PÉCSI TUDOMÁNYEGYETEM ÁLLAM- ÉS JOGTUDOMÁNYI KARÁNAK
DOKTORI ISKOLÁJA

DR. SERBAKOV MÁRTON TIBOR

EGYES SZÉLSŐSÉGES TERRORISTA CSOPORTOK INTERNETHASZNÁLATA EGYES ASPEKTUSAINAK ELEMZÉSE

PHD ÉRTEKEZÉS

Témavezető:
PROF. DR. GÁL ISTVÁN LÁSZLÓ
tanszékvezető egyetemi tanár

PÉCS, 2022

Tartalomjegyzék

I. BEVEZETÉS

1. A témaválasztás indokolása

Schmid 2004-es megállípítása, hogy valószínűleg a terrorizmus a legfontosabb szó a politikai szótárban[1], napjainkban is igaz, esetleg a koronavírus vagy a migráció előzheti meg. A globalizáció legfőbb biztonsági, rendészeti kihívásai a migráció és a terrorizmus.[2]

Az internet az életünk már megkerülhetetlen, elengedhetetlen része. Sajnos az már a terrorizmusnak is szinte állandó elemévé vált.

A koronavírus (COVID-19) világjárvány felgyorsította a digitális világ felé való elmozdulást.[3] A járvány megfékezésére bevezetett zárlatok idején az online radikalizációnak fokozottan magas a kockázata. A távolságtartási szabályok fokozzák az extrémizmus terjedését. Zárlatok idején otthonrekedt milliók fordulnak az internet és a közösségi média felé.[4] Ezen tényezők miatt is a terroristák internethasználatának kutatása fontosabb, mint valaha.

Természetesen a „(…) terrorcselekmények megakadályozása komplex tevékenységet, és szervezetrendszert igényel,"[5] és úgy vélem, a mai digitalizált világunkban a terrorizmus és a terrorizmus finanszírozás elleni harcban, főleg a terrorcselekmények megelőzésében az internetnek kulcsszerepet kell játszania. Véleményem szerint a legtöbb terrorista akciónak, az azokhoz vezető radikalizáció folyamatának, a szervezésnek etc. van előjele az interneten, de tudni szükséges azt, hogy mit, hol és hogyan kell figyelni. A hatékonyabb terrorizmus és terrorizmusfinanszírozás elleni harc, a terrorcselekmények nagyobb sikerrel történő megakadályozása és a radikalizáció megelőzése szempontjából

[1] SCHMID, A.: Terrorism - The Definitional Problem. Case Western Reserve Journal of International Law, 2004. Vol. 36. No. 2. 376. o.

[2] RITECZ Gy.: a terrorizmus és a migráció viszonya a számok alapján. Acta Humana, 2016/5. 103. o.

[3] Covid 19 and E-commerce: Findings from a survey of online consumers in 9 Countries. United Nations UNCTAD, 2020. 4. o. https://unctad.org/system/files/official-document/dtlstictinf2020d1_en.pdf (2021.06.14.)

[4] MALIK, N.: Self-Isolation Might Stop Coronavirus, but It Will Speed the Spread of Extremism. Foreign Policy. (2020, March 26). https://foreignpolicy.com/2020/03/26/self-isolation-might-stop-coronavirus-but-spread-extremism/ (2021.06.21.)

[5] KOVÁCS I.: Rendvédelmi ismeretek I. Magyar Rendészettudományi Társaság, Budapest, 2021. 32. o.

elengedhetetlen az egyes terrorszervezetek internetes aktivitásának beható és naprakész ismerete. Értekezésemmel ehhez az ismeretanyaghoz kívánok hozzájárulni.

2. A kitűzött kutatási feladat célkitűzése, rövid összefoglalása

Disszertációmban átfogó képet kívánok nyújtani korunk terroristáinak, különös figyelemmel a szélsőséges iszlám által motivált és a szélsőjobboldali terroristák internethasználatáról, mely méretét tekintve hatalmas léptékű, és kihívást jelentő vállalkozás, számos akadállyal, nehézséggel és kérdéssel.

Bemutatom a terroristák internethasználatának alapvetéseit, hogy általánosságban az egyes terrorszervezetek, terrorista csoportok, magányos terroristák milyen tevékenységek végzésére használják a világhálót. Röviden rávilágítok a terroristák okostelefonos alkalmazás használatára is.

A magyar szakirodalomban jelenleg nem létezik a terroristák internethasználatát mélységeiben tárgyaló monográfia. Jelen értekezés ezt az űrt kívánja betölteni.

A választott téma (maga a terrorizmus jelensége is) interdiszciplináris megközelítést igényel, ezért a bűnügyi tudományok[6] közül elsősorban a kriminológiai irányából közelítő értekezésem óhatatlanul és szükségesen is átlépi annak határait, és többek között rendészettannal, akár hadtudománnyal is színeződik. A vizsgált tárgyból adódóan informatikai kérdéseket is szükséges érintenem, melyekben olyan mélységekben szándékozom csak elmerülni, amennyire a mű tárgyának megértéséhez feltétlenül szükséges.

Végső célkitűzésem az, hogy a művem a terrorizmus elleni harc szereplői számára a gyakorlatban is hasznosítható tudásanyagot nyújtson, de ha értekezésem az ehhez szükséges színvonalat a legnagyobb igyekezetem ellenére sem éri el, bízom benne, hogy legalább képes lesz a tárgyalt témát illetően termékeny diszkussziót, vitát generálni és a jelen munkánál jobb, további műveket inspirálni.

3. Az értekezés szerkezete

A téma kontextusba helyezéséhez és megértéséhez elengedhetetlen a terrorizmus definíciójának, típusainak, történetének, és napjainkban történt változásainak

[6] HORNYÁK Sz.: A büntetőjog-tudomány és a bűnügyi tudományok rendszere. In: BALOGH Á. – TÓTH M. (szerk.): Magyar Büntetőjog. Általános Rész. Osiris Kiadó, Budapest, 2015. 31-34. o.

bemutatása.
A terrorrorizmus témáját bármilyen irányban megközelítve az első problémával már akkor szembesülünk, mikor azt szeretnénk eldönteni, hogy egyáltalán mit is nevezünk annak. A terrorizmusnak számtalan definíciója létezik. Még ha el is döntjük, hogy a szakirodalom és különféle szervezetek, kormányok mit tekint terrorizmusnak, akkor sem lehetséges általánosságban a terroristák internethasználatáról írni, mivel a terrorizmusnak sokféle tipizálása is létezik. Az II. fejezetben röviden felvázolom a terrorizmus definíciójának kérdését és a terrorizmus típusait.
Csak a meghatározások és a tipizálás alapvetéseinek tisztázása után érdemes a III. fejezetben a nemzetközi terrorizmus történetét dióhéjban felvázolni, és korunkban a jelenségét illető változásokat bemutatni.
A IV. fejezet a média és terrorizmus kapcsolatának vázlatos történetét és elméletét tárgyalja, és rávilágít arra, milyen változásokat hozott a média és terrorizmus kapcsolatába az internet és a közösségi média megjelenése.
Az V. fejezet a terroristák internethasználatának alapvetéseit mutatja be, hogy a szakirodalom szerint mire használják a terroristák a világhálót, továbbá ebben a fejezetben tisztázom, hogy jelen értekezésben mit értek terroristák internethasználata alatt, és mit nem.
Úgy vélem, komplexitásuk miatt külön fejezetet érdemel a terroristák dark webes jelenlétének kérdése és a méltatlanul alulkutatott terroristák okostelefonos alkalmazás használatáta, melyek a VI. és VII. fejezetben kerülnek bemutatásra.
A VIII. fejezet a terrorizmus finanszírozás internethez köthető technikáit és forrásait mutatja be.
A IX. fejezet az online történő radikalizáció kérdését tárgyalja, és a terrorcselekményeket előrejelző internetes magatartásokat.
A X. fejezet három szélsőséges iszlám által motivált terrorszervezet, az al-Kaida, az Iszlám Állam (továbbiakban IS) és a Boko Haram internethasználatát illetően próbál átfogó képet nyújtani.
A XI. fejezet a szélsőjobboldali terroristák online jelenlétét tárgyalja.
A XII. fejezet az online terjedő összeesküvés-elméleteket, és az azokhoz fűződő terror-kockázatot tárgyalja, fő fókuszában a The Great Replacement és a QAnon elméletekkel. Vitatható lehet, hogy az incelek melyik fejezetbe illenek. Érvelni lehetne amellett, hogy a XI. fejezetben lenne a helyük, mint alt-jobb szereplők, de sajátos nézeteik miatt külön, a XIII. fejezetben kerülnek tárgyalásra.
A XIV. fejezetben a 3D nyomtatott lőfegyverek, online elérhető tervrajzaik és ezek

terrorista célokra való felhasználhatóságát mutatom be.
A XV. fejezet a koronavírus (COVID-19) pandémia hatását vizsgálja a terroristák internethasználatára.
A XVI. fejezet tárgya a terrorizmus elleni küzdelem és a terrorcselekmények megelőzésének egyes elméleti kérdései, különös tekintettel az internethez kötődő megelőzési módszerek.

4. A kutatás nehézségei és korlátai

Fontos volt számomra, hogy a munkám a gyakorlat, a terrorizmus elleni harc szereplői számára is felhasználható legyen, ezért a magyar nyelvű és idegeny nyelvű szakirodalom mellett kutatásom során kifejezetten sok internetes forrásra is kellett támaszkodnom, melynek okai a következők: Internethez kötődő témám nagyon modern, napról napra formálódik. Számos ahhoz kötődő forrás (még) csak az interneten lelhető fel, és a legtöbb esetben csak idegen nyelven. Számos kérdést, amit dolgozatomban vizsgálok, nem is dolgoz még fel tudományos munka, amire támaszkodhatnék. Témám nem minden aspektusával foglalkozik magyar szerző, annak erősen nemzetközi, globalizált természete miatt sok külföldi forrásból kellett dolgoznom. Az internetes források különösen kritikus értékelést igényeltek.
Jelen dolgozatnak nem tárgya a terroristák által elkövetett kibertámadás, a kiberterrorizmus. Jelen disszertáció fókusza a terroristák internethasználatának egyes aspektusai, nem pedig az ehhez fűződő elhárítási, eltávolítási módok, technikák, kérdések, melyeket csak röviden tárgyal.
Minden típusú terrorista internethasználatának minden egyes aspektusát a terjedelmi korlátok miatt nem tudom tárgyalni, a vizsgált témát illetően szelektálni kényszerültem. Számos, a dolgozatból a terjedelmi korlátok miatt kimaradt aspektus kölön műben való feldolgozást, vizgálatot érdemelne. Külön vizsgálatot és bemutatást érdemelnének még, a teljesség igénye nélkül: a terrorista tartalmak internetről való eltávolítása, a terroristák online aktivitásának visszaszorítására hozott jogszabályok, egyezmények, irányelvek, a szabályozás lehetőségei, az erre szolgáló gépi eszközök, az egyes felületek felhasználási feltételei és irányelvei, a terrorista tartalmak tekintetében, az EU válaszai a terroristák internethasználatára, a téma magyar vonatkozásai, a magyar és további külföldi esetek elemzése a terroristák internethasználata szempontjából, más típusú terroristák, más terrorszervezetek, magányos terroristák internetes aktivitása is. Valamennyi fejezet által

taglalt kérdés további vizsgálatra, kifejtésre volna érdemes.

5. A kutatás módszerei

Kutatásom során a témához fűződő terjedelmes mennyiségű magyar és idegennyelvű szakirodalmat tekintettem át: monográfiákat, tankönyveket, tanulmánykötéteket, szaktanulmányokat, továbbá számos terrorizmussal foglalkozó szervezet dokumentumait, jelentéseit, bírósági határozatokat és jogszabályokat vizsgáltam meg.
A témához kapcsolódó számos magyar és idegennyelvű internetes forrást is felhasználtam.

6. A kutatás hipotézisei

Hipotéziseim a következők:
1. A terrorizmus jelensége 9/11 óta változáson esett át.
2. Az internet és a közösségi média elterjedése drasztikus változást hozott a terrorizmus jelenségébe.
3. A dark web napjaink terroristáinak fontos eszköze.
4. A terroristák kihasználják az okostelefonos alkalmazások előnyeit.
5. Az internethez kötődő terrorizmus finanszírozási források és technikák, főleg a kriptovaluták használata egyre nagyobb fenyegetést jelentenek.
6. A radikalizáció folyamatában korunkban kulcsszerepet játszik az internet.
7. Az interneten a terrorcselekményének többségének vannak előjelei.
8. Nem csak a muszlim elkövetők képviselik az egyedüli komoly terrorveszélyt.
9. Több online terjedő összeesküvés-elmélet terror-kockázatot képvisel.
10. Az incel elkövetők terroristák, és a főként online táplált és inspirált nőgyűlölő terrorizmusuk valós fenyegetést képvisel.
11. Az utóbbi évekbeli szélsőjobboldali terrorhullámba tartozó támadások között online kapcsolat állhat fenn.
12. Az online terjedő 3D lőfegyver tervrajzok komoly (terror-) veszélyt képviselnek.
13. A koronavírus (COVID-19) világjárvány hatott a terrorizmusra, és megnövelte a terroristák internethasználatának fenyegetését is.
14. A terroristák internethasználatának behatóbb ismerete hozzájárulhat a terrorcselekmények hatékonyabb megelőzéséhez.

II. A TERRORIZMUS DEFINÍCIÓJA ÉS TÍPUSAI

1. A terrorizmus definíciója

1. A meghatározás problémája

A terrorizmus meghatározása erősen problematikus. Számtalan szakértőnek, államnak, nemzetközi szervezetnek etc. van saját meghatározása. A definíció irodalma olyan hatalmas, és kérdése olyan komplex, hogy annak a részletes ismertetése a jelen korlátok között lehetetlen.

Mégis, a definíció kérdését szükséges legelsőként tárgyalni. Hogyan is elemezhetnénk egy jelenséget, vagy annak bármely aspektusát tudományos hitelességgel, ha azt nem tudjuk definiálni?

Ahogy Ganor fogalmaz: „A terrorizmus definiálásáért vívott küzdelem néha olyan nehéz, mint maga a terrorizmus elleni harc."[7]

Kérdés, hogy megragadható-e egyáltalán a terrorizmus lényege? Az egy komplex és többdimenziós jelenség, és a kifejezést a megnyilvánulások olyan széles skálájára használják (például narko-terrorizmusra, kiberterrorizmusra), hogy eltűnődhetünk azon, hogy egységes koncepcióról van-e szó[8], továbbá be kell látnunk, hogy nincs valódi esszenciája, alapvető lényege a terrorizmus koncepciójának, mert az ember alkotta konstrukció.[9]

Bartkó szerint nem adható minden előfeltételnek megfelelő válasz arra, pontosan mi a terrorizmus, könnyebb a terrorizmus jelenségének egyetlen elemére, a terrorcselekményre fókuszálni, mert a bűncselekményt felépítő tényállási elemek összegyűjthetők. A terrorizmus tekintetében nem adható egyetlen egzakt válasz, az több, részigazságokat magukban hordozó állítások halmaza. Hogy mi a terrorizmus, arra egy politikatudományi, egy (büntető/nemzetközi) jogi, és egy kriminológiai válasz adható, amelyek Bartkó szerint együtthatásukban vizsgálandók, mert egyik sem él meg a másik nélkül. Ezeknek a fogalmaknak az ismerete elengedhetetlen egy hatékony és időtálló büntetőpolitika kidolgozásához, mert a megalkotott definíciórendszerben minden

[7] „The struggle to define terrorism is sometimes as hard as the struggle against terrorism itself." Saját fordítás. GANOR, B.: Defining Terrorism: Is One Man's Terrorist another Man's Freedom Fighter? Police Practice and Research: An International Journal, 2002. Vol. 3. No. 4. 304. o.

[8] SCHMID (2004): i.m. 380. o

[9] Uo. 384. o.

fogalmi/tényállási elemnek önállóan is kiemelt szerepe van a terrorizmus elleni küzdelem kriminálpolitikai stratégiájának kidolgozásában.[10]

Bakóczi a terrorizmus kutatása és vizsgálatának nehézségei tekintetében öt fő akadálycsoportot sorol: 1. Egy egységesen elfogadott nemzetközi és nemzeti fogalmi meghatározás hiányát. 2. Az egységes, hiteles, hivatalos kriminálstatisztikai adatgyűjtési rendszerek hiányát, az önálló nemzeti és nemzetközi terrorcselekményi statisztikák kiadásának az elmaradását. 3. A terrorizmust és az ellene irányuló küzdelmet szükségszerűen övező konspiráltságot és titkosságot. 4. Az adatgyűjtés korlátait, a kutatás tárgyának nehéz elérhetőségét, a bűnügyi iratok anyagának korlátozott hozzáférhetőségét. 5. A terrorcselekmények körében jelentkező rejtettséget. Bakóczi az első helyen szerepelteti az akadálycsoportok listájában az egységesen elfogadott nemzetközi és nemzeti fogalmi meghatározás hiányát,[11] mely a probléma kiemelt fontosságát érzékelteti.[12]

A definícióval kapcsolatos vita a 2001. szeptember 11-i terrortámadás (továbbiakban 9/11) óta változó intenzitással, de szinte folyamatosan napirenden szerepelt, az Iszlám Állam (továbbiakban IS) terrorszervezet megjelenése pedig újra előtérbe helyezte.[13] Létezik olyan álláspont is, hogy a terrorizmust lehet ugyan definiálni, de szükségtelen.[14] Perry utal rá, hogy a definíció keresését szokás a Szent Grál kutatásához hasonlítani, azonban a Grállal szemben sok kutató bukkant terrorizmus meghatározásra, és az azt illető konszenzus legalább olyan elérhetetlennek tűnik, mint a Grál maga.[15] A meghatározások magas száma miatt azok taxatív felsorolása gigászi vállalkozás lenne. Schmid és Jongman a terrorizmus 109 definícióját vizsgálja.[16] Wang és Zhuang 200 feletti számot említ.[17]

---

[10] BARTKÓ R.: A terrorizmus elleni küzdelem kriminálpolitikai kérdései. UNIVERSITAS-GYŐR Nonprofit Kft., Győr, 2011.55. o

[11] BAKÓCZI A.: Megismerési akadályok a terrorizmus kutatásában. Belügyi Szemle, 2015/7–8. 90. o.

[12] SERBAKOV M. T.: A terrorizmus definíciójának kérdése. Büntetőjogi Szemle, 2019/2. 87. o.

[13] SZALAI M. – WAGNER P.: A terrorizmus fogalmának kiterjesztése? Értelmezési lehetőségek Orlando kapcsán. KKI-elemzések, 2016/19. 3. o.

[14] RAMSAY, G.: Why terrorism can, but should not be defined. Critical Studies on Terrorism, 2015. Vol. 8. No. 2. 211-228. o.

[15] PERRY, N. J.: The Numerous Federal Legal Definitions of Terrorism: The Problem of too Many Grails. Journal of Legislation, 2004. Vol. 30. No. 2. 249. o.

[16] SCHMID, A. P. – JONGMAN, A. J.: Political Terrorism: A New Guide to Actors, Concepts, Data Bases, Theories & Literature. Transaction Publishers, New Brunswick, 2008. 4–5. o. Idézi: HORVÁTH L. A.: A terrorizmus csapdájában. Zrínyi Kiadó, Budapest, 2014. 12. o.

[17] WANG, T. – ZHUANG, J.: The True Meaning of Terrorism and Response to Terrorism. Social Sciences,

A meghatározásokban mégis vannak közös elemek: Resperger a közös jellemzőkként sorolja a politikai, vallási, ideológiai indíttatást; az erőszak alkalmazását; a félelem kiváltásának szándékát; és a kormányzat és a társadalom megrendítését.[18]

2. Egy nemzetközileg elfogadott definíció hiánya

Schmid szerint ebben a fázisban egy univerzálisan elfogadott definíciót illető konszenzus hiánya inkább politikai, mint jogi, vagy szemantikai probléma.[19] Egy nemzetközi szinten elfogadott jogi definíció a terrorizmust illetően máig nincsen.[20]

Talán a legnagyobb kérdés a definíciós vitában, hogy egyáltalán kinek van hatalma azt megalkotni. A nemzeti parlamenteknek, a kormányoknak, bíróságoknak vagy akadémikusoknak? Áldozatoknak, a médiának, vagy az ENSZ-nek?[21]

Ki jogosult egyes államokat, szervezeteket, személyeket terroristának minősíteni, és meghatározni a fogalom kritériumait? Egy ország, vagy szervezet milyen kritériumok alapján és mikor „szűnik meg" terroristának lenni?[22] Kis-Benedek szerint az ENSZ lenne leginkább az a nemzetközi szervezet, amely hivatott lenne a definíció meghatározására, ám ott vannak a legnagyobb viták a fogalmat illetően.[23]

Egy nemzetközileg elfogadott jogi definíció híján a nemzetközi közösség két módszert alkalmaz a meghatározásra. Egyrészt törekszik meghatározni, mi nem jellemzi a terrorizmust (pl.: idegen megszállás elleni nemzeti és függetlenségi harc a nemzetközi jog szerint nem terrorista cselekmény), másrészt a terrorcselekmények azon jellemzői alapján igyekszik azt körülírni, amelyeket a nemzetközi közösség rendszeresen elítél (pl.: válogatás nélküli erőszakos támadások). Tálas szerint ilyen értelemben viszonylag egyetértés van abban, hogy mit tekinthetünk, illetve büntetőjogilag általában mit tekintenek az egyes országok büntető törvénykönyvei terrorista módszerrel elkövetett cselekményeknek, illetve terrorista tevékenységnek: többnyire olyan cselekményeket,

---

2017. Vol. 6. No. 6. 161. o.

[18] RESPERGER I.: A nemzetbiztonsági szolgálatok tevékenysége – biztonsági kihívások, kockázatok és fenyegetések. In: RESPERGER I. (szerk.): A nemzetbiztonság elmélete a közszolgálatban. Dialóg Campus Kiadó, Budapest, 2018. 76. o.

[19] SCHMID (2004): i.m. 390. o.

[20] Uo. 394. o.

[21] Uo. 385. o.

[22] JÓZSA L.: Globális terrorizmus – fogalmi keretek. In: TÁLAS P. (szerk.): Válaszok a terrorizmusra avagy van-e út az afganisztáni „vadászattól" a fenntartható globalizációig. SVKH–CHARTAPRESS, Budapest, 2002. 93. o.

[23] KIS-BENEDEK J.: Dzsihadizmus, radikalizmus, terrorizmus. Zrínyi Kiadó, Budapest, 2016. 145. o.

amelyek egyébként is bűncselekmények.[24] Tóth szerint a tételes jog szemléletétől, vizsgálati és fogalomrendszerétől egy jelenségcsoport kriminológiai megközelítése sokszor jelentősen eltér. A szervezett bűnözés vagy a terrorizmus meghatározására évente részben eltérő fogalmak tucatjai jelennek meg, sokszor az aktuális események mentén kiegészítve a jelenség változatos összetevőit. Ezek a definíciók azonban alapvetően előnyben részesítik a kriminalitással összefüggésbe hozható szociológiai, esetleg pszichológiai szempontokat, a strukturális viszonyokat, a hatásmechanizmusokat, egyes csoportok, közösségek indíttatását, mások reakcióit, a motivációk társadalmi beágyazottságát és hatásait vizsgálják. Tóth szerint gyakran megfigyelhető, hogy a szerzők úgy hiszik, ha minél több kritériumot sorolnak fel, annál pontosabb lesz a megközelítése, leírása a jelenségcsoportnak, emiatt a szervezett bűnözés és a terrorizmus tekintetében esetenként nagyon bonyolult, komplex definíciókat alkotnak. Tóth szerint ezek az elemzések hasznosak, tanulságokkal bírnak a tételes jog kodifikátorai és alkalmazói számára is, de nem léphetnek fel olyan igénnyel, hogy az egzakt fogalmi ismérvekkel, egységesen értelmezendő összetevőkkel működő anyagi büntetőjog teljes körűen befogadja a megállapításaikat, valamennyi, egymástól részben eltérő kritériumot értelmező rendelkezések vagy tényállási elemek részévé téve. A kriminológia a gyakran a több dimenziót felölelő definíciók összes lehetséges jellemzőit keresi, a tételes jognak viszont az alkalmazhatóság és a jogbiztonság miatt meg kell elégednie a „feltétlenül szükséges, de egyben elégséges, ugyanakkor egyértelműen definiálható és definiált fogalmi ismérvekkel."[25]

Vannak elfogadott meghatározásai a fogalmat illetően, pl. az ENSZ-nek, a NATO-nak, vagy az Európai Uniónak (továbbiakban EU). Az EU-ban a közösség egy saját meghatározást törekszik elfogadni, ugyanakkor a tagállamok továbbra is fenntartják a jogot, hogy a közösségi normákat tiszteletben tartva megfogalmazzák, számukra mi a terrorfenyegetettség.[26]

Vitatott, hogy a terrorizmus elsősorban büntetőjogi (európai felfogás), vagy büntetőjogi és politikai kategóriaként (amerikai felfogás) értelmezendő-e. Továbbá a nemzetközi szakirodalom egyre határozottabban elkülöníti a nemzetközi terrorizmuson belül a régi

[24] TÁLAS P.: A nemzetközi terrorizmus és a szervezett bűnözés hatása a nemzetközi biztonságra és Magyarország biztonságára. ZMNE Stratégiai Védelmi Kutatóintézet Elemzések, Budapest, 2007. 5–6. o.

[25] TÓTH M.: A terrorcselekmény büntetőjogi szabályozásának és gyakorlatának változásai. Hadtudomány, 2013/1-2. 30–31. o.

[26] HORVÁTH (2014): i.m. 13. o.

és az új típusú terrorizmust.[27]

3. Miért nehéz definiálni a terrorizmust?

Schmid tucatnál is több okát jelöli meg annak, hogy miért nehéz a terrorizmust definiálni, többek közt: A terrorizmus „vitatott koncepció", arról eltérnek a politikai, jogi, társadalomtudományi és hétköznapi elképzelések. A definíció kérdése a (de-)legitimizációhoz és kriminalizációhoz kötődik; sok típusa van, különböző formákkal és manifesztációkkal; és a kifejezés jelentésbeli változásokon ment át a több mint 200 éves létezése alatt.[28]

Bartkó szerint a fogalomalkotás nehézségeinek forrásai: a politikai reagálás megkésettsége, vagy olykor a politikai szerepvállalás elmaradása; a terrorizmus alapvető jellegzetességében rejlő ok - hogy a terroristák mint alvó ügynökök élnek köztünk; a kulturális meg nem értettség, amiért a társadalom egyéb tagjai, valamint a bűnüldöző hatóságok nem tudják, vagy nem képesek a merényletek erkölcsi alátámasztásaként szolgáló főként ideológiai okokat felmérni, megérteni; a terrorizmus sokszínűsége; végül a terrorizmus elleni küzdelem komplexitása, mivel a terrorizmus ellen folytatott harc már nem képezi le a hagyományos bűnüldözés metodikáját, az sokkal összetettebb annál.[29]

4. A terrorizmus szó eredete

A „terrorizmus" évszázadok óta általában a „másik oldal" megjelölésére használt pejoratív kifejezés. Ez a szó a politikai leíró szerepe, a jogi terminusként való használata kevésbé régre nyúlik vissza. A terror szó, mely a latin „terrere-ből" ered, a nyugat-európai nyelvekbe a francián keresztül férkőzött be a XIV. században, az angol nyelvben először 1528-ban használták. A terrorizmus szó politikai vonatkozásait a nagy francia forradalom idején nyerte. A Maximilien Robespierre vezetette francia törvényhozó testület rémuralma alatt 17.000 embert végeztek ki nyilvánosan, ez volt a „regime de la terreur."[30] A konzervatív angol politikus, Edmund Burke használta a legelsők között a

[27] TÁLAS (2007): i.m. 5–6. o.

[28] SCHMID (2004): i.m. 395. o.

[29] BARTKÓ (2011): i.m. 18–22. o.

[30] YOUNG, R.: Defining Terrorism: The Evolution of Terrorism as a Legal Concept in International Law and Its Influence on Definitions in Domestic Legislation. Boston College International and Comparative Law Review, 2006. Vol. 29. No. 1. 27. o.

„terrorizmus” és a „terrorista” szavakat, ezzel akarta felhívni a figyelmet a jakobinus állam túlkapásaira. A késő XIX. században az orosz anarchisták adoptálták a kifejezéseket, az állami tisztviselők leszúrását, megfojtását vagy lelövését büszkén „terrorizmusnak” nevezték. Azóta kevesen használták magukra ezeket a szavakat, azok ellenségek leírására használt pejoratív jelzőkké váltak.[31]

A „terrorizmus” szó első definícióját (système, régime de la terreur) a Francia Akadémia fogalmazta meg 1798-ban, a közelmúlt tapasztalatai nyomán.[32]

5. A címkézés jelensége

Townshend szerint azért nehéz megfelelő definíciót találni, mert a terrorista szó használata esetén címkézésről van szó, mert ezt leírást majdnem soha sem adoptálta önkéntesen személy vagy csoport. Ezt mások használják rájuk, elsősorban a megtámadott államok kormányai, melyek megbélyegzik erőszakos ellenfeleiket ezzel a súlyos mellékjelentéseket, embertelenséget, kriminalitást, és a tényleges politikai támogatás hiányát magában hordozó címmel. Az államok könnyen is gyártanak terrorizmus definíciókat.[33]

Példák címkézésre:

2002-ben Irak vádolta az USA-t állami terrorizmussal.[34]

Barack Obama amerikai elnök a 2013-as Boston maratoni bombatámadást terrorista cselekménynek minősítette, mert szerinte: „Bármikor, ha bombatámadás ártatlan civileket céloz, az terrorista cselekmény.”[35]

Joe Biden, akkor még megválasztott elnök, hazai terroristáknak („domestic terrorists”) nevezte az USA Capitoliumát 2021. január 6-án megostromló Trump-támogatók tömegét.[36]

---

[31] BARKER, J.: The no-nonsense guide to terrorism. Verso, London, 2003. 10. o.

[32] TOWNSHEND, Ch.: A terrorizmus. Magyar Világ Kiadó, Budapest, 2003. 45. o.

[33] TOWNSHEND, Ch.: Terrorism: A Very Short Introduction, Third Edition. Oxford University Press, Oxford, 2018. 4. o.

[34] Iraq accuses US of state terrorism. BBC News. (2002, February 20). http://news.bbc.co.uk/2/hi/middle_east/1830640.stm (2021.11.03.)

[35] „Anytime bombs are used to target innocent civilians, it’s an act of terror,” Saját fordítás. LANDLER, M.: Obama Calls Blasts an ‘Act of Terrorism’. The New York Times. (2013, April 16). https://www.nytimes.com/2013/04/17/us/politics/obama-calls-marathon-bombings-an-act-of-terrorism.html (2021.11.03.)

[36] Joe Biden slams pro-Trump mob as 'domestic terrorists'. Deutsche Welle. (2021, January 7). https://www.dw.com/en/joe-biden-slams-pro-trump-mob-as-domestic-terrorists/a-56163969 (2021.11.03.)

Nelson Mandelát, Menáhém Begín-t, Gerry Adams-t és Jasszer Arafatot kezdetben terroristának neveztek, később államférfiaknak és a béke megteremtőinek. Mandela, Begín és Arafat ráadásul Nobel-békedíjban is részesült.[37] A dél afrikai kormány ellen irreguláris eszközöket használó Mandelát Terry Dicks, brit parlamenti képviselő 1990-ben még terroristának nevezte, de néhány évvel később Mandela lett a Dél-afrikai Köztársaság első demokratikusan megválasztott elnöke, ráadásul Nobel-békedíjban is részesült.[38] Ahogy Ganor fogalmaz: „Valaki terroristája valaki másnak a szabadságharcosa."[39] Bács szerint nézőpont kérdése: „Terrorista vagy szabadságharcos? Forradalmár vagy államellenes összeesküvő? A haladás apostola vagy felforgató? Gerilla vagy útonálló? A klasszikus válasz a kérdésre abból indul ki, hogy honnan nézzük. Ha a fennálló rend szempontjából tekintjük, akkor minden eszme és annak minden képviselője, aki nem pusztán ellenérzéssel viseltet arend intézményeivel és képviselőivel szemben, de cselekvő módon, parlamenten kívüli eszközökkel igyekszik elérni a rend megváltoztatását, de legalábbis olyan eszméket terjeszt, amelyek célul tűzik a kialakult politikai, társadalmi és gazdasági rend és az annak alapját képező társadalmi viszonyok megváltoztatását: terrorista, felforgató, államellenes összeesküvő."[40]

Horváth szerint univerzális, nemzetközileg elfogadott meghatározással csak úgy találkozhatunk, ha valaki önkényesen kisajátítja a jogot, hogy egy mindenre kiterjedő megfogalmazást próbáljon meg elfogadtatni, ám hozzáteszi, hogy az ilyen próbálkozás minden bizonnyal kudarcra ítélt, hiszen már a lázadó és a terrorista között is nehezen tehető különbség.[41]

6. Példák definíciókra

A magas számú definíciók közül példálózó jelleggel ismertetek néhányat. Az idegen nyelvűeket magam fordítom.

---

[37] WEISS, P.: Terrorism, Counterterrorism and International Law. Arab Studies Quarterly, 2002. Vol. 24. No. 2–3. 11. o.

[38] HEGEMANN, H. – KAHL, M.: Was ist Terrorismus? Eine schwierige Begriffsbestimmung. In: HEGEMANN, H. – KAHL, M. (szerk.): Terrorismus und Terrorismusbekämpfung: Eine Einführung. Springer VS, Wiesbaden, 2018. 13. o.

[39] „One man's terrorist is another man's freedom fighter,"

GANOR: i.m. 287. o.

[40] BÁCS Z.: A terrorizmus egyes latin-amerikai ideológiai támaszai. Nemzetbiztonsági Szemle, 2021/1. 17. o.

[41] HORVÁTH (2014): i.m. 12. o.

Ganor szerint „terrorizmus a civilek vagy civil célpontok elleni erőszak szándékos alkalmazása vagy azzal történő fenyegetés, politikai célok elérése érdekében."[42] Vass szerint ez egy nemzetközileg egységesen elfogadható definíció.[43] Kiss is ezt a meghatározást tartja a leginkább használhatónak.[44] Magam is ezt az álláspontot képviselem.

Barker szerint terrorizmus: „erőszak alkalmazása, vagy azzal való fenyegetés; civil célpontok ellen; politikai célokból."[45]

Korinek meghatározása: „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 cselekménysor. Az eszköz viszont jogi lényegét tekintve köztörvényes, erőszakos bűncselekmény."[46]

Bartkó szerint a terrorizmus kriminológiai értelemben: „egy olyan jellemzően államon belüli, illetve államhatáron átnyúló (transznacionális) társadalmi jelenség, amely a civil szférába tartozó személyek, vagy jelentős értékű javak ellen intézett célzott jogtalan támadással kívánja megvalósítani ideológiai bázisát adó azon társadalmi-politikai célkitűzéseit, melyek egyébként a szervezet valamennyi tagja által alkalmazott erőszak legitimációjául szolgálnak, és amelyet a láthatatlanság, a változatosság, a váratlanság, valamint a nagyfokú mobilitás és a kiváló reprodukciós készség kriminológiai ismertetőjegyei jellemeznek."[47]

Resperger Clausewitz háború fogalmának („A háború tehát erőszak alkalmazása, hogy ellenfelünket akaratunk teljesítésére kényszerítsük."[48]) analógiájára alkotta meg a saját

---

[42] „terrorism is the intentional use of, or threat to use, violence against civilians or against civilian targets, in order to attain political aims." GANOR: i.m. 294. o.

[43] VASS Gy.: A terrorizmus finanszírozása elleni küzdelem nemzetközi aspektusai. PhD Értekezés. Nemzeti Közszolgálati Egyetem, Budapest, 2016. 46.o

[44] KISS Z. L.: A terrorizmus elleni küzdelem szociológiai természetű kihívásai. Hadtudomány, 2005/4. 182–187. o.

[45] BARKER, J.: The No-Nonsense Guide to Terrorism. Verso, London 2003. 23. o

[46] KORINEK L.: A terrorizmus. In: GÖNCZÖL K. – KEREZSI K. – KORINEK L. – LÉVAY M. (szerk.): Kriminológia-Szakkriminológia. CompLex Kiadó Jogi és Üzleti Tartalomszolgáltató Kft., Budapest, 2006. 447. o.

[47] BARTKÓ (2011): i.m. 54. o

[48] CLAUSEWITZ, C. von: A háborúról. Zrínyi Kiadó, Budapest, 2013. 39. o. Idézi: RESPERGER I.: A

terrorizmus fogalmát: „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."[49]

A NATO szerint a terrorizmus: „Félelmet vagy rettegést keltő erő vagy erőszak törvénytelen használata vagy azok használatával való fenyegetés, személyek vagy tulajdon ellen, kormányok, vagy társadalmak kényszerítésére vagy megfélemlítésére, vagy egy népesség felett az irányítás átvételére történő kísérlet során, politikai, vallási, vagy ideológiai célok elérése érdekében."[50]

Az ENSZ Kábítószer-ellenőrzési és Bűnmegelőzési Hivatala szerint „tágabb értelemben a terrorizmus felfogható úgy, mint a kényszerítés egy módja, amely félelem terjesztése érdekében erőszakot alkalmaz, vagy annak alkalmazásával fenyeget, hogy ezáltal politikai vagy ideológia célokat érjen el."[51]

Az Institute for Economics & Peace Global Terrorism Index terrorizmus definíciója: „illegális erővel és erőszakkal való fenyegetés vagy annak tényleges alkalmazása egy nem állami szereplő által, egy politikai, gazdasági, vallási, vagy társadalmi cél elérése érdekében, félelmen, kényszerítésen vagy megfélemlítésen keresztül."[52]

A Global Terrorism Database szerint: „Egy nem állami szereplő jogtanal erővel vagy erőszakkal való fenyegetése, vagy azok tényleges használata politikai, gazdasági, vallási

---

nemzetbiztonsági szolgálatok tevékenysége – biztonsági kihívások, kockázatok és fenyegetések. In: RESPERGER I. (szerk.): A nemzetbiztonság elmélete a közszolgálatban. Dialóg Campus Kiadó, Budapest, 2018. 76. o.

[49] Uo. 76. o.

[50] „The unlawful use or threatened use of force or violence, instilling fear and terror, against individuals or property in an attempt to coerce or intimidate governments or societies, or to gain control over a population, to achieve political, religious or ideological objectives." MC 0472/1 MILITARY COMMITTEE CONCEPT FOR COUNTER – TERRORISM. North Atlantic Military Committee, 2016. 5. o. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_01/20160817_160106-mc0472-1-final.pdf (2021.10.28.)

[51] „(…) terrorism can be broadly understood as a method of coercion that utilizes or threatens to utilize violence in order to spread fear and thereby attain political or ideological goals." United Nations Office On Drugs And Crime: Education For Justiceuniversity Module Series: Counter-Terrorism: Module 1: Introduction To International Terrorism. United Nations, Bécs, 2018. 1. o. https://www.unodc.org/documents/e4j/18-04932_CT_Mod_01_ebook_FINALpdf.pdf (2021.10.28.)

[52] „the threatened or actual use of illegal force and violence by a non-state actor to attain a political, economic, religious, or social goal through fear, coercion, or intimidation." Global Terrorism Index 2017: Measuring and Understanding the Impact of Terrorism. Institute for Economics and Peace, 2017. 6. o. https://reliefweb.int/sites/reliefweb.int/files/resources/Global%20Terrorism%20Index%202017%20%284%29.pdf (2021.11.01.)

vagy társadalmi cél elérése érdekében, félelem, kényszer, vagy megfélelmítés révén."[53]

A terrorizmus elleni küzdelemről szóló 2017/541 Irányelv 3. cikke a terrorista bűncselekményeket a következőképp határozza meg:

„(1) A tagállamok meghozzák a szükséges intézkedéseket annak biztosítására, hogy terrorista bűncselekményként határozzák meg a nemzeti jogban bűncselekményként meghatározott következő olyan szándékos cselekményeket, amelyek jellegük vagy összefüggéseik folytán komoly kárt okozhatnak egy államnak vagy egy nemzetközi szervezetnek, amennyiben azokat a (2) bekezdésben felsorolt célok egyike véghezvitelének érdekében követik el: a) személy élete elleni támadás, amely halált okozhat; b) személy testi épsége elleni támadás; c) emberrablás vagy túszejtés; d) kormányzati létesítmény vagy közintézmény, közlekedési rendszer, infrastrukturális létesítmény – beleértve az informatikai rendszert is –, kontinentális talapzaton rögzített építmény, közterület vagy magántulajdon olyan súlyos megrongálása, amely emberi életet veszélyeztethet vagy jelentős gazdasági veszteséget idézhet elő; e) légi jármű, vízi jármű vagy más tömegközlekedési, illetve áruszállító eszköz hatalomba kerítése; f) robbanóanyag vagy lőfegyver, ideértve a vegyi, biológiai, radiológiai vagy nukleáris fegyvereket, előállítása, birtoklása, megszerzése, szállítása, rendelkezésre bocsátása vagy felhasználása, valamint a vegyi, biológiai, radiológiai vagy nukleáris fegyverekkel kapcsolatos kutatás és fejlesztés; g) veszélyes anyag kiengedése, vagy tűzvész, árvíz vagy robbanás előidézése, amely emberi életet veszélyeztet; h) a víz- vagy áramellátásnak, illetve más létfontosságú természeti erőforrás ellátásának olyan megzavarása vagy megszakítása, ami emberi életet veszélyeztet; i) a 2013/40/EU európai parlamenti és tanácsi irányelv (1) 4. cikkében említett, rendszert érintő jogellenes beavatkozás azokban az esetekben, amelyekre az említett irányelv 9. cikkének (3) bekezdése vagy 9. cikke (4) bekezdésének b) vagy c) pontja alkalmazandó, valamint a 2013/40/EU irányelv 5. cikkében említett, adatot érintő jogellenes beavatkozás azokban az esetekben, amelyekre az említett irányelv 9. cikke (4) bekezdésének c) pontja alkalmazandó; j) az a)–i) pontban felsorolt cselekmények elkövetésével való fenyegetés. (2) Az (1) bekezdésben említett célok az alábbiak: a) a lakosság súlyos megfélemlítése; b) egy kormány vagy egy nemzetközi szervezet jogellenes kényszerítése arra, hogy az valamilyen intézkedést megtegyen vagy ne tegyen meg; c) egy ország vagy egy nemzetközi szervezet alapvető politikai, alkotmányos, gazdasági vagy társadalmi

[53] „The threatened or actual use of illegal force and violence by a non-state actor to attain a political, economic, religious, or social goal through fear, coercion, or intimidation. Global Terrorism Database." https://www.start.umd.edu/gtd/ (2021.12.16.)

struktúráinak súlyos destabilizálása vagy lerombolása."[54]

7. A terrorizmus kifejezés túlhasználatáról és a terrorista és a tömeggyilkos (mass murderer vagy mass shooter) közötti elhatárolás problémájáról

Az orlandói „Pulse" szórakozóhelyen, Omar Mateen 2016-os tömeggyilkosságával kapcsolatban Szalai és Wagner a terrorizmus fogalmának inflálódásának[55] folyamatára figyelmeztet, mely során a nyugati közvéleményben a terrorizmus kifejezés jelentése egyre tágul. Egyre több eseményt jellemeznek így, ami hosszú távon negatívan hathat a terrorizmus elleni küzdelem hatékonyságára.

Az orlandói eset első értelmezései terrorcselekményről, és a radikális iszlamizmus terjedéséről szóltak, de a később nyilvánosságra került információk már más motivációra engedtek következtetni. A szerzők szerint kérdéses a határ a gyűlölet-bűncselekmények, politikai gyilkosságok és a terrorista merényletek között.[56]

Hogy egy adott eset kapcsán használható-e a terrorizmus kifejezés, annak eldöntésére egy mélyebb vizsgálatra van szükség.[57] Szalai és Wagner arra világít rá, hogy egy-egy esemény kapcsán a terrorizmus mellett más értelmezések is felmerülnek, felmerülhetnek, de a média egyre gyorsabban és egyre szélesebb körben használja a terrorizmus kifejezést, legalábbis, muszlim elkövető esetén. A kifejezés túlhasználata akár a nyugati társadalmak biztonságát is csökkenthető veszélyekkel járhat. Fenyegetés érzetét kelthet a társadalomban, mely radikális válaszokhoz vezethet, amik nemcsak hatástalanok lehetnek a fenyegetés csökkentése szempontjából, de akár erősíthetik is azt. Továbbá, ha a terrorizmus definícióját a közvélemény egyre tágabban értelmezi, akkor az a törvényhozás szintjén is megjelenhet, ami hatósági visszaéléseknek adhat teret, és megnehezíti a terrorizmusellenes stratégiák hatékony működését. Végül a merényletek terrorcselekményként értelmezése és az IS vagy al-Kaida felelősségvállalásának szinte automatikus elfogadása a terroristák törekvéseinek kedvez, mert nekik érdekük, hogy a média felkapja az esetet. Szalai és Wagner szerint fontos, hogy a dzsihadista

[54] AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2017/541 IRÁNYELVE (2017. március 15.) a terrorizmus elleni küzdelemről, a 2002/475/IB tanácsi kerethatározat felváltásáról, valamint a 2005/671/IB tanácsi határozat módosításáról. 13. o.

[55] A kifejezés „pongyola használatára" Perry is figyelmeztet. PERRY: i.m. 252–254. o.

[56] SZALAI – WAGNER: i.m. 3. o.

[57] Uo. 6–7. o.

terrorizmus keltette közhangulatnak ellenálljunk, és megőrizzük a pontos definícióval nem rendelkező terrorizmus kifejezés legfontosabb tartalmi jellemzőit, és mindig különbséget tegyünk a politikai célú és az egyéb motivációjú „közönséges" erőszak között.[58] Egyetértek azzal, hogy a terrorizmus kifejezéssel óvatosan kell bánni, az csak megfontoltan használandó, nem szabad a túlhasználattal „elkoptatni."

Egy adott elkövetés tekintetében tehát vitás lehet, hogy azt terrortámadásnak, vagy pedig tömeggyilkosságnak nevezzük-e. Az elhatárolás kérdése különösen nehéz például a szélsőjobboldali terrorizmus témájának kutatása során.[59]

A határ sokszor nagyon vékony, bizonytalan és erősen vitatott. Úgy vélem, a tömeggyilkos és a terrorista hasonló fokban veszélyes a társadalomra, mindkét elkövető cselekményét ugyanolyan fontos megakadályozni. Az ártatlan áldozat számára mindegy, hogy tömeggyilkosnak vagy pedig terroristának minősített elkövető veszi el az életét.

Az elhatárolás külön dolgozat tárgya lehetne.

8. Következtetések

Nem realisztikus abban bíznunk, hogy a közeljövőben megszületik egy nemzetközileg egységesen elfogadott terrorizmus definíció. Egyetértek Waldron-nal, aki szerint a lényeg nem az, hogy definiáljuk a terrorizmus szót, hanem hogy megértsük azt, annak érdekében, hogy kitalálhassuk, mit tehetünk ellene.[60] A definiálásra való törekvés közelebb vihet a terrorizmus természetének megértéséhez, mely által a terrorizmus elleni harc is hatékonyabbá válhat, az véleményem szerint nem csupán önmagáért való akadémiai okoskodás.

2. A terrorizmus típusai

Cunningham szerint az egyik fő probléma a terrorizmus paramétereinek megértésével kapcsolatban egy hasznos tipológia kifejlesztésnek a kérdése, mivel annak még általánosan elfogadott tipológiája sincsen.[61] Tipizálása számos módon lehetséges.[62]

[58] Uo. 9–10. o.

[59] TAYLOR, H.: Domestic terrorism and hate crimes: legal definitions and media framing of mass shootings in the United States. Journal of Policing, Intelligence and Counter Terrorism, Vol. 14. No. 3. 2019. 227. o.

[60] WALDRON, J.: Terrorism and the Uses of Terror. The Journal of Ethics, 2004. Vol. 8. No. 1. 35. o.

[61] CUNNINGHAM, Jr. W. G.: Terrorism Definitions and Typologies. In: Moore, R. S. (szerk.): Terrorism: Concepts, Causes, and Conflict Resolution. U.S. Defense Threat Reduction Agency, Fort Belvoir, 2003.

A terrorcselekmények elkövetői legtöbbször politikai, vallási, etnikai vagy morális ügy érdekében cselekszenek. Jellemzően így hatalmazzák fel magukat az erőszak alkalmazására a „magasabb rendű cél" érdekében. Ezekből az eszmékből, eszmerendszerekből, ideológiákból a terrorizmus történelme alatt nagyon sok akadt, ennek megfelelően a terrorizmus az ideológiai alapon is osztályozható. A legjellemzőbbek a következők:

Politikai ideológiák: különböző politikai szélsőségek (szélső-baloldali és szélsőjobboldali szervezetek, anarchista, nihilista csoportok).

Szélsőséges vallási ideológiák: az alap jellemzően a hit szélsőséges értelmezésében keresendő, és kétségtelenül napjaink egyik nagy fenyegetése az iszlám indíttatású terrorizmus, de léteznek számos más vallások által átitatott szélsőséges csoportok is.

Etnikai és nemzeti függetlenségi ideológiák: lényegében a politikai ideológiákhoz tartozó, de mégis külön kezelendő kategória, mely politikai-filozófiai töltetét tekintve talán a legtágabb.

Tematikus: azok a csoportok tartoznak ide, amelyek különböző politikai, gazdasági vagy társadalmi vonatkozású – sokszor erkölcsi, morális – céljaik elérése érdekében olyan erőszakos módszereket alkalmaznak, amelyek már megvalósítják a terrorcselekmény tényállását, kimerítik a terrorizmus fogalmát (ilyenek lehetnek a különböző környezetvédelmi, globalizációellenes csoportok is). A fentieken túl, természetesen a terrorizmust – mivel az egy sok összetevőből álló, komplex rendszer – több szempont szerint osztályozhatjuk.[63] Például az alkalmazott eszközök szerint beszélhetünk az ún. hagyományos eszközökről; a modernitás, illetve posztmodern technikát a politikai erőszak szolgálatába állító ún. techno-, cyber- és nano-terrorizmusról; a narkoterrorizmusról; és a tömegpusztító fegyverek bevetését is latolgató ún. „szuper-"/„legvégső-" vagy „mega"-terrorizmusról.[64]

A terrorizmus típusait tekintve Korinek megkülönböztet állami és nem állami terrorizmust; kisebb jelentőséget tulajdonít a nemzeti és nemzetközi terrorizmus elhatárolásának. Ideológiai indíttatást tekintve megkülönböztet szélsőjobboldali és szélsőbalos szervezeteket, etnikai, faji, vallási okokra visszavezethető, vagy ilyen célok

---

23. o.

[62] TÓTH D.: A terrorizmus típusai és a kiberterrorizmus. In: RAB Virág (szerk.): XII. Országos Grastyán Konferencia előadásai. PTE Grastyán Endre Szakkollégium, Pécs, 2014. 286–296. o.

[63] KISS T.: A terrorizmus arculatváltásának hatása a helyszíni reagálóerők felkészítésére. Honvédségi Szemle – Hungarian Defence Review, 2021/5. 19. o.

[64] KISS Z. L.: A terrorizmus elleni küzdelem szociológiai természetű kihívásai. Hadtudomány, 2005/4. 182–187. o.

által vezérelt terrorizmust. Az alkalmazott eszközök és módszerek alapján tipizál nukleáris-, biológiai-, környezeti- és ökoterrorizmust. Korinek említi a „városi terrorizmust" (urban terrorism) és a virtuális terrorizmust (cyberterrorism), és elkülöníti a szervezet tagjaként, de legalábbis meghatározott csoporthoz tartozó terroristákat és az egyedül tevékenykedő „magányos farkasokat."[65] Somkuti és Major a terrorizmus modern kori megjelenési formáit állami terrorizmusra és nem állami terrorszervezetekre osztja. Előbbiekhez tartozik a szélsőjobboldali állami terrorizmus és a szélsőbaloldali állami terror, utóbbiakhoz pedig az anarchista, a nacionalista/etnikai terrorszervezetek, a vallási terrorizmus, a politikai (célokat követő) és az egyéb terrorszervezetek.[66]

Az EUROPOL a terrorszervezeteket motivációjuk forrásai alapján kategorizálja. Ugyan sok csoportnak kevert a motiváló ideológiája, ám ezekben általában egy ideológia, vagy motiváció dominál. Az EUROPOL szerint a terrorizmus típusai: dzsihadista, jobboldali, baloldali és anarchista terrorizmus, etno-nacionalista és szeparatista, és az egyetlen üggyel foglalkozó terrorszervezetek (single issue).[67] Az FBI (Federal Bureau of Investigation, Szövetségi Nyomozó Iroda, továbbiakban FBI) hazai (domestic) és nemzetközi terrorizmus között tesz különbséget, a terrorszervezet eredete, bázisa és céljai alapján.[68]

[65] KORINEK L.: A terrorizmus. Belügyi Szemle, 2015/7-8. 17-19. o.

[66] SOMKUTI B. – MAJOR Cs.: A terrorizmus modern kori megjelenési formái. In: BEBESI Z. (szerk.): Terrorelhárítási alapismeretek. Dialóg Campus, Budapest, 2016. 113–129. o.

[67] EUROPEAN UNION TERRORISM SITUATION AND TREND REPORT 2018 (TESAT 2018). 64.o https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-2018-tesat-2018 (2021.03.02.)

[68] Terrorism Report - 2002-2005. V. o. https://www.fbi.gov/file-repository/stats-services-publications-terrorism-2002-2005-terror02_05.pdf/view (2021.03.02.)

III. A NEMZETKÖZI TERRORIZMUS TÖRTÉNETE ÉS JELENSÉGÉNEK VÁLTOZÁSA NAPJAINKBAN

1. A terrorizmus története dióhéjban

A terrorizmus bonyolult jelenség, hosszú és összetett történelemmel,[69] melyet dolgozatomban csak vázlatosan mutatok be, fókuszomat inkább az utóbbi évtizedekben történt változásaira helyezem, mivel azok felvázolása a dolgozatom témájának megértése szempontjából elengedhetetlen.

Bartkó Gearty „Terror" című könyvére utal, mely szerint a szakemberek öt történelmi mozgalmat különítenek el a terrorizmus történeti fejlődésében: az első az ókor terroristái, a szikarioszok, egyes szerzők szerint még a júdeai zelóták és az indiai thugok. A második a középkori asszaszinok, a harmadik az 1793-1794-ig tartó jakobinus terror, melyet követ a XIX. századi ír nacionalisták, és az Ír Köztársasági Hadsereg. A tagolásban az ötödik az oroszországi anarchisták korszaka.[70] Bartkó ezeket kiegészíti a két világháború közötti időszakkal, mikor a terrorizmus már nem kormányok, állami vezetők ellen irányuló forradalmi erőszakot jelentette, hanem a totalitárius diktatúrák polgáraikkal szemben alkalmazott, a teljes és feltétel nélküli engedelmesség fenntartására irányuló elnyomásra utalt.[71]

A terrorista csoportok elődei már a Római Birodalomban is jelen voltak.[72] Az első századi Palesztinában a zelóták szektája az egyik első csoport volt, akik szisztematikus terrort gyakoroltak, a rómaiakat ölték, váratlanul csaptak le vallási, politikai személyek, és épületek ellen is. Flavius Josephus őket sicarii-nek nevezi, mely a latin sicarius-ból (tőrös ember) ered.[73]

Az asszaszinok 1090-től 1275-től két századon át végezték a tevékenységüket, és politikai céljaik is voltak, az iszlám vallás beteljesítésére, megtisztítására.[74]

---

[69] BLUMENAU, B.: Terrorism, History and Neighbouring Disciplines in the Academy. In: ENGLISH, R. (szerk.): The Cambridge History of Terrorism. Cambridge University Press, Cambridge, 2021. 124–146 o.

[70] GEARTY, C.: Terror. Holnap Kiadó, Budapest, 1994. 31. o. Idézi: BARTKÓ (2011): i.m. 59–66. o.

[71] BARTKÓ (2011): i.m. 66. o.

[72] BODA J.: A terrorizmus rövid története és az ellene való fellépés lehetőségei. Rendvédelem-történeti Füzetek (Acta Historiae Preasidii Ordinis), 2007/16. 46. o.

[73] CHALIAND, G. – BLIN, A.: Zealots and Assassins. In: CHALIAND, G. – BLIN, A. (szerk.): The History of Terrorism: From Antiquity to Al Qaeda. University of California Press, Berkeley, 2007. 55–58. o.

[74] RAPOPORT, D. C.: Fear and Trembling: Terrorism in Three Religious Traditions. The American Political

A modern terrorizmus történeti szakaszolását illetően Rapoport felosztásában az első az „anarchista hullám", amely az 1880-as években indult Oroszországból és egy évtized leforgása alatt elérte Nyugat-Európát, a Balkánt és Ázsiát. Ezt a hullámot tekinti Rapoport a történelem első globális, vagy valóban nemzetközi terrorista jelenségének, és a modern terrorizmus kezdetének. A második, az „antikolonialista hullám" az 1920-as években jelent meg, és kb. az 1960-as évekig tartott. Ezt követte a harmadik, az „új baloldali hullám", amely a 20. század végére el is halt, és már csak Nepálban, Spanyolországban, az Egyesült Királyságban, Peruban, és Kolumbiában működnek még ehhez kapcsolódó csoportok. 1979-ben jelent meg a „vallási hullám". Rapoport spekulációja szerint, a megelőző három hullám mintája alapján, 2025-re eltűnhet ez a hullám, és egy új jelenhet meg.[75] Hoffman a mondern nemzetközi terrorizmus megjelenését 1968-ra teszi.[76] A modernkori terrorizmus megjelenését Horváth az 1960-as évek repülőgép-eltérítéseihez köti.[77]

A terrorizmust illető akadémiai érdeklődés a XIX. században indult, az anarchista terrorizmus 1880-1914-ig tartó „aranykorára" való reakcióként. A nyugati világban a jelenség eredetét és természetét illető szisztematikus kutatás az 1970-es években kezdődött, amikor Nyugat-Európában, az USA-ban és Japánban terrorista taktikákat kezdtek alkalmazni olyan csoportok, mint a Vörös Hadsereg Frakció (Rote Armee Fraktion, RAF), a Vörös Brigádok (Brigate Rosse, BR), a Ír Köztársasági Hadsereg (Provisional Irish Republican Army, vagy Irish Republican Army, IRA), a Weather Underground, és a Japán Vörös Hadsereg (Nihon Sekigun, JRA).[78]

2. A terrorizmus természetének változása

2001 szempember 11-én 19 al-Kaidához tartozó terrorista eltérített négy utasszállító repülőgépet, melyek közül kettőt belereptettek New Yorkban a World Trade Center

---

Science Review, 1984. Vol. 78. No. 3. 664. o.

[75] RAPOPORT, D. C.: The Four Waves of Modern Terrorism. In: CRONIN, A. K. – LUDES, J. M. (szerk.): Attacking Terrorism: Elements of a Grand Strategy. Georgetown University Press, Washington, D.C., 2004. 47.o

[76] HOFFMAN, Bruce: Inside Terrorism. Columbia University Press, New York, 2017. 1–494. o.

[77] HORVÁTH (2014): i.m. 11. o.

[78] DIETZE, Carola: Introduction: Writing the History of Terrorism. In: DIETZE, Carola – VERHOEVEN, Claudia (szerk.): The Oxford Handbook of the History of Terrorism. Oxford University Press, New York, 2022. 1. o.

ikertornyaiba, melyek röviddel azután összeomlottak. A harmadik gép a Pentagonba csapódott. A negyedik gép utasai ellenálltak, a gép egy pennsylvania-i mező zuhant. A támadásban közel háromezer ember vesztette életét. Érzékeltetésképp: a teljes XX. század során 34 terrortámadás ölt meg több mint ötszáz embert. 9/11-ig egy terrorszervezet sem ölt többet 500 embernél.[79]

Barker szerint mind a terrorizmus, mind az ellene folytatott harc 9/11-el új korszakába érkezett.[80] Így véli Korinek is, aki 9/11 után kevésbé kiszámítható, új típusú terrorizmusról beszél, mely totális háborút vív, korlátlan eszközeiben, módszereiben, és célpontjaiban.[81]

1990 előtt a terrorszervezetek fókuszában főleg állami, vagy katonai célpontok voltak, és céljuk jól meghatározott követeléseik érvényesítése volt. A Szovjetunió felbomlásával és a bipoláris világ megszűnésével új hatalmi pólusok alakultak ki. A kapitalista és szocialista blokkok ellentétét felváltotta a nyugati és az iszlám kultúra szembenállása. A terrorszervezetek is igazodtak a nemzetközi politikai folyamatokhoz: Megváltozott a szervezeti struktúrájuk, az elkövetés módja, formája és a célpontjaik köre, mely bővült: előtérbe kerültek a puha célpontok, azaz a gyengén védett, vagy nehezebben védhető helyek, ahol nagy tömeg jelenlétére lehet számítani és egy esetleges támadás jelentős médiafigyelmet vonhat magára. Az IS megjelenése és 2006 utáni tevékenysége megváltoztatta a terrorszervezetek működési modelljeit. Megjelent a korábban ismeretlen pókháló típusú szervezeti felépítés és a hozzá fűződő elkövetési modellek.[82]

Új típusú elkövetési formák jelentek meg. Napjainkban megjelent a kiadások csökkentésére törekvés, amely erősen megnehezíti a rendvédelmi szervek feladatát. Az egyre többféle és többszintű biztonsági rendszerek kiépítése, rendszabályok, protokollok bevezetése érezhető hatással van az elkövetői oldalon igénybe vehető eszköztárra. Izraelben, az elmúlt években egyre gyakoribbá váltak a nyílt helyeken (pl.: buszmegállókban, pályaudvarokon) késsel elkövetett támadások. Nem a hatékonyságra való törekvés, hanem az egyszerűség és elérhetőség a fontos a terroroisták számára. Az izraeli rendészeti szolgálatok híresek a felderítési tevékenységükről, így az ellenőrzés szigorodásával egyenes arányban szűkült a terroristák mozgástere. Megjelentek a paralel támadások, melyek célja egy időben és több helyszínen az áldozatszám maximalizálása. Ezek jelentős terhet rónak a rendvédelmi és az első reagáló szervekre is. Alternatív

[79] HOFFMAN: i.m. 1–494. o.

[80] BARKER, J.: A terrorizmus. HVG Kiadói Rt., Budapest, 2003. 17–19. o.

[81] KORINEK (2006): i.m. 450. o.

[82] JASENSZKY N. (szerk.): Mindennapi biztonság. Terrorelhárítási Központ, Budapest, 2019. 7. o.

formája a másodlagos támadás, amely során az első támadást követően újabb, időben eltolt támadásra kerül sor azért, hogy tovább fokozzák az első reagáló erők leterheltségét, vagy akár azok váljanak célponttá. Olyan célpontokat választanak, ahol sok ember van és válogatás nélkül ölnek, ezzel próbálva maximalizálni az áldozatok számát. Jellemző lett a „hibrid támadás", amely során például egy fegyveres támadást robbantásos öngyilkos merénylet követ. Az elkövetők az esetek többségében nem akarnak elmenekülni, egyéni motivációjuk a mártírhalál. Napjaink terrorizmusa nem az ideológiai vagy bármely más követelésekről szól, hanem a halottak számának maximalizálásáról és a félelemkeltésről.[83] A terrorcselekmények elkövetési formái egyre változatosabbak. A robbantások a leggyakoribbak, de emberrablások, túszejtések, gyújtogatások is előfordulnak, és megjelent a kiberterrorizmus is. Európában megjelentek a gépjárművel tömegbe hajtásos elkövetések, előfordultak gépfegyveres, illetve egyre gyakoribbak a késes támadások. 2018-ban három olyan eset volt, amikor a tervezett támadások kapcsán a vegyi, biológiai, radiológiai vagy nukleáris fegyverek használata is felmerült.[84]

Kiss is rámutat arra, hogy a terrorizmus fajtáihoz, formáihoz fűződő elkövetések jellege az elmúlt évtizedekben jelentősen változott. A támadások központjában már nem túszejtések és követelések állnak, hanem elsősorban aktívlövész-szituációk és öngyilkos robbantások. Jó példa erre a 2020. novemberi bécsi terrorcselekmény, mely megközelítőleg kilenc perce alatt az elkövető folyamatosan mozgott, és válogatás nélkül nyitott tüzet a belvárosi szórakozóhelyek vendégeire és az utcán tartózkodókra, majd az odaérkező rendőrökre. Négyen életüket vesztették, huszonkét személy megsebesült. A támadó 20:00 óra körül kezdett lövöldözni, majd 20:09-kor az osztrák rendőrség bécsi különleges szolgálatának két odaérkező tagjával tűzharcba keveredett, melynek során meghalt. A támadás tekintve az elkövető motivációit és az elkövetés jellegét illeszkedik abba a folyamatba, amely az elmúlt években Nyugat-Európában megkezdődött.[85]

Fábián is rávilágít az utóbbi négy-öt évben történt jelentős változásokra. A terrorcselekmények sok esetben nem igényelnek jelentős finanszírozást, előzetes szervezést, előkészítést, létrejött az „olcsó és egyszerű" terrorizmus. Az elkövetők legtöbbször olyan cselekmények révén követik el tettüket, melyekről korábban sem a

[83] JASENSZKY: i.m. 8–9. o.

[84] NAGY K. – MEZEI J.: A biztonságtudatosítás megjelenése a terrorelhárítás területén. Nemzetbiztonsági Szemle, 2019/4. 106. o.

[85] KISS T.: A terrorizmus arculatváltásának hatása a helyszíni reagálóerők felkészítésére. Honvédségi Szemle – Hungarian Defence Review, 2021/5. 17. o.

jogalkotó, sem a közvélemény nem gondolta, hogy terrorcselekmény tipikus megvalósítási formái lennének.[86] Ahogy Bartkó fogalmaz: „Az egyes elhárítási eszközök a terrorista akciókkal együtt fejlődnek, így továbbra is alátámasztódni látszik a mára már „közhelynek" tekinthető állítás, miszerint a bűnözők egy lépéssel mindig a bűnüldöző hatóságok előtt járnak."[87]

Az Europol 2021-es jelentése arról számol be, hogy az EU-ban 2020-ban a legtöbb dzsihadista terrortámadás egyszerű volt, melyek esetében a modus operandi kezdetleges módszerekből állt, mint késelés, gázolás, gyújtogatás. Kivétel a bécsi támadás, mely során lőfegyvert használtak (de az sem volt igazán szofisztikált elkövetés).[88]

2019-2020-ban globálisan egy szélsőjobboldali terrorhullám volt tapasztalható: (Pittsburgh,) Christchurch, Poway, El Paso, Halle, Bærum és Haunau, mely Macklin szerint a jobboldali extrémisták erőszakos online szubkulturális miliőiben ösztönzött láncreakció.[89]

A terroristák kezében megjelentek a modern technológia vívmányai, köztük az internet, a közösségi média, az okostelefonok és az azokhoz kötődő alkalmazások és a 3D nyomtatás elterjedése és fejlődése. Ezek hatalmas változást hoztak a terrorizmus jelenségébe.

3. Az EU-t érintő migrációs nyomás és a terrorizmus kapcsolata

A nemzetközi, főleg az EU-t érintő migrációs nyomás az elmúlt két évtizedben egyre nőtt, az EU tagállamai egyre több a fejlődő országokól érkező migráns fogadására kényszerültek.[90] A migráció és a kriminalitás között összefüggés van.[91] Az előbbi

[86] FÁBIÁN P.: A terrorcselekmény büntetőjogi szabályozásának jelene és aktuális kérdései. Büntetőjogi Szemle, 2018/2. 49. o.

[87] BARTKÓ (2011): i.m. 68. o.

[88] European Union Terrorism Situation and Trend report (TESAT) 2021. Europol, 2021. 7. o. https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-2021-tesat (2021.09.12.)

[89] MACKLIN, G.: The El Paso Terrorist Attack: The Chain Reaction of Global Right-Wing Terror. CTC Sentinel, 2019. Vol. 12. No. 11. 1. o.

[90] TRIANDAFYLLIDOU, A. – MAROUKIS, T.: Migrant smuggling: Irregular migration from Asia and Africa to Europe. Palgrave Macmillan, London. 2012. 1. o. Idézi: BARTKÓ R.: Az illegális migráció és a terrorizmus kapcsolata az EUROPOL és FRONTEX jelentéseire tekintettel. In: BARTKÓ R. (szerk.): A terrorizmus elleni küzdelem aktuális kérdései a XXI. században. Gondolat Kiadó, Budapest, 2019. 167. o.

egyszerre lehet terrorista cselekmények eszköze és katalizátora.[92] A FRONTEX adatai alapján 2015-ben a migrációs krízis csúcsán közel 1 800 000 illegális határátlépést rögzítettek az EU államai, míg 2016-ban 511 047-et, mely jóval alacsonyabb, de még mindig kirívóan magas.[93] Bartkó az EUROPOL és a FRONTEX jelentéseit elemezve a következő megállapításokat teszi: A terrortámadások, illetve letartóztatások területi eloszlását vizsgálva, az adatokból jól látszik, hogy az illegális migránsok potenciális célállomásai a terrortámadások és a terroristagyanús személyek tekintetében a legfertőzöttebbek. Kiemelve a vallási indíttatású, dzsihadista merényletek potenciális elkövetőit, és az ezzel gyanúsítottakat, az adatok még beszédesebbek. A vallási indíttatású merénylők száma azokban az államokban magas, és tipikusan az irreguláris migránsok célországaiban fordulnak elő a legnagyobb valószínűséggel. Bartkó összefoglalva megállapítja, hogy ugyan nem tekinthető az illegális migráns terroristának, azonban a – főként vallásilag motivált és legitimált – terrorizmus a megváltozott biztonsági helyzet egyértelmű haszonélvezője, mely az EU-ban 2015 óta a jelentések alapján is érzékelhető.[94] Az EU tagállamai által jelentett adatok szerint 2019-ben összesen 141 846 illegális határátlépést fedeztek fel az külső határok mentén, ami 4,9%-os csökkenés a 2018-ban felfedezett esetekhez képest, és 92%-os csökkenés a migrációs krízis 2015-ös csúcsához viszonyítva, amikor ez a szám 1,8 millió volt. Az illegális határátlépések száma 2019-ben 2013 óta a legalacsonyabb szintre ért. A számok 2019-ben negyedik éve csökkenő tendenciát mutatnak, és a 2011-eshez voltak hasonlíthatóak.[95] Ritecz 2018-ban a következő megállapítást tette: „Az irreguláris migráció, a „migránsok" 2015 óta közbeszéd tárgya, sőt még napjainkban, 2018 nyarán is a média és a politika egyik meghatározó témája. Pedig gyakorlatilag több mint két éve

---

[91] KŐHALMI L.: A migráció és a kriminalitás néhány összefüggése. Jura, 2016/1. 94–99. o.

[92] HAUTZINGER Z.: A terrorizmus elleni küzdelem idegenjogi eszközei. In: GAÁL Gy. – HAUTZINGER Z. (szerk.): Pécsi Határőr Tudományos Közlemények XVI.: Modernkori veszélyek rendészeti aspektusai. Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoportja, Pécs. 2015. 203. o.; Lásd még: ÉBERHARDT Gábor: Migráció és terrorizmus. Hadtudományi Szemle, 2019/3. 37–59. o.

[93] Risk Analysis for 2018. FRONTEX, Varsó, 2018. 8. o. https://frontex.europa.eu/assets/Publications/Risk_Analysis/Risk_Analysis/Risk_Analysis_for_2018.pdf (2021.10.07.) Idézi: BARTKÓ R.: Az illegális migráció és a terrorizmus kapcsolata az EUROPOL és FRONTEX jelentéseire tekintettel. In: BARTKÓ R. (szerk.): A terrorizmus elleni küzdelem aktuális kérdései a XXI. században. Gondolat Kiadó, Budapest, 2019. 167. o.

[94] Uo. 180. o.

[95] Risk Analysis for 2020. FRONTEX, Varsó, 2020. 22. o. https://euagenda.eu/upload/publications/untitled-301445-ea.pdf (2021.10.07.)

vége a migrációs hullámnak."[96] Magyarországra Éberhardt objektív adatok elemzésével újabb migrációs hullám érkezését prognosztizálja.[97]

A hazai jelent illetően osztom Gál álláspontját: „Magyarországon az illegális tömeges migráció és a terrorizmus két olyan veszélyfaktor, amely szerencsére de facto nincs még jelen a mindennapokban, de fel kell készülnünk rá, és mindent meg kell tenni a megelőzés, a biztonság fokozása érdekében."[98] Resperger szerint egy extrémista terrortámadás Magyarországon főként hazánk nemzetközi szerepvállalása kapcsán fenyeget.[99]

[96] RITECZ Gy.: Az Európába irányuló tömeges irreguláris migráció felfutásának és megszűnésének okai. Hadtudomány, 2018/3–4. 66. o.

[97] ÉBERHARDT G.: Magyarország az újabb tömeges nemzetközi migráció kapujában. Belügyi Szemle, 2021/3. 366. o.

[98] GÁL I. L.: Korrelációs kapcsolat az illegális migráció és a terrorizmus finanszírozásának volumene között. In: GAÁL Gy. – HAUTZINGER Z. (szerk.): Pécsi Határőr Tudományos Közlemények XXI.: A bűnüldözés és a bűnmegelőzés rendészettudományi tényezői. Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoportja, Pécs, 2019. 217. o.

[99] RESPERGER I.: A nemzetbiztonsági szolgálatok tevékenysége – biztonsági kihívások, kockázatok és fenyegetések. In: RESPERGER István (szerk.): Nemzetbiztonsági alapismeretek. Dialóg Campus Kiadó, Budapest, 2018. 86. o.

IV. A MÉDIA ÉS A TERRORIZMUS KAPCSOLATA

1. Elméleti és történeti háttér

A terrorizmus és a média egymástól elválaszthatatlanok. A terroristák a nyilvánosságot megcélzó látványos cselekedetek végrehajtására törekednek.[100] Mindig is a közösség figyelmét igyekeztek megragadni. Már a középkori asszaszinok is törekedtek a köz figyelmének megragadására, Rapoport szerint merényleteikkel a thug-okkal összehasonlítva (akiket három fél érdekelt: merénylő, áldozat, istenség) egy további felet is megcéloztak, a közösséget, amelynek a szimpátiáját figyelemfelkeltő tetteikkel kívánták felkelteni. Célközönségük eléréséhez nem szorultak tömegmédiára, mert merényleteiket feltűnő módon hajtották végre: szakrális helyeken és királyi udvarokban ölték meg prominens áldozataikat, általában ünnepnapokon, mikor sok tanúra számíthattak.[101]

Wilkinson szerint a terroristák médiahasználatának négy fő célja van: elsősorban a propagandájuk közzététele és a félelemkeltés. A második cél a nagyobb, anyagi támogatás érdekében történő mozgósítás a terrorszervezet számára. A harmadik a kormányok és mindazon szervezetek lejáratása, melyeknek kötelességük lett volna megvédeni az állampolgáraikat, a negyedik cél pedig további terrortámadásokra való inspiráció, akár toborzással.[102]

Fordulópontnak tekinthető a média által is közvetített terrorizmus megjelenésében a Népi Front Palesztina Felszabadításáért 1968. július 22-én elkövetett kereskedelmi repülőgép-eltérítése.[103]

Kőhalmi rámutat, hogy a világunkban, amelyben az erőszak egyre hangosabb, csak az a terrorista szervezet képes nagyobb visszhangot kelteni a nyilvánosság figyelméért folyó konkurenciaharcban, amelyik különösen kegyetlen módon támad. A legújabb terrorhullámban fokozódási kényszer van, konkurenciaharc a nyilvánosság figyelméért. Kőhalmi szerint a terrorizmus globalizációja erőszakot felszabadító jelleggel bír, mivel a nemzetközi terrorista csoportok esetében hiányzik az általában fékező hatással bíró, egy

[100] FERWAGNER P. Á. – KOMÁR K. – SZÉLINGER B.: Terrorista szervezetek lexikona: Gavrilo Principtől Oszama bin Ladenig. Maxim Könyvkiadó, Szeged, 2003. 14. o.

[101] RAPOPORT (1984): 664–665. o.

[102] WILKINSON, P.: The Media and Terrorism: A Reassessment. Terrorism and Political Violence, 1997. Vol. 9. No. 2. Idézi: KORINEK (2015): i.m. 19–20. o.

[103] FERWAGNER – KOMÁR – SZÉLINGER: i.m. 14. o.

adott miliőre vagy politikai projektre való szociális visszacsatolás. A vonatkozási csoport hiányában az erőszak generálódik, amely a terroristák vallási, vagy szekuláris motivációjától független.[104]

A jelentősebb létszámú és szervezettebb terrorista csoportokban a médiához, PR-hoz és marketinghez értő vezetők és tagok szerepe legalább olyan fontos, mint akár a műveleti tervezőké, robbantási és fegyverszakértőké, etc. A médiafelelős tagok felmérik és véleményezik az egyes támadások médiafigyelmét. Vizsgálják, hogy azok milyen hatást váltanak ki a közvéleményből. A terrorista csoportok vezetői tisztában vannak azzal, hogy akcióik közvetlen hatásait a médiafigyelem érzelmileg fokozza, ennek köszönhetően a közelmúlt és napjaink terrorista taktikájának egyik fő eleme a minél nagyobb publicitás elérésére való törekvés.[105] Az IS-nek is van médiaosztálya, amelynek specialistái minden nyilatkozatot és propagandaterméket ellenőriznek, és a legmegfelelőbb időben és módszerrel teszik közzé azokat.[106]

Korinek figyelmeztet, hogy a média akaratlanul is a terrorizmus szövetségesévé válik multiplikátor (megsokszorozó) szerepe miatt, ugyanis a terroristáknak ma már nem is szükséges birtokolniuk a tömegtájékoztató eszközt, akcióik úgyis automatikusan felkeltik a tömegtájékoztatás figyelmét, így a törekvésük, hogy minél szélesebb körben tudassák a létüket és céljaikat, sikeres lesz. Korinek – Hankiss kifejezését használva – a média és a terrorizmus kapcsolatát „társadalmi csapdának" nevezi. A demokratikus társadalmak az információhoz jutás korlátozásmentes jogát kívánják meg, de ugyanez közlési csatorna is a terroristák számára. Korinek konklúziója szerint diktatúrában ez könnyen megoldható a média beszabályozásával, de ha nyitott társadalmat kívánunk, akkor a terrorizmust, mint egy átmenetileg megoldhatatlannak látszó kísérőjelenséget, el kell fogadnunk.[107] Margaret Thatcher 1979-től 1990-ig hivatalban lévő angol miniszterelnökre utal, a terrorizmus oxigénjének nevezte a médiát, és azt javasolta, hogy a média ne figyeljen a terrortámadásokra, ne tájékoztasson róluk, mert úgy vélte, így a terrorizmus az oxigénjétől megfosztva elhalna. A média ezt a javaslatot általánosságban elutasította.[108] Camphuijsen és Vissers a terrorizmus és a tömegmédia kapcsolatát

[104] KŐHALMI L.: Gondolatok a vallási indíttatású terrorizmus ürügyén. Belügyi Szemle, 2015/7–8. 53–54. o

[105] BERACZKAI A.: A terrorizmus és a média. Kard és Toll, 2006/2. 102–112. o. Idézi: HORVÁTH (2014): i.m. 54. o.

[106] PRANTNER Z.: Iszlám Állam - A világ legvéresebb terrorszervezete. Pannon-Literatúra Kft., Kisújszállás, 2016. 104. o.

[107] KORINEK (2006): i.m. 451–452. o.

[108] CAMPHUIJSEN, M. – VISSERS, E.: Terrorism and the Mass Media: A symbiotic relationship? Social

„szimbióta” kapcsolatnak nevezi, mely szerintük nem mindig létezett, de a tömegmédia növekedése létrehozta és intenzitásában növelte azt. A szerzők szerint ugyan a média és terrorizmus nem áll teljes függésben, de nagyban profitálhatnak egymásból. Ez a kapcsolat megmagyarázza, miért nem működött Thatcher javaslata. A médiának nem állt érdekében nem tudósítani a támadásokról, mivel azoknak nagy hírértéke van, azokról profitáló tudósítania. Így a média is támaszkodik a terrorizmusra.[109] Moring szerint a média nem teheti meg, hogy nem tudósít a terrorizmusról és az ellene tett válaszlépésekről, mert ez a hírközlés alap-ethoszának mondana ellent. Mai világunkban, amelyben a szóbeszéd valós időben terjed az interneten és mobiltelefonokon keresztül, amúgy is nem kívánatos eredményre vezetne.[110] A média nem teljesen megbízható szövetségese a terroristáknak, mivel a túl sok áldozatot követelő támadások elidegeníthetik a potenciális támogatóikat és szimpatizánsaikat.[111] Horváth szerint a média alkalmas lenne arra, hogy jobban bemutassa a terrorizmus valódi arcát, az erőszakot, a szervezett bűnözéssel való kapcsolatának káros hatásait, ehhez azonban a sajtóetikai normák betartása és a szenzációhajhászat féken tartása szükséges. Több háttérmunkát, az ok-okozati összefüggések megvilágítását, pontos tájékoztatást, és a terrorizmus kevésbé látható következményeinek bemutatására oknyomozási módszerek kiterjesztését szorgalmazza.[112]

2. Az internet hatása a terrorizmus és média kapcsolatára

Az internet (Internetworking System – hálózatok hálózata) katonai kutatásból ered. A szovjet szputnyik 1957-es fellövését követően az USA-ban a „szputnyik-sokkot” ellensúlyozandó, többirányú fejlesztésbe kezdtek. Ezek egyikeként a hadsereg vezetésének megbénításának megakadályozására több vezetési pontot alakítottak ki, melyeket földalatti kábellel kötöttek össze. Később egyre több katonai és civil kutatóintézet és egyetem csatlakozott a hálózatra, mely később szétvált katonaira és

Cosmos, 2012. Vol. 3. No. 1. 14. o.

[109] Uo. 21–22. o

[110] MORING, T.: Terrorism, Media and the State: An Incestuous Spiral. In: HUSBAND, Ch. (szerk.): Social Cohesion, Securitization and Counter-terrorism. Vol. 11. No. 11. University of Helsinki, COLLeGIUM: Studies across Disciplines in the Humanities and Social Sciences, Helsingfors, 2012. 80. o.

[111] FERWAGNER – KOMÁR – SZÉLINGER: i.m. 23. o.

[112] HORVÁTH (2014): i.m. 62. o.

civilre, amely utóbbit 1993-tól lehet szabadon használni.[113]

A számítógépes hálózatokat a 60-as években a hidegháború amerikai reakciójaként fejlesztették ki, majd 1989-ben Tim Berners-Lee létrehozta a világhálót, 1990-ben megírta az első böngészőt is, az pedig fokozatosan általánosan használt rendszerré vált.[114]

A számítástechnika, főleg az internet közvetítésével megjelent, egyre szaporodó, egyre veszélyesebb bűncselekmények valamennyi bűnügyi tudomány számára kihívást jelentenek. A számítógépes környezetben elkövetett bűncselekmények kihívás az anyagi büntetőjog, a büntető eljárásjog és a kriminalisztika számára is.[115] A legfontosabb kibertérből érkező fenyegetéseket Berki a következőképp csoportosítja: kiberbűnözés, kiberkémkedés, hacktivizmus, kiberterrorizmus, kiberhadviselés.[116]

Az internet sok szempontból forradalmasította a terrorizmust.[117] A terroristák fokozott internethasználata óriási minőségi változást hozott a terrorizmus jelenségében, úgy vélem, legalább akkorát, mint a 9/11-es terrortámadás az új típusú terrorizmus[118] elhozatalával.

Tálas 2008-ban arról számol be, hogy 1997-ben még csak 12 „terrorista weboldalt" tartottak számon a szakértők, de 2008-ra az ilyen weboldalak száma már több ezer volt.[119]

Az internet felrúgta a terrorizmus és a média kapcsolatának klasszikus szabályait. A világháló elterjedése óta a terroristák már nem szorulnak a tradicionális tömegkommunikációs eszközökre, immár szűretlen módon juttatják el a világhoz az

---

[113] NAGY Z. A.: A kiber-háború új dimenzió – a veszélyeztett állambiztonság (Stuxnet, DuQu, Flame – a Police malware). In: GAÁL Gy. – HAUTZINGER Z. (szerk.): Pécsi Határőr Tudományos Közlemények XIII: Tanulmányok „A Biztonság Rendészettudományi Dimenziói – Változások És Hatások" Című Tudományos Konferenciáról. Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport, Pécs, 2012. 221. o.

[114] KOUDELA P.: Játékelmélet a kiberbiztonságban. Hadtudomány, 2019/4. 39. o.

[115] NAGY Z. A.: A joghatóság problémája a kiberbűncselekmények nyomozásában. In: HOMOKI-NAGY M. – KARSAI K. – FANTOLY Zs. – JUHÁSZ Zs. – SZOMORA Zs.– GÁL A. (szerk.): Ünnepi Kötet Dr. Nagy Ferenc Egyetemi Tanár 70. Születésnapjára. Szegedi Tudományegyetem Állam- és Jogtudományi Kar, Szeged, 2018. 755. o.

[116] BERKI G.: A kibertér, annak veszélyei és a kibervédelem jelenlegi helyzete Magyarországon. Nemzetbiztonsági Szemle, 2018/3. 8. o.

[117] LIEBERMAN, A. V.: Terrorism, the Internet, and Propaganda: A Deadly Combination. Journal of National Security Law and Policy, 2017. Vol. 9. No. 1. 101. o.

[118] KORINEK (2006): i.m. 450. o

[119] TÁLAS P.: A terrorizmusról hét évvel 9/11 után. Nemzet és Biztonság, 2008/9. 75. o.

edzésükről, kivégzéseikről, akcióikról szóló tartalmakat.[120] A terrorcselekményeiket a közösségi média felületein saját maguk közvetítik élőben, kivégzésekről és további embertelen cselekedeteikről szóló videóik a közösségi médián keresztül milliókhoz jutnak el.[121]

Haig szerint az internet használata azért előnyős a terroristák számára, mert az könnyen elérhető, a szabályok minimálisak, a cenzúra hiányzik, a célközönség óriási lehet, nagyon gyors információáramlást és anonim kommunikációt tesz lehetővé számukra, olcsón biztosít a propagandához sokszínű multimédiás környezetet, és már a hagyományos tömegmédia (televízió, rádió etc.) is egyre gyakrabban alapoz forrásként az internetre. Ezeket az előnyöket a terroristák felismerik és kihasználják.[122] A terrorszervezetek az internetet toborzásra is már régóta használják.[123]

Az internet már az extrémista csoportok propagandájának egyik legfontosabb médiuma. A propaganda terjesztésének egyik célja az új tagok megnyerése, a másik az ideológiájuk vagy annak egyes aspektuaival szembeni szimpátia keltése. Az interneten nem csupán iszlamista propaganda lelhető fel, azt bal- és jobboldali extrémista és más csoportok is intenzíven felhasználják kommunikációs csatornaként.[124] Erőszakos extrémista csoportok visszaélnek az internet sebezhetőségeivel és nyíltságaival, azt felhasználva radikalizációra, toborzásra és a fiatalok felkészítésére. Fiatalok radikalizációjának médiumaként használnak chat szobákat, közösségi háló oldalakat, mint a Facebook, Twitter, YouTube, és online videojáték videókat is. Terrorszervezetek, mint például a Boko Haram, az IS és az Al-Kaida, és más extrémista csoportok stratégiailag felfedezték az internetet a tevékenységeik elősegítésére. Ugyan a nemzetközi közösség és kormányok világszerte erőfeszítéseket tettek az erőszakos extrémista csoportok internettel való visszaélése ellen, terrorista csoportok továbbra is megtalálják a módjait anyagaik online terjesztésére. Apau szerint ezért fontos, hogy a kormányok felismerjék, hogy a fiatalok online radikalizációjának folyamata egy globális

[120] ÖZKAYA, E.: The Use of Social Media for Terrorism. NATO Defence Against Terrorisim Review, 2017. Vol. 9. 8. o.

[121] Uo. 2. o .

[122] HAIG Zs.: Internet terrorizmus. Nemzetvédelmi Egyetemi Közlemények, 2007/2. 84–85. o.

[123] GUADAGNO, R. E. – LANKFORD, Adam – MUSCANELL, Nicole L. – OKDIE, Bradley M. – MCCALLUM, Debra M.: Social Influence in the Online Recruitment of Terrorists and Terrorist Sympathizers: Implications for Social Psychology Research. Revue Internationale de Psychologie Sociale, 2010. Vol. 23. No. 1. 27. o.

[124] NITSCH, H.: Terrorismus und die Nutzung des Internet. In: RÜDIGER, T.-G. – BAYERL, P. S. (szerk.): Cyberkriminologie: Kriminologie für das digitale Zeitalter. Springer VS, Wiesbaden, 2020. 198. o.

és sokoldalú jelenség, melyben a közösségi médiát használják eszközként, erőszakos magatartásra való ösztönzésre. A közösségi média szerepét nem szabad izolálni, hanem más kommunikációs platformok és jelentős társadalmi tényezők (mint politikai, társadalmi, kulturális, gazdasági, és pszichológiai okok) kontextusában kell vizsgálni.[125] Piazza és Guler 2019-ben 6.000 személyt vizsgált 6 arab országból, hogy kiderítsék, hogy azok, akik használják az internetet politikai hírek követésére vagy politikai nézetek kinyilvánítására, nagyobb valószínűséggel támogatják-e az IS-t. Arra jutottak, hogy azok a válaszadók, akik a híreket online követik, jelentősen nagyobb valószínűséggel támogatják az IS-t, mint azok, akik azt a televízióban vagy a nyomtatott sajtóban teszik, továbbá akik online fórumokat használnak politikai nézetek kinyílvánítására, nagyobb valószínűséggel fejezik ki a támogatásukat az IS felé. Az online politikai diszkussziókban résztvevők nagyobb valószínűséggel támogatják az IS-t, mint azok, akik hagyományos politikai tevékenységet folytatnak, bár kevésbé, mint azok, akik pörlekedő politikai magatartást tanúsítanak, mint a politikai tüntetésen való részvétel.[126]

3. Terroristák a közösségi médián

Korunk terroristáinak potens fegyverévé vált a közösségi média.[127] „A közösségi média eszközei alatt (…) azokat az eszközöket értjük, amelyen a tartalmat a felhasználók állítják elő, osztják meg egymás közt, amihez a felületet egy adott szolgáltató biztosítja. Ezen tartalom lehet írott, képi, videó, zene formátum. A közösségi média eszközei ez által a közösségi oldalak, kép- és videó megosztó oldalak, illetve a blogok, mikroblogok."[128] Példa a Facebook, Twitter, Instagram, YouTube etc.
A közösségi média felületei könnyen kezelhetőek, megbízhatóak és ingyenesek, ráadásul pont a terroristák célközönsége körében a legnépszerűbbek. Általuk a terroristák őket meg tudják szólítani, kifejezetten a fiatalokat, feléjük kinyúlva, szemben

[125] APAU, R.: Youth And Violent Extremism Online: Countering Terrorists Exploitation And Use Of The Internet. African Journal on Terrorism, 2018. Vol.7. No. 1. 22. o.

[126] PIAZZA, J. A. – GULER, A.: The Online Caliphate: Internet Usage and ISIS Support in the Arab World, Terrorism and Political Violence, 2019. 1. o.

[127] KASZNÁR A.: Terroristák a közösségi hálón. In: LEZSÁK, S. (szerk.): Túlélési ösztön: Írások a Magyar Hírlapban megjelent Nemzeti Fórumos szerzőktől 2015-2021. Antológia Kiadó és Nyomda Kft., Lakitelek, 2021. 49–51. o.

[128] BÁNYÁSZ P. – ORBÓK Á.: A NATO kibervédelmi politikája és kritikus infrastruktúra védelme a közösségi média tükrében. Hadtudomány, 2013/1. elektr. sz. 196. o.

a régebbi típusú terrorista weboldalakkal, amik esetében a terroristáknak kellett várnia a látogatókra, hogy azok keressék fel őket. A fájlok és videók megosztása, feltöltése vagy letöltése már nem igényel számítógéphez való hozzáférést, és ahhoz nincs szükség technikában jártas tagokra.

