DOI: 10.38146/BSZ.2018.2.7

KASZNÁR ATTILA

A kibervédelem fontossága a terrorelhárítás jelenlegi és jövőbeni rendszerében

A kiberfenyegetettség mind nagyobb próbatétel a nemzetbiztonsági és a terrorelhárítási szolgálatok számára, mivel az információs technológia fejlődése által kínált lehetőségeket a terrorszervezetek egyre gyakrabban használják fel képességeik bővítésére és javítására.[1] Mindamellett, bár mind több és több a jele az újfajta veszélynek, látni kell, hogy a védekezés terén – sem a társadalmi, az egyéni és a vállalati szegmensben, sem a rendvédelmi és nemzetbiztonsági szektorban – még mindig nincs meg az a fajta elvárható tudatosság, amely szükségesnek mutatkozhat. *„Mindenekelőtt két olyan állítás fogalmazható meg, amelyben mindenki egyetért, aki így vagy úgy kiberbiztonsággal foglalkozik. Az egyik, hogy a kiberbiztonság, illetve a kiberfenyegetettség a következő évtizedek egyik legfőbb biztonsági kihívását jelenti. A másik, hogy a kiberbiztonság megvalósítására irányuló erőfeszítések jelenleg elég fragmentáltak, azaz a különböző szereplők hatékony együttműködése még hagy maga után kívánnivalót."*[2]

Biztató pontként említhető, hogy a hazánkban jelenleg is érvényben lévő Nemzeti biztonsági stratégia külön is kiemeli a kiberbiztonság szerepét: *„Az állam és a társadalom működése – a gazdaság, a közigazgatás, vagy a védelmi szféra mellett számos más területen is – mind meghatározóbb módon a számítástechnikára épül. Egyre sürgetőbb és összetettebb kihívásokkal kell számolnunk az informatikai- és telekommunikációs hálózatok, valamint a kapcsolódó kritikus infrastruktúra fizikai és virtuális terében. Fokozott veszélyt jelent, hogy a tudományos és technológiai fejlődés szinte mindenki számára elérhetővé vált eredményeit egyes államok, vagy nem-állami – akár terrorista – csoportok arra használhatják, hogy megzavarják az információs és kommunikációs rendszerek, kormányzati gerinchálózatok rendeltetésszerű működését."*[3] A jogszabályban foglaltak bizakodásra adnak okot, amikor jel-

1 Gianluca Riglietti: Defining the threat: what cyber terrorism means today and what it could mean tomorrow. The Business and Management Review, vol. 8, no. 3, 2016, p. 12.

2 Hankiss Ágnes: Kiberbiztonság: az Európai Parlament feladatai. Magyar Rendészet, különszám, 2013, 27. o.

3 Magyarország Nemzeti Biztonság Stratégiája, 31. bek. http://2010-2014.kormany.hu/download/f/49/70000/1035_2012_korm_hatarozat.pdf

zik, hogy a legfelsőbb politikai döntéshozó szinten felismerték a problémát, a mindennapok tapasztalatai azonban azt mutatják, hogy a társadalom kiterjedt felületén mutatkoznak veszélyhelyzetet előidéző hiányosságok.

Az a speciális – a hagyományos társadalmi közegnél jóval nehezebben feltárható, illetve ellenőrizhető – fenyegetettségi környezet, amelyet a kibertér bővülése és használatának mindennapossá válása hozott, korábban sosem látott nehézségeket idézett elő a terrorelhárítás feladatrendszerében. A kiberterrorizmus ugyanis szerves része az aszimmetrikus hadviselésnek, amely *„a hibrid hadszínterek hibrid fenyegetései által a hibrid műveletek és az ellenük való védekezés lehetősége (kontrahibrid műveletek), a jelenlegi kor egyik fő kihívása”*[4]. E kihívások pedig új válaszmechanizmusok kidolgozását teszik szükségessé, mivel a korábbi biztonsági környezetre tervezett reakciók az új dimenziókban nem vagy nem elég hatékonyan alkalmazhatók, márpedig olyan *„időkben, mint amilyen a miénk, mikor nemcsak vízszintesen, hanem függőlegesen is történik minden, az ember helyesen cselekszik, ha megtanul a frontkatona óvatosságával élni”*[5], és minden figyelmét az új veszélyek leküzdésére fordítja.

