NEMZETBIZTONSÁGI SZEMLE
9. évfolyam (2021) 3. szám 54–64. • DOI: 10.32561/nsz.2021.3.4

Eck Gábor[1]

# A terrorizmus és az információs tér kapcsolódási pontjai

*Links between Terrorism and the Information Space*

*A digitális kultúra, a mobileszközök és a közösségi média nélkülözhetetlen részévé vált az életünknek. A legfrissebb felmérések szerint a Föld népességének 60 %-a használja az internetet, így a közösségi média alkalmazóinak száma meghaladja a 3,8 milliárdot. Egy átlagos internetező naponta közel 6 óra 45 percet tölt el a világhálón, ebből közel 2 óra 30 percet közösségi média használatával. Ezek a számok folyamatosan emelkedő tendenciát mutatnak. A világ népességének jelentős része elérhető a virtuális térben, ezért érdemes megvizsgálni, hogy a terrorizmus és az abban érintett személyek hogyan viszonyulnak a digitalizáció nyújtotta lehetőségekhez, és ez milyen kihívások elé állítja a biztonságért felelős szerveket.*

***Kulcsszavak:*** *internet, közösségi média, biztonság, terrorizmus*

*The digital culture, the use of cellular devices and the use of the social media have become an essential part of our lives. According to the latest surveys, 60 percent of the world's population uses the Internet, which means that there are more than 3.8 billion social media users. The average internet users spend nearly 6 hours and 45 minutes a day on the web, including nearly 2 hours and 30 minutes using social media. These figures show an upwarding trend. A significant part of the world's population is available in the cyberspace, so it is worth to see how terrorism and people affected by this phenomenon react to the potential of digitalisation and what kind of new challenges security bodies face.*

***Keywords:*** *internet, social media, security, terrorism*

[1] Doktori hallgató, Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola, e-mail: eck.gabor@icloud.com

## 1. Bevezetés

Manapság olyan világban élünk, amelyben a számítógépek, az okoseszközök és a rajtuk keresztül elérhető hálózatok aktív és nem elkerülhető részei mindennapjainknak, segítik, támogatják szervezik azt, ám ha nem figyelünk kellően oda, irányíthatják is tevékenységünket.[2] Természetesen e technikai vívmányok tudatos használatával kényelmesebben tarthatunk lépést felgyorsult világunkkal. Minél jobban átszövi életünket a technika, annál inkább megjelennek biztonsági kérdések is a használattal, valamint a felhasználókkal kapcsolatban, hiszen minden új, az életünk részét képező dolognak vannak árnyoldalai, „alternatív felhasználási" lehetőségei.

Tanulmányomban rá kívánok világítani a terrorizmus elleni küzdelem és az információs tér, valamint az ott használt eszközök kölcsönhatásaira, be kívánom mutatni a terrorszervezetek internetes törekvéseit, az azokhoz kapcsolódó fenyegetéseket és kihívásokat.

Célom, hogy a fogalmi meghatározások tisztázása, a terrorizmus kibertérben zajló mozzanatainak bemutatása és az azokra adható válaszok révén élesítsem a képet az online világban tapasztalható biztonsági kihívásokról.

## 2. Terrorizmus – kiberterrorizmus

A terrorizmus meghatározásával kapcsolatban sok álláspont született, de nemzetközileg elfogadott terminust nem sikerül még alkotni. Érdemes a teljesség igénye nélkül néhány definíciót ismertetni.

Benjamin Netanjahu szerint: „A terrorizmus a polgárokon gyakorolt szándékos, módszeres erőszak, amely az általa kiváltott félelmen keresztül politikai célokat kíván megvalósítani."[3]

A NATO által használt definíció szerint a terrorizmus „[e]rőszak jogellenes alkalmazása, vagy azzal való fenyegetés, amely félelmet vagy rettegést kelt, egyének vagy tulajdon ellen, kormányok vagy társadalmak kényszerítésére vagy megfélemlítésére, vagy a lakosság feletti ellenőrzés megszerzésére, politikai, vallási vagy ideológiai célok elérésére".[4]

Korinek László meghatározásában:

> „A terrorizmus eltérő eszmerendszerekből merítő, sajátos logikának engedelmeskedő, változatos formákat öltő módszeres erőszak alkalmazása, 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, etnikai tartalmú radikális változás kikényszerítése, a cél elérésére alkalmazott

[2] Vö. *Global Digital Overview. Digital in 2020.*
[3] Benjamin Netanjahu: *Harc a terrorizmus ellen*. Pécs, Alexandra, 1995. 20.
[4] Nato Unclassified: MC 0472/1 Military Committee Concept For Counter-Terrorism.

cselekménysor. Az eszköz viszont jogi lényegét tekintve köztörvényes, erőszakos bűncselekmény."[5]