A közösségi médián keresztül a terroristák a mainstream médiát is képesek táplálni. Korunk tudósítói és újságírói nagymértékben támaszkodnak a közösségi médiára, mint információforrásra. Weimann szerint a közösségi média vált a terrorizmus és az ellene való harc új csataterévé.[129] A közösségi médiát a terroristák Özkaya szerint a következő tevékenységekre használják: propaganda terjesztése, toborzás, kommunikáció, figyelem megragadása.[130]

A terroristák Bányász szerint az alábbi területeken használhatják a közösségi médiát, ahogy többségüket az elmúlt években használták is: információgyűjtés, social engineering, kapcsolattartás, propaganda, új tagok toborzása, támogatók szerzése, pszichológiai és információs hadviselés, kibertámadás. Jelenleg még nincs meg a humán és technikai képességük létfontosságú rendszerelem ellen elkövetett kibertámadásra, azonban a dark weben vásárolhatnak ilyen szolgáltatást.[131]

2016-ra az IS már a Facebookon és a Twitteren kívül a Youtube-on és az Instagramon is megtalálható volt.[132] Az IS, a Hamasz, a Hezbollah, és az Al-Nuszra Front (szíriai terrorszervezet, az al-Kaidához kötődik) és az Arab-félsziget al-Kaidája (továbbiakban AQAP) is mind megtalálhatók a Twitteren, az utóbbi két hivatalos felhasználói fiókkal is. Az AQAP a Twitteren vállalta magára a Charlie Hebdo magazin ellen elkövetett párizsi merényletet. Az IS számos kivégzésről szóló videót, például egy elfogott jordániai pilóta élve elégetését is osztott meg a Twitteren.[133]

Mihály a terrorista motivációkat és a közösségi médiaplatformoknak ezek érvényesítésében játszott szerepét a következőképp foglalja össze:

A félelemkeltés, elrettentés esetében a szociális médiaplatformoknak a live (élő) kivégzések (YouTube-on, Facebookon) elrettentő képek, videók tekintetében van

---

[129] WEIMANN, G.: Social Media's Appeal to Terrorists. Insite Blog on Terrorism & Extremism. (2014, October 3).
https://news.siteintelgroup.com/blog/index.php/entry/295-social-media's-appeal-to-terrorists (2021.06.14.)

[130] ÖZKAYA: i.m. 49–53. o.

[131] BÁNYÁSZ P.: Kiberbűnözés és közösségi média. Nemzetbiztonsági Szemle, 2017/4. 71. o.

[132] PRANTNER Zoltán: Iszlám Állam - A világ legvéresebb terrorszervezete. Pannon-Literatúra Kft., Kisújszállás, 2016. 104. o.

[133] POE, Ted: Time to silence terrorists on social media. CNN. (2015, February 26). http://edition.cnn.com/2015/02/25/opinion/poe-terrorism-social-media/ (2021.12.17.)

jelentősége. A propaganda terjesztésénél, ideológia ismertetésénél a tájékoztató videók közzétételének, lelkesítő beszédek tartásának (YouTube, egyéb videómegosztó portálok), szimbolumok, jelképek használatában. A toborzásnál a fiatalokat célozzák meg, elsősorban YouTube, Twitter használatával. A kapcsolattartás, szervezés, merényletek koordinálása esetében WhatsApp, Telegram, Facebook Messenger valamint egyéb üzenetküldésre alkalmas applikációkat használnak. Politikai nyomásgyakorláshoz céljaik elérése érdekében bármely előbb említett platformon megjelenő fenyegető tartalmat tesznek közzé.[134] Az előbbi kategorizáláshoz hozzáadható még az adománygyűjtés a különféle felületeken.

Horváth a 2013-as Boston maratoni robbantásos merénylet médiareprezentációjával kapcsolatban a közösségi média szerepét hangsúlyozza. Ennek felületein a felhasználók a robbantás után szinte rögtön, valós időben osztották meg az általuk ismert információkat, saját képeiket és videóikat. Még a gyors reagálású online híroldalak is csak órákkal később közölték a közösségi médiában már megjelent információkat, az „amatőr" hírközlés sokkal gyorsabb volt a rangos hírügynökségeknél is. A közösségi média „vadászai" a gyanúsítottak felhasználói fiókjait gyorsan átfürkészve, jó minőségű képeket és pontos információkat tártak fel az elkövető testvérpárról, míg a TV adásaiban ezek csak órákkal később váltották fel az elmosódott, rossz minőségű képeket. Horváth továbbá a közösségi médiában megfigyelhető komoly kockázatot jelentő, magánszemélyek által végzett boszorkányüldözésre emlékeztető, jelenségre figyelmeztet, az ún. „csináld magad antiterrorizmusra". A merénylet után a közösségi oldalak felhasználói a közösségi médián elkezdték a tetteseket kutatni, a keresés élén a 4chan fórummal, ahol két lehetséges elkövetőt meg is neveztek. A fórum felhasználói nem foglakoznak személyiségi jogokkal, már több embert kergettek öngyilkosságba zaklatással. A fórum egyik gyanúsítottja rendőri védelmet kért, a másik már a robbantások előtt eltűnt, már korábban meghalt. Így annak ellenére, hogy a hatóságok számos, a munkájukat segítő információhoz jutottak a hajsza alatt, ezek az ellenőrizhetetlen, nagy hírveréssel járó tájékoztatók a nyomozást ténylegesen akadályozták.[135]

---

[134] MIHÁLY L. D.: Az Európai Unió válasza az új globális kihívásokra, avagy a médiamegosztóplatform-szolgáltatások terrorista tartalmaival szembeni fellépés jogi eszköztára. In: TAMÁS Cs. G. (szerk.): Magyarország és a közép-európai térség az Európai Unióban: Díjnyertes pályázatok 2020. Országgyűlés Hivatala, Budapest, 2021. 120–121. o.

[135] BÁNYÁSZ P.: A közösségi média szerepe a települések életében, kiemelten a rendkívüli események kezelésében. Településföldrajzi Tanulmányok, 2013/2. 132–145. o. Idézi: HORVÁTH (2014): i.m. 58. o.

4. A jövő – terror deep fake használatával?

Clarke szerint ugyan a mesterséges intelligencia és a gépi tanulás nem állami szereplők számára nehezebben megközelíthető, a dezinformáció és a „deep fake-ek" új és összetett kihívásokat állítanak a terrorizmus elleni harc szereplői elé.[136] A deep fake kifejezés a „Deep Learning" és „Fake" szavak kombinációjából[137] 2017-ben jelent meg, mesterséges intelligencia (MI) technológiákkal generált realisztikus fotó, audió, videó és más hamistványok leírására.[138] Ez a technika felhasználható a célszemély arcképeinek vagy arcmozgásainak egy forrás-személyről készült videóra való ráhelyezésére, abból a célból, hogy olyan videó jöjjön létre, melyben a célszemély úgy viselkedik, ahogy a forrás-személy. A létrejött hamisítvány gyakran jóformán megkülönböztethetetlen az eredetitől.[139] Ezen hamisítványok ártó szándékkal való használatának csak az emberi fantázia szab határt.

Caldwell et al. a mesterséges intelligencia és az ahhoz fűződő technológiák bűncselekmények elkövetésében való lehetséges alkalmazásait azonosították, és osztályozták őket a fenyegetési szintjük alapján.[140] Magas fenyegetési szintet képvisel az audio/videó megszemélyesítés (deep fake), vezető nélküli járművek fegyverként való használata, az áldozatra szabott phishing, MI által irányított rendszerek bomlasztása, nagyléptékű zsarolás, MI által írt álhírek.[141]

Fennáll a lehetősége a deep fake technológia terroristák általi használatának.

---

[136] CLARKE, C. P.: Trends in Terrorism: What's On the Horizon in 2020. Foreign Policy Research Institute. (2020, January 2).
https://www.fpri.org/article/2020/01/trends-in-terrorism-whats-on-the-horizon-in-2020/ (2021.07.15.)

[137] HAN, Y.: Deepfakes: A Terror in the era of AI? NortonLifeLock. (2020, May 11). https://www.nortonlifelock.com/blogs/research-group/deepfakes-terror-era-ai (2021.07.19.)

[138] Deep Fakes and National Security. https://fas.org/sgp/crs/natsec/IF11333.pdf (2021.07.19.)

[139] HAN: i.m.

[140] CALDWELL, M. – ANDREWS, J. T. A. – TANAY, T. – GRIFFIN, L. D.: AI-enabled future crime. Crime Science, 2020. Vol. 9. No. 1. 1. o.

[141] Uo. 6–9. o.

V. A TERRORISTÁK INTERNETHASZNÁLATÁNAK ALAPVETÉSEI

1. Mire használják a terroristák az internetet, azaz mit értek terroristák internethasználata alatt?

Mielőtt tisztázom, jelen dolgozatban mit értek terroristák internethasználata alatt, bemutatom, a szakértők szerint a terroristák mire használják az internetet.
A terroristák kezében a számítástechnikai eszközök és az internet új „fegyverként" jelent meg, akik fel- és kihasználják a modern technika lehetőségeit.[142] Az internethez fűződő technológiák fejlődésével és egyre szélesebb körű elterjedésével, idővel a terroristák internethasználata változott, kiszélesedett, fejlődött, eltolódott az egyes tevékenyégeik fontossága, hangsúlyossága.
Következzen néhány csoportosítás:
Furnell és Warren 1999-es tanulmánya szerint a terroristák négy tevékenység végzésére használják a világhálót: 1. Propagandára és publicitásra. 2. Adománygyűjtésre. 3. Információ elhintésére. 4. Biztonságos kommunikációra.[143]
Cohen 2002-ben öt tevékenységet sorol fel: 1. Tervezés. 2. Finanszírozás. 3. Koordinálás és műveletek. 4. Politikai akció. (A média figyelmének felkeltése céljából.) 5. Propaganda.[144]
Ugyan Thomas 2003-ban már sokkal több tevékenységet sorol, de kategorizálása kevésbé letisztult: 1. Profilalkotás: Az internefelhasználók demográfiája lehetővé teszi a terroristáknak a szimpatizáns felhasználók megcélzását, és hogy tőlük adományokat kérjenek, ha megtalálják a megfelelő „profilt". Az online újságokban és folyóiratokban kulcsszavak keresésével a terroristák összeállíthatnak egy profilt az ellenük kifejlesztett ellenintézkédesekből, vagy a rendszer sebezhetőségeiről. 2. Propaganda. Az internet olyan mértékben nem kontrollálható, cenzúrázható, mint az újságok vagy a TV, az a

[142] NAGY Z. A.: Tradicionális bűncselekmények számítógépes hálózatokon. JURA, 2007/1. 127. o.

[143] FURNELL, S. – WARREN, M.: Computer Hacking and Cyber Terrorism: The Real Threats in the New Millennium. Computers and Security, 1999. Vol. 18. No. 1. 30–31. o. Idézi: CONWAY, M.: Terrorist 'Use' Of The Internet And Fighting Back. Information & Security: An International Journal, 2006. Vol. 19. 11. o.

[144] COHEN, F.: Terrorism and Cyberspace. Network Security, 2002. Vol. 5. 18–19. o. Idézi: CONWAY (2006): i.m. 11. o.

terroristák rádió és TV állomásaként, vagy nemzetközi hírlapjaként szolgálhat. 3. Anonim és titkos kommunikáció: Az internet felhasználható anonim módon, a személyazonosságot elrejtve. Olyan internetes eszközöket érhetnek el a terroristák, melyekkel anonimizálhatják magukat, és elrejthetik személyazonosságukat. Már 2003-ban online titkosítási szolgáltatások (encryption services) titkosítási kulcsokat (encryption keys) ajánlottak szolgáltatásokhoz, melyeket nagyon nehéz feltörni. A spammimic.com weboldal például szöveget „spam-ben" (kéretlen tömeges kereskedelmi e-mailben) elrejteni képes eszközöket kínált. 4. „Kiberfélelem" generálása: Egy kibertámadás potenciális hatásai (utasszállító repülőgépek lezuhanása, kritikus infrastruktúra tönkretétele, tőzsdepiac tönkretétele etc.) „kiberfélelmet" generálnak. Egy személy vagy szervezet online nagyobbnak és fenyegetőbbnek is tűnhet, mint a valóságban. A világhálón terjeszthető dezinformáció, fenyegető üzenetek, és a támadásokról készült felvételek. 5. Finanszírozás. 6. Irányítás és felügyelet: (command and control): Az interneten az irányítást és felügyeletet nem hátráltatja a földrajzi távolság és a kifinomult kommunikációs eszközök hiánya. Támadások koordinálásához és megtervezéséhez szükséges eszközökhöz már az átlag állampolgár, a kormányellenes tüntető és a terrorista is hozzáfér. 7. Toborzás. 8. Információ gyűjtése célpontokról. Például a Muslim Hackers Club weboldalalán olyan amerikai oldalakra vezető linkek szerepeltek, melyek szenzitív információt fedtek fel, mint az Amerikai Titkosszolgálat (US Secret Service) kódnevei és rádiófrekvenciái. 9. A tervezés kockázatainak csökkentése: Az internet távolságot helyez a támadást tervezők és a célpontok közé. 10. Információ ellopására vagy adat manipulálása. Ez akkor a legveszélyesebb, ha fizikai támadással kombinálják, például kritikus infrastruktúra ellen. 11. Rejtett üzenetek küldése: A szteganográfia, melybe az üzenetek grafikus fájlokban történő elrejtése is tartozik, elterjedt művészet a bűnözők és terroristák között. Az interneten titkosító szoftverek is beszerezhetőek. 12. Az internet lehetővé teszi kevés anyagi forrással rendelkező csoportoknak fejlett országokban hatalmas propagandagépezetek működtetését. 13. Cégek bomlasztása. 14. Azzal cselekedetekre mobilizálható csoport vagy diaszpóra, és hackerek is. 15. Visszaélés a jogi normákkal: A legkevesebb, hogy ignorálják a jogi előírásokat online, de akár magát az internetet is használják bűncselekmények elkövetésére, pl. hackeléssel és vírusok küldésével, miközben a jogszabályok védik őket a jogtalan megfigyeléstől. 16. Figyelem elterelése egy valódi támadásról.[145]

[145] THOMAS, T. L.: Al Qaeda and the Internet: The Danger of "Cyberplanning." Parameters, 2003. Vol. 33. No. 1. 112–122. o. Idézi: CONWAY (2006): i.m. 11. o.

Weimann 2004-es felosztásában: 1. Pszichológiai hadviselés. 2. Publicitás és propaganda. 3. Adatbányászat. 4. Adománygyűjtés. 5. Toborzás és mobilizáció. 6. Kapcsolattartás. 7. Információ megosztása. 8.Tervezés és koordináció.[146] Conway 2006-os tanulmánya szerint a terroristák internethasználata öt fő tevékenységet foglal magában: 1. Információ-szolgáltatást (information provision), mely a publicitást, a propagandát és a pszichológiai hadviselést foglalja magában. 2. Finanszírozást. 3. Networking-et. 4. Toborzást. 5. Információgyűjtést.[147] Maras szerint 2016-ban a terroristák az internetet felhasználják: 1. Propagandájuk terjesztésére. 2. Toborzásra. 3. Pénzszerzésre. 4. Oktatásra, és műveletek tervezésére.[148] Fishman 2019-es felosztásában: 1. Tartalom hosztolására (content hosting). 2. Közönség-fejlesztésre. 3. Brand-kontrollra. 4. Biztonságos kommunikációra. 5. Közösség fenntartására. 6. Finanszírozásra. 7. Információ gyűjtésére és gondozására.[149] Tartalom hosztolása: A terrorszervezetek a propaganda széles skáláját termelik, képek, videók, audiofájlok formájában. A tárolók az internetre kerültek, fájlmegosztó oldalakra. Bizonyos terrorszervezetek, mint az IS, használnak felhőszolgáltatásokat is média tárolására és video-streamelő szolgáltatásokat propaganda terjesztésére. Másoknak, mint a Hamász-nak és az Atomwaffen Division-nek, saját weboldala van. Közönség fejlesztés: a terroristáknak több okból is szüksége van közönségre, erről korábban már esett szó. Brand-kontroll: A modern terrorszervezetek használtak és használnak web fórumokat (pl.: al-Hesbah), hivatalos weboldalakat (pl.: Atomwaffen, Hamász és Hezbollah), Twitter-t, és például Telegram csatornákat, hogy a célközönségük felé jelezhessék a közétett anyagaik autentikus voltát. A brand-kontroll következetességet kíván, ami a tech platformokra fontos szerepet ró a terrorszervezetek ilyen tevékenysége elleni küzdelemben. A közösség fenntartására: Az online üzenetküldő alkalmazások és közösségi média platformok zárt csoportjaival és a brand-del ellátott online fórumokkal elválaszthatóak a csoport tagjai a külsősöktől. Finanszírozás: A dititális térben a terroristák használhatnak tradícionális pénzügyi küldőket, mint a Western Union, elektronikus bankátutalásokat és online fizetési rendszereket (pl.: Paypal vagy Venmo),

[146] WEIMANN, G.: www.terror.net: How Modern Terrorism Uses The Internet. Special Report. United States Institute Of Peace, Washington D.C., 2004. 5–10. o.
https://www.usip.org/sites/default/files/sr116.pdf (2021.07.13.)

[147] CONWAY (2006): i.m. 9–30. o.

[148] MARAS, M. H.: A terrorizmus elmélete és gyakorlata. Antall József Tudásközpont, Budapest, 2016. 244–245. o.

[149] FISHMAN, B.: Crossroads: Counter-terrorism and the Internet. Texas National Security Review, 2019. Vol. 2. No. 2. 84–86. o.

adománygyűjtéseket rendezhetnek P2P transzfereket olyan platfromokkal, mint a GoFundMe vagy Messenger Payments.[150]

Látható, hogy amikor az előbbi szerzők a terroristák internethasználatáról beszélnek, abba a körbe nem veszik bele a kibertámadást, azaz a kiberterrorizmust. Magam is ilyen értelemben használom a terroristák internethasználata kifejezést.

Hasznosnak tartom Bőczné Neparáczki kategóriáit, aki az információtechnológia terrorista célú felhasználásának két csoportját különíti el: „Az információtechnológia „hard" típusú alkalmazásakor a terroristák kifejezetten kibertámadást hajtanak végre (például kritikus infrastruktúrákat irányító információs rendszert bénítanak meg, tesznek működésképtelenné azzal, hogy terheléses támadást indítanak, férgeket, vírusokat küldenek stb.). Másrészről az információtechnológia „soft" típusú alkalmazása esetén a terroristák az információs rendszer segítségével tartják a kapcsolatot (például az interneten keresztül kommunikálnak egymással), saját weboldalt működtetnek és azt médiaként használják (például a célpont ellen végrehajtott támadás felvételét megosztják, vagy közleményeikben üzennek a világ számára), új terroristacsoport-tagokat vagy támogatókat toboroznak, terjesztik propagandájukat, az internet segítségével szereznek adatokat a lehetséges célpontról (például épület alaprajzokat), a terroristák kiképzéséhez szükséges online kiadványokat tesznek közzé, vagy anyagi forrás szerzésére is igénybe veszik az internetet."[151]

Bőczné Neparáczki szerint szerint a kiberterrorizmus fogalma – hasonlóan a kiberbűnözéshez – gyűjtőfogalom: „A kiberterrorizmus szűkebb értelemben informatikai környezettől függő bűnözési forma, az ún. tisztán kiberbűncselekmény terrorista célú elkövetését jelenti, amely az információtechnológia hard típusú felhasználásával valósul meg. A kiberterrorizmus tágabb értelemben magában foglalja az informatikai környezet által elősegített terrorista cselekményeket, azaz az információtechnológia soft típusú terrorista célú felhasználásának büntetendő formáit. Ezek a terrorista cselekmények az információtechnológia felhasználása nélkül is bűncselekményt valósítanak meg, de elkövetésüket segítheti, megkönnyítheti az információs rendszer felhasználása."[152]

Ahogy fentebb említettem, jelen dolgozatban a „terroristák internethasználata" alatt – Bőczné Neparáczki kategóriáit kölcsönvéve – az információtechnológia terrorista célú

[150] Uo. 84–86. o.

[151] BŐCZNÉ NEPARÁCZKI A. V.: A kiberterrorizmus büntető anyagi jogi megítélése. Ügyészek Lapja, 2020/1. 76–77. o.

[152] Uo. 79–80. o.

felhasználásának „soft” típusú alkalmazását[153] értem. Ezt nevezem terroristák internethasználatának. A kiberterrorizmus kifejezést magam „szűk értelemben”[154] használom, az alatt a terroristák által elkövetett kibertámadást értem, mely a jelen dolgozatnak nem tárgya. Az egyéb internetes tevékenységeikre használom a terroristák internethasználata kifejezést.

A kiberterrorizmus kérdését illetően Dornfeld nézeteivel értek egyet: „A kiberterrorizmusról szóló diskurzus kapcsán sokszor kevéssé kap helyet a terroristák egyéb internetes tevékenységének vizsgálata, amely talán a legkomolyabb negatív hozadéka a kiberterrorizmus veszélyessége túlértékelésének. Ezek jóval kevésbé ijesztő tevékenységek, mint például egy erőmű felrobbantása, de véleményem szerint jóval veszélyesebbek. Az elmúlt évek nyugat-európai terrortámadásaiban jelentős szerepet játszott a terroristák internetes kommunikációja, az aktív dzsihadista propaganda és persze azok a pénzügyi támogatások, amelyeket a terrorszervezetek az internet segítségével szereztek meg. Véleményem szerint ez egy olyan téma, amivel szemben a jövőben még keményebben kell fellépnie a nemzetközi közösségnek.”[155] Ugyanakkor nem vetem el annak a lehetőségét, hogy a jövőben a helyzet változhat, és az információtechnológia Bőczné Neparáczki felosztása szerinti „hard” típusú alkalmazása[156] a jelenleginél sokkal nagyobb veszélyt képvisel majd.

2. Extrémisták által gyakran használt platformok és applikációk

A Polarization and Extremism Research Innovation Lab szerint az extrémisták (továbbá terroristák) által gyakran használt platformok és applikációk a következők:

Toxikus online közösségek: 4Chan, Gab, 8Kun, KiwiFarms, incels.co.

Extrémisták által használt mainstream oldalak: Reddit, Discord, iFunny, Twitch, Tik Tok, YouTube, Facebook, Twitter, Instagram, Teamspeak (Steam, Xbox, vagy PS4-en keresztül), VKontake (VK).

Korlátozottan moderált alkalmazások és oldalak: Minds, BitChute, Riot Chat, Rocket

[153] Uo. 76–77. o.

[154] Uo. 79–80. o.

[155] DORNFELD L.: Kiberterrorizmus – a jövő terrorizmusa? In: MEZEI K. (szerk.): A bűnügyi tudományok és az informatika. Pécsi Tudományegyetem Állam- és Jogtudományi Kar, MTA Társadalomtudományi Kutatóközpont, Budapest-Pécs, 2019. 61. o.

[156] BŐCZNÉ NEPARÁCZKI: i.m. 76–77. o.

Chat, Parler, MeWe, DLive, Rumble.

Ezek az oldalak és applikációk a különböző fokú tartalom-moderálást alkalmaznak, mely gyakran a felhasználók jelentésére támaszkodik. Extrémisták gyakran élnek vissza az ilyen bizalommal, tartalmaik terjesztéséhez és toborzáshoz.

Fokozottan titkosított és anonimizáló alkalmazások és szolgáltatások: A következő alkalmazások titkosítást és más magánéletet óvó technológiákat alkalmaznak: Telegram, Signal, Wickr, WIRE, Jitsi Meet, PIA VPN, Nord VPN, Proton VPN, Protonmail, Unseen.is Email, Tutanota Email, Tor/Onion böngészők, Brave böngésző, Threema, Keybase.[157]

Ezen felületek nyomonkövetése fontos a terroristák internetes aktivitásának ismerete szempontjából.

[157] Building Resilience & Confronting Risk In The Covid-19 Era: A Parents & Caregivers Guide To Online Radicalization. PERIL & Southern Poverty Law Center. 17. o. https://www.splcenter.org/sites/default/files/splc_peril_covid_parents_guide_jan_2021_1.pdf (2021.10.05.)

VI. TERRORISTÁK A DARK WEBEN

1. Az internet rétegei: a felszíni web, a deep web, a dark web

A terroristák dark webes tevékenységeinek megértéséhez szükséges az internet rétegeinek, és az ahhoz kötődő fontosabb fogalmak tisztázása, továbbá a dark web tartalmainak rövid bemutatása is.

Az internet mérete az utóbbi évtizedekben hatalmasat nőtt. 1991-ben még mindössze egy (info.cern.ch), 2014-re 1 milliárd, mára több mint 1,5 milliárd weboldal található a world wide web-en, melyből kevesebb, mint 200 millió aktív.[158] Az internet rétegekből áll. A felső réteg a keresőmotorok által könnyen hozzáférhető felszíni web (surface web). Az alsóbb rétegek méretét illetően nincs egyetértés, de annyi biztos, hogy hatalmasak. A deep web (mély web), azaz a nem indexelt weboldalak száma egyes becslések szerint 400-500-szor nagyobb a felszíni web indexelt, kereshető weboldalainál,[159] más szerzők szerint az internet 90%-a a deep web.[160] A dark web (nevezik még dark netnek, magyarul sötét webnek vagy sötét netnek, a továbbiakban dark web) a deep web része, melynek tartalmai szándékosan rejtettek. Hozzáféréséhez speciális szoftverekre van szükség, mint a Tor. A dark web legális és illegális tevékenységek elfedésére egyaránt használható, de anonimitását nem csak bűnözők, hanem a bűnüldöző szervek, a katonaság és a hírszerző szolgálatok is kihasználhatják.[161] A dark weben böngészni önmagában még nem illegális (könnyen azzá válhat),[162] annak legális oldala is van. Található például sakk klub, és a „Tor Facebookja," a BlackBook (http://blkbookppexymrxs.onion/) közösségi háló is.[163] The New York

[158] Total number of Websites. Internet Live Stats. https://www.internetlivestats.com./total-number-of-websites/ (2022.01.18.)

[159] RUDESILL, D. S. – CAVERLEE, J. – SUI, D.: The Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box. Woodrow Wilson International Center for Scholars, Washington, DC, 2015. 4. o. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2676615 (2021.07.31.)

[160] RATHOD, D.: Darknet Forensics. International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), 2017. Vol. 6. No. 4. 78. o.

[161] FINKLEA, K.: Dark Web. Congressional Research Service, Washington DC, 2017. 1. o. https://www.fas.org/sgp/crs/misc/R44101.pdf (2021.08.02.)

[162] Kiberbűnözés és a virtuális tér veszélyei – interjú az Internet Világnapja alkalmából. Birosag.hu. (2018. május 18.) https://birosag.hu/hirek/kategoria/magazin/kiberbunozes-es-virtualis-ter-veszelyei-interju-az-internet-vilagnapja (2021.08.02.)

[163] GUCCIONE, D.: What is the dark web? How to access it and what you'll find. CSO Online. (2021,

Times volt az első fő digitális médiaorgánum, ami megnyitotta az oldalát a dark weben.[164]

A Tor böngészőt sokan online magánéletük megóvására használják: katonaság, rendőrség, újságírók, ún. whistleblower-ek[165] is (pl. Edward Snowden, Julian Assange). A Tor anonimitása miatt a dark web bűnözői aktivitás melegágya is, többek között kábítószerrel kapcsolatos bűnözésnek, gyermekpornográfiának, fegyverkereskedelemnek, és bérgyilkosok felbérlésének is (Több csoport kínál ilyen szolgáltatást, de létezésük nem bizonyított.[166]).[167] A terroristák más felületeken végzett tevékenységeiket a dark web felé fordulva egészítik ki, ugyanis annak titkosításokkal rendkívül erősen védett platformjain a felhasználók IP címeit a bűnüldöző szervek nehezen tudják lekövetni, ezért nagyfokú anonimitást biztosít.[168] A dark webet övezik legendák, mint a „red room-ok" (vörös szobák), melyekben embereket és állatokat kínoznak, erőszakolnak vagy ölnek meg élő közönség előtt, pénzért,[169] melyek valószínűleg csak városi legendák.[170] Mivel a Tor a tartalomszűröket is kikerüli, így használatával akár Kínából is elérhető – többek közt – az ott feketelistára tett YouTube is.[171]

July 1). https://www.csoonline.com/article/3249765/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html (2021.08.09.)

[164] PALIY, G.: What Is The Dark Web? Business 2 Community. (2017, November 27). https://www.business2community.com/cybersecurity/what-is-the-dark-web-01961365 (2021.08.09.)

[165] „Szó szerinti jelentése „sípfújó", és olyan személyekre használják, akik arra hívják fel a figyelmet, ha egy intézmény vagy szervezet törvénytelenül működik, vagy akár csak rosszul irányítják. A whistleblowerek tipikusan belülről jönnek, bizalmas értesüléseik munkájukból vagy a szervezetben betöltött más szerepükből következően vannak – léteznek azonban kívülről jövő whistleblowerek is, akik hosszas adatgyűjtés, nyomozás után jutnak a leleplező adatokhoz. A whistlerblowereket sok helyen a törvény is védi." Forrás: Aki megfújja a sípot. Nyelv és Tudomány. (2013. augusztus 21.) https://www.nyest.hu/hirek/aki-megfujja-a-sipot (2021.08.02.)

[166] MOORE, D. – RID, T.: Cryptopolitik and the Darknet. Survival*:* Global Politics and Strategy, 2016. Vol. 58. No. 1. 24. o.

[167] Tor And The Deep Web: Everything You Secretly Wanted To Know. https://www.whoishostingthis.com/blog/2017/03/07/tor-deep-web/ (2020.03.28.)

[168] ÖZKAYA: i.m. 53–59. o.

[169] What is the Deep Web? The Definitive Guide [2020]. https://www.thedarkweblinks.com/what-is-the-deep-web/ (2021.08.02.)

[170] HARPER, I.: Dark Web Red Rooms: Urban Legend or Worst Content on the Deep Web? The Dark Web Journal. https://darkwebjournal.com/dark-web-red-rooms/ (2021.08.02.)

[171] DEVECSAI J.: Kábítószerek és bérgyilkosok a netről. DigitalHungary. (2017. október 11.). https://www.digitalhungary.hu/konferenciak/evolution/Kabitoszerek-es-bergyilkosok-a-netrol/5056/

1994-ben Ellsworth alkotta meg az „invisible web” (láthatatlan web) kifejezést[172], ezzel utalva az információra, ami láthatatlan volt az abban az időben használt konvencionális keresőmotorok számára. 2001-ben Bergman alkotta meg a „deep web” kifejezést a “The Deep Web: Surfacing the Hidden Value”[173] című tanulmányában. Deep web meghatározása nem különbözött Ellsworth invisible web-jétől, de kerülte azt a kifejezést, mert az ő fő célja a deep web oldalak azonosítására és azok keresésre szolgáló automatizált eszközök felfedezése volt, hogy ezek a láthatatlan oldalak láthatóvá váljanak a felszíni weben, és fel akarta mérni a deep web méretét és jellemezni a tartalmait. Mivel Bergman tanulmánya volt az első átfogó invisible/deep web kutatás, és azt web kutatók közössége felkapta, a deep web kifejezés győzedelmeskedett az invisible web felett, a web nem indexelt forrásaira való utalásban.[174] Dilipraj a „deep webet” a következőképpen definiálja: „Az információs tartalom az interneten (weboldalak, dokumentumok, fájlok, képek etc.) amik: hozzáférhetetlenek a konvencionális keresőmotorok általi közvetlen kereséseken keresztül; amikhez csak célzott keresésekkel vagy kulcsszavakkal lehet hozzáférni; amelyek nem indexeltek vagy nem indexelhetőek a konvencionális keresőmotorok által; amelyek biztonsági mechanizmusok által védettek, mint a login ID-k, jelszavak, tagsági regisztrációk és díjak. Röviden: „deep webnek” vagy „invisible webnek” vagy „hidden webnek” nevezzük az információs tartalmat az interneten, amely nem hozzáférhető közvetlenül konvencionális keresőmotorokon keresztül, hanem egy célzott megközelítést igényel.”[175]

(2021.08.02.)

[172] ELLSWORTH, J. H.: Education on the Internet. Sams Publishing, Indianapolis, 1994. 1–591. o.

[173] BERGMAN, M. K.: The Deep Web: Surfacing Hidden Value. The Journal of Electronic Publishing, 2001. Vol. 7. No. 1.

[174] DILIPRAJ, E.: Terror In The Deep And Dark Web. Air Power Journal, 2014. Vol. 9. No. 3. 126. o.

[175] „The information content on the internet (web pages, documents, files, images, etc) which are: inaccessible through direct queries in the conventional search engines; l which can be accessed only through targeted queries or keywords; which are not indexed or which are unable to be indexed by the conventional search engines; which are protected by security mechanisms like login IDs, passwords, membership registrations and fees. In short, the information content on the internet which cannot be accessed directly through conventional search engines but requires a targeted approach is called the ‘deep web’ or ‘invisible web’ or ‘hidden web’.” Saját fordítás. Uo. 126–127. o.

2. A Tor böngésző

A világot az internet egy globális entitássá változtatta, mely ára a magánélet lett. Minden internetkliensnek van egy egyéni azonosítója, Internet Protocol-cím (IP cím) formájában, ami lefordítható a lokációjára a helyi internetszolgáltató (Internet service provider, ISP) segítségével. A magánélet hiánya vezetett az anomin kommunikációs hálózatok (anonymous communication networks, ACN-ek) használatához, melyek számos technikai megoldással rejtik el a kliens IP címét. A Tor mellett közéjük tartozik plédául a Java anonymous proxy (JAP), Hotspot Shield és UltraSurf etc. A Tor az egyik legnépszerűbb.[176] Kedvelt még az I2P és a Freenet. Ezeknek a hálózatoknak az architektúrája miatt méretük nehezen felbecsülhető, de a Tor tűnik a legnagyobbnak, távoli második az I2P, a többi jelentősebb kisebb méretben és népszerűségben.[177] A dark web használatához nem kell speciális hardvert vagy szoftvert vásárolni, elegendő egy ingyenes böngészőt letölteni, például a Tor-t.[178]
Tor egy ingyenes, nyílt forráskódú (open source) szoftver, ami segít az anonimitást megőrizni online. Sokban hasonlít egy szokványos web böngészőre, a különbség, hogy a Tor az internethez a Tor hálózaton keresztül csatlakoztatja a felhasználót. Használatával az internetforgalom egy szerverek hálózatán véletlenszerűen irányított, mielőtt az eléri a végső célját, hogy a felhasználó lokációja és identitása védve maradjon. A Tor „The Onion Router" (A Hagyma Böngésző) neve arra utal, hogy úgy védi a felhasználó adatait, hogy több rétegű titkosításba foglalja, mint egy hagymát.[179] Léteznek dark web keresőmotorok is, de a legjobbak is küszködnek a folyamatosan változó színtér miatt, így azokkal a keresés élménye az 1990-es évekre emlékeztet. Még az egyik legjobb keresőmotor, a Gram keresési eredményei is gyakran repetitívek és irrelevánsak. Opció még az link listák használata, mint The Hidden Wiki, de az ezeken található indexek is gyakran hibaüzenetet adnak. A leghíresebb dark web keresőmotor jelenleg a Duck Duck Go. A Tor dark web oldalainak címei .onion-nal végződnek, és kevert az elnevezési rendszerük, így ezek az URL-ök megjegyezhetetlenek.[180] A weboldalak a dark weben

[176] SALEH, S. – QADIR, J. – ILYAS, M. U.: Shedding Light on the Dark Corners of the Internet: A Survey of Tor Research. Journal of Network and Computer Applications, 2018. Vol. 114. 1. o.

[177] MOORE – RID: i.m. 15. o.

[178] BECKSTROM, M. – LUND, B.: Casting Light on the Dark Web: A Guide for Safe Exploration. Rowman & Littlefield Publishers, London, 2019. 41.o.

[179] How To Use Tor Browser: Everything You MUST Know in 2021. vpnMentor. (2021, July 12). https://www.vpnmentor.com/blog/tor-browser-work-relate-using-vpn/ (2021.08.02.)

[180] RAZALI, N. B. – SURADI, N. R. binti M.: A Nest for Cyber Criminals: The Dark Web. IEEE, 2019. 2. o.

tehát nem úgy végződnek, hogy „.com”, vagy „.org” vagy más gyakori domain végződések, hanem „.onion” vagy „.i2p.”, és gyakran betűk és számok hosszú sorából állnak.[181]

3. Anonimitást elősegítő deep web és dark web techológiák

Az anonimitás a kiberbűnözés egyik sarokköve, mely már szabadon hozzáférhető technológiákkal is megvalósítható.[182] Néhány anonimitást elősegítő deep web és dark webhez kötődő technológia a teljesség igénye nélkül:

A Tor használatának elfedéséhez többen VPN-t[183] használnak.

Az Invisible Internet Project (I2P) egy névtelen átfedő hálózat (overlay network, hálózat a hálózatban) ami védi a kommunikációt a megfigyeléssel szemben. Használható e-mailezéshez, web böngészéshez, blogoláshoz, fórumozáshoz, weboldal hosztolásához, fájlmegosztáshoz és valós idejű chateléshez.

A Free Anonymous Internet project (FAI) egy decentralizált deep web szolgáltatás, ami blockchain technológiát használ a megszokott World Wide Web privát, biztonságos, peer-to-peer (egyenrangú felek közötti, P2P) alternatívájának létrehozására. Saját bitcoin kódon alapuló digitális fizetőeszköze és beépített decentralizált piaca is van. Lehetővé teszi a felhasználóinak a saját média tartalmaik közzétételét és a mások tartalmainak biztonságos böngészését.

Free Net: egy ingyenes anonim fájlmegosztást, „freesite-ok” (csak a Freenet-en elérhető oldalak) böngészését és létrehozását, fórumokon való chatelést lehetővé tevő szoftver.

---

https://www.academia.edu/40783401/A_nest_for_cyber_criminals_-the_dark_web (2021.08.03.)

[181] GEHL, R. W.: Illuminating the ‘dark web’. The Conversation. (2018, October 30). https://theconversation.com/illuminating-the-dark-web-105542 (2021.08.03.)

[182] SZÁSZ A.: A kiberbűnözés társadalmi kontextusa. In: KOVÁCS J. – KÖKÉNYESSY Zs. – LÁSZLÓFI V. (szerk.): A normán innen és túl: Tanulmányok a Történeti Kollégium konferenciájának előadásaiból. ELTE BTK Történeti Kollégium, Budapest, 2017. 105. o.

[183] VPN használatával (a Virtual Private Network, virtuális magánhálózat rövidítése) biztosítható, hogy a számítógép ne legyen követhető. A következőképpen működik: a számítógép az internetszolgáltató helyett egy VPN-kiszolgálóhoz csatlakozik egy biztonságos, titkosított kapcsolaton keresztül. Ezután a VPN-kiszolgáló csatlakozik a keresett webhelyhez. Ott a szokásos módon rögzítik a látogatás adatait, azonban a VPN-kiszolgáló IP-címe, és nem a saját számítógép IP-címe alapján. Mire jó a VPN? Valóban anonim böngészést nyújt! VPN szerver. (2021. március 8.). https://www.vpnszerver.hu/mire-jo-a-vpn/ (2021.08.03.)

Decentralizált, hogy kevésbé legyen sebezhető a támadásokkal szemben, és rendkívül nehéz lekövetni, ha „darknet" módban használják, ahol a felhasználók csak a barátaikkal lépnek kapcsolatba. A Freenet csomópontok általi kommunikációja titkosítással ellátott, és más csomópontokon továbbítódik, hogy rendkívül nehezen lehessen meghatározni, ki kéri az információt és annak tartalmát. A ZeroNet egy új rendszer, mely torrent technológián alapul, Bitcoin titkosítással kombinálva, mely még nem igazán kiforrott, de ígéretesnek tűnik a jövőben.[184] A ZeroNet magyar találmány, megalkotója Kocsis Tamás, aki a következőként fogalmaz a hálózatról: „Olyan hálózatot fejlesztek, amelyben a weboldalakat a látogatók maguk üzemeltetik, nincs szükség szolgáltatókra vagy központi szerverre. Magyarul nem kell fizetni azért, hogy egy oldal felkerüljön a hálózatra. A felhasználó készít egy weboldalt, ami letöltődik a látogatók gépére, innentől pedig ők is teljes értékű kiszolgálói lesznek az oldalnak. A felhasználók egymás rendszeréről töltik le ezeket az oldalakat; még internetkapcsolatra sincs szükség, hogy valaki dolgozzon a saját oldalán. A hálózat előnye, hogy biztonságos, mert a megtámadása nagyon időigényes, és óriási kapacitásra volna szükség hozzá."[185] A koronavírus pandémia miatt sokkal többen dolgoznak otthonról, ezért a biztonságos otthoni munkavégzés miatt VPN-t használók tábora sok országban nagyot nőtt. A NordVPN VPN szolgáltató adatai szerint 2020. március 11-től március 23-ig a VPN technológiájának globális használata 165%-os növekedést mutatott.[186]

4. A dark web tartalmai

Barratt et al. öt kategóriába sorolja a dark web tartalmait: 1. „Szórakoztatási értékű" tartalmak melyek a felszíni weben szigorúan szabályozottak, mint a pornográfia. 2. Magára a dark webre utaló tartalmak, pl. instrukciók a Tor, a rejtett szolgáltatások, titkosítás etc. használatáról 3. Illegális, vagy szigorúan szabályozott árucikkekre specializálódó piacok és kereskedelmi vállalkozások, mint a kriptopiacok. 4. Scam és adathalász (phishing) oldalak, átverések, csaló szolgáltatások. 5. Szolgáltatások,

[184] RATHOD: i.m. 78. o.

[185] VALAHOVITS Sz. É.: Magyar találmány: cenzúrázhatatlan internet. Válasz.hu. (2017. április 21.). http://valasz.hu/techvilag/egy-magyar-fiatalember-feltalalta-a-cenzurazhatatlan-internetet-123507 (2021.08.04.)

[186] PALMER, D.: VPN use surges as coronavirus outbreak prompts huge rise in remote working. ZDNet. (2020, March 23). https://www.zdnet.com/article/vpn-use-surges-as-coronavirus-outbreak-prompts-huge-rise-in-remote-working/ (2021.08.05.)

melyekben a felhasználók határozzák meg a kommunikáció vagy a Tor használatának céljait és tartalmát, mint az anonim e-mail programok, chatszolgáltatások, közösségi hálózatok, nyílt témájú fórumok, és P2P fájlmegosztás. Ezekben megjelenhetnek az előző pontokban tárgyalt tartalmak, de ezek egy felügyelettől, politikai beavatkozástól vagy cenzúrától mentes teret is jelentenek. Tévhit, hogy a dark web a hatóságok számára áthatolhatatlan, amit az is mutat, hogy egyre több kábítószer kriptopiac és dark web pedofil hálózat tagjait és vezetőit tartóztatják le. A hagyományos bűnüldöző technikák, köztük a fedett nyomozó alkalmazása is sikeresek lehetnek a digitális környezetben.[187] Moore és Rid 2015. január és március között egy website keresőrobottal (web crawler) végzett kutatása során 300.000 címet vizsgált, és arra jutott, hogy a Tor rejtett szolgáltatásain található weboldalak leggyakrabban bűnözői irányultságúak. Ezek közé tartozik a kábítószerkereskedelem, a jogosulatlan pénzügyi tevékenység és az erőszakos, a gyermeket és állatokat szerepeltető pornográfia. 2015 eleji vizsgálatuk során még arra jutottak, hogy majdnem hiányzik az dzsihadizmus a Tor rejtett szolgáltatásain, csupán egy maréknyi aktív oldalt találtak. Moore és Rid a pénzügyi kategóriát 3 prominens alkategóriára osztja: Bitcoin-alapú pénzmosási módszerek, illegálisan szerzett bankkártyákkal és lopott felhasználói fiókokkal, és hamis pénzzel való kereskedelem. A Tor dark webén a kábítószerek széles tárháza a leggyakoribb árucikk. Sokféle eladó létezik, az egy oldallal rendelkezőktől a közösségi piacokig, mint az Agora. Sok eladó csalónak tűnik. Website-ok szolgáltatnak linkeket szexuális erőszakot, állatokkal folytatott közösülést és gyemekpornográfiát szerepeltető videókhoz. Vannak közösségek fétisek megvitatására és megosztására is. Más illegális szolgáltatások között találhatók a hamis okiratok, lopott, vagy más illegálisan szerzett felszerelések, lőfegyverek, rosszindulatú szoftverek, amik személyes felhasználói fiókok begyűjtésére specializálódtak vagy szolgáltatásmegtagadásos/túlterheléses (Denial-of-service, DoS) támadásokra. Több oldal bérgyilkos szolgáltatást kínál, de nincs jele, hogy bárki is sikeresen kapcsolatba lépett volna már velük. Sok az „egyéb" kategóriába sorolt oldal magáról a dark webről szól. Ezek a „meta oldalak" közé hoszting szolgáltatások és oktatóanyagok tartoznak a Tor használatáról. Az „egyéb" kategóriába tartoznak még személyes blogok, újságírók drop site-jai, és más ártalmatlan szolgáltatások. A legtöbb oldal a „none" („semmi") kategórába került. A félresikerült és tartalom nélküli oldalak tömege mutatja, mennyire megbízhatatlan egy rejtett-szolgáltatás platform a legtöbb

[187] BARRATT, M. – ALDRIDGE, J. – MADDOX, A.: Dark Web. In: WARF, Barney (szerk.): The SAGE Encyclopedia of the Internet. SAGE Publications, Ltd., Thousand Oaks, 2018. 185–188. o.

felhasználó számára. Sok oldal nem volt hozzáférhető nyitólapján túl, mert bejelentkezést kértek, ezek legális volta nem tiszta.[188]

Gulyás a dark weben elkövetett bűncselekmények széles skálájára mutat rá 2021-ben: Legjellemzőbbek a különböző fizetőeszközzel, vagy azt helyettesítő szolgáltatásokkal történő visszaélések, hamis dokumentumok, és személyazonosító okmányok forgalmazása, kábítószer és gyógyszer kereskedelem, a hamisított gyógyszerek forgalmazása, továbbá fegyverkereskedelem. Elérhetőek különféle szolgáltatások is, a hackerbérléstől kezdve a bérgyilkosságig, de akár migráns útvonalat is lehet vásárolni. Ezek a bűncselekmények színtere általában valamelyik piac, azaz „Black Market", más néven „Crypto Market", ahol a fizetőeszköz jellemzően virtuális valuta, mint a Bitcoin, vagy Monero. A piacokon kívül a másik terület azok az oldalak és fórumok, chatszobák, Pastebin stílusú oldalak, ahol a kiberbűnözők árusítják termékeiket és szolgáltatásaikat, illetve kölcsönös információcserével fejlesztik eszközeiket, technikájukat, valamint módszereiket. A megvásárolható sérülékenységeknek, exploitoknak a piacokon kívül dedikált oldalaik is vannak, ahol akár nulladik napi sérülékenységeket (0Day vulnerability), vagy különböző rendszerekhez exploitokat, lehet vásárolni részletes utasítással egyetemben. Léteznek még ún. „Doxing" oldalak, amik ismert személyek, „celebek", üzletemberek, politikusok magánéletével kapcsolatos illegálisan megszerzett bizalmas adatokat hoznak nyilvánosságra.[189]

Mirea et al. felmérése során a következő mindennapi általános társalgásra szolgáló dark webes fórumokon tölttettek ki online kérdőívet: The Hub (thehub7gqe43miyc.onion); Intel Exchange (rrcc5uuudhh4oz3c.onion); Darknet Central (2u7kil26qazmrmb6.onion); és DarknetM Avengers (avengerfxkkmt2a6.onion).[190] Felmérésük eredményeként arra jutottak, hogy a dark web nem olyan „dark", mint az a szakirodalomból tűnik, úgy vélik, az nem kriminogén. A felmérésben résztvevők arról hagyományos nyílt forrásokból szereztek tudomást, és a dark web használata során a szólásszabadság a fő húzóerő, ami miatt azt rendszeresen használják mindennapi tevékenységek végzésére. A szerzők nem tagadják, hogy a dark web biztonsági kockázatot jelent, és komoly kutatást igényel. Úgy gondolják, a dark weben nem a bűnözés a norma, hanem azt különböző egyének különböző célokra használják.[191] Úgy vélem, a dark web fórumain végzett ilyen

[188] MOORE – RID: i.m. 18–24. o.

[189] GULYÁS A.: Vállalatbiztonság és a dark web. Biztonságtudományi Szemle, 2021/3. 29–30. o.

[190] MIREA, M. – WANG, V. – JUNG, J.: The not so dark side of the darknet: a qualitative study. Security Journal, 2019. Vol. 32. 107. o.

[191] Uo. 114. o.

felmérés, de még a face-to-face interjú sem festhet reális képet a dark web kriminogén vagy nem kriminigén voltáról, mert e fórumok használói természetesen nem, vagy kisebb valószínűséggel fognak negatív képet festeni önmagukról, magukat nem fogják inkriminálni. A dark webről úgy vélem reálisabb képet kaphatunk gépi módszerek, pl. keresőrobotok használatával. Moore és Rid kutatása[192] alapján a dark web egyértelműen kriminogén képet fest. Véleményem, hogy a dark web kriminogén.

5. A terroristák a dark weben

1. A terroristák dark webre „üldözése"

Moore és Rid 2015. január és március közötti kutatása során még arra jutottak, hogy majdnem hiányzik az dzsihadizmus a Tor rejtett szolgáltatásain, csupán egy maréknyi aktív oldalt találtak. A szerzők szerint a dark weben a propaganda nem ér messzire, és az újoncokat kezdetben elijesztheti, hogy egy „jogellenes" cselekményt kell véghezvinniük, szemben egy egyszerű, Google kereséssel. A rejtett szolgáltatások gyakran nem elég stabilak vagy hozzáférhetőek a hatékony kommunikációhoz, más platformok jobban megfelelnek a kommunikációs igényeknek. Dzsihadisták azonban gyakran használják a Tor-t a felszíni weben, a fokozottabb anonimitás miatt.[193] A terroristák dark webes jelenléte 2015 óta jelentősen nőtt: a 2015. novemberi párizsi terrortámadások után hírei és propagandája terjesztése céljából az IS a dark web felé fordult, hogy megvédje támogatóinak azonosságát és az anyagaikat a hacktivisták tevékenységétől. Ez az után történt, hogy több száz IS-hez köthető weboldal került eltávolításra az Anonymous hacker kollektíva Operation Paris (OpParis) kampányának részeként. Az IS mediaügynöksége, az Al-Hayat Media Center egy IS-hez kötődő fórumon közzétett egy linket és instrukciókat arról, hogyan érhető el az új dark webes oldaluk.[194]

Az terroristák közösségi médiás jelenléte ellen számos platform ellenlépéseket tett. Például a Twitter kifejezetten keményen lépett fel a terroristák felhasználói fiókjaival szemben, de a terroristák alkalmazkodó képesek, céljaik elérése és a kommunikáció biztosítása érdekében folyamatosan alternatív lehetőségeket keresnek.[195] Az internet

[192] MOORE – RID: i.m. 7–38. o.

[193] Uo. 18–22. o.

[194] WEIMANN (2018): i.m. 3. o.

[195] ALKHOURI, L. – KASSIRER, A.: Tech for Jihad: Dissecting Jihadists' Digital Toolbox. Flashpoint, USA, 2016. 1. o.

felszíni része és a közösségi média helyett kénytelenek biztonságosabb és rejtettebb alternatívákat keresni, mint a dark web, és különféle alkalmazások.[196] A felszíni web használata a terroristák számára kockázatosabb: ott felügyelhetőek, lekövethetőek, megtalálhatóak. Ezzel szemben a dark weben decentralizált és anonim hálózatok használatával a lebukás elkerülhető, és a terrorista platformok zártak maradhatnak.[197] A terrorista szervezetek korábbi intenzív nyilvános webes jelenléte visszaszorult (a kisebb szervezeteknek még mindig vannak internetes felületeik, gyerekeknek szóló weboldalaik, illetve terrorizmussal szimpatizáló csoportok még mindig megtalálhatók a közösségi média felületein).[198] Besenyő és Gulyás szerint a terroristák felszíni webről való elüldözése biztonsági szempontból kontraproduktív volt, kommunikációjuk nehezebb lekövethetősége miatt.[199] A szerzők e véleményével egyetértek, hozzátéve, hogy a terroristák felszíni webes jelenlétének visszaszorításának biztonsági szempontból előnyei is vannak, például az arra fogékonyabbak számára propagandájuk így nehezebben fellelhető, így ideológiájuk kevesebbeket képes radikalizálni, elkövetésekre inspirálni.

2. Mire használják a terroristák a dark webet?

A terroristák a dark webet Özkaya felosztásában a következő tevékenységekre használják: támadások megtervezése, finanszírozásra és üzleti tranzakciókra, fegyverek és hamis útlevelek megszerzésére.[200]

Besenyő és Gulyás szerint a terroristák a dark weben ugyanazokat a tevékenységeket végzik, mint a felszíni weben, csak biztonságosabban. Információval és propagandával látják el a szimpatizánsaikat, toboroznak és radikalizálnak, koordinálják az akcióikat és pénzt gyűjtenek. A dark web alkalmas illegális termékek megvásárlására is. Források szerint a 2015-ös párizsi terrortámadások elkövetéséhez használt fegyvereket a dark weben vásárolták egy „DW guns" álnevű német dark web árustól, aki dark webes

https://www.flashpoint-intel.com/wp-content/uploads/2016/08/TechForJihad.pdf (2021.07.05.)

[196] ÖZKAYA: i.m. 53. o.

[197] WEIMANN, G.: Terrorist Migration to the Dark Web. Perspectives on Terrorism, 2016. Vol. 10. No. 3. 40–41. o.

[198] HAIG Zs.: Információs műveletek a kibertérben. Dialóg Campus Kiadó, Budapest, 2018. 301-302. o.

[199] BESENYŐ, J. – GULYÁS, A.: The Effect Of The Dark Web On The Security. Journal Of Security and Sustainability Issues. 2021. Vol. 11. No. 1. 113–114. o.

[200] ÖZKAYA: i.m. 53–55. o.

oktatóanyagokat alapján startpisztolyokat alakított át éles fegyverekké, és azokat a feketepiacon adta el.[201]

A terroristák a dark weben biztonságosabban kommunikálhatnak, mint valaha. 2016 márciusában a francia belügyminiszter, Bernard Cazeneuve a Nemzetgyűlés előtt a terroristák dark web használatára hívta fel a figyelmet.

A dark webet virtuális fizetőeszközök használatával terroristák és más bűnözők felhasználják összegek rejtett utalására. Korunkban Weimann ezt a trendet tartja a legriasztóbbnak a dark web terroristáknak nyújtott lehetőségei közül.[202] A dark weben végzett terrorizmus finanszírozást a terrorizmus finanszírozásával foglalkozó fejezetben tárgyalom részletesebben.

Malik 2018-as „Terror in the Dark" című jelentésében a következő trendekre világít rá a terroristák dark web használatát illetően: A terroristák a titkosítást használják rejtőzködésre. A felszíni web a közösségi média cégek és hatóságok fokozott általi felügyelete a szélsőséges tartalmak a közösségi média platformjairól való gyorsabb eltávolításához vezetett. A terrorcselekmények megtervezésére a dark webes extrémista hálózatokat fokozottabban használják. A toborzók a dark webet használják terrorcselekmények megtervezésére és kezdeményezésére, mivel ott kisebb az esély a lebukásra. Miközben a kezdeti kapcsolatfelvétel a felszíni weben történhet meg, a további instrukciókat gyakran végpontok közötti titkosítással ellátott alkalmazásokon (ezekről bővebben később) adják arról, hogyan férhetnek hozzá dzsihadista weboldalakhoz a dark weben. A terroristák a dark webet felhasználják toborzásra: a titkosított csatornák, mint a Telegram, és a dark web színterei nehezen hozzáférhetőek, emiatt tömeges toborzás ezeken ritkán történik, ehelyett az IS emberei az érdeklődő szimpatizánsokat a felszíni web és a közösségi média platformjairól a biztonságosabb dark web felé irányítják, a további interakció és indoktrináció színterére. A terroristák a dark webet felhasználják propaganda tárolására: Az extrémista és terrorista tartalmak felszíni webről és deep webről való eltávolítása, főleg a mesterséges intelligencia által végzett tömeges eltávolítás növeli annak a kockázatát, hogy a tartalmakat terjesztő vagy terrorszervezeteknek anyagi támogatást nyújtó személyek bíróság elé állításához szükséges bizonyítékok elveszhetnek. Ezek közül az anyagok közül sok újra előbukkan a felszíni weben. A tech cégek és a bűnüldöző hatóságoknak együtt kell működni az anyagok hatékony archiválása céljából, hogy a viselkedésminták megérthetők legyenek. A terroristák kriptovalutákat használnak adománygyűjtésre, és a lebukás elkerülése

[201] BESENYŐ – GULYÁS: i.m. 113–114. o.

[202] WEIMANN (2018): i.m. 4–5. o.

érdekében. A kriptovaluták ugyanazt a fajta anonimitást biztosítják a pénzügyi környezetben, mint a titkosítás a kommunikációs rendszerekben. A bitcoinnal végzett adománygyűjtéssel és online pénzügyi tranzakciókkal a terroristák és más bűnözők el tudják kerülni a pénzügyi szabályozók és más harmadik személyek beavatkozását.[203] Besenyő és Gulyás rávilágít arra, hogy a dark webet szélsőjobboldali és anarchista mozgalmak is használják nézeteik terjesztésére és kommunikációra. Az utóbbi évtizedekben erősödő jobboldali extrémizmus tartalmait a közösségi média platformok szűrik, emiatt az ezeket a nézetek vallók is dark web felé fordultak. A szerzők itt is rámutatnak, hogy a közösségi média cenzúrájának hátulütője, hogy a bűnüldöző szervek a dark webre kényszerült szervezetek kommunikációját szem elől téveszthetik, ami veszélyes. A szerzők rávilágítanak arra, hogy nagyon nehéz beférkőzni az extrémista fórumok és chat szobák belső köreibe, mivel azokban különböző tagsági szintek vannak, szigorú hitelesítéssel. Találhatóak még olyan blogok és oldalak, melyeken olyan „tankönyvek" találhatóak, mint az „Anarchist cookbook" vagy „Anarchist poison book", bomba és méregkészítési instrukciókkal.[204]

6. Bünüldöző technikák a dark weben

A bűnüldöző szervek számos technikával képesek a dark weben bűnözőket elkapni, melyek terroristákkal szemben is alkalmazhatók: fedett műveletekkel, hackeléssel, OSINT[205] alkalmazásával, tömeges adatgyűjtéssel, a lefoglalt adat átvizsgálásával, a pénzmozgások, főleg a Bitcoin útjának nyomonkövetésével, a postai rendszer követésével (pl. kábítószer vásárlása esetén).[206] Nyeste és Szendrei rámutat arra, hogy a dark weben az információgyűjtés problematikus, de itt is megvannak a speciális keresőmotorok és egyéb lehetőségek, az információk kinyerésére (célszoftverek: például Tor, I2P, Freenet, Deepdotweb.com, Reddit, GRAMS). Az OSINT felhasználható a bűnös tevékenységek feltérképezésére, szervezett bűnözői csoportok beazonosítására,

[203] MALIK, N.: Terror in The Dark: How Terrorists use Encryption, the Darknet and Cryptocurrencies. The Henry Jackson Society. London, 2018. iv. o. https://henryjacksonsociety.org/wp-content/uploads/2018/04/Terror-in-the-Dark.pdf (2021.08.09.)

[204] BESENYŐ – GULYÁS: i.m. 112. o.

[205] Az OSINT-ről: DOBÁK I.: OSINT – Gondolatok a kérdéskörhöz. Nemzetbiztonsági Szemle, 2019/2. 83–93. o.

[206] COX, J.: 7 Ways the Cops Will Bust You on the Dark Web. Vice. (2016, June 26). https://www.vice.com/en/article/vv73pj/7-ways-the-cops-will-bust-you-on-the-dark-web (2021.08.05.)

bomlasztására, bűncselekmények megelőzésére, korábban elkövetett cselekménnyel kapcsolatos információk beszerzésére, bővítésére, a célszemély kilétének megállapítására, a célszeméllyel kapcsolatos adatok bővítésére, a bűncselekmény elkövetési módjának megállapítására, tanulmányozására.[207] A dark weben végzett munkájuk során a bűnüldöző szerveknek a szakértők bevonása elengedhetetlen.[208]
Példák jelenleg használt módszerekre dark webes bűnözők elfogása során:
Memex: A U.S. Defense Advanced Research Projects Agency (DARPA) fejlesztette ki a Memex keresőmotort, ami segít a Védelmi Minisztériumnak (Department of Defense) az emberkereskedelem elleni küzdelemben és illegális tevékenységek felfedésében a dark weben. A Memex tradícionális keresőmotorokkal nem hozzáférhető oldalak millióin szánt végig, indexelve azokat, köztük több ezer olyat, melyek csak dark web böngészőkkel találhatóak meg. Nem fedi fel az IP címeket vagy a dark web használók azonosságát, de analizálja a tartalmat, mintákat és kapcsolatokat fedez fel, amik lekövethetőek és visszanyomozhatóak a használóhoz.
Hálózati nyomozási technikák (Network Investigative Techniques): 2011-2012-ben az „Operation Tornado" fedőnevű nyomozás során az FBI a módszert alkalmazta a dark weben gyermekpornó oldalokat látogató legalább 25 személy IP címének a felfedésére. Hollandia rendőrségének szakemberei írtak egy web crawler-t, ami Tor weboldalak után kutatta át a dark webet. A hatóságok le tudták szűkíteni az oldalakat azokra, amik a gyermekpornográfiához kapcsolódtak, és felfedték egy „Pedoboard" nevű oldal az igazi IP címét, Bellevue, Nebraskában. Az IFB a kapott információ birtokában le tudta nyomozni Aaron McGrath-ot, három gyermekpornó oldal gazdáját.[209]
A Tor anonimitásának áthatolására az FBI a Metasploit applikációt használta az „Operation Torpedo" során.[210]
Hagyományos technikák: Például beszirvárgás fedett nyomozókkal, és személyek követése nyilvános helyeken. 2014 novemberében az „Operation Onymous" művelet rejtett Tor szolgáltatások tucatjainak lefoglalásához vezetett. Nem ismert, hogy a hatóságok hogyan tudták az oldalakat lekapcsolni, szakértők spekulációja szerint kormányzati hackerek DoS támadást alkalmazhattak, amik elárasztják a Tor relay-eket

[207] NYESTE P. – SZENDREI F.: Nyílt forrású információszerzés a bűnüldözésben. Nemzetbiztonsági Szemle, 2019/2. 66. o.

[208] KEHOE, S. R.: The Digital Alleyway: Why the Dark Web Cannot Be Ignored. Police Chief Magazine. (2018, June 12). https://www.policechiefmagazine.org/the-digital-alleyway/ (2021.08.05.)

[209] VOGT, S. D.: The Digital Underworld: Combating Crime on the Dark Web in the Modern Era. Santa Clara Journal of International Law, 2017. Vol. 15. No. 1. 114–115. o.

[210] RUDESILL – CAVERLEE – SUI: i.m. 10. o.

szemét-adattal, hogy a célzott oldalakat olyan Tor relay-ek használatára kényszerítsenek, amiket megfigyeltek, ezáltal lekövetve az IP címüket. De lehetséges, hogy a hatóságok hagyományos technikákat, mint informátorokat vagy fedett nyomozókat alkalmaztak. A Silk Road esetében a hatóságok szerint a drogbáró Ulbricht saját hibái vezettek az elfogásához, és nem volt szükség kifinomult módszerekre.[211]

A dark web vizsgálatára alkalmas az Apache Tika szoftver is.[212] Az Apache Tika toolkit (eszközkészlet) több mint ezer különféle fájltípust (mint PPT, XLS és PDF) észlel és von ki azokból metaadatokat és szöveget. Ezek a fájltípusok egyetlen interfészen keresztül értelmezhetők, így a Tika hasznos lehet a keresőmotorok indexelésében, tartalomelemzésben, fordításban és még sok másban.[213]

A BlackWidow egy nagymértékben automatizált moduláris rendszer, mely valós időben és folyamatosan figyeli a dark web szolgáltatásokat, és az összegyűjtött adatokat egyetlen elemzési keretben egyesíti. Gépi fordítási technikák felhasználásával képes a fórumok és a felhasználók közötti kapcsolatokat vizsgálni, nyelvi korlátok ellenére is. A fórumok között jelentős átfedés mutatkozik, még különböző nyelveken is. A valós idejű információgyűjtés potenciálját szemlélteti Schäfer et al. egy hét darab dark webes fórumon és a felszíni weben végzett tanulmány elvégzésével, mellyel demonstrálják, hogy a BlackWidow képes thread-ek (kommentszálak), szerzők és tartalmak kinyerésére a dark web fórumokból, és tovább dolgozza fel őket kiberbiztonsági szempontból releváns információ kinyerése érdekében.[214]

Ha valaki bizonyos lépéseket tesz az online azonosságának elfedése érdekében, például Tor használatával, vagy ha utánanéz a Windows operációs rendszeren kívüli más lehetőségeknek, azzal az NSA (National Security Agency, Nemzetbiztonsági Ügynökség) megfigyelését kockáztatja. Ha valaki az USA-n, Kanadában, az Egyesült Királyságon vagy az ún. Five Eyes[215] ország egyikén kívül van, amely az NSA-val

---

[211] VOGT: i.m. 115–117. o.

[212] MATTMANN, C.: Searching deep and dark: Building a Google for the less visible parts of the web. The Conversation. (2017, January 9). https://theconversation.com/searching-deep-and-dark-building-a-google-for-the-less-visible-parts-of-the-web-58472 (2021.08.05.)

[213] Apache Tika - a content analysis toolkit. https://tika.apache.org/ (2021.08.06.)

[214] SCHÄFER, M. – STROHMEIER, M. – LIECHTI, M. – FUCHS, M. –ENGEL, M. – LENDERS, V.: BlackWidow: Monitoring the Dark Web for Cyber Security Information. In: Minárik, T. – Alatalu, S. – Biondi, S. – Signoretti, M. – Tolga, I. – Visky, G. (szerk.): 2019 11th International Conference on Cyber Conflict: Silent Battle. NATO CCD COE Publications, Tallinn, 2019. 3. o.

[215] „Kanada, Ausztrália, Új-Zéland, az Egyesült Királyság (UK) és az Egyesült Államok (USA) tagjai a Five Eyes hírszerző közösségnek, a világ legexkluzívabb hírszerző klubjának. (…) A második

együttműködik a felügyeleti erőfeszítéseiben, akkor a Tor-webhelyének felkeresése automatikus ujjlenyomatot hoz létre nála. Más szavakkal: a magánéletet óvó módszerek egyszerű keresése az USA-n kívülről az NSA XKeyscore-ja futtatását indítja el. Továbbá elég a nyílt forráskódú Linux Linux Journal fórumának meglátogatása, hogy valakit ujjlenyomatozzanak, függetlenül attól, hogy hol él, mert az XKeyscore forráskódja azt extrémista fórumként jelöli. A Tails operációs rendszer keresése is ezzel az eredménnyel jár.[216] 2014-ben az XKeyscore nevű NSA program forráskódjának vizsgálata (melyet a Snowden leaks fedtek fel), azt mutatta, hogy ha bármely felhasználó szimplán megkísérli letölteni a Tor-t, az automatikusan ujjlenyomatozva lesz, mely által az NSA megismerheti a Tor felhasználók millióinak azonosságát.[217] Az NSA az XKeyscore használatával gyűjti be és analizálja az internet adatokat, mellyel a felhasználó minden internetes aktivitását felügyelheti.[218]

7. A dark webhez fűződő dilemmák

A dark web biztonsági kockázatai a következők: a bűnözői elemek jelenléte, az illegális cselekmények elkövetésének lehetősége, gyanús (illegális tartalomhoz vezető) linkek, a bűnöldöző szervek jelenléte, vírusok, hackerek és a web kamera eltérítésének lehetősége. Illegális dolgokba lehet botlani, akár egy félreütéssel vagy egy óvatlan kereséssel.[219]

Weimann szerint a dark web elleni fellépés esetén figyelembe kell venni annak nem terrorista használóit és felhasználhatóságát, és társadalmi hasznait is. Kérdés, hogy fontosabb-e a magánélet védelme, mint a terrorista fenyegetéstől való biztonság, továbbá a magánélet, a szólásszabadság és a felügyelet nélküli kommunikáció elvesztésének ára

világháborúban az Egyesült Királyság és az Egyesült Államok közötti hírszerzési együttműködésből nőtt ki, a hidegháború alatt tovább érett, és ma továbbra is valamennyi tag nemzeti érdekeinek védelmét szolgálja." COX, J.: Canada and the Five Eyes Intelligence Community. Canadian Defence and Foreign Affairs Institute, Calgary, 2012. 4. o.

[216] TUCKER, P.: If You Do This, the NSA Will Spy on You. Defense One. (2014, July 7). https://www.defenseone.com/technology/2014/07/if-you-do-nsa-will-spy-you/88054/ (2021.08.03.)

[217] WEIMANN, G.: Going Darker? The Challenge Of Dark Net Terrorism. Wilson Center, Washington, DC, 2018. 8. o. https://cyber.haifa.ac.il/images/Publications/darkweb_Gabriel%20Weimann.pdf (2021.08.03.)

[218] ZETTER, K.: Use privacy services? The NSA is probably tracking you. Wired. (2014, April 7). https://www.wired.co.uk/article/nsa-targeting-tor-users (2021.08.03.)

[219] SYMANOVICH, S.: How to safely access the deep and dark webs. Norton. (2020, July 23). https://us.norton.com/internetsecurity-how-to-how-can-i-access-the-deep-web.html (2021.08.09.)

meghaladje-e az előnyöket. Nagyon alacsony a terroristák száma a Telegram, Tor, és a más titkosított applikációkon terrorcselekményt elkövetni nem szándékozó használók túlnyomó többségéhez képest. Weimann szerint a terroristák a dark webbe férkőzésének egy tevékenységeik elleni nemzetközi kutatást kellene megindítania, amelynek nem szabad korlátoznia a legitim, törvényes véleménynyilvánítási szabadságot.[220] Jogosan mutat rá Rubasundram, hogy a magánéletnek és anonimitásnak is kell hogy legyen helye a társadalomban, de észszerű keretek között. A kulcskérdés, hogy: „Tényleg a biztonságunk árán akarunk magánéletet?"[221] Chertoff arra figyelmeztet, hogy a dark web természeténél fogva anonim és képtelen különbséget tenni a bűnözők és rendes felhasználók között. A bűnöldöző szerveknek olyan taktikákat kellene alkalmazniuk, melyek tiszteletben tartják az átlagos felhasználó adatvédelmét, miközben leleplezik a bűnözőket. A leghatékonyabb módja ennek, ha az illegális oldalakat keresik az illegális felhasználók helyett. Kormány-hackerek de-anonimizáló eszközöket helyezhetnek el az oldalhoz hozzáférő felhasználók számítógépeire. Ha szimplán csak leállítanak egy oldalt, egy másik fog helyette felbukkanni. Másrészről, ha vádat emelnek egy illegális oldal felhasználói ellen, a jövőbeli felhasználók, akik illegális oldalakhoz való hozzáférést fontolgatnak, hezitálni fognak, a kockázat miatt, hogy elkaphatják őket. A végső opció az lenne, hogy megkísérelhetnék feltörni a Tor-t, azonosítani minden Tor felhasználót. Ez a Silk Road esetét alapul véve valószínűleg azt eredményezné, hogy a szolgáltatás egy robosztusabb verzióját alkotnák meg, ezáltal gátolva a kormányzati törekvéseket, továbbá ez el is pusztítana egy hasznos eszközt a legitim felhasználók kezében. Az USA olyan módokon alkotmányosan elkötelezett az internetes véleménynyilvánítás szabadágának védelme mellett, ami sok országról nem mondható el. Néhány ország teljes kontrollt szeretne az internet forgalma felett. Ők a szólászabadságot a hatalmuk fenyegetéseként látják, és a dark webet, mint eszközt, amely lehetővé teszi a másképp gondolkodóknak, hogy szabadon beszéljenek. Az internet természeténél fogva számítógépek nemzetközi hálózata. Az illetékesség a legjobb esetben is ködös, tehát a kormányoknak meg kell találniuk az együttműködés módjait abban, hogy legalább kölcsönösen elfogadható dark webre irányuló szabályozást dolgozzanak ki. Ahogy a politikai döntéshozóknak éberen kell figyelniük a dark web fejlődését, és gondoskodni arról, hogy a hatóságok rendelkezzenek megfelelő

[220] WEIMANN (2018): i.m. 9. o.

[221] RUBASUNDRAM, G. A.: The Dark Web and Digital Currencies: A Potent Money Laundering and Terrorism Opportunity. International Journal of Recent Technology and Engineering (IJRTE), 2019. Vol 7. No. 5. 481. o.

erőforrásokkal és jogi támogatással a dark weben történő rendfenntartáshoz. A dark webre vonatkozó politikának árnyaltnak és átgondoltnak kell lennie, hogy egyensúlyt találhasson az adatvédelmet szem előtt tartó felhasználók igényei és az állam illegális tevékenységek megállítása iránti felelőssége között.[222] Egyetértek Jardine véleményével, aki szerint a kényelmetlen valóság az, hogy ténylegesen azoknak a demokratikus nemzeteknek kell foglalkoznia a rendszer negatív következményeivel, amelyek kifejlesztették és hosztolják a Tor network nagy részét, miközben annak kevés előnyét látják. Szabad országokban a technológia használatának lehetősége azt jelenti, hogy szaporodnak a Silk Road-hoz hasonló oldalak, az anonim gyemekpornó website-ok és a trollok, de az előnyök (az állami megfigyelés vagy vállalati tartalom megfigyelés elkerülése és a cenzúra megkerülése) minimálisak. Léteznek más kevésbé nehézkes programok (privát keresőmotorok, mint a Duck Duck Go, és VPN-ek) és nagyjából ugyanaz a hatásuk, mint a Tor-nak, de nagyobb letöltési sebességgel és kisebb potenciállal a visszaélésre, mivel ezek megőrzik a felhasználók adatait és együtt tudnak működni a hatóságokkal, ha érvényes bírósági végzést kapnak. Ezért, hacsak valaki nem végez illegális tevékenységeket, a teljes anonimitást nyújtó program, mint a Tor alkalmazásának a liberális demokratikus országokban korlátozott a szükségessége. Fontos hangsúlyozni azt is, hogy az internet technológiájának gyors fejlődése mennyire meghaladta a jogi szabályozást is. A fentiek alapján valószínűtlen, hogy a Tor nettó haszonnal jár a demokratikus országokban. Az nagy valószínűséggel több kárt okoz, mint hasznot.[223]

A dark web használata a szabad országokban nem illegális, és Moore és Rid szerint valószínűleg nem is kell, hogy az legyen, de ezek a széleskörben abúzált platformok éles kontrasztban a szélesebb nyilvános kulcsú infrastruktúrával (Public Key Infrastructure) szabad prédák, és azoknak is kell lenniük a legagresszívebb hírszerző és bűnüldöző technikákkal szemben, ahogy a beható akadémiai kutatásnak is. A szerzők szerint az ilyen tisztán elbarikádolt, szabad-tűz zóna még hasznos is lehet az állam számára, és a Tor-nak a tech vitáknak komoly részét kell képeznie. A dark web kérdésével nem szembenézni felelőtlenség lenne.[224]

---

[222] CHERTOFF, M.: A public policy perspective of the Dark Web. Journal of Cyber Policy, 2017. Vol. 2. No. 1. 36–37. o.

[223] JARDINE, E.: The Dark Web Dilemma: Tor, Anonymity and Online Policing. Centre for International Governance Innovation, London, 2015. 7. o. https://www.cigionline.org/sites/default/files/no.21.pdf (2021.08.09.)

[224] MOORE – RID: i.m. 32–33. o.

8. Javaslatok

A titkosszolgálati eszközök alkalmazására kiváló platformot jelentenek a dark web színterei. Véleményem szerint fontos a dark weben folyó kriminalitás, az illegális piacok, a pedofil oldalak, a terrorista oldalak és egyéb bűnözői elemek bűnüldöző szervek általi nyomon követése, felügyelete, tanulmányozása, fedett ügynökök, szakértők alkalmazása. A felbukkanó illegális piacokat és pedofil oldalakat el kell távolítani. A terrorizmus elleni harc, a terrorcselekmények megelőzése és terrorizmus finanszírás elleni küzdelem szempontjából különösen elengedhetetlennek tartom a terroristák dark webes aktivitásának (is) nyomon követését, tanulmányozását.

VII. A TERRORISTÁK ÉS AZ OKOSTELEFONOS ALKALMAZÁSOK

1. Okostelefonos alkalmazások a terrorizmus szolgálatában, és ezen applikációk csoportosítása

Az okostelefonok[225] és az azokhoz kötődő alkalmazások részei a többség mindennapjainak. Az okostelefonok és az egyéb hordozható készülékek megváltoztatták a világ nagy részének kommunikációját. E technológiák használatát a terroristák is hamar átvették.[226] A terroristák okostelefonos alkalmazás használata és internethasználata között sok átfedés van, ezeken is hirdethetik propagandájukat, kommunikálhatnak, koordinálhatják tevékenységeiket, oktathatnak, gyűjthetnek adományokat etc. Ezen alkalmazások letöltéséhez, és sokszor a használatukhoz is netkapcsolat szükséges, a terroristák okostelefonos applikáció-használatát az internethasználatuk egy távoli aspektusának tartom, és indokoltnak vélem ezen értekezésben való vizsgálatukat. A téma méltatlanul alulkutatott, főleg a magyar szakirodalomban.

Alkhouri és Kassirer a következő eszközöket sorolja a terroristák digitális „szerszámosládájába": biztonságos böngészők, a VPN-ek és proxy szolgáltatások, védett e-mail szolgáltatások, okostelefonos biztonsági alkalmazások, titkosítással ellátott üzenetküldő alkalmazások, és propaganda applikációk.[227] Jelen fejezetben a terroristák által használt alkalmazásokat Alkhouri és Kassirer kategorizálását (okostelefonos biztonsági alkalmazások, titkosítással ellátott üzenetküldő alkalmazások, és okostelefonos propaganda applikációk[228]) követve mutatom be. Az alkalmazások tipizálhatók még mint terrorista fejlesztésű és nem terroristák által fejlesztett, de általuk használt alkalmazásokként.

---

[225] KRAUT, A. – KŐHALMI, L. – TÓTH, D.: Digital dangers of smartphones. Journal of Eastern-European Criminal Law, 2020. Vol. 7. No. 1. 36–49. o.

[226] ALKHOURI, L. – KASSIRER, A.: Tech for Jihad: Dissecting Jihadists' Digital Toolbox. Flashpoint, USA, 2016. 1. o.
https://www.flashpoint-intel.com/wp-content/uploads/2016/08/TechForJihad.pdf (2021.07.05.)

[227] Uo. 1. o.

[228] Uo. 1. o.

1. Biztonsági alkalmazások

Az okostelefonos alkalmazások használata kockázatokkal is jár a terroristák számára. Óvintézkedések hiányában harmadik személyek könnyen hozzáférhetnek a szenzitív adataikhoz, például a GPS lokációjukhoz, vagy IP címükhöz. A biztonsági kockázatok csökkentése érdekében ezért további alkalmazásokat használnak. A következő biztonsági applikációk kedveltek a terroristák körében: Locker, FAKE GPS, D-Vasive Pro, AMC Security, ESET Mobile Security, Battery Saver, Call/SMS Blocker, Privasy Locker, APP Manager, iSHREDDER PRO, Override DNS, DNSCrypt, Net Guard, AFWall, F-Secure Freedome, Hide.me, Tutanota.[229]

2. Titkosítással ellátott üzenetküldő alkalmazások

A terroristák a lebukást elkerülendő, szívesen élnek ún. end-to-end encryptionnel (végpontok közötti titkosítással) ellátott alkalmazások használatával.[230]

Az ilyen általában okostelefonról és számítógépről is elérhető applikációkat terroristák már évek óta használnak diszkrét kommunikációra.

Szívesen használják a svájci Threema-t, mely nem gyűjt és igényel személyes adatokat, és titkosítása minden szempontból (pl. fájlok, audiók etc. tekintetében) erős.[231] 2016-ban, Dakkában, Banglades fővárosában a Holey Artisan Bakery-ben elkövetett terrortámadás során, hogy a „digitális lábnyomukat elrejtsék", az elkövetők a Threema-t használták kommunikációra, és annak használatával töltöttek fel képeket az áldozataikról. Az alkalmazás erős titkosítottsága megnehezítette a bangladesi hatóságok dolgát, hogy a bűncselekménnyel kapcsolatban digitális nyomokat gyűjtsenek. A Threema még a szervereiről is törli az üzeneteket.[232] A digitális nyom a következő: „A nyomozás során kiemelkedő szerepe van a digitális adatnak. Nemcsak az online, hanem a digitális környezetben megvalósított bűncselekmények is mindig digitális lábnyomot hagynak maguk után, amelyekből digitális adatok nyerhetők ki. Ezt hívjuk digitális nyomnak."[233] A Threema-t használta továbbá a Srí Lankán, 2019. április 21.

---

[229] Uo. 5–6. o.

[230] PAGANINI, P.: The Role of Technology in Modern Terrorism. InfoSec Institute. (2018, February 3). https://resources.infosecinstitute.com/the-role-of-technology-in-modern-terrorism/#gref (2021.07.06.)

[231] ALKHOURI – KASSIRER: i.m. 7–8. o.

[232] BAGCHI, I.: Terrorists used app to hide digital footprint. The Times of India. (2016, July 6). https://timesofindia.indiatimes.com/world/Terrorists-used-app-to-hide-digital-footprint/articleshow/53070343.cms (2021.07.06.)

[233] TORMA A. – BENDES Á. L.: A cybercrime és a gyermekpornográfia összeolvadása. In: BENDES Á. –

húsvétvasárnapi terrortámadásokat elkövető National Thowheed Jama'ath (NTJ) terrorista sejt is.[234] A 2006-ban megalkotott orosz VKontakte közösségi háló, az „orosz Facebook" a legnépszerűbb közösségi oldal Oroszországban. 2019-ben összesen 400 millió regisztrált felhasználója volt.[235] 2021. július 5-én a VKontakte katalógusa szerint ez a szám már 663 millió volt.[236] (A katalógus 2021.07.06-án már nem volt elérhető.) Alkhouri és Kassirer szerint a VKontakte alapítója, Pavel Durov nevéhez köthető Telegram tűnik a terroristák kedvenc alkalmazásának.[237]

Az IS a Telegramot használta például a 2016-os berlini karácsonyi vásáron elkövetett merénylet elkövetőinek toborzásához is. A 2017-es, 15 emberéletet követelő szentpétervári terrortámadást is az alkalmazással tervezték meg.

A Telegram rendkívül magas fokú titkosítással, privát chat szobákkal, önmegsemmisítő üzenetekkel rendelkezik, könnyű hozzá csatlakozni és új felhasználói fiókokat létrehozni.[238] Az alkalmazás csatornáin belül a felhasználók végtelen mennyiségű fotót, videót, dokumentumot, hangüzenetet oszthatnak meg. Akár 1,5 GB méretű fájlok megosztására is alkalmas.[239] Egy kutatás során 2017. június és december között 98 angol nyelvű oktatóanyagokat terjesztő csatornát elemeztek a Telegramon, melynek eredményeként megállapították, hogy a vizsgált csatornáknak átlagosan 98,7 tagja volt, a legtöbb követővel rendelkezőnek pedig több mint 350. Ezeken a támogatók több mint 7560 fotót, 563 videót, 300 hangüzenetet, 8243 fájlt, és 689 URL linket osztottak meg. A csatornákon három féle anyag jelenléte volt túlsúlyban: Robbanóanyagok készítése: információ és lépésről lépésre lebontott instrukciók robbanóanyagok szintetizálására, rögtönzött robbanószerkezetek és útmutatás robbantószerrel elkövetett

---

NAGY M. – TÓTH D. (szerk.): Lépést tud-e tartani a jog a XXI. század kihívásaival? Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola, Pécs, 2019. 20. o.

[234] RAZEEK, T.: 'Threema' app used by 21/4 terrorists Encryption, a barrier against war on terror? Ceylon Today. (2019, September 29). https://ceylontoday.lk/print-more/41446 (2021.07.06.)

[235] Still don't know Vkontakte, the Russian Facebook with 70 Million active users? E-commerce Nation. (2019, January 2). https://www.ecommerce-nation.com/still-dont-know-vkontakte-the-russian-facebook-with-70-million-active-users/ (2021.07.06.)

[236] https://vk.com/catalog.php (2021.07.05.)

[237] ALKHOURI – KASSIRER: i.m. 7–8. o.

[238] TAN, R.: Terrorists' love for Telegram, explained. It's become ISIS's "app of choice." Vox. (2017, June 30).
https://www.vox.com/world/2017/6/30/15886506/terrorism-isis-telegram-social-media-russia-pavel-durov-twitter (2021.07.06.)

[239] CLIFFORD, B.: "Trucks, Knives, Bombs, Whatever:" Exploring Pro-Islamic State Instructional Material on Telegram. CTC Sentinel, 2018. Vol. 11. No. 5. 25. o.

terrorcselekményekhez. Alacsony technológiájú (low-tech) támadások: információ és útmutatás olyan akciókhoz, amelyekhez nem kell robbantószer (mint késsel, gépjárművel elkövetett támadások, gyújtogatás, vonatkisiklatás etc.). Műveleti biztonság és kiberbiztonság: információ a lebukás elkerüléséről, és az elfogás kockázatának csökkentéséről terrorcselekmények elkövetése esetén; instrukciók az online aktivitás megfigyelésének elkerüléséhez, köztük a titkosítást maximalizáló alkalmazások és szolgáltatások installálásáról, mint VPN-ek, anonim böngészők, önmegsemmisítő programok, titkosított üzenetküldő alkalmazások és e-mail szolgáltatások etc.[240] Clifford és Powell 2017. június 1. és 2018. október 24. között 636 IS-t támogató angol nyelvű tartalmú csatornát vizsgált meg a Telegramon. Megállapították, hogy a Telegram továbbra is létfontosságú a terrorszervezet kommunikációs ökoszisztémájában. A platform funkcionális lehetőségei, és az alkalmazás használati feltételeinek relatíve laza betartatása miatt az IS szimpatizánsok számára a Telegram kiváló médium a kapcsolattartásra és tartalmak felfedezésére. Az angol nyelvű IS támogatók visszaélnek a Telegram lehetőségeivel és globális szinten kommunikálnak hasonlóan gondolkodókkal, hivatalos és nem hivatalos médiatermékeket terjesztenek és oktatóanyagot kínálnak. Az angolul beszélő IS támogatók a Telegramon komolyan veszik a műveleti biztonságot (operational security), de a nagyobb közönség elérése érdekében történő további támaszkodásuk a nem biztonságos nyilvános platformokra a műveleti biztonsági óvintézkedések következetlen alkalmazásával jár, és növeli a sebezhetőségüket. Az IS területének elvesztése és a nyilvános felületeken való jelenlétük elleni szigorú fellépés arra kényszeríti az angol nyelvű támogatókat, hogy a terrorszervezet katonai aktivitására koncentráljanak, biztosítsák a Telegramos hálózataik ellenálló képességét, kiegészítsék a hivatalos médiatermékeket nem hivatalosokkal, és hogy új módszereket fejlesszenek ki a műveletekhez való online útmutatáshoz. [241]

A Telegramon megtalálható többek közt az IS, az Al-Kaida, az al-Nuszra Front, a Hamasz, a Hezbollah és a tálibok.[242] Később újabb jelenségként tűnt fel az alkalmazáson a szélsőjobboldali terrorizmust támogató tartalmak fokozott megjelenése.[243]

---

[240] Uo. 25–26. o.

[241] CLIFFORD, B. – POWELL, H.: Encrypted Extremism: Inside the English-Speaking Islamic State Ecosystem on Telegram. Program on Extremism: The George Washington University, Washington D.C. 2019. 3. o.

[242] Terrorists on Telegram.

https://www.counterextremism.com/terrorists-on-telegram (2021.07.06.)

[243] HAYDEN, M. E.: Far-Right Extremists Are Calling for Terrorism on the Messaging App Telegram. Southern Poverty Law Center. (2019, June 27).

2015 decemberében James Comey, az FBI volt igazgatója, felszólította a felhasználók számára end-to-end encryption-t biztosító tech cégeket, hogy gondolják át az „üzleti modelljüket", és hagyjanak fel annak alkalmazásával.[244]

Oroszország és Irán próbálkozott a Telegram betiltásával,[245] azonban az sem Oroszországban[246], sem Iránban nem járt sikerrel.[247] Az orosz tiltási kísérlet ráadásul ellentétes hatást ért el: híressé tette az alkalmazást.[248] 2018-ban a Telegram szigorított – a hatóságoknak átadja felhasználók IP címét és telefonszámát, ha bírósági végzést kap arról, hogy a felhasználó terrorista gyanús.[249] 2019. november 21-22-én az Europol hágai központjában az Europol szélsőséges internetes tartalmakkal foglalkozó egysége (European Union Internet Referral Unit (EU IRU)) koordinálásával lezajlott az IS online propagandája elleni 16. Referral Action Day, melyhez 9 online szolgáltatást nyújtó, köztük a Telegram, Google, Files.fm, Twitter, Instagram és a Dropbox képviselői csatlakoztak.[250] Ennek az összehangolt akciónak a fókuszában az online terrorista

---

https://www.splcenter.org/hatewatch/2019/06/27/far-right-extremists-are-calling-terrorism-messaging-app-telegram (2021.07.06.)

[244] PAGANINI, P.: Islamic State launches the Kybernetiq magazine for cyber jihadists. Security Affairs. (2016, January 9).
http://securityaffairs.co/wordpress/43435/hacking/kybernetiq-magazine-cyber-jihad.html (2019.12.10.)

[245] KARASZ, P.: What Is Telegram, and Why Are Iran and Russia Trying to Ban It? The New York Times. (2018, May 2).
https://www.nytimes.com/2018/05/02/world/europe/telegram-iran-russia.html (2021.07.07.)

[246] KOLOMYCHENKO, M.: Russia tries more precise technology to block Telegram messenger. Reuters. (2018, August 30).
https://www.reuters.com/article/us-russia-telegram/russia-tries-more-precise-technology-to-block-telegram-messenger-idUSKCN1LF1ZZ (2021.07.07.)

[247] FAGHIHI, R.: Iran's conservatives return to Telegram after failed ban. Al-Monitor. (2018, November 28).
https://www.al-monitor.com/pulse/originals/2018/11/iran-telegram-ban-conservative-media-rejoin-tasnim-fars.html (2021.07.07.)

[248] PRINS, N.: An Analysis of the Russian Social Media Landscape in 2019. Linkfluence.
https://www.linkfluence.com/blog/russian-social-media-landscape (2021.07.07.)

[249] GHOSHAL, A.: Telegram's updated privacy terms make it unsafe for terrorists – but what about the rest of us? TNW. (2018, August 30).
https://thenextweb.com/insider/2018/08/30/telegrams-updated-privacy-terms-make-it-unsafe-for-terrorists-but-what-about-the-rest-of-us/?fbclid=IwAR1Zw6___iJIO82DQpA6U75Pg-OPzmdvWfEOK1G04zSor_WxFs0ZNOd6-Ko (2021.07.07.)

[250] Referral Action Day Against Islamic State Online Terrorist Propaganda. Europol. (2019, November 22). https://www.europol.europa.eu/newsroom/news/referral-action-day-against-islamic-state-online-terrorist-propaganda (2021.07.07.)

tartalmak terjesztése volt, különös tekintettel a propaganda videókra, publikációkra, valamint terrorizmust és erőszakos extrémizmust támogató közösségi média felhasználói fiókokra. 2015 júliusa óta az Europol szélsőséges internetes tartalmakkal foglalkozó egysége együttműködik a bűnüldöző hatóságokkal és az online szolgáltatást nyújtókkal, a terroristák internettel való visszaélésének az EU Internet Forum keretirányelvben történő kezelése érdekében. A megelőző másfél évben az Europol együttműködött a Telegrammal a terroristák online aktivitása elleni fellépés érdekében. Az Europol sajtóközleménye szerint a Telegram komoly erőfeszítéseket tett a rossz szándékú tartalmak elleni fellépésre alkalmas technikai képességeinek megerősítésével, és azzal, hogy szoros partnerséget ápol nemzetközi szervezetekkel, mint az Europol.[251] Az Europol 2021-es jelentése szerint az online tevékenykedő dzsihadisták 2020-ban továbbra is küszködtek a hálózataik újjáépítésével, miután 2019-ben eltávolították őket a Telegramról. A dzsihadista propaganda változatos felületeken vált elszórttá, és egyértelmű igyekezet látszik az IS támogatóktól az irányba, hogy biztosítsák az IS üzeneteinek eljuttatását a célközönséghez.[252] Az IS online útkeresését bővebben az IS internethasználatáról szóló fejezetben tárgyalom.

