható cselekményeket egyformán lehessen megítélni, azok motivációjától, vagy éppen a végrehajtás formájától függetlenül. A terrorizmus elleni küzdelem dimenziónak rendszerében tehát központi helyet kapnak a büntetőjogi eszközök.[78]

[76] A terrorizmus elleni hatékony küzdelem csak az integrált bűnüldözés keretében képzelhető el. Ezzel kapcsolatban ld. részletesen Herke Csongor: Integrált bűnüldözés. Tremmel Flórián –Fenyvesi Csaba – Herke Csongor: *Kriminalisztika.* Budapest, Ludovika Egyetemi Kiadó, 2012, 424–440. o.

[77] A Tanács kerethatározata (2002. június 13.) a terrorizmus elleni küzdelemről, 2002/475/IB, HL 2002 L 164, 2002. június 22., 3.

[78] Bartkó Róbert – Farkas Ádám: A terrorizmus elleni harc nemzetközi jog trendjei. In.: Farkas Ádám – Végh Károly (szerk.): *Új típusú hadviselés a 21. század második évtizedében és azon túl – intézményi és jogi kihívások.* Budapest, Zrínyi Kiadó, 2020, 127. o.

A terrorizmus bármely formájáról is legyen szó, a jelenlegi anyagi jogi fegyverzet annak minden, modern kori megnyilvánulásával szemben hatékony eszköz a hatóságok kezében, így büntetőjogi szempontból nem jelent problémát, ha a terrorista akció a kibertér felhasználásával kerül elkövetésre. Minthogy azonban a kifejezetten a kibertérben elkövetett terrorista akciók száma nem mondható kimagaslónak, hiszen a terroristák legfőbb célzata, a félelemkeltés még mindig a klasszikus végrehajtási módokon érhető el a legeredményesebben, figyelmünket alapvetően a terroristák egyéb internet-használati aktivitására kell fordítanunk. Ennek egyrészt az az oka, hogy az egyéb bemutatott célok révén az internet a terrorista szervezetek erősödéséhez, az egyes akciók előkészítéséhez szervesen járulhat hozzá közép-, és hosszútávon, másrészt pedig az, hogy ezen internet-használati tevékenység hatóságok általi feltérképezése, lekövetése hozzá tudja segíteni a demokratikus államokat korunk egy legnagyobb biztonsági kihívásával, a nemzetközi terrorizmussal szembeni átfogó fellépés eredményességéhez.

A kiberterrorizmus tehát valós veszély, és ahogyan szokás mondani, „jobb félni, mint megijedni" ezen a fronton, ugyanakkor fontos, hogy a fellépés irányát és módszertanát jól tudjuk súlypontozni az ellene való küzdelemben. Ebben a tekintetben pedig álláspontom szerint az egyéb internet-használati tevékenységet kell a fókuszpontba helyezni – mivel a klasszikus értelemben vett kiberterrorista akciókkal szembeni fellépés kereteit az anyagi büntetőjog biztosítja -, hiszen ebben a szegmensben lehet a leghatékonyabban megakadályozni a kriminalitás eszkalálódását. A biztonsági kihívás tehát adott, az eszközrendszer pedig folyamatosan fejlődik. Ugyanakkor ez egy olyan próbatétel, ahol az védelmi rendszerek, felderítési módszerek fejlődése is szabadabb környezetben tud megvalósulni. A hangsúly egyértelműen a folyamatos fejlődés igényén van, hiszen maga a kibertér is az állandó változások terrénuma. Ahogyan *Nagy* fogalmaz már hivatkozott tanulmányában: „a technológiai fejlődés növekedésének üteme exponenciális, azoknak az országoknak, amelyek nem tartanak lépést napjaink fejlődésével, nem alkalmazkodnak a változásokhoz, a lemaradásuk is exponenciális lesz".[79]Az elmúlt időszak védelmi fejlesztései azonban arra engednek következtetni, hogy a demokratikus erők nem kívánnak ilyen mérvű hátrányba kerülni a terrorizmus elleni küzdelemben. Ez pedig mindenképp bizakodásra, biztonságérzetünk erősödésére adhat alapot.