Jelen tanulmány nem kíván komplex válaszokat adni a kiberterror elleni védekezés kérdéseiben, hanem elsősorban felderítési szempontból kívánja felhívni a figyelmet arra, milyen összetett strukturális nehézségekkel kell szembenézni a kibertérből érkező terrorfenyegetettségek elhárításakor, amelyek tulajdonképpen a terrorizmus és a kibertér konvergenciájának tekinthetők[6], e meghatározást több szakértő is elfogadottnak tartja.[7]

Az elsődleges feladatot a preventív fellépésben, vagyis a felderítőmunkában szükségszerűen bekövetkezett változások adják. A terrorelhárításhoz kötődő – de ugyanígy igaz a megállapítás minden nemzetbiztonsági felderítőmunkára is – felderítés lehetőségei számos aspektust alapul véve rendkívül kiterjedtek a kibertér adta lehetőségek hatására, mindamellett talán ennél hangsúlyosabban jelentkeznek az új típusú közeg jelentette nehézségek, mivel *„a hagyományos tevékenységeket megkönnyítő szerepén túl, az internet komoly biztonsági kockázatokat is magában rejt”*[8].

4 Resperger István: Az aszimmetrikus hadviselésre adható válaszok. Honvédségi Szemle, 2017/1., 24. o.
5 Márai Sándor: Füves könyv. Helikon Kiadó, Budapest, 2005, 99. o.
6 Gabriel Weimann: Cyberterrorism – How Real Is the Threat? Special Report, no. 119, United States Institute of Peace, 2004. https://www.usip.org/sites/default/files/sr119.pdf
7 Dorothy E. Denning: Cyberterrorism. 24 August, 2000, p. 1. http://palmer.wellesley.edu/~ivolic/pdf/Classes/Handouts/NumberTheoryHandouts/Cyberterror-Denning.pdf
8 Szijártó Lívia: Az internethasználat biztonságetikai kérdései. A virtuális lét rejtett veszélyforrásai. Nemzetbiztonsági Szemle, 2016/1., 46. o.

A felderítés újonnan jelentkező nehézségeit azok a kiterjedt lehetőségek (anonimitás, közösségi, illetve kapcsolattartó szolgáltatások, sötét web stb.) okozzák, amelyek nyomán a szolgálatok információszerző lehetőségei eddig nem tapasztalt nehézségekbe ütközhetnek.

A terrorizmus ugyanis nem statikus jelenség, hanem komplex rendszer, amelynek egyes momentumai a fejlődés irányába mutató evolúciós folyamatok összetevőinek tekinthetők, a *„fejlődése során végig követhető a módszerek, eszközök és elkövetők változása”*[9]. A kijelentés úgy is értelmezhető, hogy *„a terrorizmus nem ér véget az erőszakos tettel, ez csak a kezdete”*[10], a folyamat ugyanis folytatódik, mint azt a társadalmi funkcionális folyamatmodellek híven leírják, interakciók következtében megtörténik visszajelzés, és az inputok hatására újabb folyamatok generálódnak. Ezek természetesen mindig változó tényezőkből állnak össze, és a környezetük, valamint az az által gyakorolt hatás is minden esetben más, azonban közös bennük, hogy mindegyik a rendszer – a terrorizmus – része. Egy ilyen fejlődési lépcsőnek, a rendszer egy folyamatának tekinthető maga a kiberterrorizmus is.

Az előbbiek tekintetében elmondható, hogy a sikeres elhárítómunka is minden esetben dinamikus tevékenység kell hogy legyen, amely ennek jellegzetességei okán egyértelmű, hogy számos ponton, jelen esetben a kiberterrorizmus jelentette új, szokatlan feladatok miatt nehézségekbe ütközik. A nehézségek jellegzetessége azonban, hogy azok minden esetben ideiglenesek, mivel az új típusú feladat (input) generálta válaszok, azaz megoldások (output) részben vagy egészben feloldják a problémát; természetesen nem hagyható figyelmen kívül, hogy az output a visszajelzés folytán inputként fog jelentkezni, vagyis ismételt elhárítási nehézséget okoz, ez azonban maga a már leírt jellegzetesség.