Resperger István úgy véli: „A terrorizmus terroristák (egyének vagy csoportok) által, politikai célok elérése érdekében, főként a polgári lakosságon, erőszakos eszközökkel folytatott tevékenység, abból a célból, hogy akaratukat az ellenfélre kényszerítsék."[6]

A fogalom vizsgálata során joggal merül fel a kérdés, hogy a virtuális téren keresztül hogyan lehetséges erőszakot alkalmazni, vagy azzal olyan módon fenyegetni, hogy az alkalmas legyen a kitűzött célok elérésére. Az elmúlt évek terrortámadásai megismertették velünk a félelemnek azon szegmenseit, amelyek képesek a tőlünk nagyobb távolságra lévő borzalmakat is érezhetővé tenni. Egy bekövetkezett támadás híre szinte azonnal eljut a világ bármelyik részére, a helyszínen tartózkodó emberek élő, egyenes adásban közvetítik a történéseket, így a technika segítségével jóformán a saját bőrünkön érezzük a következményeket, az események részeseivé válunk. Érdemes elgondolkodni azon, hogy a mindenáron érvényesülő közléskényszerünk, a rettenet ilyen módon való transzportálása mennyire segíti a terroristákat céljaik elérésében, gondolok itt a megfélemlítésre, kényszerítésre, valamint az irányítás átvételére. Bruce Schneier amerikai biztonsági szakértő szerint a terrorizmus valódi lényege nem maga a cselekmény, hanem az arra adott reakció."[7]

Természetesen a terroristák számára nem csak a korábban említett közvetett módon érhető el az információs tér nyújtotta potenciál, annak pozitívumait aktívan is használják céljaik megvalósítása érdekében. Ezen a ponton elkerülhetetlen egy újabb fogalom, a kiberterrorizmus definíciójának a vizsgálata. A terrorizmushoz hasonlóan a kiberterrorizmusnak sincs egy egységesen elfogadott és kiforrott meghatározása. A téma szakértői egyetértenek abban, hogy a terrorizmus és a kibertér fogalmaiból kell kiindulni, és azokat ötvözve lehet legközelebb jutni a keresett értelmezéshez.

A terrorizmus fentebb említett fogalmát tehát ki kell egészítenünk a kibertér fogalmával, ami egy újabb komoly kihívás, hiszen minden terület a saját maga számára jelentős tényezőket emeli ki. Munk Sándor ebből a gondolatból kiindulva a következőket mondja: „egyes alkalmazás- vagy szakterületek a kérdések megválaszolásával (ha eddig nem tették volna meg) maguk és mások számára is pontosabban meg tudják határozni kibertér-értelmezésük részletes tartalmát, illetve, hogy a különböző értelmezések összehasonlíthatók, eltéréseik feltárhatók".[8] Ettől függetlenül szükséges egy olyan fogalmi meghatározás, amely felülemelkedik a fenti problémán, és ad egy általános, mindenki számára elfogható definíciót. Haig Zsolt és Kovács László álláspontja szerint a kibertér az elektronikus kommunikációs technológiák, valamint az azokon megtalálható szolgáltatások és információk, adatok alkotta virtuális tér.[9]

---

5 Gönczöl Katalin et al.: *Kriminológia – Szakkriminológia.* Budapest, CompLex, 2006. 447.

6 Resperger István: A nemzetbiztonsági szolgálatok tevékenysége – biztonsági kihívások, kockázatok és fenyegetések. In Resperger István (szerk.): *A nemzetbiztonság elmélete a közszolgálatban.* Budapest, Dialóg Campus, 2018. 76.

7 Bruce Schneier: *A biztonságról.* Budapest, HVG, 2010. 16.

8 Munk Sándor: A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései. *Haditechnika,* (2018), 1. 114.

9 Haig Zsolt – Kovács László: Fenyegetések a cybertérből. *Nemzet és Biztonság,* 1. (2008), 5. 61–69.

Dorothy E. Denning amerikai információbiztonsági kutató a kiberterrorizmusra mint a terrorizmus és a kibertér fúziójára tekint. Véleménye szerint azokat a számítógépek, hálózatok és az azokban tárolt információk elleni jogellenes támadásokat és támadásokkal való fenyegetéseket lehet általában kiberterrorizmusnak nevezni, amelyek a kormányzatok vagy azok szervei ellen irányulnak, illetve a politikai vagy társadalmi céljaikkal, érdekeikkel szemben igyekeznek őket valamire kényszeríteni. Ahhoz, hogy a jelenséget vagy a tevékenységet kiberterrorizmusnak minősíthessük, a támadásnak személyekkel vagy vagyonnal szembeni erőszakkal kell járnia, illetve elegendő kárt kell okoznia a félelem kiváltásához.[10]

## 3. Hacker – kiberterrorista – online terrorista

Meg kell vizsgálnunk, hogy a fenti meghatározásokkal összefüggésbe hozható személyek között hogyan lehet különbséget tenni. Ahogyan a valós körülmények között is igen komoly feladatot, elhatárolási problémát jelenthet a felkelőt a terroristától megkülönböztetni,[11] ugyanúgy a virtuális térben megjelenő szereplők között is elengedhetetlen az eltérések megállapítása. De kik is ezek a szereplők, van-e közöttük kapcsolat, és ha igen, akkor ennek mik a jellemzői?