FELHASZNÁLT FORRÁSOK

[1] Ambrus István: *Digitalizáció és büntetőjog.* Budapest, Wolters Kluwer Hungary Kft, 2021.

[2] Bartkó Róbert – Farkas Ádám: A terrorizmus elleni harc nemzetközi jog trendjei. In.: Farkas Ádám – Végh Károly (szerk.): *Új típusú hadviselés a 21. század második évtizedében és*

[79] Nagy: i. m. (2018), 38. o.

azon túl – intézményi és jogi kihívások. Budapest, Zrínyi Kiadó, 2020.

[3] Bartkó Róbert: *A terrorizmus elleni küzdelem kriminálpolitikai kérdései.* Győr, UNIVERSITAS-Győr Nonprofit Kft, 2011.

[4] Bartkó Róbert: *Az irreguláris migráció elleni küzdelem eszközei a hazai büntetőjogban.* Budapest, Gondolat Kiadó, 2019.

[5] Bartkó Róbert: Az Unió 2017/541. sz. Irányelvének hatása a V4 országainak büntető anyagi jogszabályalkotására. In: Bartkó Róbert (szerk.): *A terrorizmus elleni küzdelem aktuális kérdései a XXI. században.* Budapest, Gondolat Kiadó, 2019.

[6] Beers R – Taylors FX: Narco-Terror: The Worldwide Connection Between Drugs and Terror. *Terrorsim and Goverment Information*, 2002.

[7] Berry LV – Curtis GE, Hudson RA – Kollars NA: *A Global Overview of Narcotics-Funded Terrorist and Other Extremist Groups*, Library of Congress 2002.

[8] Böröcz Miklós: Az Európai Unió közös kül-, és biztonságpolitikájának néhány főbb kihívása napjainkban. *Terror & Elhárítás*, 2013/2. szám.

[9] Cian C. Murphy: Counter-Terrorism Law and Policy: Operationalisation and Normalisation of Exceptional Law after the 'War on Terror. Diego Acosta Arcarazo –Cian C. Murphy: *EU Security and Justice Law: After Lisbon and Stockholm*. London, Hart Publishing Ltd., 2014

[10] Clarke L – Leppard D: Photos link more IRA Men to Colombia. *Sunday Times*, 2002.

[11] Dornfeld László: Kiberterrorizmus – a jövő terrorizmusa? In. Mezei Kitti (szerk.): *A bűnügyi tudományok és az informatika.* Pécs, Budapest, PTE ÁJK – MTA Társadalomtudományi Kutatóközpont, 2019.

[12] Edvi Illés Károly: *Az anyagi büntető törvények és a sajtótörvény.* Budapest, Grill Károly Könyvkiadó Vállalata, 1907.

[13] Farkas Ádám: A terrorizmus elleni harc, mint kiemelt ágazatközi fegyveres védelmi feladat. *Szakmai Szemle*, 2017/3. szám.

[14] Farkas Ádám: Gondolatok a 21. századi biztonságról, államról, védelemről. *Hadtudomány*, 2018/elektronikus szám.

[15] Farkas Ádám: Gondolatok a terrorveszélyhelyzetről. *Szakmai Szemle*, 2016/3. szám.

[16] Gál István László: *A terrorizmus finanszírozása. Die Terrorismusfinanzierung,* Pécs, Pécsi Tudományegyetem Állam- és Jogtudományi Kar Gazdasági Büntetőjogi Kutatóintézet Pécs, 2010.

[17] Gergely Attila: A terrorizmus természetrajza. *Kapu*, 1994/10-11. szám.

[18] Gerhard Wisnewski – Wolfgang Landgraeber – Ekkehard Sieker: *Das RAF-Phantom Neue Ermittlungen in Sachen Terror.* München, Knaur Taschenbuch Verlag, 2008.