A kiberterrorizmust minden esetben a terrorizmus rendszerének egyik folyamataként kell értelmeznünk, ezáltal pedig figyelembe kell vennünk, hogy az általa támasztott kérdésekre adott válaszok milyen új inputokat generálhatnak, és ezek maximális optimalizálására, illetve kezelhetőségére kell törekedni.

Milyen új feladatot teremt a kibertér? A felsorolás számos elemet tartalmazhat, és valószínűsíthető, hogy egyiket sem lehetne teljesnek tekinteni, mert – pontosan annak dinamikus voltánál fogva – újabb és újabb tagokkal

9 Bács Zoltán György: A radikalizáció és a terrorizmus kapcsolata, egyes formái, gondolatok a megelőzés lehetséges perspektíváiról. Nemzetbiztonsági Szemle, 2017/1., 5. o.

10 Marie-Helen Maras: A terrorizmus elmélete és gyakorlata. Antall József Tudásközpont, Budapest, 2016, 240. o.

lenne kiegészíthető, ezért e tanulmány szubjektíven emel ki néhányat a legfontosabbnak ítélt tényezők közül.

Globális lehetőségek

A terrorizmusra általános értelemben is igaz, hogy *„minden más bűncselekménytől különbözik abban, hogy egyfelől ideológiai-politikai motivációt követ, másfelől globális, azaz természeténél fogva átnyúlik földrészeken és országhatárokon”*[11]. A kibertér már a létezésével megteremti annak a lehetőségét, hogy a terrorizmus említett sajátosságait érvényesíteni tudja. Mára bátran kijelenthető, hogy az internet alapjaiban változtatta meg a terrorizmus lehetőségeit, a módszerek széles kínálatát nyújtva, miközben új nehézségek elé állította az terrorelhárításban részt vevő szolgálatokat. Ennek egyik legjellemzőbb példája a radikalizáció terén lelhető fel. *„Az internet átvitt értelemben úgy tekinthető, mint az elektronikus világ fő út- és vasúthálózata, amely rendkívül hatékony »szállítást« tesz lehetővé, és nagyon messzire és szétszórtan élő személyeket is elér, valamint befolyásolni képes azok közösségi és egyéni világnézetét.”*[12] A világháló globális elterjedésével párhuzamosan vált igazzá, hogy *„a radikalizációs folyamat fontos elemévé lépett elő az internet”*[13], amely meggyorsította és határok nélkülivé tette a szélsőséges eszmék terjesztését.

A radikalizálni kívánók szempontjából

A radikális tanoknak az azokra esetlegesen fogékony személyekhez történő eljuttatásának az internet korszakában gyakorlatilag csak nyelvi akadálya lehet, egyébként könnyebben, gyorsabban, konspiráltabban, és a szolgálatok hagyományos felderítő tevékenysége elől jóval védettebben van rá lehetőség. A különböző, gyakran védett internetes felületek a kapcsolattartás (sok terrorista használ a kommunikációja során titkosítást, amely megnehezíti az ellenük való fellépést[14]), a tiltott kereskedelem és más illegális tevékenységek so-

11 Hankiss Ágnes: Vékony jégen. Arc és Álarc, 2017/1., 85. o.
12 Alfred Rolington: Hírszerzés a 21. században. A mozaikmódszer. Antall József Tudásközpont, Budapest, 2015, 100. o.
13 Zalai Noémi: A XX. század háborúi és a terrorizmus elleni harc jellemzőinek összehasonlítása katonai, politikai és társadalmi kontextusok alapján. Szakmai Szemle, 2008/2., 49. o.
14 Dorothy E. Denning: i. m. 3. o.

rát teszik lehetővé úgy, hogy jellegzetességeik, valamint nagy mennyiségük következtében is számos problémát okozhat a szűrésük.[15]