Kazári szerint a *hacker* olyan kimagasló számítástechnikai tudású személy, aki szigorúan segítő jelleggel feltárja a számítógépes rendszerek/alkalmazások előnyeit és hibáit, illetőleg javít azokon.[12] A meghatározásból ki kell emelnünk a segítő jelleget, tehát a hackerek a meglévő többlettudásukat a közjó, az internet népének boldogulása szolgálatába állítják. A hackerkultúra nem gazdasági vagy társadalmi formáció, egy valódi hacker szabadelvű, a hierarchikus viszonyokat erősen tagadó, a materiális javak megszerzését figyelmen kívül hagyó entitás, aki megelégszik a többiek figyelmével, elismésével, és ezért minden alkotását szabadon hozzáférhetővé teszi.[13]

Természetesen ebben a szubkultúrában is megjelentek, megjelennek olyanok, akik a fenti etikai szemléletet nem vagy nem teljesen gondolják követendőnek, és céljuk az anyagi haszonszerzés vagy egészen egyszerűen csak kellemetlenség, probléma okozása másoknak, illetőleg ezek kombinációja. Ennek a morális határnak az átlépésével sokkal inkább beszélhetünk kiberbűnözőkről, mint a közösséget önérdek nélkül támogató, magas színvonalú specialistákról. Ezek a személyek ideális alanyai lehetnek egy terrorszervezet célkitűzéseit – akár a valódi cél ismerte nélkül – támogató, a virtuális térben a szükséges háttértudást biztosító sejtnek. Elmondhatjuk, hogy kiberterrorista az, aki a speciális számítástechnikai tudásával a valódi célok ismeretével vagy azok tudta nélkül terrortevékenységet támogat. Így a terrorizmus, a kiberterrorizmus és a kiberbűnözés elleni fellépésnek egy közös, bűnüldözői és nemzetbiztonsági szegmensekkel is rendelkező feladatrendszernek kell lennie.

---

10 *Statement of Dorothy E. Denning.* Georgetown University, (é. n.).

11 Lásd bővebben: Resperger István: Az aszimmetrikus hadviselés és a terrorizmus jellemzői. *Hadtudomány,* (2010), 4. 74.

12 Kazári Csaba: *Hacker, cracker, warez. A számítógépes alvilág titkai.* Budapest, Computer Panoráma, 2003. 18.

13 Eric S. Raymond: *How To Become A Hacker.*

Természetesen nem szabad megfeledkeznünk arról a kategóriáról sem, amikor a terrorcselekményekhez köthető személyek az informatikai, technikai, infokommunikációs eszközök biztosította lehetőségeket használják célkitűzéseik elérése érdekében. A fenti lehetőségek használata során technikailag nincs különbség a „rendes" (rendeltetésszerű) és a rosszindulatú igénybevétel között. Az ilyen esetekben a külső szemlélő számára teljes az azonosság, és a használatban rejlő anomáliák sok esetben még az alapos adatelemzés során sem, vagy csak részben kimutathatók.

## 4. Lehetőségek a kibertérben

A fogalmak tisztázását követően érdemes áttekinteni, hogy a terrorszervezetek szervezői, a terrorcselekmények tervezői, elkövetői mennyire közvetlen módon látják hasznát a kibertérhez kapcsolódó infokommunikációs eszközök és hálózatok által kínált technikai újdonságoknak.

### *4.1. Toborzás – ideológiaterjesztés – támogatás*

Tevékenységük során a terroristák a toborzás, a kapcsolattartás, a támogatások megszerzése és továbbítása (terrorfinanszírozás), valamint az ideológia-terjesztés (indoktrináció) területén is támaszkodhatnak a kibertér által biztosított lehetőségekre. Ezek értelmezhetők úgy is, mint a mindenki számára elérhető és használható technológia fejlődésében rejlő esély, és úgy is, mint egy állandóan változásban lévő és fejlődő területen fellelhető, az átlagos, hétköznapi ember tudását meghaladó, speciális szakértelmet kívánó lehetőségek.