[19] Gunaratna R: *Inside Al Quaeda: Global Network of Terror*. London, Hurst&Company, 2002.
[20] Herke Csongor: Integrált bűnüldözés. Tremmel Flórián – Fenyvesi Csaba – Herke Csongor: *Kriminalisztika.* Budapest, Ludovika Egyetemi Kiadó, 2012.
[21] Jessica Davis: *New Technologies but Old Methods in Terrorism Financing.* London, Royal United Services Institute for Defence and Security Studies, 2020.
[22] Kecskés András – Halász Vendel – Bujtár Zsolt: *Tőzsdeuniverzum.* Budapest, HVGORAC Kiadó, 2019.
[23] Kelemen Roland – Németh Richárd: A kibertér fogalmának és jellemzőinek multidiszciplináris megközelítése. In: Farkas Ádám (szerk.): *Védelmi alkotmányosság az új típusú biztonsági kihívások erőterében.* Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2018.
[24] Kelemen Roland: A kibertérből érkező fenyegetések jelentősége a hibrid konfliktusokban és azok várható fejlődése. *Honvédségi Szemle*, 2020/4. szám.
[25] Kelemen Roland: Pillanatképek a kivételes állapot elméleti kérdéseinek köréből. *Katonai Jogi és Hadijogi Szemle*, 2016/1-2. szám.
[26] Kelemen Roland: Radikalizálás, dezinformálás és tömegpszichózis modern köntösben: a hibrid konfliktus kibertérben. *Jog Állam Politika,* 2021/3. szám.
[27] Korinek László: A terrorizmus. Gönczöl Katalin – Kerezsi Klára – Korinek László – Lévay Miklós (szerk.): *Kriminológia-Szakkriminológia*. Budapest, CompLex kiadó, 2006.
[28] Korinek László: *Kriminológia.* Budapest, Magyar Közlöny Lap- és Könyvkiadó Kft, 2010.
[29] Lajtár István: A kiberbűnözésről. *Ügyészek Lapja* 2019/1. szám.
[30] Mezei Kitti – Szentgáli-Tóth Boldizsár: Az online platformok használatában rejlő veszélyek: a dezinformáció és a kibertámadások jogi kockázatai. In. Chronowski Nóra – Szentgáli-Tóth Boldizsár – Szilágyi Emese (szerk.): *Demokrácia – Dilemmák. Alkotmányjogi elemzések a demokráciaelv értelmezéséről az Európai Unióban és Magyarországon.* Budapest, ELTE Eötvös Kiadó, 2022.
[31] Mezei Kitti: *A kiberbűnözés aktuális kihívásai a büntetőjogban.* Budapest, TKJTI, L'Hartmann, 2020.
[32] Mezei Kitti: A modern technológiák kihívásai a büntetőjogban, különös tekintettel a kiberbűnözésre. *Állam- és Jogtudomány*, 2020/4. szám.
[33] Mezei Kitti: Cyberterrorism – How real is the threat? In.: Szőke Gergely László (szerk.): *Studia Iuridica Auctoritate Universitatis Pécs Publicata. Essays of Faculty of Law University of Pécs Yearbook of 2017-2018.* Pécs, Pécsi Tudományegyetem, 2020.
[34] Nagy Zoltán András: A jövő tegnap óta tart. A modern technikai-technológiai folyamatok kihívásai a jog területén. *Belügyi Szemle*, 2018/10. szám.