A radikalizálódásra alkalmas személyek szempontjából

A szélsőséges nézetekre és cselekményekre fogékonyságot mutató, legtöbbször valamilyen társadalmi vagy szociális zsákutcából kiutat kereső személyek lehetősége a téves, később végzetesnek bizonyuló „válaszok" elérésére nemcsak nagyobb, mint a világhálón kívüli életben, de mivel legtöbbször rendkívüli frusztráltság jeleit mutatják, ezért a vélt vagy valós anonimitás miatt, biztosabbnak is tűnhet számukra ez a megoldás. Vagyis aktívabban kereshetik az internetes felületeken a segítséget, emiatt tulajdonképpen tálcán kínálják önmagukat a szélsőséges ideológusoknak, vagy a már radikalizálódott személyeknek. Az elmúlt időszak európai terrorcselekményeit végrehajtó személyek pszichológiai hátterének elemzése is megerősíteni látszik az iménti feltevést, mivel az elkövetőkre igaznak bizonyult, hogy azok *„számos esetben megpróbálnak kapcsolatot teremteni terrorszervezetekkel, de ami még jellemzőbb, hogy az interneten keresztül radikalizálódott személyekkel vesznek fel kapcsolatot"*[16]. Ezek a személyek, annak ellenére, hogy jogilag elkövetővé válnak, gyakorlatilag maguk is áldozatok, akik sebezhetőségükből kifolyólag *„legfeljebb csak szimbolikus kapcsolatban állnak az akció valódi céljával"*[17].

Információbőség

A kibertér világa bebizonyította, hogy terrorelhárítási szempontból is igaz, hogy *„van annál nagyobb probléma is, mint kevés információval rendelkezni – mégpedig az, ha túlságosan sok információ vesz körül bennünket"*[18]. Az információs társadalomban generálisan jelentkező probléma az információ-

15 Az említett probléma a jelzettnél is súlyosabb gondokat okozhat a web sötét oldala esetében. Az általa okozott nehézségekre jelen tanulmány külön nem tér ki.

16 Farkas Johanna: A magányos merénylők radikalizálódása. Acta Humana, 2016/5., 23. o.

17 Boda József: Biztonsági kihívások – nemzetbiztonsági válaszok. In: Gaál Gyula – Hautzinger Zoltán (szerk.): Tanulmányok a „Biztonsági kockázatok – rendészeti válaszok" című tudományos konferenciáról. Pécs, 2014, 42. o. [Pécsi Határőr Tudományos Közlemények XV.]

18 Jasenszky Nándor: Adatszerzés – Információhasznosulás – Biztonságtudatos vállalati kultúra. In: Szamos Tamás (szerk.): A nyílt információgyűjtés fejlődő területei. Belügyi Tudományos Tanács, Budapest, 2015, 58. o.

többlet, ebből adódóan mára mindinkább háttérbe szorul a humán erőforrás információhordozó képességének fontossága a munkaerő információszintetizáló képességéhez képest. Az előző gondolatból adódóan, ma már a szolgálatok számára sem elsődleges cél a mind több adat és információ felhalmozása, mivel annak korlátlansága gátolhatja az eredményes munkát. Inkább *„az információk szelektálása, szűkítése, gyors értékelése, megfontolt elemzése, mindez pedig szoros határidővel, hiszen a legfőbb szempont a politikai vezetés döntéseinek információs támogatása, alternatívák felállítása”*[19]. Különös fontosságú az információtöbblet kezelése, mivel az

1. lassíthatja a feldolgozás sebességét, ami jelentékeny – akár emberéletekben is mérhető – időveszteséget okozhat;
2. lehetőséget adhat a terroristáknak a zavaró információhalmazban való elrejtőzésre;
3. megfelelő, manipulált kontextusok felállítása mellett, a szolgálatok félrevezetését, megzavarását is lehetővé teheti.

Térinformatika

„A térinformatikai adatok/információk és eszközök alkalmazása igen nagy előnyökkel jár a terrorelhárító tevékenységben, ugyanakkor a terroristákat is hasznos információkhoz segítheti a támadások szervezésében. Mind a terroristák, mind a terrorelhárítók számára ugyanazok az általános pozitívumok: a megnövekedett információmennyiség[20] *és a jó minőségű térinformatikai részletek.”*[21] Az általános vélekedés szerint a térinformatika a modern társadalom egyik kiemelkedő hatású technikai vívmányának tekinthető, azonban, mint az a jelenlegi biztonságpolitika egyik legnagyobb tekintélyű nemzetközi szakértőjének soraiból is levezethető, a kép ennél jóval árnyaltabb, és a pozitív hozadékok mellett az alkalmazása során megjelennek a társadalom egészének rendszerét (gazdaság, politika, kultúra stb.), valamint az egyén személyét is érintő fenyegetések.