A szkeptikus dzsihadista egyik alkalmazásban sem bízik meg teljesen, mivel a többségük nyugati fejlesztésű. 2013 februárjában a Global Islamic Media Front (GIMF) kifejlesztette az Asrar al-Darshah (Secrets of Chatting) nevű titkosító plugin alkalmazást, ami élő beszélgetések titkosítását teszi lehetővé üzenetküldő platformokon, mint a Paltalk, Google Chat, Yahoo, MSN és Pidgin.[253]

Az IS saját fejlesztésű titkosítással ellátott chat alkalmazása az Alrawi.[254]

A TrueCrypt biztonságos kommunikációs alkalmazást 2004-ben indította útjára a programozó és bűnöző Paul Le Roux. Az IS titkosított kommunikációra és fájlmegosztásra használja.[255]

A RocketChat egy nyílt-forrású üzenetküldő szolgáltatás, mely elérhető okostelefonról

---

251 Europol and Telegram Take On Terrorist Propaganda Online. Europol. (2019, November 25). https://www.europol.europa.eu/newsroom/news/europol-and-telegram-take-terrorist-propaganda-online (2021.07.07.)

252 European Union Terrorism Situation and Trend report (TE-SAT) 2021. Europol, 2021. 8. o. https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-2021-tesat (2021.09.07.)

253 ALKHOURI – KASSIRER: i.m. 7-8. o.

254 CONSTINE, J.: ISIS Has Its Own Encrypted Chat App. TechCrunch. (2016, January 16). https://techcrunch.com/2016/01/16/isis-app/?guccounter=2 (2021.07.07.)

255 WEIMANN (2016): i.m. 42. o.

és PC-ről is, 2018. december közepe óta pedig IS csatornák is megtalálhatóak rajta. A Nashir News Agency és sok más IS-hez köthető média csoport a támogatókat sürgette az applikációhoz való csatlakozásra.

A Yahoo Together egy mobilos üzenetküldő alkalmazás, terroristák által kedvelt.

A Vibert az utóbbi időkben a terroristák fokozottan használják.

A Discord egy üzenetküldő applikáció videojátékosoknak, több mint 130 millió regisztrált felhasználóval rendelkezik, a platform a chat közösségeit szerverekre osztja, és IS-barát szerverek is találhatók rajta, például az „Al Bagdadi" vagy „dawlatulislambiqiyah".

Korábban az IS próbálkozott a Riot és TamTam platformokkal is, de ezek a cégek gyorsan reagáltak ellenük, ezért felhagytak a használatukkal.

Az üzenetküldő cégek gyors reakciója vagy padig közömbössége határozza meg, hogy hova „migrálnak" a terrorista csoportok. [256]

Al-Khabir al-Taqni, egy dzsihadista-támogató és önjelölt biztonsági szakértő a Twitteren 33 okostelefonos üzenetküldő alkalmazást rangsorolt biztonságosság szempontjából, mint nem biztonságos, mérsékelten biztonságos, biztonságos és legbiztonságosabb.[257]

3. Propaganda alkalmazások

Az IS és más terrorszervezetek saját propaganda alkalmazásokat is fejlesztettek.

Az Amaq médiaegységhez köthető The A'maq Agency az egyik első dzsihadista fejlesztésű okostelefonos alkalmazás, mely az IS támogatóknak hírekkel és harctéri videókkal szolgál. Az Al-Bayan Radio applikáció az IS hivatalos rádió állomása. Ezzel az alkalmazással Korán felolvasások, radikális előadások, és IS hadműveletekkel kapcsolatos bejelentéseket hallgathatóak.

Az afgán tálibokhoz köthető a hírek, jelentések, bejelentések, cikkek és videók nézését lehetővé tevő 2016. április 1-én útjára indított Voice of Jihad alkalmazás.

Az IS dzsihadista témájú, gyerekeknek készült Ábécé alkalmazása az arab betűket tanítja meg.[258] A 2016. május 10-én megjelent alkalmazásban többek közt kezdőbetűket

---

[256] KATZ, R.: A Growing Frontier for Terrorist Groups: Unsuspecting Chat Apps. Wired. (2019, September 1). https://www.wired.com/story/terrorist-groups-prey-on-unsuspecting-chat-apps/?fbclid=IwAR3d9byhbjIhYKMka_7bSRRF2FmXhLamDuQhSOV_2XC3cQnvSZmOYqF0_Xo (2021.07.07.)

[257] KATZ, R.: Almost Any Messaging App Will Do—If You're ISIS. Vice. (2016, July 14). https://www.vice.com/en/article/kb7n4a/isis-messaging-apps (2021.07.07.)

[258] ALKHOURI – KASSIRER: i.m. 7–9. o.

lehet társítani különböző erőszakos ábrákhoz, pl. rakétához, puskához, tankhoz.[259] Az applikáció neve „Huroof", az IS „Zeal Hivatala" jelentetette meg. A „Hivatal" sajtóközleménye szerint az „megtanítja az oroszlánkölyköknek az ábécé betűit". Az IS oroszlánkölyöknek nevezi a gyermekeket, a felnőtt terroristákat pedig oroszlánoknak.[260]

Az IS 2013-ban indította útjára a Dawn of Glad Tidings alkalmazását, mely a terroristák számára a résztvevő twitteres felhasználói fiókokból tweetek tízezreinek küldését tette lehetővé, ezáltal pedig a twitteres közösségi média kampány magas szintű szervezését.[261] Ha valaki letölti az alkalmazást, az IS a felhasználó nagy mennyiségű személyes adatához kér hozzáférést. Miután megtörtént a regisztráció, az applikáció olyan tweeteket tesz közzé a feliratkozó fiókján keresztül, amelyek tartalmáról egy a IS-es közösségi média-felelős dönt. Ugyanazt a tartalmat tweeteli minden feliratkozó, olyan gyakorisággal, hogy az alkalmazás ki tudja kerülni a Twitter spam-szűrő algoritmusait. A használó fiókja ezen kívül teljesen használható marad.[262]

A terroristák nem csupán saját fejlesztésű alkalmazásaikat használják propaganda célokra: Weiss és Hassan szerint az IS használja a Zellót, egy számítógéphez és okostelefonokhoz fejlesztett hangfájlokat megosztó titkosított közösségi média alkalmazást, mely népszerű a célközönsége körében. Gyakorlatilag adóvevővé változtatja az okostelefont, lehetővé téve hitszónokok beszédeinek diszkrét hallgatását.[263]

„A generációelmélettel foglalkozó kutatók, az 1995-2010, évek között születetteket tekintik egy új generációnak, mégpedig egy digitális generációnak, akik már az információs társadalom digitalizált világában nőttek fel (…)." Ők a Z generáció.[264]

---

[259] KATZ, R.: ISIS's Mobile App Developers Are in Crisis Mode. Vice. (2016, June 3). https://www.vice.com/en/article/qkj34q/isis-mobile-app-developers-are-in-crisis-mode (2021.07.07.)

[260] REISINGER, D.: ISIS Has Launched A Mobile App—For Children. Fortune. (2016, May 11). http://fortune.com/2016/05/11/isis-mobile-app-children/ (2021.07.07.)

[261] MOHAMEDOU, M-M. O.: A Theory of ISIS: Political Violence and the Transformation of the Global Order. Pluto Press, London, 2018. 205. o.

[262] BERGER, J. M.: How ISIS Games Twitter. The Atlantic. (2014, June 16). ttps://www.theatlantic.com/international/archive/2014/06/isis-iraq-twitter-social-media-strategy/372856/ (2021.11.29.)

[263] WEISS, M. – HASSAN, H.: Az Iszlám Állam: A terror hadserege belülről. HVG Kiadó Zrt., Budapest, 2015. 205–206. o.

[264] ZSIGOVITS L.: A Z generáció paradigmái a bűnüldözés és a bűnmegelőzés platformján. In: GAÁL Gy. – HAUTZINGER Z. (szerk.): Pécsi Határőr Tudományos Közlemények XXI.: A bűnüldözés és a bűnmegelőzés rendészettudományi tényezői. Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoportja, Pécs, 2019. 113. o.

A rövid videók megosztására alkalmas TikTok applikáció 2019 szeptemberében a legnépszerűbb nem játékos alkalmazás volt. Kifejezetten a Z generáció körében népszerű, használóinak harmada 18 év alatti. Az IS a TikTok-ot is használta toborzásra, mint propaganda eszközt. Az alkalmazásba fegyverekkel, halottakkal pózoló terroristákról szóló videókat, és IS dalokat töltöttek fel. Néhány videó kifejezetten a potenciális terroristákat célozta meg. A videók között fiatal lányokat megcálzó is volt, melyek a „dzsihád szerető"(„jihad lover") kifejezést használták, és olyan nők szerepeltek bennük, akik „dzsihádistának és büszkének" („jihadist and proud") vallották magukat. A videók filterekkel és szívecskékkel is el voltak látva, használva a TikTok lehetőségeit. Az applikációról két tucat felhasználói fiókot távolítottak el. A TikTok közösségi politikája kifejezetten tiltja a terrorizmus promótálását, és ki is jelenti, hogy tiltásra kerülnek a terrorszervezetek és más szervezett bűnözői elemek. A TikTok gyorsan fellép az ellentmondásos tartalmakkal szemben, azokat cenzúrázva. Az alkalmazás több ezer tartalom moderátort foglalkoztat Kínában és az USA-ban.[265]

2. A terrorista alkalmazások gyenge pontja?

Lényeges információ, hogy valamennyi terrorista-fejlesztésű alkalmazás kizárólag androidra készül. A fő különbség az iPhone és Android eszközök között, hogy az utóbbi lehetővé teszi felhasználói számára a kijelölt app store-on kívüli alkalmazások készítését és telepítését. Android applikációkat lehet készíteni és installálni függetlenül APK (Andoid application package) fájlokként, anélkül hogy valaha is a Google Play Store-ba kerülne. Ezt technika a „sideloading", mely megkönnyíti a hatóságok és önjelölt igazságosztók dolgát, mivel a Google Play-en és IOS store-on kívüli alkalmazásokba könnyebb álcázott malware-t helyezni és az IS támogatók közé beszivárogni. Gyakori védekezési módszer az ilyen megtévesztés ellen az egyénileg generált checksum file-ok által történő hitelesítés, amivel megállapítható, hogy az eredeti fájlon eszközöltek-e változtatást, de nem minden IS támogató él ezzel a biztonsági intézkedéssel.[266]

Mit lehet tenni a terroristák end-to-end encryption-nel ellátott alkalmazásokkal való visszaélésével szemben? A hatóságoknak a végpontoknál kell meghackelniük a

[265] MEISENZAHL, M.: ISIS is reportedly using popular Gen Z app TikTok as its newest recruitment tool. Business Insider. (2019, October 21).
https://www.businessinsider.com/isis-using-tiktok-to-target-teens-report-2019-10 (2021.07.07.)

[266] KATZ, R.: ISIS's Mobile App Developers Are in Crisis Mode. Vice. (2016, June 3).
https://www.vice.com/en/article/qkj34q/isis-mobile-app-developers-are-in-crisis-mode (2021.07.07.)

szoftvert, főleg 0day[267] igénybe vételével. Az end-to-end encryption feltörésével próbálkozni nem járható út. Továbbá a terroristák gyenge operációs biztonságát (opsec) kell kihasználni, például a nem elég erős jelszavak kitalálásával.[268]

Az IS aktivitása a web-alapú interneten megfigyelhető keresőrobotokkal és keresőmotorokkal, de a bűnüldöző hatóságoknak és titkosszolgálatoknak nehezebb dolga van a titkosított üzenetküldő alkalmazásokon lévő információk kinyerése tekintetében, pedig azok értékesek lehetnek a terrorcselekmények megelőzése és megakadályozása szempontjából.[269] Bodo és Speckhard egy IS-támogató Telegram felhasználók azonosítására irányuló kreatív módszerek felfedezésére irányuló kutatás során arra jutottak, hogy lehetséges behatolni a Telegramos IS chat szobákba, és azokon belül megtalálni a közösségi médiás felhasználói fiókokat, és OSINT alkalmazásával[270] az IS támogatók személyazonosságát felfedni. Közülük legtöbben az IS instrukciói ellenére sem teszik meg a megfelelő óvintézkedéseket, mint VPN vagy Proxy hálózat használata. A módszer még a Telegram Secret Chat-jében is működik.[271]

3. Következtetések

Ahogy Moutot rámutat, az okostelefon a terroristák kezében ugyan komoly „fegyver" lehet, viszont az a titkosszolgálatok számára is egy eszköz a lekövetésükre, így az „kétélű kard" a terroristák kezében.[272]

A terroristák által használt okostelefonos applikációk, továbbá az általuk frekventált online platformok és virtuális terek mind olyan felületek, amelyek lehetőséget adnak információszerzésre, felderítésre, leplezett eszközök használatára, terror-elhárítási

[267] 0day egy a szoftver szolgáltatója és antivírus szolgáltatója előtt is ismeretlen sebezhetőséget megcélzó kibertámadás. A 0day sebezhetőségeknek piaca is van, szervezetek fizetnek kutatóknak, akik felfedeznek ilyen sebezhetőségeket. Van fehér, szürke és fekete piaca a 0day sebezhetőségeknek. Zero-day (0day) exploit. https://www.imperva.com/learn/application-security/zero-day-exploit/ (2021.07.07.)

[268] GRAHAM, R.: How Terrorists Use Encryption. CTC Sentinel, 2016. Vol. 9. No. 6. 25. o.

[269] BODO, L. – SPECKHARD, A.: Identifying Nefarious Telegram Users without the Help of Telegram Itself: Testing Solutions for Intelligence and Security Professionals in Fighting ISIS in the Encrypted Social Media Space. International Center for the Study of Violent Extremism, London, 2017. 2–3. o.

[270] BODO – SPECKHARD: i.m. 6. o.

[271] Uo. 10–11. o.

[272] MOUTOT, M.: Smartphones: a double-edged sword for terrorists. Phys.org. (2018, November 13). https://phys.org/news/2018-11-smartphones-double-edged-sword-terrorists.html (2021.07.07.)

célból[273], továbbá fedett ügynökök terroristák közé történő beépülésére és ezáltal terrorcselekmények elkövetésének és toborzás megakadályozására A terroristákhoz kötődő alkalmazásokat fel kell törni, továbbá megfigyelő malware-ekkel ellátott hamis terrorista alkalmazásokat szükséges fejleszteni[274], ezek használatával terroristák közé beszivárogni és ezáltal terrorcselekményeket megelőzni.[275] Véleményem szerint a hatékony terrorizmus elleni harchoz, minél több terrorcselekmény megelőzéshez és a terrorizmus fenyegetésének visszaszorításához hozzájárul a terroristák által használt okostelefonos alkalmazások beható és naprakész ismerete. A téma kevés hazai szakirodalommal rendelkezik, az több kutatást érdemelne.

[273] FINSZTER G.: Szabályozott felderítés – titkosított büntetőeljárás. Miskolci Jogi Szemle, 2019/2. különsz. 280–281. o.

[274] KATZ, R.: Almost Any Messaging App Will Do—If You're ISIS. Vice. (2016, July 14). https://www.vice.com/en/article/kb7n4a/isis-messaging-apps (2021.07.07.)

[275] SERBAKOV M. T.: Az online felületek és okostelefonos alkalmazások, mint a terrorcselekmények előrejelző rendszerei. In: GAÁL Gy. – HAUTZINGER Z. (szerk.): Pécsi Határőr Tudományos Közlemények XXI.: A bűnüldözés és a bűnmegelőzés rendészettudományi tényezői. Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoportja, Pécs, 2019. 124. o.

VIII. A TERRORIZMUS FINANSZÍROZÁSÁNAK INTERNETHEZ KÖTŐDŐ TECHNIKÁI ÉS FORRÁSAI[276]

1. A terrorizmus finanszírozás alapvetéseiről, röviden

A terrorizmus finanszírozását Gál a következőképp határozza meg: „A terrorizmus finanszírozása azt a tevékenységet jelenti, amelynek során közvetve vagy közvetlenül terrortámadások megvalósításához anyagi eszközöket bocsátanak rendelkezésre."[277]

Gál a terrorizmus költségeit két oldalra osztja: a terroristák (finanszírozási igény) és a társadalom oldalára (károk és áldozatok). Rávilágít a terrorizmusnak a téma szempontjából talán legfontosabb jellemezőjére: hogy az egyes támadások elkövetéséhez nincs szükség sok pénzre. Az akciók kivitelezéséhez szükséges költségek három nagy csoportra oszthatók: műveleti költségek, az adminisztratív költségek és a merénylők családtagjainak adott dotáció.[278]

Powell, az USA volt külügyminisztere a pénzt a „terrorizmus oxigénjének" nevezte.[279] Azonban ahogy már szó esett róla, az egyes terrortámadásoknak a végrehajtása relatíve olcsó.[280] Rendkívül pusztító támadások is végrehajthatóak nagyon kicsi összegekből is.[281] Tálas a terrorizmus finanszírozása elleni küzdelem korlátaira figyelmeztet, arra, hogy az új típusú terrorizmust képviselő terroristák merényleteinek szervezése és végrehajtása viszonylag olcsó, és számos szakértő szerint a terrorcselekmények finanszírozásához szükséges pénzügyi tranzakcióknál e terrorcsoportok könnyen meg tudják kerülni és valószínűleg meg is kerülik a „hivatalos és követhető" csatornákat.[282]

---

[276] A „terrorizmus finanszírozásának forrásai és technikái" Gál szóhasználata. Lásd: GÁL I. L.: A terrorizmus finanszírozásának fogalma és technikái a XXI. században. Szakmai Szemle, 2016/2. 91. o.

[277] GÁL I. L.: A tőkepiac büntetőjogi védelme Magyarországon. Kódex Nyomda Kft, Pécs, 2019. 153. o.

[278] Uo.152–153. o.

[279] Remarks On Financial Aspects of Terrorism at Office of Financial Crimes Enforcement Network. U.S. Department of State Archive. https://2001-2009.state.gov/secretary/former/powell/remarks/2001/5979.htm (2021.09.12.)

[280] GÁL I. L.: A terrorizmus finanszírozásának fogalma és technikái a XXI. században. Szakmai Szemle, 2016/2. 94. o.

[281] BARADARAN, S. – FINDLEY, M. – NIELSON, D. – SHARMAN, J.: Funding Terror. University of Pennsylvania Law Review, 2014. Vol. 162. No. 3. 481. o.

[282] TÁLAS P.: Kelet-Közép-Európa és az új típusú terrorizmus. In: TÁLAS Péter (szerk.): A terrorizmus anatómiája. Zrínyi Kiadó, Budapest, 2006. 19–20. o.

Az Europol 2019-es Terrorism Situation and Trend Reportja (továbbiakban TE-SAT) szerint 2018-ban az EU-tagállamokban elkövetett terrorcselekmények többségének elkövetéséhez semennyi, vagy csak minimális finanszírozásra volt szükség, és azok előkészítésükben és végrehajtásukban is kifinomulatlanok voltak. A jelentés szerint az elkövetők különböző módokon, nyomok hagyása nélkül tudták az akciókhoz szükséges anyagi forrásokat biztosítani. Amikor külső anyagi forrásokra van szükségük, a terroristák különféle módszerekhez folyamodnak, melyek az egyszerűtől a rendkívül összetettig terjednek.[283] A 2020-as TE-SAT rávilágít, hogy a magányos terroristák, a kis sejtek és az idegen terrorista harcosok pénzügyi igényei kicsik, és általában tudják magukat és a tevékenységeiket finanszírozni legitim forrásokból is, esetleg csalások vagy kisebb bűncselekmények elkövetéséből.[284] Az utóbbi években jellemző kezdetleges módszerekkel elkövetett támadásokhoz nincs szükség finanszírozásra, ezeket tehát nem lehet úgy megakadályozni, hogy a terroristát elvágjuk finanszírozási forrásaitól, más szavakkal, terrorizmus finanszírozás elleni eszközökkel az ilyen akciók nem megelőzhetőek.

Az ilyen támadások megelőzése szempontjából a büntetőjogi eszközök is szinte hatástalanok: „(…) a terrorizmus finanszírozásával szemben a büntetőjogi eszközök hatékonysága a nullához konvergál."[285] Az elmúlt évek nagyobb terrortámadásainak tapasztalata alapján 8-10.000 USD-ből már komoly akció hajtható végre. Egy ilyen összeget egy 4-5 fős önfinanszírozó sejt 2-3 év alatt bármelyik fejlett, vagy közepesen fejlett országban bármilyen legális munkával meg tud takarítani, így képes támadást végrehajtani, más külső források, a külső finanszírozásán szüksége nélkül. Ezért a pusztán büntetőjogi eszközrendszerre támaszkodó küzdelem nem lehet hatékony a terrorizmus finanszírozása ellen.[286]

Maga a terrortámadás olcsó, de egy terrorszervezet működéséhez nagy költségvetés szükséges. A toborzás, edzőtáborok, a szállásolás, a fegyverek etc. mind pénzbe kerülnek. Szükség lehet még pénzre hivatalos személyek megvesztegetéséhez is, és sok

[283] European Union Terrorism Situation and Trend Report (TE-SAT) 2019. Europol, 2019. 17. o. https://www.europol.europa.eu/activities-services/main-reports/terrorism-situation-and-trend-report-2019-te-sat (2021.09.12.)

[284] European Union Terrorism Situation and Trend report (TE-SAT) 2020. Europol, 2020. 22. o. https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-te-sat-2020 (2021.09.12.)

[285] GÁL I. L.: Új biztonságpolitikai kihívás a XXI. században: a terrorizmus finanszírozása. Szakmai Szemle, 2012/1. 15. o.

[286] Uo. 15. o.

csoport illetményt fizet a „visszavonult” tagoknak és a halott terroristák vagy öngyilkos merénylők családjainak is. Egy nagyobb és aktívabb terrorszervezet költségvetése az évi több száz millió dollárt is elérheti.[287] Egyetértek Gállal, mi szerint a terroristákat nagyon nehéz elvágni anyagi forrásaiktól, de van értelme próbálkozni, mert az a terrorszervezet, amelyik nem jut elég pénzhez a működési költségeihez, lassan elsorvad.[288]

A CIA becslései szerint az al-Kaida fenntartása évente körülbelül 30 millió USD-be került, amit majdnem csupán donációkból gyűjtött össze.[289] 9/11 az al-Kaidának körülbelül 400.000-500.000 USD-ba került, melyből megközelítőleg 300.000 USD érkezett átutalás formájában a 19 eltérítő USA-beli bankszámláira.[290] A közhiedelemmel ellentétben bin Laden az al-Kaidát nem a személyes vagyonán vagy üzletek hálózatával támogatta, hanem a pénzügyi előadók anyagi forrásokhoz tudatosan és nem tudatosan adakozó donoroktól, mecsetektől, szimpatizáló imámoktól és NGO-któl, mint például alapítványoktól jutottak hozzá.[291]

2. A terrorizmus finanszírozás technikái és forrásai

A terroristák finanszírozási forrásait illetően az általam legrelevánsabbnak tartott szakirodalmi felosztások a következők:

Gál felosztásában a terrorizmus finanszírozásának forrásai és technikái: bűncselekmények elkövetése, adományok és törvényes üzleti tevékenység.[292] Sieber és Vogel egy további forrást ad az előbbiekhez. A szerzőpáros szerint a terrorszervezetek finanszírozási forrásai: a donációk, bűncselekmények, prima facie legális üzleti tevékenység vállalkozások segítségével, továbbá egy terület

[287] FREEMAN, M.: The Sources of Terrorist Financing: Theory and Typology. Studies in Conflict and Terrorism, 2011. Vol. 34. No. 6. 462. o.

[288] GÁL I. L.: A terrorizmus finanszírozása. PTE Állam- és Jogtudományi Kar Gazdasági Büntetőjogi Kutatóintézet, Pécs, 2010. 11–12. o.

[289] ROTH, J. – GREENBURG, D. – WILLE, S.: National Commission on Terrorist Attacks Upon the United States: Monograph on Terrorist Financing: Staff Report to the Commission. National Commission on Terrorist Attacks upon the United States, Washington D.C., 2004. 19. o.

[290] Uo. 13. o.

[291] Uo. 17. o.

[292] GÁL I. L.: Bejelentés vagy feljelentés? : A pénzmosás és a terrorizmus finanszírozása elleni küzdelemmel kapcsolatos feladatok és kötelezettségek. Penta Unió, Pécs, 2009. 169–171. o.

kontrollálásából származó bevétel.[293]

Freeman a terroristák finanszírozásának forrásait négy általános kategóriába sorolja: állami támogatás, illegális tevékenységeket, legális tevékenységek és népi támogatás. Az állami támogatás sokkal gyakoribb volt a hidegháború idején, azóta jelentősége nagymértékben csökkent. Az illegális tevékenységek általi jövedelemszerzésbe beletartozik a zsarolás vagy „forradalmi adók", emberrablás és a váltságdíj, lopás, csempészés, kisebb bűncselekmények elkövetése, kalózkodás és áruk hamísítása. A terroristák gyakran végeznek legális üzleti tevékenységet, pénzszerzés céljából. Finanszírozási formaként sok terrorista csoport támaszkodik a szimpatizáló népesség támogatására. Ebbe beletartoznak a jótékonysági adományok, a külföldön élő szimpatizáló diaszpóra közösségek pénzére való támaszkodás, és a tagdíjak is.[294]

Clunan szerint terroristák bevételhez jutnak jogellenes tevékenységek által, mint kábítószer-kereskedelem, emberkereskedelem, fegyverkereskedelem, csempészet, emberrablás, rablás, gyújtogatás, melyek kompatibilisek a tradícionális pénzmosási eszközökkel is. Clunan rámutat, hogy a terroristák pénzt szereznek még legitim humanitárius és üzleti tevékenységből is. Jótékonysági szervezetek, amelyek pénzt gyűjtenek háború sújtotta társadalmak humanitárius segélyeire, nem mindig vannak tudatában, hogy a befolyt összegek terrorizmust finanszíroznak. Jótékonyságoknál dolgozó korrupt egyének vagy a kedvezményezett szervezetek is elterelhetik a pénzösszegeket terrorszervezetek felé.[295]

Bell a terrorizmus finanszírozásának négy forrását sorolja: szimpatizánsoktól érkező hozzájárulás, bűncselekményekből származó bevétel, legális üzleti tevékenységből származó jövedelem, és egy idegen kormány támogatásából származó jövedelem. Bell szerint az előbbi négy forrás elméletben négy különböző terrorizmus finanszírozási modell létezését sugallhatja, melyek a következők: a népi támogatásos modell/Popular Support model (ahol a támogatás donációkból érkezik), a bűncselekményekből származó bevételi modell/Criminal Proceeds model (ahol a bevétel bűnözésből származik), a vállalkozói modell/Entrepreneurial model (ahol cégek generálják a bevételt) és az állami támogatásos modell/State Sponsor model (ahol a pénzügyi támogatás idegen államtól érkezik). Bell hozzáteszi, hogy ez a csoportosítás túlegyszerűsítő és félrevezető, mert

[293] SIEBER, U. – VOGEL, B.: Terrorismusfinanzierung: Prävention im Spannungsfeld von internationalen Vorgaben und nationalem Tatstrafrecht. Duncker & Humblot, Berlin, 2015. 10. o.

[294] FREEMAN: i.m. 465–470. o.

[295] CLUNAN, A. L.: The fight against terrorist financing. Political Science Quarterly, 2006. Vol. 121. No. 4. 570. o.

egy kifinomultabb modell, ahol a finanszírozás több forrásból származik, és ahol a lehetőség a fő tényező, ami befolyásolja egy adott csoport finanszírozási forrásainak kombinációját, realisztikusabb megközelítés.[296]

A különböző terroristák finanszírozás forrásai között eltérések mutatkoznak. Az idegen terrorista harcosok finanszírozási forrásai és annak mértéke különbözni fog a nagyobb terrorszervezetekhez képest.[297]

A Pénzügyi Akciócsoport (Financial Action Task Force, a továbbiakban FATF) a legfontosabb nemzetközi standard-meghatározó a pénzmosás elleni és a terrorizmus finanszírozása elleni küzdelem terén.[298] A 1989-es párizsi G-7 csúcstalálkozón hívták életre.[299] Jelenleg 37 tagországból és 2 regionális szervezetből áll.[300] A 2015-ös „Emerging Terrorist Financing Risks" FATF jelentés felosztásában a hagyományos terrorizmus finanszírozási módszerek és technikák a következők: a magándonációk, a non-profit szervezetekkel történő visszaélés, ezek rossz célra történő használata, bűnözői tevékenységből származó bevétel, a helyi és diaszpóra lakosságok és cégek zsarolása, emberrablás és váltságdíj, önfinanszírozás, legitim üzleti tevékenység,és a terrorizmus állami szponzorálása.[301] Az előbbi módszerek és technikák napjainkban is elterjedtek és továbbra is jelentős kockázatot jelentenek.[302] A FATF jelentés szerint „előretörő terrorizmus finanszírozási fenyegetések és sebezhetőségek": az idegen terrorista harcosok, adománygyűjtés a közösségi médián keresztül, új fizetési termékek és szolgáltatások (virtuális fizetőeszközök, előre fizetett/prepaid kártyák, internet-alapú fizetési szolgáltatások), és a természeti erőforrások kizsákmányolása (olaj és gázszektor, bányászati szektor).[303] A FATF szerint a terroristák interneten végzett toborzása gyakran

[296] BELL, R. E.: The Confiscation, Forfeiture and Disruption of Terrorist Finances. Journal of Money Laundering Control, 2003. Vol. 7. No. 2. 106–107. o.

[297] FATF REPORT: Terrorist Financing Risk Assessment Guidance. FATF, Párizs, 2019. 30. o. http://www.fatf-gafi.org/media/fatf/documents/reports/Terrorist-Financing-Risk-Assessment-Guidance.pdf (2021.09.12.)

[298] BERGSTRÖM, M.: The Global AML Regime and the EU AML Directives: Prevention and Control. In: KING, C. – WALKER, C. – GURULÉ, J. (szerk.): The Palgrave Handbook of Criminal and Terrorism Financing Law. Palgrave Macmillan, London, 2018. 35. o.

[299] History of the FATF. FATF. https://www.fatf-gafi.org/about/historyofthefatf/ (2021.09.12.)

[300] FATF Members and Observers. FATF. https://www.fatf-gafi.org/about/membersandobservers/ (2021.09.12.)

[301] FATF REPORT: Emerging Terrorist Financing Risks. FATF, Párizs, 2015. 13–20. o. https://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf (2021.09.12.)

[302] Uo. 23. o.

[303] Uo. 24–42. o.

nagyon szorosan kapcsolódik a pénzügyi támogatás iránti felhívásaikhoz.[304]Acharya találóan fogalmaz a terrorizmus finanszírozásának adaptív természetéről: „Ha ma a terrorizmus szívében a radikális ideológia és extrémizmus található, a finanszírozás annak az éltető vére. Az úgynevezett „új terrorizmus" fenyegetése nem csupán a terroristák által használható fegyverekben rejlik, hanem az arra való képességükben is, hogy ezeket a fegyvereket innovatív, diszkrét és komplex adománygyűjtési és pénzátutalási technikákon keresztül megszerezzék és használják. Mint bármely kereskedelmi vállalkozás, a finanszírozáshoz és az átutalás módjaihoz való hozzáférés kritikus a terrorszervezetek fenntartásához, és létfontosságú a tevékenységeik előkészítéséhez és kivitelezéséhez."[305]

3. A terrorizmus finanszírozásának internethez kötődő technikái és forrásai

1. Terrorizmus finanszírozás online kiskereskedők és piacok használatával

Terroristák olyan online kiskereskedőket és piacokat is felhasználnak szervezeti igényeik és műveleti tevékenységeikhez szükséges javak és alapanyagok beszerzésére, mint az Amazon, eBay, Alibaba és más regionálisan specifikus platformok. E felületeken a támadásaikhoz szükséges fegyvereket és alkatrészeket is be szokták beszerezni. Ezeket a felületeken sokszor propagandatermékek és különböző áruk eladásával gyűjtenek anyagi forrásokat, ezáltal kisebb összegekhez jutnak, miközben üzenetüket is terjesztik. Davis úgy véli, a legtöbb ilyen tevékenység inkább egyének és sejtek támogatását szolgálja, mintsem nagyobb terrorszervezetekét, és valószínűleg az ilyen bevételeket inkább a napi megélhetésre költik, mint közvetlenül terrortámadásokra. Példaként hozható az amerikai bázisú neonáci szélsőséges csoport, az Atomwaffen Division, melynek tagjai könyvek árusításával, főleg a „Siege" című mű az Amazon CreateSpace felületén történő eladásával gyűjtöttek pénzt. A „Siege" az USA-beli neonáci, James Mason esszéinek gyűjteménye, és az Atomwaffen ideológiai sarokköve.

[304] FATF REPORT: Financing of Recruitment for Terrorist Purposes. FATF, Párizs, 2018. 4. o. https://www.fatf-gafi.org/media/fatf/documents/reports/Financing-Recruitment-for-Terrorism.pdf (2021.09.12.)

[305] ACHARYA, A.: Targeting Terrorist Financing: International Cooperation and New Regimes. Routledge, London and New York, 2009. 7. o.

A terroristák és extrémisták számára a propaganda árusítása valószínűleg nem generál jelentős profitot, de mégis jelent egy kis bevételi forrást, és hasonlóan gondolkodók laza hálózatait is kialakítja, és lehetővé teszi a potenciális újoncoknak a propagandához való hozzáférést is. Online kiskereskedőket és piacokat terrorszervezetek és hozzájuk köthető személyek zsákmányolt dolgok eladására is használták már. Például az IS területén zsákmányolt antikvitásokat kínáltak eladásra az eBay-en és Facebook-on, de adtak el régiségeket a Skype, WhatsApp vagy a Kik üzenetküldő szolgáltatások használatával is. Az IS hasznot húzott ezek értékesítéséből, úgy hogy azokat a forrásnál megadóztatta, és úgy is, hogy a zsákmányolt antikvitásokat közvetítőknek értékesítette. Davis szerint valószínűtlen, hogy a terrorszervezet ezek közvetlen online értékesítését végezte volna.[306]

2. Adománygyűjtés és közösségi finanszírozás a közösségi médián

A terroristák visszaélve az internet hozzáférhetőségével, anonimitásával és a közösségi média gyors terhedésével szimpatizánsaiktól globális szinten gyűjtenek adományokat. Ezt a jelenséget a FATF növekvő terrorizmus finanszírozási fenyegetésnek tartja. A terrorszervezetek a közösségi hálón propagandájukat terjesztése mellett adománygyűjtő kampányokat is szerveznek. P2P horizontális kommunikációval (mint a Facebook, Twitter, Instagram etc. használatával) széles közönséget tudnak elérni, mely kommunikáció néha okostelefonos üzenetküldő alkalmazásokon folytatódik (mint a WhatsApp vagy Viber), és ezeknél is biztonságosabb kommunikációs hálózatokon (mint a Surespot). Növekvő terrorizmus finanszírozási kockázat a terroristák közösségi finanszírozás (crowdfunding) használata is.[307] „A közösségi finanszírozás alapvető gondolata külső finanszírozás gyűjtése egy nagy közönségtől (a tömegtől, crowd), ahol minden egyes egyén egy nagyon kicsi összeget ad, ahelyett hogy tapasztalt befektetők egy kis csoportjától kérnének."[308]

[306] DAVIS, J.: New Technologies but Old Methods in Terrorism Financing. Royal United Services Institute for Defence and Security Studies, London, 2020. 1. o. https://static1.squarespace.com/static/5e399e8c6e9872149fc4a041/t/60b0ab3b05f173456658076b/1622190920308/New+Technologies+but+Old+Methods+in+TF.pdf (2021.09.12.)

[307] FATF REPORT (2015): i.m. 30–31. o.

[308] „The basic idea of crowdfunding is to raise external finance from a large audience (the "crowd"), where each individual provides a very small amount, instead of soliciting a small group of sophisticated investors." Saját fordítás. BELLEFLAMME, P. – LAMBERT, T. – SCHWIENBACHER, A.:

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.[309]

A terrorizmus finanszírozás a közösségi medián számos formát tud ölteni. Az adakozók néha nincsenek is tudatában, hogy terroristákat finanszíroznak, mivel terroristák adománygyűjtést hamis jótékonysági kampányokkal is folytatnak, amelyek esetében az adományozók azt hiszik, hogy humanitárius célokra adakoznak. A terroristák és a támogatóik a potenciális finanszírozókat komunikációs platformok felé irányítják. A hatósági megfigyelés előli rejtőzködés érdekében a terroristák az adakozókat titkosítással ellátott okostelefonos alkalmazások használatára buzdítják, ezzel is nehezítve a terrorizmus finanszírozása elleni harcot.[310]

Az adománygyűjtésről szóló hirdetéseket általában a közösségi hálón vagy tematikus oldalakon helyezik el, valamint specializált médián, zárt fórumokon és privát üzenetekben küldik őket. Hogy a adománygyűjtés valódi célját elfedjék, ezek a hirdetések általában nem tartalmaznak közvetlen hivatkozást a terrorizmus finanszírozására történő adománygyűjtésre, hanem kétértelmű nyelvezetet használnak, vagy a jótékonysági és humanitárius célokra való gyűjtés álcája mögé rejtőznek. Az adománygyűjtésre irányuló hirdetések és az azokhoz tartozó pénzügyi részletek szöveg helyett más formátumban is lehetnek (például képben, vagy videóban), ami lehetetlenné teszi azok felfedezését hagyományos keresőmotorokkal, és megnehezíti az ilyen hirdetéseket tartalmazó oldalak azonosítását, továbbá az ismert pénzügyi részletek segítségével az ilyen hirdetések megtalálását.[311]

2017 novemberében napvilágra került az al-Kaidával összeköttetésben álló Al-Sadaqah (önkéntes adakozás) nevű szervezet közösségi média kampánya a Facebook-on. A

Crowdfunding: tapping the right crowd. SSRN Electronic Journal, 2012. Vol. 29. No. 5. 1. o.

[309] 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 (2021.09.12.)

[310] YUEN, S.: It's not just Russia — terror financiers are also using social media propaganda. CNBC. (2018, January 1).
https://www.cnbc.com/2017/12/18/social-media-propaganda-terror-financiers-operate-on-internet.html (2021.09.12.)

[311] FATF REPORT (2015): i.m. 32. o.

felhasználói fiókjai hamar törlésre kerültek, de a szervezet folytatta a Bitcoin-os finanszírozás iránti kampányát egy Telegram-os csatornán, továbbá a Twitter-en is.[312] Felmerülhet a kérdés, hogy az adakozás miért játszik olyan jelentős szerepet a terrorizmus finanszírozásában. Az oka, hogy az alamizsna, a „zakat" az iszlám öt oszlopának egyike.[313] A zakat a hívő vagyona egy meghatározott hányadának a kötelező adakozása. Miközben a legtöbb ilyen jótékony adomány a muszlim világban a szegények támogatására szolgál és az iszlám vallás üzenete terjesztésére, ezeket főleg tehetős közel-keleti országokban dzsihád finanszírozására is felhasználták. Problematikus, hogy a valódi jótékonyság és a terrorizmust támogató között nehéz különbséget tenni.[314]

1) Új fizetési termékek és szolgáltatások

Az 2015-ös „Emerging Terrorist Financing Risks" FATF jelentés új fizetési termékek és szolgáltatásokként a virtuális fizetőeszközöket, az előre fizetett (prepaid) kártyákat, és az internet-alapú fizetési szolgáltatásokat sorolja fel.[315]

Ezen 2015-ös FATF jelentés szerint az elektronikus, online és új fizetési szolgáltatások egy sebezhetőséget jelentenek, ami rövidtávon növekedhet, ahogy ezek a rendszerek általános használata fokozódik. Az új fizetési termékek és szolgáltatások nagy része globális szinten elérhető és felhasználható pénzösszegek gyors átutalására. 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. Ez a technológia pénzeszközök anonim átutalását teszi lehetővé nemzetközi szinten, melyek során ugyan a fizetőeszköz eredeti vásárlása látható lehet (pl. a bankrendszeren keresztül), de a virtuális fizetőeszköz összes ezt

[312] MALIK, N.: Terror in The Dark: How Terrorists use Encryption, the Darknet and Cryptocurrencies. The Henry Jackson Society, London, 2018. 41. o.

[313] ROTH, J. – GREENBURG, D. –WILLE, S.: National Commission on Terrorist Attacks Upon the United States: Monograph on Terrorist Financing: Staff Report to the Commission. National Commission on Terrorist Attacks upon the United States, Washington D.C., 2004. 21. o. https://govinfo.library.unt.edu/911/staff_statements/911_TerrFin_Monograph.pdf (2021.09.12.)

[314] KAPLAN, E.: Tracking Down Terrorist Financing. Council On Foreign Relations. (2006, April 4). https://www.cfr.org/backgrounder/tracking-down-terrorist-financing (2021.09.17.)

[315] FATF REPORT (2015): i.m. 35–38. o.

követő átutalását nehéz nyomon követni.[316]

2) Virtuális fizetőeszközök

Mindenekelőtt fogalmilag el kell határolni egymástól a kriptovalutákat (cryptocurrencies), a virtuális fizetőeszközöket (virtual currencies) és a digitális fizetőeszközöket (digital currencies).

„A digitális fizetőeszköz az összes elektronikus pénz leírására használt általános kifejezés, amely magába foglalja mind a virtuális fizetőeszközt, mind a kriptovalutát. Az lehet szabályozott és nem szabályozott."[317] A virtuális fizetőeszköz: „A virtuális fizetőeszközök a digitális fizetőeszközök egy típusa, amelyeket általában az alkotóik kontrollálnak, és amelyeket egy adott virtuális közösség tagjai használnak és fogadnak el."[318] Minden virtuális fizetőeszköz digitális (csak online léteznek), de nem minden digitális fizetőeszköz virtuális, mert azok egy adott virtuális környezeten kívül léteznek. A „kripto" a kriptovalutában arra utal, hogy sok titkosítási algoritmust és kriptográfiai technikát használnak a hálózat biztonságának biztosítására. Ez a biztonságossági szint a kriptovaluták hamisítását is megnehezíti.[319]

A kriptovaluta és az elektronikus pénz nem szinonimák.[320] A kriptovaluták esetében nincs jegybanki, vagy állami elfogadás: „azokat mindenki önként elfogadhatja olyan értéken, amennyiért akarja: csak a kereslet és kínálat határozza meg az árfolyamot, így a monetáris politika eszközrendszere sem működhet. A kriptovalutákat – bár pénz funkcióval bírnak – nem nevezhetjük törvényes fizetőeszköznek, azaz pénznek. Sok esetben a virtuális valutát és a kriptovalutákat egymás szinonimájaként használják. A virtuális valuta sokkal tágabb kör. A virtuális valuták digitális formában megjelenő, de állami szabályozás nélküli valuták. A kriptovaluták ezen belül képeznek egy csoportot, amelyeknek az a sajátos ismérvük, hogy kriptográfiai hitelesítő folyamatok – tipikusan blokklánc technológia – által lehet őket létrehozni."[321]

---

[316] Uo. 35. o.

[317] PEREZ, Y. B.: The differences between cryptocurrencies, virtual, and digital currencies. The Next Web. (2019, February 19).
https://thenextweb.com/hardfork/2019/02/19/the-differences-between-cryptocurrencies-virtual-and-digital-currencies/ (2020.09.12.)

[318] Uo.

[319] Uo.

[320] SIMON B.: A kriptovaluták és a kapcsolódó rendészeti kihívások. In: MEZEI Kitti (szerk.): A bűnügyi tudományok és az informatika. Pécsi Tudományegyetem Állam- és Jogtudományi Kar – MTA Társadalomtudományi Kutatóközpont, Budapest – Pécs, 2019. 169–186. o.

[321] Uo. 170. o.

Egyszerűen összefoglalva: „(…) a digitális fizetőeszköz az általános kifejezés az olyan pénzekre, amik kizárólagosan a digitális térben léteznek. A virtuális fizetőeszközök és kriptovaluták digitális fizetőeszközök, mert azok online léteznek. A virtuális fizetőeszközök a digitális fizetőeszközök egyik formája, amelyek a virtuális világban elérhetők (gondoljunk a fejlesztők által létrehozott online közösségekre). A kriptovaluták digitális fizetőeszközök, mert online léteznek, de azok kriptográfiai algoritmusok által létrehozott virtuális fizetőeszközök is."[322]

A NAV Központi Irányítás Pénzmosás Elleni Információs Iroda 2016-os éves jelentése a virtuális fizetőeszközöket a következőképp határozza meg: „Virtuális fizetőeszközök alatt alapvetően azokat a digitális térben létező fizetőeszközöket értjük, amelyek valamilyen matematikai-kriptográfiai mechanizmus alapján, decentralizált rendszerben működnek. Legismertebb képviselőjük a Bitcoin, azonban jelentős számú hasonló elven működő eszköz létezik."[323]

Az első működő kriptovaluta, a Bitcoin (BTC), mely a legnépszerűbb is, és az jelenti a technológiai és a funkcionális standardot is sok más kriptovaluta számára. Más népszerű kriptovaluták közé tartozik az Ethereum (ETH), Ripple (XRP), Litecoin (LTC), Bitcoin Cash (BCH), Dash (DASH), és a privacy coin-ok, köztük a ZCash (ZEC) és a Monero (XMR).[324]

A kriptovalutákhoz rendészeti kihívások is kapcsolódnak,[325] a gyakorlatban számos visszaélésre volt velük már példa.[326] A kriptobűncslekmények során okozott anyagi károk esetén meglepően nagy összegekről beszélhetünk: 2020 első öt hónapjában a kriptolopások, hackelések, és csalások által okozott kár összesen 1,36 milliárd USD összegre rúgott. A kriptobűncselekmények során ellopott összegek 2019-ben 4,5 milliárd USD összeget tettek ki.[327]

---

[322] PEREZ: i.m.

[323] Éves jelentés 2016. év. Nemzeti Adó- és Vámhivatal Központi Irányítás Pénzmosás Elleni Információs Iroda, 2016. 14. o.

[324] MCBRIDE, M. – GOLD, Z. – SCHRODEN, J. – FREY, L.: Cryptocurrency: Implications for Special Operations Forces. CNA, Arlington, 2019. 5. o. https://www.cna.org/CNA_files/PDF/CRM-2019-U-020186-Final.pdf (2021.09.12.)

[325] SIMON: i.m. 169–186. o.

[326] TÓTH D.: A virtuális pénzekkel kapcsolatos visszaélések. In: BARÁTH N. E. – MEZEI J. (szerk.): RENDÉSZET-TUDOMÁNY-AKTUALITÁSOK: A rendészettudomány a fiatal kutatók szemével. Doktoranduszok Országos Szövetsége, Rendészettudományi Osztálya, Budapest, 2019. 243. o.

[327] Cryptocurrency Crime and Anti-Money Laundering Report. CipherTrace, 2020. 6. o. https://ciphertrace.com/wp-content/uploads/2020/06/spring-2020-cryptocurrency-anti-money-laundering-

Az internetes pénzügyi tranzakciók száma növekszik. Tóth arra világít rá, hogy újabb típusú fizetési eszközök, virtuális fizetőeszközök jelennek meg, mint például a Bitcoin és a Litecoin, melyek jogi státusza nem tiszta. Az információs technika fejlődése ugyan könnyebbé tette a pénzügyi szolgáltatások használatát, de a technológia a bűnelkövetőknek egyre több lehetőséget ad a velük való visszaélésre.[328] Ezek a technológiák jellezmői kockázatokat jelentenek bűncselekmények, köztük pénzmosás és terrorizmus finanszírozás megkönnyítése szempontjából. Bizonyos virtuális fizetőeszközök határok nélküli, P2P természete a terroristáknak lehetőséget ad a szabályozott szektoron kívüli pénzátutalásra, kívül a pénzmosás elleni és a terrorizmus finanszírozása elleni hatóságok működési területén.[329]

A pénzmosás és a terrorizmus finanszírozás elleni harc, valamint a kriptovalutákkal történő adóelkerülés tekintetében hasonlóak a szabályozási kihívások: Az anonimitás akadályozza a kriptovalutás tranzakciók megfelelő felügyeletét, lehetővé téve kétes tranzakciók előfordulását a szabályozási kereteken kívül, mely lehetővé teszi bűnszervezetek számára, hogy kriptovaluták használatával könnyedén „tiszta pénzhez" jussanak. A kriptovaluták, kripto-piacok és kripto-játékosok természete határokon átnyúló, gyakran nincs olyan központi közvetítő, például kibocsátó, amely a szabályozás fókuszpontja lehetne. Nincsenek olyan szabályok, amelyek a kriptovalutákkal kapcsolatos anonimitást lelepleznék, és e szabályok hiánya miatt azok a lényeges szabályok, amelyeknek jelenleg vonatkozhatnak kriptovalutákra, teljesen hatástalanok. Nehéz megtalálni az egyensúlyt a kiberbiztonság, az adatvédelem és a magánélet védelme között. Továbbá a jogalkotásnak mindig arányosnak kell lennie, hogy ugyan foglalkozzon a tiltott magatartással, de ne fojtsa el a technológiai innovációt.[330]

---

report.pdf (2021.09.12.)

[328] TÓTH, D.: Credit card fraud with a comparative law approach. In: GORAN, I. – ANGELINA, S. (szerk.): International Scientific Conference "Towards a Better Future: Democracy, EU Integration and Criminal Justice", Conference Proceedings, Volume I. Faculty of Law - Kicevo, University "St. Kliment Ohridski", Bitola, 2019. 232. o.

[329] KEATINGE, T. – CARLISLE, D. – KEEN, F.: Virtual currencies and terrorist financing: assessing the risks and evaluating responses. Policy Department for Citizens' Rights and Constitutional Affairs, 2018. 9. o. https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf (2021.09.12.)

[330] HOUBEN, R. – SNYERS, A.: Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion. Policy Department for Economic, Scientific and Quality of Life Policies (European Parliament), Brüsszel, 2018. 53–56. o.
http://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf (2021.09.12.)

Három fő jellemző határozza meg, hogy milyen szinteket érhet el egy virtuális fizetőeszköz: a centralizáció foka, a likviditás és konvertibilitás, és a hálózati hatások – amikor egy szolgáltatás annál hasznosabbá válik minden felhasználó számára, minél többen használják azt. Hasonló okokból az online ajándékkártyák egyre népszerűbbek a terroristák körében. 2017. januárban egy washingtoni rendőrt letartóztattak, amiért az IS-t kísérelte meg anyagilag támogatni Google Play ajándékkártyák használatával, melyeket végül egy FBI-informátornak adott, nem pedig valódi IS-támogatónak. Mivel az online ajándékkártyák rendelkeznek a korábban felsorolt jellemzőkkel, a likviditással és konvertibilitással, amelyek szükségesek ahhoz, hogy egy fizetési mechanizmus nagyszámú ember számára felhasználható legyen, ezért egy stratégiát szükséges kifejleszteni annak megakadályozására, hogy azok az illegális finanszírozás eszközévé váljanak.[331]

Dion-Schwarz et al. hat tulajdonságot azonosít, melyek hiánya korlátozhatja a kriptovaluták terrorizmus finanszírozására történő felhasználását: anonimitás, használhatóság, biztonság, elfogadottság, megbízhatóság és volumen. Az anonimitás a használó azonosságának elrejtésének és védésének képességét jelenti. A használhatóság arra vonatkozik, hogy a használó milyen könnyen tud tranzakciókat végezni és kezelni a valutáját. A biztonság annak fokát jelöli, hogy a kriptovaluta infrastruktúra mennyire biztosítja a titoktartást, integritását és pontosságát a tranzakcióknak és felhasználói fiókoknak. Az elfogadáson a szerzők annak a mértékét jelölik, hogy a valutát mennyire fogadja el egy felhasználói közösség, továbbá a felhasználók közösségének a méretét. A megbízhatóság azt jelöli, hogy a felhasználók milyennek látják a tranzakciók sebességét és rendelkezésére állását. A volumen a kriptovaluta infrastruktúrában végrehajtott tranzakciók időátlagolt összesített mértékére vonatkozik.[332]

1. Mennyire jelentenek komoly terrorizmus finanszírozási kockázatot a virtuális fizetőeszközök?

2018-ban Keatinge et al. arra világított rá, hogy kiberbűnözés és dark web piacokkal kapcsolatban ugyan léteztek dokumentált esetek virtuális fizetőeszközök jogellenes

[331] GOLDMAN, Z. K. – MARUYAMA, E. – ROSENBERG, E. –SARAVALLE, E. – SOLOMON-STRAUSS, J.: Terrorist Use Of Virtual Currencies: Containing the Potential Threat. CNAS, 2017. 19. o. https://www.lawandsecurity.org/wp-content/uploads/2017/05/CLSCNASReport-TerroristFinancing-Final.pdf (2021.09.12.)

[332] DION-SCHWARZ, C. – MANHEIM, D. – JOHNSTON, P. B.: Terrorist Use of Cryptocurrencies Technical and Organizational Barriers and Future Threats. RAND Corporation, Santa Monica, 2019. 23. o. https://www.rand.org/pubs/research_reports/RR3026.html (2021.09.12.)

használatáról, de 2018-ban még kevés velük elkövetett terrorizmus finanszírozás eset volt ismert. A szerzők szerint a jelenlegi formájukban és a jelenlegi alkalmazási szintjükön még valószínűleg nem nyújtanak a terroristák számára jelentős előnyöket más finanszírozási módszerekkel szemben, amiket már eddig is használnak. Mindazonáltal ismertek esetek, amelyek mutatják, hogy a vallásilag és politikailag motivált extrémisták használtak már virtuális fizetőeszközöket – még ha kevés alkalommal és rendszertelen módon is – és törekedhetnek a használatuk kiterjesztésére. A közeljövőben a terroristák virtuális fizetőeszköz használata a szerzők szerint valószínűleg specifikus és korlátozott alkalmi célokat foglal majd magában, köztük: adománygyűjtés vagy illegális tárgyak megszerzése a dark weben; adományok kérése közösségi médián és titkosított üzenetküldő platformokon végzett közösségi finanszírozás keretében; és P2P értéktranszfer használatával történő nemzetközi pénzátutalások terrorista hálózatok tagjai között.[333]

Teichmann szintúgy 2018-ban megállapítja, hogy a kriptovaluták alkalmasak terrorizmus finanszírozására és anonim támogatóktól származó nagyszámú alacsony összegű donáció gyűjtésére, viszont esetükben nehéz nagyobb összegeket használni, továbbá szinte használhatatlanok a mindennapi élet tevékenységeinek finanszírozására. Teichmann úgy véli, azok inkább fegyverek és robbanóanyag vagy robbantószerek dark weben történő vásárlására szolgáló tőke felhalmozására alkalmasak, ezért veszélyt jelentenek.[334]

Az előbbi két szerzőhöz hasonló álláspontón lévő, ugyancsak 2018-as National Terrorist Financing Risk Assessment (2018 NTFRA) szerint ugyan vannak elszigetelt példák arra, hogy terrorista csoportok és támogatóik virtuális fizetőeszközökben kértek adományokat, valamint azokat pénz mozgatására, vagy termékek vagy szolgáltatások vásárlására használták, de a virtuális fizetőeszközök jelenleg nem jelentenek komoly terrorizmus finanszírozási fenyegetést, de alapos megfigyelést igényelnek, mert a felhasználásuk mértéke valószínűleg csak nőhet. A szabályozás és a felügyelet hiánya világszerte a legtöbb országban a kockázatot csak növeli. [335] Keatinge és Keen is alacsonynak ítéli meg a kriptovaluták fenyegetését terrorizmus finanszírozás szempontjából, és ők is felismerik a lehetőséget az azokkal történő visszaélésre: „A

[333] KEATINGE – CARLISLE – KEEN: i.m. 9. o.

[334] TEICHMANN, F. M. J.: Financing terrorism through cryptocurrencies – a danger for Europe? Journal of Money Laundering Control, 2018. Vol. 21. No. 4. 517. o.

[335] National Terrorist Financing Risk Assessment. 2018. 3. o.
https://home.treasury.gov/system/files/136/2018ntfra_12182018.pdf (2021.09.12.)

Facebook nemrégiben bejelentett saját kriptovalutájának, a „Libra-nak ” elindításáról szóló terve fényében a közösségi média és a kriptovaluta konvergenciája elkerülhetetlenül egy komoly részletekre kiterjedő vizsgálatot von magára, és továbbra is egy figyelemmel kísérendő terület marad terrorizmus finanszírozásra történő visszaélés lehetőségével kapcsolatban."[336]

Weimann rámutat arra, hogy a dark webet virtuális fizetőeszközök használatával terroristák és más bűnözők felhasználják összegek rejtett utalására is. Korunkban Weimann ezt a trendet tartja a legriasztóbbnak a dark web terroristáknak nyújtott lehetőségei közül. Kriptovalutákat gyakran használnak tranzakciókhoz illegális kereskedelem során, zsaroláshoz, pénzmosáshoz. Weimann is rávilágít, hogy a terroristák is használhatják a webet adománygyűjtésre, pénzátutalásra és virtuális fizetőeszközök használatával robbantószerek, fegyverek vásárlására.[337]

A kriptovaluták a közösségi finanszírozás új formáit vezetik be, a legtöbb esetben egyértelmű különbséget téve a hamis célzattal, de valójában terrorizmus finanszírozásra szolgáló közösségi finanszírozás online kampányok és az explicit módon militarista célokat szolgáló kampányok között. Az olyan közösségi finanszírozás kampányok, amelyek digitális fizetőeszközökben kérnek adományokat, explicitebbek a terrorizmus finanszírozási szándékaikkkal kapcsolatban. Ezek a kampányok nem javasolják a használóiknak az egymás közti interakciót, hanem inkább arról adnak útmutatást, hogy tudják minél jobban megőrizni az anonimitásukat.[338]

Davis 2020-as álláspontja szerint a kriptovaluták nem fogják helyettesíteni a hagyományos terrorizmus finanszírozási módszereket. A készpénzfutárok, a hawala rendszer, a bankszektor és más pénz mozgatására szolgáló módszerek szerves részei maradnak a terroristák finanszírozási technikáinak. Kriptovalutákat és más pénzügyi technológiákat (financial technologies, fintech) alkalmaznak, amikor az számukra praktikus, és amikor el kívánják homályosítani a pénzeszközök forrását és érkezési

[336] KEATINGE, T. – KEEN, F.: Social Media and Terrorist Financing What are the Vulnerabilities and How Could Public and Private Sectors Collaborate Better? Global Research Network on Terrorism and Technology: Paper No. 10, Royal United Services Institute for Defence and Security Studies, 8. o. https://rusi.org/sites/default/files/20190802_grntt_paper_10.pdf (2021.09.12.)

[337] WEIMANN (2018): i.m. 4–5. o.

[338] BARONE, D. M.: Cyber Jihad and Terrorism Financing: New Methods – Old Rules. ITSTIME. (2018, August 16). https://www.itstime.it/w/cyber-jihad-and-terrorism-financing-new-methods-old-rules-by-daniele-maria-barone/ (2021.09.12.)

helyét.[339]

Vitathatatlan, hogy a kriptovaluták terrorizmus finanszírozási kockázatot jelentenek, de vitatható, hogy milyen fokút. Úgy tűnik, jelenleg nem képviselnek nagyon magas fokú terrorizmus finanszírozási fenyegetést, de tekintve a modern technika, főleg a kriptovaluták gyorsan fejlődő és változó világát, ez a fenyegetés könnyen fokozódhat, az mindenképp figyelemmel kísérendő.

2. Virtuális fizetőeszközzel elkövetett terrorizmus finanszírozás esetek

Az Ibn Taymiyyah Media Center (ITMC), a Mujahideen Shura Council in the Environs of Jerusalem (MSC) médiaszárnya „Jahezona" („Szerelj fel minket", arabul) elnevezésű online kampányával 2016. június végétől már kísérletezett virtuális fizetőeszközzel. A kampány keretében a Bitcoin-os fizetést is lehetővé tették. Infografikákat töltöttek fel a Twitter-re, QR kódokkal, amik egy Bitcoin címhez vezettek. Ugyan a Twitter gyakran törölte a Jahezona felhasználói fiókjait, azok mindig visszatértek.[340]

A „Fund the Islamic Struggle without Leaving a Trace" („Finanszírozd az Iszlám Küzdelmet Nyomok Hagyása nélkül") egy deep web oldal, ami egy Bitcoin címre kér adományokat dzsihád finanszírozására. Az Amreeki Witness álnévvel az internetre feltöltött „Bitcoin wa Sadaqat alJihad" elnevezésű PDF dokumentum, melynek címe lefordítva „Bitcoin és az erőszakos fizikai küzdelem adománya"(„Bitcoin and the Charity of Violent Physical Struggle") egy útmutató a dark web titkos pénzügyi tranzakciókra való felhasználásához.[341]

2016-ra az IS és az al-Kaida terroristái már kértek kripto-adományokat a közösségi médián. Az IS, mint sok más terrorszervezet „központi parancsnoksága" látszólag soha nem kért Bitcoin adományokat, hanem azt a harcosai, „dolgozói" tették az IS nevében, a közösségi médián és más platformokon, már legalább 2015-től kezdve. 2017-re az IS már régóta kapott Bitcoin adományokat a világ minden tájáról, még az USA-ból is, ahol ismertek esetek például New York és Virginia államból is. A mai napig találhatóak a

[339] DAVIS, J.: New Technologies but Old Methods in Terrorism Financing. Royal United Services Institute for Defence and Security Studies, London, 2020. 2. o. https://static1.squarespace.com/static/5e399e8c6e9872149fc4a041/t/60b0ab3b05f173456658076b/1622190920308/New+Technologies+but+Old+Methods+in+TF.pdf (2021.09.12.)

[340] FANUSIE, Y.: The New Frontier in Terror Fundraising: Bitcoin. The Cipher Brief. (2016, August 24). https://www.thecipherbrief.com/column_article/the-new-frontier-in-terror-fundraising-bitcoin (2021.09.12.)

[341] WEIMANN (2016): i.m. 42. o.

Telegram alkalmazásban Bitcoin adományokra való felhívások IS-hez köthető csatornákon. Az IS terrorcselekmények finanszírozására is használt Bitcoin-t, köztük a 2019 áprilisában Sri Lankán elkövetett húsvéti robbantásokhoz is.[342]
Az utóbbi években pénzügyi nehézségekkel küszködő al-Kasszám Brigádok, a Hamász katonai szárnya támogatóit 2019 elején Bitcoin-os közösségi finanszírozásra hívta fel. A terrorszervezet infografikát töltött fel a Bitcoinról a közösségi médiára, és megadott egy Bitcoin címet is, amire az adományokat várta. Egy napon belül 900 USD érkezett a Hamász digitális bankszámlájára. Napokkal később a terrorszervezet egy további Bitcoin címet tett közzé, és kevesebb, mint egy héten belül a digitális pénztárcákra több mint 2.500 USD értékű Bitcoin érkezett.[343] A New Jersey állami Somerset megyében letartóztattak egy személyt, amiért anyagilag, és kis összegű Bitcoinnal is támogatta a Hamászt, és azzal büszkélkedett a közösségi médián.[344] Az al-Kasszám Brigádok weboldala Bitcoin oktatóanyagot tartalmaz és egy pénztárca cím generátort is, hogy minden új donációhoz új felhasználói fiókot hozzon létre. Ezek az adományok egy forrás szerint 2019. augusztus végéig elérték a 12.000 USD-t, egy másik forrás szerint pedig 2019. augusztus végéig a terrorszervezet Bitcoin bányászata 195.000 USD értékben hozott kriptovalutát a Hamász számára. Palesztinában a civilek a Bitcoin-t még fokozottabban használják, mint Hamász. Valószínűleg az al-Kasszám Brigádok Bitcoin-os adománygyűjtő kampánya növelte a civil lakosság tájékozottságát a témában. A palesztinek a Bitcoin-t nemzetközi pénztranszferhez és az izraeli kontroll megkerüléséhez használják, és a legtöbb palesztin forrás becslése szerint a régióban a civil használat messze túlsúlyban van a Bitcoin-hoz fűződő terrorista aktivitással szemben.[345]
A tény hogy a Hamász megváltoztatta az adományozás mechanizmusát, úgy, hogy a

[342] KATZ, R.: Tales of Crypto-Currency: Bitcoin Jihad in Syria and Beyond. The Daily Beast. (2019, October 13). https://www.thedailybeast.com/the-bitcoin-jihad-in-syria-and-beyond-tales-of-crypto-currency (2021.09.12.)

[343] FANUSIE, Y.: Hamas Military Wing Crowdfunding Bitcoin. Forbes. (2019, February 4). https://www.forbes.com/sites/yayafanusie/2019/02/04/hamas-military-wing-crowdfunding-bitcoin/#306575c34d7f (2021.09.12.)

[344] Somerset County Man Charged With Attempts To Provide Material Support To Hamas, Making False Statements, And Making Threat Against Pro-Israel Supporters. United States Department of Justice. (2019, May 22). https://www.justice.gov/usao-nj/pr/somerset-county-man-charged-attempts-provide-material-support-hamas-making-false (2021.09.12.)

[345] CUEN, L.: In Palestine, Civilians Are Using Bitcoin More Than Hamas. CoinDesk. (2019, August 22). https://www.coindesk.com/palestinian-civilians-are-using-bitcoin-more-than-terrorists (2021.09.12.)

weboldala minden tranzakciónál egy új digitális pénztárcát generált, megnehezítette a szervezet kriptovalutás finanszírozásának követését. Eredetileg az al-Kasszám Brigádok az adakozókat arra kérték, hogy küldjenek Bitcoin-t egy digitális címre vagy pénztárcára. Egyetlen pénztárcára még fel lehet hívni a kriptovaluta tőzsdék figyelmét („red flaggelve" azokat), ami elméletben lehetővé tenné számukra azt, hogy megakadályozzák az összegek céljukhoz való áramlását, a rendszereiken keresztül, de a minden egyes donációhoz külön generált pénztárca ezek megjelölését megnehezíti. 2019. március 26. és április 16. között 0,6 Bitcoin-t (kb 3.300 USD értékben) küldtek a website által generált pénztárcákra. Az adománygyűjtő kampány négy hónap alatt kb. 7.400 USD összeget hozott.[346]

Az IS híreket közlő Akhbar al-Muslimin weboldal továbbra is folytatja a 2017 végén elkezdett online adománygyűjtő kampányát. Az oldal néha a felszíni weben, néha a dark weben működik. Az oldalt 2019. április 1-én frissítették, melyen egy link található, ami Bitcoin adományokra hív fel. Erre a linkre kattintva a felhasználó eljut egy 2017. december 7-i dátummal ellátott oldalra, és minden egyes kattintás egy újabb Bitcoin pénztárcát generál az adakozni szándékozónak. A Hamász hasonló oldalt üzemeltet, ami egy új pénztárcát hoz létre minden egyes donor számára.[347]

2020. augusztus 13-án az Amerikai Egyesült Államok Igazságügyi Minisztériuma (Department of Justice, DOJ) jelentette be három, az al-Kasszám Brigádokhoz, az al-Kaidához és az IS-hez fűződő terrorizmus finanszírozó kiber-kampány leszerelését. Ezek a terrorszervezetek kifinomult kiber-eszközöket használtak a műveleteik finanszírozására, köztük kriptovalutában kértek adományok támogatóktól világszinten. A kormányzat három polgári vagyonelkobzási keresetlevelet és egy büntetőfeljelentést nyújtott be négy weboldal, négy Facebook oldal, több mint 300 kriptovaluta felhasználói fiók és több millió USD lefoglalásával kapcsolatban. A kormány keresetlevele szerint al-Kasszám Brigádok Bitcoin adományokra való felhívást tett közzé a közösségi média oldalán és hivatalos weboldalain, azt állítva, hogy az ilyen adományok lenyomozhatatlanok lesznek, és azokat erőszakos célokra használják fel. A terrorszervezet weboldalaira oktatóvideók kerültek fel a Bitcoin címekre történő anonim adományozásról. Az Egyesült Államok Pénzügyminisztériumának adóhatósága (Internal

[346] REUTERS: Crypto terror financing: Hamas shifts tactics in bitcoin fundraising. The Jerusalem Post. (2019 April 26). https://www.jpost.com/middle-east/crypto-terror-financing-hamas-shifts-tactics-in-bitcoin-fundraising-587930 (2021.09.12.)

[347] LIV, N.: Jihadists' Use of Virtual Currency. ICT, Herzliya, 2019. 6. o. https://www.ict.org.il/images/Jihadists%20use%20of%20virtual%20currency%202.pdf (2021.09.12.)

Revenue Service, IRS), Egyesült Államok Bevándorlási és Vámhivatal Belbiztonsági Nyomozóegysége (United States Immigration and Customs Enforcement Homeland Security Investigations, HSI) és az FBI képes volt lenyomozni és elkobzást kezdeményezni a 150 kriptovaluta fiók tekintetében, amikről és ahova az al-Kasszám Brigádok összegeket utalt pénzmosás céljából. A kormány nyomozása továbbá fényt derített arra, hogy az al-Kaida és ahhoz kötődő terrorista csoportok egy Bitcoin-os pénzmosó hálózatot működtettek, közösségi média platformok és titkosított üzenetküldő alkalmazások használatával, kriptovalutában történő donációk kérése céljából. Néhány esetben a terrorszervezet jótékonyságnak állította be magát, miközben a valóságban terrorcselekmények elkövetéséhez gyűjtöttek adományokat. Az al-Kaida és a szövetségesei kifinomult technikákat használtak az adománygyűjtéseik elfedésére, de a hatóságok a szervezetekhez fűződő 155 virtuális fizetőeszköz összeget azonosítottak és kezdeményezték azok elkobzását. A kormányzati nyomozás felderítette, hogy az IS-hez köthető személyek hasznot akartak húzni a koronavírus pandémiából, úgy, hogy hamis egyéni védőeszközöket (personal protective equipment, PPE), mint N95 maszkokat árultak vásárlóknak globális szinten. Az ilyen eladásokból befolyt bevételekből az IS műveleteit támogatták volna.[348]

A virtuális fizetőeszközök relevanciája a terrorizmus finanszírozás tekintetében a fent tárgyalt esetek fényében jól láthatóan növekszik. Ez a tendencia a jövőben előre láthatóan csak növekedni fog.

3. A stablecoin kockázata

Katona rávilágít, hogy a stablecoin-nak nincsen egyértelműen meghatározott normatív meghatározása.[349] A Global Digital Finance (GDF) nemzetközi piaci önszabályozó szervezet definíciója szerint: „a stablecoin olyan kriptoeszköz, amely fizetési és forgalmi eszközként, valamint felhalmozási eszközként működik, és olyan módon strukturált, hogy minimalizálja az árfolyam volatilitását."[350] Más meghatározás szerint: „A stablecoin olyan blokklánc alapú kriptopénz, amely a kriptopénzekre jellemző

[348] Report of the Attorney General's Cyber Digital Task Force: Cryptocurrency Enforcement Framework. United States Department of Justice, Washington, D.C., 2020. 11. o. https://www.justice.gov/archives/ag/page/1326061/download (2021.09.12.)

[349] KATONA T.: Decentralizált pénzügy – A blokkláncon működő pénzlegó-rendszer lehetőségei. Hitelintézeti Szemle, 2021/1. 78. o.

[350] Stablecoin: Taxonomy and Key Considerations. Global Digital Finance, 2019. https://www.gdf.io/wp-content/uploads/2019/05/GDF-Stablecoin-Key-Considerations_9-MAY-SUMMIT-DISCUSSION.pdf (2021.09.12.) Idézi: Uo. 78. o.

folyamatos és jelentős árfolyam ingadozásokat szeretné kiküszöbölni és stabil árfolyamokhoz kötött."[351]

A FATF elismerte, hogy a stablecoin-ok ugyan ösztönözhetik a pénzügyi innovációt és hatékonyságot, valamint javíthatják a pénzügyi befogadást , de más nagyméretű értékátviteli rendszerekhez hasonlóan a stablecoin-ok felhasználhatók pénzmosásra vagy terrorizmus finanszírozásra is.[352]

A FATF megállapította, hogy a stablecoin-ok ugyanazokkal a potenciális pénzmosási/terrorizmusfinanszírozási kockázatokkal rendelkeznek, mint egyes virtuális eszközök, anonimitásuk, globális elérhetőségük és illegális pénzeszközök elrejtésére való képességük miatt. Konstrukciójuktól függően lehetővé tehetnek anonim P2P tranzakciókat nem hosztolt tárcákon keresztül. Ezek a tulajdonságok pénzmosás/terrorizmus finanszírozás sebezhetőséget jelentenek, amelyek tömeges elfogadás esetén csak fokozódnak.[353]

3) Internetes pénzügyi szolgáltatások

„Az internetes pénzügyi szolgáltatások interneten keresztüli hozzáférési mechanizmusokat biztosítanak ügyfelek számára előre feltöltött számlákhoz (prefunded account) amelyek felhasználhatók a rajtuk tárolt pénz vagy érték más olyan személyek vagy vállalkozások számára történő átutalására, akik ugyanannál a szolgáltatónál számlával rendelkeznek."[354]

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. A FATF szerint nem világos, hogy ezeket a tranzakciókat milyen mértékben használták fel a terrorizmus finanszírozására.[355] A

[351] Mi az a Stablecoin? Virtuális Cash. (2019. július 29.). https://www.virtualis.cash/mi-az-a-stablecoin/ (2021.09.12.)

[352] FATF REPORT 2019-2020. FATF, Párizs, 2020. 14. o. www.fatf-gafi.org/publications/fatfgeneral/documents/annual-report-2019-2020.html (2021.09.12.)

[353] FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins. FATF, Párizs, 2020, 2. o. www.fatf-gafi.org/publications/virtualassets/documents/report-g20-so-called-stablecoins-june-2020.html (2021.09.12.) Továbbá: Investigating the impact of global stablecoins. G7 Working Group on Stablecoins, 2019. 7. o. https://www.bis.org/cpmi/publ/d187.pdf (2021.09.12.)

[354] FATF REPORT (2015): i.m. 37. o.

[355] Uo. 37–38. o.

2015-ös „Emerging Terrorist Financing Risks” FATF jelentés szerint az online fizetési rendszerek használata terrorizmus finanszírozás támogatására inkább e fizetési rendszer elterjedtségének a szélesebb pénzügyi rendszerben való visszatükröződését jelzi, és nem pedig azt, hogy az online fizetési rendszerek jobban ki lennének téve a terrorizmus finanszírozásának.[356]

2017-ben közel-keleti illetőségű iszlamista harcosok Bitcoin-t, továbbá online fizetési szolgáltatásokat használtak, mint a PayPal, terrorista tevékenységek finanszírozására Indonéziában. Harcosok pénzt küldtek a terrorista sejtjeiknek Indonéziában, főleg Java-ban, PayPal és Bitcoin utalásokon keresztül. Mivel a vidéki területeken korlátozott az internet-hozzáférés, a virtuális pénzt készpénzre kell váltani, hogy a való életbeli tranzakciók során tudjanak fizetni.[357]

4. Virtuális világok és a nagyon sok szereplős online szerepjátékok (MMORPG-k) lehetséges szerepe a terrorizmus finanszírozásban

Alternatív kommunikációs csatorna lehet még bűnözők, terrorizmus finanszírozók, pénzmosók számára az online videojátékok, az ún. nagyon sok szereplős online szerepjátékok (Massively Multiplayer Online Role Playing Game, MMORPG), mint például a World of Warcraft és a virtuális világok, mint a Second Life chat szobái és privát üzenetei.[358] Aggodalomra adhat okot, hogy a Second Life, a World of Warcraft és az Entropia Universe megkötés nélkül és a lebukás kicsiny esélye mellett biztosít lehetőséget nagy összegek határokon keresztüli átjuttatására.[359] Irwin et al. úgy tartják, hogy pénzmosás és terrorizmus finanszírozás előfordulhat virtuális világokban.[360]

---

[356] Uo. 38. o.

[357] YUNIAR, R. W.: Bitcoin, PayPal Used to Finance Terrorism, Indonesian Agency Says. The Wall Street Journal. (2017, January 10). https://www.wsj.com/articles/bitcoin-paypal-used-to-finance-terrorism-indonesian-agency-says-1483964198 (2021.09.12.)

[358] IRWIN, A. – SLAY, J.: Detecting Money Laundering and Terrorism Financing Activity in Second Life and World of Warcraf. In: VALLI, C. (szerk.): Proceedings of the 1st International Cyber Resilience Conference ICR2010. Edith Cowan University, Perth, 2010. 41. o.

[359] Uo. 43. o.

[360] IRWIN, A. S. M. – SLAY, J. – CHOO, K-K. R. – LIU, L.: Money laundering and terrorism financing in virtual environments: a feasibility study. Journal of Money Laundering Control, 2014. Vol. 17. No. 1. 50–75. o.

Pillanatnyilag ezek a virtuális világok nincsenek alávetve a való világ szigorú pénzügyi kontrolljainak és bejelentési kötelezettségeinek, így kiváló lehetőséget biztosítanak a bűnözőknek, köztük terrorizmus finanszírozóknak arra, hogy illegális tevékenységeiket ellenőrzés hiányában és büntetlenül végezhessék.[361] Eszteri 2015-ben arra a következtetésre jut, hogy az online játékok terroristák általi használatától az NSA elemzésében[362] foglaltakhoz képest nem feltétlenül kell tartani, és ezt nem csak az támasztja alá, hogy eddig (2015-ig) egy ilyen eset sem ismert, hanem, hogy ezen szervezetek céljaival sokkal jobban összeegyeztethető az anonim, titkosított csatornákon keresztüli kommunikáció.[363]

Az online videojátékokon keresztül végzett pénzmosással kapcsolatban fejti ki Moiseienko és Izenman, hogy a játékon belüli tárgyak és fizetőeszközök gyakran való-életbeli értékkel rendelkeznek, és azok alkalmasak bűncselekményekből származó jövedelem mozgatására vagy befektetésére, de azzal kapcsolatban viszont nincsenek tiszta elvárások, hogy a videojáték működtetői mit tudnának tenni, vagy mit kellene tenniük, hogy a bűnözői tevékenységet azonosítsák.[364] Egyre több gazdasági bűncselekményt követnek el videojátékokon keresztül.[365]

5. A koronavírus (COVID-19) pandémia hatása a terrorizmus finanszírozásra és annak online aspektusaira

A FATF a kérdést illetően a következő megállapításokat teszi: A COVID-19-hez fűződő olyan bűnözés fokozódása, mint csalás, kiberbűnözés, állami támogatások vagy nemzetközi pénzügyi támogatás hűtlen kezelése vagy sikkasztása, új bevételi forrásokat generál bűnözők számára. A koronavírus megfékezésére szolgáló intézkedések hatnak a

[361] IRWIN – SLAY (2010): i.m. 41. o.

[362] NSA: Games: A Look at Emerging Trends, Uses, Threats and Opportunities in Influence Activities. 2007. http://www.propublica.org/documents/item/889134-games (2021.09.12.) Idézi: ESZTERI D.: A World of Warcraft-tól a Bitcoin-ig: Az egyén, a gazdaság és a tulajdon helyzetének magán- és büntetőjogi elemzése a virtuális közösségekben. Doktori értekezés. Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola, Pécs, 2015. 231. o.

[363] ESZTERI: i.m. 231. o.

[364] MOISEIENKO, A. – IZENMAN, K.: Gaming the System: Money Laundering Through Online Games. RUSI Newsbrief, 2019. Vol. 39. No. 9. 1. o.

[365] Counter-terrorists win: Financial crime through video games is on the rise. The Economist. (2019, November 7). https://www.economist.com/finance-and-economics/2019/11/07/financial-crime-through-video-games-is-on-the-rise (2021.09.12.)

„bűnözői gazdaságra" és változtatják a bűnözői viselkedést, úgy, hogy a profitorientált bűnelkövetők más illegális cselekedetek felé fordulhatnak. A pandémia a kormányok és a magánszektor pénzmosás és terrorizmus finanszírozás elleni (AML/CFT) kötelezettségeinek végrehajtási képességére is hatással van: a felügyeletre, szabályozásra, eljárási reformokra, a gyanús tranzakciók jelentésére és a nemzetközi kooperációra. A FATF szerint ezek a fenyegetések és sebezhetőségek növekvő pénzmosási és terrorizmus finanszírozási kockázatot jelentenek, melyek a következő eredményekkel járhatnak: A bűnözők megtalálhatják a módjait az ügyfél-átvilágítási eljárások megkerülésének. Növekedhet a visszaélés az online pénzügyi szolgáltatásokkal és virtuális eszközökkel illegális összegek mozgatására és elrejtésére. Előfordulhat visszaélés a gazdasági stimulus intézkedésekkel és csődbűncselekmény illegális jövedelmek elrejtése és mosása céljából. Fokozódhat a nem szabályozott pénzügyi szektor használata, további lehetőséget adva bűnözőknek illegális összegek mosására. Előfordulhat a hazai és nemzetközi pénzügyi támogatások és rendkívüli segélyalappal való visszaélés és annak hűtlen kezelése. Bűnözők és terroristák kihasználják a COVID-19-et és az ahhoz kapcsolódó gazdasági hanyatlást, hogy új készpénz-intenzív és magas likviditású üzletágak felé mozduljanak el fejlődő országokban. AML/CFT szabályozási válaszok segíthetnek a vírus elleni intézkedések gyors és hatékony végrehajtásában. Ezek közé tartoznak: Hazai koordináció a COVID-19-nek AML/CFT kockázatokra és rendszerekre való hatásának felmérése érdekében. Megerősített kommunikáció a privát szektorral. Az ügyfél-átvilágítási eljárások tekintetében bátorítás a kockázatalapú megközelítés teljes használatára. Elektronikus és digitális fizetési lehetőségek támogatása.[366]

Az Európa Tanács pénzmosás elleni bizottsága (Moneyval)[367] 2020-as felmérése szerint úgy tűnik, hogy a pandémia alatti korlátozások alatt a bűnözés általános szintje stabil maradt vagy enyhén csökkent is, melynek oka a helyváltoztatás és a határokon átnyúló utazás korlátozása volt. Néhány bűncselekmény tekintetében azonban emelkedés volt megfigyelhető. A Moneyval leszögezi, hogy az észlelt néhány tendencia tekintetében még korai lenne tipológiák kidolgozása a COVID-19 válság újdonsága és az elegendő információ hiánya miatt. Nem jelentettek növekedést kábítószer-kereskedelem, terrorizmus finanszírozás, nonprofit szervezetekkel visszaélés és bennfentes

[366] COVID-19-related Money Laundering and Terrorist Financing – Risks and Policy Responses. FATF, Párizs, 2020. 4. o. https://www.fatf-gafi.org/media/fatf/documents/COVID-19-AML-CFT.pdf (2021.09.12.)

[367] NAGY H.: A pénzmosás magyarországi jogi szabályozásának vázlata. Magyar Rendészet, 2020/1. 97. o.

kereskedelem tekintetében, de számos joghatóság a medicrime, a kiberbűnözés és a korrupció növekedésére mutatott rá. A világjárvány megfékezésére tett intézkedések által okozott gazdasági hanyatlás miatt fennáll annak a veszélye, hogy a pénzmosás és a terrorizmus finanszírozása elleni intézkedéseket enyhítik, vagy kevésbé kezelik prioritásként a gazdaság fellendítése és a fizetések folyamatának felgyorsítása érdekében.[368]

6. Következtetések

A bűnözők, köztük a terrorizmus finanszírozók és a terroristák folyamatosan fejlesztik a technikáikat, előszeretettel használnak egyedi, vagy kísérleti jellegű szolgáltatásokat céljaik elérése érdekében.[369] A terroristák és az őket finanszírozók a pénzügyi források előteremtése, mozgatása és használata tekintetében folyamatosan kiskapuk és új módszerek után kutatnak.[370] A terrorista csoportok műveleteik finanszírozásához szükséges bevételszerzési és pénzátutalási módszereik tekintetében haladnak a modern technológia új trendjeivel (mint kriptovaluták és a dark web használata), de használják a hagyományos módszereket is (mint a zakat és hawala).[371]

Tevékenységeik végzéséhez a terroristák számos és változatos módon használják fel az internetet, köztük a finanszírozásukhoz szükséges anyagi források beszerzésére is. A terrorizmus finanszírozásának internethez kötődő technikáinak és forrásainak jelentősége a vonatkozó technológiák fejlődésével és az internet egyre széleskörűbb elérhetőségével egyre nő.

---

[368] COMMITTEE OF EXPERTS ON THE EVALUATION OF ANTI-MONEY LAUNDERING MEASURES AND THE FINANCING OF TERRORISM MONEYVAL: Money laundering and terrorism financing trends in MONEYVAL jurisdictions during the COVID-19 crisis. Council of Europe, Strasbourg, 2020. 5. o. https://rm.coe.int/moneyval-2020-18rev-covid19/16809f66c3 (2021.09.12.)

[369] MCCROSSAN, S.: Combating the Proliferation of Mobile and Internet Payment Systems as Money Laundering Vehicles. ACAMS CAMS-FCI, USA, 2015. 15. o.
https://www.acams.org/wp-content/uploads/2015/08/Combating-the-Proliferation-of-Mobile-and-Internet-Payment-Systems-as-ML-Vehicles-S-McCrossan.pdf (2021.09.12.)

[370] Current Efforts by the FATF to Monitor and Take Action against Terrorist Financing. FATF. (2019, February 22).
https://www.fatf-gafi.org/publications/methodsandtrends/documents/fatf-action-against-terrorist-financing-feb-2019.html (2021.09.12.)

[371] PASCA, V. – ORZA, D. S.: Terrorism: between the need for funding and obtaining funding sources. Journal Of Eastern-European Criminal Law, 2019. Vol. 6. No 1. 227. o.

Keatingle és Danner szerint a terrorszervezetek sikeresen alkalmazzák a közösségi médiához hasonló új technológiákat, és várhatóan fokozottabban fogják majd használni az innovatív fizetési megoldásokat, kriptovalutákat és más pénzügyi innovációkat, amik számukra anonimitást biztosítanak. A leggyakoribb bevételszerzési tevékenységeik, mint az adományok, adóztatás, zsarolás, rablás, bankfosztogatás, bűnözői körökkel való együttműködés és emberrablás váltságdíjért biztosan megmaradnak. A szerzőpáros szerint ez azt sugallja, hogy míg például a kriptovaluták terroristák általi felhasználása eddig korlátozott volt (és szerintük gyakran eltúlzott), az új technológiák megjelenése lehetőségeket kínál az innovatívabb adománygyűjtési és pénzmozgatási technikák kifejlesztésére, új opciókat adva a már bevált, hagyományos bevételi forrásokhoz, amely lehetővé teszi a terrorista csoportoknak, hogy elérjék a kívánt autonómiát és a pénzügyi fenntarthatóságot.[372] A terrorizmus és a terrorizmus finanszírozása elleni küzdelemben kritikus fontosságú ismerni a terroristák finanszírozási technikáit és forrásait. A szerzők egyetérteni látszanak abban, hogy a terrorizmus finanszírozás internethez fűződő technikái és módszerei jelentőségük tekintetében még a hagyományos technikák és módszerek mögött helyezkednek el, de a jövőben relevanciájuk nőhet. A terrorizmus elleni küzdelem szereplői általi figyelemmel kísérésük épp ezért elengedhetetlen fontosságú.

[372] KEATINGE, T. – DANNER, K.: Assessing Innovation in Terrorist Financing. Studies in Conflict & Terrorism, 2021. Vol. 44. No. 6. 467. o.

IX. AZ ONLINE TÖRTÉNŐ RADIKALIZÁCIÓ

1. Az internet szerepe a radilizációban

A minőségi propaganda, a videók, képek, magazinok etc. egyre fontosabb lett a terrorszevezetek branding stratégiájában. A vonzó digitális médiát és az új módszereket az IS-en kívül más terrorszervezetek is adoptálták. A „szívekért és az elmékért" vívott harcban ki kell tűnniük a regruták elnyeréséhez, egy egyre versengőbb környezetben. Amikor a propaganda képes a nézőket bevonni, és egy erős narratívát prezentálni, mely megcélozza a helyi közösségek push pull tényezőit, akkor valószínűleg hatása van a sebezhető egyének radikalizációs folyamatára.[373]

A radikalizáció definiálása problémás.[374] Olyan nézet is létezik, hogy meghatározás nélkül könnyebb helyzetben lennénk, mivel azzal kezdődnek a valódi nehézségek.[375] Ahogy Kőhalmi frappánsan mutat rá: „Radikálisnak tekinthetjük az öngyilkos merénylő tettét, aki ugyan a robbantást végrehajtja, de saját maga is belepusztul ördögi tervének kivitelezésébe. Hasonló jelzővel illethető a sportoló, aki reggeltől estig, minden más dolgát félretéve csak az edzésre koncentrál."[376]

A radikalizálódás és a toborzás egyéni jellegű és komplex folyamat.[377] A radikalizmus katalizátorai közé tartozik a szegénység, a munkanélküliség, a lehetőségek hiánya, a fiatalkori bűnözés, a csempészet, a kábítószer, a társadalmi, politikai és gazdasági marginalizáció és nem utolsó sorban az ideológiai hatások. Mindezek egymást erősíthetik, vagy átfedhetik, földrajzilag eltérő környezetben érvényesülnek és a radikalizmus melegágyát képezhetik. Ahhoz, hogy fel tudjunk lépni ellene, létfontosságú a gyökerek megismerése, és hogy területekre lebontva ismerjük meg a radikalizáció

---

[373] ZEIGER, S. – GYTE, J.: Prevention of Radicalization on Social Media and the Internet. In: SCHMID, A. P. (szerk.): Handbook of Terrorism Prevention and Preparedness. International Centre for Counter-Terrorism, Hága, 2021. 361. o.

[374] SOHN, W.: „Radikalisierung" Ein Hilfsmittel zur rhetorischen Bewältigung der aktuellen Sicherheitslage. Kriminalistik, 2017. No. 2. 67–72. o. Idézi: KŐHALMI L.: A vallási terrorizmus útjai. JURA, 2021/2. 32. o.

[375] SOHN: i.m. 68. o. Idézi: KŐHALMI (2021): i.m. 32–33. o.

[376] KŐHALMI (2021): i.m. 32–33. o.

[377] KIS-BENEDEK J.: Dzsihadista fészkek, mint a terrorizmus lehetséges kiindulópontjai. Hadtudomány, 2017/1–2. 97. o.

történetét és összefüggéseit.[378] Bihari szerint a radikalizmus bármely ország esetében fenyegető lehet, hiszen beszélhetünk szélsőjobboldali, baloldali és iszlám fundamentalizmushoz kötődő radikalizmusról. Szuggesztív erejénél fogva a vallási elemmel bíró radikalizmus lehet a legveszélyesebb.[379]

Az interneten kívül a radikalizációs folyamatban kulcsszerepet játszanak még a közvetítők, a szociális hálózat és a börtönök.[380]

Ugyan még 2014-ben is jelentek meg olyan vélemények, mi szerint az internet nem fokozza a terrorizmust, például Benson „Why the Internet Is Not Increasing Terrorism" című tanulmánya,[381] de ez a nézet már erősen elavult, napjainkban nehezen védhető.

Conway álláspontjával értek egyet, aki szerint az internet jelentős és sokoldalú szerepet játszik korunk erőszakos extrémizmusában és terrorizmusában.[382] A világháló radikalizáció folyamatának hajtóereje és elősegítője.[383] Conway Rapoportra utal, aki amellett érvel, hogy a strukturális tényezők nagyon fontos hatással vannak az általa megállapított terrorizmus hullámokra. A történelmben az új kommunikációs technológiák (újságok, rádió, TV etc.) kifejezetten nagy befolyással voltak a terrorizmus történelmének alakulására[384], és Conway szerint nem valószínű, hogy ez az internet esetében másképp lenne. Korunkban számos erőszakos extrémistája is úgy gondolhatja, hogy erőfeszítéseiknek van hatása, ami azon látszik, hogy mennyi időt és pénzt fektetnek az online kampányaikba. Anekdotikus bizonyítékok is erre mutatnak: elég csak arra gondolnunk, hogy az IS online milyen hatékonyan érte el a fiatal nőket, ami „dzsihadista feleségek" Szíriába áramlásához vezetett. A családok különböző országokból a „kalifátusba" utazásának fokozódása, és a korábbiakhoz képest nem szokványos terrortámadások (gázolások, késelések) terjedése korrelálni tűnik az ilyen típusú terrortámadásokra való felhívásokkal. Conway persze elismeri, hogy az

[378] Uo. 110–111. o.