[35] Nagy Zoltán András: Kiberbűncselekmények, kiberháború, kiberterrorizmus – avagy ébresztő Magyarország! *Magyar Jog*, 2016/1. szám.
[36] Napoleoni L: *Modern Jihad: Tracing the Dollars Behind the Terror Networks*. London, Pluto Press, 2003.
[37] Neparáczki Anna Viktória: A kiberterrorizmus büntető anyagi jogi megítélése. *Ügyészek Lapja,* 2020/1. szám.
[38] Neparáczki Anna Viktória: *A terrorizmus elleni fellépés eszközei a magyar és a német anyagi büntetőjogban. PhD értekezés*, Pécs, 2017.
[39] Rostoványi Zsolt: Terrorizmus és szabadság. Fundamentum, 2001/4. szám.
[40] Sean S. Costigan – David Gold: *Terronomics ASHGATE.* Printed in Great Britain, 2007.
[41] Sean S. Costigan – David Gold: *Terronomics ASHGATE.* Printed in Great Britain, 2007.
[42] Serbakov Márton Tibor: *Egyes szélsőséges terrorista csoportok internethasználata egyes aspektusainak elemzése PhD értekezés.* Pécs, Pécsi Tudományegyetem, 2022.
[43] Sieber – Vogel.: *Terrorismusfinanzierung: Prävention im Spannungsfeld von internationalen Vorgaben und nationalem Tatstrafrecht.* Berlin, Duncker & Humblot, 2015.
[44] Simicskó István (2016): A terrorizmus elleni védelem fokozása a különleges jogrendi kategóriák bővítésével. *Hadtudomány*, 3-4. szám.
[45] Steven Mark Levy: *Federal Money Laundering Regulation (Banking, Corporate, and Securities Compliance)*. New York, 2003.
[46] Szádeczky Tamás: Terrorizmus a kibertérben. *Infokommunikáció és Jog,* 2008/5. szám.
[47] Szövényi György: A terrorizmus jellegzetességei az ezredfordulón. *Európai Tükör*, 1998/3. szám.
[48] Thomas J. Bierstecker – Sue E. Eckert (szerk.): *Countering th Financing of Terrorism*. London, New York, 2008.


UNIVERSITY OF PUBLIC SERVICE
LUDOVIKA

Military and Intelligence CyberSecurity Research Paper 2022/12.

Szerző(k) / Author(s):
Prof. Dr. Gál István PhD – Dr. habil. Bartkó Róbert PhD

Kézirat lezárásának ideje / Manuscript closing time:
2022.11.15.

Szerkesztők / Editors:
Dr. Farkas Ádám PhD
Dr. Magyar Sánor PhD

Kiadó / Publisher:
Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar
Nemzetbiztonsági Intézet Katonai Nemzetbiztonsági Tanszék
University of Public Service (Hungary), Faculty of Military Sciences and Officer Training, National Security Institute Department of Military National Security

Kiadó képviselője / Representative of the publisher:
Prof. Dr. Resperger István PhD

Elérhetőségek /Contacts:
https://hhk.uni-nke.hu/oktatasi-egysegek/katonai-nemzetbiztonsagi-tanszek/katonai-nemzetbiztonsagi-kiberter-muveleti-szakcsoport/research-paper

farkas.adam@uni-nke.hu | magyar.sandor@uni-nke.hu

1011 Budapest, Hungária krt. 9-11. /9-11. Hungária Blvd., Budapest, H1011

ISSN:
2786-3778

A borító https://www.stockvault.net/photo/270507/cyber-security-web-security-network-security címen elérhető ingyenes háttérkép felhasználásával 2021. február 25-én készült.

The cover was created on 25. February 2021, using a free wallpaper available at https://www.stockvault.net/photo/270507/cyber-security-web-security-network-security.

A sorozat egyes számaiban foglalt vélemények, állásfoglalások a szerzők saját véleményét tükrözik. Azok nem tekinthetők sem a kiadó, sem a szerzőt foglalkoztató intézmények hivatalos álláspontjának.
The opinions and resolutions included in each issue of the series reflect the authors' own opinions. They should not be construed as an official point of view of either the publisher or the institutions employing the author.

Nemzeti Kutatási, Fejlesztési és Innovációs Hivatal
AZ NKFI ALAPBÓL MEGVALÓSULÓ PROGRAM