19 Laufer Balázs: Az új kihívások hatása a nemzetbiztonságra – a nemzetbiztonsági szolgálatok megváltozott szerepe napjainkban. Felderítő Szemle, 2010/3–4., 56. o.

20 Ebben az esetben azonban szükséges visszautalni a túlzott mennyiségű információval összefüggésben kifejtett gondolatokra, ami természetesen a terroristák számára is jelentkezhet negatívumként.

21 Marie-Helen Maras: i. m. 498. o.

Internetes média

Külön problémakörbe tartoznak az internetes médiában terjedő, az általános megítélésben propagandaanyagokként értelmezett terroristavideók, amelyek tartalma azonban ennél sokkal bonyolultabb. Az utóbbi időben elsősorban az Iszlám Állam által, profin készített és terjesztett, brutális kivégzéseket, valamint kínzásokat bemutató videók ugyanis túlmutatnak a propagandán, és hatásmechanizmusuk – sokkoló, félelmet keltő tartalmuk – alapján a terrortevékenység egy új fajtájának tekinthetők. Az új típusú támadások megfelelnek azon kitételnek, *hogy „a globalizált és interdependenssé váló mediatizált külpolitikai közegben a terrorista akciók szimbolikus értékű agresszióként aposztrofálhatók, a támadások egész társadalmak, kultúrák és politikai berendezkedések számára hordoznak üzenetet, az erőszakos cselekmények félelemkeltésre irányuló hatásfoka a korábbi trendekhez képest sokszorosára nőtt”*[22]. Az említett digitális tartalmak elleni fellépés elsődleges fontosságú lehet a jövő terrorelhárító tevékenységében.

Az internet mint a terrortámadás eszköze és helyszíne

Mind több jele mutatkozik annak, hogy a világháló maga is egyben terroristaeszközzé, illetve terroristacélponttá válik. Indokolt a jelen idő használata, mivel a kibertámadások mára a mindennapok részévé váltak, de valószínűsíthető az is, hogy a jelenlegi tudásszint mellett a szakértők számára sem felfogható az a méretű állam, társadalom, továbbá egyén elleni támadási potenciál és felület, amelyet a jövő információs társadalma hordoz majd magában. Az informatikai fejlődésben a következő áttörést a mesterséges intelligencia felhasználása jelentheti, ez várhatóan alapjaiban alakítja át az emberiség életét, és félő, hogy sosem látott lehetőségeket kínál majd a terroristáknak is, miközben minden korábbinál nehezebb feladat elé állítja a felderítő és elhárító szolgálatokat.

Összegzés

A kibertérrel kapcsolatos, illetve *„az információs technológia terrorista csoportok, vagy egyének általi saját célok elősegítése érdekében való felhaszná-*

22 Király Zoé Adrienn: A terrorizmus médiainterpretációja és a terrorista szervezetek médiahasználatának változása a digitális korban. Politikatudományi Tanulmányok, 2016/1., 12. o.

lása"[23] témájában végzett kutatások alapján mind fontosabbnak tekinthető a strukturális és technológiai újítások alkalmazása annak érdekében, hogy sikerrel lehessen felvenni a küzdelmet a terrorizmus újszerű biztonsági kockázataival. Fontos annak a kérdésnek a megválaszolása, hogy a *„jelenlegi kibervédelmi szervezetek alkalmasak-e a kiberhadviselés kezelésére, ha nem, akkor pedig milyen szervezetfejlesztés szükséges e feladatok ellátásához?"*[24]

Talán az egyik legmeghatározóbb feladatként jelentkezhet a kiberalapú felderítési potenciál további növelése, amelynek során *„alapvetően azon kommunikációs csatornák és formák ellenőrzése lehet meghatározó, amelyet a társadalom békés tagjai között meghúzódó terroristák is használhatnak (így pl. a mobiltelefonok, valamint az internet-alapú szolgáltatások)"*[25]. Az információszerző mechanizmusok megfelelő irányú fejlesztése azonban csak abban az esetben lehet eredményes, ha ezzel párhuzamosan megtörténik a hozzá tartozó értékelőkapacitás fejlesztése is.