[379] BIHARI R.: Radikalizmus a Nyugat-Balkánon. Hadtudomány, 2020/elektr. sz. 168. o.

[380] BJELOPERA, J. P.: American Jihadist Terrorism: Combating a Complex Threat. Congressional Research Service, Washington, D.C., 2013. 2. o.

[381] BENSON, D. C.: Why the Internet is Not Increasing Terrorism. Security Studies, 2014. Vol. 23 No. 2 293–328. o. Idézi: CONWAY, M.: Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research. Studies in Conflict & Terrorism, 2017. Vol. 40. No. 11. 77. o.

[382] CONWAY (2017): i.m. 91. o.

[383] SILBER, M. D. – BHATT, A.: Radicalization in the West: The Homegrown Threat. New York Police Department, New York, 2007. 8. o.

[384] RAPOPORT, D. C.: The Four Waves of Rebel Terror and September 11. Anthropoetics, 2002. Vol. 8. No. 1. 3. o. Idézi: CONWAY (2017): i.m. 91. o.

internetnek a korunk radikalizációs folyamataiban játszott szerepével kapcsolatban elméletileg megalapozott, empirikusan igazolható társadalomtudományi kutatásra lenne szükség.[385]

Bizonyított, hogy hatékony kommunikációs eszközként az internet komoly szerepet játszik a magányos farkas terroristák radikalizációjának folyamatában.[386] Egyre több terrorizmusban résztvevő személy használta az internetet valamilyen módon az erőszak felé vezető útján. Reeve szerint az internet kétségtelenül egy radikalizációt segítő eszköz, lehetővé téve a felhasználóknak, hogy egymással és akár terroristákkal interaktáljanak, kapcsolatba lépjenek. Fellelhetnek információt, erőszakos extrémista ideológiát, propaganda videókat és publikációkat is. Az internet a logisztikához és felderítéshez is eszközöket nyújt, a virtuális tanulásra, távoktatásra is. A felhasználó internethasználata a radikalizáció során az igényei és érdekei szerint változik.

Néhányan már amellett érvelnek[387], hogy a terrorista ismeretek tömeges elterjedése miatt a terrorista csoportokban való tagság már a személyes megítélésen alapul.[388] Olyanra is volt példa több esetben is, hogy egy merénylő nem tartozott konkrétan valamely terrorszervezethez, azonban az elektronikus tömegtájékoztatási eszközök segítségével sugárzott propagandával egyetértve, a radikalizálódás irányába fordult, a szervezetnek „hűségesküt téve."[389]

Az internet, a közösségi média és más 21. századi kommunikációs platformok miatt a terrorizmus egyre inkább magányos vállalkozássá válik, melyet elsősorban formális szervezeteken kívül tevékenykedő magányos szereplők követnek el.[390] Maras különbséget tesz hazai kinevelésű magányos farkas (domestically educated lone wolf) iszlamista magányos farkas között.[391] Véleményem szerint szükségtelen a hazai

[385] CONWAY (2017): i.m. 91. o.

[386] ZEMAN, T. – BŘEŇ, J. – URBAN, R.: Role of internet in Lone Wolf Terrorism. Journal of Security & Sustainability Issues, 2017. Vol. 7. No. 2. 185. o.

[387] KIRBY, A.: The London Bombers as ' Self-Starters ': A Case Study in Indigenous Radicalization and the Emergence of Autonomous Cliques. Studies in Conflict & Terrorism, 2007. Vol. 30. No. 5. 425. o. Idézi: REEVE, Z.: Engaging with Online Extremist Material: Experimental Evidence. Terrorism and Political Violence, 2019. 2. o.

[388] REEVE: i.m. 2. o.

[389] BARTKÓ R.: Az Unió 2017/541. Sz. Irányelvének hatása a V4 országainak büntető anyagi jogszabályalkotására. In: BARTKÓ R. (szerk.): A terrorizmus elleni küzdelem aktuális kérdései a XXI. században. Gondolat Kiadó, Budapest, 2019. 144. o.

[390] HOFFMAN, B. –WARE, J. – SHAPIRO, E.: Assessing the Threat of Incel Violence, Studies in Conflict & Terrorism, 2020. Vol. 43. No. 7. 576. o.

[391] MARAS: i.m. 86–89. o. Idézi: BÁCS, Z. Gy. – KASZNÁR, A.: Is the Lone Perpetrator Really Alone?

kinevelésű mellett csupán az iszlamista magányos farkasokra korlátoznunk a kategorizálást. Miért ne létezhetne például szélsőjobboldali magányos farkas, akit külföldi tanok ihlettek?

Nemzetbiztonsági és a terrorizmus eleni harc szempontjából a társ nélküli elkövető jelenti az egyik legfontosabb kihívást.[392] A Global Terrorism Index 2020 arra világít rá a szélsőjobboldali terrorizmussal kapcsolatban, hogy az ilyen támadások többségét olyan magányos farkasok követik el, akik nem kötődnek kifejezett terrorista csoporthoz vagy szélsőjobboldali szervezethez, annak ellenére, hogy lehetett kapcsolatuk más szélsőjobboldali személyekkel vagy inspirálhatták őket más szélsőjobboldali támadások. Nyugaton az ideológiai terrorizmus más formáinál is megfigyelhető az „affiliated" (valamihez kötődő) terrorizmustól az „unaffiliated" (nem nem kötődő) felé történő, és a személyestől az online történő radikalizáció felé való eltolódás.[393]

Mind a dzsihadista és a jobboldali extrémista propaganda arra ösztönzi az egyéneket, hogy erőszakos cselekedeteket hajtsanak végre autonóm módon, az elkövetőket „mártírként" és „szentként" dicsőítve.[394]

Online radikalizálta önmagát például Dylann Roof, aki 2015 júniusában 9 fekete egyháztagot ölt meg az Emanuel Emanuel afrikai metodista-episzkopális templomban.[395] Ha korábban nem volt az, mára már egyértelművé vált, hogy ugyan a terroristák katonai semlegesítése és a terrorista szervezkedések megakadályozása kiemelt fontosságú célok, és azoknak is kell lenniük, de ezek nem elegendőek az erőszakos extrémizmus globális fenyegetésének semlegesítéséhez. Gátat kell szabni az új extrémisták áradatának. Az erőszakot igazoló szélsőséges nézetek kialakításával vagy elfogadásával való radikalizáció is lehetséges út a terrorizmusban felé, de természetesen nem az egyetlen. A radikális nézetek nem feltétlen vezetnek terrorizmushoz, és azok

---

Honvédségi Szemle – Hungarian Defence Review, 2018. 146. évf. 1. különsz. 20. o.

[392] BÁCS, Z. Gy. – KASZNÁR, A.: Is the Lone Perpetrator Really Alone? Honvédségi Szemle – Hungarian Defence Review, 2018. 146. évf. 1. különsz. 24. o.

[393] Global Terrorism Index 2020: Measuring the Impact of Terrorism. Institute for Economics & Peace, Sydney, 2020. 64. o. https://visionofhumanity.org/wp-content/uploads/2020/11/GTI-2020-web-1.pdf (2021.03.01.)

[394] European Union Terrorism Situation and Trend report (TE-SAT). Europol, 2020. 6. o. https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-te-sat-2020 (2021.07.15.)

[395] BERMAN, M.: Prosecutors say Dylann Roof 'self-radicalized' online, wrote another manifesto in jail. The Washington Post. (2016, August 22). https://www.washingtonpost.com/news/post-nation/wp/2016/08/22/prosecutors-say-accused-charleston-church-gunman-self-radicalized-online/ (2021.10.14.)

nem mindig annak az előjelei. A legtöbb radikális ideát valló nem vesz részt terrorizmusban, és sok terrorista, még azok is, akik egy ügyért harcolnak, nem mélyen ideologizáltak és nem feltétlenül radikalizálódnak hagyományos értelemben.[396]

2. Terrorcselekményre figyelmeztető magatartások az interneten

A figyelmeztető magatartások (warning behaviours) olyan magatartások, melyek empirikusan bizonyítottan megelőzik a terrortámadásokat és más előre kitervelt erőszakos incidenseket, például tömeggyilkosságot vagy iskolai lövöldözést. Ezek fontos szerepet játszhatnak a magányos farkas terroristák fenyegetésének értékelésében.
Ilyen magatartások gyakran előznek meg terrorcselekményeket. Mindezt a radikalizációs folyamat előzi meg, mely során az egyén fokozatosan egyre hajlamosabb lesz az előre megfontolt erőszakra, egy ideológia előmozdítása céljából.
A legtöbb magányos farkas terrorista az önradikalizáció (selfradicalisation) folyamatán egy át, melyben a média szerepe döntő. Cohen rávilágít arra, hogy vitathatatlan, hogy az internet az a médium, melynek az utóbbi évtizedben a legnagyobb hatása volt a radikalizációra. Ugyan elősegítette a folyamatát, de új lehetőségeket is adott a támadásokat megelőző figyelmeztető magatartások felfedezésére.[397]
Meloy és O'Toole a figyelmeztető magartatásokat nyolcféleképp tipologizálja:
1. Útvonal figyelmeztető viselkedés (Pathway): Egy támadás kutatása, tervezése, előkészítése és végrehajtása.
2. Fixáció (Fixation): Egyre patológiásabb belefeledkezést, ráfixálódást (preokkupációt) jelző viselkedés egy személy vagy ügy iránt.
3. Azonosulás (Identification): Erős azonosulás korábbi támadókkal, szoros kapcsolat fegyverekkel, más katonai eszközökkel, felszereléssel, önmagát egy adott ügyet előmozdító ügynökként látja.
4. Új agresszió (Novel aggression): A ténylegesen megcélzott erőszakhoz nem kötődő erőszakos magatartás, az erőszakra való képesség mutatása.
5. Energia-robbanás (Energy burst): Általában a támadás előtti napokban vagy hetekben

[396] BORUM, R: Radicalization into Violent Extremism I: A Review of Definitions and Applications of Social Science Theories. Journal of Strategic Security, 2011. Vol. 4. No. 4. 8. o.

[397] COHEN, K.: Who will be a lone wolf terrorist? Mechanisms of self-radicalisation and the possibility of detecting lone offender threats on the Internet. FOI, Swedish Defence Research Agency, Stockholm, 2012. 4. o.

a célhoz kötődő tevékenységek gyakorisága vagy változatossága megugrik.
6. Szivárogtatás (Leakage): A szándék közlése egy harmadik fél felé.
7. Végső eszköz (Last resort): Növekvő kétségbesés és aggodalom kifejezése, azzal a végkövetkeztetéssel, hogy nincs más lehetséges út, mint az erőszak.
8. Közvetlenül kommunikált fenyegetés (Directly communicated threat).[398]
Cohen szerint Meloy és O'Toole tipológiájából a legkönnyebb három figyelmeztető magatartást kikövetkeztetni egy személy internetes kommunikációjából: a szivárogtatást, a fixációt, és az azonosulást.[399]
Rose és Morrison tanulmányában fontos tanulságok vonhatóak le a szivárogtatás illetően. Az általuk vizsgált mintába 31 az USA-ban magányos-farkas (lone-actor) terrorizmusban résztvevő, vagy azt tervező személy tartozik, akiket mind elítéltek. Erőszakos cselekedeteket aktívan tervezők és/vagy elkövetők mellett a mintába tartoznak még segítők (facilitators). Ők olyan nem erőszakos magatartásban vettek részt, mely során segítséget nyújtottak, vagy bátorítottak másokat, terrort, és sérelem okozását megcélzó erőszakos cselekmények elkövetésében. A mintába tartoztak még izolált „diádok" (két csoporttól függetlenül működő magányos terrorista) és „triádok" (három csoporttól függetlenül működő magányos terrorista). A szerzők azért vették be őket a mintába, annak ellenére, hogy technikailag nem „magányosak", mert a „diádok" és „triádok" gyakran csak akkor alakulnak, amikor a magányos terrorista másokat kifejezetten támadás végrehajtásához toboroz. Mindegyik vizsgált személyt az IS inspirálta, de annak irányítása és felügyelete nélkül, autonóm és független módon működtek, az edzésük, felkészülésük, célpont-választásuk és a végrehajtás tekintetében. A mintában szereplők 2014. január 31. és 2019. január 31. 2019 között segítettek, terveztek, vagy követtek el sikeresen támadásokat. 2014 elejétől kezdte az IS a közösségi médiát magányos támadások elkövetésére felhívásra felhasználni.
A minta túlnyomóan férfiakból állt (27 fő), csupán négy magányos elkövető volt nő. Főleg vagy civileket (51,6%; 16), vagy bűnüldöző szerveket (35,5%, 11) vettek célba, ritkábban katonákat (19,4%, 6), kormánytisztviselőket (6,24%, 2), csupán egy esetben egy meghatározott személyt. A minta 38,7%-a (12) teljesen egyedül cselekedett, 32,3%-a (10) diádban, 29% (9) triádban.
A magányos elkövetők 83,9%-a (26) mutatott szivárogtató figyelmeztető magatartást, mely mutatja a magányos terroristák szivárogtatásának elterjedtségét. 26 szivárogtatás

[398] MELOY, J. R. – O'TOOLE, M. E.: The Concept of Leakage in Threat Assessment. Behavioral Sciences and the Law, 2011. Vol. 29. No. 4. 513–527. o. Idézi: Uo. 18. o.
[399] Uo. 4. o.

esetében 76,9% (20) volt a „támadó”, csupán 3,8% (1) „segítő.”. Az esetek 19,2%-ában (5) a magányos elkövető támadó és segítő szerepben is volt.

A minta többsége más, IS szimpatizánsnak vélt felé szivárogtatott. (80.8%, 21). A nyilvánosság felé 65,4% szivárogtatott, köztük a Twitterre posztolt írásbeli nyilatkozatokkal. Az egyik egyén például azt tweetelte, hogy „al-Qa’ida said it loud and clear: we are fighting the American invasion and their hegemony over the earth and the people.” Tíz személy (38,5%) család és barátok felé szivárogtatott. Pédául az egyik személy egy ismerősének elmondta azt, hogy szereti Allahot, és szerinte az összes nem muszlim amerikait meg kellene ölni. Csak egy személy szivárogtatott bűnüldöző szerv felé. Az esetek többségében (20), a magányos szereplő két vagy több itt említett csoport felé is szivárogtatott. Például 17 a 21-ből, aki általa IS szimpatizánsnak vélt felé szivárogtatott, emellett a nyilvánosság vagy a család és barátok felé is tette azt. A szivárogtatás többsége (76,9%) más általuk IS szimpatizáns felé történt, 65,4% a nyilvánosság felé, 38,5% a család és közeli barátok felé.

A tanulmány arra jutott, hogy a szivárogtatás verbálisan és írásban is történik.[400] Először, amikor az online szivárogtatások nagy számát figyelembe vesszük, érvelhetnénk amellett, hogy az összes szkeptikus internetes aktivitás szigorú ellenőrzése kifejezetten informatív és hatékony lenne a terrorelhárítás számára, főleg, hogy az elektronikus szivárogtatást sokkal egyszerűbb lenyomozni, mint például a papíralapú levelekét.[401] Lehetetlen az összes potenciális terrorista kommunikáció manuális keresése.[402] Rose és Morrison szerint a leginformatívabb szivárogtatások nem mindig online találhatóak meg, és még ha tüzetesen keresnénk és találnánk is online szivárogtatást, nem minden szivárogtató követ el terrorcselekményt.[403] A szerzők mintájában leggyakrabban a Facebookon osztották meg a támogatást, melyet privátabbnak, és a köz felé kevésbé nyitottnak tartanak, mint például a Twitter.[404] A

[400] ROSE, M. M. – MORRISON, J.: An exploratory analysis of leakage warning behavior in lone-actor terrorists. Behavioral Sciences of Terrorism and Political Aggression, 2021. 1–36. o.

[401] MUELLER, J. – STEWART, M. G.: Terrorism, counterterrorism, and the internet: The American cases. Dynamics of Asymmetric Conflict, 2015. Vol. 8. No. 2. 176–190. o. Idézi: ROSE – MORRISON: i.m. 1–36. o.

[402] ZEMAN, T. – BŘEŇ, J. – URBAN, R.: Role of internet in Lone Wolf Terrorism. Journal of Security & Sustainability Issues, 2017. Vol. 7. No. 2. 2. o. Idézi: ROSE – MORRISON: i.m. 1–36. o.

[403] ROSE – MORRISON: i.m. 1–36. o.

[404] KWON, S. J. – PARK, E., – KIM, K. J.: What drives successful social networking services? A comparative analysis of user acceptance of Facebook and Twitter. The Social Science Journal, 2014. Vol. 51 No. 4. 534–544. o. Idézi: ROSE – MORRISON: i.m. 1–36. o.

szerzőpáros szerint fontos figyelembe venni az online interakciók értékelésénél azok heterogenitását, a platformok, és rajtuk folyó kommunikáció változatosságát és a felek már meglévő offline és online kapcsolatát.

Rose és Morrison rámutat arra, hogy nem meglepő módon a magányos terroristák nem a legnyilvánosabb és legkönnyebben hozzáférhető platformokon osztják meg a gondolataikat. A szerzők szerint ezért fontos, hogy a terrorizmus elleni harc szereplői ne támaszkodjanak az internetre, mint az egyes terrorista esetekkel kapcsolatos információk azonosításának és megszerzésének fő eszközére, hanem inkább kiegészítő forrásként használják. Ezt a javaslatot támogatva számos kutató[405], amellett érvel, hogy az internet inkább a radikalizálódás folyamatába nyújt betekintést, mintsem a támadások előkészítésébe. (Véleményem szerint mindekettőbe betekintést nyújt, vitatható, milyen arányban.) Rose és Morrison tanulmányában a minta 38,7%-a küzdött valami mentális betegséggel. Kutatásuk rámutatott arra, hogy a szivárogtatás nem egységes koncepció, és hogy bizonyos típusai bizonyos személyek felé történnek, bizonyos típusú médiumokon keresztül. Például extrémista ideológia iránti támogatás leggyakrabban írásos szövegben és az interneten került szivárogtatásra. A szándék és a részletek gyakrabban kerültek szivárogtatásra más IS szimpatizánsnak tartott személyek felé verbális kommunikáció útján, offline. A szerzők beimerik, hogy kutatásuk csak a felszínt kaparta a szivárogtatás és a magányos terroristák más figyelmeztető magatartásait illetően, inkább csak egy betekintést nyújt. E komplex jelenségek sokkal behatóbb kutatást érdemelnének.[406]

A szivárogtatások felhasználhatók a jövőbeli magányos farkas terroristák azonosítására vitafórumokon vagy radikális weboldalakon, félautomata módszerekkel. Ezeknek a módszereknek a legnagyobb hátránya azonban az, hogy nem tudnak különbséget tenni a jövőbeni magányos farkas terroristák és az olyan radikálisok között, akiknek nincs valódi szándéka terrorcselekményt elkövetni.[407]

3. Ellenpropaganda, mint fegyver az online radikalizációval szemben?

Egyetértek Lieberman-nal, hogy a terrorelhárításnak olyan kreatív megoldásokat is

[405] Például ZEMAN – BŘEŇ – URBAN: i.m.185–192. o. Idézi: ROSE – MORRISON: i.m. 1–36. o.

[406] ROSE – MORRISON: i.m. 1–36. o.

[407] ZEMAN – BŘEŇ – URBAN: i.m. 185. o.

számításba kellene vennie, támogatnia és alkalmaznia, mint az ellenpropaganda. Lieberman több szempontú megközelítést ajánl az USA-nak az IS internetes propagandája elleni harcban. Először is a propagandát terjesztő megfékezését a büntető igazságszolgáltatás eszközével, másodszor a propaganda eltávolítását a közösségi média platformjairól, harmadszor pedig a terrorista csoport ellenpropagandával történő hitelteleníté sét és aláásását.[408] Az ellenpropaganda csak úgy lehet hatékony, ha a terroristák online aktivitásával fel tudja venni a versenyt gyakoriságában, hogy a keresőmotorok első keresései kiadják azokat, továbbá meg kell felelnie a célközönségének, nem szabad unalmasnak lennie, hiszen a fiatal internetezőket az izgalmak vonzzák.[409] Magánszemélyek sajátos, potenciálisan hatékony, terroristák hitelességének aláásására alkalmas ellenpropagandájára példa Watfe, Youssef Helali, Mohammed Damlakhy és Aya Bro szíriai menekültek tevékenysége, akik az életüket kockáztatva, általuk készített videókban parodizálták az IS-t és propagandáját.[410] Youtube csatornájukon több százezret is meghaladó nézettségi számú videójuk van.[411] Az ISIS Mario című kreatív, szatirikus videójukban a videojáték világába helyezve egy terrorista kerül Mario szerepébe, akadályokat vesz és pontokat gyűjt, például egy túsz lefejezésével, hogy végül megmentse elrabolt, maszkos, terrorista hercegnőjét. A videót több mint nyolcvanezren látták.[412] A terrorizmus érvényesülési útja a szubjektív lélektani nyomásgyakorlás, a kollektív félelem,[413] a négy szíriai videói pedig ez ellen hatnak, és a potenciális támogatók elidegenítésére is alkalmasak lehetnek. Ahogy Kőhalmi megállapítja, egy terrorszervezet sem számíthat jó kilátásokra közép- és hosszútávon, a népesség egy bizonyos része, egy mögöttük álló szűkebb csoport nélkül, akikből további tagokat toborozhatnak.[414]

[408] LIEBERMAN: i.m. 109. o.

[409] Uo. 122–123. o.

[410] LETSCH, C.: Laughing at Isis: Syrian video artists go beyond fear to ridicule jihadis. The Guardian. (2015, March 12). https://www.theguardian.com/world/2015/mar/12/laughing-at-isis-syrian-video-artists-jihadis-refugee-islamic-state (2021.12.30.)

[411] https://www.youtube.com/channel/UCKdzJMxUSGJzNJ95ppd-ohg (2021.12.30.)

[412] ISIS Mario. https://www.youtube.com/watch?v=Ih_V45B5uEo (2021.12.30.)

[413] TOWNSHEND, Ch.: A terrorizmus. Magyar Világ Kiadó, Budapest, 2003. 23. o

[414] KŐHALMI (2015): i.m. 57–58. o.

X. SZÉLSŐSÉGES ISZLÁM MOTIVÁLTA TERRORSZERVEZETEK INTERNETHASZNÁLATA

1. Az al-Kaida internethasználata

1. Az al-Kaida születése

A Szovjetunió 1979. december 25-én kezdte meg afganisztáni hadműveletét. 1985-re, katonai jelenléte csúcsán 120 ezer katonája harcolt az országban.[415] Kovács Kolontárira utal, aki a katonai akciót négy ponttal indokolja: Afganisztánban történt belső politikai hatalmi harcok; a kabuli vezetés folyamatosan vesztett az ország irányításából; Moszkva a közép-ázsiai szovjet köztársaságok közvetlen szomszédságában kockázatosnak ítélt egy instabil országot; a Szovjetunió tartott az USA afganisztáni megjelenésétől. Az afgán vezetés továbbá a szovjet bevonulást számtalanszor kérte.[416] A Szovjetunió beavatkozásával létrejött helyi háború a mudzsahedek közt szent háborús értelmezést nyert, amelyben szerepe volt Abdullah Azzamnak is. Az Afganisztánba áramló mudzsahedek segítésére Azzam 1984-ben létrehozta a Maktab Al-Khadamat (MaK – Szolgálati Hivatal) szervezetet. Az önkéntesek közt jelent meg Oszama bin Laden, aki részt akart venni a háborúban. Bin Laden és Azzam együttműködése megromlott, és 1988. augusztus 11-én bin Laden Pesavarban létrehozta az Al Qaeda al Sulbah (Szilárd Alap) szervezetet. Az új szervezet vonzóbb és népszerűbb volt a Szolgálati Hivatalnál, mert bin Laden megvonta anyagi támogatását korábbi szervezetétől. 1989. november 24-én Azzamot gyerekeivel együtt felrobbantották, szervezete beolvadt az al-Kaidába. Bin Laden megpróbált az egész muszlim világban egy, a Nyugattal szembeni ellenségeskedést, különösen az USA-val szemben kiváltani, mely utóbbi magában foglalta volna annak katonai képességeinek csökkentését és politikai erejének gyengülését a Közel-Keleten.[417]

Az al-Kaida 2001-ben 9/11-el vált közismertté. A terrorszervezet folyamatosan változik,

[415] KOVÁCS M. K.: Az al-Káida céljai, szervezete és működése, módszerei és eljárásai a Nyugat ellen 1989 és 2015 között. Hadtudományi Szemle, 2021/1. 54. o.

[416] KOLONTÁRI A.: Az afganisztáni szovjet beavatkozás külső és belső körülményei. In: DÁVID F. – KOLONTÁRI A. – LENGYEL G. (szerk.): Afganisztán – 1979-89-99-2009. Moszt, Pécs, 2010. 32–38. o. Idézi: Uo. 54. o.

[417] Uo. 54. o.

2001 után jelentősen átalakult. Annak tekintetében Bin Laden 2011-es halálakor megtalált adathordozók révén számos új kutatási eredmény és információ került napvilágra.[418]

2. Internethasználatának fejlődése

Ugyan akkoriban napjainkhoz képest a terroristák internethasználata még gyerekcipőben járt, de szakértők már 2003-ban fogalmaztak úgy, hogy „az al-Kaida imádja az internetet."[419]

9/11 óta az USA számos az al-Kaidához köthető weboldalt figyelt meg:

Az alneda.com titkosított információt közölt biztonságosabb oldalakhoz való hozzáférésről, híreket az al-Kaidáról, cikkeket, fatvákat (a muszlim jog alkalmazásáról szóló döntéseket), és könyveket.

Az assam.com a dzsihád szócsöve volt Afganisztánban, Csecsenföldön és Palesztinában.

A almuhrajiroun.com a szimpatizánsokat arra hívta fel, hogy merényeljék meg Musharraf pakisztáni elnököt.

A jihadunspun.net-en egy 36 perces bin Laden videó volt elérhető.

A 7hj.7hj.com a látogatókat kibertámadások elkövetésére oktatta.

Az aloswa.org bin Laden felvételekből vett idézeteket, és vallásjogi rendelkezéseket tartalmazott, melyek „igazolták" a terrortámadásokat és az al-Kaida céljait.

Az (állítólag nem létező) Islamic Studies and Research Center által működtetett drasat.com állítólag a leghitelesebb volt a több tucat al-Kaida híreket közzétevő oldal közül.

A jehad.net, alsaha.com, és islammemo.com al-Kaidához fűződő kijelentéseket tettek közzé.

A mwhoob.net és aljehad.online politikai/vallási énekeket tartalmazott, üldözött muszlimokról szóló képekkel.[420]

Bin Laden fontosnak tartotta a centralizált médiát és a propaganda intelligens időzítését. Egy koherens és autentikus médiastratégiát kulcsfontosságúnak tartott a nyugat elleni harcban, és úgy gondolta, a média összes ágának egy kézben tartásával a leszakadt

[418] WAGNER P.: Az al-Káida metamorfózisa. MKI-tanulmányok, 2011/30. 3. o.

[419] THOMAS, T. L.: Al Qaeda and the Internet: The Danger of "Cyberplanning." Parameters, 2003. Vol. 33. No. 1. 112. o.

[420] Uo. 113. o.

csoportok is megfékezhetőek.[421]

2006 őszén al-Zarqawi és az AQI (AlQaida in Iraq) vezetősége létrehozott egy minden média-aktivitást felügyelő központot, az AlFurqan Institute for Media Production-t, mely később még az IS-nek is gyártott propagandát, köztük kivégzéseket és lefejezéseket. Abu Muhammad al-Furqan lett az IS első információs minisztere és fő média-koordinátora, Rakkában egy légicsapás végzett vele 2016 szeptember 7-én.

Centralizált koordináció alatt számos al-Kaida médiatermék született. Számos magazin és rengeteg weboldal jött létre. 2008-ra az al-Kaida 4000 weboldalt működtetett. A bin Laden által 1988-ban felállított As-Sahab 2005-ben 16 videót jelentetett meg, 2006-ban 58-at, és több mint 90-et 2007-ben, miközben egy hollywoodi stúdióhoz hasonlóan figyelte, hogy mi tetszhet a közönségnek. Az ún. „Jihad Academy" támadásokról és öngyilkos robbantásokról szóló képekkel inspirált. Al-Zarqawi-ról 2004-ben Irakban készült egy propaganda-videó, melyben lefejezte az amerikai üzletembert, Nicholas Berg-et. A videót egy nap alatt félmillió alkalommal töltötték le. A Camp of the Sword online magazin főleg harcosok képzésére fókuszált, állítva, hogy az önképző programjuk nem igényelt valós edzőtábort.[422] Az AQAP több mint egy évtizede él a közösségi média és online propaganda használatával.[423]

3. Online inspiráló ereje

A terrorszervezetek dinamikus rendszerek, melyek idővel adaptálódnak és fejlődnek. Hagyományosan az az elképzelés élt, hogy ezen szervezetek strukúrája centralizált, hierarchikus, melyek csúcsán a vezetők kontrollálják az egész szervezet műveleteit. Ezeknek a hagyományos struktúráknak jól meghatározott irányítás és felügyeleti lánca volt, az ágak és személyek feladatkörei pedig specializáltak voltak. Ez következetességet tett lehetővé a hierarchikus terrorszervezeteknek a specifikus személyeken keresztül megosztott üzenetük tekintetében, de fokozott kockázatot is jelentett, ha ezzel a személlyel/egységgel történt valami.

Az internet és a közösségi média az információ megosztását felgyorsította, csökkentette annak költségeit, és növelte annak komplexitását. Ez pedig támogatta sok terrorszervezet hálózati stílusú struktúrába való átszerveződését, és fokozta az egyének és sejtek önálló

[421] HANKISS, Ágnes: Behind the Scenes of Al-Qa`ida's Media Strategy. Journal of Strategic Security, 2019. Vol. 12. No. 2. 63–66. o.

[422] Uo. 67–68. o.

[423] ZEIGER – GYTE: i.m. 362. o.

működésre való képességét, főleg a szervezet üzeneteinek megosztását illetően. Ez a reorganizáció nagyobb rugalmasságot, a reakcióképességet, ellenállóságot és közönség elérését tette lehetővé. Ennek eredményeként a szélesebb terrorista hálózatok működőképesek maradhatnak akkor is, ha egy vagy több sejt súlyosan megsérül vagy akár elpusztul.

9/11 után az al-Kaidán nőtt a nyomás, edzőtáborokat vesztett Afganisztánban, és sok szenior vezetőjét megölték vagy elfogták. Hogy releváns maradhasson, akár csak laza kapcsolatokon keresztül is, de az al-Kaidának a megközelítését más erőszakos extrémista csoportok inspirálására és irányítására kellett áthelyeznie. Abu Musab al-Suri volt ennek az áthelyeződésnek és stratégiának a fő kezdeményezője, és az internetet felhasználták ennek a változtatásnak a lehetővé tételére. Ennek a megközelítésbeli változásnak jelentős globális hatásai lettek, melyek helyi, al-Kaidához köthető csoportok alakulásához vezettek, amelyek támadásokat követtek el Baliban, Londonban, és Madridban. Napjainkban a modern terrorista hálózatok tipikusan szélesen elszórt, kisebb sejtekből állnak, melyek összefonódva kommunikálnak és koordinálják a kampányaikat. A kapcsolatok gyakran ideiglenesek és intenzitásukban változóak, mindig az adott feladattól függően. Ez lehetővé tette a csoportoknak, hogy ne csak szélesebb belső kapcsolatokat alakítsanak ki, hanem külsőket is, amelyek általában a közös normákon, értékeken és kölcsönös tiszteleten alapulnak, nem pedig formális bürokratikus struktúrákon keresztül alakulnak ki. A hálózati megközelítés jegyeit példázza a 2015. januári Charlie Hebdo támadás Párizsban. Az elkövetők egy barátja, Amedy Coulibaly, aki maga is két terrortámadást követett el januárban, közzétett egy videót, állítva, hogy a támadások az IS nevében történtek. A videó gyenge minősége viszont azt sugallta, hogy az nem volt közvetlenül az al-Hayat Media-hoz, az IS médiaközpontjához köthető, hanem ez inkább egy kisebb sejt független tevékenysége lehetett. A Charlie Hebdo támadást elkövető Kouachi fivérek állítólag 20.000 USD-t kaptak az AQAP-tól, mely rámutatott az ad hoc külső koalíciók növekvő szerepére, amit az autunóm módon kommunikáló hálózatok tesznek lehetővé.[424]

Hankiss rámutat arra, hogy az elmúlt évtized európai terrorcselekényeinek elkövetőit erős személyes kapcsolatok fűzték az al-Kaida olyan európai kulcsembereihez, akiktől elméleti felkészítést és logisztikai támogatást kaptak. Európában az elmúlt években az IS-hez köthető terrortámadások elkövetői már évekkel korábban kapcsolatba kerültek és terrorcselekmények előkészítésében vettek részt al-Kaida-tagokkal. Az idegen harcosok Szíriába utaztatását is ezek a régi hálózatok szervezték. A párizsi és a brüsszeli

[424] ZEIGER – GYTE: i.m. 360. o.

terrortámadások elkövetői közül azokat fűzte a legerősebb kapcsolat az al-Kaida néhány veterán terroristájához, ideológusához és toborzójához, akik az IS frankofon hálózatában is kulcsszerepet játszottak. Ezek az akár évtizedes kapcsolatok fennállnak a német és a nagy-britanniai sejtek, radikális közösségek esetében is.[425]

Az al-Kaida támogatta a hazai kinevelésű (homegrown) magányos farkas elkövetéseket. 2010. márciusában, a médiaszárnya, As Sahab, közzétett egy „A Call to Arms" című angol nyelvű videót az amerikai születésű Adam Gadahn szóvivő szereplésével. Az USA-ban, Izraelben és az Egyesült Királyságban élő dzsihadistákat megcélzó videóban Gadahn Nidal Hasan-t, a 2009-es Fort hood-i lövöldözőt „úttörőként" dicsőítette, amiért nem keltette fel a bűnüldöző szervek figyelmét külföldi képzéssel, vagy társakra való támaszkodással. Gadahn a potenciális terroristákat realisztikusan megtámadható, és általuk ismert olyan célpontok kiválasztására ösztökélte, melyeknek szimbolikus, főleg gazdasági jelentősége is van.

A 2011. június eleji angol nyelvű „Do Not Rely on Others, Take the Task upon Yourself" („Ne támaszkodj másokra, vedd a feladatot magadra") videóüzenetben Gadahn még egyértelműbb hangsúlyt helyezett a magányos farkas műveletekre. A videóban az elkövetéshez fegyvereket ajánl. Példának hozza az USA-t, ahol könnyű lőfegyverhez jutni, és akár automata rendszerű lőfegyver is beszerezhető, például fegyverbemutatókon, háttérellenőrzés és bármiféle azonosítás nélkül.[426]

Az al-Kaida arab nyelvű magazinja a Ṣadā al-Malāḥim.[427]

Az AQAP 2010-ben indította el az Inspire nevű online magazinját, mely célja nyugati dzsihadisták kinevelése volt. Szerkesztője a szaúdi születésű, később az USA-ban élő Samir Khan volt, aki az AQAP-hoz Jemenben csatlakozott 2009-ben. Az USA elhagyása előtt, mint dzsihadista blogger és a Jihad Recollections online magazin, az Inspire előfutárának megalkotójaként volt hirhedt. Khan és az online publikációi homegrown (belföldön kitermelt) dzsihadistákat neveltek ki. Erre számos példa hozható.

2010 novemberében Mohamed Osman Mohamud-ot, egy szomáliai születésű honosított USA-i állampolgárt egy FBI „sting operation" részeként tartóztatták le, miután Portland Pioneer Courthouse terén fel próbált robbantani egy furgont, melyről azt hitte, robbanószerrel van tele. A Szövetségi Igazságügyi Minisztérium szerint cikkeket írt a

[425] HANKISS Á.: A színfalak mögött - az al-Kaida médiastratégiája. ARC ÉS ÁLARC, 2018/3–4. 216. o.

[426] BJELOPERA: i.m. 8. o.

[427] MACDONALD, S.: Terrorist Narratives & Communicative Devices: Findings from a Study of Online Terrorist Magazines. In: ZEIGER, S. (szerk.): Expanding Research on Countering Violent Extremism. Hedayah and Edith Cowan University, Perth, 2016. 128. o.

Jihad Recollections-be.

2011 júliusában Naser Abdo U.S. Army közlegényt a texas-i Fort Hood közelében tartóztatták le, amiért a térségben lövöldözést és bombatámadást tervezett. Birtokában találtak egy robbanószerkezet összeállításáról szóló Inspire cikket.

2012 novemberében Miguel Alejandro Santana Vidriales-t letartóztatták, amiért három másik három személlyel azt tervezte, hogy csatlakoznak az al-Kaidához, vagy a tálibokhoz. A DOJ szerint bombakészítésről és fegyverek használatáról az Inspire cikkeit olvasta.[428]

Az Inspire inspirálta a 2013-as Boston Maratoni merénylet elkövetőit is.[429] A testvérek, Tamerlan és Dzhokhar Tsarnaev más online propaganda mellett olvasták az Inspire magazint, és azt állították, hogy az első számban szereplő „How to Make a Bomb in Your Mother's Kitchen" („Hogyan készíts bombát anyukád konyhájában") című cikkből tanultak meg bombát készíteni.[430]

2019. december a 6-án Szaúd-Arábia Légeierejének Second Lieutenant-ja, Mohammed Saeed Alshamrani megölte az USA Haditengerészetének (U.S. Navy) három tengerészét, és megsérített nyolc másik személyt, a floridai Naval Air Station Pensacola-ban. 2020. február elején az AQAP magára vállalta a támadást. Nem tiszta, hogy a szervezetnek a támadásban közvetlen szerepe volt-e, de ha igen, az azt jelentené, hogy ez lenne 9/11 után az első olyan USA-beli halálos terrortámadás, amit külföldi terrorszervezet szervezett. Alshamrani a közvetlenül a támadás előtt közzétett közösségi média posztjában bin Laden és al-Awlaki szavai köszönnek vissza, mely az al-Kaida propagandájának maradandó befolyását mutatja.[431]

4. Reakció a koronavírus pandémiára

2020. március 31-én az al-Kaida közleményt adott ki a koronavírusról, azt isteni büntetésnek nevezve, ami „felfedte az Egyesült Államok által dominált világgazdaság törékenységét". A közlemény szerint itt az idő, hogy a muszlimok magukévá tegyék az áhitatot és megbánják bűneiket, és felszólítja a nyugatiakat, hogy térjenek át az iszlámra,

[428] BJELOPERA: i.m. 16–17. o.

[429] WARD, A.: ISIS's Use of Social Media Still Poses a Threat to Stability in the Middle East and Africa. RAND Corporation. (2018, December 11). https://www.rand.org/blog/2018/12/isiss-use-of-social-media-still-poses-a-threat-to-stability.html (2021.11.15.)

[430] ZEIGER – GYTE: i.m. 362. o.

[431] CLARKE, C. P.: The Pensacola Terrorist Attack: The Enduring Influence of al-Qa`ida and its Affiliates. CTC Sentinel, 2020. Vol. 13. No. 3. 16. o.

és kritizálta az USA-t a globális katonai műveletei miatt. A közlemény továbbá rámutat a nyugati vezetők „kőszívűségére”.[432] Az al-Kaida vezetősége az iszlámot egy „higiénia-orientált vallásnak” nevezte, a Koránból idézve részleteket, melyek rávilágítottak a tisztaság fontosságára, az arc eltakarására köhögés esetén, és az önkéntes karanténra a járvány idején. Az al-Kaida nőknek szóló magazinja, az Ibnat al Islam immunerősítő zöld tea recepteket közölt.[433]

2. Az IS internethasználata

1. Az IS-ről röviden

Az IS korunk talán legveszélyesebb terrorszervezete.[434] 2014 júniusában lett közismert, amikor szinte váratlanul épített ki egy új típusú szervezetet a Közel-Keleten.[435] Előzményei 1999-ig nyúlnak vissza, hivatalosan 2014-ben alakult meg. Azóta több nevet adoptált, többek között ezzel jelezve aktuális hovatartozását: Dzsamjat at-Tauhid wal-Dzsihad, al-Kaida Iraki frakciója (al-Qaeda in Iraq/AQI), Iraki ISIS (The Islamic State in Iraq/ISI), Iraki és Szíriai ISIS (The Islamic State in Iraq and Sham/ISIS/ISIL), ISIS (Islamic State/IS).[436] A nyugati média az ISIL, vagy ISIS kifejezést használja, jelezve, hogy fegyveres szervezetről és nem államról van szó. Ez Kis-Benedek szerint nem helyes, mert a szervezet pont az állam létrehozását hangsúlyozza.[437]

Az IS az al-Kaidából vált ki, az Abu Muszab al-Zarqawi vezette Jama’ alTawhid wal-Jihad nevű szervezethez tartozott, majd a térség vezető szervezetévé, esernyőszervezetté vált. Ahogy korábban az al-Kaida, az IS is primus inter pares (első az egyenlők között) terrorista szervezet lett, melynek minden nagyobb terrorcsoport hűségesküt tett: a nigériai Boko Haram és a szomáliai al-Shabaab 2015 márciusában, a líbiai Iszlám Fiatalok Súra Tanácsa (Islamic Youth Shura Council) 2014-ben, az afganisztáni tálibok

[432] Extremist Content Online: Extremists Plot Anti-Semitic Harassment Campaign Targeting Philadelphia Jewish Day School. Counter Extremism Project. (2020, April 6). https://www.counterextremism.com/press/extremist-content-online-extremists-plot-anti-semitic-harassment-campaign-targeting (2021.10.04.)

[433] HANNA: i.m.

[434] GÁL I. L.: A tőkepiac büntetőjogi védelme Magyarországon. Kódex Nyomda Kft, Pécs, 2019. 151. o.

[435] KIS-BENEDEK J.: Katonai biztonság Marokkótól Iránig. Zrínyi Kiadó, Budapest, 2018. 246. o.

[436] SZŰCS L.: Szíria és az Iszlám Államnak nevezett terrorszervezet egyedi vonásai 2018-ig. Szakmai Szemle, 2019/1. 8–9. o.

[437] KIS-BENEDEK J.: Katonai biztonság Marokkótól Iránig. Zrínyi Kiadó, Budapest, 2018. 246. o.

2015-ben.[438]

2014 júniusának közepén az IS elfoglalta Moszult, az iraki Ninive tartomány székhelyét, mellyel akkora területhez jutott a Közel-Keleten, mint Nagy-Britannia. Alig ezer harcosa könnyen foglalta el a várost a 30 ezer, amerikaiak által kiképzett iraki katonától és rendőrtől, akik elmenekültek, több tízmillió USD értékű Humvee harci terepjárót és Abrams harckocsit hagyva hátra.[439]

Az IS a történelem leggazdagabb terrorszervezete volt.[440] 2015-ös összbevételét becslések 1 és 2,4 milliárd USD közé teszik.[441]

Szervezete uralma csúcsán 30.000 főt tett ki, és „hibrid" (terrorista és katonai) műveleteket, módszereket alkalmazott hibrid finanszírozással (egyes országok Szaúd-Arábia, Katar, Jemen támogatása, olajjövedelmek, adók, emberrablások és a nemzetközi műkincsek kereskedelme).[442]

2. Az IS úttörő internethasználata

Az IS esetében a terroristák internethasználatának az eddig említett valamennyi aspektusával találkozhatunk. Eddig példátlanul mesteri internethasználata új fejezetet nyitott a terroristák internethasználatában és általánosságban a nemzetközi terrorizmus jelenségében.

Kétségtelenül az IS a történelem eddig legsikeresebb technológia-orientált terrorszervezete. Tagjai és támogatói számos tevékenységre használják a felszíni webet, a deep webet, dark webet, a közösségi médiát és titkosított üzenetküldő alkalmazásokat, köztük propagandájuk terjesztésére, toborzásra, követőik terrorcselekmények elkövetésének inspirálására vagy arra közvetlen utasításra.[443] Online jelenlétét

[438] RESPERGER I.: A nemzetbiztonsági szolgálatok tevékenysége – biztonsági kihívások, kockázatok és fenyegetések. In: RESPERGER I. (szerk.): Nemzetbiztonsági alapismeretek. Dialóg Campus Kiadó, Budapest, 2018. 73. o.

[439] WEISS – HASSAN: i.m. 13. o.

[440] CLARKE, C. P. – JACKSON, K. – JOHNSTON, P. B. – ROBINSON, E. – SHATZ, H. J.: Financial Futures of the Islamic State of Iraq and the Levant: Findings from a RAND Corporation Workshop. RAND Corporation, Santa Monica, 2017. iii. o.
https://www.rand.org/content/dam/rand/pubs/conf_proceedings/CF300/CF361/RAND_CF361.pdf (2021.11.17.)

[441] Uo. 8. o.

[442] RESPERGER I.: Terrorista szervezetek, módszerek, eljárások. Szakmai Szemle, 2018/2. 11. o.

[443] BODO – SPECKHARD: i.m. 2. o.

ugyanolyan komolyan veszi, mint a csatatéri műveleteit.[444]

3. (Online) propagandája

1) A propagandagépezet

A szakirodalomban a tekintetben egyetértés látszik, hogy az IS 2013-2014-ben indított online propagandakampánya minőség és mennyiség tekintetében példátlan volt. Az angol nyelvű „Islamic State News" és „Islamic State Report" hírleveleket 2014-ben követte a Dabiq online magazin megjelenése, mely két éven át az angolul beszélő internetezők befolyásolásának egyik legfontosabb eszköze volt.[445]

Az IS fejlett média-infrastruktúrát hozott létre. A 2006-ban az al-Kaida és IS által alapított, már említett al-Furqan Institute for Media Production az interneten megosztott filmeket, audio-anyagokat, lemezeket, brosúrákat és különféle más anyagokat gyártott. 2013-ban az IS létrehozta a prédikációk és vallási énekek (nashid-ok) gyártására és megosztására specializálódott Ajnad Media Foundation-t, továbbá az arab tartalmakat készítő I'tisaam Media Foundation-t. 2014-ben állította fel az idegen harcosok toborzását megcélzó angol, német, orosz és francia tartalmak gyártásához az AlHayat Media Center-t.[446] Nem csak hivatalos szervei gyártanak propagandát. Lakomy 2018 szeptember 15 és 2018 október 15 között végzett kutatást az IS propagandatermékeit illetően a World Wide Web felszíni részén. Ennek során fedezte fel többek között az arab és angol nyelvű, IS-hez fűződő Ghuraba (idegenek) weboldalt, melyet az IS Ahlut-Tawhid Publications nem hivatalos propaganda-sejtje működtetett. A címe a kutatás előtt és ideje alatt is változott. A Ghuraba használt ritkább domain-okat, mint as .top, .host, vagy .website, de népszerűeket is, mint a .com. A .com domain nevet használó cím nem tartalmazott utalást az szélsőséges iszlamizmusra, a dzsihádra, vagy az IS-re, de október elején eltávolították, nem úgy, mint a .website domain-t használó URL-t. Az Ahlut-Tawhid Publications website szervereit Mekkából és Abu Dhabiból működtették.[447]

---

[444] HAMMING, T. R.: Global Jihadism after the Syria War. Perspectives On Terrorism, 2019. Vol. 13. No. 3. 11. o.

[445] LAKOMY, M.: Between the "Camp of Falsehood" and the "Camp of Truth": Exploitation of Propaganda Devices in the "Dabiq" Online Magazine. Studies in Conflict & Terrorism, 2020. 1. o.

[446] PASHENTSEV, E. N. – BAZARKINA, D. Y.: ISIS Propaganda on the Internet, and Effective Counteraction. Journal of Political Marketing, 2021. Vol. 20. No. 1. 19. o.

[447] LAKOMY, Miron: Picturing the Islamic State's online propaganda: vanishing or resurfacing from the World Wide Web? European University Institute, Fiesole, 2018. 2. o.

Az IS addig példátlanul magas szintű propagandájával a közösségi médiát is használta toborzáshoz és ellenségei megfélemlítéséhez,[448] szimpatizánsainak radikalizálódásában és a toborzásban annak szerepe meglehetősen nagy.[449] Az IS az újoncok megcélzására, motivációjára, felkészítésére irányuló mesteri közösségi média használata és más kiber-módszerei viszont messze meghaladják az AQAP Inspire magazinját útnak indító Anwar al-Awlaqi-ét.[450] A terrorszervezet nem elégszik meg az al-Kaida 2011. május 2-án megölt volt vezetője, Oszama bin Laden által alkalmazott videoüzenetekkel. A közösségi média minden fajtáját használják, applikációkat is készítenek, komoly hardverháttérrel és informatikai szakemberekkel is rendelkeznek.[451] Okostelefonos applikációkat nem csak használnak, fejleszenek is.[452]

Többek között felhasználta a Twitter, Facebook és Instagram felületeit, ellenségei, szimpatizánsai és a közvélemény befolyásolására, erőteljes, érzelmekkel teli tartalmakkal, melyek sokszor a tagjait félelmetes harcosoknak ábrázolták. A lefejezésekről és kivégzésekről szóló tartalmak célja a megfélemlítés. Ezekkel teljes kontrasztban az IS olyan képeket is megosztott, melyeken a terroristái Snickers-t esznek és kismacskákat gondoznak.[453] Igaz, hogy a macska mellett néha kalasnyikov hevert. Az ilyen tartalmak arra is szolgálhatnak, hogy kevésbé látsszanak szörnyetegeknek.[454] Nissen szerint a macska történelmi utalás Abu Huraira-ra, Mohammed Próféta társára, aki szerette ezeket az állatokat.[455]

Az IS kommunikációja során a legmodernebb technikai megoldásokat alkalmazza,

---

[448] FARWELL, J. P.: The Media Strategy of ISIS. Survival, 2014. Vol. 56. No. 6. 49. o.

[449] KIS-BENEDEK J.: Az Iraki és Levantei Iszlám Állam (ISIL) és az ellene folytatott küzdelem tendenciái. Hadtudomány, 2016/1–2. 31. o.

[450] DOYLE, P.: Four Policy Actions Needed to Strengthen US and Coalition Efforts
Against al-Qa'ida, ISIL, and Hizballah. In: BYRNE-DIAKUN, R. M. (szerk.): Georgetown Security Studies Review: What the New Administration Needs to Know About Terrorism and Counterterrorism. Georgetown Security Studies Review, USA, 2017. 100. o.

[451] HORVÁTH A.: A terrorizmus és a média kapcsolatáról. Acta Humana, 2016/5. 38. o.

[452] KATZ, R.: ISIS's Mobile App Developers Are in Crisis Mode. Vice. (2016, June 3).
https://www.vice.com/en/article/qkj34q/isis-mobile-app-developers-are-in-crisis-mode (2021.07.07.)

[453] FARWELL: i.m. 50. o.

[454] GRÜN, G.: Tweets as weapons: How 'Islamic State' is fighting its battles... digitally. Deutsche Welle. (2015, June 03).
https://www.dw.com/en/tweets-as-weapons-how-islamic-state-is-fighting-its-battles-digitally/a-18493604 (2021.12.17.)

[455] NISSEN, T. E.: Terror.com – IS's Social Media Warfare in Syria and Iraq. Contemporary Conflicts, 2014. Vol. 2. No. 2. 1–8. o. Idézi: FARWELL: i.m. 50. o.

videóikat a filmes eszközök profi használata jellemzi. További sajátosság, hogy kommunikációja sok nyelven folyik. Általában arabul és angolul, de számos esetben más nyelveken is, például német, francia, mandarin, orosz, kurd etc. nyelven.[456]

2) Az IS propaganda-stratégiája

Farwell szerint az IS propagandatevékenységének stratégiája kétirányú: egy kifelé és egy befelé irányuló. A befelé irányuló az IS által elfoglalt területeken élő népességet tartja szem előtt, célja a „szívük és elméjük elnyerése." Az ehhez kapcsolódó tevékenységeket főleg offline végzik. A kifelé irányuló stratégia komplexebb, és két célközönsége van: a potenciális követők és az ellenség.[457]

Az IS kommunikációja Arany et al. szerint hármas cél mentén halad: első a kalifátus promóciója és konszolidációja, második az új harcosok toborzása, harmadik a félelemkeltés és elrettentés. Célcsoportjaik a sikeresen toborozhatók, a szunnita muszlimok, és az ellenségnek tekintett kormányok és társadalmak.[458]

Az IS közösségi oldalakon, és egyéb internetes felületeken végzett propagandájának legfőbb célcsoportja a nyugaton élő instabil vagy radikalizálható, sokadik generációs lakosság. Közülük sokan érkeztek a kalifátus kikiáltását követően az IS területére, aztán később terroristasejtek tagjaként tértek vissza Európába, vagy harcoltak helyben. A nem csatlakozóktól pedig pénzügyi támogatást kaphattak.[459]

Az IS pop-kultúrával gazdagon fűszerezett propagandájával a fiatalokat veszi célba.[460]

Horváth 2015-ben arra világított rá, hogy az IS az al-Kaida és szövetségesei gyakorlatát követve szinte minden létező módszerrel próbálkozott új tagokat toborozni, a fiatalokat megnyerni, mesterien használva az internetet és a közösségi médiát, vallási és etnikai közösségekben nyíltan és burkoltan is buzdítva a fiatalokat a dzsihád követésére. Horváth példaként hozza, hogy milyen sok már Németországban született muzulmán gyökerű fiatal utazott Irakba és Szíriába. A jelenség nem korlátozható Németországra, szinte minden nyugat-európai országban megfigyelhető a dzsihád iránti fogékonyság. A beszervezettek életkora egyre alacsonyabb, nagyon sok középiskolás korú szökik meg,

[456] ARANY A. – N. RÓZSA E. – SZALAI M.: Az Iszlám Állam Kalifátusa: Az átalakuló Közel-Kelet. Osiris Kiadó Kft., Budapest, 2016. 222. o.

[457] FARWELL: i.m. 49–55. o. Idézi: DE CUIA, Ch.: Is (Islamic State) And The West: The Role Of Social Media. Libera Università Internazionale degli Studi Sociali Guido Carli, Róma, 2014/2015. 21–22. o.

[458] ARANY – N. RÓZSA – SZALAI: i.m. 220–221. o.

[459] VARGA M.: Társadalmi biztonság a terrorizmus árnyékában. Hadtudomány, 2017/1–2. 134. o.

[460] ZEIGER – GYTE: i.m. 361–362. o.

hogy csatlakozzon az IS-hez. Egyre több volt a lányok és fiatal nők[461] aránya a beszervezettek között, annak ellenére, hogy a nőket elsősorban korábban is a harcosok szexuális igényei kielégítésére szervezték. Az IS a beszervezettek útját fizeti és megszervezi, ha kell, kíséretet és hamis dokumentumokat is biztosít.[462]

3) Az IS fő propagandatermékei

Az Al-Hayat Media sok potenciális regrutákat és szimpatizánsokat megcélzó HD videót gyártott Európa nyelvein, amik az IS-es életet spirituálisan kielégítőnek, az európai államokat pedig immorálisnak és törvénytelennek mutatták.[463]

Állítólag IS-témájú videojáték is létezik (előzetes mindenképp): a Salil alSawarem (The Clanging of Swords/A kardok csengése). Ez az FPS (first person shooter, belső nézetes lövöldözős) játékot a népszerű Grand Theft Auto franchise-ról mintázták, célja az IS népszerűsítése. Előzetese számos weboldalon és felületen megjelent. Állítólagos 2014-es megjelenésekor források szerint csupán a játékos csatornákon 3,5 milliárd[464] megtekintéssel büszkélkedhetett.[465] Al-Rawi rámutat, hogy kérdéses, hogy a játék valóban elkészült-e, és az sem tiszta, ki fejlesztette, mivel a játékhoz sok link vezet, főleg torrent oldalakra. A linkek viszont vagy nem működnek, vagy rosszindulatú weboldalakhoz vezetnek. Az előzetest egyértelműen nem az IS centralizált média-központjai készítették, mint az Al-Hayat, Al-Furqan, és Al-Ethar, mert a terrorszervezet ellenzi az olyan szórakozási formákat, mint a zenehallgatás, és a videojáték, mert azok elterelik a figyelmet a hitről és az imáról. A játékot/előzetesét IS területén kívüli szimpatizáns készíthette. A „Salil al-Sawarem" az IS motivációs vallási énekének címe is, a játékkal nem összekeverendő.[466]

Mint több másik terrorszervezet, az IS rendelkezik online magazinokkal, melyek fontos szerepet játszanak a radikalizációban. Céljuk nem csupán az inspiráció, technikai instrukciókat is nyújtanak magányos elkövetők számára, és tanácsokkal is látják el őket a csatlakozásról.[467] Az IS online magazinjai közé tartoznak a Dabiq, a Rumiyah, a Dar al-Islam, és a Konstantiniyye. A földrajzi értelemben vett kalifátus elvesztése után a

[461] A női terroristákról: NAGY M.: A női terrorizmus. Pécsi Tudományegyetem Állam-és Jogtudományi Kar, Pécs, 2021.

[462] HORVÁTH L. A.: A terrorista csoportok toborzásáról. Belügyi Szemle, 2015/7–8. 116–117. o.

[463] ZEIGER – GYTE: i.m. 361. o.

[464] Erősen megkérdőjelezhető szám. AL-RAWI, A.: Video Games, Terrorism, and ISIS's Jihad 3.0. Terrorism and Political Violence, 2018. Vol. 30. No. 4. 740–760. o.

[465] AL-RAWI: i.m. 740–760. o. Idézi: ZEIGER – GYTE: i.m. 361–362. o.

[466] AL-RAWI: i.m. 740–760. o.

[467] ZEIGER – GYTE: i.m. 361–362. o.

From Dabiq to Rome és a Youth of the Caliphate.[468] Az Istok az orosz nyelvű magazinja.[469]

4) Az IS propagandájának változása

A korábban tárgyalt Dawn of Glad Tidings alkalmazás segítségével az IS tagjai, 2014-ben, Moszul elfoglalása idején a Twitteren akár napi 44.000 tweet-et tettek közzé.[470]

A közösségi médián a aktivitásuknak gátat szabni sziszifuszi küzdelemnek tűnt. Az IS-t támogató Twitter fiókok olyanok voltak, mint a hidra levágott feje, egyet eltávolítottak, kettő nőtt a helyébe.[471]

Milton rámutatott arra, hogy függetlenül attól, hogy területei elvesztése után milyen lesz az IS szervezete, már birtokában lesz egy jól fejlett ismeretrendszer arról, hogyan keltsenek szimpátiát a potenciális támogatóikban a média használatával. Mivel a terrorszervezet továbbra is fejleszteni és használni fogja a médiához kötődő képességeit, Milton szerint kritikus fontosságú fejleszteni azt a képességünket, hogy az IS és hasonló szervezetekkel szemben fel tudjuk venni a harcot a „média csataterén", hogy az ilyen szervezetek fenyegetését csökkenthessük.[472]

Az IS propagandagépezete 2015-ben volt a csúcsán, kibocsátása 2017 végére nagyot zuhant, mennyiségben és minőségben is. Korábban a propaganda inkább a tömeg szimpátiájának elnyeréséről és a toborzásról szólt, a téma később inkább a háború lett, instruálóbb és uszítóbb jelleggel.[473] Ugyan 2015. január és 2018. júliusa között az IS hivatalosan közzétett vizuális propaganda mennyisége jelentősen csökkent, Milton figyelmeztetett, hogy valószínűleg ebben hullámzás várható. 2015 januárja óta száz IS médiafelelős vált „mártírrá." Kifejezetten az iraki médiahivatal tűnt tartósnak: 2016 során és 2017 decemberében Irak egyes részeinek az IS irányítása alóli felszabadítása után ugyan csökkent az iraki médiahivatal termelése, de később az iraki produkciók száma újra enyhe növekedést mutatott. Az IS Irakon és Szírián kívüli médiahivatalai a szervezet teljes kibocsátásához arányítva több propagandát gyártanak, mint valaha. Az

[468] LAKOMY, M.: Islamic State's Online Propaganda: A Comparative Analysis. Routledge, London, 2021. 1. o.

[469] MACDONALD: i.m. 128. o.

[470] FARWELL, J. P.: The Media Strategy of ISIS. Survival, 2014. Vol. 56. No. 6. 51. o.

[471] LIEBERMAN: i.m. 102. o.

[472] MILTON, D.: Down, but Not Out: An Updated Examination of the Islamic State's Visual Propaganda. Combating Terrorism Center at West Point, United States Military Academy, West Point, 2018. 51. o

[473] WINTER, Ch.: Inside the collapse of Islamic State's propaganda machine. Wired. (2017, December 20). https://www.wired.co.uk/article/isis-islamic-state-propaganda-content-strategy (2022.01.05.)

IS hivatalos vizuális termékei főleg katonai témájúak lettek.[474]

Milton szerint, ha az IS propagandatermelése teljesen meg is szűnne, már így is egy brandet épített ki magának, és elfoglalta a helyét a dzsihádban. Milton szerint azt kellene vizsgálni, miért olyan vonzó még mindig, a harctéri sikertelenségei ellenére is. Több figyelmet kellene annak szentelni, hogy miért olyan tartós és ellenálló a brandje, a motiváció, inspiráció, vonzerő szempontjából. Milton továbbá figyelmeztet, hogy attól, hogy az IS vizuális propagandát közzétevő képessége csökkent, még nem szabad arra a következtetni, hogy a médiacsoportja már ne lenne olyan fontos, vagy ne lenne fenyegető. Azt sem jelenti, hogy az IS online tevékenységeinek más aspektusai is csökkenést mutatnának, pl. a toborzás, motiváció, vagy koordináció az olyan titkosított platformokon, mint a Telegram. A propagandatermelés pedig újra növekedhet, mert az IS médiatevékenysége ellenálló és fejlődésre képes.[475] Ahogy 2017-ben többen is megfogalmazták: „az Iszlám Állam vesztésre áll a csatatéren, de nyerésre az interneten."[476]

4. Az IS online útkeresése

Az IS online jelenlétét illetően megfigyelhető a kezdetben főleg a nyílt interneten végzett aktivitás után egy megfelelő platform iránti keresés.

Amiért a fő platformok, mint a Facebook, Twitter, YouTube és a Telegram egyre „barátságtalanabbak" lettek az IS-szel szemben, a terrorszervezet vállalkozások és játékosok számára tervezett, kevésbé ismert üzenetküldő alkalmazásokon terjeszkedett. Iraki és szíriai területvesztései után újratervezte a technológia használatának stratégiáját a toborzás és koordináció terén.[477]

2018 végén az IS támogatók a Telegramon alternatív platformok és szoftverek használatát kezdték javasolni. Az IS ez után kiépítette a jelenlétét számos nyílt forráskódú (open source) decentralizált platformon. Főleg hivatalos propagandát

[474] MILTON: i.m. IV. o.

[475] Uo. 8. o.

[476] RATNESAR, R.: Islamic State Is Dying on the Battlefield—and Winning on the Internet. Bloomberg. (2017. July 20). https://www.bloomberg.com/news/articles/2017-07-20/islamic-state-is-dying-on-the-battlefield-and-winning-on-the-internet (2022.01.05.)

[477] KATZ, R.: A Growing Frontier for Terrorist Groups: Unsuspecting Chat Apps. Wired. (2019, September 1).
https://www.wired.com/story/terrorist-groups-prey-on-unsuspecting-chat-apps/?fbclid=IwAR0rzGUvrw5SoMJy1_XGd-wHuTF6cgTGUrQlsWkpQr8_eZq_l6vSK0YKWcQ (2020.07.05.)

terjesztő felhasznólói fiókokat és oldalakat hoztak létre a Mastodon, Nextcloud, Rocket.Chat and ZeroNet felületeken, melyek ellenállóak, anonimak, és felhasználási lehetőségük szerteágazó, ezért előnyösek a terroristák online kommunikációs és disztribúciós stratégiája szempontjából. E platformokon a dzsihadista aktivitás viszont 2018-ban nem tudott húzóerővé válni, valószínűleg az alternatív felületek kisebb felhasználói bázisa, és ezért gyengébb tájékoztató képessége miatt. A Telegram maradt a terrorista-szimpatizánsok platformja.[478]

A Telegram alternatívájaként az IS ismételten új és kisebb platformokkal kísérletezett. 2019. április 14-én a Nashir News Agency propaganda-terjesztő csoport az új közösségi média oldalát hirdette a Koonekti közösségi média platformon. 13 órán belül az oldal 28 lájkot kapott és ugyan megkapta a hitelesítést, de pár órával később eltávolították. A Go Like platformot az IS hasonlóan sikertelenül tesztelte. A korábbi próbálkozásokat vizsgálva, a kis és közepes méretű applikációk, platformok és szolgáltatások használatának mintája fedezhető fel. Korábbi példák közé tartozik a Baaz, Viber, Kik, Ask.fm, Discord és más, köztük egy személy által működtetett mikro-platformok. Úgy tűnik a Telegram és bizonyos esetekben a kisebb platformok stabil alternatívájának bizonyult a decentralizált internet (decentralised web, DWeb), a jelenlegi world wide web altenatívája. Az IS DWeb platformokkal és applikációkkal is kísérletezik.

Bármely Telegram-alternatívának, ideértve a decentralizált internet szolgáltatásokat, kifejezett jellemzőkkel kell bírnia, hogy azokat terroristák széleskörben adoptálják. A kisebb platformok sikeres használata a következő tényezőkön múlik: 1. Biztonság: magas biztonság (pl.: végpontok közötti titkosítás), az IS médiafelelősök és végfelhasználók műveleti biztonsága (operational security, OPSEC) növelése érdekében. 2. Stabilitás: az IS médiafelelősei és támogatóinak védettségének mértéke a platform tulajdonosa és/vagy harmadik személyek beavatkozásától (pl.: tartalom és felhasználói fiók eltávolítás vagy DoS támadások). 3. Felhasználhatóság: mennyire könnyű az alkalmazásokat telepíteni, feliratkozni a platformokra és mennyire használhatóak napi szinten. 4. Közönség elérésére való képesség.

Amikor a tech vagy közösségi média cégek felmérik a terroristák általi visszaélés lehetőségét, ezeket a tényezőket számba kell venni. Az IS médiaszakértőinek megfigyelése elengedhetetlen fontosságú a támogatást igénylő platformok azonosításában. A megfigyelésbe bele kell vonni a szélesebb propaganda-elosztó ökosztisztémát és a nagyobb és kisebb platformok közötti dinamikus és komplex

[478] Internet Organised Crime Threat Assesment (IOCTA) 2019. Europol, Hága, 2019. 49. o. https://www.europol.europa.eu/iocta-report (2022.01.05.)

interakciókat is. A kutatás fókuszának inkább az elosztó-ökoszisztámára kell irányulnia és annak egyéni elemeire, mint magára a propagandaanyagra. Rendszeralapú megközelítésre van szükség a terroristák kisebb platformokkal való visszaélése elleni küzdelemhez. A terroristák internethasználatát övező vizsgálatnak ki kell terjednie a Dwebre is. Egy sikeres fellépési műveletnek a rendszerelmélettől tanuló bizonyítékokon alapuló kutatáson kell alapulnia. Bármilyen ellenlépés nem kívánt következményekkel is járhat, mint tömeges migráció a decentralizált internetre, amit nehezebb megérteni, befolyásolni és bomlasztani.[479]

Katz arra világít rá, hogy az IS-nek a Telegramról való eltávolítása után nincs fő otthona a weben. Így online nehezebb megtalálható, de a tagjainak is nehezebb egyesülni és toborozni. A Telegram eltávolító algoritmusa sokkal célzottabb volt, mint korábban bármikor. A korábbi eltávolító kampányok az IS felhasználóinak csatornáira és chat csoportjaira fókuszáltak, melyek után az IS mindig visszatért, de most a platform a „felégetett föld" taktikát alkalmazva nem csak a csatornákat, hanem azok létrehozóit és használóit is törölte, támogatóktól a top médiafelelősökig. Sok tartalék felhasználói fiókot is eltávolítottak, és mikor újakat hoztak létre, azokat is gyorsan eltávolították. Sok újságíró, akadémikus és terrorizmuskutató is eltávolításra került, és nem tudott új fiókot létrehozni. A kampány váratlanul érte az IS-t. A tagok elvesztették egymással a kapcsolatot, miközben az egész média infrastruktúra, amely olyan csoportok köré épült, mint a Nashir News, Fursan al-Rafa, és Invasion Brigades, gyorsan szétesett. Az IS az interneten új otthon után nézett. Első állomása volt a Riot, egy nyílt forráskódú üzenetküldő kliens, ahonnan egyszer már 2017 őszén eltávolításra került. Az IS használta üzenetküldő platformok közül a Riot-hoz a legkönnyebb csatlakozni, elég egy felhasználónév és jelszó. Csatlakozni lehet chat csoportokhoz URL vagy meghívó nélkül is, ezáltal sokkal hozzáférhetőbb a Telegramnál. Az IS hálózat részei hamarosan ellepték a Riot-ot chat szobákkal. Napokkal az után, hogy a Telegram elkezdte a tisztítást, az IS Riot fiókjai törlésre kerültek. Az IS-hez köthető csoportok ez után még hetekig hirdették a Riot szobáikat, de eltávolításuk folytatódott. Még mindig lehet találni sok ilyen szobát a Riot-on, de a terrorszervezet hálózata, mint egész, más otthont keresett és talált is a TamTam-on, egy Telegramhoz hasonló üzenetküldő platformon. A TamTam-ot is sikertelenül próbálta használni 2018 tavaszán az IS. A platformon egyértelművé vált az új jelenléte, mikor azon vállalta magára először a

[479] ISIS Use of Smaller Platforms and the DWeb to Share Terrorist Content. VOX-Pol. (2019, July 3). https://www.voxpol.eu/isis-use-of-smaller-platforms-and-the-dweb-to-share-terrorist-content/ (2022.01.06.)

2019. november 29-i London Bridge-en történt késelést. December 1-re több száz nyilvános és privát IS csatorna, csoport és fiók lepte el a TamTam-ot, köztük a fő IS-hez köthető média egységek, mint a Halummu és Mutarjim. Az IS innen is hamarosan eltávolításra került. Így járt más platformokon is, köztük a kanadai Hoop Messenger-en, ami azonnal elkezdte a fiókok és csatornák eltávolítását (de úgy tűnik, az IS újakat hoz ott létre). Az IS sikertelenül próbálkozott még kevésbé ismert közösségi média platformokkal, mint az egyesült állomokbeli MeWe-vel, és egy nyílt forráskódú Twitter alternatívával, a német fejlesztésű Mastodon-nal. Ugyan az IS még mindig át tud csúszni a Telegram résein, például jelöletlen csatornákkal és diszkrét felhasználói nevekkel, de kétszámjegyű platformon szóródott szét, mely tendencia folytatódni fog a felkészült platformokon, melynek nagy jelentősége van. Katz szerint a széleskörben használt platformokon elhelyezkedő centralizált online menedékek az egyik legfontosabb változó volt az IS növekedésében és fenntartásában. Egy ilyen központ stabilitást ad az olyan szervezeteknek, mint az IS, a propaganda megbízható áramlását biztosítva, a hamis propaganda megjelölését lehetővé téve, és a leendő regrutáknak a kapcsolatfelvételhez kijelölt helyszínt nyújtva. Ahogy arról korábban szó esett, korábban a terrorszervezet nyílt színen toborott olyan platformokon, mint a Twitter. Ahogy a Twitter egyre keményebben lépett fel ellenük, 2015-ben a Telegram-ra váltottak, kihasználva annak lehetőségeit, a csatornákat, chat csoportokat, médiaarchiválást és a végpontok közötti titkosítást. Katz szerint ugyan az olyan technológákról, mint a dark web, gyakran gondolják, hogy megfelelnek az IS biztonsági igényeinek, azok nagyrészt alkalmatlanok a közönség eléréséhez, mivel az IS-nek ott kell lennie, ahol a felhasználók jelen vannak, különben csak „magához beszél egy üres szobában". A kutatók feladatát nehezíti az IS egyik platformról a másikra ugrálása, de a leendő újoncoknak is nehezebb azt online megtalálni. Az IS sokáig nem fog eltűnni, de Katz szerint kritikus csapás érte, mely tendenciának folytatódnia kell.[480] Egy IS támogató a Hoop és TamTam platformokról a tartalmaik eltávolításáról egy kutatók által közzétett tweet-et osztott meg a Twitter-en, hozzátéve, hogy: „Stand your ground brothers, we're getting to them, and there are blessings and victory in doing that." („Álljátok a sarat, testvérek, kezdünk az idegeikre menni, áldás és győzelem van abban.") Miközben a kutatók a bomlasztásukról beszélnek, ők mulatnak

[480] KATZ, R.: ISIS Is Now Harder to Track Online—but That's Good News. Wired. (2019, December 16). https://www.wired.com/story/opinion-isis-is-now-harder-to-track-onlinebut-thats-good-news/ (2022.01.07.)

rajta, hogy bizonytalanságban tartják az ellenük küzdőket.[481] Mivel az IS nem talál online otthont, erre a célra létrehozhat egy alkalmazást is.[482]

5. A földrajzi értelemben vett „kalifátus" elvesztése után

2019 márciusában Baguz elestével az IS elvesztette területeit, földrajzi értelemben vett „kalifátusa" megszűnt létezni.[483]

Abu Bakr al-Baghdadi, az IS vezetője 2019. október 26-án felrobbantotta magát, amikor az amerikai erők egy rajtaütés során sarokba szorították, Idlibben, Szíria északi részén.[484] Mark Esper, az USA védelmi minisztere szerint al-Baghdadi halála „egy pusztító csapást jelent az IS maradványai számára".[485] Egy nappal később al-Baghdadi valószínű utódjának tartott Abu Hassan al-Muhajirt, az IS szóvivőjét egy amerikai légicsapás ölt meg.[486] Speckhard szerint a dzsihadisták azt fogják gondolni, hogy Trump nyilatkozatával szemben a vezetőjük mártírhalált halt. Al-Baghdadi a követőit is erre szólította fel. Speckhard szerint „mártírhalála" sokakat fog inspirálni, és halála nem jelenti az IS végét is.[487]

---

[481] AMARASINGAM, A.: Telegram Deplatforming ISIS Has Given Them Something to Fight For. VOX-Pol. (2020, January 1). https://www.voxpol.eu/telegram-deplatforming-isis-has-given-them-something-to-fight-for/ (2022.01.07.)

[482] GILBERT, D.: Islamic State Can't Find an Online Home — So They Might Build Their Own App. Vice. (2019, December 3). https://www.vice.com/en_ca/article/d3ane7/islamic-state-cant-find-an-online-home-so-they-might-build-their-own-app (2022.01.07.)

[483] JOHNSTON, P. B. – ALAMI, M. – CLARKE, C. P. – SHATZ, H. J.: Return and Expand? The Finances and Prospects of the Islamic State After the Caliphate. RAND Corporation, Santa Monica, 2019. IX. o. https://www.rand.org/content/dam/rand/pubs/research_reports/RR3000/RR3046/RAND_RR3046.pdf (2022.01.05.)

[484] COHEN, Z.: Inside the dramatic US military raid that killed ISIS leader Baghdadi. CNN. (2019, October 28). https://edition.cnn.com/2019/10/27/politics/bagdhadi-inside-the-raid-timeline/index.html (2022.01.06.)

[485] BRITTON, B. – HAYES, M. – ROCHA, V. – WAGNER, M.: Baghdadi's death: More details emerge from US raid: Defense secretary: Baghdadi's death "marks a devastating blow for the remnants of ISIS". CNN. (2019, October 29). https://edition.cnn.com/politics/live-news/baghdadi-monday-dle-intl/index.html (2022.01.06.)

[486] HUBBARD, B. – SHOUMALI, K.: Likely Successor to Dead ISIS Leader Also Reported Killed. The New York Times. (2019, October 30). https://www.nytimes.com/2019/10/27/world/middleeast/al-baghdadi-successor-reported-killed.html (2022.01.06.)

[487] SPECKHARD, A.: Baghdadi Just Confirmed ISIS 'Martyrdom' Narrative, Ensuring ISIS Will Live. The International Center for the Study of Violent Extremism (ICSVE). (2019, October 30). https://www.icsve.org/baghdadi-just-confirmed-isis-martyrdom-narrative-ensuring-isis-will-live/

Mindezek ellenére a „virtuális Kalifátus” él, új tartalmakat generál, régieket hasznosít újra, az online kommunikáció és toborzás terén továbbra is aktív. Az IS internetes aktivitása továbbra is fenyegetést jelent. Az IS, az al-Kaida, és más extrémista csoportok mellett több mint 150 közösségi média felületen van jelen.[488]

Hogy az IS területeinek elvesztése, és katonai veresége nem fogta vissza az internetes jelenlétüket, jól demonstrálja, hogy a terroristák internethasználata, online radikalizációs képességei és álatlánosságban a terrorizmus fenyegetése ellen nem elegendőek a katonai eszközök.

6. Az IS Facebookon használt eltávolítást megkerülő taktikái

2020 előtti két évben a Facebook átláthatósági jelentése (transparency reporting) azt mutatja, hogy a cég a terrorizmushoz kötődő posztok 99%-át, kb. 26 millió tartalmat felfedezi és eltávolítja, még mielőtt azokat jelentenék. Az Institute for Strategic Dialogue (ISD) egy IS-támogató felhasználói fiók (továbbiakban fiók) hálózatot vizsgált a Facebookon. Ez a száz fiókból álló és több tízezer embert elérő hálózat egy szelete a független, de összefonódó hálózatoknak, melyek terrorista tartalmat terjesztenek a platformon. Az ISD kvalitatív kutatása ennek az ökoszisztémának csak a felszínét szántotta, példázva, milyen betekintés nyerhető manuális nyomozással. Hogy érthető legyen a probléma valódi mértéke és természete, egy ilyen analízist automatizáltan kell végezni. Az ISD kutatása 2020. április 07-től július 30-ig, 87 napon át tartott, mely során egy magát Fuouaris Upload-nak nevező IS támogató Facebook fiókok hálózatát követte, analizálta és elemezte annak viselkedését. A megfigyelés során 288 támogató fiókot fedeztek fel, mely közül sok több ezer követővel rendelkezett. A fiókok harmada (90) egy Luqmen Ben Tachafin nevű felhasználó irányítása alatt állt, ami a hálózat magját jelentette. Május 21-ig a hálózat 50 videót osztott meg, és több mint 34.000 nézettséget ért el. A 3 hónapos analízis során a Fuouaris Upload kiterjedt más hálózatokra is. A SoundCloud-on 2020-ban 18 brand-del ellátott fiókot kontrollált, melyek 91 IS audio-tartalmat tettek közzé. Ugyan a Fuouaris Upload fiókok 70%-a a megfigyelési időtartam alatt eltávolításra került, ezek a decentralizált hálózatok komoly szívósságot mutattak. 62 fiók került eltávolításra a fő fiókok közül, de 28 megmaradt, mely a moderáció egyenetlenségét mutatja. Ahogy az egyes fiókok eltávolításra

(2022.01.06.)

[488] SPECKHARD, A.: Is ISIS Still Alive and Well on the Internet? Homeland Security Today. (2019, January 14). https://www.hstoday.us/subject-matter-areas/terrorism-study/is-isis-still-alive-and-well-on-the-internet/ (2022.01.07.)

kerültek, az IS-es felhasználók gúnyolták a moderátorokat azért, mert nem értik a jelenlétük mértékét a felületen.[489] A kutatás az IS támogatók automatizált vagy manuális felfedezést és a terrorista tartalmak és felhasználói fiókok moderálásának akadályozását célzó új elkerülő-taktikáira mutat rá. A kutatás 6 fő taktikát azonosított: 1. Felhasználói fiók eltérítése: A Facebook egyik fő kiskapujával visszaélve két alkalmazással eltérítik más felhasználók fiókjait. Az alkalmazások lehetővé teszik a platform által küldött jelszó-helyreállítási üzenet eltérítését. Több fiók oktatóvideókat gyártott és osztott meg a módszerről. 2. Tartalom elfedése: A Facebookon az IS tartalmak kozmetikai módosításokkal élnek túl, például videó effektekkel, melyek népszerű hírcsatornák (mint France24 és BBC) megjelölését helyezik a propagandára, és az IS ikonográfiát elhomályosítják. Az ilyen tartalmak megkerülik a Facebook terrorista anyagok automatizált felfedezésére szolgáló hashing technológiáját, mely úgy látszik, nem képes felimerni az enyhén szerkesztett hivatalos terrorista médiát. 3. Link megosztás: Kommentszekciókban dzsihadista oldalakhoz vezető linkek megosztása. 4. Koordinált ún. „raid-ek" (rajtaütés, továbbiakban raid): Az IS támogatók hálózatai a Facebookon szervezett raid-eket terveznek, készítenek elő és hajtanak végre más Facebook oldalak, köztük a US Department of Defence, US Army, US Air Force Academy és Trump oldalai ellen, melyek során a kommentszekciókat elárasztják terrorista anyaggal. 5. Hashtag eltérítése: Több ilyen raid célja a globális tüntetések (pl. Libanonban és az USA-ban) körüli megosztottság generálása. IS-hez kötődő fiókok George Floyd avatarját használva posztolták, hogy: „marching to the edge you make it a challenge and we will revenge #The_Black_Is_Back." Ez a 2014-es Ferguson tüntetések alatti IS támogató fiókok taktikájára emlékeztet, akik a megosztó társadalmi problémák körüli online diskurzus eltérítését célozták és propagandát terjesztettek népszerű hashtag-ek használatával. 6. Szöveganalízis kijátszása/Gaming Text Analysis: Szöveganalízis moderálás megkerülése ún. „broken text" (szándékosan hibás szöveg) formátum vagy specializált betűtípus használatával a posztokban.[490]

7. Covid és az IS

Az IS a hivatalos al-Naba nevű hetente megjelenő hírlevelében egy egész oldalas

[489] AYAD, M.: The Propaganda Pipeline: The ISIS Fuouaris Upload Network on Facebook. Institute for Strategic Dialogue, London, 2020. 2. o. https://www.isdglobal.org/wp-content/uploads/2020/07/The-Propaganda-Pipeline.pdf (2022.01.07.)

[490] Uo. 2–4. o.

infografikát tett közzé a COVID-19 fertőzés megakadályozásáról. Hírleveleiben január óta figyelemmel kísérte a koronavírust, és rendszeresen tájékoztatott róla. „Egy új vírus terjeszt halált és rettegést Kínában", írta az al-Naba januárban. Ahogy a vírus terjedt, az IS egyre jobban kritizálta a kínai kormányt. A terrorszervezet szerint a járvány Isten büntetése, amiért Kína sanyargatja az ujgur népességet. A terrorszervezet azt tanácsolja, hogy „helyezzétek a hitetek Istenbe és keressetek Benne menedéket a betegségektől" és „az egészségesek ne lépjenek a járvány földjére, és az az által sújtottak ne távozzanak onnan". (Ehhez képest az IS hajt végre műveleteket Algériában, Egyiptomban, Irakban, Afganisztánban, Indiában, a Fülöp-szigeteken és Indonéziában, ahol vannak igazolt koronavírusos esetek.) Az IS szorgalmazza a kézmosást, és azt tanácsolja követőinek, hogy „ásításkor és tüsszentéskor takard el a szádat." Egy hadíszt is idéz a kórokozókról és fertőzésekről. Az al-Naba újabb száma szerint a koronavírus „további nyomást és terhet" ró a kormányokra, azok együttműködési képességeit a terrorizmus elleni harc terén csökkenti és biztonsági szempontból olyan rést jelent, amit ki kell használni „a párizsi, londoni, brüsszeli és más csapásokhoz hasonló" terrorcselekmények elkövetéséhez, és a foglyok kiszabadításaihoz.[491] Az IS Irakban támadásait fokozta a pandémia idején.[492]

8. Következtetések

Véleményem szerint a jövő terrorszervezetei tanulni fognak majd az IS úttörő és folyamatosan fejlődő internethasználatából és zseniális propagandatevékenységéből. Úgy vélem át fogják majd venni a módszereiket, azokból okulnak majd, és valószínűleg tovább is fejlesztik őket. A terrorizmus elleni harcnak erre fel kell készülnie.

[491] JOHNSON, B.: ISIS: Cities Distracted by Coronavirus Should be Hit with Attacks Like Paris, London, Brussels. Homeland Security Today. (2020, March 24). https://www.hstoday.us/subject-matter-areas/counterterrorism/isis-cities-distracted-by-coronavirus-should-be-hit-with-attacks-like-paris-london-brussels/ (2021.10.04.)

[492] HANNA, A.: What Islamists Are Doing and Saying on COVID-19 Crisis. Wilson Center. (2020, May 14). https://www.wilsoncenter.org/article/what-islamists-are-doing-and-saying-covid-19-crisis (2021.10.04.)

3. A Boko Haram internethasználata

1. A Boko Haram elnevezése és ideológiája

A Boko Haram Nigéria, illetve Nyugat-Afrika talán legismertebb terrorszervezete. Célja az ország teljes iszlamizálása és a saría, az iszlám törvénykezés általános bevezetése.[493] Nigéria legfőbb biztonsági fenyegetése, több támadást hajtott ott végre, mint bármely más fegyveres csoport.[494]

Részleges saría az északi államokban már 1999-től bevezetésre került, néhány államban 2000 és 2003 között, ám a Boko Haram ezt hiányosnak és nem megfelelőnek tartja.

A Boko Haram elnevezése vitatott. Elden szerint a terrorszervezet teljes, hivatalos neve „Jama'tu Ahlus Sunna Lidda'awati wal Jihad" vagy „People Committed to the Propagation of the Prophet's Teachings and Jihad" (A Próféta Tanai és a Dzsihád Hirdetésére Elkötelezett Emberek[495]), rövidítése JASLWJ vagy JAS. A szervezetnek számos nevet adtak már, köztük „Ahlulsunna wai'jama'ah hijra" és „Nigériai Talibán" és „Yusufiyyah szekta", vagy „Yusufiyah" (Yusuf mozgalma); vagy „Al-Sunna wal Jamma". Bázisát Kanamában, a Yobe államban, a Niger határ közelében a helyiek úgy ismerték, mint „Afganisztán".[496]

Az Encyclopaedia Britannica szerint a szervezet eredeti neve „Jamāʿat Ahl al-Sunnah li-l-Daʿawah wa al-Jihād", amit gyakran úgy fordítanak, hogy „Association of the People of the Sunnah for Preaching and Jihad" (A Szunna Népének Szövetsége az Prédikálásért és Dzsihádért"[497]) vagy „People Committed to the Prophet's Teaching for Propagation and Jihad") (A Prófétának a Hirdetésről és Dzsihádról Szóló Tanai Mellett Elkötelezett Emberek[498]) A Boko Haram nevet, mint a „a nyugatiasodás szakrilégium" a szomszédai adták neki az életmódja és tanításai alapján. Ennek népszerű értelmezései a „nyugati oktatás bűn" vagy a „nyugati oktatás tiltott". A Boko Haram ellenzi a nyugatiasodást,

[493] NESZMÉLYI Gy. I.: Őrségváltás Afrika óriásánál: Nigéria gazdasági és társadalmi kihívásai. In: VÁGÁNY J. – FENYVESI É. (szerk.): Multidiszciplináris kihívások, sokszínű válaszok: Tanulmánykötet. Budapesti Gazdasági Egyetem, Kereskedelmi, Vendéglátóipari és Idegenforgalmi Kar, Közgazdasági Intézeti Tanszéki Osztály, Budapest, 2016. 133. o.

[494] KULUNGU, M.: Does Boko Haram Pose a Threat to the US? Counter Terrorist Trends and Analyses, 2019. Vol. 11. No. 2. 9. o.

[495] Saját fordítás.

[496] ELDEN, S.: The geopolitics of Boko Haram and Nigeria's 'war on terror'. The Geographical Journal, 2014. Vol. 180. No. 4. 414–415. o.

[497] Saját fordítás.

[498] Saját fordítás.

ami szerinte negatívan hat az iszlám értékekre, és a nyugati hatásoknak tudható be a nigériai korrupció, és a kevés gazdag és a sok szegény közötti mély szakadék is.[499]

Agbiboa szerint a Boko Haram kifejezés a hausza boko (könyv) és az arab haram (tiltott) szavak kombinációja. Így a Boko Haramot úgy értelmezi, hogy „a nyugati oktatás tiltott.”. A terrorszervezet inkább „a nyugati kultúra tiltott” elnevezést részesíti előnyben.[500] Lock egy hausza-angol szótár alapján arra mutat rá, hogy a boko szónak négy jelentése van: nyugati oktatás, latin ábécé, világi, és csalás. Lock szerint a boko koncepciója erősen kötődik az idegenhez, idegen befolyáshoz.[501] Walker rámutat, hogy a terrorszervezet jól láthatóan nem teljesen utasítja el a modern világot, mivel előszeretettel használja a nyugati oktatás gyümölcseit, például okostelefonokat, kamerákat, YouTube-ot, automata fegyvereket etc. A Boko Haram viszont gyűlöli azokat az észak-nigériaiakat, akiket „yan boko-nak” neveznek, a „könyv gyermekeit”. Ez az elit, amit a britek Nigéria gyarmatosítására használt közvetett uralmának politikája hozott létre, akiket a könnyű pénz és züllesztő nyugati értékek elfordítottak Allah elől. A yan boko spirituálisan és morálisan korrupt, vallási áhitat nélküli, és a saját gazdagításán munkálkodik, ahelyett hogy a muszlim ummának (közösségnek) szentelné magát.[502]

A terrorszervezet a nyugati oktatást bűnnek tartja, világnézetük középkori szinten elmaradott. Vezetőjük egy már eltávolított YouTube videóban azt is állította, hogy a Föld lapos.[503]

2. A Boko Haram története

Kővári szerint Nigéria sokáig a térség meghatározó államának tűnt, amely rendelkezett azokkal a tulajdonságokkal, hogy a térség középhatalmaként akár regionális biztonsági komplexum központi elemévé váljon. Azonban az állandósuló belpolitikai válság, a Boko Haram térnyerése északon beláthatatlan időre megakasztotta az ország

[499] Boko Haram. Britannica. https://www.britannica.com/topic/Boko-Haram (2021.06.14.)

[500] AGBIBOA, D. E.: Why Boko Haram Exists: The Relative Deprivation Perspective. African Conflict and Peacebuilding Review, 2013. Vol. 3. No. 1. 145. o.

[501] BUBA, M.: Newman, Paul: A Hausa-English Dictionary: book review. Lexikos, 2008. Vol. 18. No. 1. 456-462. o. Idézi: LOCK, E.: Nigeria: Understanding Boko Haram. Conflict Studies Quarterly, 2020. No. 30. 80–81. o.

[502] WALKER, A.: What Is Boko Haram? United States Institute Of Peace, Washington D.C. 2012. 7. o. https://www.usip.org/publications/2012/05/what-boko-haram (2021.06.14.)

[503] BESENYŐ, J. – MAYER, Á.: Boko Haram in Context: The Terrorist Organizations’s Roots in Nigeria’s Social History. Defence Against Terrorism Review, 2015. Vol. 7. No. 1. 48. o.

konszolidációs folyamatát, és annak az esélyét, hogy helyreállítsa vezető szerepét a térségben.[504]

A 2001 őszi utcai erőszakban jelentek meg először Nigériában olyan erőszakos csoportok, melyek hűségesküt tettek a Yobe államból származó Ustaz Mohammed Yusuf vallási tanítónak. 2002 első felében Yusuf ezeket a csoportokat egy szervezetbe egyesítette, amit először „Yusufiyya Dawah-nak" (Yusuf tanítványai) nevezett el, aztán a populista Boko Haram nevet adoptálta. A szervezetet formálisan Maiduguriban, Borno állam fővárosában alapították, mint „Ahl as-Sunnah wa al-Jama'a ala Minhaj as-Salaf" (A Próféta Útja és a Szalafita Megközelítés Szerinti Közösség Népe[505] arabul) Yusuf-fal, mint vallási útmutatójával és de facto vezetőjével.