Az új technológiák drámai mértékben megnövelik a terrorizmussal összefüggésbe hozható online tartalmak globális elérhetőségét. A közösségi média lehetővé teszi a terrorszervezetek, -csoportok számára, hogy propagandájukat terjesszék, és azonnal, költség és nagyobb fáradság nélkül toborozzanak követőket a világ bármely pontjáról. Néhány évtizeddel ezelőtt az egyéni radikalizációs folyamat személyes kontaktust igényelt, ezt követően a radikális imámok audió-felvételek terjesztésével próbálták minél szélesebb körben terjeszteni tanaikat, Oszáma bin Láden faxot használt vallási rendeleteinek továbbítására.[14]

Mára ez megváltozott, a szimpatizánsok nemcsak a terrorszervezetek által működtetett honlapokon, online magazinokon keresztül – mint például az Iszlám Állam által üzemeltetett Dabiq, Rumiya, Dar al-Islam vagy a Konstantiniyye –, hanem a közösségi média segítségével biztosított csatornákon is iránymutatást kaphatnak az ideológia elsajátítására, a szervezethez történő fizikai csatlakozásra, a támadások kivitelezésére. A közkedvelt közösségimédia-platformok „egy kattintással" lehetőséget biztosítanak felhasználók százezreinek elérésére, vagy akár nagy terjedelmű fényképek, videóanyagok továbbítására is. Az Iszlám Állam (ISIS) nevű terrorszervezet felismerte a közösségi média erejét és azt, hogy a toborzásuk szempontjából érdekes

[14] Kate Zernike – Michael T. Kaufman: *The Most Wanted Face of Terrorism*.

korosztályú személyek elsősorban ezekről a platformokról tájékozódnak. Az ISIS propagandistái 2015-ben egy hónap alatt 1146 bejegyzést tettek a Twitteren, amelyek között volt fotó, esszé, videó, nyilatkozat, rádiótájékoztató, szöveges összefoglaló; magazinok, plakátok, brossúrák, teológiai értekezések láttak napvilágot, és mindez oroszul, törökül, arabul, kurdul, franciául és angolul egyaránt megjelent.[15]

Ez a kiterjesztett világ komoly lehetőséget nyújt azoknak is, akik nem akarnak, mernek valódi, kézzelfogható segítséget nyújtani a terroristák toborzásához, ideológiájuk terjesztéséhez, de helyeslő magatartásukkal, a hirdetett tanokkal való rokonszenvük kimutatásával meghatározó ösztönzői lehetnek a radikalizációs folyamatoknak. Ezzel a tevékenységükkel pótolják a radikalizálódási folyamat érzelmi és pszichológiai részét, erősítve magukban az „egyetlen helyes út" szellemiségét. Sok esetben ebből a szerepkörükből tovább lépve, már közvetítőként funkcionálnak, kapcsolatot biztosítanak a már megnyert, beszervezett személyek és a terroristák között, illetőleg segítséget nyújtanak a terrorcselekmény elkövetőinek a célterületre való bejutáshoz, az ott-tartózkodáshoz és rejtőzködéshez. Természetesen a segítségnyújtás, támogatás megjelenhet egyéb, anyagi jellegű – a terrorizmus finanszírozásának klasszikus forrásain, lehetőségein túlmutató – formában is. A közösségi média és az online felületek alkalmazása nagyon sokrétű lehetőséget biztosít a terrorizmus pénzügyi támogatásának területén. Például amikor az egyik terrorszervezethez kapcsolódó személyek a Twitteren keresztül igyekeztek adományokat gyűjteni, arra kérték az adományozókat, hogy Skype-on vegyék fel velük a kapcsolatot. Itt aztán arra kérték az adományozókat, hogy szerezzenek be valamilyen nemzetközi feltöltőkártyát (ez lehet mobiltelefon-jóváírás, programok vásárlását vagy az internetes tartalom elérését biztosító vásárlás), és küldjék el nekik a jogosultságot igazoló azonosítókat. Az adománygyűjtő elküldte az azonosítókat Szíriába, ahol alacsonyabb áron értékesítették azokat, az ebből származó készpénz pedig a terrorszervezethez került.[16]

Az Iszlám Állam kötelékébe tartozó külföldi harcosok folyamatosan használták az internetet, posztjaikban törekedtek bemutatni a csatlakozó dzsihadistákra váró „kihagyhatatlan" lehetőségeket, így erősítve az esetleges kétkedőket.[17]

## *4.2. Kapcsolattartás*

A terroristák egymás közötti kommunikációjuk során az átlagemberek számára is elérhető, alkalmazható és használatukhoz kiemelkedő informatikai tudást nem igénylő kommunikációs hálózatokat, valamint az azokon működő és/vagy hozzájuk kapcsolódó eszközök kínálta lehetőségeket használják ki és alkalmazzák rossz szándékkal. Bármely szokványos készülék a hozzá tartozó hálózati elérésekkel és néhány konspirációs jellegű rendszabállyal jelentős segítséget nyújthat egy terrorcselekmény előkészítése, illetve végrehajtása során szükséges kommunikáció megkönnyítéséhez. A kapcsolattartásra kiváló lehetőséget biztosítanak a különböző infokommunikációs eszközök,

[15] Charlie Winter: Fishing and ultraviolence. *BBC News,* 2015. augusztus 1.