Mind több jele mutatkozik, hogy a kibertér védelme az egyik leglényegesebb momentum. Az információtechnológia fejlődése és terjedése merően újszerű eszközöket teremtett a szélsőséges ideológiákat megjelenítő személyek és csoportok – különösen a terrorista csoportok – számára, és ezek alapjaiban változtatják meg a globális biztonsági környezetet. Az internet, valamint annak speciális alkalmazásai (különösen a közösségi felületek) révén a radikalizációs folyamatok a korábbiaknál gyorsabban, szélesebb körben és jóval kevésbé ellenőrizhetőn mehetnek végbe. A közösségi oldalak és egyéb kapcsolattartó alkalmazások elterjedésével a szélsőséges eszmék közvetítésében gyakorlatilag mindössze a nyelvi különbségek jelentkezhetnek nehézségként. Elsősorban az Iszlám Állam utóbbi időben kifejtett tevékenysége bizonyosságát adta, hogy az internet egyben kiemelkedő propagandafelületet is teremt a különböző terrorista csoportoknak, ezek professzionális kihasználására pedig egyre nagyobb erőfeszítéseket tesznek. Kiemelt probléma lehet az egyes terrorszervezetek kibertámadásokra irányuló törekvése is, ezekkel olyan anyagi és eszmei károkat okozhatnak, amelyek korábban nem vagy csak kevéssé ismert hatású demoralizáló és sokkoló hatást válthatnak ki a közvéleményben.

23 Mitko Bogdanoski – Drage Petreski: Cyber terrorism – global security threat. International Scientific Defence, Security And Peace Journal, July 2013, p. 59.

24 Boda József – Boldizsár Gábor – Kovács László – Orosz Zoltán – Padányi József – Resperger István – Szenes Zoltán: A hadtudományi kutatási irányok, prioritások és témakörök. Állománytudományi Műhelytanulmányok, 2016/16., 18. o.

25 Dobák Imre: Technikai típusú információgyűjtés a változó biztonsági kihívások tükrében. Hadmérnök, 2017/2., 243. o.

„Nem különösebben homályos, se nem igazán új az a gondolat hogy mind a technikai fejlődés, mind a társadalmi változás megváltoztatja a stratégiai környezetet is – és így az eszközöket is, amelyekkel a háborúkat vívják."[26] A globális terrorban bekövetkezett alapvető, stratégiai változások megkövetelik a gyökeres szemléletváltoztatást a terrorelhárítás területén is, hiszen a rendvédelmi szerveknek *„évtizedes hagyományok alakították ki a szervezeti kultúra- és értékrendszerüket"*[27]. Az új típusú fenyegetést jelentő terrorszervezetek nemcsak jól finanszírozottak, hanem a modern technikai megoldások implementálására is fogékonyak.[28] A modern, kibereszközöket is felhasználó terrorizmus, és annak mélyre nyúló társadalmi beágyazottsága, olyan flexibilis szociológiai állapotot teremtett, illetve a mesterséges intelligencia a jövőben olyan változásokat idéz elő, amelynek következtében elengedhetetlen, hogy a nemzetbiztonsági és terrorelhárító szolgálatok a korábbi, statikus alapokon építkező tevékenységüket a korábbiaknál eredményesebb, a napi változásokat aktívabban követő metódusok alapján végezzék. Sosem szabad figyelmen kívül hagyni, hogy a terroristák is tisztában vannak az alapszabállyal, az ellenséget *„Ott támadd meg, ahol készületlen! Ott ronts rá, ahol nem is számít rá."*[29]

26 Roland Dannreuther: Nemzetközi biztonság. Antall József Tudásközpont, Budapest, 2016, 297. o.

27 Zalai Noémi: Új típusú kihívások: generációváltás a nemzetbiztonsági szolgálatoknál. Nemzetbiztonsági Szemle, 2016/1., 35. o.

28 Sarah Gordon – Richard Ford: Cyberterrorism? Symantec.com, 2003, p. 9. https://www.symantec.com/avcenter/reference/cyberterrorism.pdf

29 Szun-Ce: A háború művészete. Cartaphilus Kiadó, Budapest, 2006, 12. o.