2004 első felében a Boko Haram a Yobe állambéli Kanamába költözött, közel a nigeri határhoz. Felállította „Afganisztán" elnevezésű bázisát, egy minden nyugati dolgot elutasító valódi muszlim társadalom létrehozása és katonai kiképzés céljából. Röviddel ezután a Boko Haram elkezdett rendőrőrsöket támadni és rendőröket ölni. A helyiek a „nigériai Talibánnak" nevezték.[506]

A Boko Haram 2009-ben fellázadt. Fegyveres akciói július 25-től 30-ig tartottak, melyek kiterjedtek Bauchi, Kano, Yobe és Borno államokra. A lázadást végül leverték, miután elfogták és megölték (állítólag rendőrségi őrizetben) a mozgalom vezetőjét, Yusuf-ot. Becslések szerint több mint 700 ember veszítette életét, számos középület semmisült meg.[507]

A 2009 nyári fegyveres akciói után a terrorszervezet jelentős technikai fejlődésen ment keresztül és létszáma is egyre bővült. Mind az AQIM-mal (al-Qaeda in the Islamic Maghreb), mind pedig a szomáliai al-Shababbal szorosabbra fűzte kapcsolatát.[508] A Hezbollahhal is lehetett kapcsolata.[509] Az al-Shabaab, a Boko Haram, illetve a Szahara

---

[504] KŐVÁRI L.: Az északi regionális biztonsági komplexum és az Északi-sarkvidéki Tanács. Felderítő Szemle, 2019/1. 20. o.

[505] Saját fordítás.

[506] BODANSKY, Y.: The Boko Haram and Nigerian Jihadism. ISPSW Strategy Series: Focus on Defense and International Security, Institut für Strategie- Politik- Sicherheits- und Wirtschaftsberatung ISPSW, Berlin, 2015. 6. o.
https://www.files.ethz.ch/isn/187751/318_Bodansky.pdf (2021.06.14.)

[507] ADESOJI, A.: The Boko Haram Uprising and Islamic Revivalism in Nigeria. Africa Spectrum, 2010. Vol. 45. No. 2. 98. o.

[508] NESZMÉLYI Gy.: Nigéria perspektívái: kibontakozás vagy káosz és terrorizmus? Nemzet és Biztonság, 2012/2. 69. o.

[509] BESENYŐ, J. – KERESZTES, V.: Hezbollah and Boko Haram: Cooperation or Imitation? Strategic

és a Száhel dzsihadista szervezetei között egyértelműen kimutatható a kooperáció, különösen a harcosok és fegyverek áramlása, illetve a módszerek, technikák átadása terén. Az al-Shabaab és az AQIM támogatása döntő szerepet játszott abban, hogy a Boko Haram módszerei alig két alatt év drámaian fejlődtek.[510]

Az új vezetője, Abubakar Shekau az interneten 2010 júliusában a következő üzenetet tette közzé: „Ez egy üzenet Goodluck Jonathan elnöknek és mindenkinek, aki a kereszténységet képviseli. Szent háborút hirdetünk! Harcolni fogunk a keresztények ellen, mert mindenki tudja, mit tettek a muszlimokkal!" A szervezet elkezdett megváltozni.[511]

Yusuf halálát fordulópontnak szokás tekinteni a Boko Haram fejlődésében. A vallási mozgalomból terrorszervezetté alakulás jól látszik a választott célpontokon, ami a kormányzatiaktól elmozdult a civil célpontok felé. Shekau vezetése alatt ez a stratégiai történő változás 2010-ben kezdődött, amikor a Boko Haram támadásainak 64%-a civileket vett célba. Célpontjainak típusa 2011-től 2013-ig kiegyensúlyozottabb volt. Ennek az egyik oka az, hogy a kormány biztonsági erőket kezdett el bevetni ellenük. A közösségi média térnyerése miatt a Boko Haramnak látványosabb támadásokat kellett végrehajtania, hogy releváns lehessen a globális dzsihadista szférában.

2014-ben az esetek 74%-ában civileket vettek célba, a kormány ellen csupán a támadásainak 22%-a indult.

Annak ellenére, hogy a kormányzat a kemény célpontokat igyekszik védeni, a Boko Haram a fókuszát a puha célpontok támadására helyezte, mivel ezek nagyobb médiavisszhangot generálnak.[512]

Kővágó a Boko Haram célpontjainak vizsgálatakor két nagy korszak között tesz különbséget. Az első kezdete a 2002-es megalakulás Yusuf vezetésével. Kővágó szerint a szervezet 2009-ig radikális volt, de alapvetően nem erőszakos. Fő céljaik közt szerepelt a társadalmi egyenlőtlenségek és a korrupció felszámolása, a saríára épülő jogrendszer felállítása, de akkoriban még elsősorban vallási szektaként működtek. Yusuf

---

Impact, 2016. Vol. 61. No. 4. 29–40. o.

[510] MARSAI V. – TRESZKAI Á.: Radikális iszlamista csoportok az afrikai kontinensen. In: MARSAI V. (szerk.): Afrika a globalizált világban: Lehetőségek és kihívások. Dialóg Campus, Budapest, 2019. 268. o.

[511] CASCAIS, A.: 10 years of radicalization: Boko Haram. Deutsche Welle. (2019, July 29). https://www.dw.com/en/10-years-of-radicalization-boko-haram/a-49781704 (2021.06.14.)

[512] STEVENSON, J. A. – PATE, A. – ASIAMA, E.: Effective counter-terrorism against Boko Haram: empirical assessments of coercion, delegitimization, incentivization and denial strategies in Nigeria (2009-2014). In: HENTZ, J. J. – SOLOMON, H. (szerk.): Understanding Boko Haram: Terrorism and Insurgency in Africa. (Contemporary Terrorism Studies). Routledge, Abingdon, 2017. 192–193. o.

halála után, Shekau vezetése alatt radikalizálódott látványosan a szervezet, és egy szélsőségesebb vonalat kezdett el követni. 2009-től folyamatosan támadtak puha, katonai és rendvédelmi célpontokat egyaránt, de ebben az időszakban még leginkább csak helyi keretek között mozogtak. Kővágó szerint a második nagy korszak az IS-hez való csatlakozástól napjainkig tart. Ekkor kezdte el a Boko Haram a szomszédos országokra, elsősorban Kamerunra, Nigerre és Csádra is kiterjeszteni befolyását.[513]

A Boko Haram 2011 augusztusában megtámadta az ENSZ abujai központját, első nemzetközi célpont elleni támadásaként.

A nemzetközi figyelem fókuszába 2014 áprilisában került, amikor 276 iskoláslányt rabolt el a Borno állam Chibok városából, mely elindította a világszintű „bring back our girls" (hozzátok vissza a lányainkat) kampányt.[514] Egy hónappal ez után Shekau egy videóban kijelentette, hogy azok a lányok, akik nem szöktek meg, a „rabszolgái". Dabiq magazinjában az IS dicsérte a lányok elrablását és a „rabszolgaság visszaállítását", ami segített megalapozni Shekau IS-nek tett hűségesküjét 2015 márciusában. Azóta Shekau harcosai több száz nőt raboltak el. Legalább 700 nigériai nő volt a Boko Haram fogságában 2019-ben.[515]

Az Amnesty International szerint a hatóságok az eset után 7 évvel sem képesek megvédeni a gyermekeket. A chiboki iskoláslányok közül 2021 áprilisában több mint 100 még mindig fogságban volt. 2014 óta számos esetben raboltak el tömegesen gyermekeket. 2020 decembere és 2021 márciusa között legalább öt emberrablási esetről számoltak be Nigéria északi részén. A további támadások kockázata a régióban körülbelül 600 iskola bezárásához vezetett.[516]

---

[513] KŐVÁGÓ P.: Az AQIM és a Boko Haram támadásainak okai és trendjének alakulása. In: MARSAI V. – VOGEL D. (szerk.): Közel Afrikához: A válságkezelés és a stabilizáció lehetőségei és kihívásai a fekete kontinensen. Dialóg Campus Kiadó, Budapest, 2017. 181. o.

[514] AFZAL, M.: From "Western education is forbidden" to the world's deadliest terrorist group: Education and Boko Haram in Nigeria. Foreign Policy at Brookings, Washington D.C. 2020. 5. o. https://www.brookings.edu/wp-content/uploads/2020/04/FP_20200507_nigeria_boko_haram_afzal.pdf (2021.06.14.)

[515] PEARSON, E. – ZENN, J.: Boko Haram, the Islamic State, and the Surge in Female Abductions in Southeastern Niger. ICCT, Hága, 2021. 3. o. https://icct.nl/app/uploads/2021/02/Pearson-And-Zenn-research-paper.pdf (2021.06.14.)

[516] Nigeria: Seven years since Chibok, the government fails to protect children. Amnesty International. (2021, April 14).
https://www.amnesty.org/en/latest/news/2021/04/nigeria-seven-years-since-chibok-the-government-fails-to-protect-children/ (2021.06.14.)

A Boko Haram 2014-ben volt hatalma csúcsán. Ekkor katonailag egy nagyjából Belgium nagyságú területet tartott ellenőrzése alatt Nigéria északkeleti részén.[517]

A 2015-ös Global Terrorism Index a Boko Haramot az IS-t is megelőzve a világ leghalálosabb terrorszervezetének nevezte. 2014-ben a terrorszervezet számlájára írható halálesetek száma 6.644 volt, ami 317%-os növekedés volt a korábbi évhez képest. Az IS az évben 6.073 halálesetért volt felelős. A két terrorszervezet számlájára volt írható 2014-ben a terrorizmus miatti halálok 51%-a. 2014-ben Nigéria tapasztalta a legnagyobb növekedést a terrorizmusnak betudható halálesetek számában, az évben az országban a terrortámadások 7.512 emberéletet követeltek, ami több mint 300%-os növekedés volt 2013-hoz képest. Nigéria adott otthont 2014 öt leghalálosabb terrorszervezetei közül kettőnek, a Boko Haramnak és a Fulani harcosoknak.[518]

A 2020-as Global Terrorism Index szerint 2019-ben Nigéria tapasztalta a második legnagyobb csökkenést a terrorizmus miatti halálos áldozatok tekintetében, mely szám 2.043-ről 1.245-re esett, mely 39,1% csökkenés, ami főleg a Fulani szélsőségesek számlájára írt terror-áldozatok számának csökkenésének volt köszönhető. A Boko Haramnak tulajdonított halálesetek száma enyhén nőtt is, amely az elmúlt évtizedben Nigéria legaktívabb terrorszervezete volt. Nigériában a terrorizmus következtében bekövetkezett halálesetek száma 2019-ben 83 százalékkal alacsonyabb, mint annak 2014-es csúcspontján.[519]

A szunnita terrorszervezet miatt 2016-ig 1,5 millió ember kényszerült otthonának elhagyására, 2015-ben többen a szomszédos országokba, Csádba, Kamerunba és Nigerbe menekültek. Kis-Benedek szerint ez is hozzájárult az Afrikából Európába irányuló menekültáradathoz, amelynek útvonala főként Líbián keresztül vezet.[520]

---

[517] MARSAI – TRESZKAI: i.m. 277. o.

[518] Global Terrorism Index 2015: Measuring and Understanding the Impact of Terrorism. Institute for Economics and Peace, Sydney, 2015. 4. o. https://www.visionofhumanity.org/wp-content/uploads/2020/10/2015-Global-Terrorism-Index-Report.pdf (2021.06.14.)

[519] Global Terrorism Index 2020: Measuring the Impact of Terrorism. Institute for Economics and Peace, Sydney, 2020. 2. o. https://www.visionofhumanity.org/wp-content/uploads/2020/11/GTI-2020-web-2.pdf (2021.06.14.)

[520] KIS-BENEDEK J.: Az Iraki és Levantei Iszlám Állam (ISIL) és az ellene folytatott küzdelem tendenciái. Hadtudomány, 2016/1–2. 33. o.

3. A Boko Haram darabokra szakadása

A Boko Haram az IS-nek tett 2015. márciusi hűségesküje belharcokhoz és széthasadáshoz vezetett. A terrorszervezet már négy különálló alcsoportból áll: a Shekau által vezetett frakcióból; a 2012-ben elszakadt és az al-Kaidával szövetségre lépett Ansaru al-Musulmina fi Bilad al-Sudanból (Ansaru); az Islamic State West Africa Province-ból (ISWAP), ami Abu Masab al-Barnawi vezetése alatt 2016-ban szakadt el; valamint a Bakurából, ami Shekau-hoz maradt hűséges, de konfliktusban van az ISWAP-pal. Jelen tanulmányban Boko Haramra utalva Afzal módszerét követve a szervezet egészét értem. A Boko Haram jelenleg főleg a Csád-tó régiójából működik, ahol Kamerun, Csád, Niger és Nigéria határai találkoznak, és alkalmanként betör ezekbe az országokba, nemzetközivé téve a konfliktust.[521]

A terrorszervezet 2015-ben majdnem 2.000 civilt ölt meg Bagában, 2018-ban egy Nigériai katonai bázis elleni támadásuk során több mint 100 katona vesztette életét.

Taktikái közé tartozik az emberrablás, lövöldözés, robbantásos támadás, lefejezések. Már nem a világ legveszélyesebb terrorszervezete, de messze nem legyőzött. 2019-ben amerikai hírszerzési becslések szerint 4.000-6.000 aktív harcosból állt, más becslések szerint háromszor ennyiből. 2019 környékén a Boko Haram növelte a puha célpontok elleni támadásait, és nőket és gyerekeket bátorított arra, hogy váljanak öngyilkos merénylővé. A támadások többsége a Borno államban történt, ezt követi Kamerun legészakibb része.

A terrorszervezet sikereit magyarázza, hogy továbbra is nagy számban toboroz, főleg a Csád-tó környékén, ahol a klímaváltozásnak is köszönhetően a szegénység és erőszak egyre nő, ahogy a szárazság a tó méretét csökkenti. Sikeresen toboroz az elkeseredett népességből kis kölcsönökkel és nagyobb jutalmak ígéretével, de teszi azt fiatal fiúk elrablásával és erőszakos besorozásával is. Cronin szerint a Boko Haram 2019-ben kevésbé támaszkodott online toborzási technikákra.[522]

Nyugat-Afrika dzsihadista térképe továbbra is alakulóban van: egy megerősödött Shekau frakcióval a Csád-tó régiójában és Borno központjában, egy feltámadó ISWAP-al (beleértve az ISGS-t, ami már hivatalosan ISWAP része) Bornóban és a Száhel övezetben, és egy új erőre kapott Ansaruval Északnyugat-Nigériában. Az Ansaru vállalta magára 2020 januárjában az északnyugat-nigériai Potiskum város emírjének

[521] AFZAL: i.m. 5. o.

[522] CRONIN, C.: Don't Forget About Boko Haram: A 2019 Update. American Security Project. (2019, June 24). https://www.americansecurityproject.org/dont-forget-about-boko-haram-a-2019-update/ (2021.06.14.)

konvoja elleni támadást. Shekau frakciója az ISWAP mellett a regionális kormányzatoknak katonailag kevésbé prioritása, talán azért, mert Shekau frakciója formálisan nem IS provincia, annak ellenére, hogy potenciálisan nagyobb veszélyt jelent a civilekre. Mindazonáltal frakciója egy releváns dzsihadista szereplő, kifejezetten azután, hogy a Bakura már Shekauhoz hűséges.[523]

4. Boko Haram és a koronavírus pandémia

Ugyan statisztikák szerint a COVID-19 afrikai terjedése messze nem volt olyan, mint Kínában, Európában vagy Amerikában, de a világ legszigorúbb korlátozásait kellett bevezetni a megfékezése érdekében. Ugyanakkor Afrika elzárkózott fő támogatóitól, ezzel nehezítve gazdasági helyzetét és kockáztatva az társadalmai amúgy is gyenge stabilitását.[524] A pandémia elleni harcban az egyik legnagyobb problémát a tömeges éhínség jelenti, melyet 2020-ra már a COVID-19 előtt is megjósoltak a szakértők.[525]

Nigéria zárlati intézkedései sebezhetőbbé tették a népességet a Boko Haram toborzásával szemben. Az népességének több mint fele kevesebb, mint napi 2 USD-nek (kb. 630 HUF) megfelelő összegből él.[526] A Boko Haram kampányai erősítésére használja ki a játvány okozta nyomorúságot. A terrorszervezet szokása munkanélküli fiatal felnőtteket toborozni szegény családokból. Jelenleg fokozza a fiatal férfiak toborzását. Ez megújult erőszakhoz vezetett a Csád-tó régiójában.[527] A Boko Haram megerősítette támadásait Nyugat-Afrikában és új területhez jutott Mozambikban.[528]

Shekau a koronavírus nigériai megjelenése óta számos hangüzeneteket tett közzé. Egy 2020. április 14-i üzenetben egyetértett az IS/al-Kaida narratívával, hogy a koronavírus a

[523] ZENN, J.: Is the 'Bakura Faction' Boko Haram's New Force Enhancer Around Lake Chad? Terrorism Monitor, 2020. Vol. 18. No. 2. 5. o.

[524] BESENYŐ, J. – KÁRMÁN, M.: Effects of COVID-19 pandemy on African health, poltical and economic strategy. Insights into Regional Development, 2020. Vol. 2. No. 3. 630. o.

[525] BESENYŐ J. – Kármán M.: A COVID-19 pandémia az afrikai kontinensen. Biztonságtudományi Szemle, 2020/2. 39. o.

[526] AGBIBOA, D. E.: COVID-19, Boko Haram and the Pursuit of Survival: A Battle of Lives against Livelihoods. City & Society, 2020. Vol. 32. No. 2. 1–2. o.

[527] BELLINGER, N. – KATTELMAN, K.: How the coronavirus increases terrorism threats in the developing world. The Conversation. (2020, May 26). https://theconversation.com/how-the-coronavirus-increases-terrorism-threats-in-the-developing-world-137466 (2021.08.31.)

[528] SIMONS, G. – BIANCA, C.: The Specter of Terrorism During the Coronavirus Pandemic. E-International Relations. (2020. May 8). https://www.e-ir.info/2020/05/08/the-specter-of-terrorism-during-the-coronavirus-pandemic/ (2021.06.14.)

világ gonoszai elleni büntetés és elutasította a tudományt, ami mással magyarázná a vírus eredetét. Szerinte a Boko Haram immunis a vírussal szemben, amit az imádságnak és a hitetlenek megbüntetésének tud be. Szerinte a társadalmi távolságtartás (social distancing) rossz dolog, de önmagának ellentmondva azt is állította, hogy a Boko Haram társadalomtól való izolációja megakadályozza, hogy elkapják a vírust, továbbá a világ számos vezetőjét vezeklésre szólította fel.[529]

A Boko Haram kijelentése, mi szerint elutasítja a társadalmi távolságtartással kapcsolatos kormányzati intézkedéseket, a támogatását növelheti, mert a távolságtartási és zárlati intézkedések nagyon népszerűtlenek. A szélsőséges csoportok ilyen jellegű kijelentései (az IS szerint a mecseteknek nyitva kellene maradniuk) fokozhatják a vírus terjedését.[530]

5. Shekau halála

Shekau halálhíréről az utóbbi 12 évben már többször számoltak be, ennek ellenére később mindig feltűnt egy újabb videóban.

Az ISWAP 2016-ban vált ki Shekau csoportjából, ami vallási és ideológiai vitákra vezethető vissza azzal kapcsolatban, hogy a Boko Haram civileket ölt, amit az ISWAP ellenzett.

2021 áprilisában csapott össze újra Shekau frakciójával, akik rajtaütöttek egy ISWAP brigádon, emiatt májusban az ISWAP támadta meg Shekau egy bázisát. Az ISWAP 2021 májusában megtámadta Shekaut a Sambisa erdőben.[531] Amikor az ISWAP elfoglalta az erdőt, Shekau megadta magát és órákon át tanácskozott velük, akik lemondásra szólították fel, amit elutasított és felrobbantotta magát.[532] Ha valóban halott, az a két frakció közötti harc végét és akár egybeolvadásukat is eredményezheti. Ezzel konszolidálhatják befolyásukat az északkelet-nigériai régió felett, ahol 2009 óta már több mint 40.000 ember veszítette életét, és több mint 2 millió kényszerült otthonának

[529] OLAYOKU, P.: Boko Haram and the Covid-19 Propaganda Dynamics. Spoor Africa, 2020. 9. o. https://spoorafrica.org/storage/data/spoorafrica.org/6b7b0ab7-c49d-49ae-98ca-30febb4a61cf.pdf (2021.06.14.)

[530] BURCHILL, R.: Extremism in the time of COVID-19. Bussola Institute, Brüsszel 2020. 15-16. o.

[531] Nigerian army investigates reports of Boko Haram leader's death. Al Jazeera. (2021, May 21). https://www.aljazeera.com/news/2021/5/21/nigeria-investigates-reports-of-boko-haram-leaders-death (2021.06.14.)

[532] ABDULLAHI, M. – ADEBAJO, K.: Boko Haram Strongman, Shekau, Dead As ISWAP Fighters Capture Sambisa Forest. HumAngle. (2021, May 20). https://humangle.ng/boko-haram-strongman-shekau-dead-as-iswap-fighters-capture-sambisa-forest/ (2021.06.14.)

elhagyására, ahogy a harc a szomszédos Csádra, Kamerunra és Nigerre is kiterjedt.[533] Shekau halála az IS befolyását is növelheti a régióban.[534] Abu Musab al-Barnawi ISWAP vezető audió-üzenetben számolt be Shekau haláláról.[535]

6. A Boko Haram internethasználata

1) A Boko Haram korai internethasználata

2009-ben a Boko Haramnak még nem volt online stratégiája. Újságírókat keresett fel, és audió kazettákat osztogatott a nigériai utcákon, korábbi vezetője, Yusuf előadásairól.[536] A Boko Haram az IS, az al–Kaida és sok más terrorszervezet mellett stratégiailag felfedezte az internetet a tevékenységei elősegítéséhez.[537]

2013 óta már folyamatosan teszi közzé videóit és más online kiadványait. A videók között találhatóak támadásokról készült felvételek, vezetők üzenetei és hűtlen tagok lefejezései is.

Az internet és a közösségi média lehetővé tették a terrorszervezet számára, hogy Nigérián kívüli terrorista csoportokkal is együttműködjön és terjessze ideológiáját. Néhány videóban tagjai azzal is fenyegetőztek, hogy megtámadják az Egyesült Államokat.[538]

A Boko Haram üzeneteinek elérése kiszélesedett az internet és közösségi média fokozódó használatával, tovább növelve a közönségét. A Boko Haram 2010-es újjáéledésétől napjainkig az internet-hozzáférés gyorsan nőtt Nigériában, 2012 és 2015 között megtriplázódott, nagyrészt a mobiltechnológia elterjedése miatt. 2016-ra a

[533] Nigerian army investigates reports of Boko Haram leader's death. Al Jazeera. (2021, May 21). https://www.aljazeera.com/news/2021/5/21/nigeria-investigates-reports-of-boko-haram-leaders-death (2021.06.14.)

[534] BURKE, J.: Rise of Isis means Boko Haram's decline is no cause for celebration. The Guardian. (2021, May 22). https://www.theguardian.com/world/2021/may/22/rise-isis-means-boko-haram-decline-no-cause-celebration (2021.06.14.)

[535] Boko Haram leader 'is dead,' jihadist rivals claim. Deutsche Welle. (2020, June 6). https://www.dw.com/en/boko-haram-leader-is-dead-jihadist-rivals-claim/a-57795611 (2021.06.14.)

[536] COX, K. – MARCELLINO, W. – BELLASIO, J. – WARD, A. – GALAI, K. – MERANTO, S. – PAOLI, G. P.: Social Media in Africa: A Double-Edged Sword for Security and Development: Research report. United Nations Development Programme, Cambridge, 2018. 22. o. https://www.africa.undp.org/content/rba/en/home/library/reports/social-media-in-africa-.html (2021.06.14.)

[537] APAU, R.: Youth And Violent Extremism Online: Countering Terrorists Exploitation And Use Of The Internet. African Journal on Terrorism, 2018. Vol. 7. No. 1. 22. o.

[538] KULUNGU: i.m. 9. o.

népesség 46%-ának volt internet-hozzáférése, de az ország északi része elmarad a gazdaságilag fejlettebb dél mögött. Ez emelkedés egybeesett a Boko Haram fokozódó internethasználatával. 2015-ben 28 volt elérhető a YouTube-on és Twitteren, míg 2012-ben csak 6.

A propaganda online terjesztése csökkenthette a sajtót rendszeresen tájékoztató szóvivő szükségét is. Qaqa, a Boko Haram szóvívője a halála után nem is került helyettesítésre.

A hagyományos módszerek, a szórólapok és a helyi szintű prédikálás földrajzi elérése korlátozott. Ugyan a nigériai újságokban rövid sajtónyilatkozatokkal a szervezet üzenetét terjesztették országos szinten, de ennek közvetett volta miatt a narratívájuk irányítása kikerült a Boko Haram kezéből, és tartalmaik korlátozottabbak voltak, főleg vizuálisan. Az üzenetek ilyen módokon való terjesztése további aggályokkal jár, tekintve a terjesztést, az olvasottságot, amik korlátozza a célközönség elérését.

Ezzel szemben a javuló internet-hozzáférés és az okostelefonok fejlődő technológiája lehetővé tette a videók közvetlen letöltését, nézését és megosztását. Bizonyos videók igen nagy nézettséget generáltak, mint a 2014. május 5-i felvétel, melyben Shekau magára vállalta a chiboki iskoláslányok elrablását. A Sahara Reporters híroldal YouTube csatornája, a SaharaTV által feltöltött videó egy hónap alatt közel 500.000 megtekintést generált. A forgalom nagy része Nigérián kívülről származott, amin az is segített, hogy a videóhoz a Sahara Reporters angol fordítást is adott, továbbá az, hogy a téma globálisan felkapott volt. A videó jól illusztrálta, hogy ilyen módszerrel a Boko Haram már egy globalizált közönség elérésére képes. Az internetre támaszkodásnak persze vannak hátulütői is, például a vidéki területeken való korlátozott internet-hozzáférés.[539]

2) Az IS-nek tett hűségeskü hatása a Boko Haram online képességeire

A Boko Haram online stratégiájáról a Cox et al. a következő fő megállapításokat teszi: A terrorszervezet a közösségi médiát főleg propaganda megosztására, és kisebb mértékben újoncok bevonzására és tevékenységeinek koordinálására használja. A Boko Haram korábban a média hagyományosabb formáit részesítette előnyben, mint audió kazetták, szórólapok, szabadtéri előadások, de 2015 óta nagyobb mértékben támaszkodott a YouTube-ra, Twitterre és Facebookra az üzenetei terjesztéséhez. A Boko Haram közösségi média használata nem annyira kifinomult, mint az al-Shabaab és IS-é,

[539] MAHMOOD, O. S.: More than propaganda A review of Boko Haram's public messages. Instutute for Security Studies, Pretoria, 2017. 24–25. o.
https://www.ecoi.net/en/file/local/1426834/1226_1521122538_war20.pdf (2021.06.14.)

de fejlődött az IS-nek tett hűségesküje óta.[540] Hatásuk a Boko Haramon erősen érezhető. A terrorszervezet az IS taktikáit másolja, kifejezetten a közösségi média (főleg a YouTube) használatában. Nyomtatott és videó-propagandája kísértetiesen hasonlít az IS-ére. Még Shekau és más vezetők öltözete is az IS-t és a tálibokat másolja. Shekau az interneten tett hűségesküt, egy hivatalos közvetítésben, melyet az IS néhány nappal később elfogadott azzal, hogy azt az Al-Furqan médiaszárnyának egy szóvivője megerősítette.[541] A terrorszervezet az IS-nek tett hűségesküje és a „rebranding" által hozzájutott az IS jól megalapozott és jelentős közösségi média-bázisához és szakértelméhez.

Mikor 2015-ben létrejött az ISWAP, a terrorszervezet Media Office of West Africa Province névvel felállította a saját médiaosztályát, és fokozottabban használta a YouTube-ot és Twittert is. 2015-ben létrehozta saját arab nyelvű Twitter fiókját, @Al Urwah al-Wuthqa-t, és javított a közzétett videói minőségén is. A változások ellenére a Boko Haram videóinak tartalmi lényege nem változott.

A közösségi média is egyre szélesebb körben elérhető Nigériában. Mivel az elégedetlen fiatalság egyre inkább a Twitter, Facebook, YouTube és más közösségi média platformokhoz fordul, a Boko Haram egyre jobban fókuszál az online tevékenységeire, amit az IS-szel való kapcsolat is segít. A Boko Haram növekedését a potenciális újoncainak állammal szembeni sérelmei is segítették. Cox et al. szerint úgy tűnik, a Boko Haram a közösségi médiát elsődlegesen propaganda célokra használja, és csak kisebb mértékben toborzásra és koordinációra.[542]

Kommunikációs csatornáin az IS is megosztott ISWAP felvételeket, saját stilisztikájával feljavítva, ami fokozódó együttműködést és a két szervezet közötti kommunikációt jelez.[543] Nem véletlen, hogy az ISWAP használja a legnagyobb szakértelemmel a YouTube-ot.[544]

3) Toborzás a közösségi média használatával

Maza et al. rávilágít arra, hogy a legtöbb terrorszervezethez hasonlóan a Boko Haram

[540] COX – MARCELLINO – BELLASIO – WARD – GALAI – MERANTO – PAOLI: i.m. 22. o.

[541] ANUGWOM, E. E.: The Boko Haram Insurgence in Nigeria: Perspectives from Within. Palgrave Macmillan, London, 2019. 200. o.

[542] COX – MARCELLINO – BELLASIO – WARD – GALAI – MERANTO – PAOLI: i.m. 22-23. o.

[543] Facing the Challenge of the Islamic State in West Africa Province. International Crisis Group. (2019, May 16). https://www.crisisgroup.org/africa/west-africa/nigeria/273-facing-challenge-islamic-state-west-africa-province (2021.06.14.)

[544] ONYIA, Ch.: Understanding the ISIS Threat in the Lake Chad Basin. African Journal on Terrorism, 2020. Vol. 9. No. 1. 65. o.

különböző módszerek és taktikák alkalmazásával toboroz, például jobb élet és gazdasági helyzet hamis ígéretével. Erőszakkal is soroznak be, elrablással és fenyegetéssel. Toborzási taktikájuk még küszködő kereskedők készpénzes kölcsönnel való támogatása, de radikalizációra és toborzásra felhasználják az intézményes vallást és internetet is, főleg a közösségi média felületeit. A gyanútlan személyeket meggyőzik arról, hogy a nyugati civilizáció nem csak haram (tiltott), hanem az aláássa az iszlám hagyományos családi, vallási és társadalmi értékeit is. Ezzel a negatív narratívával csalogatnak olyanokat a szervezetbe, akik úgy hiszik, hogy egy pozitív társadalmi változáshoz járulnak hozzá.[545] A Boko Haram toborzott börtönökből szabadított rabok közül is.[546]

Salifu és Ewi 2017-ben arra világít rá, hogy a felfogás, miszerint a Boko Haram a közösségi médiát használja toborzáshoz, összhangban áll a nigériai vezető, Muhammadu Sanusi, Kano emírjének álláspontjával is, aki szerint a Boko Haramhoz csatlakozó fiatalokat ebben a közösségi média befolyásolta. Viszont Salifu és Ewi szerint a szakirodalmi áttekintés nem olyan kategorikus a közösségi média szerepével kapcsolatban, mely egyes elemzők szerint a Boko Haram toborzásának növekvő, de még nem jelentős forrása. Néhány elemző szerint a terrorszervezet ugyan használta a közösségi médiát, de nem olyan mértékben és olyan hozzáértő módon, mint más terrorszervezetek, például az IS.[547]

Botha et al. 2017-es monográfiája szerint a Boko Haram toborzáshoz főleg a hagyományos közösségi hálózatokat használja. Online toborzása nem olyan erős, mint például az IS-é, de mégis jentős. Nagyobb hatása lehet a közösség nyomásának, például a barátokénak.[548]

Összességében a Boko Haram leggyakoribb toborzási stratégiái a család és közösségi hálózatok felhasználása, prédikálás a mártírságról, pénzügyi ösztönzés, sorozás, az

[545] MAZA, K. D. – KOLDAS, U. – AKSIT, S.: Challenges of Countering Terrorist Recruitment in the Lake Chad Region: The Case of Boko Haram. Religions, 2020. Vol. 11. No. 2. 14–15. o.

[546] ONUOHA, F.: Boko Haram and the evolving Salafi Jihadist threat in Nigeria. In: PÉROUSE DE MONTCLOS, M-A. (szerk.): Boko Haram: Islamism, politics, security and the state in Nigeria. African Studies Centre, Leiden, 2014. 163. o.

[547] SALIFU, U. – EWI, M.: Boko Haram and violent extremism: Perspectives from peacebuilders. Institute for Security Studies, Pretoria, 2017. 7–8. o. https://media.africaportal.org/documents/policybrief97_1.pdf (2021.06.14.)

[548] BOTHA, A. – EWI, M. – SALIFU, U. – ABDILE, M.: Understanding Nigerian citizens' perspectives on Boko Haram. Institute for Security Studies, Pretoria, 2017. 35. o. https://issafrica.s3.amazonaws.com/site/uploads/monograph196.pdf (2021.06.14.)

interneten, és a szemtől szemben történő toborzás.[549]

Malefakis 2019-ben arról számol be, hogy a Boko Haram kevésbé sikeres a közösségi média használatával történő közvetlen toborzásban, mint például az IS vagy al-Kaida. Más terrorszervezetekkel szemben, melyek közösségi médián toboroznak, a Boko Haram inkább a fizikai valóságban történő, szemtől szembeni toborzásra támaszkodik, mivel a legtöbb helyszínen, ahol tevékenykednek, a népesség körében alacsony az olvasottság, és kevésbé értenek a modern technológiához. Mindazonáltal a Boko Haram a közösségi médiát számos tevékenységre használja: terrortámadások magukra vállalására, sejt-tagokkal és szimpatizánsokkal való kommunikációra és tájékoztatására, propaganda terjesztésére.[550]

Sinkó 2021-es tanulmányában igazolja, hogy a közösségi média kulcsszerepet játszik a Boko Haram online toborzásában. Sinkó szerint ugyan az online befolyásolás fontos a toborzás szempontjából, de hangsúlyozni kell, hogy a helyi viszonyok között az továbbra is többnyire offline, tényleges kapcsolatok útján jön létre.[551]

Úgy vélem, csak idő kérdése, hogy a Boko Haram online toborzásának a jelentősége nőjön, a modern technológia és az internet-hozzáférés nigériai terjedésével.

4) A Boko Haram internethasználata napjainkban

A Statista adatai szerint 2021 januárjában Nigériának már körülbelül 33 millió aktív közösségi média felhasználója volt. A WhatsApp alkalmazás a legnépszerűbb felület az országban, több mint 90 millió felhasználóval, ezeket követi a Facebook, YouTube, és Instagram.[552] Az okostelefonok népszerűek Nigériában: a Statista adatai alapján 2020-ban a nigériai népesség 41,4%-a mobil eszközzel internetezett, mely arány 2025-re előreláthatólag 64,9%-ra fog nőni. 2020-ban a mobil internet használók száma Nigériában 85,26 millió volt.[553]

A Boko Haram használja a YouTube-ot, Twittert, és Facebookot, és van egy blog12

[549] OMENMA, J. T. – HENDRICKS, Ch. – AJAEBILI, N. C.: al-Shabaab and Boko Haram: Recruitment Strategies. Peace and Conflict Studies, 2020. Vol. 27. No. 1. 14. o.

[550] MALEFAKIS, M. A.: Social Media Dynamics in Boko Haram's Terrorist Insurgence. Policy Brief No. 50. Toda Peace Institute, Tokyo, 2019. 5–6. o. https://toda.org/assets/files/resources/policy-briefs/t-pb-50_medinat-a.-malefakis_social-media-dynamics-and-boko-harams-terrorist-insurgence.pdf (2021.06.14.)

[551] SINKÓ, G.: Shifting the Battle to Social Media: The Effectiveness of Boko Haram's Online Strategy in Terms of its Recruitment. Belügyi Szemle, 2021/1. különsz. 137. o.

[552] Total number of active social media users in Nigeria from 2017 to 2021. Statista. https://www.statista.com/statistics/1176096/number-of-social-media-users-nigeria/ (2021.06.14.)

[553] Mobile internet user penetration in Nigeria from 2015 to 2025. Statista. https://www.statista.com/statistics/972900/internet-user-reach-nigeria/ (2021.06.14.)

hivatalos weboldala a „http://www.usufislamicbrothers.blogspot.com” címen.[554] Már a Telegram üzenetküldő alkalmazást és WhatsApp-ot is használja. Az ISWAP egyszerre 50 WhatsApp fiókot is üzemeltet. Azért ilyen sokat, mert azokat az alkalmazás működtetői folyamatosan törlik. Ha onnan az összes fiókot törlik, átváltanak a Telegram használatára. A Boko Haram a technológiai eszközeihez, számítógépekhez, okostelefonokhoz támadásai során szokott hozzájutni.[555]
A Boko Haram egy frakciója által a Csád-tó Bohoma-félszigetén 2020. március 23-án körülbelül 400 harcos motorcsónakokon érkezve megtámadta a csádi helyőrséget. Körülbelül 100 katona vesztette életét, 50 megsérült, néhányukat foglyul ejtettek. A dzsihádisták 24 katonai járművet semmisítettek meg, amiket már nem tudtak elvinni. A Telegram üzenetküldő alkalmazáson a JAS vállalta magára a támadást.[556]
2020 decemberében több mint 300 diákot raboltak el a Katsina állambeli Kankara városából. Az iskolának 839 diákja van, közülük 333 tűnt el a támadásban.[557] Shekau a WhatsApp-on egy audió-üzenetben vállalta fel a több mint 300 iskolásfiú elrablását.[558]

7. Következtetések

A Boko Haram elleni hatékony fellépésnek rendkívül komplexnek kellene lennie[559], melynek részletes kifejtése jelen értekezés keretein túlmutat.
Egyetértek Arlettel, aki rávilágít arra hogy a terroristák a legújabb technológia segítségével tudnak toborozni és megszerezni a szükséges erőforrásokat, ezért
a terrorelhárítási szervek számára is elengedhetetlen a legmodernebb szoftverek, például nyílt forráskódú programok használata, mint a Google Earth vagy a különféle kép- és mozgóképelemző alkalmazások. A Boko Haram aktivitásának műholdas képek általi vizsgálatával elsajátíthatók a lépések, melyek ezek a programok hatékony használatához

[554] OGUNLANA, S. O.: Halting Boko Haram / Islamic State’s West Africa Province Propaganda in Cyberspace with Cybersecurity Technologies. Journal of Strategic Security, 2019. Vol. 12. No. 1. 91. o.

[555] Boko Haram: How di insurgents dey get internet to post videos, make calls from inside bush? BBC News. (2020, December 7) https://www.bbc.com/pidgin/tori-55212200 (2021.06.14.)

[556] Behind the Jihadist Attack in Chad. International Crisis Group. (2020, April 6). https://www.crisisgroup.org/africa/central-africa/chad/derriere-lattaque-jihadiste-au-tchad (2021.06.14.)

[557] Több mint háromszáz diákot rabolt el a Boko Haram. Honvedelem.hu. (2020. december 16.). https://honvedelem.hu/hirek/tobb-mint-haromszaz-diakot-rabolt-el-a-boko-haram.html (2021.06.14.)

[558] Nigeria's Boko Haram behind schoolboys' abduction - audio message. Reuters. (2020, December 15). https://www.reuters.com/article/nigeria-security-kidnappings-idUSKBN28P2DL (2021.06.14.)

[559] OLOFINBIYI, S. A.: The Intractable Malaise: Understanding the Patterns That Maintain the Terrorist Stronghold in Nigeria. SAGE Open, 2021. No. 2. 8. o.

szükségesek. A terrorszervezetek aktivitása gyakran megjelenik nyomtatott és virtuális felületeken, ezért a műholdképek elemzésén túl értékes információk gyűjthetők másodlagos források nyílt forráskódú szoftverekkel való tanulmányozásával is.[560]

Álláspontom szerint a Boko Haram internethasználatának jelentősége a jövőben nőni fog, tekintve az egyre növekvő internet-hozzáférést Nigériában és az IS potenciálisan nagyobb befolyását a terrorszervezetre. A Boko Haram internetes aktivitásának, az online történő toborzásának fejlődését, esetleges változásait figyelemmel kell kísérni.

[560] ARLETT A.: Hírszerzés nyílt forráskódú programok használatával. Stratégiai Védelmi Kutatóintézet: NÉZŐPONTOK, 2019. 5. sz. 1. o.

XI. A SZÉLSŐJOBBOLDALI TERRORIZMUS ONLINE

1. A szélsőjobboldali terrorizmus és globális előretörése

Mudde a jobboldali extrémizmus 26 szakirodalmi definíciója alapján annak 58 jellemzőjét azonosítja, és rávilágít, hogy ezek közül csak öt jelenik meg valamilyen formában legalább a vizsgált szerzők felénél: nacionalizmus, rasszizmus, xenofóbia, anti-demokrácia és erős állam.[561]

A jobboldali extrémizmus elleni küzdelem egyik kihívása, hogy nincs egy csoportokat összekötő egyesítő ideológiai rendszer. Több alapul szolgáló hitrendszert vizsgáltak már szélsőjobboldali szereplőknél, köztük kormányellenes, antiglobalista, bevándorlásellenes, szuverén polgár mozgalmakat (sovereign citizen movements), paramilitáris csoportokat, neonácikat, odinistákat és faji ideológiai alapú csoportokat.[562]

A jobboldali extrémizmus összetett ideológiáinak részletes[563] ismertetése jelen dolgozat kereteit szétfeszítené, ezért azokban csak olyan mélységben merülök el, amennyire a jelen mű célkitűzéséhez feltétlenül szükséges.

Előzetesen szükséges az alt-right (alt-jobb) definiálása: „Ugyan a mozgalom hirhedten nehezen meghatározható, néhány átfogó téma körvonalazható: a bevándorlást és a multikulturalizmust határozottan elutasítja a legtöbb, ha nem az összes alcsoport; a feminizmust intenzíven kritizálják, különösen a manoszféra közössége, amely több klánra oszlik, különböző célokkal és szubkultúrákkal (men's rights activists, Men Going Their Own Way, pick-up artists, incelek)."[564]

9/11 óta a jobboldali terrorizmust elhomályosította a szélsőséges iszlám terrorizmus okozta aggodalom. Ez kezd megváltozni. Az utóbbi évtizedben szélsőjobboldali terroristák világszerte szalagcímekre kerültek, például a 2011 júliusában, a norvégiai Oslóban és Utøya szigetén, 2015 júniusában a dél-karolinai Charleston-ban, 2017

[561] MUDDE, C.: The Ideology of the Extreme Right. Manchester University Press, Manchester/New York, 2000. 11. o.

[562] HOLT, T. J. – FREILICH, J. D. – CHERMAK, S. M.: Examining the Online Expression of Ideology among Far-Right Extremist Forum Users. Terrorism and Political Violence, 2020. 2. o.

[563] A jobboldali extrémizmus ideológiájáról bővebben: BOROSS Zs. A.: A jobboldali extrémizmus összetett ideológiája – mint a terrorizmus potenciális hivatkozása. TERROR & ELHÁRÍTÁS, 2017/4. 23–48. o.

[564] DAFAURE, M.: The "Great Meme War:" the Alt-Right and its Multifarious Enemies. Angles, 2020. Vol. 10. No. 2. 1. o.

januárjában Québec-ben, 2019 márciusában Christchurch-ben és 2019 augusztusában az El Paso-ban elkövetett merényletekkel. Ahogy a nyilvánosság egyre tájékozottabb a jobboldali terrorizmus fenyegetésével kapcsolatban, és a politikai döntéshozók elkezdik a problémát kezelni, fontos, hogy azt a terrorizmus e típusának a lehető legalaposabb megértése mellett tegyék.[565]

Az extrém jobboldal erőszakát és terrorizmusát mostanáig relatíve gyakori incidensek jellemezték, kevés áldozattal. Mivel az utóbbi két évtizedben elhomályosította a nagy léptékű, sok áldozatot követelő dzsihadista terrorizmus, a szélsőjobboldali terrorizmus alacsonyan szerepelt a biztonsági napirenden. Ugyanakkor a kisebb, de gyakori extrém jobboldali támadások is például több száz migránst öltek meg Oroszországban, 2006 és 2010 között. Az USA-ban 9/11 óta több embert öltek meg jobboldali extrémisták, mint iszlamisták. A Norvégiában 2011. július 22-én, és az új-zélandi Chistchurch-ben, 2019. március 15-én elkövetett terrortámadások bizonyították, hogy az extrém jobboldali nézetek által inspirált magányos elkövetők készek és képesek nagyszámú ember megölésére. Ezek az incidensek többé nem kivételes esetek, hanem Bjørgo és Ravndal szerint ezek új mércét állítottak az extrém jobboldali terroristák egy új generációja elé. Műveleteiket egyedül hajtják végre, de virtuális közösségek kötik össze őket az interneten, ahol számos személy inspirálódott példaképei modus operandijának utánzására, és arra, hogy őket túl próbálja szárnyalni. Azzal, hogy egyre több törvényhozó, politikus és kutató megkésve felismeri az extrém jobboldal terrortámadásokra való potenciálját, a tárgy visszakerült a napirendre. Egyetértek Bjørgo és Ravndal álláspontjával, hogy a témát illetően több kutatáson alapuló tudásra van szükség, mégpedig az erőszak volumenéről, a célpontok kiválasztásáról, az elkövetőkről, és a könnyítő körülményekről.[566]

2. A szélsőjobboldali terrorizmus fokozódása az EU-ban

Bartkó 2019-ben az Europol jelentéseiből[567] kiindulva rögzítette, hogy az elmúlt

[565] BLACKBOURN, J. – MCGARRITY, N. – ROACH, K.: Understanding and responding to right wing terrorism. Journal of Policing, Intelligence and Counter Terrorism, 2019. Vol. 14. No. 3. 183. o.

[566] BJØRGO, T. – RAVNDAL, J. A.: Extreme-Right Violence and Terrorism: Concepts, Patterns, and Responses. ICCT Policy Brief, Hága, 2019. 2. o. https://icct.nl/app/uploads/2019/09/Extreme-Right-Violence-and-Terrorism-Concepts-Patterns-and-Responses-4.pdf (2021.07.21.)

[567] European Union Terrorism Situation and Trend report (TE-SAT) 2015. Europol, 2015. https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-

években a dzsihadista terrorizmus erősödött meg az EU területén.[568] A szélsőjobboldali terrorizmus megerősödése is megfigyelhető: Az Europol 2019-es Terrorism Situation and Trend Report-ja (továbbiakban TE-SAT) szerint az ahhoz fűződő letartóztatások száma viszonylag alacsony volt, de harmadik éve nőtt. A 2018-as terrorizmushoz fűződő büntetőügyek alapján a dzsihadista terrorista elítélések száma volt a legmagasabb, de a baloldali és jobboldali terrorista elítélésekben növekvés volt tapasztalható.[569] A trend folytatódik. Az Europol 2020-as jelentése szerint 2019-ben 3 EU tagállam összesen hat jobboldali terrorcselekményt jelentett (egy befejezett, egy sikertelen, négy megakadályozott), 2018-ban csak egyet. Két támadást jelentett Németország, melyek a nemzeti jogszabályok szerint nem minősítettek terrorizmusnak, de azokat jobboldali extrémisták követték el, és három életet követeltek.[570] A 2021-es TE-SAT szerint 2020-ban egy sikertelen jobboldali támadásról számolt be Belgium, egy megakadályozottról Franciaország, és egy befejezettről és egy megakadályozottról Németország. A haunau-i támadás 9 életet követelt. 2020-ban számos tagállamban tartóztattak le szélsőjobboldali terrortámadást vagy erőszakos extrémista támadást elkövetni tervezőket. Az erőszakos online közösségekhez köthető gyanúsítottak egyre fiatalabbak. Erőszakos neonáci és fehér felsőbbrendűsűget hirdető csoportokat szereltek le és/vagy tiltottak be számos tagállamban. 2020-ban a köz tudatossága nőtt a klíma- és ökológiai problémákkal kapcsolatban, mely ahhoz vezetett, hogy a jobboldali extrémisták fokozottabban hirdetnek ökofasiszta nézeteket. Videojátékokat és videojátékos kommunikációs alkalmazásokat fokozottabban használják jobboldali terrorista és extrémista propaganda

---

trend-report-2015 (2021.07.27.); European Union Terrorism Situation and Trend report (TE-SAT) 2016. Europol, 2016. https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-te-sat-2016 (2021.07.27.); European Union Terrorism Situation and Trend report (TE-SAT) 2017. Europol, 2017. https://www.europol.europa.eu/activities-services/main-reports/eu-terrorism-situation-and-trend-report-te-sat-2017 (2021.07.27.); European Union Terrorism Situation and Trend report (TE-SAT) 2018. Europol, 2018. https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-2018-tesat-2018 (2021.07.27.)

[568] BARTKÓ R.: Az illegális migráció és a terrorizmus kapcsolata az EUROPOL és FRONTEX jelentéseire tekintettel. In: BARTKÓ R. (szerk.): A terrorizmus elleni küzdelem aktuális kérdései a XXI. században. Gondolat Kiadó, Budapest, 2019. 177. o.

[569] European Union Terrorism Situation and Trend Report (TE-SAT) 2019. Europol, 2019. 6–7. o. https://www.europol.europa.eu/activities-services/main-reports/terrorism-situation-and-trend-report-2019-te-sat (2021.07.15.)

[570] European Union Terrorism Situation and Trend report (TE-SAT) 2020. Europol, 2020. 6. o. https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-te-sat-2020 (2021.07.15.)

terjesztésére, főleg fiatalok között. A COVID-19 felgyorsította a jobboldali extrémista propaganda online terjesztését, akik visszaélnek a pandémiával hogy támogassák az akceleracionalista narratíváikat és az antiszemita, bevándorlás-ellenes és anti-iszlám nézeteket valló összeesküvés-elméleteiket.[571]

3. Szélsőjobboldali elkövetők internethasználatának sajátosságai a nagyobb terrorcselekményekkel kapcsolatban

A Stormfront-on, a legrégebbi, legnagyobb, leglátogatottabb és legaktívabb jobboldali extrémista web fórumon[572] 2008-ban egy felhasználó amellett érvelt, hogy Nagy-Britannia a muszlim bevándorlás miatt polgárháborúval néz szembe. 2011. július 22-én ugyanez a személy, akit Anders Breivik néven azonosítottak, 77 embert ölt meg az Oslo belvárosában és Utøya szigetén elkövetett terrortámadás során, Norvégiában. Röviddel a támadás előtt egy 1500 oldalas manifesztumot posztolt a Stormfront-ra, és ezreknek küldte el e-mailben. Az eset nem elszigetelt. Korunk terroristái az extrémista fórumok és a közösségi média platformjainak aktív használói.[573] Az utóbbi években számos jelentősebb szélsőjobboldali terrortámadást kísért az elkövető által közzétett részletes manifesztum, amiben felvázolták az ideológiájukat, a motivációikat és a taktikai megfontolásaikat. Mivel az ilyen manifesztumok hamar a szélsőjobboldali erőszak esszenciális részévé váltak, Ware szerint sürgősen részletes elemzésükre van szükség.[574] A jobboldali extrémisták célpontjai történelmileg a zsidó, fekete, leszbikus, meleg, biszexuális, transznemű és queer (LGBTQ+) közösségek voltak, de azokat meghatározhatják egy kis és nagyvárosokon vagy országokon belüli kényes kérdések is. A radikális jobboldal ellenfeleiről gyűlölet-tartalmakat terjeszt online.[575] Viszonylag új a fokozott figyelem az erőszakos nyugati jobboldali extrémisták és

[571] European Union Terrorism Situation and Trend Report (TE-SAT) 2021. Europol, 2021. 78. o. https://www.europol.europa.eu/cms/sites/default/files/documents/tesat_2021_0.pdf (2022.01.21.)

[572] SCRIVENS, R.: Exploring Radical Right-Wing Posting Behaviors Online, Deviant Behavior, 2020. 3. o.

[573] KLEINBERG, B. – VAN DER VEGT, I. – GILL, P.: The temporal evolution of a far-right forum. Journal of Computational Social Science, 2021. Vol. 4. No. 1. 1–2. o.

[574] WARE, J.: Testament to Murder: The Violent Far-Right's Increasing Use of Terrorist Manifestos. ICCT Policy Brief, Hága 2020. 1. o. https://icct.nl/app/uploads/2020/03/Jaocb-Ware-Terrorist-Manifestos2.pdf (2021.07.21.)

[575] SCRIVENS, R. – DAVIES, G. – FRANK, R.: Measuring the Evolution of Radical Right-Wing Posting Behaviors Online, Deviant Behavior, 2018. 1. o.

terroristák internethasználatának széleskörű elterjedtségét illetően, mely legalább részben egy reakció a 2015-2016-ban online feltörő gyűlölet tartalomra, ami az USA-beli elnöki kampányból, és később Trump megválasztásából, a Brexit népszavazásból, az IS által inspirált vagy utasított terrortámadások áradatából, és a háború sújtotta Szíriából, Irakból és Afganisztánból nagyszámú menekült Európába érkezéséből eredt. A szélsőjobb előnyére kívánja fordítani a félelmet és dühöt, amit a terrortámadások és a menekültválság generáltak, valamint a többi esemény által generált felfokozott érzelmet, hogy növelje politikai erejét és új követőket toborozzon, többek között az interneten keresztül. 2017-ben fokozottabb figyelem irányult az internet szerepére a szélsőjobboldali tevékenység tekintetében a 2017. augusztusi, Virginia állambeli, charlottesville-i „Unite the Right" felvonuláson történtek nyomán. 2018 során további figyelem irányult az online szélsőjobboldali tevékenységek – beleértve a dezinformációt és radikalizációt – politikai következményeivel kapcsolatos aggodalmakra, legalább részben az USA-ban elkövetett sikeres és sikertelen terrortámadások miatt, amelyek úgy tűnt, hogy jelentős online alkotóelemeket tartalmaztak. A 2019. március 15-i chistchurchi terrortámadás ezeket az aggodalmakat a „mainstreambe emelte". Ez a támadás különösen internet-centrikus volt, a manifesztum online megosztását illető előre megtervezett stratégiával és Facebook live video streammel. A 2019. áprilisi zsinagóga elleni terrortámadás Poway-ben, a 2019. augusztusi lövöldözés egy El paso-i Walmart-ban, a 2019. októberi halle-i, és más hasonló terrortámadások még tovább fokozták a jobboldali extrémisták internethasználatára irányuló figyelmet.[576]

4. Az utóbbi évek jelentős nemzetközi szélsőjobboldali terrorcselekmények elkövetőinek internethasználata és globális összefüggései

A szélsőjobb nemzetköziesedésében a webnek kulcsszerepe van. Az Európai, és amerikai szélsőjobboldali szervezetek egyre jobban támaszkodnak az internetre, köztük a megfigyelés elkerülésére. Az internet kommunikációs lehetőségei támogatják a transznacionális szolidaritást. Az izolált egyének közös identitást találhatnak a szélsőjobboldali weboldalakon, mely meggyőzi őket, hogy nincsenek egyedül, hanem

[576] CONWAY, M. – SCRIVENS, R. – MACNAIR, L.: Right-Wing Extremists' Persistent Online Presence: History and Contemporary Trends. ICCT, Hága, 2019. 2. o. https://icct.nl/app/uploads/2019/11/Right-Wing-Extremists-Persistent-Online-Presence.pdf (2021.07.21.)

egy közösség részei, noha az virtuális. Az internet megkönnyíti a mobilizációt is, csökkentve a kommunikáció költségeit, megoldja a vezetés és networking problémáit, és transznacionális és globális események szervezését teszi lehetővé. A kiberbűnözőkhöz hasonlóan a jobboldali extrémisták is felhasználhatják illegális és szürke zónás tevékenységekre, pl. hackelésre, tömeges fenyegető e-mailekre, és csalásra. Az internet hatékony eszköz lehet a „fantomsejtek" hálózatán alapuló, egyes amerikai radikális jobboldali aktivisták által támogatott „vezető nélküli ellenállás" koncepciójának hatékony megvalósításában is.[577] A tradícionális média és az internet szerepe egyre elismertebb, mint fontos tényező a radikális jobboldali mobilizáció megértésében.[578]

Globális szinten egy szélsőjobboldali terrorhullám volt tapasztalható az utóbbi években: (Pittsburgh), Christchurch, Poway, El Paso, Halle, Bærum és Haunau.

Macklin szerint ez egy a jobboldali extrémisták erőszakos online szubkulturális miliőiben ösztönzött láncreakció. E digitális ökoszisztéma egy kumulatív lendületet táplál, ami arra szolgál, hogy csökkentse az abban résztvevők erőszak iránti ingerküszöbét. Egyik terrorcselekmény ösztönzi és inspirálja a másikat, „szentek" és „mártírok" növekvő kánonját létrehozva.[579] Az Europol 2020-as jelentése is megerősíti, hogy a jobboldali támadások Christchurch-ben, Poway-ban, El Paso-ban, Bærum-ban és Halle-ban egy világszintű erőszakos incidens-hullám részei voltak, amik elkövetői hasonló transznacionális online közösségek tagjai voltak és egymást inspirálták.[580]

A 2020. február 19-i haunau-i és a 2019. október 9-i halle-i terrortámadások, az ismétlődő zavargások, az erőszakos jobboldali extrémista incidensek számának konzisztens növekedése, melyet a 2018 Annual Report on the Protection of the Constitution[581] mutat, mind jelzi, hogy az erőszakos jobboldali extrémizmus és még

---

[577] CAIANI, M. – KRÖLL, P.: The transnationalization of the extreme right and the use of the Internet. International Journal of Comparative and Applied Criminal Justice, 2014. Vol. 39. No. 4. 2. o.

[578] RYDGREN, J.: The Radical Right: An Introduction. In: RYDGREN, J. (szerk.): The Oxford Handbook of the Radical Right. Oxford University Press, New York, 2018. 9. o.

[579] MACKLIN: i.m. 1. o.

[580] European Union Terrorism Situation and Trend report (TE-SAT) 2020. Europol, 2020. 6. o. https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-te-sat-2020 (2021.07.15.)

[581] 2018 Annual Report on the Protection of the Constitution (Facts and Trends). https://www.verfassungsschutz.de/en/public-relations/publications/annual-reports/annual-report-2018-summary (2021.07.21.) Idézi: CANIGLIA, M. – WINKLER, L. – MÉTAIS, S.: The Rise Of The Right-Wing Violent Extremism Threat In Germany And Its Transnational Character. ESISC, Belgium, 2020. 1. o. http://www.esisc.org/publications/analyses/the-rise-of-the-right-wing-violent-extremism-threat-in-germany-and-its-transnational-character (2021.07.21.)

inkább általánosságban a jobboldali extrémista ideológiák egyre nagyobb kihívást jelentenek a német hatóságok számára. A legutóbbi németországi terrortámadások egy globális összefüggést jeleznek a jobboldali extrémisták viselkedésében. Több közös elem mellett, úgy tűnik, hogy e támadások modus operandija korábbi jobboldali terrortámadásokhoz – mint az új-zélandi christchurch-i vagy az USA-bel paso-i – kapcsolódik, és általuk inspirált. Úgy látszik, a közösségi média gyors elterjedése a jobboldali extrémista radikalizációt és toborzást is megkönnyíti. Ezek felületein a radikalizált személyek kommunikálhatnak és tartalmakat oszthatnak meg egymással, és lehetővé teszik a jobboldali extrémisták gyorsan kiterjedő hálózatának világszintű fejlődését. Ahogy az terjed, és különböző ütemben fejlődik a világ különböző részein, a korábban lokálisnak gondolt kihívás transznacionális karaktert ölt.[582] A jobboldali extrémista csoportoknak és terroristáknak hosszú ideje jó nemzetközi összeköttetéseik vannak, a fő célközönségük általában a saját nemzetük volt, de a livestreaming (élő internetes közvetítés) egyre gyakoribb használatával, az angol nyelvű manifesztumokkal és a közösségi média platformjaival, mint a személyes hálózataik fő elősegítőjével, a jobboldali terrorizmus egyre inkább globális színtérre tolódik.[583]

Clarke a jövőre nézve a globális terrorizmust illetően az egyik legnagyobb aggodalmat keltő trendnek az erőszakos fehér felsőbbrendűséget hirdető extrémista szervezetek és más, a jobboldali extrémizmus különféle formái által motivált csoportok terjedését tartja.[584]

1. Pittsburgh

2018. október 27-én Robert G. Bowers a Tree of Life pittsburgh-i zsinagógában nyitott tüzet. Támadása során megölt 11 embert és 6 ember (Más forrás szerint 8.[585]) megsérült. Bowers-nek felhasználói fiókja volt a Gab közösségi média oldalon, mely 2016 nyarán indult a Facebook és Twitter alternatívájaként, ahol szabad a gyűlöletbeszéd. Az oldalt

[582] CANIGLIA – WINKLER – MÉTAIS: i.m. 1. o.

[583] KOEHLER, D.: The Halle, Germany, Synagogue Attack and the Evolution of the Far-Right Terror Threat. CTC Sentinel, 2019. Vol. 12. No. 11. 14. o.

[584] CLARKE, C. P.: Trends in Terrorism: What's On the Horizon in 2020. Foreign Policy Research Institute. (2020, January 2).
https://www.fpri.org/article/2020/01/trends-in-terrorism-whats-on-the-horizon-in-2020/ (2021.07.15.)

[585] TOBIAS, Adam Z. – ROTH, Ronald N. – WEISS, Leonard S. – MURRAY, Keith – YEALY, Donald M.: Tree of Life Synagogue Shooting in Pittsburgh: Preparedness, Prehospital Care, and Lessons Learned. Western Journal of Emergency Medicine, 2020. Vol. 21. No. 2. 374. o.

hamar ellepték az alt-jobb képviselői. Bowers Gab-fiókját deaktiválta a cég, de nagyon aktív volt a hálózaton. 19 nappal a támadása előtt legalább 68 alkalommal posztolt és reposztolt mémeket. Megszállott volt a zsidókkal, számos velük kapcsolatos összeesküvés-elmélet foglalkoztatta, többek közt a „fehér fajírtás" elmélet. Sok alt-jobbos elkövetőhöz hasonlóan, valószínűleg Bowers is online radikalizálódott.[586]

Az elkövető az online posztjaiban összeesküvés-elméletekre utalt arról, hogy a fehér embereket „globalisták" veszik célba, és gyűlöletét a zsidókra irányította. Röviddel a támadása előtt a Gab-ra posztolta, hogy: „I can't sit by and watch my people get slaughtered. Screw your optics, I'm going in." („Nem tudom tétlenül nézni, ahogy lemészárolják a népemet. Teszek a látásmódotokra, behatolok!")

Egy nappal a támadás után az az amerikai neonáci Andrew Anglin, a The Daily Stormer weboldal alapítója, arról panaszkodott, hogy a terrorcselekmény megnehezíti a fehér felsőbbrendűséget hirdetők és neonácik támogatókhoz és politikai hatalomhoz jutását. Számos más szélsőjobboldali nézeteket valló is hasonlóan vélte.

Ahogy Anglin írta: „Look, kids: you're not going to fight the Jews and overthrow the system with random terrorist attacks," („Figyeljetek, gyerekek: nem fogtok a zsidók ellen harcolni és megdönteni a rendszert egy véletlenszerű terrortámadással.")

Mások ünnepelték a támadást: A 4chan oldalon névtelen kommentelők izgatottak voltak, hogy az eset „véletlen redpill-elheti[587]" (felnyithatja a szemüket) a nyilvánosságot az ügyükkel kapcsolatban. Mások azt sajnálták, hogy a célbavett zsidók nem voltak stratégiailag fontosabb személyek.[588]

Pittsburgh valószínűleg nem a terrorhullám része, az inkább Christchurch-től indulhatott.

2. Christchurch

„2019. március 15-én Brenton Tarrant romba döntötte Új-Zéland elképzelését az

[586] AMEND, A.: Analyzing a terrorist's social media manifesto: the Pittsburgh synagogue shooter's posts on Gab. Southern Poverty Law Center. (2018, October 28). https://www.splcenter.org/hatewatch/2018/10/28/analyzing-terrorists-social-media-manifesto-pittsburgh-synagogue-shooters-posts-gab (2022.01.27.)

[587] A pill-ekről lásd az incelekről szóló fejezetet.

[588] HAUSLOHNER, A. – OHLHEISER, A.: Some neo-Nazis lament the Pittsburgh massacre: It derails their efforts to be mainstream. The Washington Post. (2018, October 30). https://www.washingtonpost.com/national/some-neo-nazis-lament-the-pittsburgh-massacre-it-derails-their-efforts-to-be-mainstream/2018/10/30/3163fd9c-dc5f-11e8-85df-7a6b4d25cfbb_story.html (2022.01.26.)

alacsony szintű terrorfenyegetettségéről."[589] Az ausztrál származású magányos elkövető az új-zélandi Christchurch két mecsetében megölt 50 embert, sok másikat megsebesítve (egy személy később belehalt a sérüléseibe). Röviddel a támadás előtt 74 oldalas manufesztumát e-mailben elküldte politikusoknak és sajtóorgánumoknak, és a támadásának egy részét Facebookon livestreamelte.[590] A manifesztum címe „The Great Replacement" (A nagy kicserélés), mely nevét Renaud Camus Great Replacement-jében kidolgozott összeesküvés-elméletekről kapta. Egy héten belül az új-zélandi Chief Censor (Fő Cenzor) „objectionable publication-ként" (kifogásolható anyagként) osztályozta a manifesztumot, és a terrorcselekményről FPS videojátékhoz hasonló stílusban készült 17 perces videót. A videóhoz a nézők valós időben kommentelhettek, amely a „performance crime-nak" (teljesítménybűnözés) egy formája, mely célja más alt-jobb elkövetők inspirálása volt. Ezek az anyagok ugyan betiltásra kerültek Új-Zélandon, de különféle oldalon még mindig elérhetőek. Törökországban Erdogan elnök a választási kampánya részeként többször is visszajátszott elhomályosított részletet a videóból. Besley és Peters felteszi a kérdést, hogy a betiltásuk nem-e csak mélyebbre, sötétebb oldalak felé tereli ezeket, mint a 4chan és 8chan, ahol továbbra is radikalizálhatják az arra fogékonyakat.[591] Az elkövető által látogatott chat szobában a követők éljenezték és bátorították őt, miközben embereket ölt. Tarrant továbbá videojátékokat, és az egyik legnépszerűbb youtuber-t, PewDiePie-t említette és ún. „easter egg-eket" hagyott hátra, ami játékos terminológiában rejtett üzenetet vagy képet jelent.[592] Hogy hatalmas tömegeket érjen el, Tarrant az elkövetés megkezdése előtt a kamerába mondta, hogy „remember lads, subscribe to PewDiePie." („ne felejtsetek el feliratkozni PewDiePie-ra, fiúk."), mellyel az egyik legtöbb feliratkozóval rendelkező youtuber-re, Felix Kjellberg-re utalt. Kjellberg, – youtuber nevén PewDiePie – mélységesen elítélte a cselekményt. Azzal, hogy rákényszerítette Kjellberg-re, hogy nyilatkozzon a támadásról, az elkövetőnek sikerült elérnie, hogy annak híre eljusson PewDiePie követőinek

[589] BATTERSBY, J.: Security sector practitioner perceptions of the terror threat environment before the Christchurch attacks. Kōtuitui: New Zealand Journal of Social Sciences Online, 2019. Vol. 15. No. 2. 1. o.

[590] CROTHERS, Ch. – O'BRIEN, T.: The Contexts of the Christchurch terror attacks: social science perspectives. Kōtuitui: New Zealand Journal of Social Sciences Online, 2020. Vol. 15. No. 2. 248. o.

[591] BESLEY, T. – PETERS, M. A.: Terrorism, trauma, tolerance: Bearing witness to white supremacist attack on Muslims in Christchurch, New Zealand. Educational Philosophy and Theory, 2020. Vol. 52. No. 2. 112. o.

[592] DUFF, M.: Gaming culture and the alt-right: The weaponisation of hate. Stuff. (2019, March 24). https://www.stuff.co.nz/national/christchurch-shooting/111468129/gaming-culture-and-the-alt-right-the-weaponisation-of-hate?cid=app-iPhone (2021.07.22.) Idézi: BESLEY – PETERS: i.m. 112. o.

tízmillióihoz.[593] A 8chan /pol-ján sok névtelen felhasználó (anon) úgy utalt Tarrant-ra, mint „Saint Tarrant" („szent Tarrant") középkori inspiráltságú ikonográfiával együtt.[594]
A terrortámadásról készült videó még mindig terjed a Facebook-on. A cég 2019. szeptember végéig legalább 3 millió posztot távolított el.[595] A christchurch-i támadás során az internet terrorista célokra való felhasználásának eddig példátlan elemei voltak tapasztalhatóak. Az elkövetésről készült livestreamelt videó és Tarrant manifesztuma gyorsan elterjedt az interneten, ami az online terrorista tartalmak ellen történő harc új kihívásaira mutatott rá.[596] A terroristák gyakran új technológiák korai alkalmazói, az újonnan felbukkanó platformokat felhasználják online kommunikációra és a terjesztési stratégiájukhoz. Elegendő tervezéssel és szimpatizáló online közösségek támogatásával a terrorcselekmények gyorsan el tudnak terjedni az interneten, mielőtt a hálózati szolgáltatók és bűnüldöző szervek reagálhatnának.[597] Tálas et al. 2019-es jóslata, mi szerint Tarrant további elkövetőket ösztönzhet, beigazolódott.[598]

3. Poway

2019. április 27-én John Timothy Earnest egy poway-i zsinagógában egy embert megölt, és hármat megsebesített. A támadás előtt egy manifesztumot töltött fel az internetre, melyben azt írta, az új-zélandi terrortámadás volt a saját támadásának a katalizátora, továbbá, hogy azért cselekedett így, "because the Jewish people are destroying the white race." („mert a zsidók tönkreteszik a fehér fajt.") Earnest magára vállalt egy a kaliforniai

[593] LORENZ, T.: The Shooter's Manifesto Was Designed to Troll The violent rhetoric was written for an audience. The Atlantic. (2019, March 15). https://www.theatlantic.com/technology/archive/2019/03/the-shooters-manifesto-was-designed-to-troll/585058/ (2021.07.22.)

[594] EVANS, R.: Ignore The Poway Synagogue Shooter's Manifesto: Pay Attention To 8chan's /pol/ Board. Bellingcat. (2019, April 28). https://www.bellingcat.com/news/americas/2019/04/28/ignore-the-poway-synagogue-shooters-manifesto-pay-attention-to-8chans-pol-board/ (2021.07.27.)

[595] UBERTI, D.: The Christchurch Terror Attack Video Is Still Spreading on Facebook. Vice. (2019, November 13). https://www.vice.com/en/article/wjw93n/the-christchurch-terror-attack-video-is-still-spreading-on-facebook (2021.07.22.)

[596] Internet Organised Crime Threat Assesment (IOCTA) 2019. Europol, Hága, 2019. 48. o. https://www.europol.europa.eu/iocta-report (2021.07.21.)

[597] Uo. 9. o.

[598] TÁLAS P. – RÁCZ A. – AMBRUS A.: Az új-zélandi muszlimellenes terrortámadás és tanulságai. Nemzet és Biztonság – Biztonságpolitikai Szemle, 2019/3. 52–61. o.

Escondido-ban 2019. március 24-én az Dar-ul-Arqam Mosque and Islamic Center-ben történt gyújtogatást is.[599]

4. El Paso

2019. augusztus 3-án az Allenből származó 21 éves Patrick Wood Crusius egy El paso-i Walmart-ban tüzet nyitott a vásárlókra egy GP WASR-10 típusú fegyverrel, 20 ember életét kioltva. Később 2 személy belehalt a sérüléseibe, mellyel az áldozatok száma 22-re emelkedett. A támadás során 26-an sérültek meg.[600] Az elkövető 2019. június 19-én a fegyverét az internetről vásárolta, és hozzá 1000 darab 7,62 x 39 milliméteres üreges hegyű lőszert. Valamikor 2019. augusztus 3. előtt létrehozott egy „The Inconvenient Truth" (A kellemetlen igazság) című dokumentumot, mely úgy kezdődik, hogy „This attack is a response to the Hispanic invasion of Texas. They are the instigators, not me. I am simply defending my country from cultural and ethnic replacement brought on by the invasion." („Ez a támadás egy válasz Texas hispán inváziójára. Ők az uszítók, nem én. Én szimplán csak védem az országomat az invázió által hozott kulturális és etnikai felcseréléstől.") Crusius augusztus 3-án, az elkövetést megelőzően azt feltöltötte az internetre. [601]

5. Bærum

2019. augusztus 10-én a norvég Bærum-ban az Al-Noor Islamic Centre mecsetében Philip Manhaus nyitott tüzet. Egy ember megsérült.[602] Az elkövetőnek a rendőrség szerint szélsőjobboldali és bevándolásellenes nézetei voltak. A támadása előtt egy Tarrant-ra utaló üzenetet posztolt az EndChan fórumra, melynek moderátorai eltávolították a posztot és a fő domain is offline került az elkövetés után.[603]

---

[599] Assessing the Threat of Mass Attacks in Texas: A State Intelligence Estimate. Texas Fusion Center Intelligence & Counterterrorism Division Texas Department of Public Safety, Texas, 2020. 16–17. o. https://www.dps.texas.gov/director_staff/media_and_communications/2020/txMassAttackAssessment.pdf (2021.07.22.)

[600] MACKLIN: i.m. 1. o.

[601] United States of America v. Patrick Wood Crusius, Case 3:20-cr-00389-DCG 02/06/20 1–2. o. https://www.justice.gov/usao-wdtx/file/1245756/download (2021.07.22.)

[602] Norway mosque shooting: Man opens fire on Al-Noor Islamic Centre. BBC. (2019, August 10). https://www.bbc.com/news/world-europe-49308016 (2021.07.27.)

[603] Norway mosque attack: Bruised suspect Manshaus appears in court. BBC. (2019, August 12). https://www.bbc.com/news/world-europe-49318001 (2021.07.29.)

6. Halle

2019. október 9-én, a zsidó ünnep, jom kippur idején a 27 éves Stephan Balliet erőszakkal próbált meg behatolni a zsinagógába, a németországi Halle/Saale-ben, hogy online livestreamelt vérfürdőt rendezzen. Az épületbe nem sikerült bejutnia, ezért véletlenszerűen lelőtt egy arra járó nőt. Majd egy másodlagos célpontjához, egy török étteremhez ment, ahol lelőtte a második áldozatát. Koehler szerint az elkövető egy a korábbi terrortámadások által inspirált „copycat attacker" (utánzó elkövető). A halle-i támadás számos trendet tükröz és bizonyít, beleértve a jobboldali terrorizmus internacionalizálódását, továbbá ez volt az első alkalom, hogy terrorista házi készítésű lőfegyvert használt az elkövetéséhez. Az elkövető egy sisakra szerelt okostelefont használt a Twitch nevű játékos platformon történő livestreamhez. Délelőtt 11:57-kor közzétett egy linket a Twitch livestreamről a 4chan anime board-jához lazán kötődő, már eltávolított Meguca nevű közösségi média képhálózat oldalra, és a manifesztumát is oda töltötte fel. A Twitch szerint csak 5-en látták élőben a livestreamet, az adminisztrátoroknak 30 percbe telt megtalálni és eltávolítani a videót, amit addigra körülbelül 2200-an láttak. [604]

Az elkövető egyértelműen a világ figyelmét akarta. "I believe the Holocaust never happened," („Úgy hiszem, a holokauszt soha nem történt meg"), mondta az Amazon tulajdonú Twitch-en, a livestream során. A christchurch-i elkövető nyomdokaiban járt, akinek a livestreamelt támadása 2019 márciusában elárasztotta a Facebook-ot, de azzal ellentétben, a halle-i merénylet videója nem terjedt el online. Miután a Twitch-ről eltávolították, a felvétel tovább keringett a Telegramon, 4chan-en, és más kevésbé szabályozott oldalakon, potenciálisan több tízezreket elérve, de az elkövető anti-szemita propagandája nem terjedt el a nagyobb platformokon, mint a Facebook és YouTube. Hat hónappal azelőtt a Facebook nem tudta visszafogni Tarrant videójának terjedését. Mire azt egy felhasználó flag-elte, 29 perccel azután, miután az élőben ment, addigra a támogatók letöltötték a videót és legalább 800 szerkesztett verzióját készítették el. Arról 24 órán belül 300.000 vagy több példány került vissza a Facebookra.

A halle-i zsinagógai lövöldözés a Big Tech „viral" erőszak elleni szövetségének, „The Global Internet Forum to Counter Terrorism-nek" az első nagy tesztje volt. A 2017-ben alapított Facebook, Twitter, Microsoft és YouTube közötti társulás egy önálló terrorizmusellenes csoport, amelybe az Amazon is beletartozik, cégeknek és kormányoknak segít valós időben koordinálni a támadásokra adott választ. Fő eszköze a

[604] KOEHLER: i.m. 14. o.

terrorista tartalom elleni harcban a 200.000 „hash-ből”, vagy digitális ujjlenyomatból álló megosztott adatbázisa, amiket a platformok létező propaganda azonosítására használhatnak. Miután a Twitch eltávolította a lövöldöző videóját, megosztotta a tartalom hash-ét a társulás adatbázisával, mely azután tovább osztotta azt a többi partnerével. A cél az, hogy lehetővé tegyék a hash-t a biztonsági eszközeikbe helyező cégeknek, hogy lenyomozzák a tartalmat a platformjaikon vagy, hogy egyáltalán megakadályozzák a feltöltést. A társulás nagyrészt sikeres volt a halle-i lövöldözésről készült videó terjedésének visszafogásában, mely ugyan a kisebb oldalakon elérhető maradt, köztük a BitChute and Kiwi Farms platformokon. A Big Tech cégeknek egymással közeli kapcsolata van, ezzel szemben a tevékenységek koordinálása nehezebb a több száz kisebb platformokon. Ezek a kapcsolatok kulcsfontosságúak lesznek, ahogy a fehér felsőbbrendűséget hirdetők és más erőszakos szereplők virálissá próbálják tenni a terrortámadásaikat.[605]

7. Haunau

2020. február 19-én, este 10 körül Tobias Rathjen tüzet nyitott a németországi Haunau Midnight vízipipa bárjában, megölve 3 embert. Azután 2 km-t autózott a Kesselstadt városrészbe, ahol az Arena Bar & Cafe-ra nyitott tüzet, további 5 ember életét kioltva. Ez után elautózott az otthonáig, ahol lelőtte az anyját, és önmagával is végzett. A támadás utáni órákban fény derült arra, hogy több az internetre feltöltött anyaga alapján az elkövetőre hatott a tradicionális szélsőjobb, a faji alapú és a bevándorlásellenes narratívák kombinációja, és több obskúrus összeesküvés-elmélet. Crawford és Keen szerint az ügy a további kutatás szükségességét szemlélteti ezen ideák kereszteződésének és az online ökoszisztémának tekintetében, ahol ezek virágzanak, és ahol az olyan elképzelések, mint a „the Great Replacement” elmélet hevesen propagáltak, melynek aspektusai visszaköszönnek Rathjen manifesztumában. A szerzők szerint ez az átfogó idea köti össze a látszólag különböző terrortámadásokat egy ideológiailag analóg terrorcselekmények globális hálózatában. Az elkövető 2020. február 13-án Youtube csatornát hozott létre, amire 14-én egy videót töltött fel, „Tobias Rathjen” címmel, melyben az USA állampolgárait figyelmeztette rejtett katonai bázisokra, ahol gyermekeket kínoznak. A videó leírásába linkelt személyes weboldalára

[605] UBERTI, D.: The German Synagogue Shooter's Twitch Video Didn't Go Viral. Here's Why. Vice. (2019, October 11). https://www.vice.com/en/article/zmjgzw/the-german-synagogue-shooters-twitch-video-didnt-go-viral-heres-why (2021.07.22.)

Rathjen 3 videót töltött fel németül, amiből a hatóságok csak kettőhöz tudtak hozzáférni, egy 24 oldalas német nyelvű szöveg mellett, amit sokan manifesztumként értelmeznek, két rövidebb melléklettel együtt. A tény, hogy német és angol nyelven tett közzé anyagokat, és kezdetben angolul vett fel videót, jelzi, hogy globális közönséget kívánt elérni, és a szélsőjobboldali terrorizmus további internacionalizálódására mutat rá.[606] A hatóságok a cselekményt hazai terrorizmusként (domestic terrorism) kezelik. A nyomozók szerint Rathjen egyedül cselekedett, de a hatóságok próbálták kideríteni, hogy voltak-e mások, akik tudtak a terrorcselekményről vagy támogatták azt, és utánanéztek az elkövető minden lehetséges hazai vagy külföldi kapcsolatának. Rathjen nem volt büntetett előéletű és nem volt a német belföldi hírszerző ügynökség szeme előtt. „Már olyan etnikai csoportjaink, fajok és kultúrák vannak köztünk, amik minden szempontból destruktívak", írta Rathjen a 24 oldalas szónoklatában. „A következő népekeket teljesen ki kell írtani"– írta, és felsorolt két tucat, főleg muszlim országot. Rathjen továbbá részletezte az attól való félelmét, hogy évek óta állami megfigyelés alatt áll és ezt okolta azért, hogy nem tudott kapcsolatot létesíteni nőkkel. Azt is állította, hogy többször megkereste a rendőrséget az összeesküvés elméleteivel. 2013 óta volt fegyvertartási engedélye. Németország 83 millió lakosából 5,4 milliónak vannak lőfegyverei. A fegyvertulajdonosoknak háttérellenőrzésen kell átmennie, ebbe az is beletartozik, hogy nem lehetnek elmebetegek.[607] Peter Neumann, a londoni International Centre for the Study of Radicalisation igazgatója szerint a manifesztum alapján az elkövető úgy tűnik „mint aki egész éjjel összeesküvés videókat néz a YouTube-on. Szélsőjobb + Incel + valami, ami egy jelentős mentális problémának tűnik."[608]

5. A szélsőjobboldali terroristák internetes aktivitásának visszafogásának és kutatásának nehézségei

2014 és 2017 között az IS közösségi média platformok széles skáláján tartott fenn

[606] CRAWFORD, B. – KEEN, F.: The Hanau Terrorist Attack: How Race Hate and Conspiracy Theories Are Fueling Global Far-Right Violence. CTC Sentinel, 2020. Vol. 13. No. 3. 1. o.

[607] MCHUGH, D. – RISING, D. – JORDANS, F.: German gunman calling for genocide kills 9 people. Associated Press. (2020, February 20). https://apnews.com/b5736c3dba1d677e89ef947bcf5ab213 (2021.07.22.)

[608] HUME, T.: Gunman Kills 9 in Hookah Bars in Suspected Far-Right Terror Attack in Germany. Vice. (2020, February 20). https://www.vice.com/en/article/z3byd9/gunman-kills-9-in-hookah-bars-in-suspected-far-right-terror-attack-in-germany (2021.07.22.)

virágzó közösségeket. A fő platformok agresszív felhasználói fiók és tartalom eltávolító politikájának köszönhetően a látható közösségek már majdnem eltűntek. Christchurch után többször felmerült a kérdés, hogy a fő platformok miért nem tudják az extrém jobboldalt ugyanúgy kiűzni.[609]

Conway rávilágít, hogy az extrém jobboldal nem hasonlítható az IS-hez, az inkább egy gyorsan változó „szcéna", mint csoport, és miközben az abba tartozó személyek követtek el terrorcselekményeket, nagyon kevés csoport van hivatalosan terroristának megjelölve, mert relatíve kevés támadóról lehetett bizonyítani, hogy formális csoport tagja vagy egyáltalán támogatója. Ők inkább úgy jellemezhetőek, hogy közös extrém jobboldali szólamokat támogatnak. Ugyan ez nem teljesen akadályozza meg az online platformokat a tartalmak eltávolításában, mivel azoknak nem kell terrorista természetűnek lennük, hogy eltávolíthatóak legyenek, de bonyolítja a helyzetet. Hatalommal bíró szereplők – államfők, fő politikai pártok, néhány tradícionális médiaorgánum és a nyugati közvélemény jelentős része is azonosulnak ezzel a tartalommal. Ez a közösségi média cégeket sebezhetővé teszi az elfogultság vádjával szemben. Amikor az online cégek fel is lépnek az extrém-jobboldali tartalommal szemben, azok fő képviselői sokkal jobb helyzetben vannak ahhoz, hogy kiépítsék és fenntartsák a saját közösségi média platformjaikat. Ez kifejezetten igaz az extrém-jobboldali aktivistákra az USA-ban, akik hivatkozhatnak az Első Alkotmánymódosításra. A fő közösségi média cégek az utóbbi években lépéseket tettek a gyűlölet visszafogására a platformjaikon. Nagyobb rajtuk a nyomás Christchurch és az azt követő más jobboldali terrortámadások óta.[610]

Az utóbbi idők online szélsőségek visszaszorítása iránti nemzetközi erőfeszítései közé tartozik az Egyesült Királyság kormányának a fenyegető online tartalmak hatékonyabb kezelését megcélzó 2019. áprilisi „Online Harms White Paper-e."[611]

2019. május 15-én az új-zélandi miniszterelnök és a francia elnök állam- és kormányfőket, és média- és online szolgáltatók, vállalatok vezetőit hívta egybe. A „Christchurch Call" egy, a találkozón elfogadott felhívás, elköteleződés a terrorista és erőszakos szélsőséges online tartalmak eltávolítására.[612]

---

[609] CONWAY, M.: Routing the Extreme Right. The RUSI Journal, 2020. Vol. 165. No. 1. 1. o.

[610] Uo. 6. o.

[611] Online Harms White Paper.
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/973939/Online_Harms_White_Paper_V2.pdf (2021.06.21.)

[612] Christchurch Call. https://www.christchurchcall.com/ (2021.06.21.)

2017-ben a Facebook, Microsoft, Twitter és YouTube létrehozta a Global Internet Forum to Counter Terrorism-t. 2019-ben hozzájuk csatlakozott a Dropbox, Amazon és WhatsApp. A fórum a 2015 decemberében létrehozott EU Internet Forum-ra építkezik és jelenleg a Christchurch Call inspirálja.[613]

A főbb, és sok kisebb közösségi média cégek által közös lépések történtek a támadáshoz közvetlenül kötődő tartalmak platformjaikról való eltávolítására. Végső soron a probléma nem az extrém jobboldali terrorista tartalmak fő közösségi média platformokra való feltöltése és terjedése, mert ezeket hasonlóan kezelhetők, mint az IS tartalmai. A probléma árnyaltabb, az az extrém jobboldali tartalom fő platformokról történő eltávolításának helyénvalóságára vonatkozik.[614]

6. A 8chan fórum és a terror „játékosítása”

A 8chan online fórumot Fredrick Brennan indította 2013-ban, mint a „szólásszaszabadság utópiáját”, de az erőszakos extrémisták gyülekezőhelyévé, megafonjává és toborzó-platformjává vált.[615]

8chan-t a christchurch-i, a poway-i és az El paso-i terrortámadások elkövetői is használták. Az oldal különböző témájú társalgó csoportok széles skáláját tartalmazta, az animéken és kriptovalutákon át a politikáig és videojátékokig. Az oldal /pol/ board-ja jobboldali extrémisták találkozóhelye volt, célja volt anonim tagokat erőszakos cselekedetek elkövetésére radikalizálni. A christchurch-i elkövető manifesztumát, továbbá egy linket a Facebook Live-on livestreamelt támadásáról a 8chan-ra posztolta. A videót kevesebb, mint 200-an nézték meg a Facebookon, mielőtt azt az oldal eltávolította volna, de a 8chan által milliókhoz jutott el. Az El paso-i támadás elkövetője is töltött fel manifesztumot az oldalra, melyben Tarrant-ot dicsőítette. A poway-i elkövető is használta az oldalt.[616] Az El paso-i elkövető, Crusius a támadás kezdetét a

[613] LUYTEN, K.: Addressing the dissemination of terrorist content online. European Parliamentary Research Service, 2020. 2–3. o.
https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/649326/EPRS_BRI(2020)649326_EN.pdf (2021.07.29.)

[614] CONWAY (2020): i.m. 6. o.

[615] ROOSE, K.: 8chan Is a Megaphone for Gunmen. ‘Shut the Site Down,’ Says Its Creator. The New York Times. (2019, August 4). https://archive.is/JrNGc (2021.07.29.)

[616] ÇELIKSOY, E. – OUMA, S.: Terrorist Use Of The Internet. Bilişim Hukuku Dergisi, 2019. Vol. 1. No. 2. 250–252. o.

8chan /pol board-ján jelentette be és egy négy oldalas manifesztumot csatolt a poszthoz, és egy dokumentumot, amelyben szerepelt a neve. A poszt archivált változata fellelhető, mely Unix-idő szerint 1564848920-kor készült, ami 2019. augusztus 3, 16:15-nek (UTC) – helyi El paso-i idő szerint (UTC-6) 10:15-nek felel meg, pont mielőtt az első jelentések megjelentek a lövöldözésről. Ezt az eredeti thread-et (kommentszálat) szinte azonnal eltávolították a moderátorok, akiknek már gyakorlata volt az ilyenek eltávolításában. A poszt archivált változatára csak három válasz érkezett. Az első egy névtelen (a 8chan szóhasználatával anon), aki azt állítja, hogy a 8chan a „board of peace" („a béke fóruma"), ami nem fogadja el az erőszakot. Ez a szóhasználat mém a névtelenek között, gúnyosan utal arra, hogy az iszlám a „béke vallása". A következő posztoló azt írta, hogy: „Every shabbat" („minden sabbat"), reményét kifejezve, hogy ilyen támadás minden hétvégén történjen. Az eredeti thread gyorsan eltávolításra került, de más névtelenek újra kiposztolták a poszt másolatait és a manifesztumhoz vezető linket. Körülbelül két órával az elkövetés után került fel egy következő poszt, melyben többen szidták a lövöldözőt a „shitty" („silány") és „0 effort manifesto" („0 erőfeszítéses manifesztuma") miatt. Az elkövető szavaiban nincs semmi új. Ugyanarról a fehér emberek „felcserélésről" fejti ki a félelmeit, mint ami Tarrant-ot motiválta és leírja, hogy erősen motiválta az ő manifesztuma. A 8chan használói sok időt szenteltek Tarrant manifesztumának terjesztésére, hogy több elkövetést inspiráljanak.[617] Azt több nyelvre is lefordították.[618] Az El paso-i események is bizonyítják, hogy ez a stratégia működik. Evans szerint a két legfontosabb tanulság az El paso-i lövöldözésből az, hogy a 8chan /pol board-ja továbbra is szándékosan radikalizálja a tömeggyilkosokat, továbbá az ártatlanok lemészárlása „játékosítva" („gamified") lett. Az utóbbit világosan illusztrálja néhány komment, amiket Evans az El paso-i események után fedezett fel. Ebben a thread-ben miután egy névtelen képernyőképet posztol az El paso-i elkövető thread-jéről, azt kérdezi: „Is nobody going to check these incredible digits?" („Senki nem nézi meg ezeket az elképesztő számokat?") Az állítás valószínűleg az elkövető áldozatainak magas számára utal. (Vagy az ismétlődő „14-re" a poszt ID-ben, vagy más hasonlóra.) Christchurch után a 8chan használói gyakran kommentelték Tarrant áldozatainak magas

[617] EVANS, R.: The El Paso Shooting and the Gamification of Terror. Bellingcat. (2019, August 4). https://www.bellingcat.com/news/americas/2019/08/04/the-el-paso-shooting-and-the-gamification-of-terror/ (2022.02.29.)

[618] EVANS, R.: Ignore The Poway Synagogue Shooter's Manifesto: Pay Attention To 8chan's /pol/ Board. Bellingcat. (2019, April 28). https://www.bellingcat.com/news/americas/2019/04/28/ignore-the-poway-synagogue-shooters-manifesto-pay-attention-to-8chans-pol-board/ (2021.07.27.)

számát és utaltak a szándékukra, hogy „beat his high score”[619] („megverjék a high score-ját”). Gyakran került fel egy kép Christchurch-t követő hónapokban „beatmyscore.png” címmel, melyen az áll, hogy: „You call that a killing, Ahmed? This is a killing!” („Ezt hívod ölésnek, Ahmed? Ez egy ölés.”). Evans szerint ez bizonyítja az igazi újítást, amit a 8chan a globális terrorizmusba hozott: a tömeges erőszak játékosítását, mely nem csak a „high score-okra” való utalásokban látszik, hanem abban is, ahogy Tarrant elkövette a támadását – élőben közvetítetve úgy, hogy a lövöldözése majdnem úgy nézett ki, mint egy FPS videojáték. Ez tudatos volt, és az is, hogy ehhez szórakoztató és inspiráló aláfestő zenét választott. A poway-i zsinagógai lövöldöző Tarrant-ot próbálta utánozni ezekben a taktikákban, zenei playlist-et posztolva a lövöldözése mellé. Jelenleg nem ismert, hogy az El paso-i elkövető megpróbálta-e livestreamelni a mészárlását, de a 8chan posztjai azt sugallják, hogy a névtelenek őt „ourguy-ként” („mi fickónk”) vállják fel, és az eseményről szóló hírek live chat-jeit megpróbálták elárasztani.[620] 2019. Augusztus 19-én a 8chan, más néven Infinitychan offline került, amikor a Cloudflare megvonta a támogatást az oldaltól, ejtve azt, de csak az El Paso után.[621] Sok használója a Discord-ra migrált át.[622] Örökségének továbbvitelére a legjelentősebb példa a „8kun”, mely legtöbbször megbízhatóan csak a dark web-en érhető el.[623]

A szélsőjobboldali terror „játékosítása” és az ahhoz kapcsolódó versengés, fokozódási kényszer az online fórumokban rendkívül aggasztó jelenség, melyet nem szabad szem elől téveszteni.