[16] Lásd a Pénzügyi Akciócsoport nevű kormányközi szervezet (Finantial Action Task Force, FATF) jelentését: *Emerging Terrorist Financing Risks*.

[17] Aris Roussinos: Jihad selfies, these british extremists in Syria love social media. *Vice,* 2013. december 5.

a közösségi oldalak és chatalkalmazások, mint ahogyan ezt a 2015. november 13-án Párizsban és 2016. március 22-én Brüsszelben végrehajtott terrortámadások után páratlan nemzetközi összefogással végrehajtott nyomozás adatai alátámasztották.[18]

A hétköznapi eszközök, technológiák, hálózatok terroristák, terrorszimpatizánsok általi használata komoly lehetőséget biztosít a terrorellenes fellépés hatékonyságának fokozására. A platformokon kihelyezett privát üzenetek lehetővé teszik a nemzetbiztonsági szolgálatoknak, hogy az adatok elemzése során terroristákat azonosítsanak és figyeljenek meg, kapcsolati hálókat térképezzenek fel, terrorizmushoz köthető tevékenységek mintázatait ismerjék fel. A nemzetbiztonsági szolgálatok e tevékenységük során az egyszerű, formális logikai és a kötött elemző-értékelő eljárásokra, valamint a komplex elemző-értékelő modellekre egyaránt támaszkodnak. Az eljárások és modellek – a terroristák azonosításán, megfigyelésén, kapcsolataik megismerésén túl – lehetőséget biztosítanak korai előrejelző rendszerek kiépítésére is.[19]

A kibertérben folytatott kommunikációjukban rejlő biztonsági deficitekkel a terrorszervezetek vezetői is tisztában vannak, voltak. Oszáma bin Láden az 1990-es években felhagyott műholdas telefonkészüléke használatával, miután sajtóhírek jelentek meg arról, hogy az amerikai nemzetbiztonsági szolgálatok ellenőrzik azt.[20] A sors fintora ugyanakkor, hogy rejtekhelyének felderítéséhez jelentősen hozzájárult testőre műholdas telefonhívásainak megfigyelése, rögzítése.[21] A Snowden-botrány kirobbanása előtt is jellemző volt a digitális konspiráció a terrorszervezetekre. Az al-Káida 2007-ben adta ki a „Mujahedeen Secrets”[22] nevű titkosító programját, amelyet hosszú időn keresztül használtak a szervezeten belül a szenzitív adatok védelmére.[23]

Az Edward Snowden által kiteregetett információk rávilágítottak arra, hogy az amerikai hatóságok mennyire támaszkodnak a terrorizmussal összefüggésbe hozható személyek megfigyelése során az interneten folytatott – sok esetben titkosítatlan – információcserékre, illetőleg az azok feldolgozásából és elemzéséből nyert adatokra.[24]

Ennek hatására a terroristaszervezetek rendkívüli gyorsasággal változtatták meg az internetes kommunikációjukhoz kapcsolódó biztonsági előírásokat. Az információcseréjük védelme érdekében többféle módszert alkalmaznak, ilyenek például a végpontok közötti titkosítás, a teljes eszköz titkosítása, VPN[25] és TOR[26] használata.

---

18 Mágó Károly: 14 terrorista járt Magyarországon a párizsi és brüsszeli merénylők közül. *Origo,* 2016. szeptember 30.

19 Kenedli Tamás – Vida Csaba: Elemző-értékelő tevékenység. In Dobák Imre (szerk.): *A nemzetbiztonság általános elmélete.* Budapest, Nemzeti Közszolgálati Egyetem, Nemzetbiztonsági Intézet, 2014.

20 Ronald Kessler: Why Osama bin Laden stopped using his intercepted phone. *The Washington Times,* 2018. augusztus 5.

21 Owais Tohid: Bin Laden bodyguard’s satellite phone calls helped lead US forces to hiding place. *The Christian Science Monitor,* 2011. május 2.

22 Nyílt forráskódú titkosító software, elsősorban e-mailen folytatott kommunikáció biztosítására.

23 See Morten Storm et al.: *My Life Inside al Qaeda and the CIA*. New York, Atlantic Monthly Press, 2014. 182–183.

24 Eric Schmitt – Ben Hubbard: ISIS Leader Takes Steps to Ensure Group’s Survival. *The New York Times,* 2015. július 21.