---

[619] A high score videojátékokban az elért legmagasabb eredmény.

[620] EVANS, R.: The El Paso Shooting and the Gamification of Terror. Bellingcat. (2019, August 4). https://www.bellingcat.com/news/americas/2019/08/04/the-el-paso-shooting-and-the-gamification-of-terror/ (2022.02.09.)

[621] GONIMAH, D.: What is 8chan and Why Was it Banned? Storyful. (2019, November 12). https://storyful.com/resources/blog/what-is-8chan/ (2021.07.29.)

[622] GLASER, A.: Where 8channers Went After 8chan. Slate. (2019, November 11). https://slate.com/technology/2019/11/8chan-8kun-white-supremacists-telegram-discord-facebook.html (2021.07.29.)

[623] CRAWFORD, B.: Chan Culture and Violent Extremism. Global Network on Extremism & Technology. (2019, December 31). https://gnet-research.org/2019/12/31/chan-culture-and-violent-extremism-past-present-and-future/ (2021.07.29.)

7. Két szélsőjobboldali szervezet online aktivitása

1. Feuerkrieg Division

A német nyomozók figyelmét a szélsőjobboldali „Feuerkrieg Division” (FKD) nevű terrorszervezet keltette fel. Az észt rendőrség egy 13 (!) éves gyermeket azonosított annak vezetőjeként, aki „Commander” („Parancsnok”) néven jelent meg online. Az FKD világszerte aktív, és a közelmúltig 15 országban – köztük Németországban – mintegy 70 tagja volt. A 13 éves „Commander" a tagok toborzásáért és a felvételükről való döntésért felelt. Bombagyártási instrukciókat terjesztett, szeretett volna Londonban terrortámadást, és katonai kiképző táborok szervezését javasolta februárra, az NSDAP „100. születésnapjára.” Mivel 14 év alatti, Észtországban nem vonható büntetőeljárás alá. A „Parancsnok” által 2018 októberében társalapított FKD propagandáját videók, képek és írások formájában terjesztette közösségi hálózatokon és a Telegramon. Az FKD a jobboldali terroristákat „szenteknek" tartja, és tagjaikat a követésükre szólítja fel. Az FKD 2020. február 8-án jelentette be felszámolását. A belső chat-ekben azonban látszik, hogy a nyilatkozat csak a nyilvánosságnak szól, és a szervezet új névvel működik tovább.[624]

2. The Base

Rinaldo Nazzaro, más néven „Norman Spear" és „Roman Wolf", a The Base nevű militáns csoportot Oroszországból irányítja, melyet az FBI egy főbb terrorelhárítási feladatként kezel. Az FBI által előkészített bírósági dokumentumok a The Base-t úgy jellemzik, mint fajilag motivált erőszakos extrémista csoportot, ami meg akarja gyorsítani az USA kormányának bukását és egy fehér etno-államot akar létrehozni. A 2018 júliusában alapított szervezet online szerez követőket, titkosított üzenetküldő alkalmazásokkal kommunikál és a tagokat paramilitáris képzésben való részvételre

[624] BAUMGÄRTNER, M. – HÖFNER, R. – LEHBERGER, R.: RechtsterrorismusMitgründer der "Feuerkrieg Division" gefasst. Der Spiegel. (2020, April 9). https://www.spiegel.de/politik/deutschland/rechtsterrorismus-mitgruender-der-feuerkrieg-division-gefasst-a-d88e6b8f-7a96-4c56-8904-85bb72653663?utm_source=dlvr.it&utm_medium=[facebook]&utm_campaign=[spontop]&fbclid=IwAR01kQfV5avns0voCiI1SCFXe_FipiYntLxMhRqg6hTJ3rTlOLI6NVNQp3A#ref=rss (2021.07.29.)

buzdítja.[625] Propagandája nagy fenyegetést jelent, mivel az az egyéneket a magányos farkas és terrorista sejt-orientált mentalitás felé tereli.[626]

8. Következtetések

Álláspontom megegyezik Répásiéval, abban, és erősen problematikusnak tartom, hogy „… az iszlamista terrorizmussal számos hasonlóságot mutató szélsőjobboldali terrorizmus, és általában véve a politikai jobbszélhez köthető gyilkosságok a szükségesnél jóval kisebb figyelmet kapnak a hatóságok és a média részéről."[627]

A potenciális radikalizáló képességük miatt aggályosnak tartom, hogy fentebb említett manifesztumok könnyűszerrel, akár akaratlanul is megtalálhatóak az interneten. 2020. május 14-én a „The Great Replacement" Google keresésre a 9. a találat volt Tarrant manifesztuma PDF formátumban.[628] A társadalomra, az elkövető környezetére is felelősség hárul, hogy felismerjék a radikalizálódás jeleit. Mivel az online felületek, a weboldalak és fórumok „korai figyelmeztető rendszerként" funkcionálnak a terrorcselekményeket illetően[629], a jobboldali extrémisták által frekventált online felületek nyomon követését az ilyen típusú terrorcselekmények megelőzése szempontjából elengedhetetlen fontosságúnak tartom.

Rendívül veszélyes jelenség a terrorhullám. A jövőben egy ilyen hullám felismerése kritikus fontosságú, figyelni kell az elkövetők által közzétett manifesztumokra, és az ezekben fellelhető közös elemekre. Kutatást igényel, hogy egy ilyen hullámot hogyan lehet megakadályozni, azt megtörni.

---

[625] DE SIMONE, D. – SOSHNIKOV, A. – WINSTON, A.: Neo-Nazi Rinaldo Nazzaro running US militant group The Base from Russia. BBC. (2020, January 24). https://www.bbc.com/news/world-51236915 (2021.07.29.)

[626] MAKUCH, B. – LAMOUREUX, M.: Neo-Nazis Are Organizing Secretive Paramilitary Training Across America. Vice. (2018, November 20). https://www.vice.com/en/article/a3mexp/neo-nazis-are-organizing-secretive-paramilitary-training-across-america (2021.07.29.)

[627] RÉPÁSI K.: Az új-zélandi terrortámadást követő szélsőjobboldali merénylethullám. Szakmai Szemle, 2021/2. 59. o.

[628] TARRANT, B.: The Great Replacement. https://www.ilfoglio.it/userUpload/The_Great_Replacementconvertito.pdf (2020.05.14.)

[629] CONWAY (2006): i.m. 21. o.

XII. AZ ONLINE TERJEDŐ ÖSSZEESKÜVÉS-ELMÉLETEK ÉS A HOZZÁJUK FŰZŐDŐ TERRORVESZÉLY

1. Összeesküvés-elméletek és káros következményeik

Összeesküvés-elméletek Sternisko et al. szerint: „(…) elméletek arról, hogy hatalommal rendelkező emberek egy csoportja titokban egy rosszindulatú vagy törvénytelen cél érdekében dolgozik."[630]

Léteznek valódi összeesküvések, melyekről a társadalom belső szakmai dokumentumokból, kormányzati vizsgálatokból vagy a visszaélést bejelentő személyektől (whistleblowerek) értesül. Például a Volkswagen konspirált, hogy meghamisíthassa a dízelmotorjain végzett emissziós teszteket, az NSA titokban kémkedett civil internethasználók után. Az összeesküvés-elméletek viszont még döntő bizonyíték nélkül is sokáig megmaradnak a köztudatban, és a társadalmat több módon károsítják. A valódi összeesküvések feltárása sokkal inkább történik a konvencionális gondolkodás, a hivatalos beszámolókkal kapcsolatos egészséges szkepticizmus, valamint a bizonyítékok körültekintő mérlegelése és a belső konzisztencia iránti elkötelezettség segítségével. Az összeesküvéses gondolkodást ezzel szemben az elméletbe nem illeszkedő információkkal kapcsolatos hiperszkepticizmus, az előnyben részesített elméletet alátámasztó bizonyítékok egyoldalú értelmezése és a következetlenség jellemzi.

Miért olyan népszerűek az összeesküvés-elméletek? A magukat kiszolgáltatottnak vagy tehetetlennek érzők nagyobb valószínűséggel támogatnak és terjesztenek összeesküvés-elméleteket. Ez jól megfigyelhető az internetes fórumokon. Az emberek hajlamosak összeesküvéses magyarázatot adni a valószínűtlen eseményekre. Ezek az elméletek egyfajta megküzdési mechanizmusként működnek, melyekkel a bizonytalanságot próbálják kezelni, úgy, hogy a fenyegető eseményekkel kapcsolatban az összeesküvőket hibáztatják. Az ilyen elméletek általában megkérdőjelezik a hagyományos politikai

[630] „(…) theories that a powerful group of people are secretly working towards a malevolent or unlawful goal". Saját fordítás. STERNISKO, A. – CICHOCKA, A. – VAN BAVEL, J. J.: The dark side of social movements: social identity, non-conformity, and the lure of conspiracy theories. Current Opinion in Psychology, 2020. Vol. 35. 1. o.

magyarázatokat. Az összeesüvés-elméleteket a közösségi média felerősíti.[631]

Krízisek idején mindig jelentek meg ilyen új elméletek, mely alól a koronavírus pandémia sem kivétel. Az ilyen elméletek jelentős és káros következményekkel járnak.[632] Hatással vannak az emberek egészségére, kapcsolataira és biztonságára. A bennük való hit széles körben elterjedt időkben, kultúrákban és társadalmi környezetekben. Nem racionális mérlegelésen, hanem negatív érzelmeken alapulnak. Szorosan összefüggnek a csoportközi konfliktus mögött álló pszichológiai motivációkkal.[633]

Ezek a teóriák veszélyt jelentenek a demokráciákra. A közösségi média megjelenésével az összeesküvés elméletekben hívők új felülethez jutottak, melyeken eddig példátlan sebességgel terjeszthetik nézeteiket és veszélyes társadalmi mozgalmakat szervezhetnek.[634] Az olyan összeesküvés-elméletek, mint a Pizzagate, COVID-19 összeesküvések, és QAnon, gyorsan terjednek, ezekben a narratívákban hívő személyek pedig hajtottak végre veszélyes való életbeli cselekményeket. A valódi összeesküvések és az összeesküvés-elméletek a demokráciát a maguk sajátos módján veszélyeztetik. Ahogy korábban szó volt róla, valódi összeesküvésekre általában a szabad és független sajtó nyomozásának köszönhetően derül fény, és felfedi a korrupciót a kormányzatban vagy az iparban, ezért egy valódi összeesküvés felfedezése a demokratikuis intézmények erejét igazolja. Ezzel szemben az összeesküvés-elméletek egyenesen a demokratikus intézményeket szándékozzák aláásni.[635] Az online peremközösségek (fringe communities) felületein a felhasználók a mainstream hírekben gyanakvást ébresztő paranoid ideákat és összeesküvés-elméleteket találhatnak és oszthatnak meg egymással.[636]

---

631 LEWANDOWSKY, S. – COOK, J.: Az összeesküvés-elméletek kézikönyve. Center for Climate Change Communication, Fairfax, 2020. 3–4. o.

632 DOUGLAS, K. M.: Are Conspiracy Theories Harmless? The Spanish Journal of Psychology, 2021. Vol. 24. 1–7. o.

633 VAN PROOIJEN, J.-W. – DOUGLAS, K. M.: Belief in conspiracy theories: Basic principles of an emerging research domain. European Journal of Social Psychology, 2018. Vol. 48. No. 7. 897. o.

634 STERNISKO – CICHOCKA – VAN BAVEL: i.m. 4. o.

635 TANGHERLINI, T. R. – SHAHSAVARI, S. – SHAHBAZI, B. – EBRAHIMZADEH, E. – ROYCHOWDHURY, V.: An automated pipeline for the discovery of conspiracy and conspiracy theory narrative frameworks: Bridgegate, Pizzagate and storytelling on the web. PLOS One, 2020. Vol. 15. No. 6. 34. o.

636 PAPASAVVA, A. – BLACKBURN, J. – STRINGHINI, G. – ZANNETTOU, S. – DE CRISTOFARO, E.: "Is it a Qoincidence?": A First Step Towards Understanding and Characterizing the QAnon Movement on Voat.co. In: LESKOVEC, J. – GROBELNIK, M. – NAJORK, M. – TANG, J. – ZIA, L. (szerk.): WWW '21: Proceedings of the Web Conference 2021. Association for Computing Machinery, New York, 2021. 460.

2. Összeesküvés-elméletek és a terrorveszély

Az FBI a szélsőséges összeesküvés-elméleteket hazai terrorista (domestic terrorist) fenyegetésként azonosította. Egy 2019. május 30-i intelligence bulletin az FBI phoenix-i területi irodájából az „összeesküvés-elmélet által vezértelt hazai extrémistákat" („conspiracy theory-driven domestic extremists") egy növekvő fenyegetésként jellemzi, és hozzáteszi, hogy ez az első jelentés, ami így tesz. Számos, köztük néhány addig nyilvánosságra nem hozott szélsőséges hiedelem által motivált erőszakos incidenshez fűződő letartóztatást sorol fel. A dokumentum kifejezetten említi a QAnon-t.[637] Az FBI az USA-t a hazai erőszakos extrémisták növekvő veszélyére figyelmeztette, azt 2021 első számú terrorista fenyegetésének nevezve.[638]

A koronavírus egyik hatásaként fokozódik a cyber-enabled crime, a terrorizmus és az információs hadviselés, például dezinformációs kampányok és álhírek terjesztése, amik aláássák a társadalom szövetét, zavargásokhoz vezetnek, és növelik a félelmet, az idegességet és bizonytalanságot.[639] Rathjen 2020. február 19-i haunau-i merénylete is példázza, hogy az összeesküvés-elméleteknek szerepük lehet a terrorizmusra való radikalizációban.[640]

A QAnon összeesküvés-elmélet hívei jelen voltak az Amerikai Egyesült Államok Capitoliumának 2021. január 6-i ostroma során, melyet többen, köztük Joe Biden terrorizmusként jellemeztek.[641]

---

o.

[637] WINTER, J.: Exclusive: FBI document warns conspiracy theories are a new domestic terrorism threat. Yahoo! News. (2019, August 1). https://news.yahoo.com/fbi-documents-conspiracy-theories-terrorism-160000507.html (2021.12.08.)

[638] SCHULTE, S.: FBI warns America about domestic terrorism following attack on US Capitol. ABC 7 Chicago. (2021, January 14). https://abc7chicago.com/domestic-terrorism-fbi-us-capitol-building-the-internet/9634442/ (2021.12.28.)

[639] GRADOŃ: i.m. 134. o.

[640] CRAWFORD, B. – KEEN, F.: The Hanau Terrorist Attack: How Race Hate and Conspiracy Theories Are Fueling Global Far-Right Violence. CTC Sentinel, 2020. Vol. 13. No. 3. 1–8. o. Idézi: AMARASINGAM, A. – ARGENTINO, M.-A.: The QAnon Conspiracy Theory: A Security Threat in the Making? CTC Sentinel, 2020. Vol. 13. No. 7. 41. o.

[641] Joe Biden slams pro-Trump mob as 'domestic terrorists'. Deutsche Welle. (2021, January 7). https://www.dw.com/en/joe-biden-slams-pro-trump-mob-as-domestic-terrorists/a-56163969 (2021.11.03.)

3. The Great Replacement elmélet

2019. március 15-én Tarrant, a christchurch-i terrorcselekmény elkövetője az elkövetés előtt bejelentette a szándékait a 8chan-on, manifesztumát az oldalra linkelte, és livestreamelte a támadását Facebookon egy linken keresztül, amit a 8chan's /pol/ felületére is kiposztolt. Earnest, a 2019. áprilisi Poway-i és Crusius, a 2019. augusztusi El paso-i támadások elkövetői is posztoltak manifesztumot a 8chan-ra, és mint Tarrant, azokban mindketten merítettek a „The Great Replacement" elméletből, Crusius explicit, Earnest implicit módon. Tarrant manifesztuma kifejezetten említi az elméletet, mint a támadás motivációját. Ezen összeesküvés-elmélet fő ideái évek óta jelen vannak a szélsőjobboldali körökben, de az Institute for Strategic Dialogue extrém jobboldali miliőkben végzett kutatása szerint a teória nem csak az erőszakos extrém jobboldali csoportokban dominál a „dark social" platformokon, hanem a szélsőjobb nyelvezetében és ideológiáiban, a xenofób és nativista csoportokban, európai és azon túli politikai pártokban is. Különösen az elmélet központi szerepe a Christchurch terrortámadásban igényli, hogy újraértékeljük az olyan csoportok fenyegetését, akik továbbra is támogatják és terjesztik az elméletet online. A francia filozófus és író Renaud Camus alkotta meg a kifejezést a 2011-es Le Grand Remplacement (The Great Replacement) című könyvében. A teória támogatói amellett érvelnek, hogy a fehér európai népességeket migrációval és a kisebbségi közösségek növelésével etnikai és kulturális szinten szándékosan felcserélik. Az idea gyakran demográfiai prognózisokra támaszkodik, hogy nyugati populációs változásokra mutasson rá, és arra, hogy az etnikailag fehér populációk kisebbséggé válhatnak. Bizonyos etnikai és vallási csoportok – elsősorban a muszlimok – tipikusan kiemeltek, mint kulturálisan összeegyeztethetetlenek a nyugati országokban élő fő csoportok életével, és ezért különös fenyegetést jelentenek. A teória szorosan kapcsolódik más fehér felsőbbrendűséget hirdető, etno-nacionalista és nativista körökben népszerű elméletekhez, köztük a white genocide/fehér fajírtás és Eurabia ideáihoz, úgy, hogy ezek a koncepciók gyakran szinonimaként használtak. A „white genocide" („fehér fajírtás") kifejezést először David Lane népszerűsítette, amellett érvelve, hogy a fehér lakosságokat bevándorlással, integrálással, abortusszal és fehér emberek elleni erőszakkal cserélik fel. Abban különbözik a Great Replacement elmélettől, hogy az gyakran explicit módon anti-szemita összeesküvés elméletekhez kapcsolódik, arra utalva, hogy a zsidók szándékosan szervezik a lakosság felcserélését. Az „Eurabia-t" a 2000-es évek elején Bat Ye'or (más néven Gisèle Littman) indítványozta, amellett

érvelve, hogy a nyugati országokat lassan iszlám uralom alá hajtják. Breivik, norvég terrorista sokat utalt az Eurabia iszlamizáció elméletre. 2011 óta a „Great Replacement" ezen ideák egy aggasztóbb és potencionálisan veszélyes területre fejlődését kezdte el képviselni, a fehér emberek teljes felcserélését és az elit összeesküvését hangsúlyozva.[642] A Generation Identity Europe Census 2012 áprilisa és 2019 áprilisa között 1,5 millió a Great Replacement elméletre hivatkozó angol, francia, és német nyelvű tweet-et azonosított, melyek mennyisége a Christchurch-t megelőző hét évben egyenletesen nőtt. 2014-től 2018-ig a teóriát említő tweetek száma 120.000-ről 330.300-ra emelkedett, túlnyomó többségük francia felhasználóktól származott. Az extrém jobboldali közösségek választékos módszerekkel közvetítik az elméletet, köztük dehumanizáló rasszista mémekkel, demográfiai adatok elferdítésével és már tévesnek bizonyított tudományos eredményekkel. Az elméletet propagálók megtalálták a módjait, hogy különböző internetes peremközösségek sérelmeit beépítsék, a bevándorlásellenes, anti-LGBTQ+, abortuszellenes és intézményellenes narratívák összekapcsolásával. A teória szélsőséges cselekedetek elkövetésére képes inspirálni a híveit, a nem-erőszakos etnikai tisztogatástól, a „remigráción" át a népírtásig, részben azért, mert képes a krízis narratíváival sürgető érzést kelteni.[643]

4. A QAnon

1. A „The Storm" („A vihar") összeesküvés eredete és kapcsolata a QAnonnal

A QAnon hívők szerint a titkos háború Trump és a „deep state" (mély állam) hálózata között el fog vezetni a „Viharhoz", a leszámolás napjához, amikor Trump ellenfeleit letartóztatják vagy kivégzik.[644]
„The Storm" elmélet online azonnal felkapottá vált. Ez egy „meta-összeesküvés" amelyben a 2016-os választásokba való orosz beavatkozás és a Trump kampánnyal való esetleges összejátszással kapcsolatos vizsgálatok tekintetében minden fordítva van. Az

[642] DAVEY, J. – EBNER, J.: 'The Great Replacement': The Violent Consequences Of Mainstreamed Extremism. Institute for Strategic Dialogue, London, 2019. 7–8. o.

[643] Uo. 7–8. o.

[644] COURTY, A.: QAnon believers will likely outlast and outsmart Twitter's bans. The Conversation. (2020, July 24). https://theconversation.com/qanon-believers-will-likely-outlast-and-outsmart-twitters-bans-143192 (2021.10.21.)

elmélet szerint Robert Mueller demokraták és hollywoodi celebek százai ellen készül eljárást indítani egy masszív, globális pedofil hálózatban való szerepük miatt, melyet „globalisták" működtetnek, akik Trump elpusztítására konspirálnak, aki ennek az „ellenpuccsnak" a feje. Néhány hét leforgása alatt a teória majdnem minden összeesküvés-elmélet hívő megszállotságává vált, különösen Alex Jones-nak és az InfoWars[645] oldalának, és prominens közösségi média szereplőknek, mint Liz Crokin. A „The Storm" Trump 2017. október 6-i rejtélyes megjegyzéseiből eredeztethető, amikor azt mondta egy katonai vezetők gyülekezetére, hogy az „a vihar előtti csend" („the calm before the storm"). Mikor megkérdezték Trump-ot, hogy ez alatt mit értett, azt válaszolta, hogy: „Majd meglátják." („You'll see.") Három héttel később egy névtelen posztoló a 4chan üzenőfalán – az alt-jobb egyik legfőbb fórumán – azt állította, hogy magas szintű „Q" nemzetbiztonsági igazolvánnyal rendelkezik, és elkezdett rejtélyes üzeneteket közzétenni, melyeket „hírszerzési morzsáknak" („intel drops") nevezett, melyek célja informálni a nyilvánosságot arról, valójában mi is történik a Fehér Házban, és mit jelentettt Trump furcsa megjegyzése. „QAnon" (az anon az anonymous rövidítése) szerint Trump megjegyzése Mueller késő októberi vádemeléseire utalt. „QAnon" szerint Trump után sosem nyomoztak, a vádemelések a globális pedofihálózat masszív konspirációja ellen irányultak, melyet magas szintű demokraták és más „globalisták" működtetnek, akik egy olyan „mély állam" összeesküvésben vesznek részt, melynek célja egy Trump megbuktatására irányuló puccs. Ugyanez a pedofil gyűrű volt a „Pizzagate" összeesküvés-elmélet fókusza, ami hónapokig izgalomban tartotta a szélsőjobbot a 2016-os választás utáni hónapokban. Ennek hívői, köztük Jones azt állította, hogy a Clinton kampányfőnök, John Podesta email-ei, melyeket a kampány során hackerek eltérítettek, és közzétettek a Wikileaks-en, felfedték azt, hogy ő, Clinton, és rengeteg másik ember egy washington-i pizzériából működő pedofil-gyűrű része volt.

A teória új, kiterjesztett verzójában a gyűrű globálissá vált. „QAnon" és az összeesküvés-elméleteket gyártók a 4chan, 8chan, és a Twitter felületein azt állították, hogy ez a pedofil-gyűrű Mueller nyomozásának a valódi fókusza. Az volt az általános meggyőződés a közösségi médián, hogy hamarosan köztük Clinton, Obama, Podesta, Soros, és McCain szenátor, és számos hollywood-i celeb és demokraták elleni letartóztatási hullám fog hamarosan megtörténni. „QAnon" tekintetében már hamar hitelességi probléma állt fent, mert 2017. november elején egy olyan forgatókönyvet tett közzé, mely szerint napokon belül letartóztatások százai és masszív társadalmi zűrzavar

[645] InfoWars. https://www.infowars.com/ (2021.10.21.)

fog bekövetkezni. Novemberben ilyen nem történt, de ez nem fogta vissza követőinek lelkesedését. A Southern Poverty Law Center (SPLC) Hate Tracker-e – mely az extrémista ideológiák és állítások Twitter-es terjedését ellenőrzi – szerint közéjük tartozik a radikális jobboldali közösségi média felhasználók jelentős része.[646]

2. A QAnon alapjai és fejlődése

A QAnon egy nagy esernyőelmélet, egy metanarratíva, ami több évszázados rasszista nézetekkel fűzi egybe a jelenkori politikát. Ideája lényegében az, az összes amerikai elnök John F. Kennedy és Donald Trump között egy globalista elitből álló „The Cabal" nevű titkos társasággal (A cabal szó magyarul nagyjából titkos társaságnak felel meg.) dolgozott együtt az amerikai demokrácia aláásásán és a saját aljas céljaik elérésén. Ebbe a titkos társaságba tartozik Soros és a Rothschild család is, de a teória inkább elitellenes, mint explicit módon antiszemita. A mítosz összes változatában ez a „Cabal" célja az amerikai szabadság elpusztítása és alávetni a nemzetet egy világkormány akaratának. A mítosz néhány verziójában a titkos társasághoz köthető pedofília, véráldozat, sátánizmus, és más bűnök is. A QAnon egy reményteli összeesküvés-elmélet. A „Vihar" közeleg. Trump titokban Mueller-rel dolgozik a nemzet elpusztítására törekvő „mély állam" letartóztatásán. A vádiratokat már benyújtották, már bármelyik nap bekövetkezhetnek a letartóztatások, és azokat katonai büntetőeljárások és valószínűleg kivégzések is követik.

A QAnon sok szempontból úgy viselkedik, mint a legtöbb összeesküvés-elmélet.

Alapvető vonzereje a narratívája, mely megmagyarázza a felkavaró és zavarbaejtő eseményeket, és megnyugtatja a hívőit, ők értik a háttérben lévő valódi értelmet, nem úgy, mint a nem hívők. A QAnon narratívája az irányíthatatlan események feletti kontroll érzését nyújtja a hívőknek. Az elmélet követőei folyamatosan emlékeztetik egymást, hogy „bízzanak a tervben" („trust the plan"), hogy Trump és a csapata okkal teszi a lépeseit, beleértve, hogy a terveiket az interneten, kétes üzenőfalakon osztják meg.[647]

---

[646] NEIWERT, D.: Conspiracy meta-theory 'The Storm' pushes the 'alternative' envelope yet again. Southern Poverty Law Center. (2018, January 17). https://www.splcenter.org/hatewatch/2018/01/17/conspiracy-meta-theory-storm-pushes-alternative-envelope-yet-again (2021.10.25.)

[647] ZUCKERMAN, E.: QAnon and the Emergence of the Unreal. Journal of Design and Science, 2019. No. 6. 3–4. o.

John F. Kennedy Jr. és még két másik személy 1999 júliusában vesztette életét, amikor balesetett szenvedtek egy kisméretű repülőgéppel, testüket az Atlanti-óceánban találták meg. QAnon szerint ez másképp történt: JFK Jr. túlélt egy „mély állam" merényletkísérletet, és hamarosan visszatér, hogy bosszút álljon, és segítsen Trump-nak a világban minden rosszért felelős, globálisan aktív, sátánista, pedofil elit titkos társaság legyőzésében. A QAnon világnézet kifejezetten hajlamos ilyen jóslatokba bocsátkozni, és sok hívője türelmetlenül várja az olyan világmegváltó eseményeket, mint „the Storm" és a „Great Awakening" („Nagy Felébredés", amikor a népesség ráeszmél arra, hogy évtizedek óta hazudtak nekik). A legtöbb ilyen mozgalom túlélheti az ilyen próféciák be nem teljesedését, ha bizonyos feltételek teljesülnek. Hogy JFK Jr. nem tért vissza, csak egy QAnon számos nem teljesült proféciái közül. Hillary Clinton-t nem tartóztatták le, eliteket nem öltek meg és nem küldtek a Guantánamói-öbölbe, több százezer vádirat nem került nyilvánosságra, az ígért aranykor nem jött el, de a mozgalom tovább él.[648] QAnon az interneten született, és továbbra is ott toboroz.[649] 2017 október 28-án egy magát „Q-nak" nevező felhasználó, aki azt állította, hogy magas szintű biztonsági engedéllyel rendelkezik, a 4chan oldal „politically incorrect" szekciójában (Később a 8chan-on és az azt követő 8kun-on.[650]) rejtélyes üzeneteket tett közzé. Q azt állította, hogy titokban azon munkálkodik, hogy tájékoztassa a nyilvánosságot Trump „mély állammal" vívott harcáról. Az ezt követő években magukat „Q-nak" állító felhasználók több mint 4.000 posztot tettek közzé, melyek, „Qdrops" vagy „breadcrumbs-ként" ismertek, amelyek egy metaösszeesküvés-elmélet növekedését táplálták. A QAnon teória már összeköti az oltásellenességet, az anti-5G összeesküvés-elméleteket, az antiszemitizmust és a bevándorlóellenességet és számos bizarr elméletet, köztük azt, hogy a világ egy pedofil elit rabszolgája, akik ritualisztikus gyermekáldozatok által törnek világuralomra.[651]

[648] AMARASINGAM, A. – ARGENTINO, M.-A.: QAnon's Predictions Haven't Come True; So How Does the Movement Survive the Failure of Prophecy? Religion Dispatches. (2020, October 28). https://religiondispatches.org/qanons-predictions-havent-come-true-so-how-does-the-movement-survive-the-failure-of-prophecy/ (2021.11.02.)

[649] BEENE, S. – GREERB, K.: A call to action for librarians: Countering conspiracy theories in the age of QAnon. The Journal of Academic Librarianship, 2021. Vol. 47. No. 1. 2. o.

[650] FRANCESCANI, C.: The men behind QAnon. ABC News. (2020, September 22). https://abcnews.go.com/Politics/men-qanon/story?id=73046374 (2021.11.05.)

[651] GALLAGHER, A. – DAVEY, J. – HART, M.: The Genesis of a Conspiracy Theory: Key trends in QAnon activity since 2017. Institute for Strategic Dialogue, London/Washington DC/Beirut/Toronto, 2020. 3. o. https://www.isdglobal.org/wp-content/uploads/2020/07/The-Genesis-of-a-Conspiracy-Theory.pdf

A legsikeresebb összesküvés-elméletek formálódnak és fejlődnek, hogy relevánsak maradhassanak.[652] 2020-ra Q összeesküvés-elmélete jelentősen kiterjedt. Hívei számát több százezerre becsülik. Állításaik összetettek, maguknak ellentmondók, és több ideológia keveredik bennük.[653]

Az utóbbi időkben a Q-hívők számos koronavírussal kapcsolatos összeesküvés-elméletet is terjesztettek, köztük olyan állításokat, hogy a vírus csupán átverés, vagy egy kínai biofegyver, mely célja rontani Trump újraválasztási esélyeit.[654]

Továbbá arról, hogy az elit a koronavírust használja fel arra, hogy az embereket chippel lássák el, hogy a kormányok 5G tornyokat állítanak a zárlatok alatt a népesség megfigyelésére, és sok más evangélikus kereszténységbe csomagolt apokaliptikus jóslatot, mely egyre jobban meghatározza a mozgalmat. A QAnon gyökerei populisták, célja neheztelést ébreszteni az átlagemberben. A zavaros állításai hasonlítanak korábbi elméletekre, de a közösségi média felületet adott a híveinek, hogy megosszanak, promótáljanak, kapcsolatba lépjenek egymással. Történtek lépések ellene. 2020 júliusában a Twitter felfüggesztett 7.000 QAnon-hoz fűződő fiókot. Augusztusban a Facebook több mint 790 QAnonhoz kötődő csoportot, 100 oldalt, és 1.500 hirdetést törölt, és korlátozta több száz más Facebook-csooport fiókjait és több ezer Instagram fiókot.[655] QAnon, a szélsőjoboldali öszeesküvés-elméletek bizarr ötvözete számos embert radikalizált erőszakos cselekmények elkövetésére. Ugyan kevésbé szervezettebbek, mint a dzsihadisák vagy a jobboldali extrémisták, de Amarasingam és Argentino szerint a QAnon új biztonsági fenyegetést képvisel.[656]

2018-ban a Time magazin Q-t az internet 25 legbefolyásosabb embere közé sorolta. Q „drops-ai", a 4chan és 8chan-re posztolt több ezer rejtélyes írása számtalan YouTube videóhoz, podcast-hoz, és számos online és offline íráshoz, vezetett, melyek a „Q Clearance Patriot" szavait próbálják értelmezni. 2019. márciusban, a QAnon követők által írt „QAnon: An Invitation to a Great Awakening" című könyv az Amazon másodk

---

(2021.11.05.)

[652] BEENE – GREERB: i.m. 2. o.

[653] DE SMEDT, T. – RUPAR, V. – JAKI, S. – CAUBERGHS, O. – VOUÉ, P. – CABALLERO, J.: The QAnon superconspiracy - Analysis of tweets during the 2020 US presidential election. 2020. 2. o. https://www.researchgate.net/publication/348281072_The_QAnon_superconspiracy_-_Analysis_of_tweets_during_the_2020_US_presidential_election (2021.12.08.)

[654] COURTY: i.m.

[655] DE SMEDT – RUPAR – JAKI – CAUBERGHS – VOUÉ – CABALLERO: i.m. 2. o.

[656] AMARASINGAM, A. – ARGENTINO, M.-A.: The QAnon Conspiracy Theory: A Security Threat in the Making? CTC Sentinel, 2020. Vol. 13. No. 7. 37. o.

legeladottab könyve volt.[657]

„Q" pólók és táblák gyakran láthatóak Trump eseményein. Még QAnon hirdetőtáblák is bukkantak fel az USA-ban. "Q-s" termékek vásárolhatók az Amazonon. A Qanon applikáció meglepően népszerű volt az Apple App Store-ján, amíg el nem távolították.[658]

3. QAnon-hoz köthető elkövetések

QAnon hívőkhöz 2017 óta köthetők különféle fegyveres elkövetések, emberrablási kísérletek, zaklatások, emberölés.[659]

2018 júniusában a nevadai Matthew Wright egy AR-15 típusú gépkarabéllyal, egy kézifegyverrel és extra lőszerrel felfegyverkezve egy páncélozott teherautót vezetett egy a hídhoz, közel a Hoover-gáthoz. Ott 90 perces fegyveres patthelyzetbe került a rendőrséggel, miközben egy jelentés közzétételét követelte a Hillary Clinton e-mailváltásaival kapcsolatos kormányzati vizsgálatról. Letartóztatása után leveleket írt Trumpnak és más tisztviselőknek, magát „szerény hazafinek" nevezve és QAnon szlogeneket idézett, mint a „Great Awakening" és „Where we go one, we go all" („Ahová egyikünk megy, oda mindanyian megyünk").

Michael Lewis Arthur Meyer-t, a tucson-i helyi veterán-segítő csoport vezetőjét, 2018 júliusában, Arizonában letartóztatták, miután megszállt egy tornyot egy cementgyárban, amiről azt állította, hogy egy pedofil gyűrűt szállásol. Az FBI bulletin szerint Meyer azt állította, hogy a bűnöldöző szervek azt elfedték, és QAnon-t hivatkozta, miközben ő és egy fegyveres csoport a gyűrűt kereste.

Az FBI bulletin elkészülte után történtek még incidensek Arizona és Colorado államokban. Timothy Larson-t 2019 szeptemberében azzal vádolták, hogy feszítővassal rongálta az oltárt a sedona-i Chapel of the Holy Cross-ban, miközben a katolikus egyházról és a szexkereskedelemről ordított. Larson közösségi médiája tele volt QAnon utalásokkal és pro-Trump mémekkel.

2019. decemberben a coloradoi Parkerben Cynthia Abcug-ot azzal vádolták, hogy más QAnon hívőkkel együtt az egyik tőle elvett gyermeke elrablását tervezte. Abcug úgy hitte, hogy a gyermekét sátánimádók és pedofilok tartották fogva.

---

[657] ZUCKERMAN: i.m. 3. o.

[658] COLLINS, B. – ZADROZNY, B.: The far right is struggling to contain Qanon after giving it life. NBC News. (2018, August 11). https://www.nbcnews.com/tech/tech-news/far-right-struggling-contain-qanon-after-giving-it-life-n899741 (2021.12.08.)

[659] COURTY: i.m.

2019. decemberben Anthony Comello azt állította egy New York City bíróságon, hogy a QAnon vezette egy Gambino maffiavezér, Francesco Cali megöléséhez, akiről azt állította, hogy a Trump ellen munkálkodó mély állam tagja volt.[660] A QAnon már nem csupán egy perem (fringe) összeesküvés-elmélet, hanem egy olyan ideológia, ami demonstrálta, hogy képes nagyon gyorsan erőszakra radikalizálni.[661]
A szélsőjobboldlai összeesküvés-elmélet a 2020-as elnökválasztás előtt vált különösen népszerűvé.[662] Hónapokig Trump azt állította, hogy a novemberi elnökválasztást elcsalták, ezért nem választották újra. Trump szavai a QAnon hiedelmeit tükrözték és táplálták azokat. A QAnon hívők a Capitol Hill-t megostromlók első soraiban voltak.[663] Az összeesküvés-elmélet Németországban is terjed.[664]
Biden 2021. január 20-i beiktatása után több Q-hívő feladta, mások még mindig „bíznak a tervben" („trust the plan").[665]

4. A Q-hívők aktivitása online platformokon

Gallagher et al. nyomon követte a teóriáról szóló diszkussziókat a Facebook, Twitter, Instagram és YouTube platformokon, arra jutva, hogy mind a négy felület komoly szerepet játszik az elmélet terjedésében, és a társalgás jelentősen növekedett 2020-ban, különösen az elnökválasztást megelőzően. A szerzők analízise rámutat arra, hogy a teória és hívői fontos szerepet játszottak a dezinfomáció terjesztésében a koronavírust és George Floyd halálához kötődő tüntetéseket illetően. Gallagher et al. szerint a QAnon közösség be akarja feketíteni Trump politikai ellenfeleit, miközben támogatóit

[660] MCINTIRE, M. – ROOSE, K.: What Happens When QAnon Seeps From the Web to the Offline World. The New York Times. (2020, February 9). https://www.nytimes.com/2020/02/09/us/politics/qanon-trump-conspiracy-theory.html (2021.12.09.)

[661] AMARASINGAM, A. – ARGENTINO, M.-A.: The QAnon Conspiracy Theory: A Security Threat in the Making? CTC Sentinel, 2020. Vol. 13. No. 7. 42. o.

[662] FERRARA, E. – CHANG, H. – CHEN, E. – MURIC, G. – PATEL, Jaimin: Characterizing Social Media Manipulation in the 2020 U.S. Presidential Election. First Monday, 2020. Vol. 25. No. 11.

[663] ARGENTINO, M.-A.: QAnon and the storm of the US Capitol: The offline effect of online conspiracy theories. Quartz. (2021, January 7). https://qz.com/1954265/the-attack-on-the-us-capitol-shows-the-real-danger-of-qanon/ (2021.12.09.)

[664] FELDEN, E. – WILDON, J. – HÖHN, A. – SANDERS, L.: As Donald Trump exits, QAnon takes hold in Germany. Deutsche Welle. (2021, January 19). https://www.dw.com/en/as-donald-trump-exits-qanon-takes-hold-in-germany/a-56277928 (2021.12.09.)

[665] DICKSON, E. J.: QAnon Believers Struggle With the Two Hardest Words: 'President Biden'. Rolling Stone. (2021, January 20). https://www.rollingstone.com/culture/culture-news/qanon-joe-biden-inauguration-donald-trump-1116733/ (2021.12.09.)

bálványozza. A választás előtt komoly szerepet játszottak a dezinformáció terjesztésében.[666] Gallagher et al. Facebookhoz és Instagramhoz kötődő megállapításai a következők: a felületeken a QAnon körüli társalgás és az ebben résztvevők jelentős növekedése volt megfigyelhető 2020-ban. A legfőbb növekedés 2020 márciusában történt, ekkor a Facebook használók száma március 2. és 8. között átlagban napi 344 volt, mely március 22 és 29 között 898-ra növekedett. Hasonlóan, a Twitter felhasználók átlagos száma az első heti 37.302-höz képest az utolsó hétre 89.338-re növekedett. 2020 márciusában a Facebook csoportok tagszáma 120%-ot nőtt, és az azokban folyó társalgás pedig 91%-ot. További kutatást éremelne az, hogy miért növekszik ilyen gyorsan a QAnon közösség, de Gallagher et al. szerint a lehetséges magyarázat lehet az, hogy ez a melléktermék annak, hogy a koronavírus-zárlatok miatt az emberek több időt töltenek a közösségi médián, vagy ez lehet egy koordinált tevékenység eredménye is. A Twitter QAnon forgalma 2017 óta változatosabb volt, és gyakran való életbeli eseményekre reagált. A legnagyobb, 249%-os növekedés a Twitter-es társalgásban 2018 januárjában történt, két hónappal a mozgalom létrejötte után, mikor a közösség a #ReleaseTheMemo hashtag-et használta. Ez a trend médiafigyelmet vont magára, kutatások pedig a Twitteren orosz botok bevatkozását sugallták. Ekkor még nem látszott fokozódás a Facebook-os társalgásokban. Más jelentős Twitteren és Facebookon látható ugráshoz vezető események közé tartozik a Q követők első feltűnése Trump-felvonulásokon 2018 augusztusában, és Jeffrey Epstein 2019. augusztusi halála. Elsősorban az USA-hoz köthető, de nemzetközi szinten is terjed. A top négy ország, melyek vezették a QAnon diszkussziót a Twitteren az USA, az Egyesült Királyság, Kanada és Ausztrália. Az USA volt felelős a Q-hoz fűződő hashtag-ek 89,5%-áért 2017. október és 2019 októbere között. Ez az arány később csökkent, jelezve, hogy az elmélet elkezdett nemzetközi szintre jutni. A YouTube fontos szerepet játszik a Q-hoz fűződő tartalom megosztásában: az összes Q-hoz fűződő Facebook poszt 20,4%-a tartalmazott YouTube linket, míg ez az arány 5% volt a Twitteren. Ezek a link-megosztások is jelentős növekedést mutattak 2020 márciusában.[667]

2020. június 20 és szeptember 9 között több mint 240 millió választással kapcslatos tweet rögzítésével Ferrara et al. tanulmányában felmérte a közösségi média manipulációt a 2020 november 3-i amerikai elnökválasztással kapcsolatban. Ferrara et al. a közösségi média manipuláció két kiugró dimenziójának jellemzésére fókuszált, az automatizálás (pl. botok használata), és torzítás (pl. narratívák manipulációja, összeesküvés-elméletek

[666] GALLAGHER – DAVEY – HART: i.m. 3–4. o.

[667] Uo. 4–5. o.

és pletykák terjesztése). A tanulmány szerint csupán néhány ezer bot képes volt ennél sokkal több ember társalgásában megugrásokat generálni, politikai eseményekkel kapcsolatban.

Ferrara et al. felfedezte, hogy a botok az azonos politikai nézeteket vallók által előállított tartalmak fogyasztását is fokozzák, tovább rontva a politikai visszhangkamrák (political echo chambers, amikor a felhasználók az interneten csak a hasonló gondolkodású társaikkal kommunikálnak[668]) problémáját.

Ferrara et al. egyértelmű kapcsolatot lát a botok, hiperpartizán (szélsőségesen pártos[669]) sajtóorgánumok, és összeesküvés-elméletes csoportok között, a politikai narratívák torzítására és dezinformáció propagálására történő szisztematikus törekvést sugallva. A szerzők kutatása fényt derít a közösségi média manipuláció különféle formáira, amik veszélyeztethetik a választás integritását. Ferrara et al. analízise három fő összeesküvés-elméletes csoportra fókuszált: QAnon, „gate" összeesküvések, Covid összeesküvések. Vizsgálatuk szerint a QAnon-hoz fűződően több az aktivitás és a felhasználó, mint a -gate narratívák esetében. A leggyakrabb hashtag-et, a #wwg1wga-t több mint 600.000 tweet szerepeltette 140.000 felhasználótól, ezzel szemben az #obamagate hashtag 414.000 tweet-ben szerepelt 125.000 felhasználótól. A Q-közösség hashtag használata aktívabb felhasználói bázist jelez.[670]

5. A Capitolium ostroma

Miután Trump beszédet mondott a támogatóinak, arra kérve őket, hogy „küzdjenek" a választás „ellopásának" megállításáért, Trump támogatók egy csoportja megpróbálta megakadályozni Biden választási győzelmének megerősítését, ezért 2021. január 6-án megrohamozta az Egyesült Államok Capitoliumát, és összecsapott a rendőrséggel, melyben négyen életüket vesztették. A rendőrök egy nőt lelőttek, míg három Trump-támogató „egészségügyi vészhelyzetben" halt meg. A Capitol Police egyik rendőre is belehalt a sérüléseibe.[671] Ahogy Matus fogalmaz: „(…) Trump személyiségében rejlő veszélyek valójában a Törvényhozás épülete elleni erőszakos támadásban

[668] GÁLIK M.: Visszhangkamrák és szűrőbuborékok. Médiakutató, 2020/1. 28. o.

[669] VARGA Á.: Textuális és állóképtartalmak: online megjelenés. In: GÁLIK M. – CSORDÁS T. (szerk.): A média gazdaságtanának kézikönyve. Nemzeti Média- és Hírközlési Hatóság Médiatanács Médiatudományi Intézete, Budapest, 2020. 178. o.

[670] FERRARA – CHANG – CHEN – MURIC – PATEL: i.m.

[671] FRANEY, J.: US Capitol storming: What you need to know. Deutsche Welle. (2021, January 7). https://www.dw.com/en/us-capitol-storming-what-you-need-to-know/a-56154560 (2021.11.02.)

manifesztálódtak. A 2021. január 6-i washingtoni tömeggyűlésen elmondott beszéde, amelyben a Kapitóliumhoz való felvonulásra és kemény harcra szólította fel híveit (fight like hell) egyenesen vezetett az erőszakos cselekményekhez. Ami történt, alátámasztja és egyértelműen igazolja a mentális egészséggel és az erőszak forrásainak kutatásával foglalkozó pszichiáterek elemzéseit és előrejelzéseit."[672]

Biden hazai terroristáknak („domestic terrorists") nevezte a Capitoliumot megostromló pro-Trump tömeget. Úgy véli, őket nem tüntetőknek, hanem „lázadó tömegnek, felkelőknek, hazai terroristáknak" („a riotous mob, insurrectionists, domestic terrorists,") kellene nevezni.[673]

Az esetnek jelentős interneten keringő összeesküvés-elméletekhez fűződő vonatkozásai is voltak.

Az ostromlók között volt a QAnon összeesküvés-elmélet egyik vezető alakja, a „Q Shaman", vagy „QAnon Shaman", más néven „Jake Angeli" (vagy Yellowstone Wolf[674]), az igazi nevén Jacob Anthony Chansley. A mozgalomnak nagy szerepe volt az országos szintű „Stop the Steal" tüntetésekben, Biden 2020-as választási győzelmét követő két hónapban.[675]

Sacco a „Domestic Terrorism and the Attack on the U.S. Capitol. CRS INSIGHT, 2021." című jelentésben azt vizsgálja, hogy kategorizálhatóak-e az ostromlók hazai terroristaként, cselekedeteik pedig hazai terrorizmusként, továbbá rávilágít a problémára a hazai szélsőséges csoportok (fringe groups), például a Boogaloo Bois és a Proud Boys terrorszervezetként való megjelölésével kapcsolatban, akik állítólag részt vettek a támadásban.[676]

A hazai terrorozmus szövetségi definíciója a következő: „Amerikaiak, akik ideológiai indíttatású bűncselekményeket követnek el az Egyesült Államokban, de hiányzik náluk a

---

[672] MATUS J.: A Trump elnökség tanulságai: Karakter és vezetés. Hadtudomány, 2020/4. 73. o.

[673] Joe Biden slams pro-Trump mob as 'domestic terrorists'. Deutsche Welle. (2021, January 7). https://www.dw.com/en/joe-biden-slams-pro-trump-mob-as-domestic-terrorists/a-56163969 (2021.11.03.)

[674] SCHAPIRO, R. – KOSNAR, M.: Capitol rioter in horned hat gloats as feds work to identify suspects. NBC News. (2021, January 8). https://www.nbcnews.com/news/us-news/capitol-rioter-horned-hat-gloats-feds-work-identify-suspects-n1253392 (2021.11.03.)

[675] GREENSPAN, R. E. – ORECCHIO-EGRESITZ, H.: A well-known QAnon influencer dubbed the 'Q Shaman' has been arrested after playing a highly visible role in the Capitol siege. Business Insider. (2021, January 9). https://www.businessinsider.com/q-shaman-qanon-influencer-capitol-siege-washington-dc-protest-riot-2021-1 (2021.11.03.)

[676] SACCO, L. N.: Domestic Terrorism and the Attack on the U.S. Capitol. Congressional Research Service, 2021. 1. o. https://crsreports.congress.gov/product/pdf/IN/IN11573 (2021.11.03.)

külföldi irányítás vagy befolyás."[677] Az FBI rendszerint két forrásra támaszkodik a hazai terrorozmus definiálásában. Elsőként, a Code of Federal Regulations Title 28 §0.85(l) szerint a terrorizmuson a következőt értjük: „személyek vagy tulajdon elleni erő és erőszak jogellenes alkalmazása egy kormány, a polgári lakosság vagy annak bármely szegmensének megfélemlítésére vagy kényszerítésére, politikai vagy társadalmi célok előmozdítása érdekében."[678] Másodszor, a Code of Laws of the United States of America Title 18 §2331(5) szűkebben határozza meg a hazai terrorizmust. Ez a definíció a USA PATRIOT Act (P.L. 107-56)[679] Section 802-ből való. A 18 U.S.C. §2331(5) szerint hazai terrorizmus elsősorban az USA területi joghatóságán belül fordul elő, mely alatt a következőket értjük: „(A) emberi életre veszélyes cselekmények, amelyek megsértik az Egyesült Államok vagy bármely állam büntető törvényeit; (B) amik úgy tűnik, hogy arra irányulnak– (i) hogy egy polgári lakosságot megfélemlítsenek vagy kényszerítsenek; (ii) hogy egy kormány politikáját befolyásoljanak megfélemlítéssel vagy kényszerítéssel; vagy iii) hogy egy kormány működését befolyásolja tömegpusztítással, merénylettel, vagy emberrablással…"[680] Sacco szerint úgy tűnik, az ostromlók cselekedeteire mindkét definíció illik.[681] Ugyan az elkövetők cselekményére illik a hazai terrorizmus meghatározása, Sacco megjegyzi, hogy az önmagában nem egy üldözhető bűncselekmény.

Míg a támadásban résztvevők olyan szélsőséges csoportokhoz tartozhatnak, mint a Proud Boys és a Boogaloo Bois, ezek az ideológiáinak voltak a híveik, Sacco kijelenti, hogy a szövetségi kormány elutasítja ezeknek a csoportoknak hazai terrorista csoportként minősítését, és helyette az egyén erőszakos bűncselekményeire fókuszál, függetlenül attól, hogy tagja-e ezeknek a csoportoknak.[682] A Capitolium ostromát

---

[677] „Americans who commit ideologically driven crimes in the United States but lack foreign direction or influence." Saját fordítás. Uo. 1. o.

[678] „the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives." Saját fordítás. United States Code of Federal Regulations Title 28 §0.85(l) Idézi: Uo. 1. o.

[679] Uniting And Strengthening America By Providing Appropriate Tools Required To Intercept And Obstruct Terrorism (USA Patriot Act) Act of 2001, PUBLIC LAW 107–56—OCT. 26, 2001. Idézi: Uo. 1. o.

[680] Code of Laws of the United States of America Title 18 §2331(5) https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title18-section2331&num=0&edition=prelim Idézi: Uo. 1–2. o.

[681] Uo. 1–2. o.

[682] Uo. 2. o.

követően Biden elnök utasította a bűnüldöző szerveket és a hírszerzést, hogy vizsgálják ki a hazai terrorizmus kockázatát.[683]

1) Az ostrom előtti online diszkussziók

Masszív publicitás előzte meg a „March for America-t," Trump és szövetségesei tweet-ekben promótálták, hirdették azt a közösségi médián, a Twitteren, Facebookon és Instagramon. A sok Trump mellett kiálló, és a választás kongresszusi jóváhagyását megakadályozni szándékozó üzenet között agresszív, erőszakos nyelvezet is felfedezhető volt. A „Storm the Capitol" („megostromolni a Capitoliomot") kifejezés 100.000 alkalommal került említésre a január 6-ot megelőző 30 nap alatt, a Zignal Labs médiacég szerint. Sok ilyen említés felkapott tweet kommentszálakban tűnt fel, melyek a Capitolium lehetséges megostromlását tárgyalták, köztük részleteket az épületbe való bejutásról. A Q-hívőknek a „storm" (jelent vihart és ostromot is) többes jelentéssel bír. QAnon hívők és milicista csoportok online arról társalogtak, hogy milyen fegyvereket és eszközöket vigyenek majd. „Pack a crowbar," („Hozz feszítővasat"), írta az egyik felhasználó a Gab-on. Más azt kérdezte, hogy: „Does anyone know if the windows on the second floor are reinforced?" („Tudja valaki, hogy a második emeleti ablakok megerősítettek-e?") Ezek ellenére nem tűnt úgy, hogy a rengeteg kommunikáció cselekvésre való széleskörű szervezést eredményezne. Az sem tiszta, hogy nagy pénzügyi támogatás, vagy koordinált adománygyűjtés állt-e a mobilizáció mögött, de néhány Trump támogató a felvonuláshoz való utazáshoz pénzügyi támogatáshoz online hálózatokon jutott hozzá. „Patriots, if you need financial help getting to DC to support President Trump on January 6th, please go to my website," („Hazafiak, ha szükségetek van pénzügyi segítségre eljutni DC-be, január 6-án Trump elnököt támogatni, kérlek, menjetek a weboldalamra") írta az esemény előtt három nappal a Titteren a Q-hívő Thad Williams, a floridai Tampából. Azt állította, több mint 27.000 USD-t gyűjtött. (A Capitolium ostroma után a PayPal és Stripe pénzátutalási szolgáltatók lekapcsolták a fiókjait. A szervezete, a Joy In Liberty website-ja közlése szerint 30.000 USD-t adott az „arra érdemes hazafiak" utazásának finanszírozására.) Más felvonulásra menők legalább egy tucat adománygyűjtő fiókot hoztak létre a GoFundMe-n, melyeket az óta az oldal leállított. A „Q Shaman-hoz" is kötődött online adománygyűjtés, decemberben nyitott egy GoFundMe fiókot, egy másik washingtoni Trump-demonstrációra utazása finanszírozása céljából, de csak 10 USD-t sikerült gyűjtenie. Retweetelte Williams

[683] Joe Biden orders review of US domestic extremism threat. Deutsche Welle. (2021, January 23). https://www.dw.com/en/joe-biden-orders-review-of-us-domestic-extremism-threat/a-56321162 (2021.11.05.)

finanszírozási ajánlatát január 3-án, de nem tudni, hogy előnye származott-e belőle.[684] Steven A. Sund volt a Capitol Police chief-je az ostrom idején. A támadást követően lemondott. Azt nyilatkozta, hogy a szerdai demonstrációval kapcsolatban hétfőn elkezdett aggódni, azt mondta, tudták, hogy az esemény nagyobb lesz, a hírszerzési adatok alapján tudták, hogy nagyobb tömegre számíthatnak, és hogy esély lesz erőszakos összecsapásokra, de szerinte semmi nem jelezte, hogy egy nagyobb tömeg elfoglalná majd a Capitoliumot. Elismerte, hogy állítólag alt-jobbos felbújtók az épület megostromlásáról és a törvényhozók célbavételéről társalogtak, de Sund szerint a múltban is bukkantak fel ilyen fenyegetések, és a közösségi médián sokszor látott már korábban ilyen retorikát, és „az emberek online sok dolgot mondanak."[685]

5. Miért kezelhetőek nehezen az összeesküvés-elméletek?

Amarasingam szerint nem egyértelmű, hogy a társadalom vagy a kormányok mit tegyenek az összeesküvés-elméletekkel. Többen amellett érvelnek, hogy ezek az ideák nem érdemlik meg, hogy velük konfrontálódjunk. Mások szerint, magukra hagyva ezek csak növekedni fognak és valódi hatással lesznek a demokráciára. Még ha lenne is ezekkel az elméletekkel való konfrontáció tekintetében konszenzus, akkor sem tiszta, hogy azt hogyan lehetne megtenni. Az összeseküvés-elméletek nagyon ellenállóak, és a terjesztőik mindig készen állnak a már várt ellenérvek elhárítására.[686]

Problematikus, hogy a közösségi média ezeket a teóriákat decentralizálja, gyorsítja terjedésüket, nem tradícionális szereplők által jelentett új kihívásokat állítva. Van arra mutató bizonyíték, hogy már csupán a konfrontáció az összeesküvés-elméletben hívőkkel megerősíti a hitüket, és a velük foglalkozás és vita tovább erősíti a világnézetüket. Ezért a kormányok és újságírók gyakran teljesen ingorálták őket, hogy ne kapjanak semmilyen felületet. Ez mind megváltozott a közösségi médiának

[684] BARRY, D. – MCINTIRE, M. – ROSENBERG, M.: 'Our President Wants Us Here': The Mob That Stormed the Capitol. The New York Times. (2021, January 9). https://www.nytimes.com/2021/01/09/us/capitol-rioters.html (2021.12.13.)

[685] DAVIS, A. C. – LEONNIG, C. D. – DEMIRJIAN, K. – HERMANN, P.: Backup was denied, former Capitol Police chief says. The Seattle Times. (2021, January 10). https://www.seattletimes.com/nation-world/backup-was-denied-former-capitol-police-chief-says/ (2021.12.14.)

[686] AMARASINGAM, A.: The Impact of Conspiracy Theories and How to Counter Them: Reviewing the Literature on Conspiracy Theories and Radicalization to Violence. In: RICHARDS, A. – MARGOLIN, D. – SCREMIN, N. (szerk.): Jihadist Terror: New Threats, New Responses. I.B. Tauris, London/New York, 2019. 33–34. o.

köszönhetően, ahol az ilyen elméleteket vallók könnyen találnak beszélgető és vitapartnereket.[687]

Rottweiler és Gill szerint: „A kognitív tényezők, mint például a kritikus gondolkodási készségek és a kognitív rugalmasság hatékonyan csökkenthetik az összeesküvéses hiedelmeket, és potenciálisan védőfaktorként működhetnek a szélsőséges hajlamok kialakulásában. A mód, ahogyan a tudást off-line és online fogyasztjuk, hatással van a „mélyfeldolgozási" képességeinkre: az induktív elemzésre, a kritikai gondolkodásra, a képzeletre és a reflexióra. Emellett létfontosságú, hogy a fiatalokat megfelelő digitális jártassággal (digital literacy) legyenek ellátva a hamis és „ellenismeretek" online észleléséhez. Míg a kormányzati szerveknek és a technológiai cégeknek ki kell venniük a részüket a hamis információk és az összeesküvés-elméletek elleni küzdelemben és felderítésben, a civil társadalomnak is proaktív szerepet kell játszania az összeesküvés-elméletek hazugságaival és mítoszaival való szembenézésben."[688]

A jövőbeli tanulmányoknak a további kontextuális és szituációs hatásokat kell vizsgálniuk az összeesküvés-elméletek és az erőszakos extrémizmus kapcsolatát illetően.[689]

6. Következtetések

A QAnon-nak magyar vonatkozása szerencsére nincs, de nemzetközi szinten egy nagyon veszélyes összeesküvés-elmélet, melynek a terjedését meg kell állítani. A Capitolium ostromát megelőző erőszakos online diszkussziókat hiba volt nem sokkal komolyabban venni. Az ostromára fel kellett volna készülni, ugyanis az online felületeken számos jel mutatott arra, hogy hatalmas, dühös, és erőszak elkövetésére kész tömeg lesz majd jelen. Sund, a Capitol Police chief kérelmezte, hogy készenlétbe helyezzék D.C. National Guard-ot,[690] melyet engedélyezni kellett volna.

[687] KOU, Y. – GUI, X. – CHEN, Y. – PINE, K.: Conspiracy Talk on Social Media. Proceedings of the ACM on Human-Computer Interaction, 2017. Vol. 1. No. 2. 1–21. o. Idézi: AMARASINGAM (2019): i.m. 33–34. o.

[688] ROTTWEILER, B. – GILL, P.: Conspiracy Beliefs and Violent Extremist Intentions: The Contingent Effects of Self-efficacy, Self-control and Law-related Morality. Terrorism and Political Violence, 2020. 14. o.

[689] Uo. 14. o.

[690] LEONNIG, C. D. – DAVIS, A. C. – HERMANN, P. – DEMIRJIAN, K.: Outgoing Capitol Police chief: House, Senate security officials hamstrung efforts to call in National Guard. The Washington Post (2021,

A Capitolium ostroma és más incidensek bizonyítják, hogy az összeesküvés-elméletek, főleg a QAnon komoly biztonsági kockázatot jelentenek. Ezeket a teóriákat véleményem szerint nem szabad „magukra hagyni", hanem azokat és követőiket tanulmányozni kell, és ellenük elsősorban oktatással kell küzdeni.

A radikalizálódó hírportálokon, fórumoldalakon rövid tanulmányokkal, hozzászólásokkal mintegy moderálni, a szélsőséges, befolyásoló propagandát, lejáratni, kiszorítani is lehet,[691] melyet szükséges lenne a rendvéldelmi szerveknek a veszélyes online összeesküvés-elméletek esetében is végeznie.

A titkosszolgálatoknak szemmel kell tartania a radiklalizált személyek és összeesküvés-elméletekben hívők által frekventált online platformokat, különösen biztonsági szempontból érzékeny események előtt. Komolyan kell venni az erőszakos cselekmények előtti előkészület online előjeleit, az ezeket tárgyaló, tervező posztokat, üzeneteket.

Napjainkban valós (terror)fenyegetést képviselnek az interneten terjedő összeesküvés-elméletek.

January 10). https://www.washingtonpost.com/politics/sund-riot-national-guard/2021/01/10/fc2ce7d4-5384-11eb-a817-e5e7f8a406d6_story.html (2021.12.15.)

[691] BOROSS (2014): i.m. 156. o.

XIII. AZ INCEL MOZGALOM, MINT NŐGYŰLÖLŐ TERRORFENYEGETÉS

1. Az incel fenyegetésének fokozódása

Az incel mozgalomról az utóbbi években idegen nyelven egyre több, magyar nyelven viszont alig lelhető fel szakirodalom. Fel kívánom hívni a figyelmet e veszélyes online szubkultúra által jelentett fenyegetésre.

A lazán szervezett, online működő incel közösséghez az USA-ban és Kanadában egyre több erőszakos cselekmény köthető. Nőgyűlölő ideológiájuk radikalizáló ereje tagadhatatlan. Több szerző véli úgy, hogy a közösség szélsőséges nézeteket valló tagjait terroristáknak, támadásaikat pedig terrorizmusnak kellene tekinteni.[692] Ugyan Magyarországon még szerencsére nem történt a mozgalomhoz fűződő incidens, de nem zárható ki, hogy az ideológia hazai elkövetőt is radikalizáljon. Fontos, hogy a magyar rendvédelmi szervek is ismerjék a közösséget és annak veszélyeit, hogy a potenciális jövőbeli elkövetéseket megelőzhessék.

2020. február 24-én egy torontói erotikus masszázsszalonban egy macsetés támadás során egy nő meghalt, egy másik megsérült. Az esetet terrorcselekményként kezelik, miután a rendőrség birtokába bizonyíték került arról, hogy azt az incel ideológia inspirálta. A 17 éves terhelt elleni emberölés vádját további ismeretek birtokában terrorcselekményre módosították. Közös nyilatkozatukban a Kanadai Királyi Lovasrendőrség és a Torontói Rendőrség közölte, hogy megállapították, hogy a támadást az „INCEL-ként ismert ideológiailag motivált erőszakos extrémista mozgalom inspirálta". Ez az első eset, hogy incel elkövetőt terrorizmussal vádolnak, továbbá hogy Kanada anti-terrorista törvényeivel járnak el nem szélsőséges iszlamista terhelt által elkövetett erőszakos cselekménnyel szemben.[693]

Az incel lazán szervezett online közösségének szélsőséges tagjaihoz fűződő észak-amerikai támadások – lövöldözések, késelések, gázolások – az utóbbi években fokozott aggodalomra adtak okot. A többek által első valódi incel-elkövetésnek tartott Elliot

[692] BRZUSZKIEWICZ, S.: Incel Radical Milieu and External Locus of Control. The International Centre for Counter-Terrorism – The Hague (ICCT) Evolutions in Counter-Terrorism, 2020. Vol. 22. 8. o.

[693] BELL, S. – RUSSELL, A. – MCDONALD, C.: Deadly attack at Toronto erotic spa was incel terrorism, police allege. https://globalnews.ca/news/6910670/toronto-spa-terrorism-incel/ (2021.06.18.).

Rodger 2014-es ámokfutása óta a halálos áldozatok száma az 50-et közelíti.[694] Egyre több szerző véli úgy, hogy a közösség szélsőséges tagjait terroristáknak és az általuk elkövetett támadásokat terrorizmusnak kellene tekinteni.[695] Az incel világnézet számos egyént radikalizált, ébresztett bennük nőgyűlöletet, és haragjukat és kiábrándultságukat táplálva inspirálta őket erőszakos cselekmények elkövetésére.[696]

2. A mozgalom megszületése és meghatározása

Az incel kifejezés első használatát 1993-ra teszik. Ebben az évben az interneten „Alana" néven ismert kanadai egyetemista létrehozott egy Alana's Involuntary Celibacy Project nevű weboldalt, melyet 1997-ben egy „INVCEL" rövidítést használó levelezőlistával bővített, mely aztán incelre rövidült.[697] „Alana" oldalának célja az volt, hogy az nemtől függetlenül támogató hálózata legyen magányosaknak, szüzeknek, és akiknek bármely okból hosszú ideje nem volt párkapcsolata. Ő alkotta meg az „involuntary celibates" (akaratlanul cölibátusban élők) kifejezést, így utalva e támogató csoport tagjaira. Miután magára hagyta a hálózatot, az elkezdett a gyűlölet és frusztráció virtuális közegévé válni, főleg a manoszféra heteroszexuális férfitagjai között.[698]

A Web 2.0 és a közösségi média megjelenése óta az antifeminizmus egy különösen rosszindulatú formája tűnt fel több online hálózaton és platformon. Belső konfliktusok és ellentmondások ellenére ezeket a változatos csoportosulásokat egyesíti a „redpill" filozófia (erről bővebben később), mely célja a férfiak felszabadítása a feminista téveszme alól. Az érdekcsoportok e laza konföderációja a manoszféra (manosphere).[699] A manoszféra virágzott az olyan online fórumokon, mint a 4/chan és Reddit, de miután a fő incel Reddit kommentszálat (thread-et), az r/incels-t 2017-ben tiltották, az incelek kisebb és rejtettebb fórumokra vándoroltak.[700]

---

[694] HOFFMAN, B. – WARE, J. – SHAPIRO, E.: Assessing the Threat of Incel Violence. Studies in Conflict & Terrorism, 2020. Vol. 43. No. 7. 565. o.

[695] BRZUSZKIEWICZ: i.m. 8. o.

[696] VAN BRUNT, B. – TAYLOR, C.: Understanding and Treating Incels: Case Studies, Guidance, and Treatment of Violence Risk in the Involuntary Celibate Community. Routledge, New York, 2020.

[697] BRZUSZKIEWICZ: i.m. 2. o.

[698] LABBAF, F.: United by Rage, Self-Loathing, and Male Supremacy: The Rise of the Incel Community. Invoke, 2019. Vol. 5. 17–18. o.

[699] GING, D.: Alphas, Betas, and Incels: Theorizing the Masculinities of the Manosphere. Men and Masculinities, 2019. Vol. 22. No. 4. 638. o.

[700] SPECKHARD, A. – ELLENBERG, M. – MORTON, J. – ASH, A.: Involuntary Celibates' Experiences of and

Egy 2001-es meghatározás szerint incel egy olyan személy „… aki szexuális kapcsolatot kíván létesíteni, de legalább hat hónapig képtelen arra hajlandó partnert találni ….”[701] Egy 2020-as definíció szerint az incelek: „… olyan fiatal férfiak agresszív, gyűlölködő és gyorsan terjeszkedő online közössége, akik azért frusztráltak, amiért képtelenek szexuális partnert találni.”[702] Az incelek heteroszexuális férfiak, akik a nőket és a társadalmat okolják a romantikus sikertelenségük miatt. Ők a legerőszakosabb részhalmaza a manoszférának, amelybe a Pick up Artists, Men Going Their Own Way és Men’s Rights Activists is tartoznak. Az inceleket mély pesszimizmus, és a nők irányában érzett erős sértettség jellemzi. Az ideológiájuk gyökere az a hit, hogy a nőknek túl nagy a hatalma a szexualitás és a romantika terén, akik az ő életüket tönkreteszik azzal, hogy őket visszautasítják.[703] A női incelek a femcelek, akik létezését a legtöbb incel nem ismeri el. Ők inkább magukat okolják a sikertelenségeik miatt.[704]

3. Az incel ideológia

A főleg fiatal férfiakból álló mozgalom az interneten született. Magukra incelként hivatkoznak, ami szóösszerántás az „involuntarily celibate-ből”. Úgy hiszik, hogy a megjelenésük a nők emancipációjával és a feminizmussal párosítva akadályozza őket abban, hogy nőkkel fizikai kapcsolatot alakítsanak ki. Ebből a sérelemből fejlesztettek ki egy antifeminista, nőgyűlölő, nihilista, önostorozó ideológiát.[705] Online közösségekben működnek. Kultúrájuk több eleme nőgyűlölő és előnyben részesíti az erőszakot. Számos

---

Grievance Over Sexual Exclusion and the Potential Threat of Violence Among Those Active in an Online Incel Forum. https://www.icsve.org/involuntary-celibates-experiences-of-and-grievance-over-sexual-exclusion-and-the-potential-threat-of-violence-among-those-active-in-an-online-incel-forum/ (2021.06.18.)

[701] DONNELLY, D. – BURGESS, E. – ANDERSON, S. – DAVIS, R. – DILLARD, J.: Involuntary Celibacy: A Life Course Analysis. The Journal of Sex Research, 2001. Vol. 38. No. 2. 159. o.

[702] HOFFMAN, B. – WARE, J.: Incels: America’s Newest Domestic Terrorism Threat. Lawfare. (2020, January 12). https://www.lawfareblog.com/incels-americas-newest-domestic-terrorism-threat (2021.06.18.)

[703] Incels (Involuntary celibates). https://www.adl.org/resources/backgrounders/incels-involuntary-celibates (2021.06.18.)

[704] KOHN, I.: Inside the World of 'Femcels'. https://melmagazine.com/en-us/story/femcels-vs-incels-meaning-reddit-discord (2021.06.18.)

[705] HASTINGS, Z. – JONES, D. – STOLTE, L.: Involuntary Celibates: Background for Practitioners. Organization for the Prevention of Violence, Edmonton, 2020. 2. o.

erőszakos incidens köthető hozzájuk, ami azt sugallja, hogy közösségeik hasonlíthatnak más ideológiailag motivált szélsőséges csoportokhoz.[706] Magukat azáltal határozzák meg, hogy képtelenek testi kapcsolathoz jutni, ami szerintük genetikai tényezőknek, a nőkben rejlő evolúciósan meghatározott jellemvonásoknak és méltánytalan társadalmi struktúrák kombinációjának köszönhető. Elsősorban a testi kapcsolathoz való hozzáférés foglalkoztatja őket. Szerintük a genetikai tényezők által befolyásolt megjelenésük és/vagy kognitív és szociális képességeik teszik őket a nők számára taszítóvá. Úgy gondolják, a nők a férfiak egy vonzó kisebbségét választják szexuális kapcsolatra, és a férfiak 20%-a monopolizálja a nők 80%-át testi kapcsolatra. Ez a „80/20 szabály*"*. Az incelek szerint a társadalom többsége figyelmen kívül hagyja, vagy szándékosan visszatartja a genetikai tényezőkről és az olyan evolúciós jegyekről szóló információkat, melyek kihatnak a szexuális kapcsolatokhoz való hozzáférésének a képességre. Aki nem fogadja el ezt a hitrendszert, az „bluepilled"személy, aki a „kék tablettát vette be". A többség hiedelmei a szexről, az intimitásról és a kapcsolatokról „bluepilled" nézetek, mert azok szerint a romantikus és szexuális kapcsolatok kialakításához a személyiség és az érzelmi összeköttetés ugyanolyan fontos, mint a fizikai vonzerő. Az incelek ezt elutasítják. Ők a „blackpill-t", „a fekete tablettát" fogadják el, mely szerint a vonzóság mérhető, és az diktálja a sikert a szexuális és romantikus kapcsolatok terén. Úgy hiszik, ezt a többségi média ignorálja, és a „genetikai alsóbbrendűségük" miatt a társadalom jobban szeretné, ha természetes szelekció útján kikerülnének a génállományból. Sokuk úgy tartja, hogy az incel és a „blackpill kutatás" elnyomása vagy ignorálása összeesküvés az ő kiirtásukra.[707]

Az incels.me weboldal társalgásainak kvalitatív elemzése során Baele et al. arra jutottak, hogy az incel világnézet szerkezete egy kizárólag a külső megjelenésen alapuló merev hármas társadalmi hierarchia. A csúcson helyezkednek el a kisebbségben lévő „alfák" („alpha"), férfi tagja a „Chads", a nők a „Stacys". Alattuk és többségben vannak az átlagos megjelenésű „béták" („betas"), ők a „normies". A hierarchia legalján van a rossz megjelenésű, kizárólag férfi kisebbség, az „incelek". Ők az „akaratlan cölibátus" áldozatai.[708]

[706] O'MALLEY, R. L. – HOLT, K. – HOLT, T. J.: An Exploration of the Involuntary Celibate (Incel) Subculture Online. Journal of Interpersonal Violence, 2020. 1. o.

[707] Incels: A guide to symbols and terminology. Moonshot, 2020. 1–19. o. http://moonshotcve.com/incels-symbols-and-terminology/ (2021.06.19.)

[708] BAELE, S. J. – BRACE, L. – COAN, T. G.: From "Incel" to "Saint": Analyzing the violent worldview behind the 2018 Toronto attack. Terrorism and Political Violence, 2019. 8. o.

Az incelek szókincse sajátos, melynek teljes ismertetése szétfeszítené a dolgozat kereteit, ezért csupán példákra szorítkozom.
„Bluepill”: Utalás az 1999-es Mátrix filmre. A „pill-ek” (tabletták) hasonlatát a manoszféra és a szélsőjobb kedveli. Az incelek szerint egy „bluepilled” férfi ismerkedési módszerei hagyományosak, nincs tisztában a valós társadalommal.
„Redpill”: Aki lenyeli a piros tablettát, annak felnyílik a szeme a valós világra, ahol a nők általánosságban jobb helyzetben vannak, elnyomásuk mítosz, és valójában hagyományos nemi szerepekre vágynak. Ha egy férfi ismeri ezeket az igazságokat, a kedvére manipulálhatja a nőket, hogy szexhez és hatalomhoz juthasson.
A „blackpill” szerint a rendszer nem játszható ki. A visszataszító, „genetikailag alsóbbrendű” férfiak sosem jutnak szexhez vagy romantikus kapcsolathoz a jelenlegi miliőben. Nincs az a személyiség, karizma, vagy „gymmaxxing” (edzőtermi edzés) ami változtat sorsukon.
„Going ER”: tömeggyilkosságot elkövetni, Elliot Rodger után elnevezve.
„Jihadpill”: Annak elfogadása, hogy az ember csak úgy juthat kapcsolathoz vagy szexhez, ha dzsihadista lesz. (Elméletileg a „jihadpill” elfogadásával nem kizárt az incel személy dzsihadistává válása, így létezhet átjárás az incel és a dzsihád között.)
„Jihadmaxxing”: Szexuális vagy romantikus kapcsolatokhoz jutás dzsihadistává válás útján.
„Moneymaxx”: Pénz keresése a „szexuális piaci érték” növelésének reményével.
Néhány incel típus:
„Baldcel”: Aki nem jut szexuális kapcsolathoz, mert kopasz.
„Fakecel”: Aki csak úgy tesz, mintha incel lenne.
„Truecel”: Valódi incel.
„Poorcel”: Aki azért incel, mert szegény.
„Ricecel”: Aki incel, mert kelet- vagy délkelet-ázsiai felmenői vannak.
„Wristcel”: aki incel, mert a csuklói vékonyak.[709]

4. Az incel elme

Az incel közösséghez tartozók az általános népességnél gyakrabban számolnak be szorongásról, depresszióról, más hangulatzavarokról, viszont csoporton belüli normáik vannak a pszichoszociális segítség igénybevétele ellen. Ezen akadályok leküzdése és a

[709] Incels: A guide to symbols and terminology. Moonshot, 2020. 1–19. o. http://moonshotcve.com/incels-symbols-and-terminology/ (2021.06.19.)

segítség hozzáférhetőbbé tétele kulcsfontosságú lenne a további erőszakos cselekmények megelőzésében. Ugyan a mozgalom erőszakos része fenyegetést jelent, fontos leszögezni, hogy az incelek többsége nem erőszakos, és esetükben az átlagnál magasabb lehet az önkárosítás veszélye.[710]

2020. december 7. és 2021. január 2 között Google Forms kérdőívvel végeztek kutatást, melyet 272 incel töltött ki. Az eredmények azt mutatják, hogy sérelmeik és ideológiájuk közös, de messze nem mindegyikük lenne hajlandó vagy kíván erőszakos cselekményt elkövetni. A válaszolók közül a legtöbben depressziósnak, magányosnak tűnnek, és nem erőszakosak. A fórumok miatt úgy érzik, tartozhatnak valahova, ahol megértik őket és elengedhetik magukat, ugyanakkor azok fokozzák a depressziójukat, öngyilkos hajlamukat és nőgyűlöletüket. A fórumok nyújthatnának pozitívabb támogatást, ahelyett, hogy ráerőltetnék a „blackpill" ideológiát egy csoportra, akiket a sérelmeik mérgessé, depresszióssá, öngyilkos hajlamúvá és reményvesztetté teszik. Nem ismert, hogy ezek a tünetek hogy nyilvánulnának meg az incel közösség hiányában. A kitöltők 71,3%-a a helyzetét állandónak látja, 97,1% számol be pszichológiai problémákról, 44,9% az autizmus jeleiről, de a legtöbb nem gondolja úgy, hogy a pszichológiai segítség válasz lenne számára. Megfontolandóak lehetnek a fórumokon pozitív és humanizáló formában történő kreatív mentális egészség és pszichológiai intervenciók, melyek tervezésébe inceleket vagy volt inceleket is fontos lenne bevonni. Az ilyen erőfeszítéseknek az önkárosítást és a mások elleni erőszakos cselekmények kockázatának csökkentését kellene megcélozniuk, és alternatív narratívát kellene kínálniuk a „blackpill" helyett, amiben a kitöltők 94,9%-a hitt.[711]

Váradi 2020-ban az egyik legnagyobb jelenlegi incel közösség, az incels.co-n szereplő leggyakoribb és a legtöbb posztolásra használt profilkép kvalitatív elemzését végezte el. Amellett érvel, hogy habár az incel közösségek nagyrészt békésnek mondják magukat és elhatárolódnak a média-reprezentációjuktól, a közösség egy jelentős része agressziót sugalló képekkel reprezentálja önmagát a weboldalakon.[712]

5. Komolyabb incel-esetek és összefüggéseik

Az incel elkövetők általában olyan célpontokat részesítenek előnyben, ahol nők gyűlnek

[710] HASTINGS – JONES – STOLTE: i.m. 2. o.

[711] SPECKHARD – ELLENBERG – MORTON – ASH: i.m.

[712] VÁRADI B.: Önreprezentáció az inceloszférában? https://eltedszk.org/2020/08/28/onreprezentacio-az-inceloszferaban/ (2021.06.19.)

össze, mint jóga stúdiók, női fitnesz órák és erotikus masszázs szalonok. Ha a támadások üteme fokozódik, ezeken a helyeken megfontolandó a biztonság növelése. Nyilvános helyeken az incel támadók hajlamosak nőket vagy párokat célba venni. Más erőszakos extrémistákhoz hasonlóan előnyben részesítik az alacsony technológia igényű (low tech), kezdetleges és az olcsóbb támadási módokat: lövöldözést, késelést, gázolást.[713]

Az incelek hősei a következő elkövetők: Elliot Rodger, Marc Lépine, Alek Minassian, Scott Beierle, Chris Harper-Mercer. Az incels.co-n szavaztak is arról, ki a kedvenc „Incel Szentjük", amit Rodger nyert.

1989-ben Marc Lépine Montreal-ban elkövetett lövöldözése során 14 nőt ölt meg és 10-et megsebesített. Az incelek egy kezdeti incel elkövetőnek és szentnek nevezik. Kifejezetten nőket vett célba, férfiakat nem ölt. Ezt belső viták során gyakran állítják szembe Rodger-rel, aki férfiakat is ölt. Támadásának napját, december 6-át az incelek ünneplik is.[714]

2014. május 23-án a kaliforniai Isla Vista-ban a 22 éves Elliot Rodger 141 oldalas önéletrajzi manifesztumot tett közzé online „My Twisted World: The Story of Elliot Rodger" címmel, ezután összesen 134 szúrással leszúrta két szobatársát és egy barátját. Ámokfutásba kezdett, mely során 6 ember meghalt, 14 megsérült, végül öngyilkos lett. Sokak szerint ő volt az első tömeggyilkos, aki az incel közösséghez köthető. Az incel fórumokon sokszor úgy hivatkoznak rá, hogy „Szent Elliot", vagy „A Legfőbb Úriember"(„The Supreme Gentleman"), és az ámokfutás évfordulóját „Szent Elliot Napként" ünneplik.[715] Manifesztumából kiolvasható, hogy úgy érezte, a nők tartoznak neki, és leírta, hogy meg fogja „büntetni az összes nőt a bűnért, hogy megvonta tőlem a szexet."[716]

2015-ben Chris Harper-Mercer lövöldözött a Umpqua Community College (Közösségi Főiskola) területén, az oregoni Roseberg közelében. Támadása során 10 ember meghalt, 8 megsérült, önmagával is végzett. Manifesztumában leírta, hogy nem voltak barátai, se állása, vagy barátnője, és szűz volt. Rodger-re „elitként" hivatkozott. Kifejezetten nem köteleződött el incel fórumok mellett, de a támadását megelőző estén az incelek körében

[713] HASTINGS – JONES – STOLTE: i.m. 2. o.

[714] Incels: A guide to symbols and terminology. Moonshot, 2020. 1–19. o. http://moonshotcve.com/incels-symbols-and-terminology/ (2021.06.19.)

[715] WITT, T.: 'If i cannot have it, i will do everything i can to destroy it.' the canonization of Elliot Rodger: 'Incel' masculinities, secular sainthood, and justifications of ideological violence. Journal for the Study of Race, Nation and Culture, 2020. Vol. 26. No. 5. 675. o.

[716] VITO, C. – ADMIRE, A. – HUGHES, E.: Masculinity, aggrieved entitlement, and violence: considering the Isla Vista mass shooting. International Journal for Masculinity Studies, 2018. Vol. 13. No. 2. 97-98. o.

népszerű 4chan fórum /r9k/ board-jára (felületére) írta, hogy: „Néhányan rendben vagytok. Ne menjetek holnap iskolába, ha északnyugaton vagytok.” A közösség alulértékelt incelnek tartja.

Scott Beierle követte el a 2018-as tallahassee-i lövöldözést, mely során egy jóga stúdióban hat nőt lőtt meg, közülük kettő meghalt. Megtámadott egy férfit is, azután magával is végzett. A YouTube csatornájára rasszista és nőgyűlölő videókat töltött fel, az egyikben Rodger érzéseit a sajátjával vetette össze. Nem tartozott a közösségbe, nincs nyoma, hogy aktív lett volna fórumokon, vagy chat szobákban, de a támadását erőszakos nőgyűlölet inspirálta, és videóiban Rodger-re hivatkozott. Az incelek „St Yogacel” néven vették fel a kánonjukba.[717]

2018. április 23-án Torontóban a 25 éves Alek Minassian egy kölcsönzött kisteherautóval hajtott a járókelők közé. 10 ember meghalt, 16 megsérült, a halálos áldozatok közül 8 nő volt. Minassian az elkövetés előtt a Facebookon az „incel forradalom” eljövetelét kiáltotta ki. A kihallgatásán azt közölte, tettével tömegeket kívánt inspirálni. Aktív tagja volt az incel szubkultúrának. A mozgalom „alapító ősatyjának” tartotta Rodger-t, kihallgatása során azt állította, kommunikált is korábban vele, de ez erősen megkérdőjelezhető.[718]

További incel elkövetők a teljesség igénye nélkül:

2020. április 21., Covina, Kalifornia: Carl Bennington-t letartóztatták, miután nőket és tizenéves lányokat fenyegetett meg. Incel ideológiát hirdetett online, és Rodger-re áldozatként utalt.

2020. május 12., Queens, New York: Joseph Miner-t letartóztatták, amikor szövetségi fedett nyomozóktól kísérelt meg illegális fegyvereket vásárolni. Egy zsidók és feketék elleni faji háborúhoz akart incel osztagot szervezni.

2020. május 20., Glendale, Arizona: A magát incelnek valló Armando Hernandez Jr. párokat megcélozva nyitott tüzet a Westgate Entertainment District-ben. Három ember megsérült. A támadásáról készült felvételt elküldte egy nőnek, remélve, hogy ezzel imponálhat neki.

2020. június 3., Richlands, Virginia: Cole Carini véletlenül felrobbantott egy házi készítésű robbanószerkezetet, megsebesítve önmagát. A nyomozók bombagyártáshoz szükséges anyagokat és incel ideológiát támogató jegyzeteket találtak az otthonában,

[717] Incels: A guide to symbols and terminology. Moonshot, 2020. 1–19. o. http://moonshotcve.com/incels-symbols-and-terminology/ (2021.06.19.)

[718] COTTEE, S.: Incel (E)motives: Resentment, Shame and Revenge. Studies in Conflict & Terrorism, 2021. Vol. 44. No. 2. 93. o.

melyekben az állt, hogy erőszakos cselekményre készült „dögös pomponlányok” ellen, hogy „egy nyilatkozatot tegyen” mint Rodger.
2020. szeptember, New York: az FBI letartóztatta a magát incelnek valló és Rodger-t csodáló David Kaufman-t, aki egy Long island-i párt egy éven át fenyegetett halálosan és szexuális erőszakkal.[719]

6. Az incel mint terrorfenyegetés

Ugyan a két fogalom nem ellentétes egymással, de egyetértek azzal az állásponttal, hogy a jelen esetben tárgyalt elkövetők tekintetében a magányos farkas (lone wolf) helyett pontosabb lenne a nőgyűlölő terrorizmus (misogynist terrorism) kifejezés használata.[720] Más szerzők is érvelnek amellett, hogy az incel erőszak nőgyűlölő terrorizmus.[721] DiBranco növekvő fenyegetésnek tartja a férfi felsőbbrendűséget hirdető terrorizmust (male supremacist terrorism).[722]
A Texas Fusion Center Intelligence & Counterterrorism Division Texas Department of Public Safety három hazai (domestic) terrorizmus típust különböztet meg: faji motivációjú, kormány-ellenes, és egyedi üggyel foglalkozó (single issue). Ugyan nem új mozgalom, de az incelek egy előretörő hazai terrorfenyegetés. Az inceleket sok rendvédelmi szerv korábban bűnözési fenyegetésként értelmezte, de arra ma már mint növekvő hazai terrorfenyegetésre tekint. Ez az utóbbi időkben nemzeti, nemzetközi szinten és Texasban elkövetett incel-támadások ideológiai természetének köszönhető. A nők visszautasításából fakadó személyes sérelem az incel forradalom iránti elköteleződéshez vezethet, és ahhoz hogy megkísérelhetik annak céljait elérni. Az incel fenyegetése hamarosan elérheti más hazai terrorizmus típusok halálosságának szintjét, akár túl meg is haladhatja azokat.[723] Clarke szerint számos ideológia hathat a

[719] Incels (Involuntary celibates). https://www.adl.org/resources/backgrounders/incels-involuntary-celibates (2021.06.18.)

[720] VALENTI, J.: When Misogynists Become Terrorists. The New York Times. (2018, April 26.) https://www.nytimes.com/2018/04/26/opinion/when-misogynists-become-terrorists.html (2021.06.19.)

[721] SQUIRREL, T.: A definitive guide to Incels part one: Incelocalypse. https://www.timsquirrell.com/blog/2018/5/30/a-definitive-guide-to-incels-part-one-incelocalypse (2021.06.19.)

[722] DIBRANCO, A.: Male Supremacist Terrorism as a Rising Threat. https://icct.nl/publication/male-supremacist-terrorism-as-a-rising-threat/ (2021.06.19.)

[723] Texas Domestic Terrorism Threat Assessment. Texas Fusion Center Intelligence & Counterterrorism Division Texas Department of Public Safety, Texas, 2020. 3. o.

terrorizmussal kapcsolatos 2021-es tendenciákra, köztük a gazdasággal és a környezettel kapcsolatos hagyományos baloldali sérelmek, összeesküvés-elméletek, mint a QAnon, és oltás- vagy 5G ellenes kampányok, és fenyegetést jelenthet az extrém nőgyűlölet és az incel mozgalom is.[724]

Ahogy arról már korábban szó esett, Szalai és Wagner a terrorizmus fogalmának inflálódására figyelmeztet, ami egy folyamat, mely során a nyugati közvéleményben a terrorizmus kifejezés jelentése egyre tágul. Egyre több eseményt jellemeznek így, ami hosszú távon negatívan hathat a terrorizmus elleni küzdelem hatékonyágára.[725]

Egyetértek azzal, hogy a terrorizmus kifejezéssel óvatosan kell bánni, az csak megfontoltan használandó, nem szabad „elkoptatni", de magam is azt az álláspontot fogadom el, hogy az incel elkövetők esetében indokolt a kifejezés használata.

Vitatható lehet, hogy milyen típusú terrorizmushoz sorolható az incelek terrorizmusa. Szélsőjobboldali, esetleg alt-jobb, single issue, vagy szimplán nőgyűlölő terrorizmus, mit új kategória?

7. A pandémia hatása a közösségre

Vu az incel szubkultúra két legaktívabb angol nyelvű fórumainak, az incels.co and incels.net oldalak chat-jeiben több mint 5 millió posztot elemezve, a zárlatok hatásait vizsgálta az incelek társalgásaira. A zárlat alatt a posztok és kommentszálak száma jelentősen nőtt, de a posztoló tagok száma enyhén csökkent. Megfigyelhető a rosszindulatú és erőszakos társalgások jelentős fokozódása is, kifejezetten azoké, melyek a pandémia következményeként a társadalomban esetlegesen bekövetkező előnyös (ahogyan ők látják) változásokról, és abban az incelek betöltött helyéről szólnak. A világjárvány kétségtelenül felerősítette az incel szubkultúrát. A zárlatok miatt az emberek több időt töltenek online, a pandémia táplálja az önsajnálatot, az szélsőséges fantáziákat és a vonzó férfiakkal és nőkkel szembeni ellenségességet. Úgy tűnik, hogy a már meglévő felhasználók tevékenysége fokozódott, nem pedig az új, alkalmi hozzászólóké. Jelentős növekedés látszik a gyilkos fantáziák terén. Nőtt a száma az

https://www.dps.texas.gov/sites/default/files/documents/director_staff/media_and_communications/2020/txterrorthreatassessment.pdf (2021.06.19.)

[724] CLARKE, C. P.: Trends in Terrorism: What's on the Horizon in 2021? Foreign Policy Research Institute. (2021, January 5) https://www.fpri.org/article/2021/01/trends-in-terrorism-whats-on-the-horizon-in-2021/ (2021.06.19.)

[725] SZALAI – WAGNER: i.m. 3. o.

olyan ölésről fantáziáló posztoknak, amelyek a „Chad-eket” és „Stacy-ket” említik, 2020 áprilisában számuk csúcsot ér el, aztán gyorsan lecsökken. Sokkal több ilyen poszt szól férfiakról, mint nőkről, a legnagyobb különbség 2020 áprilisában látszott. A koronavírust „Corona-chan-nak”, azaz „koronácskának” (a chan japánul becéző megszólítás) nevezik, és remélik, hogy megtizedeli a vonzó férfiakat, és így több esélyük lesz az ismerkedés terén.[726]

8. Az incel elleni fellépés nehézségei és lehetséges irányai

Az incelek elleni fellépést nehezíti, hogy a szélsőjobboldali közösségekhez és a dzsihadistákhoz hasonlóan ők is fokozottabban használják a dark webet a gyülekezés, társalgás és új követők radikalizálása céljából.

Az incelek tisztában vannak a média és a bűnüldöző szervek figyelmével, azt sokszor élvezik is. Hogy elkerüljék fórumaik bezárását, többen inkább cenzúrázták önmagukat és egymást. Emiatt több erőszakos incel diszkrétebb fórumokra váltott, például videojátékos témájú rejtett chat szobákba, vagy a dark webre, és olyan oldalakra is, mint a Gab, ami egy nyíltan szélsőjobboldali közösségi média oldal.

Azonban vannak kihasználandó fellépési lehetőségek. Az incel közösség nem egységes, az nagyon változatos, nincs meg benne a más erőszakos radikális mozgalmakra jellemző kohézió. Miközben a probléma tekintetében egyetértenek, a megoldásban nem. Néhányuk a céljaik eléréséhez az erőszakot elengedhetetlennek tartják, mások nem. Sok ezren aktívak ezeken az internetes fórumokon, továbbá e felületek természete eredendően civakodó, így nem meglepő, hogy a közösség nem ért egyet az önmeghatározást és a teleológiai problémákat illetően.

Az incelek büszkék a “shitposting-jukra” (szándékosan provokáló, tréfás-gúnyos bejegyzés írása), ami miatt a tényleges fenyegetés mértékét nehéz megállapítani, és könnyű túlbecsülni. Szarkazmus és szatíra jellemzi a manoszféra online kultúráját, aminek az incel is részhalmaza, ennek rétegein szakavatatlan szemek nehezen látnak át. Ezért is nehéz az incel ideológiát elemezni, és a tényleges radikalizációt felmérni. Megbotránkoztató posztokat azért is írnak, mert ezek a kapják a legtöbb figyelmet. Sok incel szerint csak a fórumokon engedhetik ki a feszültséget és oszthatják meg a legsötétebb gondolataikat, emiatt nehéz megállapítani, hogy melyik bejegyzések

[726] VU, A. V.: Cambridge Cybercrime Centre COVID Briefing Paper # 5: The Pandemic as Incels see it. University of Cambridge, Cambridge, 2020.

jelentenek fenyegetést, és melyek csupán szatíra, vagy virtuskodás és nem közvetlen erőszak előjelei.

Jelentősen gyengítheti a mozgalom szélsőséges áramlatait a közösségi média oldalak növekvő felelősségvállalása az online radikális anyagok tekintetében. Egyes fórumok viszonylag jól ellenőrzik magukat, de az eklektikusabb oldalakon, köztük a 4chan-on és a 8kun-on található bejegyzések továbbra is nők és kisebbségek elleni erőszakot szorgalmaznak, valamint helyet biztosítanak az erőszakos cselekmények előtt posztolt manifesztumok közzétételére.[727]

Az USA-ban a szigorú szólásszabadság-törvények nehezítik az online extrémizmus elleni jogszabályok elfogadását, de újságírók, tudósok, szakemberek és politikusok egyaránt alternatív intézkedéseket javasolnak az extrémista mozgalmak online térnyerése ellen. Ware et al. szerint szélesebb körű párbeszédre van szükség az extrémizmus és az erőszakos ideológiák visszaszorításáról az interneten, bevonva a tech cégeket, a terrorizmus és a radikalizálódás szakértőit, kormányokat, a fiatal közösségi média használókat, még volt extrémistákat is. Az incel mozgalom kitartó vibrálása arra enged következtetni, hogy a szerepe változatlan a radikalizálódás táplálásában. Egy ilyen radikalizálódási tényező szerepet játszhat más extrémista mozgalmak fellendítésében – például a németországi halle-i zsinagóga-lövöldöző, Stephan Balliet az idegengyűlölet mellett hasonló sérelmekkel is magyarázta a radikalizálódását. Több kutatásra van szükség a témát illetően, hogy megtalálhassuk az incel online terjedésének visszaszorításának módjait.[728]

Bőven van ok azt feltételezni, hogy az erőszakos incelek továbbra is komoly fenyegetést jelentenek. Ezt bűnüldöző szervek által közzétett figyelmeztetések is jelzik, de például 2019 szeptemberében az Amerikai Egyesült Államok Hadserege is figyelmeztetett, hogy a Joker című film vetítésein potenciálisan erőszak várható, miután „nyugtalanító és nagyon specifikus társalgásra" figyeltek fel a dark web incel chat-jeiben, de a Coloradoban 2012-ben egy Batman film (A sötét lovag – Felemelkedés) premierjén elkövetett lövöldözés is jelentős körülmény ebben.

A szalafista dzsihádisták elleni erőfeszítések politikai előnyben részesítése is bonyolítja az incelek elleni egyesült államokbeli fellépést: alkotmányosan nagyobb kihívás és

[727] WARE, J. – HOFFMAN, B. – SHAPIRO, E.: Remembering Toronto: Two Years Later, Incel Terrorism Threat Lingers. Global Network on Extremism & Technology. (2020, May 6). https://gnet-research.org/2020/05/06/remembering-toronto-two-years-later-incel-terrorism-threat-lingers/ (2021.06.21.)

[728] Uo.

politikailag kevésbé kifizetődő szembeszállni egy saját hazai választópolgároktól eredő legális extrémizmussal, mint egy külföldi eredetűvel. Továbbá a szélsőjobboldali és szélsőbaloldali radikálisokhoz hasonlóan az incelek sem felelnek meg a terrorizmus hagyományos modelljének. Az internet, a közösségi média és más 21. századi kommunikációs felületek a terrorizmust egyre inkább magányos vállalkozássá teszik, melyet elsősorban formális szervezeteken kívüli magányos szereplők követnek el. Az erőszakos incelek ezért kihívást jelentenek a klasszikus terrorizmusellenes politikáknak és stratégiáknak.[729]

Kulcsfontosságú a megelőzés: „Az incel mozgalom sérelmeivel és erőszakos tendenciáival kapcsolatos fokozott tudatosság ellenállóbbá teheti a társadalmat annak narratíváival és extrém nézeteivel szemben. A radikalizálódás ellen segíthet a család, barátok, egészségügyi szakemberek, oktatási intézmények, ifjúsági tanácsadók, polgári és egyházi intézmények. Az izoláció és a technológia által fokozott frusztrációt és elidegenedést az alternatív utak ellensúlyozhatnák az ellenálló képesség, a szocializáció, az elfogadás és az empátia fejlesztésével.

A rendvédelmi szervek az incel erőszak ellen a következő módokon is küzdhetnek: a potenciálisan bekövetkező erőszakos cselekmények jellegzetességeinek felismerésével (például: erőszakos cselekmény azonnali elkövetésére való felhívás, azok tervezése etc.); az online vagy offline fenyegető nyelvezettel kapcsolatos bejelentések kivizsgálásával; informátorok és fedett nyomozók használatával.

Hasznos lehet a már támadásokat tapasztalt helyszínek biztonságának növelése.

Az online platformok közösségi média cégek (Facebook, Instagram, Twitter etc.), és más technológiai cégek (például domain regisztrátorok, web hoszting és más web infrastruktúra cégek), online fizetési szolgáltatók, kutatók, hatóságok és a nyilvánosság általi megfigyelése hatékony lehet a támadók mobilizálása ellen."[730] Jövőbeli megelőzési mód lesz a mesterséges intelligencia általi prediktív elemzés is.[731]

[729] HOFFMAN, B. – WARE, J. – SHAPIRO, E.: Assessing the Threat of Incel Violence. Studies in Conflict & Terrorism, 2020. Vol. 43. No. 7. 576. o.

[730] ALEXANDER, D. C. – LESNIEWSKI, D.: The violent fringe of the incel movement. Police 1. (2019, September 19). https://www.police1.com/mass-casualty/articles/the-violent-fringe-of-the-incel-movement-M2E5rlB5BYTDesoL/ (2021.06.21.)

[731] SZABÓ, A. L.: Criminal Policy Approach to Lone Offenders and a Possible Model for their Identification. Nemzetbiztonsági Szemle, 2020. Vol. 8. No. 2. 76. o.

9. Következtetések

„Az incel elkövetők megtalálása és megállítása érdekében a rendvédelmi szerveknek, titkosszolgálatoknak, magánbiztonságnak, oktatóknak, egészségügyi szakembereknek és a kapcsolódó diszciplinák szereplőinek ismernie kell az incel ideológiát és szókincset, a közösségben való részvétel jeleit, és az incel gondolkodáshoz fűződő ön- és mások elleni erőszak kockázatát."[732] Ugyan az incelek többsége nem követ el erőszakos cselekményt, nem feltétlenül veszélyes a társadalomra, főleg nem terrorista, de az incel szubkultúra radikalizáló ereje a korábbi halálos áldozatokat követelő elkövetések tükrében tagadhatatlan. Mivel a közösség az arra fogékony személyeket hatékonyan képes radikalizálni, és az egyes támadásainak halálos áldozatainak száma magas, ezért az incel mozgalom szélsőséges tagjainak fenyegetését véleményem szerint hasonlóan veszélyesnek kellene tekinteni, mint a szalafita dzsihádistákét. Szerencsére Magyarországon még nem történt a közösséghez köthető erőszakos cselekmény, de nem zárható ki, hogy az ideológia hazai elkövetést is inspiráljon. Megfontolandó lehet a témát illetően a társadalom, főleg a fiatalok informálását megcélzó kampányok indítása. A potenciális támadások megelőzése szempontjából az incel jelenség rendvédelmi szervek általi naprakész ismerete, esetleges magyar fejlődésének, vonatkozásainak nyomon követése elengedhetetlen fontosságú.

[732] Webinar: Finding the Next Incel Killer. https://www.hstoday.us/subject-matter-areas/counterterrorism/webinar-finding-the-next-incel-killer/ (2021.06.21.)

XIV. A 3D NYOMTATOTT LŐFEGYVEREK, ONLINE ELÉRHETŐ TERVRAJZAIK ÉS EZEK TERRORISTA CÉLOKRA VALÓ FELHASZNÁLHATÓSÁGA

1. A probléma felvetése

Az FGC-9 gépkarabély példájával sejttetem a probléma horderejét: a fegyver digitális tervrajzával, már egy 250 USD (kb. 78.000 HUF) értékű 3D nyomtatóval, a fegyvercső elkészítéséhez szükséges eszközökre 100 USD (kb. 31.000 HUF) ráfordításával már egyesével 100 USD összegből gyártható otthon a fegyver. Egy műszakilag jártasabb ember kevesebb, mint egy hét alatt, egy gyakorlatlan pedig az interneten könnyen fellelhető részletes utasítások segítségével pár hét alatt elkészítheti a fegyvert, mely több ezer lövés leadására képes, mielőtt tönkremenne. Az FGC-9 nagy része 3D nyomtatott, a többi alkatrésze pedig beszerezhető bármely barkácsboltban, így az a hatóságok előtt ismeretlenül legyártható.[733] Az FGC-9 példája jól illusztrálja többek között azt, hogy mennyire olcsóvá és megközelíthetővé vált a 3D nyomtatás technológiája, hogy milyen nagy utat tett meg az otthoni fegyvergyártás, továbbá felveti azt is, hogy mennyire égető szükség van a témát illető hatékony, alapos és naprakész szabályozásra, megfelelő óvintézkedésekre. A fegyvert egy potenciális terrorista is könnyen elkészítheti otthon, a hatóságok tudomása nélkül.

A koronavírus pandémia hatására a lőfegyver és lőszer eladások drámai növekedést mutattak az USA-ban,[734] 2021. januárban több mint 2 millió lőfegyvert adtak el, mely az előző évhez képest 80%-os növekedés.[735] A lőfegyverek pánikvásárlása Magyarországon is megfigyelhető volt.[736] A járvány megzavarta az ellátási vonalakat, így a fegyvertulajdonosok is jobban saját kezükbe veszik a gyártást.[737]

---

[733] SCHNEIDER, A.: 3D-Printed Guns Are Getting More Capable and Accessible. Slate. (2021, February 16). https://slate.com/technology/2021/02/3d-printed-semi-automatic-rifle-fgc-9.html (2021.08.11.)

[734] CILLIZZA, C.: How coronavirus has sent gun and ammo sales through the roof. CNN. (2020, March 25). https://edition.cnn.com/2020/03/25/politics/guns-ammo-coronavirus/index.html (2021.08.11.)

[735] DENHAM, H. – TRAN, A. B.: Fearing violence and political uncertainty, Americans are buying millions more firearms. The Washington Post. (2021, February 4). https://www.washingtonpost.com/business/2021/02/03/gun-sales-january-background-checks/ (2021.08.11.)

[736] Coronavirus triggers panic-buying of guns in Hungary. Al Jazeera. (2020, March 24).

Az interneten meglepően könnyű lépésről lépésre lebontott útmutatókat találni 3D nyomtatott lőfegyverek készítéséről.[738] Clarke úgy véli, 2021-ben erőszakos nem állami szereplők továbbra is egyre jobban támaszkodhatnak fejlődő technológiákra, ideértve a 3D nyomtatást is. Terroristák is további érdeklődést mutathatnak a 3D nyomtatott lőfegyverek iránt, ahogy azt a már tárgyalt 2019-es halle-i támadás is illusztrálhatja. A jobboldali extrémisták kifejezett érdeklődést mutatnak a 3D nyomtatott lőfegyverek iránt.[739]

A high-end és a kísérleti 3D nyomtatók még mindig több ezer USD-be kerülnek, de már összeállítható gép 200 USD-ból is.

A pandémia alatt a technológia relevanciája nőtt.[740] A technológia létfontosságúvá válik az egészségügy fejlesztésében és a vészhelyzetre adott válaszban. A 3D nyomtatás egy zöldebb jövő alapja lehet. A digitalizáció miatt az Internet of Things (IoT) és Industry 4.0 környezetek egyre inkább kulcsfontosságú része lesz.[741]

2. A 3D nyomtatás árnyoldalai

Hosszasan lehetne ecsetelni a technológia hasznait és előnyeit, pl. gépészet, egészségügy, fogászat, forenzikus tudományok[742], vagy katonai alkalmazás[743] terén, de jelen fejezetben annak árnyoldalait vizsgálom. A 3D nyomtatás minden kockázatának részletes ismertetése a dolgozat kereteit szétfeszítené, így azokat csak röviden

---

https://www.aljazeera.com/news/2020/3/24/coronavirus-triggers-panic-buying-of-guns-in-hungary (2021.08.11.)

[737] KELLY, K.: The Rise of the 3D-Printed Gun. The Soapbox. (2020, May 21). https://newrepublic.com/article/157753/rise-3d-printed-gun (2021.08.11.)

[738] Például: How to Make 3D Printed Gun Parts – Step by Step Guide. Pick 3D Printer. (2021, July 12). https://pick3dprinter.com/3d-printed-gun-parts/ (2021.08.11.)

[739] CLARKE, C. P.: Trends in Terrorism: What's on the Horizon in 2021? Foreign Policy Research Institute. (2021, January 5). https://www.fpri.org/article/2021/01/trends-in-terrorism-whats-on-the-horizon-in-2021/ (2021.06.19.)

[740] KELLY: i. m.

[741] CHOONG, Y. Y. C. – TAN, H. W. – PATEL, D. C. – CHOONG, W. T. N. – CHEN, C-H. – LOW, H. Y. – TAN, M. J. – PATEL, C. D. – CHUA, Ch. K.: The global rise of 3D printing during the COVID-19 pandemic. Nature Reviews Materials, 2020. Vol. 5. No. 9. 638. o.

[742] CAREW, R. M. – ERRICKSON, D.: An Overview of 3D Printing in Forensic Science: The Tangible Third-Dimension. Journal of Forensic Sciences, 2020. Vol. 65. No. 5. 1752. o.

[743] GÁL B. – NÉMETH A.: Additív gyártástechnológiák katonai alkalmazásának vizsgálata, különös tekintettel a katonai elektronika területére. Hadmérnök, 2019/1. 231–249. o.

tárgyalom, fókuszomban a 3D nyomtatott lőfegyverek kérdése áll.

A technológiához fűződnek jogi aggályok, például a szerzői jogsértések terén, de vannak közbiztonsági, állambiztonsági összefüggései is.

Az interneten találhatóak szabadalmi oltalmat és formatervezésiminta-oltalmat sértő CAD fájlok („(…) egy elektronikus tervrajz az elkészítendő tárgyról.”[744]).[745]

A széles körben elérhető CAD fájlok miatt kompromittált részek kerülhetnek az ellátási láncba.

A technológiának egészségügyi kockázatai is vannak: A megfelelő szellőzés nélkül használt nyomtatók ultrafinom részecskéknek tehetik ki a használót, melyeknek belélegezve káros egészségügyi hatásai lehetnek.

Globális közbiztonság: 3D nyomtatással több lehetőség nyílik tiltott termékek megszerzésére.[746] A technológia nukleáris centrifuga alkatrészek is gyárthatók.

Az internetre töltött tervrajzokkal kézifegyverek, drónalkatrészek és tartozékok, kábítószerek, új pszichoaktív anyagok, és kettős felhasználású termékek nyomtathatók. A technikai innováció lehagyja a törvényhozást, mely fejlesztésre szorul.[747]

A 3D nyomtatás kiberbiztonsági fenyegetés is;[748] híd a műszaki tudományok (így tehát a fizikai bűnözés) és a kiberbűncselekmények között. A digitális fájlok fizikai előállítás céljából interneten eljuttathatók a világ bármely pontjára.[749]

Különösen a rugalmassága miatt az additív gyártás a „kettős felhasználású” megtestesítője.[750] „A kettős felhasználású termékek azok a termékek, beleértve a szoftvert és technológiát is, amelyek polgári és katonai célokra egyaránt felhasználhatók.”[751] Például a centrifugák az egészségügyben is használhatóak, de

---

[744] PARDY B.: Lőfegyvert otthon műanyagból? Ars Boni. (2019. január 7.). https://arsboni.hu/lofegyvert-otthon-muanyagbol/ (2021.08.12.)

[745] NAGY Z. A.: A 3D nyomtatás, mint a jogrendszert érintő új kihívás. Magyar Jog, 2017/10. 619–620. o.

[746] The Risks of 3D Printing. http://www.sciroccogroup.com/the-risks-of-3d-printing/ (2021.08.12.)

[747] BANERJEE, A.: Arms and the Man: Strategic Trade Control

Challenges of 3D Printing. International Journal of Nuclear Security, 2018. Vol. 4. No. 1. 1. o.

[748] FRUEHAUF, J. D. – HARTLE, F. X. – AL-KHALIFA, F.: 2016 Proceedings of the Conference on Information Systems Applied Research. Las Vegas, 2016. 2. o.

[749] SILBERGLITT, R. – CHOW, B. G. – HOLLYWOOD, J. S. – WOODS, D. – ZAYDMAN, M. – JACKSON, B. A.: Visions of Law Enforcement Technology in the Period 2024-2034. Rand Corporation, Santa Monica, 2015. https://www.ojp.gov/pdffiles1/nij/grants/248718.pdf (2021.08.15.) Idézi: FRUEHAUF – HARTLE – AL-KHALIFA: i.m. 2. o.

[750] FEY, M.: PRIF Report No. 144 3D Printing and International Security Risks and Challenges of an Emerging Technology. Peace Research Institute Frankfurt (PRIF), Frankfurt, 2017. 21. o.

[751] mkeh.gov.hu/haditechnika/kettos_felhasznalasu (2021.08.15.)

hasadó anyagok dúsítására is, nukleáris fegyverekben való alkalmazáshoz.[752] Az additív gyártás relevanciája nő a tömegpusztító fegyverek proliferációja és azok célbajuttató eszközei terén is.[753] A 3D nyomtatók segíthetik a tömegpusztító fegyverek elterjedését, és megkönnyítik azok titokban történő gyártását.[754]

A 2019-es halle-i támadás rámutat, hogy a 3D nyomtatott fegyverek terrortámadások elkövetésére is használhatóak.[755] Kérdés, hogy a terrorizmus jövője lehet-e 3D nyomtatás.[756]

Maguk a 3D nyomtatók is ki vannak téve támadásoknak. A nyomtató kompromittálása nem cél, inkább egy állomás az azzal történő támadások indításához. Például kompromittálható egy gép azért, hogy manipulálják a gyártott alkatrészek mechanikai tulajdonságait. Ha azokat például sugárhajtóművekben vagy más biztonsági szempontból kritikus rendszerekben használják, azok emberi életet veszélyeztethetnek, kritikus infrastruktúrát bomlaszthatnak, és jelentős gazdasági és társadalmi hatásokkal járhatnak. Egy kompromittált 3D nyomtató fegyverként használható, kinetikus, nukleáris/biológiai/vegyi vagy kiber kár okozásához.[757]

---

[752] FEY: i.m. 21. o.

[753] DAASE, C. – CHRISTOPHER, G. – DALNOKI-VERESS, F. – POMPER, M. – SHAW, R.: WMD Capabilities Enabled by Additive Manufacturing: NDS Report 1908. Negotiation Design and Strategy, Jupiter, FL/Monterey, CA, 2019. 10. o. http://www.nonproliferation.org/wp-content/uploads/2019/09/NDS_Report_1908_WMD_AM_2019.pdf (2021.08.30.)

[754] GAULT, M.: 3-D Printers Could Help Spread Weapons of Mass Destruction. Scientific American. (2019, September 10). https://www.scientificamerican.com/article/3-d-printers-could-help-spread-weapons-of-mass-destruction/ (2021.08.30.)

[755] VAN DER VEER, R.: Terrorism in the age of technology. https://www.clingendael.org/pub/2019/strategic-monitor-2019-2020/terrorism-in-the-age-of-technology/ (2021.08.30.)

[756] HOFFMAN, B. – WARE, J.: Is 3-D Printing the Future of Terrorism? The Wall Street Journal. (2019, October 25). https://www.wsj.com/articles/is-3-d-printing-the-future-of-terrorism-11572019769 (2021.08.31.)

[757] YAMPOLSKIY, M. – SKJELLUM, A. – KRETZSCHMAR, M. – OVERFELT, R. A. – SLOAN, K. R. – YASINSAC, A.: Using 3D printers as weapons. International Journal of Critical Infrastructure Protection, 2016. Vol. 14. No. 3. 58. o.

3. A 3D nyomtatott lőfegyverek

1. A 3D nyomtatott lőfegyverek története röviden

Cody Wilson, a Defense Distributed, egy ezeknek a fájloknak a megosztását megcélzó együttműködő közösség alapítója 2013. májusban közétette a Liberator lőfegyver tervrajzát, mely polimerből készül, és 3D nyomtató gyártja. Amíg elérhetőek voltak, a fájlokat kb. 100.000 alkalommal töltötték le az első két napon. Az amerikai hatóságok felszólították Wilson-t, hogy távolítsa el a fájlt és a más általa tervezett tervrajzokat az internetről.[758] Öt évig tartó jogi csatározás következett a tervrajzok közzétételéről[759], végül 2018-ban a Trump adminisztráció legalizálta a 3D nyomtatott lőfegyvereket. Az évben Wilsont kiskorú ellen elkövetett sexual assault-al vádolták, és ott kellett hagynia a Defense Distributed-et, ami nem szűnt meg. Ma évi 50 USD ellenében a Defcad website-on, a Defense Distributed online platformján különböző 3D nyomtatott lőfegyverek design fájljaik tölthetők el. A fájlok nem elérhetőek az USA-n kívüliek számára. Fájlok fel is tölthetők.

2019-ben egy szövetségi bíró Seattle-ben törvénytelennek ítélte a legalizálást, ezzel ideiglenesen újra lezárva a Defcad-ot. Erre reagálva 2019-ben megalakult a Deterrence Dispensed csoport. E fegyveraktivisták hálózata ugyanazt az ideológiát vallja, mint a Defense Distributed, de attól abban különbözik, hogy teljesen decentralizált, ezért rendkívül nehéz, vagy lehetetlen megállítani őket. Az USA-ban minden fegyveraktivista, így a Defense Distributed és a Deterrence Dispensed is a második alkotmánymódosításra hivatkozik. A jogi csatározás a fegyveraktivisták és az USA kormányzata között ma is folytatódik. 2020 elején 20 állam koalíciója és a District of Columbia keresetet nyújtott be a szövetségi kormányzat ellen, a Trump adminisztráció a 3D nyomtatott fegyver-fájlok online megosztását lehetővé tevő döntése miatt.[760]

---

[758] HONSBERGER, H. – RHUMORBARBE, D. – WERNER, D. – RIVA, F. – GLARDON, M. – GALLUSSER, A. – DELÉMONT, O.: How to recognize the traces left on a crime scene by a 3D-printed Liberator? Part 1. Discharge, exterior ballistic and wounding potential. Forensic Science International, 2018. Vol. 286. 246. o.

[759] PARDY B.: Az első 3D nyomtatott lőfegyverrel kapcsolatban felmerült alkotmányjogi kérdések az Amerikai Egyesült Államokban. Iustum Aequum Salutare, 2018/3. 185–202. o.

[760] M., A.: 3D printed guns: where are we now? 3D Natives. (2020, September 2). https://www.3dnatives.com/en/3d-printed-gun-020920205/#! (2021.08.30.)

2. A 3D nyomtatott lőfegyverek kriminológiai kockázatairól

Jacobs és Haberman szerint a 3D fegyvergyártással kapcsolatos fő aggályok a következők: a fémdetektorok kijátszása, a háttérellenőrzés megkerülése, a sorszám hiánya miatt a lenyomozás elkerülése, az USA-beli géppuska-tilalom megkerülése.[761]

Szabó rámutat arra, hogy a 3D nyomtatott lőfegyverek apró műanyag darabokra szedhetők szét, melyek magas biztonsági kockázatot jelentenek, mert elrejthetők és a beazonosításuk szinte lehetetlen. Így az eszköz releváns biztonsági kockázatot elsősorban a kiemelten fontos kritikus infrastruktúrák vonatkozásában jelent. Szabó szerint a 3D nyomtatási technológia fejlődése és a költségek csökkenése nem csak az otthoni - egyre szélesebb körű – felhasználást tette lehetővé, hanem a fegyvergyártás terén is jelentős változásokat hozott, mivel az nem állami szereplők számára is lehetővé vált. Azok a piaci szereplők, akik nem, vagy csak korlátozottan jutottak hozzá korábban tűzfegyverekhez, a technológiával már gyorsabban, olcsóbban, hatósági kontroll híján, és lényegesen nagyobb mennyiségben képesek használható fegyvereket előállítani.[762]

Schwartz szerint a veszélyt azok jelentik, akik 3D nyomtatót választanak fegyvergyártáshoz. Egy 3D nyomtatóval, számítógéppel és netkapcsolattal bárki az otthonát a szabályozást megkerülve fegyvergyárrá alakíthatja.[763] Ez a kockázat Magyarországon is fennáll.

3. A 3D nyomtatott lőfegyverek típusai

A 3D nyomtatott lőfegyverek három kategóriába sorolhatóak: Teljes mértékben 3D nyomtatott lőfegyverek, hibrid 3D nyomtatott lőfegyverek és lőfegyverek 3D nyomtatott tokszerkezettel.[764]

A teljes mértékben 3D nyomtatott lőfegyverek nem igényelnek nem nyomtatott nyomástűrő alkatrészeket, de tartalmazhatnak kisebb nem nyomtatott részeket, mint

---

[761] JACOBS, J. B. – HABERMAN, A.: 3D-Printed Firearms, Do-It-Yourself Guns, & the Second Amendment. Law and Contemporary Problems, 2017. Vol. 80. No. 2. 141–144. o.

[762] SZABÓ Cs.: A 3D nyomtatási technológiával előállított tűzfegyverek biztonságpolitikai kihívásainak vizsgálata a fegyverrendészet aspektusából I. Nemzetbiztonsági Szemle, 2017/4. 100. o.

[763] SCHWARTZ, C.: 3D Printing: The Potential Implications and Challenges for Law Enforcement. The Police Chief, 2015. Vol. 82. No. 3. 65. o.

[764] HAYS, G. – T., I. – JENZEN-JONES, N. R.: Desktop Firearms: Emergent Small Arms Craft Production Technologies. ARES Research Report No. 8. Armament Research Services (ARES), Perth, 2020. 13–16. o. http://armamentresearch.com/wp-content/uploads/2020/03/ARES-Research-Report-8-Desktop-Firearms.pdf (2021.08.30.)

ütőszegként szolgáló szeget, vagy elasztikus szalagot a kakas működtetéséhez. A fém alkatrészek majdnem teljes hiánya miatt az ilyen modellek kerültek a média fókuszába. A „valóban" vagy „teljes mértékben"' („True" vagy „Fully" 3D-printed (F3DP)) lőfegyverek a legtöbb esetben csak korlátozott számú lövés leadására alkalmasak, mielőtt a részek túl deformáltak lesznek vagy strukturálisan kockázatos lesz a használat. E a kategóriában a lőfegyverek vagy egylövetű pisztolyok, vagy több csövet kapcsolnak össze „pepperbox" elrendezésben, ami több lövés leadását teszi lehetővé. E kategóriában a legismertebb a Liberator pisztoly. Ide sorolható még Songbird egylövetű pisztoly, és a Washbear PM522 és Hexan (.22 LR) revolverek.[765]

Ezeket fémdetektor nem érzékeli, és mivel házi készítésűek, lenyomozhatatlanok.[766]

A hibrid 3D nyomtatott lőfegyver design-ok globálisan szabályozatlan könnyen hozzáférhető alkatrészekre támaszkodnak, mint acélcső, fém rudak és rugók. Főleg 3D nyomtatottak, de felhasználnak nem-tiltott fém részeket elsődlegesen nagyobb illesztések megerősítésére, esetleg csőnek vagy töltényűrnek. A legtöbb ilyen rész ártalmatlan, általában a hatóságok figyelmét nem keltik fel. Annak ellenére, hogy nem használnak erre a célra készült lőfegyver részeket, a hibrid design-ok bizonyos hagyományos fegyverekkel nagyjából hasonló teljesítményre képesek. Ahol elérhetők, ott szabályozatlan lőfegyver-alkatrészek (mint tölténytárak) is beépíthetők.[767]

Lőfegyverek 3D nyomtatott tokszerkezettel: az ilyen lőfegyvereket 3D nyomtatott tokszerkezet (receiver vagy frame) használatával rakják össze, de bennük a legtöbb vagy az összes nyomástűrő alkotóelem (például a cső, szán és csap) kereskedelmi forgalomban kapható, gyárilag előállított alkatrész. Ezek a design-ok, melyekre néha tágan „parts kit conversions" vagy „parts kit completions" (PKC) elnevezéssel utalnak, általában a legmegbízhatóbbak a 3D nyomtatott alkatrészeket használó lőfegyverek közül, gyakran ugyanannyira, mint a gyári lőfegyverek. Általában ezek anyagköltsége viszont a legmagasabb és nehezebben megépíthetők, ha egyes alkatrészeket törvény korlátoz.[768]

[765] HAYS – T. – JENZEN-JONES: i.m. 13. o.

[766] FERNÁNDEZ, S.: Trump administration sets into motion return of online 3D gun blueprints. The Texas Tribune. (2020, January 14). https://www.texastribune.org/2020/01/14/3d-printed-gun-blueprints-could-soon-go-back-online/ (2021.08.31.)

[767] HAYS – T. – JENZEN-JONES: i.m. 14. o.

[768] Uo. 15. o.

4. A 3D nyomtatott lőfegyverek tervrajzainak online elérhetősége

Nagy rávilágít, hogy a feltöltött 3D fájlok elérhetők a felszíni weben, vagy a deep weben és a dark weben. Ugyan a fegyverek, kábítószerek, és jogvédett tárgyak 3D fájljai a felszíni webről eltávolíthatók, eltávolítandók, azonban a deep webhez sorolható P2P (pl. torrent-) hálózatain számíthatunk elérésükre. Nagy szerint e téren domináns lesz, vagy már az a dark web. A bűnözők, terroristák titkos kommunikációjának új „tartalma" lesz a 3D-s fegyver-fájlok is, melyek leplezett módon letölthetők. 3D nyomtató vásárolható, a nyomtatáshoz fémpor legálisan beszerezhető, a fegyver alkatrészenként kinyomtatható és összeszerelhető, alkatrészekkel kiegészíthető, de Nagy szerint szakértő kell a fegyverek összeállításához, mert szakszerűtlen szerelés esetén az önveszélyes is lehet. Várható, hogy akár a legmodernebb fegyverek készítése lehetséges lesz, és egyre több fájl lesz jelen. Nagy szerint a fegyverek 3D-s tervrajzai majd elárasztják, ha el nem árasztották az internetet és akár a valós térbeli fegyverkereskedelem csökkenhet, mivel a bűnözők, terroristák majd saját eszközparkkal nyomtatnak fegyvert.[769]

Paoli szerint a 3D nyomtatott fegyverekkel kapcsolatos legnagyobb kockázatot a dark web jelenti, melyen egyének, csoportok, sebezhető és megszállott egyének is szerezhetnek fegyvereket és lőszert, anonim módon.[770] Paoli kutatásai szerint a dark weben a digitális fájlok a második leggyakrabban vásárolt fegyverekkel kapcsolatos termékek, melyek közé tartozhatnak oktatóanyagok otthoni bombagyártásról, vagy arról, hogyan alakítható át a félautomata lőfegyver automatára, valamint lőfegyverek és azok részeinek 3D modelljei is. Digitális termékek esetén a tranzakció online zajlik, ami nehezíti annak nyomon követését. Az útmutatók és 3D modellek proliferációja a kereskedelmi forgalomban kapható 3D nyomtatók minőségének javulásával együtt több lenyomozhatatlan fegyvert eredményezhet, ahogy a felhasználók is egyre inkább képesek teljesen működőképes fegyvereket gyártani. Az is valószínű, hogy a már meglévő lőfegyverek azonosító jelzésekkel ellátott eredeti részei és alkatrészei lecserélhetőbbek lesznek 3D nyomtatott részekkel és alkatrészekkel.[771]

---

[769] NAGY Z.: Visszaélés a 3D nyomtatással. Ars Boni. (2019. július 3.). https://arsboni.hu/visszaeles-a-3d-nyomtatassal/ (2021.08.31.)

[770] SHER, D.: Study shows 3D printed weapons face similar issues as any AM segment. 3D Printing Media Network. (2018, August 7). https://www.3dprintingmedia.network/arms-trade-study-reports-3d-printable-gun-files-widely-available-on-dark-web/ (2021.08.31.)

[771] PAOLI, G. P.: The Trade in Small Arms And Light Weapons on the Dark Web: A Study. UNODA Occasional Papers, Number 32. United Nations Office for Disarmament Affairs (UNODA), New York, 2018. 59–60. o.

Nem feltétlenül értek egyet az olyan véleményekkel, melyek túlhangsúlyozzák a dark web szerepét a témát illetően. 3D lőfegyver tervrajzok letöltéséhez ugyanis nem szükséges egészen a dark webig menni, azok a felszíni weben is könnyedén fellelhetőek. A Liberator tervrajza letölthető pl. a The Pirate Bay torrent oldalról is.[772] A DEFCAD felszíni weben elérhető könyvtárában is rengeteg lőfegyver és alkatrészeik tervrajza megtalálható: például 2020. 12. 04-én az FGC-9 gépkarabély 81.100 megtekintéssel és 714 letöltéssel, az M4A1 26.100 megtekintéssel, 378 letöltéssel rendelkezett.[773] Ezek a számok pedig nőnek. 2020. 12. 30-án az FGC-9 már 95.300 megtekintéssel és 784 letöltéssel, az M4A1 28.800 megtekintéssel, 404 letöltéssel büszkélkedhetett.[774] 2021. 03. 12-én az FGC-9 143.800 megtekintésnél és 1.100 letöltésnél, az M4A1 33.000 megtekintésnél, 474 letöltésnél tartott. Az oldal 2021. 03. 12-én 16.595 letölthető fájllal, 43.035 felhasználóval rendelkezett.[775] Ugyan a DEFCAD oldalról az USA-n kívülről nem lehet letölteni, de egy USA-beli személy a már letöltött tervrajz fájlt elküldheti másnak is, akár ingyenesen, akár ellenérték fejében, feltöltheti akárhová az interneten etc.

5. 3D nyomtatott lőfegyverekkel kapcsolatos esetek

2013 májusában két riporter kinyomtatta és felvitte a Liberatort egy Londonból Párizsba tartó Eurostar vonatra.

2013 májusában az ausztrál New South Wales Police két lőfegyvert nyomtatott és azokkal lőtt is. Az első elsült, és megerősítették a halálosságát, a második felrobbant.

2013 júliusában újságírók lőfegyvert nyomtattak, azt becsempészték az Izraeli Parlamentbe és ráfogták a miniszterelnökre.

2013 októberében egy razzia során 3D nyomtatott lőfegyver alkatrészeket és egy 3D nyomtatót találtak Manchesterben.

Japánban, 2014 májusában Yoshitomo Imura-t letartóztatták 3D nyomtatott lőfegyverek birtoklásáért és két év szabadságvesztésre ítélték.

2015 februárjában Ausztráliában a rendőrség 3D nyomtatott lőfegyver részeket talált, az elkövető beismerte az illegális fegyvergyártást.

2015 júniusában a rendőrség Oregon-ban lefoglalt egy AR-15-ös gépkarabélyt 3D nyomtatott alsó tokszerkezettel.

[772] Lásd: https://thepiratebay.org/description.php?id=28522986 (2021.08.31.)

[773] https://defcad.com/library/ (2020.12.04.)

[774] https://defcad.com/library/ (2020.12.30.)

[775] https://defcad.com/library/ (2021.03.12.)

2016 májusában Ausztráliában egy törvényen kívüli motoros bandákhoz fűződő razzia során lefoglaltak egy lőfegyverek nyomtatására használt 3D nyomtatót.

2016 júniusában Ausztráliában a rendőrség 3D nyomtatott lőfegyvereket talált, és figyelmeztetett egy személyt, aki lőfegyver másolatokat készített filmes kellékeknek.

2016. augusztus, USA: A Reno Repülőtéren a Transportation Security Administration egy kézipoggyászban éles lőszerrel töltött 3D nyomtatott revolvert talált.

2016. november, Ausztrália: 5 személyt 3D nyomtatott lőfegyverek birtoklásával vádoltak. A rendőrség négy géppuskát, fegyvergyártáshoz szükséges eszközöket, hangtompítókat és egy 3D nyomtatót talált.

2016. december, Ausztrália: A rendőrség 14 lőfegyvert talált. A gyanúsítottat 3D nyomtatott lőfegyverek és bokszerek eladásával vádolták.

2017. március, Ausztrália: Egy személy 3D nyomtatott lőfegyvert árult online. A rendőrség négy pisztoly-utánzatot, köztük kettő 3D nyomtatott Glock-ot, egy 3D nyomtatott Sig 250-et, két légpisztolyt, számítógépes eszközöket, és két 3D nyomtatót talált.

2018. július, Ausztrália: A rendőrség egy lakóingatlanban 3D nyomtatott kézifegyvereket és bokszereket, hamis vezetői engedélyeket, bankkártyákat és kábítószert talált.[776]

Egy 26 éves londoni hallgatót három év szabadságvesztésre ítéltek, amiért lőfegyvert nyomtatott. A rendőrség 2017 októberében két 3D nyomtatót talált nála, amik éppen egy revolver csövét nyomtatták, és alkatrészeket a Washbear és Reprringer lőfegyverekhez, melyekhez csak acélcső hiányzott, hogy működőképesek legyenek. A hallgató a tervrajzokat az internetről szerezte.[777]

A dallas-i Eric McGinnis-t lőfegyver birtoklásától két évre eltiltották, miután 2015-ben megtámadta a barátnőjét. 2016-ban megkísérelt fegyvert vásárolni, de megbukott a háttérellenőrzésen, ezért lőfegyver részeket és 3D nyomtatót vásárolt. Alig több mint egy hónap volt vissza a lőfegyvertől való eltiltásából, amikor 2017-ben letartóztatták a részben 3D nyomtatott AR-15-jével, és egy amerikai törvényhozók listájával a texasi Dallas közelében. Fegyverének 3D nyomtatott része nem volt illegális, hanem az, hogy lőfegyvert birtokolt.[778]

---

[776] DALY, A. – MANN, M. – SQUIRES, P. – WALTERS, R.: 3D printing, policing and crime. Policing and Society, 2021. Vol. 31. No. 1. 42. o.

[777] Student jailed for making 3D printed gun. BBC. (2019, September 19). https://www.bbc.com/news/uk-england-london-49761290 (2021.08.31.)

[778] Man jailed after found with 3D-printed gun and 'lawmaker hit list'. BBC. (2019, February 14).

3D nyomtatott, egyszer használatos fegyvereket is tartott D. Csaba, a csantavéri bérgyilkos, akit 2019 március elején fogott el a cseh rendőrség egy prágai hotelben. D. Csabához két 3D-nyomtatott pisztoly köthető.[779]
2020. február 15-én öt németországi tartományban tartottak házkutatásokat, és szélsőjobboldali terrorista szervezkedés gyanúja miatt elfogtak 12 személyt. E szervezet célja Németország állami és társadalmi rendjének, demokratikus berendezkedésének megdöntése volt.[780] A 2019 nyarán megalakult és radikalizálódott Der harte Kern/The Hard Core új terrorista sejt polgárháború indításának szándékával mecsetek elleni 10 koordinált támadás végrehajtását tervezte, melyeket a christchurch-i támadás inspirált. A tagok a WhatsApp-on találkoztak és az ún. „hive terrorism" jegyeit mutatták, mely során szervezett extrémista szcénákhoz kevés korábbi kötődéssel rendelkező személyek hálózatait mobilizálják erőszakos cselekedetek megtervezésére. A felfedezést megnehezíti a csoport formáció többé-kevésébé spontán természete. Tartoztak bele régóta tevékenykedő neo-nácik, és a hatóságok előtt korábban ismeretlenek is. A razzia során egy házi készítésű fegyvert is találtak. A csoportnak nemzetközi kapcsolatai is voltak, a szélsőjobboldali extrémista finn Soldiers of Odin csoporttal.[781]
2020. március 30-án egy ún. akceleracionalista (accelerationist) Telegram csatorna linkeket osztott meg, instrukciókhoz arról, hogyan kell 3D nyomtatással létrehozott alkatrészekkel pisztolyt készíteni.[782]

6. A halle-i eset elemzése a 3D nyomtatott lőfegyver szempontjából

Jackson az International Centre for the Study of Radicalisation-nel (ICSR) készített

---

https://www.bbc.com/news/world-us-canada-47243007 (2021.08.31.)

[779] 3D-nyomtatott fegyverei lehettek a szerbiai magyar bérgyilkosnak. HVG. (2019. március 21.). https://hvg.hu/vilag/20190321_3d_nyomtatas_fegyver_d_csaba_bergyilkos (2021.08.31.)

[780] Elfogtak több feltételezett szélsőjobboldali terroristát Németországban. Honvédelem.hu. (2020. február 16). https://honvedelem.hu/cikk/elfogtak-tobb-feltetelezett-szelsojobboldali-terroristat-nemetorszagban/ (2021.08.31.)

[781] HUME, T.: New German Terror Cell 'The Hard Core' Planned to Attack Mosques to Start a Civil War. Vice. (2020, February 17). https://www.vice.com/en/article/z3bymx/new-german-terror-cell-the-hard-core-wanted-to-attack-mosques-to-start-a-civil-war (2021.08.31.)

[782] Extremist Content Online: Extremists Plot Anti-Semitic Harassment Campaign Targeting Philadelphia Jewish Day School. Counter Extremism Project. (2020, April 6). https://www.counterextremism.com/press/extremist-content-online-extremists-plot-anti-semitic-harassment-campaign-targeting (2021.08.31.)

interjúja során az ICSR rávilágít a tényre, hogy az elkövető 3D nyomtatott lőfegyvert nem használt. Balliet több fegyvert konstruált, de egyik sem volt teljes mértékben 3D nyomtatott. A támadás során több házi készítésű fegyver volt a birtokában, közülük kettőt használt ténylegesen. Az ún. „Luty" géppisztollyal ölte meg két áldozatát, mely nevét Philip Luty-ról kapta, aki azt alkotta és annak design fájljait online terjesztette. Az főleg fémből készült és nem 3D nyomtató használatával. 3D nyomtatott nem fém alkotóelemek az elkövető Luty design-jában a kapcsolókapocs (trigger clip) és csőre szerelhető lámpa szerelék (torch barrel attachment) voltak. Az ICSR szerint a fegyver működőképes lett volna ezek nélkül is, és mindkét rész könnyen és olcsón beszerezhető hagyományosan gyártott formáikban is. A második fegyver egy sörétes puska volt, hozzáerősített 3D nyomtatott tölténytartóval, mely nem volt szükséges a fegyver működtetéséhez, és a fém változatai online is beszerezhetőek, elkészítéséről oktatóvideók is vannak. A támadó a második fegyverre tért át, mert az elsőben elakadtak a töltények. Balliet itt önmagát „vesztesnek" nevezte, és azt mondta, hogy: „Biztosan sikerült bebizonyítanom, hogy mennyire abszurdak az improvizált fegyverek." („I have certainly managed to prove how absurd improvised weapons are."). Ezt visszhangozta az extrémista csoport is, melynek tagja volt. Az ICSR szerint Balliet támadását, és a célt, hogy bizonyítsa a házi készítésű fegyverek járhatóságát, a szélsőjobboldali extrémista miliőben sikertelennek fogják látni.

Amikor történik egy támadást illető innováció (pl. gépjárművel emberek közé hajtás, vagy 3D nyomtatott alkotóelemek használata), akkor látható, hogy a terroristák gyakran a „sikeres" újításokat utánozzák, melyet a médiahatásban és/vagy a halálos áldozatok számában mérnek. Ezért a 2016-os nizzai terrortámadás után, mely során kamionnal hajtottak tömegbe, megnövekedett az olyan támadások száma, melyek során gépjárművel hajtottak emberek közé. Mivel a halle-i támadás a fehér nacionalisták online reakcióiból ítélve nem volt sikeres, nem biztos, hogy ez lesz, ami megmutatja a 3D nyomtatott fegyverek járhatóságát a jövőbeli elkövetőknek. Az ilyen támadások megelőzéséhez az ICSR szerint szükség van szabályozásra és intézkedésekre a fegyverek ily módon történő gyártásának korlátozására. Nem tiszta azonban, hogy pontosan hogyan kellene ezeknek a digitális természetét szabályozni, ami azért is problematikus, mert emberek évezredek óta készítenek improvizált fegyvereket.[783]

[783] JACKSON, B.: Interview with the ICSR: A 3D printed gun was not used in the Halle terror attack. 3D Printing Industry. (2019, October 18). https://3dprintingindustry.com/news/interview-with-the-icsr-a-3d-printed-gun-was-not-used-in-the-halle-terror-attack-163643/ (2021.08.31.)

7. A jogi szabályozás néhány kérdése

A 3D nyomtatással kapcsolatos jogi aggályokat illetően egyetértek Nagy sürgető szavaival: „A technológia itt van, megy előre, nem vár. A jog pedig nem várhat."[784] A szabályozással kapcsolatban azonban osztom Horváth és Kurucz aggályait: „A törvényi szabályozás eredményének kétsége hasonló origóból eredeztethető, mint a (…) jog nélkül letöltött és nyomtatott termékek esetén. A fegyverek 3D modelljeit hiába távolítanák el szerverekről, azok peer-to-peer fájlcserélőkön, tényleges tárhely nélkül, vagy akár ártalmatlan, ám ellenőrizetlen kommunikációs csatornákon (Whatsapp, Skype, Messenger, Viber) cserélhetnek gazdát, az otthoni nyomtatást meglévő modell esetén pedig lehetetlen lenyomozni, hacsak nem változik világunk Orwell lázálomszerű utópiájává. Ez a tény pedig voltaképp egy olyan kérdést vet fel, ami magát a technológia létezését vonja kétségbe: szabad 3D nyomtatót magáncélra birtokolni?"[785]

Amennyiben valaki egy lőfegyver CAD fájlját azzal a céllal tölti le, hogy 3D nyomtatóval elkészítse azt, lőfegyverrel visszaélés bűncselekmény előkészülete miatt lesz büntetendő. Pardy szerint a CAD fájlok letöltése önmagában nem feltétlenül alapozza meg a lőfegyverrel visszaélés előkészületét, példaként hozza, hogy abszurd lenne egy olyan fegyver terve miatt megbüntetni valakit, amely a legújabb Call of Duty vagy Battlefield videojáték eleme, és csupán a játék fegyverkészletének kiterjesztése miatt töltötte azt le. Ugyanígy lehetséges, hogy a CAD fájl nyomtatóra töltésével csupán egy játék pisztoly, vagy egy gyűjtői replika készül, mert eleve, és szándékosan nem „működőképes" a terv. A jogalkalmazók felelőssége eldönteni az egyedi esetek alapján, hogy mely letöltések valósítják meg a bűncselekmény előkészületét. A működőképes lőfegyver elkészítése, illetve birtoklása azonban mindenképpen megfelel a lőfegyverrel visszaélés bűntett tényállásának. Úgy vélem, Pardy által felvetett legfontosabb kérdés az, hogy hogyan lehet majd a jövőben ellenőrizni, hogy ki mit nyomtat otthon.[786] Pedig pontosan ez jelenti a legnagyobb problémát. Tehetetlen lenne a jog a témát illetően?

Szabó szerint a tűzfegyverek és robbanóanyagok 3D nyomtatási technológiával történő gyártása és értékesítése kockázatának problémája komplex kezeléséhez átfogó megközelítés szükséges, amelynek Szabó úgy véli, első lépcsőfoka lehet a 3D nyomtatót

[784] NAGY (2017) i.m. 621. o.

[785] HORVÁTH Á. – KURUCZ A.: A 3D nyomtatás története és jövőbeli kérdései. In: REISINGER A. – KECSKÉS P. (szerk.): "Ifjúság - jövőképek": Kautz Gyula Emlékkonferencia 2016. június 15. elektronikus formában megjelenő kötete. Széchenyi István Egyetem, Győr, 2017. 9. o.

[786] PARDY B.: Lőfegyvert otthon műanyagból? Ars Boni. (2019. január 7.). https://arsboni.hu/lofegyvert-otthon-muanyagbol/ (2021.08.12.)

gyártók és forgalmazók online regisztrációjának az illetékes hatóságok részére történő bevezetése[787], mely javaslatot magam is jó ötletnek tartok, valamiféle regisztrációs kötelezettségre szükség lenne a 3D nyomtatók vonatkozásában.

A 3D nyomtatott lőfegyverek fenyegetését és problémáját illetően elgondolkodtatóak Földvári professzor szavai, aki gyakran előadásokon és a pécsi Büntetőjogi Tanszéken is Gál professzor visszaemlékezése szerint a következőképp fogalmazott: „A büntetőjog nem képes arra, hogy társadalmi problémákat oldjon meg. Tovább megyek: a büntetőjog önmagában arra sem alkalmas, hogy a büntetőjogi problémákat megoldja."[788]

4. Következtetések

Egyetértek Fenyvesi javaslataival: „A 3D-s nyomtatók elleni határtalan (nemzetközi) küzdelem 2013-ban kezdődött, ami feltehetően nem áll meg a kapuknál. Reálisan fel kell készülnie a bűnüldözésnek a fegyverek, netán robbanószerkezetek továbbjuttatásának ilyen módja ellen. Ki kell dolgoznia a megelőzési, felderítési lehetőségeket, a speciális módszertant."[789]

Straub szerint a 3D nyomtatott lőfegyverek veszélyesebbek lehetnek a használójukra, mint a célpontokra.[790] Horváth és Maróti egyetért azon szerzők, szakértők álláspontjával, utalva a Liberator kapcsán megjelent véleményekre is, hogy jelenleg nagyobb veszélyt jelent egy 3D nyomtatott fegyver a használóra, mint másra. Úgy vélik, kicsi a valószínűsége, hogy aki fegyveresen készül elkövetni egy bűncselekményt, otthonában az internetről letölti, azután kinyomtatja a műanyag alkatrészeket, azokhoz hozzáteszi az ütőszeget és kipróbálás nélkül alkalmazza azt más ellen. A szerzők szerint ugyanakkor nem kétséges, hogy a gyors technológiai fejlődés miatt szélesebb körben

[787] SZABÓ Cs.: A 3D nyomtatási technológiával előállított tűzfegyverek biztonságpolitikai kihívásainak vizsgálata a fegyverrendészet aspektusából II. Nemzetbiztonsági Szemle, 2017/4. 123. o.

[788] GÁL I. L.: A büntetőjog szerepe a gazdaságban, avagy megelőzhetők-e a brókerbotrányok büntetőjogi eszközökkel? 2017. 1. o. https://ujbtk.hu/prof-dr-gal-istvan-laszlo-a-buntetojog-szerepe-a-gazdasagban-avagy-megelozhetok-e-a-brokerbotranyok-buntetojogi-eszkozokkel/ (2021.09.01.)

[789] FENYVESI Cs.: A kriminalisztika válaszai a társadalmi kihívásokra – a bűnüldözés fejlesztési lehetőségei. In: GAÁL Gy. – HAUTZINGER Z. (szerk.): Pécsi Határőr Tudományos Közlemények XXII: A hadtudománytól a rendészettudományig− társadalmi kihívások a nemzeti összetartozás évében. Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport, Pécs, 2020. 221. o.

[790] STRAUB, J.: 3D-printed guns may be more dangerous to their users than targets. The Conversation. (2019, January 7). https://theconversation.com/3d-printed-guns-may-be-more-dangerous-to-their-users-than-targets-103724 (2021.09.01.)

fognak elterjedni a 3D nyomtatók és felhasználási területük is bővülni fog.[791]

Tesztek bizonyították[792], hogy a Liberatorok képesek egy lövés leadására. A fegyver által elszenvedett károsodás és a kilőtt lövedék zavart röppályája ellenére a 3D nyomtatott fegyverek sebző potenciálja tagadhatatlan,[793] az FGC-9 modellről nem is beszélve, amik messze nem csupán egyetlen lövés leadására képesek.

A Liberator tekintetében sem nyugtatnak meg az olyan vélemények, hogy jelenleg nagyobb veszélyt jelent egy 3D nyomtatott fegyver a használójára, mintsem másra. Egy kis utánajárással akárki gyárthat otthon fegyvert, még ha annak halálossága kérdéses is. Épp elegendő, ha birtokosa egyetlen ember életét is ki tudja vele oltani, vagy azzal súlyos sérüléseket okozni. Azt a személyt, vagy annak hozzátartozóit nem fogja vigasztalni, hogy több lövés leadására már nem volt képes az elkövető, vagy hogy a második lövésnél szétrobbant a kezében a fegyver, ha az ő életét, vagy hozzátartozóét elvette egy egyszer használatos 3D nyomtatott lőfegyverrel, vagy az által súlyos sérüléseket szenvedett. A terroristák is el tudják érni a kívánt hatást akár egy egyszer használatos lőfegyverrel is. Gondoljunk bele abba, hogy ha egy terrorista bejelentené, hogy egy nagyvárosban meg fog ölni egy random embert, egyetlen lövéssel, az mekkora pánikot lenne képes kelteni, és akkor még nem is esett szó arról, mire lehet képes egy elkövető az FGC-9 gépkarabéllyal. Ahogy a filozófus Vu Csi fogalmazott: „Egyetlen ember, aki kész az életét eldobni, elég ahhoz, hogy ezreket terrorizáljon."[794] Hiba lenne a kérdéskör által felvetett aggályokat a jogalkotónak és a rendvédelmi szerveknek különösen napjainkban, a fokozódó digitalizáció, és társadalmi feszültségek korában nem komolyan venni. Kérdéses, hogy tehet-e többet a jog a problémát illetően a fenyegetés csökkentése érdekében. Szabó által felvetett 3D nyomtatót gyártók és forgalmazók online regisztrációjának az illetékes hatóságok részére történő

[791] HORVÁTH O. – MARÓTI P.: 3D nyomtatott fegyverek – vélt vagy valós veszélyek? In: GAÁL Gy. – HAUTZINGER Z. (szerk.): Pécsi Határőr Tudományos Közlemények XX.: A XXI. század biztonsági kihívásai. Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoportja, Pécs, 2018. 78. o.

[792] HONSBERGER – RHUMORBARBE – WERNER – RIVA – GLARDON – GALLUSSER – DELÉMONT (2018): i.m. 245–251. o. Idézi: HONSBERGER, H. – WERNER, D. – RHUMORBARBE, D. – RIVA, F. – GLARDON, M. – GALLUSSER, A. – DELÉMONT, O.: How to recognise the traces left on a crime scene by a 3D-printed Liberator? Part 2. Elements of ammunition, marks on the weapons and polymer fragments. Forensic Science International, 2019. Vol. 295. 144. o.

[793] HONSBERGER – WERNER – RHUMORBARBE – RIVA – GLARDON – GALLUSSER –DELÉMONT (2019): i.m. 144. o.

[794] SCHMID (2004): i.m. 417. o.

bevezetését[795] magam is jó indítványnak tartom.

[795] SZABÓ Cs.: A 3D nyomtatási technológiával előállított tűzfegyverek biztonságpolitikai kihívásainak vizsgálata a fegyverrendészet aspektusából II. Nemzetbiztonsági Szemle, 2017/4. 123. o.

XV. A KORONAVÍRUS (COVID-19) HATÁSA A TERRORISTÁK INTERNETHASZNÁLATÁRA

1. A koronavírus pandémia hatása a bűnözésre

Hogy a koronavírus világjárvány a terroristák internethasználatára tett hatását fel lehessen vázolni, először szükséges általánosságban bemutatni annak a globális terrorizmusra és extrémizmusra tett hatásait.

Ambrus 2020-as jóslata szerint, amíg nem lesz vakcina a WHO által 2020. március 11-én pandémiának/világjárványnak nyilvánított[796] koronavírus (COVID-19)-el szemben, a rendkívüli helyzet még hosszabb ideig tartani fog, ami várhatóan gazdasági recessziót jelent, melynek például munkahelyek megszűnése miatt kriminogén hatása is lehet. Így nem kizárható, hogy a globális válság miatt nőni fog a bűncselekmények száma.[797] Gál a koronavírus nyomán kibontakozó gazdasági világválságról a következő megállapításokat teszi: „1. a koronavírus feltételezhetően több halálos áldozatot fog követelni világszerte, mint a nemzetközi terrorizmus eddig összesen a világtörténelemben, 2. a COVID-19 által generált világgazdasági válság mérhető lesz a 2008-ashoz, de akár az 1929–33-ashoz is, de az is előfordulhat, hogy komolyabb lesz, mint a 2008-as, hatásában csak az 1929–33-as válsághoz lesz mérhető, de az is lehet, hogy annál is súlyosabb lesz, 3. mint minden gazdasági válság, ez is hatással lesz a bűnözésre, az ismertté vált bűncselekmények számát bizonyos bűncselekmény kategóriákban, legalább időlegesen nagy valószínűséggel emelni fogja.” [798] Gál hipotézise szerint nagy valószínűséggel 2020 második felétől a bűnözés emelkedni fog, és ez az emelkedés még ez után 1-2 éven keresztül folytatódni fog. Kérdés az emelkedés mértéke, és hogy az hogyan lassítható és mérsékelhető.[799]

A koronavírus egyik hatásaként fokozódik a cyber-enabled crime (kapcsolódó

[796] Rolling updates on coronavirus disease (COVID-19). World Health Organization. https://www.who.int/emergencies/diseases/novel-coronavirus-2019/events-as-they-happen (2021.09.28.)

[797] AMBRUS I.: A koronavírus-járvány és a büntetőjog. MTA Law Working Papers 2020/5, Magyar Tudományos Akadémia, Budapest, 2020. 22. o.

[798] GÁL I. L.: A koronavírus (COVID-19) és az általa okozott gazdasági világválság lehetséges hatásai a bűnözésre. Magyar Jog, 2020/5. 258. o.

[799] Uo. 258. o.

kiberbűncselekmények[800] vagy kibertér által elősegített bűnözés[801]), a terrorizmus és az információs hadviselés (például dezinformációs kampányok és álhírek terjesztése).[802]

2. A koronavírus hatása a terrorizmusra

Az ENSZ főtitkára 2020. április 09-én felhívta a Biztonsági Tanács figyelmét, hogy a terrorizmus fenyegetése él, és a terroristák csapásra láthatnak lehetőséget, miközben a legtöbb kormány a pandémiára fókuszál. A helyzet különösen aggasztó a Száhel övezetben, ahol az emberek a vírus és a növekvő terrorizmus kettős fenyegetésével néznek szembe. A pandémia rávilágított a gyengeségekre és a felkészületlenségre, mely betekintést nyújt abba, hogyan bontakozna ki egy bioterrorista támadás, és annak kockázatát növelheti is.[803] A terrorizmus elleni küzdelem uniós koordinátora**,** Gilles de Kerchove szerint jobboldali extrémisták és iszlamista harcosok az egészségügyi személyzet és létesítmények elleni támadásokat nagyon hatékonynak láthatják, mivel azok a társadalomban masszív sokkot generálnának.[804] Egészségügyi létesítmények, az élelmiszeripar és civil szervezetek új célpontokká váltak, nemzetközi és hazai szinten. Felbukkantak esetek élelmiszer fertőzött személyek általi beszennyezéséről, bűnüldöző szervek állományának és egészségügyi dolgozók a vírusnak szándékos kitevéséről, és vallási és oktatási intézmények elleni támadásokról. Szélsőjobboldali terroristák zaklatókampányokhoz használták olyan szervezetek feltört e-mail belépési adatait, mint a WHO.[805] Tunéziában 2 embert letartóztattak, mert rendőröket terveztek köhögéssel koronavírussal megfertőzni.[806]

---

[800] MÁTÉ I. Zs.: Informatikai rendszerek elleni támadások szakértői vizsgálata – a digitális nyomok rögzítésének szerepe. Belügyi Szemle, 2018/7–8. 38. o.

[801] VARGA Á.: Az informatikai bűnözés fogalmi meghatározása, csoportosítása és helye a hazai jogfejlődésben. In Medias Res, 2019/1. 151. o.

[802] GRADOŃ, K.: Crime in the time of the plague: fake news pandemic and the challenges to law-enforcement and intelligence community. Society Register, 2020. Vol. 4. No. 2. 134. o.

[803] Secretary-General's remarks to the Security Council on the COVID-19 Pandemic [as delivered]. United Nations. (2020, April 9). https://www.un.org/sg/en/content/sg/statement/2020-04-09/secretary-generals-remarks-the-security-council-the-covid-19-pandemic-delivered (2021.09.29.)

[804] BINDING, L.: Coronavirus: IS could exploit COVID-19 pandemic to carry out terror attacks, EU warns. Sky News. (2020, May 13). https://news.sky.com/story/coronavirus-is-could-exploit-covid-19-pandemic-to-carry-out-terror-attacks-eu-warns-11987706 (2021.09.29.)

[805] SITE Intelligence Group Launches “Bioterrorism and Public Health” Service to Support Healthcare Efforts amid Global Threats. SITE Intelligence Group. https://ent.siteintelgroup.com/Press-Release/site-

Silke szerint tövid távon a zárlati (lockdown) intézkedések a terrortámadásokat visszafogják, de az azok elkövetésére felhívó propaganda ösztönözni fog néhány incidenst. Sok – kifejezetten a szélsőjobboldali extrémizmushoz kötődő – propaganda a koronavírushoz kapcsolódó összeeskövés-elméletekre fókuszál, és ezek már inspiráltak terveket és támadásokat. Az iszlamista extrémista propaganda inkább a pandémiával elfoglalt ellenséges kormányok sebezhetőségére koncentrál, és arra, hogy ez lehetőséget ad terrortámadásokra. Jelentős növekedés tapasztalható az online extrémista aktivitást illetően, ami a rövid és középtávon növeli a radikalizáció kockázatát. Hosszú távon erősen aggasztó, hogy a pandémia gazdasági következményei által meggyengített államok sebezhetőbbek lesznek a terrorista csoportokkal szemben.[807] Terrorista csoportok, felkelők és bűnszervezetek a helyzetet hatalmuk és befolyásuk növelésére használják. Nem csupán civil lakosság elleni erőszakkal, hanem „soft" módokon is, a civil lakosságnak nyújtott „humanitárius" segélyekkel, olyan helyeken, ahol a kormányok nem akarnak, vagy nem tudnak segíteni. A helyzet lehetőséget nyújt dezinformációval a félelem és nyugtalanság növelésére is, mely fő célja bizalmatlanság keltése a kormányokkal és hatóságokkal szemben, és a saját legitimáció növelése. Jelen helyzetben a nyugati biztonsági erők kevésbé lehetnek képesek segíteni a külföldi államokat. Az, hogy a tömegmédia főleg a koronavírussal van elfoglalva, a terroristákat a tevékenységük fokozására késztetheti, hogy ezzel visszatereljék magukra a figyelmet. A pandémia alatti „social distancing" során az embereknek sokkal több szabadideje van, és sebezhetőbbek a radikalizációval szemben. A lecsökkent mozgási szabadság, a megnövelt felügyelet és biztonsági intézkedések viszont nehezítik a tervezést, felkészülést és problematikusabbá teszik a terrorcselekmények külföldi elkövetését, de nem teszik lehetetlenné.[808] A COVID-19 rövidtávon kockázatokat is jelent a terroristák

---

intelligence-group-launches-public-health-and-bioterrorism-service-to-support-healthcare-efforts-amid-global-threats.html (2021.09.30.)

[806] Tunisia arrests 2 over 'coronavirus cough attack plot' on police station. The New Arab. (2020, April 17). https://english.alaraby.co.uk/english/news/2020/4/16/tunisia-foils-extremist-plot-to-infect-police-with-coronavirus (2021.09.30.)

[807] SILKE, A.: COVID-19 and terrorism: assessing the short-and long-term impacts. Cranfield: Pool Re Solutions, 2020. 2. o. https://www.poolre.co.uk/wp-content/uploads/2020/05/COVID-19-and-Terrorsim-report-V1.pdf (2021.09.30.)

[808] SIMONS, G. – BIANCA, C.: The Specter of Terrorism During the Coronavirus Pandemic. E-International Relations, 2020. 1. o. https://www.e-ir.info/2020/05/08/the-specter-of-terrorism-during-the-coronavirus-pandemic/ (2021.09.30.)

számára: negatívan hat a műveleti tevékenységeikre, a forrásaikra és a népszerűségükre.[809]

3. Fokozódó terror a fejlődő világban

Erős kapcsolat látszik az élelmiszerbiztonság és a terrorizmus között. Több jelentős terrorszervezet gyökerei élelmiszer-biztonsági problémákhoz vezethetőek vissza (például a Fényes Ösvény felemelkedése Peruban).[810] Az élelmiszer-biztonság hiánya miatt a polgárok dühösek lesznek a kormányaikra, mely lehetőséget ad terroristáknak új tagok toborzására, azáltal, hogy lehetővé teszik, hogy a frusztrációikat levezethessék. Sok esetben a terrorszervezetek teszik meg, amit a kormányaik nem tudnak, vagy akarnak: ételt és pénzt adnak az embereknek. Ahogy a krízis kiterjed a fejlődő világra, a nemzeteknek komoly nehézséget okoz majd az élelmiszer-ellátás és a béke fenntartása. Még a pandémia előtt regionális konfliktusok élelmiszerválságot hoztak létre Afrika több részén. A nemzeti zárlat segít a koronavírust terjedését visszafogni, de más polgári és gazdasági problémákat okoz, amik erőszakhoz vezethetnek. Nigériában például sok ember nem tud pénzt keresni a zárlat miatt. Az emberek frusztráltak a kormány pandémiára adott válaszával és azzal, hogy nem képes élelmiszert adni a rászorulóknak. Ahogy Nigéria fokozatosan enyhíti a zárlatot, a munkanélküliség valószínűleg megmarad. Mozambikban és Maliban iszlamista felkelők támadásai fokozódnak a pandémia nyomán. Lehetséges, hogy itt is szerepet játszik a koronavírus pandémia okozta élelmiszerbiztonság hiány. Pakisztánban élelmiszerválság volt már a pandémia előtt is. A koronavírus miatti romló körülmények Pakisztánban a terrorizmus fokozódását okozhatják. A Lashkar-e-Taiba és Jaish-e-Mohammad terrorista csoportok a koronavírus által érintetteket közelítik meg, alapvető szolgáltatásokat és támogatást ajánlva nekik, cserébe megszerzik a helyiek hűségét és újabb újoncokhoz juthatnak. A két terrorista csoport törekvései nyomán nőtt terrorista kiképző táborok száma a régióban. Hasonló toborzási taktikák tapasztalhatóak a kontinens más részein is. Törökországban az IS toborzói pandémia eredményeként munkájukat vesztett

[809] The impact of the COVID-19 pandemic on terrorism, counter-terrorism and counering violent extremism. CTED, 2020. 2–3. o.
https://www.un.org/sc/ctc/wp-content/uploads/2020/06/CTED-Paper%E2%80%93-The-impact-of-the-COVID-19-pandemic-on-counter-terrorism-and-countering-violent-extremism.pdf (2020.07.30.)

[810] BELLINGER, N. – KATTELMAN, K. T.: Domestic terrorism in the developing world: role of food security. Journal of International Relations and Development, 2021. Vol. 24. No. 2. 1. o.

migránsokat célozzák meg Türkmenisztánból.[811]

4. Példák a pandémiára adott terrorista reakciókra

1. IS, al-Kaida, Boko Haram.

Lásd a X. fejezetet.

2. Hamász

A Hamász a fókuszát az Izraellel való feszültségről a népe túlélésére helyezte. Március 22-én a katonai szárnyával, az al Quds Brigade-al lefertőtlenítette az utcákat, és betiltotta az összes nyilvános gyülekezést és a pénteki imákat. A Hamász vezető Ismail Haniyeh az „izraeli ostrom teljes befejezésére" szólított fel a Gázai övezetben, hogy kaphassanak nemzetközi támogatást. Katarhoz és Törökországhoz fordult humanitárius segítségért. Haniyeh azt nyilatkozta, hogy a Hamász hajlandó „részleges engedményekre" fogolycserék tekintetében, az Izrael által fogvatartott idősebb foglyok és betegek szabadon bocsátása érdekében. Május 5-én a Hamász szerint nem történt jelentős előrelépés a fogolycsere-tárgyalások ügyében.[812]

3. Hezbollah

A Hezbollah reakciója kezdetben gyorsabb és alaposabb volt, mint a libanoni állami intézményeké. Közel 25.000 egészségügyi dolgozót és több mint 100 járművet vetett be a COVID-19 betegek kezelésére, és számukra ágyakat tartott fenn a beiruti kórházában. Az ország síita lakta déli részén fertőtlenítette az utcákat és ételt osztott. A harcosai Iránba utaztak és ételt osztottak és fertőtlenítették az utcákat Qom városában. A koronavírus Libanonba való behozatalával kapcsolatban a Hezbollah politikai ellenfelei a csoport kapcsolatait okolták iráni tisztiselőkkel. Március 11-én a Hezbollah karanténba helyezett legalább négy szenior vezetőt. A főtitkár, Hassan Nasrallah önkéntes karanténba vonult. Március 13-án televíziós beszédében Nasrallah azt nyilatkozta, a

[811] BELLINGER, N. – KATTELMAN, K.: How the coronavirus increases terrorism threats in the developing world. The Conversation. (2020, May 26). https://theconversation.com/how-the-coronavirus-increases-terrorism-threats-in-the-developing-world-137466 (2021.10.04.)

[812] Uo.

krízis „nem az állás rendezésére és civakodásra való” Libanon vallási felekezetei között.[813]

4. Tálibok

A Tálibok, akik a háború szaggatta Afganisztán 70%-át kontrollálják[814], teljes egészségügyi védőfelszerelésben, AK-47-esekkel felszerelve workshopokat tartottak a vírus megállításáról. Tesztelnek is, és a gyanús eseteket karanténba is helyezik, továbbá szabad áthaladást ajánlottak az egészségügyi dolgozóknak és Afganisztánban a koronavírus terjedésének megállításán dolgozó NGO-knak.[815]

5. Szélsőjobboldali reakciók

A szélsőjobboldali csoportok aktívak online az összeesküvés-elméletek, a dezinformáció, kisebbségek, kritikus infrastruktúra és Szövetségi Válságkezelési Ügynökség elleni erőszak promótálása terén. Betiltott csoportok a rendőrség és a zsidó közösség elleni támadásokra szólítottak fel. A specifikus célpontok és támadási módszerek azonosítása tekintetében szélsőjobboldali chat csoportok még tovább is mentek, mint a szalafista dzsihadista csoportok. Technikáik közé tartozik a testnedvekkel teli spray, a vírus terjesztése köhögéssel, vagy üzletekben, tömegközlekedésen a felületek érintése. A jobboldali extrémisták kifejezetten aktívak a közösségi médián, élükön az „akceleracionalistákkal” („accelerationists”) akik úgy vélik, az erőszakos cselekedetek felgyorsíthatják az általuk globálisan összekapcsoltnak és degeneráltnak tartott társadalom elkerülhetetlen összeomlását.[816] A Telegram-on, Gab-on, és chan fórumokon, továbbá a mainstreamebb platformokon, mint az Instagram, Facebook, és Twitter szélsőjobboldali csoportok és egyének öszeesküvés-elméleteket terjesztenek, dezinfomációval mélyítik a pánikot és az elégedetlenséget, és támadásokra

[813] Uo.

[814] ULLAH, R.: The Coronavirus, the War on Terrorism, and the Taliban in Afghanistan. Review Of Human Rights, 2020. Vol. 6. No. 1. 43. o.

[815] KUMAR, R.: Taliban launches campaign to help Afghanistan fight coronavirus. Al Jazeera. (2020, April 6). https://www.aljazeera.com/news/2020/04/taliban-launches-campaign-afghanistan-fight-coronavirus-200406055113086.html (2021.10.05.)

[816] WITHER, J. K.: The COVID-19 Pandemic: A Preliminary Assessment of the Impact on Terrorism in Western States. Occasional Paper Series, 2020. No. 33. 3–4. o.
https://www.marshallcenter.org/en/publications/occasional-papers/covid-19-pandemic-preliminary-assessment (2021.10.05.)

hívnak fel – közvetlen erőszakra, vagy a vírus biológiai fegyverként való használatára.[817] A legaggasztóbb a tényleges támadásokra való felhívás: A fertőzötteknek meg kellene "látogatni a helyi zsinagógát és megölelni annyi zsidót, amennyit csak lehetséges", írja egy online poszt. Egy másik: „Köhögj a helyi kisebbségedre." Egy másik kritikus infrastruktúra elleni támadásra buzdít: „Köhögj a helyi tömegközlekedéseden."[818] A mainstream közösségi média cégek már gyakorlottak az egyértelműen terrorizmushoz fűződő tartalmak eltávolításában, és jelenleg együtt dolgoznak a pandémiához fűződő dezinformáció elleni harcon[819], de az extrémisták kihasználják a közegészségügyi dezinfomáció szürkezónáját, amit nem fednek le a közösségi média korlátozásai.[820]

Egy koronavírusos betegeket kezelő Missouri állambeli kórház ellen tervezett támadást tervező férfi 2020. március 24-én meghalt az FBI-al való tűzharc során, amikor megpróbálták letartóztatni Belton-ban. A férfit rasszista és kormányellenes nézetek motiválták és több célpontot fontolgatott, mielőtt a kórház mellett döntött. Hónapok óta megfigyelés alatt állt, ami alapján potenciálisan erőszakos extrémistaként" azonosították.[821]

2020. április 1-én egy oldal felhasználói egy philadelphiai zsidó iskola tanulóinak Zoom óráit antiszemita zaklatását tervezték, Zoom linkeket és az online órák órarendjét kiposztolva és másokat az ebben való részvételre bátorítottak. Ahogy több a virtuális meeting, a jobboldali extrémisták adaptálódtak a megfélemlítő és zaklató kampányaikkal azok környezetéhez.

---

[817] KATZ, R.: The Far-Right's Online Discourse on COVID-19 Pandemic. SITE Intelligence Group. https://ent.siteintelgroup.com/index.php?option=com_acymailing&ctrl=archive&task=view&mailid=20576&key=4lfGcEyn&subid=1472-t9ir9gm3ghmVr7&tmpl=component (2021.10.05.)

[818] WEIMANN, G. – MASRI, N.: The Virus of Hate: Far Right in Cyberspace. International Institute for Counter Terrorism, Herzliya, 2020, 12. o. https://www.ict.org.il/images/Dark%20Hate.pdf (2021.10.05.)

[819] EAS Special Report, COVID-19 Disinformation. EUvsDisinfo. (2020, March 19). https://euvsdisinfo.eu/eeas-special-report-disinformation-on-the-coronavirus-short-assessment-of-the-information-environment/?highlight=special-report-%20disinformation-on-the-coronavirus-short-assessment-of-the-information-environment%2F (2021.10.05.) Idézi: WITHER: i.m. 3–4. o.

[820] MALIK, N.: Self-Isolation Might Stop Coronavirus, but It Will Speed the Spread of Extremism. Foreign Policy. (2020, March 26). https://foreignpolicy.com/2020/03/26/self-isolation-might-stop-coronavirus-but-spread-extremism/ (2021.06.21.) Idézi: WITHER: i.m. 3-4. o.

[821] Coronavirus: Man planning to bomb Missouri hospital killed, FBI says. BBC. (2020, March 26). https://www.bbc.com/news/world-us-canada-52045958 (2021.10.05.)

5. Fokozott sebezhetőség az online radikalizációval szemben a karantén idején

A Covid-19 pandémia a „social distancing" (Magyarul nagyjából társas vagy társadalmi távolságtartásnak felel meg.[822]) szabályok és a zárlatok miatt a digitális technológiák használatának megugrásához vezetett. A járvány terjedésével zárlatot vezettek be, leállítva az olyan tevékenységeket, melyekhez fizikai formában történő gyülekezés és interakció szükséges. A többség ezért az internethez és internet alapú szolgáltatásokhoz fordult, a kommunikáció és otthoni munkavégzés érdekében. A zárlat előtti számokhoz képest az internetes szolgáltatások használatában 40 és 100% közötti növekedés látszik. A videokonferencia szolgáltatások, mint a Zoom használata tízszeresére nőtt.[823] A pandémia felgyorsította a digitális világ felé való elmozdulást.[824] Az emberek több időt töltenek az interneten. Otthonrekedt milliók fordulnak közösségi média felé. Logikus, hogy a zárlat idején az online radikalizációnak emiatt is magasabb a kockázata. A „self-isolation" (önizoláció) fokozza az extrémizmus, a szélsőséges nézetek terjedését.[825] A pandémia komoly hatással volt a kiberbűnözésre is. Ez időszakban az online csalás, a zsarolóvírusok és az álhírek terjesztése is jelentős növekedést mutatott. Továbbá számottevően megnőtt a gyermekpornográfiával összefüggő bűncselekmények száma is, és az illegális termékek dark webes kereskedelme is.[826]

Rendkívül veszélyes elegyet alkotnak a növekvő gazdasági problémák, nemzetközi feszültségek, a kormányzatok intézkedéseivel való elégedetlenségek, a társadalmi feszültségek, és további konfliktus-források, például a fokozódó migrációs[827] nyomás

---

[822] ALBERT F. – DÁVID B. – HUSZTI É.: Magyar kutatók figyelmeztetnek: vigyázzunk, nehogy a távolságtartás elszigetelődéshez vezessen! Qubit. (2020. március 26.) https://qubit.hu/2020/03/26/magyar-kutatok-figyelmeztetnek-vigyazzunk-nehogy-a-tavolsagtartas-elszigetelodeshez-vezessen?fbclid=IwAR1oEzqUq_g0DZZ-XYQSQYX1gTM87IXIzE2SidLsQ9QspXRg5nxE3Wga7VU (2021.10.05.)

[823] DE', R. – PANDEY, N. – PAL, A.: Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice. International Journal of Information Management, 2020. Vol. 55. No. 1. 1. o.

[824] Covid 19 and E-commerce: Findings from a survey of online consumers in 9 Countries. United Nations UNCTAD, 2020. 4. o. https://unctad.org/system/files/official-document/dtlstictinf2020d1_en.pdf (2021.10.05.)

[825] MALIK, N.: Self-Isolation Might Stop Coronavirus, but It Will Speed the Spread of Extremism. Foreign Policy. (2020, March 26). https://foreignpolicy.com/2020/03/26/self-isolation-might-stop-coronavirus-but-spread-extremism/ (2021.10.05.)

[826] DORNFELD L.: A koronavírus-járvány hatása a kiberbűnözésre. In Medias Res, 2020/2. 204. o.

[827] A migrációs útvonalakról: BESENYŐ J.: Migrációs útvonalak. In: BESENYŐ J. – MILETICS P. – ORBÁN

Törökországon keresztül.[828] A világjárvány és az ahhoz kötődő korlátozások miatti általános mentális közhangulat a mindennapi életre erőteljesen rányomta a bélyegét.[829] A pandémia az emberek mentális egészségére is hatással van.[830]

Utalnak arra jelek, hogy a gyakran társadalmilag elszigetelt magányos terroristák esetében egyes mentális zavarok előfordulási aránya magasabb a csoportban tevékenykedő terroristákhoz és az általános népességhez képest.[831] Trimbur et al. szakirodalmi áttekintése során 2.856 dokumentumot és 25 cikket vizsgált, melynek eredményeként nem tudtak szignifikáns összefüggést azonosítani a radikalizálódás, a terrorizmus és a pszichiátriai rendellenességek között. Egyes kutatások azonban azt sugallják, hogy magas a pszichiátriai rendellenességek aránya a radikalizált személyek és a magányos terroristák között. A témát illető további vizsgálatokra van szükség.[832] A magányos farkas elkövetők mentális egészsége is nagyobb eséllyel romlik a világjárvány alatt, és főleg a közösségi média felületein rendkívül magas a radikalizálódás veszélye.[833] Ezek az egyre feszültebb emberek például 3D nyomtatóval egyre könnyebben, és a hatóságok tudomása nélkül gyárthatnak maguknak fegyvert. Ezek a tényezők számos új (köztük főleg incel) elkövetőt is kitermelhetnek, akár hazánkban is.

A jelenlegi és a várható társadalmi, politikai, és gazdasági körülmények optimális feltételeket biztosítanak a rossz szándékú elemeknek, köztük a szervezett bűnözői köröknek és terroristáknak a toborzáshoz, tervezéshez, műveletekhez. A bizonytalanság

---

B. (szerk.): Európa és a migráció. Zrínyi Kiadó, Budapest, 2019. 31–64. o.

[828] CRUMP, J.: Terrorism and security threat trends in 2021. Security Magazine. (2020, December 22). https://www.securitymagazine.com/articles/94219-terrorism-and-security-threat-trends-in-2021 (2021.10.05.)

[829] PÓCZIK Sz. – SÁRIK E. – VASS P. – BOLYKY O.: A COVID-19 pandémia egyes kriminológiai aspektusai. Belügyi Szemle, 2021/3. 376. o.

[830] JAVED, B. – SARWER, A. – SOTO, E. B. – MASHWANI, Z.-R.: The coronavirus (COVID-19) pandemic's impact on mental health. International Journal of Health Planning and Management, 2020. Vol. 35. No. 5. 993–996. o.

[831] MISIAK, B. – SAMOCHOWIEC, J. – BHUI¸ K. – SCHOULER-OCAK, M. – DEMUNTER, H. – KUEY, L. – RABALLO, A. – GORWOOD, P. – FRYDECKA, D. – DOM, G.: A systematic review on the relationship between mental health, radicalization and mass violence. European Psychiatry, 2018. Vol. 56. No. 1. 57. o.

[832] TRIMBUR, M. – AMAD, A. – HORN, M. – THOMAS, P. – FOVET, T.: Are radicalization and terrorism associated with psychiatric disorders? A systematic review. Journal of Psychiatric Research, 2021. Vol. 141. 214. o.

[833] CRUMP, J.: Terrorism and security threat trends in 2021. Security Magazine. (2020, december 22). https://www.securitymagazine.com/articles/94219-terrorism-and-security-threat-trends-in-2021 (2021.06.21.)

és a növekvő sérelmek vonzóvá teszik az erőszakos és radikalizálást támogató narratívákat.[834]

Egy megoldás lehetne egy új „misinformation flag" a YouTube-on és Facebookon, amivel megjelölhetők lennének a helytelen vagy káros tartalmak, továbbá ellen-narratívák is használhatóak extrémista tartalmak ellen. Csak a közösségi média cégek általi meggondolt, koordinált és proaktív válasszal lehet a dezinformációval szemben fellépni.[835]

A Polarization and Extremism Research Innovation Lab felsorolja az online történő radikalizáció leggyakoribb módjait. Rámutat arra, hogy a pandémia növelte az online radikalizáció kockázatát, miközben fokozta a sebezhetőséget és a hajtóerőket, amelyek a fiatalokat fogékonyabbá teszik a szélsőséges narratívák és az őket célba vevő toborzókkal szemben. A PERIL a következő okokat jelöli meg: Az online töltött idő eddig példa nélküli szintre nőtt. A szülők és gondviselők figyelme elterelt. Az otthoni digitális oktatás kockázatokkal is jár. Csökkent szocális támogatás a felnőttektől. Elzártság az olyan egyénektől, akik az új hiedelmeiket megkérdőjeleznék. Bizonytalanség és veszteség. Bűnbakkeresés és leegyszerűsített válaszok. Néhány extrémista csoport kihasználja a COVID-19-et, mint PR-lehetőséget, és közösségi szolgálatot végeznek, hogy enyhítsék a róluk alkotott képet, és ezáltal szélesítik a támogatói bázisukat. Új extrémista tartalmak keringenek.[836]

6. A koronavírus hatása a terroristák internethasználatára

Az ENSZ Terrorizmus Elleni Bizottsága az információs és kommunikációs technológia és a terrorizmus kapcsolatában 2021-ben a következő trendekre világít rá: a terroristák és erőszakos extrémista csoportok arra törekedtek, hogy az online egyre jobban

[834] HOLT, C. – BRANIFF, W. – SMITH, J.: In the Eye of the Storm: An Update: Managing Terrorism and Asymmetric Threats during Covid-19. CHC Global & START, 2020. 4. o. https://www.start.umd.edu/sites/default/files/publications/local_attachments/IntheEyeoftheStorm.pdf (2021.06.21.)

[835] MALIK, N.: Self-Isolation Might Stop Coronavirus, but It Will Speed the Spread of Extremism. Foreign Policy. (2020, March 26). https://foreignpolicy.com/2020/03/26/self-isolation-might-stop-coronavirus-but-spread-extremism/ (2021.10.05.)

[836] Building Resilience & Confronting Risk In The Covid-19 Era: A Parents & Caregivers Guide To Online Radicalization. PERIL & Southern Poverty Law Center. 5. o. https://www.splcenter.org/sites/default/files/splc_peril_covid_parents_guide_jan_2021_1.pdf (2021.10.05.)

jelenlévő globális népességet virtuális felületeken kitegyék a propagandájuknak. Sok platform küszködött a megnövekedett forgalom kezelésével, főleg az olyanok, amelyeknek kevésbé szigorú a tartalom-moderáló politikája. Ez még jobban kitette azokat a terroristák és más extrémisták általi kihasználásnak. Az online terjedő összeesküvés-elméletek miatt a nagy tech platformok felvették a harcot a dezinformáció (misinformation/disinformation) ellen azzal is, hogy kiterjesztették az akcióikat a szélsőjobboldali (vagy fajilag vagy etnikailag motivált) terrorista csoportok ellen is. Ezek az intézkedések aggodalmat kelthetnek az online kifejezés szabadsága tekintetében. Egyre elterjedtebb a cybercrime, köztük az identitáslopás, DDoS támadás, zsarolóvírus (ransomware) támadások. Több adat szükséges ennek a pandémiához kötődő intézkedések és trendekhez való kapcsolatának felfejtéséhez. Az ENSZ Terrorizmus Elleni Bizottsága a következő potenciális hosszútávú hatásokra mutat rá: A nagy közösségi média platformok ellenintézkedései következtében a terroristák és erőszakos extrémisták és platformjaikat vesztett egyének olyan kisebb felületekre vándorolhatnak, amelyek kevésbé képesek felügyelni a tevékenységeiket. (Ez már egy évek óta létező jelenség.) Az ilyen ellenintézkedések a dark web felé fordulásra is sarkallhatnak, ami a tagállamoknak további kihívást jelenthet a megfigyelés terén. A platformokról való eltávolítás növelheti az egyének társadalmi kirekesztettség érzését, ami növelheti a terroristák retorikájával és propagandájával szembeni fogékonyságukat. Az információs és kommunikációs technológia terroristák általi felhasználásával szemben alternatív narratívákat, társadalmi ellenállóságot és társadalmi befogadást előmozdító holisztikus megközelítés ajánlott, a médiában való olvasottság és a mentális egészség szolgáltatások fejlesztésével.[837]

7. Következtetések

Fontosnak tartom a koronavírus bűnözésre, terrorizmusra gyakorolt hatásának vizsgálatát.

Úgy vélem, a terrorista fenyegetés szempontjából nagy kockázatot jelent a COVID-19-pandémia. A terroristák kihasználhatják a világszinten megváltozott helyzetet, az állami

[837] Update on the impact of the COVID-19 pandemic on terrorism, counter-terrorism and countering violent extremism. United Nations Security Council Counter-Terrorism Committee Executive Directorate, 2021. 7. o. https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jun/cted_covid_paper_15june2021_1.pdf (2021.09.30.)

szervek leterheltségét és az esetleges ebből adódó biztonsági réseket terrorcselekmények elkövetésére, ezért a járvány idején (is) rendkívül komolyan kell vennünk a terroristák jelentette fenyegetést, és nyomon kell követni a kommunikációjukat minden létező általuk használt platformon a jövőbeli terrorcselekmények megakadályozása érdekében.[838] Rendkívül fontos lenne a terrorizmust erősítő körülmények enyhítése, az online terrorista és extrémista tartalmak, és a radikalizáció megfékezése is, melynek a kockázata jelen krízishelyzetben rendkívül magas.

[838] SERBAKOV M. T.: Kriminalitás a dark weben: illegális piacok, pedofil oldalak, terroristák és az ellenük való küzdelem. Büntetőjogi Szemle, 2020/1. 104. o.

XVI. A TERRORIZMUS ELLENI KÜZDELEM ÉS A TERRORCSELEKMÉNYEK MEGELŐZÉSÉNEK EGYES ELMÉLETI KÉRDÉSEIRŐL, KÜLÖNÖS TEKINTETTEL AZ INTERNETHEZ KÖTŐDŐ MEGELŐZÉSI MÓDSZEREKRŐL

1. A terrorizmus elleni harc eszközei

A terrorizmus elleni küzdelem négy legfontosabb szakterülete a politikai, katonai, igazságügyi és pénzügyi.[839] Három alkotóeleme van: a terrorizmus-elhárító tevékenyég, mely a sebezhetőség csökkentésére irányul (antiterrorism); a megelőzést célzó terrorizmus-felszámoló tevékenység (counter-terrorism); és a kialakult helyzet kezelését és a stabilitást célzó következménykezelő tevékenyég (consequence management).[840]
Az ENSZ kábítószerrel és bűnözéssel fogalakozó bécsi irodájának Terrormegelőző Csoportjának 2001-es listája szerint a terrorizmus elleni harc politikai, kormányzati; gazdasági és szociális; pszichológiai-kommunikációs-oktatási; katonai; bírósági és jogi; rendőrségi és büntetés-végrehajtási; titkosszolgálati és egyéb (pl.: bevándorlással kapcsolatos intézkedések) eszközökből áll.[841]
Vadai szerint az antiterrorista stratégia legfontosabb lehetséges elemei: a terrorizmust kiváltó feszültségek megszüntetése; biztonsági erők létszáma, kiképzettsége, technikai felszereltségének erősítése; a társadalmi mozgástér kockázatainak csökkentése; a társadalom tagjainak fokozott ellenőrzése; a média ésszerű önkorlátozása; különleges antiterrorista törvények bevezetése; nemzetközi összefogás erősítése; a potenciális terrorista célpontok fokozottabb védelme; a terroristák anyagi bázisának eliminálása; és

[839] VASS Gy.: Egységes meghatározás a terrorizmusra. Hadtudományi Szemle, 2009/4. 10. o.