25 Virtual Private Network: az adatokat megosztott vagy nyilvános hálózaton keresztül úgy küldik, fogadják, mintha a használt eszköz közvetlenül kapcsolódna a helyi hálózathoz, ezzel az eredeti kapcsolódási hálózat rejtve marad.

26 The Onion Router: az internetes forgalmat több proxykiszolgálón keresztül továbbítja, így akadályozva meg a forgalom eredetének azonosítását.

E lehetőségek megismerése és elsajátítása érdekében az ISIS kiadott egy kézikönyvet,[27] támogatva a szimpatizánsok, tagok, kapcsolódó személyek biztonságos és a hatóságok előtt rejtett kommunikációját. A leírás segítséget nyújt a titkosított kommunikációt biztosító programok, applikációk használatához, a geolokációs információk azonosításához vezető adatok titkosításához, tanácsokat ad az adatvédelmi alkalmazások kezeléséhez. Az útmutató ajánlásokat tesz arra vonatkozóan, hogy mely levelezési platformokat, közösségi oldalakat kerüljék el az olvasói, valamint felhívja a figyelmet az eszközeik biztonságos használatához szükséges beállításokra. Az ISIS tevékenységének digitális támogatása terén a platformot használók számára rendkívül nagy segítség volt az állandó jelleggel működő helpdesk szolgáltatás kialakítása is. Ez lehetővé tette, hogy magasan képzett informatikai szakemberek szakmai támogatást nyújtsanak a terrorszervezettel kapcsolatban álló személyek biztonságos kommunikációjához.[28]

## *4.3. Támadás*

A kibertérből érkező fenyegetések következő, magasabb szintje, amikor egy terrorszervezethez köthető, annak céljait támogató hackerek támadnak meg kormányzati platformokat. Ilyen volt a 2015 januárjában az Amerikai Egyesült Államok Központi Katonai Parancsnokság[29] Twitter- és YouTube-fiókjait ért célzott támadás.[30] A parancsnokság Twitter-fiókját felhasználva az ISIS üzenetet tett közzé, amely szerint az USA szíriai, afganisztáni és iraki tevékenysége miatt támadni fogják a katonai és az ahhoz köthető hálózatokat, eszközöket. Hatékonyságuk bizonyítékául a Pentagonból származó katonai információkkal kiegészített térképeket, valamint nyugalmazott amerikai tábornokok adatait tartalmazó táblázatokat tettek közzé. Az esetet követően az említett fiókok elérhetetlenné váltak. Az amerikai Védelmi Minisztérium elismerte a támadások tényét, de tagadta, hogy minősített információ került volna a terroristák kezébe.[31]

Ez az incidens rámutat arra, hogy a terroristaszervezetek műszaki, informatikai fejlettsége már komoly fenyegetést jelent, és a védelmi intézkedések tervezése során nem szabad figyelmen kívül hagyni az ilyen jellegű támadások megelőzésére, elhárítására való felkészülést. Még megválaszolandó a kérdés, hogy – mivel a fentebb leírt informatikai támadó műveletekhez hasonló méretű és hatékonyságú akció jelenlegi ismereteink szerint azóta nem történt – a terrorszervezetek jelenleg vajon rendelkeznek-e megfelelő forrásokkal és eszközökkel ilyen jellegű műveletek végrehajtására?

---

27 Madhumita Murgia: Islamic State uses detailed security manual, revealing its cyber strategy. *The Telegraph,* 2015. november 20.

28 Aaron Brantly – Muhammad al-Ubaydi: Extremist Forums Provide Digital OpSec Training. *CTC Sentinel,* 8. (2015), 5. 10–13.

29 US Central Command.

30 Everett Rosenfeld: FBI investigating Central Command Twitter hacked. *CNBC,* 2015. január 12.

31 Audrey Alexander – Bennett Clifford: Doxing and Defacements: Examining the Islamic State's Hacking Capabilities. *CTC Sentinel,* 12. (2019), 4. 22–28.

### *4.4. Válaszok*

Az online térben rejlő lehetőségek megkönnyítik a terroristák kommunikációját, segítik szélsőséges gondolataik és terveik mind szélesebb körben való terjedését. Az online terrortartalmak terjedésének megakadályozása, a véleménynyilvánítás és az információk, eszmék megismerési és közlési szabadságának maradéktalan szem előtt tartásával együtt – talán korunk legnagyobb biztonsági kihívása.

Az internetes platformokat üzemeltető technológiai cégóriások, mint amilyen a Facebook, Microsoft, YouTube és a Twitter – politikai szintekről érkező kritikák hatására – létrehozták a Terrorizmus Elleni Globális Internet Fórumot, abból a célból, hogy megakadályozzák a terroristákat és az erőszakos szélsőségeseket a digitális felületek kihasználásában. A fórum küldetése a technikai együttműködés elősegítése a kutatások eredményeinek és a tudás megosztásának előmozdítása, illetve a terrorista és erőszakos, szélsőséges tartalmak online terjedésének megakadályozása érdekében.[32] Ezt az összefogást erősíti az a tény is, hogy az Európai Unió Tanácsának 2021. március 16-án elfogadott rendelete alapján a tagállami hatóságok 2022-t követően felhatalmazást kapnak a terroristatartalmak egy órán belüli eltávolítására vagy az összes tagállamban való hozzáférhetetlenné tételére.

Hazai viszonylatban az elsődlegesen médiaszabályozással foglalkozó hatóság a Nemzeti Média- és Hírközlési Hatóság, amely 2014-óta működteti a központi elektronikus hozzáférhetetlenné tételi határozatok adatbázisát.[33] Itt kell elhelyezni az azokra a jogellenes tartalmakra vonatkozó határozatokat, amelyek elérhetetlenné tételét az eljáró hatóságok szükségesnek látják. A szolgáltatóknak a Nemzeti Média- és Hírközlési Hatóság közlését követően egy munkanap áll rendelkezésre a határozatban foglalt tartalmak blokkolására, elérhetetlenné tételére. Az adatbázisban elhelyezett információk nem nyilvánosak, azokba betekinteni csak a bíróságnak, a külön törvényben meghatározott hatóságnak, az ügyésznek, a nyomozó hatóságnak, az Országgyűlés illetékes bizottsága tagjainak és az NMHH-nak van joga.

## 5. Összefoglalás, következtetés

Kijelenthetjük, hogy a napjainkat átszövő információk – és az azokhoz kapcsolódó eszközök – védelme, a velük való gazdálkodás világunk teljes spektrumát áthatja. Így a terrorizmus irányítóit, szervezőit, támogatóit és végrehajtóit is. Kiváló példa erre Rajib Karim esete, aki a British Airways informatikai mérnökeként öngyilkos merénylőnek jelentkezett, vállalva, hogy robbanóanyagot juttat fel egy, az Egyesült Államokba tartó járatra. Al-Awlaki, az Egyesült Államokban született és tanult jemeni sejk rábeszélte, hogy inkább számítástechnikai ismereteit használja a szent cél érdekében. Karim letartóztatását követően a lefoglalt számítástechnikai eszközein tárolt tartalmak feltöréséhez több hónapi szakértői munkára volt szükség a többszintű titkosítási és védelmi rendszerek miatt.

[32] Global Internet Forum to Counter-Terrorism.
[33] Az elektronikus hírközlésről szóló 2003. évi C. törvény 159/B. § (3) bekezdés.

Megállapítható, hogy a terrorizmus aktivitása az információs térben elsősorban a kommunikációra, toborzásra és a finanszírozásra terjed ki. Ezek hatékony ellenszere a terrortartalmú közleményeket érintő tiltás, eltávolítás, illetve a gyanús pénz- és eszközmozgások szűrése, figyelése. A kormányzatok komoly nyomást helyeztek az internetes cégekre és a közösségi médiát üzemeltető vállalkozásokra ebben a vonatkozásban.

Erre válaszul a közösségimédia-platformokat üzemeltető informatikai társulások létrehoztak egy globális kezdeményezést a terroristatartalmak eltávolítása érdekében. Az illegális tartalmak megjelenése, kontroll nélkülisége komoly veszélyt és hátrányt jelent a gazdasági folyamatokra, az információk szabad áramlására és az emberi kapcsolatokra nézve.

Ezeket a veszélyeket felismerve az Európai Unió intézményei – a hasonló irányú tagállami fellépést is támogatva – ajánlások, irányelvek és rendeletek alkotásával törekszenek gátolni a törvényellenes tevékenységeket és magatartásmódokat. Ez a törekvés 2022-től újabb mérföldkőhöz fog érkezni a tagállami hatóságok tartalomeltávolítási jogkörének végrehajtására vonatkozó időbeli szűkítéssel.

## Felhasznált irodalom


Alexander, Audrey – Bennett Clifford: Doxing and Defacements. Examining the Islamic State's Hacking Capabilities. *CTC Sentinel,* 12. (2019), 4. 22–28.

Gönczöl Katalin – Kerezsi Klára – Korinek László – Lévay Miklós: *Kriminológia-Szakkriminológia*. Budapest, CompLex Kiadó, 2006.

Haig Zsolt – Kovács László: Fenyegetések a cybertérből, *Nemzet és Biztonság,* 1. (2008), 5. 61–69.

Kazári Csaba: *Hacker, cracker, warez. A számítógépes alvilág titkai.* Budapest, Computer Panoráma, 2003.

Kenedli Tamás – Vida Csaba: Elemző-értékelő tevékenység. In Dobák Imre (szerk.): *A nemzetbiztonság általános elmélete*. Budapest, Nemzeti Közszolgálati Egyetem, Nemzetbiztonsági Intézet, 2014. 191–206.

Munk Sándor: A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései. *Haditechnika,* (2018), 1. Online: https://doi.org/10.17047/HADTUD.2018.28.1.113

Netanjahu, Benjamin: *Harc a terrorizmus ellen*. Pécs, Alexandra, 1995.

Resperger István: A nemzetbiztonsági szolgálatok tevékenysége – biztonsági kihívások, kockázatok és fenyegetések. In Resperger István (szerk.): *A nemzetbiztonság elmélete a közszolgálatban.* Budapest, Dialóg Campus, 2018.

Resperger István: Az aszimmetrikus hadviselés és a terrorizmus jellemzői. *Hadtudomány,* (2010), 4. 68–77.

Schneier, Bruce: *A biztonságról.* Budapest, HVG, 2010.

Storm, See Morten – Paul Cruickshank – Tim Lister – Agent Storm: *My Life Inside al Qaeda and the CIA.* New York, Atlantic Monthly Press, 2014.

## *Internetes források*

Brantly, Aaron – Muhammad al-Ubaydi: Extremist Forums Provide Digital OpSec Training. *CTC Sentinel,* 8. (2015), 5. Online: https://ctc.usma.edu/wp-content/uploads/2015/05/CTCSentinel-Vol8Issue53.pdf

*Emerging Terrorist Financing Risks.* FATF Report, October 2015. Online: www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf

*Global Digital Overview. Digital in 2020.* Online: www.wearesocial.com/digital-2020

Kessler, Ronald: Why Osama bin Laden stopped using his intercepted phone. *The Washington Times,* 2018. augusztus 5. Online: www.washingtontimes.com/news/2018/aug/5/why-osama-bin-laden-stopped-using-his-intercepted-/

Mágó Károly: 14 terrorista járt Magyarországon a párizsi és brüsszeli merénylők közül. *Origo,* 2016. szeptember 30. Online: www.origo.hu/itthon/20160930-tobb-terrorista-is-jart-magyarorszagon.html

Murgia, Madhumita: Islamic State uses detailed security manual, revealing its cyber strategy. *The Telegraph,* 2015. november 20. Online: www.telegraph.co.uk/technology/internet-security/12007170/Islamic-States-detailed-security-manual-reveals-its-cyber-strategy.html letöltés ideje: 2021.04.25.

Nato Unclassified: *MC 0472/1 Military Committee Concept For Counter-Terrorism.* Online: www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_01/20160817_160106-mc0472-1-final.pdf

Raymond, Eric: S. *How To Become A Hacker.* Online: http://catb.org/~esr/faqs/hacker-howto.html

Rosenfeld, Everett: FBI investigating Central Command Twitter hack. *CNBC,* 2015. január 12. Online: www.cnbc.com/2015/01/12/us-central-command-twitter-hacked.html

Roussinos, Aris: Jihad selfies, these british extremists in Syria love social media. *Vice,* 2013. december 5. Online: www.vice.com/en/article/gq8g5b/syrian-jihadist-selfies-tell-us-a-lot-about-their-war

Schmitt, Eric – Ben Hubbard: ISIS Leader Takes Steps to Ensure Group's Survival. *The New York Times,* 2015. július 21. Online: www.nytimes.com/2015/07/21/world/middleeast/isis-strategies-include-lines-of-succession-and-deadly-ring-tones

*Statement of Dorothy E. Denning.* Georgetown University. Online: https://fas.org/irp/congress/2000_hr/00-05-23denning.htm

Tohid, Owais: Bin Laden bodyguard's satellite phone calls helped lead US forces to hiding place. *The Christian Science Monitor,* 2011. május 2. Online: www.csmonitor.com/World/Asia-South-Central/2011/0502/Bin-Laden-bodyguard-s-satellite-phone-calls-helped-lead-US-forces-to-hiding-place

Winter, Charlie: Fishing and Ultraviolence. *BBC News,* 2015. augusztus 1. Online: www.bbc.co.uk/news/resources/idt-88492697-b674-4c69-8426-3edd17b7daed

Zernike, Kate – Michael T. Kaufman: The Most Wanted Face of Terrorism. *The New York Times,* 2011. május 2. Online: www.nytimes.com/2011/05/02/world/02osama-bin-laden-obituary.html