[840] SZABOLCS O. (szerk.): Nemzetközi küzdelem a terrorizmus ellen: (A 2004. november 6-án rendezett országos konferencia előadásai). A Történelemtanári továbbképzés kiskönyvtára XXXVI. ELTE BTK – MTTTT, Budapest, 2005. 22–23. o.

[841] SCHMID, A. P.: Towards Joint Political Strategies for De-legitimising the Use of Terrorism. In: SCHMID, A. P.: (szerk.): Countering Terrorism through International Cooperation. ISPAC, Milánó, 2001. 266–273. o. Idézi: TÁLAS P. – PÓTI L. – TAKÁCS J.: A terrorizmus elleni küzdelem fogalmi és tartalmi keretei, különös tekintettel annak katonai dimenziójára. ZMNE Stratégiai Védelmi Kutató Központ Elemzések, 2004/3. 3. o.

a nemzeti adatbázisok egyesítése.[842]

Bolgár et al. szerint „a terrorizmus elleni harc összetett tevékenység, nemzeti és nemzetközi szinten egyaránt, mely lehetőség szerint összehangolt válságreagáló műveletek sorozata, amely politikai, gazdasági, diplomáciai, titkosszolgálati, adminisztratív, felderítő, rendőri és katonai intézkedéseket foglal magába, és nem csak a hadtudomány, de más tudományok eredményeit is felhasználja."[843]

2. A katonai fellépés

Resperger szerint a nemzetközi terrorizmus fokozódó aktivitása és veszélyessége, egyre több áldozata megköveteli a demokratikus kormányoktól és a nemzetközi szervezetektől, hogy az emberiség elleni főveszélyként küzdjenek ellene, mely csak összehangolt, egységes, a biztonság minden területére kiterjedő stratégiával lehetséges. Resperger szerint e részstratégiák egyik legfontosabb és leghatékonyabb eleme a katonai erő, melyet csak okosan, pontos felderítési adatokra támaszkodva, alaposan felkészítve a konkrét feladatra lehet felhasználni. A Magyar Honvédség nemzetközi kötelezettségeiből adódóan, válságterületeken, a konfliktus katonai megoldásában (békekikényszerítés) és a konfliktus utáni helyzetekben (békefenntartás) is alkalmazásra kerülhet, valamint hazai területen is, ezért katonáinak a terrorizmus elleni küzdelem katonai tapasztalatainak elsajátítása elengedhetetlen.[844] Wilkinson szerint, ha a katonaság kapja a domináns szerepet a terrorizmus elleni harc stratégiájának kidolgozásában, akkor az kapja majd a fő szerepet a stratégia végrehajtásában is. Wilkinson szerint az ún. military warfare model/katonai hadviselés modell alkalmazása a demokratikus kormányok számára csábító lehet, melynek előnyei: Eleget tesz a köz és média kemény fellépést követelő elvárásának. Visszatarthat a további támadásoktól és a támogatástól. Nemzetközi szinten elrettentheti az elkövetőkek, állami szponzorokat. Az ellenséges vezetés elleni pszichológiai csapás alááshatja a vezető szerepüket, vagy gyorsíthatja annak elvesztését. A stratégiai támadó hadműveletek és katonai megtorlás problémákkal és dilemmákkal is jár. Sok terrortámadás esetén nehéz vagy lehetetlen a megfelelő mennyiségű és minőségű hírszerés az elkövetők kétséget kizáró

[842] VADAI Á.: A terrorizmus a nemzetközi jogban. Egyetemi disszertáció. Budapesti Közgazdaságtudományi Egyetem, Budapest, 1997, 60. o. Idézi: KORINEK (2006): i.m. 458–459. o.

[843] BOLGÁR J. – SZTERNÁK N. – SZTERNÁK Gy.: A terrorizmussal kapcsolatos kutatások legújabb eredményei. Felderítő Szemle, 2005/4. 24. o.

[844] RESPERGER I.: Terrorista szervezetek, módszerek, eljárások. Szakmai Szemle, 2018/2. 27. o.

beazonosításához. Egy katonai támadás vagy megtorlás szélesebb konfliktust generálhat. Az ártatlan civilek halálával járó megtorlás az erkölcsi fölény és a nemzetközi közvélemény szimpátiájának elvesztésével járhat. Egy egyoldalúan véghezvitt katonai megtorlást nem biztos, hogy a fontos szövetségesek támogatnak, feszültséget kelthet a szövetségesek között, továbbá a közvéleményben fals elvárásokat ébreszthet a terrorizmus legyőzését illetően, és hasonló vagy intenzívebb katonai akció elvárásához vezethet a későbbiekben. Fennáll a jogállamot és az emberi jogok védelmét aláásó katonai túlkapás veszélye is.[845]

3. A megelőzés fontosságáról

A terrorizmus elleni küzdelemben a legfontosabb a megelőzés.

Horváth a nemzeti fellépés és a nemzetközi együttműködés fontosságát hangsúlyozza, és hogy tévedés, hogy a terrorizmusra csak katonai és rendvédelmi eszközökkel adható eredményes válasz, de „erőszak ellen erőt kell felmutatni", lehetőleg már akkor, mikor a terroristák merényletre készülnek. Legideálisabb az alvó vagy szervezkedő terrorista csoportok felderítése, és a veszély semlegesítése. A nemzetközi és nemzeti szervek és valamilyen formában a társadalom együttműködése szükséges, hogy a titkosszolgálatok felvehessék a harcot a terrorizmus ellen. Horváth azt tartaná ideálisnak, ha sikerülne a terrorizmus kiváltó okait megszüntetni, ám ez majdnem lehetetlen. Véleménye szerint a terrorizmus elleni harcnak össztársadalmivá kell válnia és komplex értelmezést kell nyernie.[846] Bartkó szerint az államnak a terroristákat érdektelenné kellene tennie a támadásaik elkövetésében, és a terrorizmust okafogyottá tevő megoldások keresését javasolja. A katonai, titkosszolgálati és egyéb eszközöket a gyűlölet fokozására képesnek tartja, ezekkel lehetetlen hosszú távon célt érni.[847] Barker szerint a terrorizmus elsődlegesen nem katonai ügynek tekintendő, hanem együttes erővel kellene próbálni javítani a körülményeken, melyekből az fakad: csökkenteni a káosz uralta területeket, és enyhíteni a nyomort a világ nagyvárosaiban. Barker a terrorizmust az emberiség elleni bűntettként kezelését javasolja, a háborúban gondolkodás helyett, mert így elkerülhető lenne a háború negatív, politikaellenes mellékhatása, a terroristák sem tetszeleghetnének hősként, ha közönséges bűnözőknek nyilvánítanák őket. Őket ugyanúgy kell üldözni,

[845] WILKINSON, P.: Terrorism versus Democracy: The Liberal State Response. Routledge, London and New York, 2006. 90–91. o.

[846] HORVÁTH (2014): i.m. 241–243. o.

[847] BARTKÓ (2011): i.m. 84–85. o.

mint más bűnözőket, le kell őket leplezni és az akcióikat megakadályozni. Nem elegendő csupán a már elkövetett terrorcselekményekre történő reakció, a megelőzéssel is foglakozni kell, és elengedhetetlen a hírszerzés fejlesztése. Barker diplomáciai erőfeszítéseket szorgalmaz a terrorizmus sújtotta területek konfliktusainak csökkentésére, esetleg végleges rendezésére. Dolgozni kell a demokrácia fenntartásán, az országos és nemzetközi gazdaság reformján, a fegyverek korlátozásán és ellenőrzésén, támogatni az alulról szervezett politikai mozgalmakat, mivel mindez enyhítheti a terrorizmushoz vezető feszültségeket.[848]

1. Terrorcselekmények megelőzése büntetőjogi eszközökkel?

Ahogy Bartkó fogalmaz: „Akár a terrorizmusra, mint kriminalitási formára, akár magára a terrorcselekményre, mint büntető anyagi jogi tényállásra fókuszálunk, a kérdés pusztán a büntetőjog világából azonban nyilvánvalóan nem közelíthető meg. Tekintettel a terrorizmus összetett természetére, valamint transznacionális jellegére, még az elsődlegesen büntetőjogi kutatást végző személynek is egyszerre kell nemzetközi jogásznak, kriminológusnak, valamint természetesen büntetőjogásznak is lennie…”[849]
A büntetőjogi eszközök önmagukban kevesek a terrorizmus ellen. Gál rávilágít, hogy az öngyilkos merénylő a jelenlegi büntetőjogi eszközökkel nem visszatartható, mert „nincs vesztenivalója”. Nem tartható vissza az elkövetéstől, még halálbüntetés kilátásba helyezésével sem, vagy ha esetleg arra is számítana, hogy lelőhetik. A legnagyobb veszteség, ami érheti, hogy nem ott és akkor hal meg, ahogy tervezte.[850] Fókuszában az ellenség mindenáron való elpusztítása áll.[851] Gál álláspontját Fábián is osztja, ő is úgy véli, hogy az új típusú terroristával szemben hatástalanok a büntetőjog eszközei, a legszigorúbb büntetések kilátásba helyezése sem jár eredménnyel.[852]
Meliá szerint nem vehető természetesnek, hogy a terrorizmus elleni harc jegyében hozott szélsőséges jogszabályok ténylegesen megakadályoznak terrortámadásokat. Történelmi tapasztalatok szerint az ilyen jogszabályok elfogadása a teljes büntetőjogot „beszennyezheti.” A végeredmény egy kíméletlenebb, a jogállam aláásásával fenyegető

[848] BARKER, J.: A terrorizmus. HVG Kiadói Rt., Budapest, 2003. 145–146. o.

[849] BARTKÓ (2011): i.m. 11. o.

[850] GÁL I. L.: A terrorizmus finanszírozása. PTE Állam- és Jogtudományi Kar Gazdasági Büntetőjogi Kutatóintézet, Pécs, 2010. 3. o.

[851] BOLGÁR – SZTERNÁK – SZTERNÁK: i.m. 18. o.

[852] FÁBIÁN P.: A terrorcselekmény büntetőjogi szabályozásának jelene és aktuális kérdései. Büntetőjogi Szemle, 2018/2. 49. o.

büntetőjog lesz.[853]

A terrorcselekmény elkövetésének minél korábbi stádiumban való megelőzése érdekében a büntetőjogi fellépés egyre preventívebb jelleget kap.[854] A terrorizmus ellen európai szinten folytatott küzdelem jegyében az Európai Parlament és a Tanács 2017. március 15-én elfogadta a terrorizmus elleni küzdelemről szóló 2017/541 Irányelvet, amely a korábbi, 2002-ben született 2002/475/IB tanácsi kerethatározatot váltja fel. Célja, hogy új kereteket adjon a terrorizmus elleni uniós küzdelemnek és szélesítse a büntetendővé nyilvánítandó cselekmények körét.[855] Az Irányelv olyan magatartások büntetendővé nyilvánítására törekszik, amelyekkel az EU sikeresebben küzdhet a terrorizmus ellen, és amelyekkel lehetséges lesz a büntetőjog eszközével kiemelni a gyanús elemeket a társadalomból még a támadásaik végrehajtása előtt (az előkészítő fázisban, vagy akár még azt megelőzően[856]). Ezen cselekményeket az Irányelv, mint a terrorizmussal összefüggő bűncselekményeket határozza meg.[857]

4. Dilemmák a terrorizmus elleni fellépést illetően

Fábián rávilágít arra, hogy az elmúlt években szinte eltűntek az olyan terrorcselekmények, ahol az elkövetők pl. emberrablás vagy gépeltérítés során követelést terjesztettek elő. A terrorizmus ugyanakkor egyre radikálisabb, kegyetlenebb és szervezettebb. Úgy véli, nem vitatható, hogy a terrorcselekmények egyre kevesebb szervezést, egyre kisebb financiális forrást igényelnek. Fábián megállapítja, hogy

---

[853] MELIÁ, M. C.: Terrorism and Criminal Law: The Dream of Prevention, the Nightmare of the Rule of Law. New Criminal Law Review, 2011. Vol. 14. No. 1. 122. o.

[854] SIEBER, U. – VOGEL, B.: Terrorismusfinanzierung: Prävention im Spannungsfeld von internationalen Vorgaben und nationalem Tatstrafrecht. Duncker & Humblot, Berlin, 2015. 1. o. Idézi: NEPARÁCZKI A. V.: A terrorizmus finanszírozása bűntettének szabályozása a nemzetközi elvárásokra figyelemmel. Ügyészségi Szemle, 2017/2. 7. o.

[855] Lásd az a terrorizmus elleni küzdelemről szóló 2017/541 Irányelv Preambulumának (2) bekezdését. Idézi: BARTKÓ R. – SÁNTHA F.: Az Európai Unió jogalkotása és hatása a terrorcselekmény hazai büntetőjogi szabályozására. In: HOMOKI-NAGY M. – KARSAI K. – FANTOLY Zs. – JUHÁSZ Zs. – SZOMORA Zs. – GÁL A. (szerk.): Ünnepi Kötet Dr. Nagy Ferenc Egyetemi Tanár 70. Születésnapjára. Balogh Elemér dékán, Szeged, 2018. 83. o.

[856] BARTKÓ R.: Az Unió 2017/541. Sz. Irányelvének hatása a V4 országainak büntető anyagi jogszabályalkotására. In: BARTKÓ R. (szerk.): A terrorizmus elleni küzdelem aktuális kérdései a XXI. században. Gondolat Kiadó, Budapest, 2019. 138. o.

[857] BARTKÓ – SÁNTHA: i.m. 83. o.

jellemzően olyan magatartásformákkal és olyan „eszközbűncselekmények” és előkészítő cselekmények révén valósultak meg az elmúlt évek terrorcselekményei, amelyeket korábban nem tipikusan ilyen cselekményként definiált sem a jogalkotó sem a bűnüldöző szervek. A szerző szerint teljesen új szemléletre van szükség a jogalkotók részéről, megteremteni annak a lehetőségét, hogy a terrorcselekmény meghatározás során nem csupán és nem jellemzően az elkövetői cselekmény önálló jellegét és tárgyát vizsgáljuk, hanem főként annak célzatát és eredményét. Továbbá nagyobb és szélesebb felhatalmazást kell adni a nyomozó hatóságoknak és titkosszolgálati szerveknek, és a bevándorlás politika is szigorúbb szabályozást igényel. Fábián a magánbiztonság vonatkozásában is jogalkotói, jogalkalmazói feladatot lát a kérdéskörben. Az elmúlt 4-5 év során elkövetett terrorcselekmények alapján megállapítható, hogy azok tipikusan a magánbiztonsági szektort érintő tömegrendezvényeken történtek. E tárgykörben a fizikai, helyi megelőzés tekintetében korábban nem ismert tárgykörben és vertikumban merül fel a magánbiztonságban dolgozó cégek és szakemberek felkészítésével, munkájával és a hivatásos szervekkel való együttműködésük kereteivel kapcsolatos jogi szabályozás szükségessége.[858]

Korinek szerint a szélsőségek sem jogi, sem politikai eszközökkel nem számolhatók fel teljesen, a polgári demokráciák alapvető jellemzőit tekintve a terrorizmus elleni harc befejezhetetlen. Öngerjesztő folyamat jöhet létre, ha az állam hagyja magát provokálni. A terrorizmus elleni harc drága, és óhatatlanul együtt jár számos szabadságjog korlátozásával. A kényszerből hozott ún. antiterrorista törvények „szükségképp diszkriminatívak” és az alkotmányos szabadságjogokat erősen csorbítják.[859] Radai és Vajda szerint: „A terrorizmus elleni küzdelem szükségszerűen együtt jár az emberi jogok korlátozásával. A megfelelő „harchoz”, megfelelő eszközök kellenek, s ezek nem léteznek áldozatok nélkül.”[860] „(…) Felvetődik tehát a tragikus kérdés, a társadalom az államnak vagy a terrorizmusnak szolgáltassa-e ki magát? A cselekvések eredményeinek ambivalenciája megteremti a 22-es csapdáját. A terrorizmus, az állam bármelyik utat is választja az ellene való fellépésben, szükségszerűen eléri a célját.”[861] Csányi szerint a jogállamiságnak még a veszély idején hűnek kell maradnia az elveihez. Az erős és stabil

[858] FÁBIÁN P.: A terrorcselekmény büntetőjogi szabályozásának jelene és aktuális kérdései. Büntetőjogi Szemle, 2018/2. 49–50. o.

[859] KORINEK (2006): i.m. 457–458. o.

[860] RADA M. – VAJDA V.: A terrorizmus elleni küzdelem, avagy a 22-es csapdája. Külügyi Szemle, 2010/1. 148. o.

[861] Uo.151. o.

jogállam a terrortámadásokra megfelelően, arányosan válaszol. Elsősorban a túlreagálástól kell tartózkodni. A terroristák célja egy erőszakspirál megindítása, melynek a végén a terrorszervezet önkénye, mint „jogos önvédelmi intézkedés" áll az állítólagos agresszív expanziós politika ellen.[862] A háborús felfogást képviselő Carr szerint a terrorizmus –ahogy az elkövetői sokszor ragaszkodnak is ehhez – a hadviselés egy formája, és csak akkor, ha ekként ismerjük el, leszünk képesek átfogó és hatékony választ kidolgozni ellene.[863] Korinek szerint a terrorizmus esetében nem hadviselésről, háborúról van szó, hanem a „kriminalitás kiemelkedően súlyos megnyilvánulásairól."[864] Korinek azt a bűnözés megnyilvánulásának tartja, mellyel szemben érhetőek el sikerek, de a teljes felszámolása illúzió. Úgy véli: „A háborús felfogás hibája, hogy lényegéből adódóan feltételezi egy vagy több meghatározott ellenség létét, a megoldást pedig az ütközetek megnyerésétől várja. Ha azonban a társadalomban létrejövő, egészen pontosan meg nem határozott okok miatt kitermelődő megnyilvánulásnak tekintjük a terrorizmust, akkor nyilvánvalóan nem egy meghatározott személyi kör, de még nem is csupán valamely szervezet fennállásához vagy elpusztításához kell kötni a győzelmet."[865]
Bartkó szerint a terrorizmus tekintetében hazai jogalkotás is kapcsolódik az elmúlt években kialakult áramlathoz, mely szerint a terrorizmus megértéséhez az nem egyszerű köztörvényes bűncselekményként kezelendő, hanem olyan „szuperdeliktumként", amely számtalan dimenzióval rendelkezik, és az ellene való küzdelemnek is több olyan eleme van, amely karakterét tekintve a közönséges hadviseléssel mutat hasonlóságot.[866]

5. Amikor a terrorcselekmények megelőzése sikertelen

A közbiztonság garantálása mindenkori az állam feladata, melyhez rendészeti jogosítványok és eszközök széles tárháza áll a rendelkezésére, és ideális esetben képes megszervezni a közhatalmi szervei közötti hatékony együttműködést. Azonban sajnos pont a terrortámadások tekintetében nem mindig képes eleget tenni az elvárásoknak.

[862] CSÁNYI Cs.: 9/11-re adott lehetséges válaszok az Egyesült Államok és Németország példáján keresztül. Acta Humana, 2016/5. 15. o.

[863] CARR, C.: Terrorism as Warfare: The Lessons of Military History. World Policy Journal, 1996/1997. Vol. 13. No. 4. 1. o.

[864] KORINEK (2015): i.m. 11. o.

[865] Uo. 34.

[866] BARTKÓ R.: A terrorcselekmény tényállásának értékelése az uniós követelmények tükrében. Belügyi Szemle, 2015/7-8. 39. o.

Többször szólnak arról a hírek, hogy az elkövető korábban már a hatóságok előtt ismertté vált, ám vagy az elégtelen információfeldolgozás, vagy a különböző szervek (rendőrség, nemzetbiztonság) közötti információáramlás hiánya, netán a köztük lévő rivalizálás miatt senki nem akadályozta meg a végrehajtásban.[867] Ezt a jelenséget magam is komoly megoldandó problémának tartom.

A megelőzés sikertelenségre számos példa hozható:

9/11- előtt az al-Kaidának olyan szervezési és logisztikai feladatokat hajtott végre, amelyek Horváth szerint elgondolkodtatóak. A terrorszervezetnek az alapos tervezés mellett egy Afganisztánból kiinduló az Egyesült Arab Emirátusokon és Németországon át az USA-ig átívelő finanszírozási, támogatási, kiképzési rendszert kellett kiépítenie, és hónapokon keresztül több országban 18 támogató napi ellátását, konspirációját, utaztatását, felderítését és pilótakiképzését kellett megoldania. Az eset rámutatott a figyelmeztető jelek és információk kezelésének és rangsorolásának fontosságára. Horváth szerint ennyi jel nem hagyható „büntetlenül" figyelmen kívül. 9/11 a biztonsággal összefüggő preventív szabályozásban, például az információcserében, a nemzetközi jog területén, a pénzügypolitikában és számos más területeken alapvető változásokat hozott.[868]

A Stormfront fórumon 2008-ban Breivik amellett érvelt, hogy Nagy-Britannia polgárháborúval néz szembe a muszlim bevándorlás miatt. 2011. július 22-én 77 embert ölt meg az Oslo belvárosában és Utøya szigetén elkövetett terrortámadás során, Norvégiában. Röviddel a támadása előtt egy 1500 oldalas manifesztumot posztolt a Stormfront-ra, és ezreknek küldte el e-mailben.[869]

Bowers, aki 2018. október 27-én a Tree of Life zsinagógában nyitott tüzet, gyakran posztolt antiszemita összeesküvés-elméleteket egy extrémista közösségi oldalra, a Gab-ra.[870]

Tarrant írt előítéletes kijelentéseket jobboldali extrémista oldalakra, mint világszerte sokan mások, és manifesztuma az elkövetését olyan kevés idővel előzte meg, hogy a bűnüldöző szerveknek nem volt ideje azt megakadályozni 2019. március 15-én. Ezért

[867] FÁBIÁN P.: Terrorcselekmények és a magánbiztonság kapcsolatának aktuális összefüggései. Magyar Rendészet, 2018/4. 99. o.

[868] HORVÁTH (2014): i.m. 209. o.

[869] KLEINBERG, B. – VAN DER VEGT, I. – GILL, P.: The temporal evolution of a far-right forum. Journal of Computational Social Science, 2021. Vol. 4. No. 1. 1–2. o.

[870] BECKETT, L.: Pittsburgh shooting: suspect railed against Jews and Muslims on site used by 'alt-right'. The Guardian. (2018, October 27). https://www.theguardian.com/us-news/2018/oct/27/pittsburgh-shooting-suspect-antisemitism (2021.10.11.)

Battersby és Ball szerint, hacsak nem kerül napvilágra a szándékára mutató új információ, addig nem megalapozott az állítás, hogy a szervek hanyagsága miatt nem került felfedezésre.[871] Ugyan nem sikerült korábban az elkövetőről információt szerezni, de a rendőrségi reakció gyors volt, és az ellenállását hamar legyőzték és letartóztatták.[872]

A halle/saale-i terrortámadással kapcsolatban a német rendőrséget a zsidó közösség kritizálta, amiért az nem volt képes megvédeni a zsinagógát.[873] Az elkövetés jom kippur idején történt, de a rendőrség nem volt tisztában a zsidó ünneppel, ezért a napra a zsinagógának nem volt különleges védelmi koncepciója (azt a zsidó közösség sem követelte).[874]

6. A titkosszolgálatok kitüntetett szerepéről a megelőzés terén

Finszter szavait idézve: „Nem véletlen, hogy a terrorizmus és a szervezett bűnözés elleni küzdelmet gyakran nevezik bűnügyi hírszerzésnek, jelezve, hogy az ilyen típusú deliktumok felderítésében csak a titkosszolgálati eszközök lehetnek eredményesek."[875]

Boda szerint a nemzetközi terrorizmus elleni hatékony fellépéshez nemzetközi összefogás szükséges, a felderítés és a hírszerzés pedig a megelőzés leghatékonyabb eszköze, a terrorszervezeteket a finanszírozási forrásaiktól el kell vágni, és fel kell készülni a támadások megelőzésére és megakadályozására.[876] Nemzetbiztonsági szempontból a nemzetközi összefogás sokat jelent a nemzetközi terrorizmus ellen, de annak fenyegetése az IS felszámolása után sem fog eltűnni.[877]

---

[871] BATTERSBY, J. – BALL, R.: Christchurch in the context of New Zealand terrorism and right wing extremism. Journal of Policing, Intelligence and Counter Terrorism, 2019. Vol. 14. No. 3. 6. o.

[872] CROTHERS – O'BRIEN: i.m. 248. o.

[873] German police criticised over Halle synagogue shootings. Financial Times. https://www.ft.com/content/d22459c8-eb42-11e9-a240-3b065ef5fc55 (2021.10.11.)

[874] Polizei war jüdischer Feiertag Jom Kippur nicht bekannt. Spiegel. (2020, Juni 10). https://www.spiegel.de/panorama/justiz/halle-anschlag-auf-synagoge-polizei-war-juedischer-feiertag-nicht-bekannt-a-7ef5bd6e-c38b-40ea-80d1-ac005a322338?fbclid=IwAR3wi7DOh10WstBd_muQ_peQxHla0To5kHmRqeWbccAmvSU1iKyOrK-qtqQ (2021.10.11.)

[875] FINSZTER G.: Rendészettan. Dialóg Campus Kiadó, Budapest, 2018. 78. o.

[876] BODA (2007): i.m. 47. o.

[877] BODA J.: A XXI. század nemzetbiztonsági kihívásai. In: GAÁL Gy. – HAUTZINGER Z. (szerk.): Pécsi Határőr Tudományos Közlemények XX.: A XXI. század biztonsági kihívásai. Magyar Hadtudományi

Bizonyos területek, mint a terrorizmus, a határokon átnyúló bűnözés, a migráció vizsgálata egyszerre tartozik a nemzetbiztonsági szervek és a bűnüldöző hatóságok feladatkörébe, az egyes területeken belül akár több szerv is végezhet egyidőben titokban információgyűjtést. Leginkább a felek konszenzusteremtő képességén múlik az együttműködés, az adatcsere. Szükséges egy közös szervezet, amely képes lehet valamennyi érintett szerv adattartamának elérésére és feldolgozására.[878]
A biztonsági szolgálatok csak az olyan gyanúsítottakat figyelhetik meg, akikről tudnak. A többiek felfedezetlenek maradnak, amíg le nem csapnak. Lehetetlen mindet azonosítani, mielőtt támadnak, ezért lehetetlen minden potenciális célpontot megvédeni. A biztonsági erők legnagyobb törekvései ellenére néhány támadás végül át fog csúszni, és sikeres lesz.[879]
A nemzetbiztonsági szolgálatok titkos információgyűjtését elősegíti a társszolgálatokkal és a nemzetközi szervezetekkel (NATO, EU, ENSZ, EBESZ) történő kooperáció és a bilaterális kapcsolatok.[880] 9/11-, majd az azt követő európai terrorcselekmények hatása a titkosszolgálatokra részben abban öltött testet, hogy jelentős politikai támogatás és elvárás mellett mind nemzeti, mind nemzetközi szinteken erősödött az együttműködés. Az érdemi, konkrét adat- és tapasztalatcserét lehetővé tevő multilaterális szervezetek megszaporodtak, létrejöttek a közös nemzetközi adatbázisok alapjai is. A nemzeti szintű információ-megosztásban rejlő kockázatok felismerése vezetett a NATO/EU tagállamok ún. (terrorellenes) fúziós vagy koordinációs központok létrehozásához. Magyarországon ennek jegyében jött létre 2003-ban a Terrorellenes Koordinációs Bizottság (TKB). Munkáját 2010-ig a Nemzetbiztonsági Hivatal, majd az után a Terrorelhárítási Központ (TEK) hangolja össze, tagja a terrorellenes küzdelemben érintett valamennyi rendőri és nemzetbiztonsági szervezet.[881] Az intézményi rendszer reformja nélkül a jövőben nem képzelhető el hatékony terrorellenes fellépés. Az önálló, fúziós központként funkcionáló

Társaság Határőr Szakosztály Pécsi Szakcsoportja, Pécs, 2018. 10. o.

[878] URBÁNYI A.: Nemzetbiztonsági vs. Bűnügyi felderítés – a megszerzett információkkal való gazdálkodás kérdései. Szakmai Szemle, 2019/4. 28. o.

[879] KIS-BENEDEK J.: The Islamic State and the intelligence. Nemzetbiztonsági Szemle, 2015/különsz. 47. o.

[880] RESPERGER I.: A nemzetbiztonsági szolgálatok tevékenysége – biztonsági kihívások, kockázatok és fenyegetések. In: RESPERGER I. (szerk.): Nemzetbiztonsági alapismeretek. Dialóg Campus Kiadó, Budapest, 2018. 31. o.

[881] KOVÁCS Z. A.: A polgári elhárítás negyedszázada (1990–2016). In: DRUSZA T. (szerk.): A magyar elhárítás fejlődése: Tanulmányok a katonai és polgári nemzetbiztonsági elhárítás múltjáról, jelenéről, jövőjéről. Dialóg Campus Kiadó, Budapest, 2019. 169–170. o.

terrorelhárítási szolgálat felállítása tekintetében Magyarország sok tekintetben példaértékű.[882]

Egyetértek Kis-Benedek és Kenedlivel: „Véleményünk szerint Európában, így Magyarországon is az ilyen típusú terrorizmus terjedésének megállítása és ellenőrzés alá vonása érdekben két fő területen kell lépéseket tenni a közeljövőben. Egyrészt meg kell állítani a terrorgyanús személyek határokon átnyúló mozgását, és ezzel egyidejűleg szükséges megakadályozni az iszlám ultrakonzervatív szunnita értelmezését valló, szalafita terrorista propagandának kitett személyek – főként fiatalok – radikalizálódását különféle intézkedésekkel."[883] Ehhez az értékes javaslathoz úgy vélem, szükséges hozzátenni, hogy a más típusú terrorista propaganda ellen is szükséges felvenni harcot.

7. A terrrocselekmények megelőzésének internethez kötődő módszerei

Egyetértek Molnárral: „Mint mindenre, így a bűnmegelőzésre is igaz, hogy csak és kizárólag folyamatos megújulás és fejlődés mellett lehet eredményes."[884]

A terrorizmus elleni harcban a hagyományos intézkedések mellett a kibertérben való védelemre és biztonságra is fokozott figyelem fordítandó. A kormányoknak és a nemzetközi szerveknek olyan intézkedéseket, szervezeti struktúrákat kell kialakítaniuk, melyek ott is lehetővé teszik a hatékony fellépést. A szolgáltatókat a nemkívánatos tartalmak, weboldalak, közösségimédia-fiókok eltávolítására folyamatosan rá kell kényszeríteni. A terrorellenes szerveknek folyamatosan monitorozniuk kell a kibertéri aktivitást, feltérképezni a weboldalakat, közösségi médiafelületeket, figyelni a rajtuk folyó információkat, és megtenni a szükséges lépéseket. A nyilvános webes aktivitás többek között ennek köszönhetően is visszaszorult, de a kibertérben mindig újabb lehetőségek nyílnak meg, és megtalálják a kapcsolattartás és kognitív befolyásolás új

[882] KASZNÁR A.: Az európai terrorelhárítás jelene és jövője. In: DRUSZA T. (szerk.): A magyar elhárítás fejlődése: Tanulmányok a katonai és polgári nemzetbiztonsági elhárítás múltjáról, jelenéről, jövőjéről. Dialóg Campus Kiadó, Budapest, 2019. 191. o.

[883] KIS-BENEDEK J. – KENEDLI T.: A terrorfenyegetettség új tendenciái és lehetséges válaszlépések. Szakmai Szemle, 2015/1. 27. o.

[884] MOLNÁR I. J.: A bűnmegelőzés értelmezése és magyarországi fejlődése. In: GAÁL Gy. – HAUTZINGER Z. (szerk.): Pécsi Határőr Tudományos Közlemények XXI.: A bűnüldözés és a bűnmegelőzés rendészettudományi tényezői. Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoportja, Pécs, 2019. 89. o.

módjait és technikáit. A hatékony terrorizmus elleni fellépés során a nemzeti és nemzetközi szerveknek, hatóságoknak a kibertér kihívásait is kezelniük kell.[885]

Alapvető nemzetbiztonsági feladat az extrémizmus elleni fellépés.[886] Az internet a rendvédelmi szervek számára is használandó kommunikációs csatornaként. A médiafigyelés kiteljesedéseként a radikalizálódó hírportálokon, fórumoldalakon rövid tanulmányokkal, hozzászólásokkal moderálni, a szélsőséges, befolyásoló propagandát, lejáratni, kiszorítani is lehet, amihez képzett, motivált állomány szükséges.[887] Egyetértek Kis-Benedekkel és Kenedlivel, hogy fontos a terrorizmus propagandájával szembeni fellépés. Különösen az online terjesztett tanok, toborzó videók felkutatása, az eredetük megállapítása és azok eltávolítása is szükséges, így megóvva a radikalizálódásra fogékonyakat.[888] Az interneten a terroristák megfigyelhetőek, a tevékenységük tanulmányozható; vannak elméletek, melyek szerint online jelenlétük valójában ellenük dolgozik. A különféle online felületek, a weboldalak és fórumok Conway szóhasználatával egy „korai figyelmeztető rendszerként" működnek a terrorcselekményeket illetően.[889] Ugyan az okostelefon is komoly „fegyver" a terroristák kezében, de azokon keresztül a titkosszolgálatok is lekövethetik őket.[890] Katona rávilágít a terrorizmus és a szervezett bűnözés elleni fellépés lehetséges stratégiáira. Ezek közül az OSINT, az emberi erőforrással végzett felderítés, az elektronikus és a nyomtatott médiumokban megjelent, valamint az internetre, közösségi oldalakra, videomegosztókra feltöltött anyagok elemzését és ezekből történő információszerzést jelenti, elsősorban a terrorizmus esetében alkalmazható. A különböző radikális nyilatkozatok felderítése a terrorcselekmény megelőzését eredményezheti.[891] Egyértelmű, hogy az internet anonimitása nem csak a terroristáknak kedvez, az lehetőséget ad fedett ügynökök beépülésére is. Például az USA-ban számos FBI-ügynöknek sikerült már

[885] HAIG (2018): i.m. 302–303. o.

[886] BOROSS Zs. A.: Humán faktor (Az emberi tényező szerepe az extrémizmus-elhárítás kérdéskörében). Nemzetbiztonsági Szemle. 2014/2. 139. o.

[887] Uo. 156. o.

[888] KIS-BENEDEK – KENEDLI: i.m. 31. o.

[889] CONWAY (2006): i.m. 21. o.

[890] MOUTOT, M.: Smartphones: a double-edged sword for terrorists. Phys.org. (2018, November 13). https://phys.org/news/2018-11-smartphones-double-edged-sword-terrorists.html (2021.10.14.)

[891] KATONA L.: A terrorizmus és a szervezett bűnözés elhatárolásának aktuális dilemmái. Felderítő Szemle, 2013/3. 70. o.

terrorszervezetekbe beépülni, és így terrortámadásokat meghiúsítani.[892] Elengedhetetlen az igazságügyi informatikai szakértők alkalmazása: „A számítógép alapú technológiák az élet egyre több területén jelennek meg. Ebből adódóan a bűnelkövetés és a bűnüldözés is egyre nagyobb számban találkozik a technológia kézzel fogható (hardver) és meg nem ragadható (szoftverek és új viselkedési minták) jellemzőivel. Ezeket a komponenseket az elkövetők hol eszközként, hol pedig egyszerű mindennapi tárgyként használják, s ily módon a cselekmények digitális lenyomatait, digitális bizonyítékait (digital evidence) hagyják maguk után. Ezek a bizonyítékok gyakran nem láthatók, vagy hétköznapi eszközökkel nem hozzáférhetők. Beszerzésükhöz, rögzítésükhöz, megőrzésükhöz és bemutatásukhoz megfelelő – a legtöbb esetben magas szintű – informatikai szakmai tudásra és gyakorlatra van szükség. Ez utóbbi képességekkel és készségekkel az igazságügyi informatikai szakértők rendelkeznek, aki a bizonyítékok feltárásával és később interpretálásával segítik a nyomozó hatóság, majd a bíróság munkáját.”[893]

Kulturális ismeret is szükségeltetik: „(…) a célterület (azaz például az adott közösség) ismerete a nemzetbiztonsági szakma eredményességét a mai napig meghatározza. Nem lehet helyes értékelést levonni anélkül, hogy ne ismernénk azt a kultúrát, társadalmat, amelyre az információ vonatkozik. És mindez a virtuális térre is igaz: nem lehet eredményes internetes kutatómunkát folytatni anélkül, hogy ne ismernénk a különböző fórumok, chatszobák, zárt közösségek belső szabályait. A szakma ma is a nemzetbiztonsági elemzés egyik jellegzetes hibájaként tartja számon azt, ha a szakember a saját kulturális beágyazottságát vetíti ki egy-egy információ értékelése során (ezt hívják „tükrözésnek”).”[894]

Ahogy Kovács rávilágít, a gép módszerek mellett, az emberi tényező fontossága nem elhanyagolható, mert „(…) a legrégibb és egyben máig legértékesebb titkosszolgálati eszköz maga az ember. (…) Egyes titkosszolgálatok a humán információszerzési képességek rovására erőteljes technikai (a kommunikációs rendszerek teljes ellenőrzésére törekvő) fejlesztéseket hajtottak végre, párhuzamosan az egyén ellenőrzéséhez szükséges, az alapjogokat korlátozó jogosítványok bővítésével. Mindez

[892] KIS-BENEDEK J.: Dzsihadizmus, radikalizmus, terrorizmus. Zrínyi Kiadó, Budapest, 2016. 195–196. o.

[893] MÁTÉ I. Zs.: A digitális bűnfelderítés gyakorlata, avagy az igazságügyi informatikai szakértő a büntetőeljárásban. In: GAÁL Gy. – HAUTZINGER Z. (szerk.): Pécsi Határőr Tudományos Közlemények XIV.: Tanulmányok „A változó rendészet aktuális kihívásai” című tudományos konferenciáról. Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoportja, Pécs, 2013. 365. o.

[894] KOVÁCS Z. A.: Adalékok az információszerzés történetéhez. In: BODA J. – REGÉNYI K. (szerk.): A hírszerzés története az ókortól napjainkig. Dialóg Campus Kiadó, Budapest, 2019. 10. o.

önmagában – mint azt a későbbi terrorcselekmények igazolták – nem bizonyult elégségesnek, így az emberi tényező (a maga kettősségével: kapcsolat és kapcsolattartó) továbbra is a hírszerzési tevékenység alapvető kelléke marad."[895]

8. Javaslatok

Egyetértek Nagy oktatást illető javaslataival: „Az új kockázatokat, akárcsak más számítástechnikai környezetben felmerülő kockázatot, az Internet árnyoldalait meg kell ismertetni a képzési formáknak megfelelő szinten, mélységben, középiskoláktól az egyetemi oktatáson át a jogalkotók a jogalkalmazók képzéséig. Jelenleg e körben bőven lenne tennivaló."[896]

Ugyan elengedhetetlen az online található szélsőséges anyagok letávolítása, de a radikalizálódás ellen is az oktatás lehet a legjobb fegyver.

A terroristák által frekventált weboldalak, online platformok és virtuális terek, az általuk használt okostelefonos applikációk, mind olyan felületek, amelyek lehetőséget adnak információszerzésre, felderítésre, leplezett eszközök használatára, terror-elhárítási célból[897], továbbá fedett ügynökök terroristák közé történő beépülésére, és ezáltal terrorcselekmények elkövetésének és toborzás megakadályozására A terroristákhoz kötődő alkalmazásokat fel kell törni, továbbá megfigyelő malware-ekkel ellátott hamis terrorista alkalmazásokat szükséges fejleszteni[898], ezek használatával terroristák közé beszivárogni és ezáltal terrorcselekményeket megelőzni.[899] Fábián a következő megállapításokat teszi: „Úgy tűnik, napjaink terroristái jellemzően magányos elkövetők. A norvég Breivikre gondolva igazat kell adnunk Hankiss Ágnesnek, aki szerint azon esetek, melyekben az elkövető valóban minden külső (eszmei, anyagi) támogatás nélkül szervezi meg és hajtja végre az akcióját, sokkal inkább tartoznak a klinikai pszichológia körébe. Az ilyen elkövetőkkel szemben a nemzetbiztonsági szolgálatok valójában

[895] Uo. 11. o.

[896] NAGY (2012): i.m. 232. o.

[897] FINSZTER (2019): i.m. 280–281. o.

[898] KATZ, R.: Almost Any Messaging App Will Do—If You're ISIS. Vice. (2016, July 14). https://www.vice.com/en/article/kb7n4a/isis-messaging-apps (2021.07.07.)

[899] SERBAKOV M. T.: Az online felületek és okostelefonos alkalmazások, mint a terrorcselekmények előrejelző rendszerei. In: GAÁL Gy. – HAUTZINGER Z. (szerk.): Pécsi Határőr Tudományos Közlemények XXI.: A bűnüldözés és a bűnmegelőzés rendészettudományi tényezői. Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoportja, Pécs, 2019. 124. o.

tehetetlenek."[900] Ugyan egyetértek azzal, hogy az ilyen elköveték támadásait rendkívül nehéz megelőzni, de, véleményem szerint az ilyen elkövetőkkel szemben sem teljesen tehetetlenek a nemzetbiztonsági szolgálatok. Egy személynek radikalizációjának, terrorcselekmény elkövetésére való szándékának gyakran vannak az nyomai a interneten, viszont ezek megtalálása és értékelése problematikus. A terroristák mindenféle szervezkedése, kommunikációja, toborzása, egy magányos személy radikalizációjának folyamata (ennek felismerésének tekintetében a személy környezetére is felelősség hárul), a terrorcselekmények előkészítése, a terrorizmus finanszírozása nem vákuumban történik, hanem ezek mind digitális nyomokat hagynak maguk után, ezeknek mindig van nyoma online térben, különböző fórumokon, platformokon, üzenetküldő alkalmazásokban etc. Ezeknek a jeleknek, nyomoknak az időben történő felfedezése a terrorizmus és terrorizmus elleni küzdelem szempontjából kritikus fontosságú.

Naprakészen szükséges ismerni és nyomon követni gépi és emberi eszközökkel, hogy a terroristák mire, miért és hogyan használják az internetet és a különféle alkalmazásokat, továbbá milyen internetes oldalakon, alkalmazásokon folytatják a tevékenységüket. Minden internethasználó megfigyelését, vagy az arra való törekvést rendkívül aggályosnak tartom, de az ismert platformok, személyek célzott megfigyelését a téma szempontjából elengedhetetlennek. A nyomozó hatóságok és titkosszolgálati szervek szerepe egyértelműen kitüntetett a terrorcselekmények megelőzése szempontjából, ahol felkészült és nyelveket jól beszélő állományra van szükség, akiknek a megfelelő szakértőket is, informatikai szakértőket, tolmácsokat etc. mindenképpen be kell vonniuk a munkájuk során. Ez persze fokozott költségekkel is jár.

A végső dilemma, és örök vita tárgya, hogy mennyit vagyunk hajlanódak feláldozni a magánéletünkből, a szabadásgunkból, a biztonságunk érdekében.

„Nagy kihívást jelent megtalálni az egyensúlyt a szabadság és a szabadságjogok korlátozása között, ami a biztonság érdekében szükséges az alapvetően felhőtlenül szórakozni, szurkolni, sportolni, pihenni, gyógyulni, kikapcsolódni, vagy akár tanulni vágyó tömeg terhére. Tény, hogy az állampolgárok célja a szabad mozgás, a szabad

[900] HANKISS Á.: Kihívások és ellentmondások a terrorizmus elleni harcban. In: DÁNOS V. (szerk.): A terrorizmus Rubik-kockája, avagy a fenyegetések komplex megközelítése: Nemzetközi tudományos-szakmai konferencia: Rubik's cube of terrorism or complex approach to the threats: International scientific and professional conference. BM Oktatási, Képzési és Tudományszervezési Főigazgatóság, Budapest, 2014. 98–99. o. Idézi: FÁBIÁN P.: A terrorcselekmény büntetőjogi szabályozásának jelene és aktuális kérdései. Büntetőjogi Szemle, 2018/2. 45. o.

akaratukból való cselekvés, illetve a felhőtlen szórakozás. Mindezek mellett elengedhetetlen a biztonsági helyzetben bekövetkezett változások miatti szigorúbb biztonsági intézkedések megtétele."[901]

[901] JASENSZKY: i.m. 13. o.

XVII. ÖSSZEFOGLALÓ: A TUDOMÁNYOS EREDMÉNYEK RÖVID ÖSSZEFOGLALÁSA, AZOK HASZNOSÍTÁSA, ILLETVE A HASZNOSÍTÁS LEHETŐSÉGEI

Jelen doktori értekezés tárgya a szélsőséges iszlám által motivált és a szélsőjobboldali terroristák internethasználatának egyes aspektusai.

A téma kontextusba helyezéséhez és megértéséhez elengedhetetlen a terrorizmus definíciójának, típusainak, történetének, és napjainkban történt változásainak bemutatása.

A terrorrorizmus témáját bármilyen irányban megközelítve az első problémával már akkor szembesülünk, mikor azt szeretnénk eldönteni, hogy egyáltalán mit is nevezünk annak. A terrorizmusnak számtalan definíciója létezik. Még ha el is döntjük, hogy a szakirodalom és különféle szervezetek, kormányok kiket tekintenek terroristáknak, akkor sem lehetséges általánosságban „a terroristák" internethasználatáról írni, mivel a terrorizmusnak sokféle tipizálása is létezik. Röviden felvázoltam a terrorizmus definíciójának kérdését és a terrorizmus típusait.

A meghatározások és a tipizálás alapvetéseinek tisztázása után dióhéjban felvázoltam a a nemzetközi terrorizmus történetét, és rávilágítottam korunkban a jelenségét illető fő változásokra.

Tárgyaltam a média és terrorizmus kapcsolatának vázlatos történetét és elméletét, és rámutattam arra, milyen változásokat hozott a média és terrorizmus kapcsolatába az internet és a közösségi média megjelenése.

Ezt követően felvázoltam a terroristák internethasználatának alapvetéseit, hogy a szakirodalom szerint mire használják a terroristák a világhálót, továbbá tisztáztam, hogy jelen értekezésben mit értek terroristák internethasználata alatt, és mit nem.

Tárgyaltam a terroristák dark webes jelenlétének kérdését és a méltatlanul alulkutatott terroristák okostelefonos alkalmazás használatátát.

Bemutattam a terrorizmus finanszírozás internethez köthető technikáit és forrásait mutatja be.

Tárgyaltam az online történő radikalizáció kérdését, és a terrorcselekményeket előrejelző internetes magatartásokat.

Három szélsőséges iszlám által motivált terrorszervezet, az al-Kaida, az Iszlám Állam

(továbbiakban IS) és a Boko Haram internethasználatát illetően próbáltam átfogó képet nyújtani.
Tárgyaltam a szélsőjobboldali terroristák online jelenlétét, és a 2019-2020-as szélsőjobboldali terrorhullámot és azok elkövetőinek internethasználatát.
Vizsgáltam az online terjedő összeesküvés-elméleteket terror-kockázat szempontjából, fő fókuszban a The Great Replacement és a QAnon elméletekkel.
Bemutattam a kölönösen internet-orientált, nőgyűlölő inceleket és a hozzájuk fűződő fő elkövetéseket.
Elemeztem a 3D nyomtatott lőfegyverek, online elérhető tervrajzaik és ezek terrorista célokra való felhasználhatóságát.
Vizsgáltam a (COVID-19) pandémia hatását a terrorizmus jelenségére és a terroristák internethasználatára.
Tárgyaltam a terrorizmus elleni küzdelem és a terrorcselekmények megelőzésének egyes elméleti kérdéseit, különös tekintettel az internethez kötődő megelőzési módszereket.
Végül a témát illetően javaslatokat fogalmaztam meg.

Hipotéziseimet illetően a következő eredményekre jutottam:

1. A terrorizmus jelensége 9/11 óta változáson esett át.

Az utóbbi évtized, főleg körülbelül az utóbbi 5-6 év során elterjedtek az olcsó és egyszerű, puha célpontok elleni terrortámadások, például gázolások, késelések, lövöldözések, és majdnem eltűntek a gépeltérítések és az olyan elkövetések, melyek során a terroristák követelést terjesztenek elő. Az elkövetések fókuszában az áldozatok számának maximalizálása, az ölés áll.
Az olcsó, egyszerű, szinte semmi szervezést és anyagi forrást nem igénylő terrorcselekmények rendkívül nehezen előzhetők meg.
A terrorizmus jelenségébe hatalmas változást hoztak a modern technológia lehetőségei, köztük az internet, a közösségi média, az okostelefonok és az azokhoz kötődő alkalmazások és a 3D nyomtatás elterjedése és fejlődése.

2. Az internet és a közösségi média elterjedése drasztikus változást hozott a terrorizmus jelenségébe.

Az internet és a közösségi média elterjedése gyökeresen megváltoztatta a terrorizmus

„játékszabályait”, nagyban megkönnyítve azt. Az internetet a terroristák számos tevékenység végzésére használhatják, többek között propagandájuk terjesztésére, elkövetéseik élő közvetítésére, kommunikációra, koordinálásra, támadások elkövetésére való felszólításra, oktatásra, adományok gyűjtésére, célpontokról információ gyűjtésére etc. Ezek az internet nyújtotta előnyök hatalmas segítséget jelentenek a terroristák számára, számtalan módon és nagyban megkönnyítve korunk terrorizmusát: Terroristák nemzeteken átívelően tudják egymással valós időben, ingyen tartani a kapcsolatot, a terrorizmus elméleti alapjait, a „know how-jait” az otthonuk kényelméből, az interneten keresztül már el tudják sajátítani, támogatóiktól adományokat kérhetnek és kaphatnak a világ minden részéről, akik akár nem is feltétlenül vannak tudatában annak, hogy terrorizmust finanszíroznak etc.

A közösségi média széleskörű használatának elterjedését kihasználták a terroristák is. Ezeken a felületeken számtalan emberhez juthatnak el a szűretlen tartalmaik.

Mielőtt a közösségi média felületek elkezdtek koordináltan és erélyesen fellépni ellenük, ezeket a platformokat el tudták lepni a terroristák, melyre jó példa az IS Twitteren végzett tevékenysége 2014-2015-ben. Az ilyen tevékenységeik elleni fellépés rendkívül nehéz, azokhoz gépi módszerek is szükségesek, melyek megkerülésére a terroristák is fejlesztettek ki módszereket, melyre példaként az IS Facebookon használt eltávolítást megkerülő taktikái.

3. A dark web napjaink terroristáinak fontos eszköze.

Az internet deep web rétegéhez tartozó, számos illegális tevékenységnek helyt adó dark web használatával a terroristák kiegészítik a felszíni weben végzett tevékenységeiket.

2015 után a felszíni webről való „elüldözésük” után a dark webet fokozottabban használják, ahol nehezebben megfigyelhetőek, de annak a felszíni webhez képest nehézkesebb és nehezebben elérhető felülete miatt a terroristák is nehezebben tudják elérni egymást és a közönségüket. Több szerző szerint hiba volt a dark webig száműzni őket, mivel ott könnyen szem elől téveszthetőek. A dark webről számos illegális szolgáltatás, és akár fegyverek is vásárolhatók.

4. A terroristák kihasználják az okostelefonos alkalmazások előnyeit.

A terroristák élnek az okostelefonos alkalmazások nyújtotta előnyökkel, azokkal végzett tevékenységeik szinte megyegyeznek az interneten végzettekkel. Számos alkalmazást

tevékenységeik biztonságosabb végzéséhez, titkos kommunikációjukhoz, adományok kéréséhez, másokat propagandájuk terjesztésére használnak. Hamis alkalmazások fejlesztése, vagy ezek feltörése lehetőséget biztosít a terroristák megfigyelésére.

5. Az internethez kötődő terrorizmus finanszírozási források és technikák, főleg a kriptovaluták használata egyre nagyobb fenyegetést jelentenek.

A terrorizmus finanszírozásában a hagyományos technikák mellett már megjelentek a modern technológiához kötődők is. Az internet kiváló eszközt nyújt ahhoz, hogy terroristák adományokat akár virtuális fizetőeszközökben, immár nemzetközi szinten, akár fedett vagy explicit módon kérjenek és kapjanak támogatóiktól és mit sem sejtő donoroktól.
A szerzők egyetérteni látszanak abban, hogy a terrorizmus finanszírozás internethez fűződő technikái és módszerei jelentőségük tekintetében még a hagyományos technikák és módszerek mögött helyezkednek el, de a jövőben relevanciájuk nőhet. A terrorizmus elleni küzdelem szereplői általi figyelemmel kísérésük épp ezért elengedhetetlen fontosságú.
Különösen aggályos, hogy az utóbbi éveben elterjedt olcsó, egyszerű terrortámadásokhoz szinte semennyi finanszírozásra nincsen szükség, tehát ezeket nem lehet a terrorizmus finanszírozás elleni harc eszközeivel megelőzni.

6. A radikalizáció folyamatában korunkban kulcsszerepet játszik az internet.

Az interneten a terroristák számtalan felületen és módon terjeszthetik ideológiájukat, propagandájukat, különféle anyagaikat, szabadon kommunikálhatnak mely valószínűleg komoly szerepet játszik korunkban a terrorizmusra való radikalizáció folyamatában. Számos terrorcselekményt elkövető személy online radikalizálódott. Megjelent az online egymást inspiráló elkövetők terrorhullámának jelensége, mely során az elkövetők egymást láncreakció-szerűen inspirálhatják, melyet illusztrál a 2019-2020-as szélsőjobboldali terrorhullám. Az internet miatt a terrorszervezetekhez tartozás akár már egyéni megítélés kérdése is lehet.
A terrorcselekmények megelőzése szempontjából kritikus fontosságú a különböző online található radikalizáló anyagok eltávolítása, az ellenük oktatásssal, felvilágosítással történő küzdelem.

7. Az interneten a terrorcselekményének többségének vannak előjelei.

„Az internet sosem felejt”, minden interneten végzett tevékenységnek digitális nyoma van. Egy személy radikalizációs folyamatának, egy terrorcselekmény megszervezésének, az arról való kommunikációnak, a szükséges eszközök beszerzésének, az online végzett terrorizmus finanszírozásnak sokszor vannak online jelei. Az olcsó, egyszerű, szinte semmi szervezést és anyagi forrást nem igénylő terrorcselekmények nehezen megelőzhetők, esetleg az elkövető online radikalizációjának és egyéb terrorcselekményt előrejelző magatartásainak, például szándéka szivárogtatásának lehetnek nyomai.
A nehézséget ezeknek az időben történő felfedezése, felismerése, valós fenyegetésüknek kritikus felmérése jelenti. Problematikus annak a pontos ismerete, hogy milyen formát öltenek, és hol történnek a terrorcselekmény elkövetésére utaló előjelek, például a szándék harmadik személy irányába történő szivárogtatása, egy személy radikalizációs folyamatának online jelei etc. Nehézkes a valódi és a nem komoly online szándéknyilatkozatok elhatárolása, és a radikalizáció sem feltétlenül vezet terrorcselekmények elkövetéséhez.
Elengedhetetlen a terroristák internethasználatának részletes, pontos, és naprakész ismerete, továbbá az információk/adatok felfedezéshez és értékeléséhez emberi és gépi módszerek és szakértők almalmazása szükéges.

8. Nem csak a muszlim elkövetők képviselik az egyedüli komoly terrorveszélyt.

Az utóbbi évek során globális szinten fokozódott a szélsőjobboldalhoz köthető erőszak. Egyre gyakrabban történnek szélsőjobbolfali nézeteket által motivált terrorcselekmények. 2019-2020-ban egy egymás által online inspirált terrorhullámot hajtottak végre egymástól látszólag független elkövetők.
A szélsőjobboldali terrorizmust nem szabad kevésbé fenyegetőként kezelni, mint a szélsőséges iszlám által motiváltat, ugyanis az komoly és fokozódó fenyegetést képvisel, ezért fokozott figyelmet és kutatást igényel meg.
A szélsőjobboldali terror „játékosítása”[902] és az ahhoz kapcsolódó versengés, fokozódási kényszer az online fórumokban egy rendkívül aggasztó jelenség, melyet nem szabad

[902] EVANS, Robert: The El Paso Shooting and the Gamification of Terror. Bellingcat. (2019, August 4). https://www.bellingcat.com/news/americas/2019/08/04/the-el-paso-shooting-and-the-gamification-of-terror/ (2022.02.09.)

szem elől téveszteni. A terrorizmus témájának elemzése során hiba azt csupán a muszlim elkövetőkre leszűkíteni, mivel a terrorizmus jelensége ennél sokkal tágabb kategória. Úgy vélem szakirodalomban több szónak kellene esnie a szélsőséges iszlám terrorizmuson kívüli más terrorizmus típusokról is.

9. Több online terjedő összeesküvés-elmélet terror-kockázatot képvisel.

Radikalizáló ereje miatt különösen nagy terror-veszélyt képvisel a „The Great Replacement elmélet", mely a 2019-2020-as szélsőjobboldali terrorhullám elkövetőinek manifesztumaiban is visszaköszön.
A QAnon összeeskövés-elmélethez számos erőszakos cselekmény köthető. 2021. január 6-án is számos hívője jelen volt az Egyesült Államok Capitoliumának ostrománál, melyet többen terrorizmusnak tituláltak, köztük Joe Biden is.
A pandémia alatti bizonytalan időkben sok, egyre elszigeteltebb ember összeesküvés-elméletekkel próbál választ adni a korunkat illető nehéz kérdésekre, bizonytalanságokra. Különösen aggasztóak a koronavírushoz kapcsolódó összeeskövés-elméletek.

10. Az incel elkövetők terroristák, és a főként online táplált és inspirált nőgyűlölő terrorizmusuk valós fenyegetést képvisel.

Az incelek rendkívül internet-orientáltak, maga a mozgalom is az interneten született, és egymást is ott ideologizálják, radikalizálják, kergetik egymást egyre mélyebb kétségbeesésbe, melyből többük úgy érzi, hogy végül csak a terrorizmus jelenthet kiutat. Elméletileg létezhet az incel és a dzsihád közötti átjárás, az ún. „jihadpill" magukévá tételével, mely annyit jelent, hogy néhányuk úgy véli, dzsihadistává válással nőkhöz juthatnak.

11. Az utóbbi évekbeli szélsőjobboldali terrorhullámba tartozó támadások között online kapcsolat állhat fenn.

Rendívül veszélyes jelenség a terrorhullám. A jövőben egy ilyen hullám felismerése kritikus fontosságú, figyelni kell az elkövetők által közzétett manifesztumokra, és az ezekben fellelhető közös elemekre. Kutatást igényel, hogy egy ilyen hullámot hogyan lehet megakadályozni, azt megtörni.

12. Az online terjedő 3D lőfegyer tervrajzok komoly (terror-) veszélyt képviselnek.

3D nyomtató és legálisan és könnyen beszerezhető eszközök (nyomtatáshoz szükséges anyag, esetleg fémcső etc.) beszerzése után, egy kis online utánajárással, a hatóságok előtt ismeretlenül már otthonról is gyártható többféle 3D nyomtatott lőfegyver. Ezek terrorcselekmények elkövetése során való használata még nem olyan elterjedt, de a technológia elkerülhetetlen fejlődésével a jövőben fokozódhat a használatuk.

13. A koronavírus (COVID-19) világjárvány hatott a terrorizmusra, és megnövelte a terroristák internethasználatának fenyegetését is.

A terroristák kihasználhatják az állami szervek a pandémia elleni küzdelem miatti leterheltségét, és a potenciálisan kialakuló biztonsági réseket. Szélsőséges nézeteket vallók maga a vírus fegyverként való használatát is javasolták.
A koronavírus pandémia megfékezése miatt bevezetett zárlatok és távolságtartási előírások miatt drámaian megnőtt az emberek online töltött ideje. A hosszú izoláció alatt sokan elmagányosodnak, kétégbeesettebbek lesznek, a pandémia a mentális egészségükre is hatásassal van, mely a fokozott online töltött idővel kombinálva azt eredményezi, hogy sebezhetőbbek lesznek általánosságban a szélsőségességek, a terroristák online terjesztett ideológiájával szemben, fogékonyabbak lesznek a radikalizációra és az összeesküvés-elméletekre. A terroristák ezeket felismerve megkettőzik az ideológiájuk online terjesztésére tett erőfeszítéseiket.

Az értekezésem tudományos eredményei segítséget nyújthanak, azok felhasználhatóak lehetnek a terrorizmus elleni harc szereplői, a bűnüldöző szervek, a titkoszolgálatok számára, de akár a jogalkotást is orientálhatják. Kutatásom a témát és annak egyes aspektusait illető további kutatást, termékeny vitát ösztökélhet, és hozzásegíthet a terrorizmus jelenségének mélyebb megértéséhez.

14. A terroristák internethasználatának behatóbb ismerete hozzájárulhat a terrorcselekmények hatékonyabb megelőzéséhez.

A terroristák internethasználatának bővebb, pontosabb ismerete által ezen internethez kötődő tevékenységeik ellen a terrorizmus elleni harc szereplői is hatékonyabban tudnak fellépni (a kommunikációjuk kifürkészésével, megzavarásával, anyagaik eltávolításával

etc. is) mely közvetetten és akár közvetlenül eredményezheti terrorcselekmények megelőzését, vagy hozzájárulhat ahhoz.
Az értekezésemben a terroristák internethasználatának számos vetületére világítottam rá, melyek alapján belátható, hogy az internet korunk terrorizmusát számos módon segíti, a radikalizációs folyamatban is fontos szerepet játszhat, számos terrortámadásnak, azok elkövetőinek vagy azok finanszírozásának vannak közvetve vagy közvetlenül internethez kötődő elemei.

Az értekezésem tudományos eredményei segítséget nyújthanak, a terrorizmus elleni harc szereplői, a bűnüldöző szervek, a titkoszolgálatok számára a terrorizmus és a terrorizmus finanszírozása elleni küzdelem terén, de akár a jogalkotást is orientálhatják. Kutatásom a témát és annak egyes aspektusait illető további kutatást, termékeny vitát ösztökélhet, és hozzásegíthet a terrorizmus jelenségének mélyebb megértéséhez.

XVIII. SUMMARY

This dissertation aims to analyse some aspects of the internet usage of radical Islamic and right-wing terrorists.

In order to understand and contextualise the topic at hand, it is essential to examine the definitions, the types, the history and the recent changes of terrorism.

When we approach the topic of terrorism we already meet the first issue when we try define it. Terrorism has countless definitions.

Even if we decide who is considered a terrorist by the scientific literature and various organizations and governments, it is not possible to write about the internet usage of "terrorists" in general, as there are many different types of terrorism.

I have briefly outlined the questions of the definition and the types of terrorism. After clarifying the definitions and the basics of the types, I have outlined the history of international terrorism in a nutshell and highlighted the main changes in its phenomenon in our time.

I have briefly outlined the the history and theory of the relationship between media and terrorism and pointed out the changes that the advent of the internet and social media has brought to their relationship.

After that, I examined the basics of the internet usage of terrorists according to the literature. I clarified what I mean by the internet usage of terrorists in my dissertation.

I discussed the issue of the dark web presence of terrorists and their use of smartphone applications, which is an undeservedly under-researched topic.

I have presented the internet-related techniques and sources of terrorist financing.

I have examined the issue of online radicalisation and the online warning behaviors before acts of terrorism.

I have attempted to give a comprehensive picture of the online activities of three terrorists organisations motivated by radical Islam, namely the Al-Qaeda, the Islamic State, and Boko Haram.

In my dissertation I have examined the online presence of right-wing terrorists and the far-right terror-wave of 2019-2020 and the internet usage of their perpetrators.

I have examined online conspiracy theories in terms of terrorist risk, with giving special attention to The Great Replacement the QAnon theories.

I have introduced the especially internet-oriented, misogynist incels, and their most relevant attacks.

I have analyzed the usability of 3D printed firearms, and their blueprints available online for terrorist purposes.
I have examined the effect of the COVID-19 pandemic on the phenomenon of terrorism and the internet usage of terrorists.
I have discussed some theoretical issues regarding the fight against terrorism and the prevention of terrorist atacks, in particular the prevention methods associated with the internet.
Finally, I have made suggestions on the subject.

Regarding my hypotheses, I came to the following results:

1. The phenomenon of terrorism has gone through changes since 9/11.

In the last decade, especially in the last 5-6 years, cheap and simple terrorist attacks against soft targets, such driving into crowds, knife attacks have become widespread, and hijackings and attacks where perpetrators present their demands have almost disappeared. Terrorist attacks now focus on maximising the number of victims, their goal is to kill as many people as possible. Cheap, simple attacks which require almost no financial funding and organising are very difficult to prevent.
The phenomenon of terrorism has been vastly transformed by modern technology, including the internet, social media, smartphones and smartphone applications, and 3D printing.

2. The internet and the spread of social media has brought a drastic change in the phenomenon of terrorism.

The spread of the internet and social media has radically changed the “rules of the game” of terrorism, making it much easier. The internet can be used by terrorists to carry out a number of activities, including spreading their propaganda, broadcasting their crimes, communicating, coordinating, inciting attacks, educating, collecting donations, gathering information about targets etc. These benefits of the internet are a huge help to terrorists, greatly facilitating the terrorism of our time in many ways: On the internet, terrorists can keep in touch with each other in real time, for free, they can learn the basics and the know-how of terrorism from the comfort of their homes, they can ask for donations from their supporters, from all over the world, who might not even

be aware of the fact that they financing terrorism etc.
Terrorists exploited the increased use of social media. On these platforms their unfilitered contents are able to reach countless people.
Before social media platforms began to act remove teir content in a coordinated and vigorous manner, these platforms were swarmed by terrorists. IS's Twitter activity in 2014-2015 is a good example. Combating such activities is extremely difficult, and also requires automated methods, which terrorists have developed tactics to circumvent, for example IS has found ways to avoid automated detection of Facebook.

3. The dark web is an important tool in the hands of todays's terrorists.

By using the dark web, which belongs to the deep web layer of the internet and hosts many illegal activities, terrorists complement their activities on the surface web.
After 2015, after their "expulsion" from the surface web, their use of the dark web increased, where it is more difficult to observe their activities, but because of its limited usability and because it is more inaccessible compared to the surface web, it is also more difficult for terrorists to reach each other and their audience.
According to several experts, it was a mistake to „banish" them to the dark web, as they much harder to track there. Many illegal services and even weapons can be purchased from the dark web.

4. Terroristx exploit the advantages presented by smartphone applications.

Terrorists exploit the benefits of smartphone applications, and their facilitated by these are almost the same as those of the internet. They use many applications to conduct their activities more securely, to communicate secretly, to solicit donations, and to spread their propaganda to others. Developing fake applications or hacking them provides an opportunity to monitor terrorists.

5. The threat of the internet-related techniques and sources of terrorist financing, especially the use of cryptocurrencies are a growing threat.

In addition to traditional techniques, those associated with modern technology have also appeared in the financing of terrorism. The internet is an excellent tool for terrorists to internationally, covertly or explicitly solicit and receive donations from their supporters

and unsuspecting donors, even in virtual currencies.
The experts seem to agree that the techniques and methods of terrorist financing on the internet are still behind traditional techniques and methods in terms of their importance, but their relevance may increase in the future. Monitoring by those involved in the fight against terrorism is therefore essential.
It is particularly worrying that the cheap, simple terrorist attacks that have become commonplace in recent years require almost no funding, so they cannot be prevented by the means of combating the financing of terrorism.

6. The internet plays a key role in today's radicalisation.

On the internet, terrorists can spread their ideology, propaganda, various materials and they can communicate freely in countless ways. Terrorists's materials online are likely to play a major role in the the radicalisation process leading to terrorism today. Several people who committed acts of terrorism have been radicalised online.

The phenomenon of the terror wave in which online perpetrators inspire each other like a chain reaction has emerged, illustrated by the far-right terror wave of 2019-2020. Because of the internet, nowadays belonging to a terrorist organization might even be a matter of individual judgment. The removal of various radicalising materials found online and the fight against them through education and information are critical for the prevention of terrorist attacks.

7. Most acts of terrorism have warning signs on the internet.

"The internet never forgets," every activity on the internet leaves a trace, digital evidence.
There are often online signs of a person's radicalisation process, the organisation of a terrorist act, the communication about it, the acquisition of the necessary tools, and the financing of terrorism online all leave traces, all have online signs.
Inexpensive, simple terrorist acts that require almost no organisation or financial resources are difficult to prevent, but the perpetrators's radicalisation process, or other warning signs before terrorist attacks such as leak of intent might sometimes have early signs online. The difficulty is discovering these signs in time, recognising them, and critically assessing their real threat.

It is problematic to know exactly what form and where the signs of preparation of a terrorist attack act take place, such as the leak of intent to a third party, the online signs of a person's radicalisation process, etc. It is difficult to distinguish between serious and non-serious online declarations of intent, and radicalisation does not necessarily lead to terrorism.
Detailed, accurate, and up-to-date knowledge of the internet usage of terrorists is essential, as well as the use of human and automated methods and experts to discover and assess the dicovered information/data.

8. Not only muslim attackers pose serious terrorist threat.

Violent acts connected to the far right have increased globally in recent years. Terrorist attacks motivated by far-right views are becoming more frequent. In 2019-2020, a wave of terror in which attackers were inspired by each other was carried out by seemingly independent perpetrators.
Far-right terrorism should not be treated as less of a threat than that motivated by radical Islam, as it poses a serious and growing threat and therefore requires increased attention and research. The "gamification"[903] of far-right terror and the associated competition, the compulsion escalate in online forums, is an extremely worrying phenomenon that should not be overlooked. In analyzing the subject of terrorism, it is a mistake to limit it to muslim perpetrators only, as the phenomenon of terrorism is a much broader category.
I believe that more should be said in the literature about other types of terrorism than radical Islamic terrorism.

9. Several consiracy theories which circulate online pose a terrorist risk.

Because of its radicalising potemntial, the „The Great Replacement" theory poses an especially serious terror-threat. This theory was referenced in the manifestos of the perpetrators of the right-wing terror-wave of 2019-2020.
Several violent acts can be connected to the QAnon conspiracy theory. On January 6, 2021, several believers were present at the siege of the U.S. Capitol, which several

[903] EVANS, Robert: The El Paso Shooting and the Gamification of Terror. Bellingcat. (2019, August 4). https://www.bellingcat.com/news/americas/2019/08/04/the-el-paso-shooting-and-the-gamification-of-terror/ (2022.02.09.)

people, including Joe Biden described as terrorism.
In the uncertain times of the pandemic, many increasingly isolated people are trying to answer the difficult questions and uncertainties of our time with conspiracy theories. Conspiracy theories related to the coronavirus are of particular concern.

10. Incel attackers are terrorists, and ther primarily online inspired misogynist terrorism poses a reat threat.

Incels are extremely internet-oriented, the movement itself was born online, and there they ideologise, radicalise, and drive each other into deeper despair, from which many of them feel that terrorism can be the only way out. Theoretically, there could be a path between incel and jihad, by embracing the so-called "jihadpill," which means that some incels believe they can only get women by becoming a jihadist.

11. There might be common online elements in the attacks of the right-wing terror wave of 2019-2020.

The terror-wave is an extremely dangerous phenomenon. In the future, recognising such a wave is critical. It is essential to study the manifestos posted on the internet by the perpetrators and to discover and assess the common elements found in them. The prevention and breaking such a wave requires research.

12. The 3D printed firearm blueprints available online pose a serious (terror-) threat.

After purchasing a 3D printer and legally and readily available tools (printing material, a metal tube, etc.), with the help of a some online research, several 3D printed firearms can be manufactured from home without the knowledge of the authorities. Their use in terrorist attacks is not yet widespread, but with the inevitable development of technology, their use may increase in the future.

13. The coronavirus (COVID-19) pandemic had an effect on terrorism, and increased the threat posed by terrorists's internet related activities.

Terrorists may take advantage of potential security vulnerabilities that may arise when the governments are occupied with fighting the pandemic. Several extremists have also

suggested the use of the virus itself as a weapon. Lockdowns and social distancing rules introduced to curb the coronavirus pandemic have dramatically increased people's time spent online.
During long isolation, many people become lonely and desperate, and the pandemic affects their mental health, which, combined with increased time spent on the internet, makes people more vulnerable to the ideology of terrorists spread online, and to extremism, conspiracy theories and radicaliation in general. Terrorists recognizing these effects of the pandemic and they are duplicating their efforts to spread their ideology online.

14. A better understanding of the use of the internet by terrorists can contribute to more effective prevention of terrorist attacks.

In my dissertation I have highlighted many aspects of the use of the internet by terrorists, which show that the internet contributes to terrorism in many ways, plays an important role in the radicalisation process, and many terrorist attacks, their perpetrators or their financing have many direct or indirect elements related to the internet.
By gaining a broader and more accurate knowledge of terrorists' internet related activities, counter-terrorism actors can also take more effective action against these activities (by scouting, disrupting, removing material, etc.), which actions can directly or indirectly contribute to the prevention of terrorist attacks.

The scientific findings of my dissertation can be helpful to the actors in the fight against terrorism, law enforcement agencies, secret services in the fight against terrorism and terrorism financing, but they may also be used to orient legislation. My research might encourage further research on the topic and some aspects of it, or a fruitful debate, and a deeper understanding of the phenomenon of terrorism.

XIX. IRODALOMJEGYZÉK

Felhasznált magyar és idegen nyelvű irodalom

2018 Annual Report on the Protection of the Constitution (Facts and Trends). https://www.verfassungsschutz.de/en/public-relations/publications/annual-reports/annual-report-2018-summary (2021.07.21.)

ACHARYA, Arabinda: Targeting Terrorist Financing: International Cooperation and New Regimes. Routledge, London and New York, 2009. 7. o.

ADESOJI, Abimbola: The Boko Haram Uprising and Islamic Revivalism in Nigeria. Africa Spectrum, 2010. Vol. 45. No. 2. 98. o.

AFZAL, Madiha: From "Western education is forbidden" to the world's deadliest terrorist group: Education and Boko Haram in Nigeria. Foreign Policy at Brookings, Washington D.C., 2020. 5. o. https://www.brookings.edu/wp-content/uploads/2020/04/FP_20200507_nigeria_boko_haram_afzal.pdf (2021.06.14.)

AGBIBOA, Daniel Egiegba: COVID-19, Boko Haram and the Pursuit of Survival: A Battle of Lives against Livelihoods. City & Society, 2020. Vol. 32. No. 2. 1–2. o.

AGBIBOA, Daniel Egiegba: Why Boko Haram Exists: The Relative Deprivation Perspective. African Conflict and Peacebuilding Review, 2013. Vol. 3. No. 1. 145. o.

ALKHOURI, Laith – KASSIRER, Alex: Tech for Jihad: Dissecting Jihadists' Digital Toolbox. Flashpoint, USA, 2016. 1. o. https://www.flashpoint-intel.com/wp-content/uploads/2016/08/TechForJihad.pdf (2021.07.05.)

AL-RAWI, Ahmed: Video Games, Terrorism, and ISIS's Jihad 3.0. Terrorism and Political Violence, 2018. Vol. 30. No. 4. 740–760. o.

AMARASINGAM, Amarnath – ARGENTINO, Marc-André: QAnon's Predictions Haven't

Come True; So How Does the Movement Survive the Failure of Prophecy? Religion Dispatches. (2020, October 28). https://religiondispatches.org/qanons-predictions-havent-come-true-so-how-does-the-movement-survive-the-failure-of-prophecy/ (2021.11.02.)

AMARASINGAM, Amarnath – ARGENTINO, Marc-André: The QAnon Conspiracy Theory: A Security Threat in the Making? CTC Sentinel, 2020. Vol. 13. No. 7. 41. o.

AMARASINGAM, Amarnath: The Impact of Conspiracy Theories and How to Counter Them: Reviewing the Literature on Conspiracy Theories and Radicalization to Violence. In: RICHARDS, Anthony – MARGOLIN, Devorah – SCREMIN, Nicolò (szerk.): Jihadist Terror: New Threats, New Responses. I.B. Tauris, London/New York, 2019. 33–34. o.

AMBRUS István: A koronavírus-járvány és a büntetőjog. MTA Law Working Papers, 2020/5, Magyar Tudományos Akadémia, Budapest, 2020. 22. o.

ANUGWOM, Edlyne Eze: The Boko Haram Insurgence in Nigeria: Perspectives from Within. Palgrave Macmillan, London, 2019. 200. o.

APAU, Richard: Youth And Violent Extremism Online: Countering Terrorists Exploitation And Use Of The Internet. African Journal on Terrorism, 2018. Vol. 7. No. 1. 22. o.

ARANY Anett – N. RÓZSA Erzsébet – SZALAI Máté: Az Iszlám Állam Kalifátusa: Az átalakuló Közel-Kelet. Osiris Kiadó Kft., Budapest, 2016. 220–221. o.

ARLETT Adél: Hírszerzés nyílt forráskódú programok használatával. Stratégiai Védelmi Kutatóintézet: NÉZŐPONTOK, 2019. 5. sz. 1. o.

Assessing the Threat of Mass Attacks in Texas: A State Intelligence Estimate. Texas Fusion Center Intelligence & Counterterrorism Division Texas Department of Public Safety, Texas, 2020. 16–17. o. https://www.dps.texas.gov/director_staff/media_and_communications/2020/txMassAttackAssessment.pdf (2021.07.22.)

AYAD, Moustafa: The Propaganda Pipeline: The ISIS Fuouaris Upload Network on Facebook. Institute for Strategic Dialogue, London, 2020. 2. o. https://www.isdglobal.org/wp-content/uploads/2020/07/The-Propaganda-Pipeline.pdf (2022.01.07.)

BAELE, Stephane J. – BRACE, Lewys – COAN, Travis G.: From "Incel" to "Saint": Analyzing the violent worldview behind the 2018 Toronto attack. Terrorism and Political Violence, 2019. 8. o.

BAKÓCZI Antal: Megismerési akadályok a terrorizmus kutatásában. Belügyi Szemle, 2015/7–8. 90. o.

BANERJEE, Arjun: Arms and the Man: Strategic Trade Control
Challenges of 3D Printing. International Journal of Nuclear Security, 2018. Vol. 4. No. 1. 1. o.

BARADARAN, Shima – FINDLEY, Michael – NIELSON, Daniel – SHARMAN, Jason: Funding Terror. University of Pennsylvania Law Review, 2014. Vol. 162. No. 3. 481. o.

BARKER, Jonathan: A terrorizmus. HVG Kiadói Rt., Budapest, 2003. 17–19. o

BARKER, Jonathan: The no-nonsense guide to terrorism. Verso, London, 2003. 10. o.

BARRATT, Monica – ALDRIDGE, Judith – MADDOX, Alexia: Dark Web. In: WARF, Barney (szerk.): The SAGE Encyclopedia of the Internet. SAGE Publications, Ltd., Thousand Oaks, 2018. 185–188. o.

BARTKÓ Róbert: A terrorcselekmény tényállásának értékelése az uniós követelmények tükrében. Belügyi Szemle, 2015/7-8. 39. o.

BARTKÓ Róbert: A terrorizmus elleni küzdelem kriminálpolitikai kérdései. UNIVERSITAS-GYŐR Nonprofit Kft., Győr, 2011. 18–22. o.

BARTKÓ Róbert: Az illegális migráció és a terrorizmus kapcsolata az EUROPOL és FRONTEX jelentéseire tekintettel. In: BARTKÓ Róbert (szerk.): A terrorizmus elleni

küzdelem aktuális kérdései a XXI. században. Gondolat Kiadó, Budapest, 2019. 177. o.

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. Gondolat Kiadó, Budapest, 2019. 138. o.

BARTKÓ Róbert – SÁNTHA Ferenc: Az Európai Unió jogalkotása és hatása a terrorcselekmény hazai büntetőjogi szabályozására. In: HOMOKI-NAGY Mária – KARSAI Krisztina – FANTOLY Zsanett – JUHÁSZ Zsuzsanna – SZOMORA Zsolt – GÁL Andor (szerk.): Ünnepi Kötet Dr. Nagy Ferenc Egyetemi Tanár 70. Születésnapjára. Balogh Elemér dékán, Szeged, 2018. 83. o.

BATTERSBY, John – BALL, Rhys: Christchurch in the context of New Zealand terrorism and right wing extremism. Journal of Policing, Intelligence and Counter Terrorism, 2019. Vol. 14. No. 3. 6. o.

BATTERSBY, John: Security sector practitioner perceptions of the terror threat environment before the Christchurch attacks. Kōtuitui: New Zealand Journal of Social Sciences Online, 2019. Vol. 15. No. 2. 1. o.

BÁCS Zoltán: A terrorizmus egyes latin-amerikai ideológiai támaszai. Nemzetbiztonsági Szemle, 2021/1. 17. o.

BÁCS, Zoltán György – KASZNÁR, Attila: Is the Lone Perpetrator Really Alone? Honvédségi Szemle – Hungarian Defence Review, 2018/1. különsz. 24. o.

BÁNYÁSZ Péter: A közösségi média szerepe a települések életében, kiemelten a rendkívüli események kezelésében. Településföldrajzi Tanulmányok, 2013/2. 132–145. o.
BÁNYÁSZ Péter: Kiberbűnözés és közösségi média. Nemzetbiztonsági Szemle, 2017/4. 71. o.

BÁNYÁSZ Péter – ORBÓK Ákos: A NATO kibervédelmi politikája és kritikus infrastruktúra védelme a közösségi média tükrében. Hadtudomány, 2013/1. elektr. sz. 196. o.

BECKSTROM, Matthew – LUND, Brady: Casting Light on the Dark Web: A Guide for Safe Exploration. Rowman & Littlefield Publishers, London, 2019. 41.o.

BEENE, Stephanie – GREERB, Katie: A call to action for librarians: Countering conspiracy theories in the age of QAnon. The Journal of Academic Librarianship, 2021. Vol. 47. No. 1. 2. o.

BELLEFLAMME, Paul – LAMBERT, Thomas – SCHWIENBACHER, Armin: Crowdfunding: tapping the right crowd. SSRN Electronic Journal, 2012. Vol. 29. No. 5. 1. o.

BELL, R. E.: The Confiscation, Forfeiture and Disruption of Terrorist Finances. Journal of Money Laundering Control, 2003. Vol. 7. No. 2. 106–107. o.

BELLINGER, Nisha – KATTELMAN, Kyle T.: Domestic terrorism in the developing world: role of food security. Journal of International Relations and Development, 2021. Vol. 24. No. 2. 1. o.

BENSON, David C.: Why the Internet is Not Increasing Terrorism. Security Studies, 2014. Vol. 23 No. 2 293–328. o.

BERACZKAI Antal: A terrorizmus és a média. Kard és Toll, 2006/2. 102–112. o.

BERGMAN, Michael K.: The Deep Web: Surfacing Hidden Value. The Journal of Electronic Publishing, 2001. Vol. 7. No. 1.

BERGSTRÖM, Maria: The Global AML Regime and the EU AML Directives: Prevention and Control. In: KING, Colin – WALKER, Clive – GURULÉ, Jimmy (szerk.): The Palgrave Handbook of Criminal and Terrorism Financing Law. Palgrave Macmillan, London, 2018. 35. o.

BERKI Gábor: A kibertér, annak veszélyei és a kibervédelem jelenlegi helyzete Magyarországon. Nemzetbiztonsági Szemle, 2018/3. 8. o.

BESENYŐ, János – GULYÁS, Attila: The Effect Of The Dark Web On The Security. Journal Of Security and Sustainability Issues, 2021. Vol. 11. No. 1. 112. o.

BESENYŐ, János – KÁRMÁN, Marianna: Effects of COVID-19 pandemy on African health, poltical and economic strategy. Insights into Regional Development, 2020. Vol. 2. No. 3. 630. o.

BESENYŐ János: Migrációs útvonalak. In: BESENYŐ János – MILETICS Péter – ORBÁN Balázs (szerk.): Európa és a migráció. Zrínyi Kiadó, Budapest, 2019. 31–64. o.

BESENYŐ, János – KERESZTES, Vivien: Hezbollah and Boko Haram: Cooperation or Imitation? Strategic Impact, 2016. Vol. 61. No. 4. 29–40. o.

BESENYŐ, János – MAYER, Ádám: Boko Haram in Context: The Terrorist Organizations's Roots in Nigeria's Social History. Defence Against Terrorism Review, 2015. Vol. 7. No. 1. 48. o.

BESLEY, Tina – PETERS, Michael A.: Terrorism, trauma, tolerance: Bearing witness to white supremacist attack on Muslims in Christchurch, New Zealand. Educational Philosophy and Theory, 2020. Vol. 52. No. 2. 112. o.

BIHARI Rita: Radikalizmus a Nyugat-Balkánon. Hadtudomány, 2020/elektr. sz. 168. o.

BJELOPERA, Jerome P.: American Jihadist Terrorism: Combating a Complex Threat. Congressional Research Service, Washington, D.C., 2013. 2. o.

BJØRGO, Tore – RAVNDAL, Jacob Aasland: Extreme-Right Violence and Terrorism: Concepts, Patterns, and Responses. ICCT Policy Brief, Hága, 2019. 2. o. https://icct.nl/app/uploads/2019/09/Extreme-Right-Violence-and-Terrorism-Concepts-Patterns-and-Responses-4.pdf (2021.07.21.)

BLACKBOURN, Jessie – MCGARRITY, Nicola – ROACH, Kent: Understanding and responding to right wing terrorism. Journal of Policing, Intelligence and Counter Terrorism, 2019. Vol. 14. No. 3. 183. o.

BLUMENAU, Bernhard: Terrorism, History and Neighbouring Disciplines in the Academy. In: ENGLISH, Richard (szerk.): The Cambridge History of Terrorism. Cambridge University Press, Cambridge, 2021. 124–146 o.

BODA József: A XXI. század nemzetbiztonsági kihívásai. In: GAÁL Gyula – HAUTZINGER Zoltán (szerk.): Pécsi Határőr Tudományos Közlemények XX.: A XXI. század biztonsági kihívásai. Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoportja, Pécs, 2018. 10. o.

BODA József: A terrorizmus rövid története és az ellene való fellépés lehetőségei. Rendvédelem-történeti Füzetek (Acta Historiae Preasidii Ordinis), 2007/16. 46. o.

BODANSKY, Yossef: The Boko Haram and Nigerian Jihadism. ISPSW Strategy Series: Focus on Defense and International Security, Institut für Strategie- Politik- Sicherheits- und Wirtschaftsberatung ISPSW, Berlin, 2015. 6. o.
https://www.files.ethz.ch/isn/187751/318_Bodansky.pdf (2021.06.14.)

BODO, Lorand – SPECKHARD, Anne: Identifying Nefarious Telegram Users without the Help of Telegram Itself: Testing Solutions for Intelligence and Security Professionals in Fighting ISIS in the Encrypted Social Media Space. International Center for the Study of Violent Extremism, London, 2017. 2. o.

BOLGÁR Judit – SZTERNÁK Nóra – SZTERNÁK György: A terrorizmussal kapcsolatos kutatások legújabb eredményei. Felderítő Szemle, 2005/4. 24. o.

BOROSS Zsigmond Attila: A jobboldali extrémizmus összetett ideológiája – mint a terrorizmus potenciális hivatkozása. TERROR & ELHÁRÍTÁS, 2017/4. 23–48. o.

BOROSS Zsigmond Attila: Humán faktor (Az emberi tényező szerepe az extrémizmus-elhárítás kérdéskörében). Nemzetbiztonsági Szemle. 2014/2. 139. o.

BORUM, Randy: Radicalization into Violent Extremism I: A Review of Definitions and Applications of Social Science Theories. Journal of Strategic Security, 2011. Vol. 4. No. 4. 8. o.

BOTHA, Anneli – EWI, Martin – SALIFU, Uyo – ABDILE, Mahdi: Understanding Nigerian citizens' perspectives on Boko Haram. Institute for Security Studies, Pretoria, 2017. 35. o. https://issafrica.s3.amazonaws.com/site/uploads/monograph196.pdf (2021.06.14.)

BŐCZNÉ NEPARÁCZKI Anna Viktória: A kiberterrorizmus büntető anyagi jogi megítélése. Ügyészek Lapja, 2020/1. 76–77. o.

BRZUSZKIEWICZ, Sara: Incel Radical Milieu and External Locus of Control. The International Centre for Counter-Terrorism – The Hague (ICCT) Evolutions in Counter-Terrorism, 2020. Vol. 22. 8. o.

BUBA, Malami: Newman, Paul: A Hausa-English Dictionary: book review. Lexikos, 2008. Vol. 18. No. 1. 456-462. o.

BURCHILL, Richard: Extremism in the time of COVID-19. Bussola Institute, Brüsszel 2020. 15-16. o.

CAIANI, Manuela – KRÖLL, Patricia: The transnationalization of the extreme right and the use of the Internet. International Journal of Comparative and Applied Criminal Justice, 2014. Vol. 39. No. 4. 2. o.

CALDWELL, M. – ANDREWS, J. T. A. – TANAY, T. – GRIFFIN, L. D.: AI-enabled future crime. Crime Science, 2020. Vol. 9. No. 1. 1. o.

CAMPHUIJSEN, Marjolein – VISSERS, Esther: Terrorism and the Mass Media: A symbiotic relationship? Social Cosmos, 2012. Vol. 3. No. 1. 14. o.

CANIGLIA, Mattia – WINKLER, Linda –MÉTAIS, Solène: The Rise Of The Right-Wing Violent Extremism Threat In Germany And Its Transnational Character. ESISC, Belgium, 2020. 1. o. http://www.esisc.org/publications/analyses/the-rise-of-the-right-wing-violent-extremism-threat-in-germany-and-its-transnational-character (2021.07.21.)

CAREW, Rachael M. – ERRICKSON, David: An Overview of 3D Printing in Forensic Science: The Tangible Third-Dimension. Journal of Forensic Sciences, 2020. Vol. 65.

No. 5. 1752. o.

CARR, Caleb: Terrorism as Warfare: The Lessons of Military History. World Policy Journal, 1996/1997. Vol. 13. No. 4. 1. o.

ÇELIKSOY, Ergül – OUMA, Smith: Terrorist Use Of The Internet. Bilişim Hukuku Dergisi, 2019. Vol. 1. No. 2. 250–252. o.

CHALIAND, Gérard – BLIN, Arnaud: Zealots and Assassins. In: CHALIAND, Gérard – BLIN, Arnaud (szerk.): The History of Terrorism: From Antiquity to Al Qaeda. University of California Press, Berkeley, 2007. 55. o.

CHERTOFF, Michael: A public policy perspective of the Dark Web. Journal of Cyber Policy, 2017. Vol. 2. No. 1. 36–37. o.

CHOONG, Yu Ying Clarrisa – TAN, Hong Wei – PATEL, Deven C. – CHOONG, Wan Ting Natalie – CHEN, Chun-Hsien – LOW, Hong Yee – TAN, Ming Jen – PATEL, Chandrakant D. – CHUA, Chee Kai: The global rise of 3D printing during the COVID-19 pandemic. Nature Reviews Materials, 2020. Vol. 5. No. 9. 638. o.

CLARKE, Colin P. – JACKSON, Kimberly – JOHNSTON, Patrick B. – ROBINSON, Eric – SHATZ, Howard J.: Financial Futures of the Islamic State of Iraq and the Levant: Findings from a RAND Corporation Workshop. RAND Corporation, Santa Monica, 2017. iii. o.
https://www.rand.org/content/dam/rand/pubs/conf_proceedings/CF300/CF361/RAND_CF361.pdf (2021.11.17.)

CLAUSEWITZ, Carl von: A háborúról. Zrínyi Kiadó, Budapest, 2013. 39. o.

CLIFFORD, Bennet: "Trucks, Knives, Bombs, Whatever:" Exploring Pro-Islamic State Instructional Material on Telegram. CTC Sentinel, 2018. Vol. 11. No. 5. 25. o.

CLIFFORD, Bennett – POWELL, Helen: Encrypted Extremism: Inside the English-Speaking Islamic State Ecosystem on Telegram. Program on Extremism: The George Washington University, Washington D.C., 2019. 3. o.

CLUNAN, Anne L.: The fight against terrorist financing. Political Science Quarterly, 2006. Vol. 121. No. 4. 570. o.

COHEN, Katie: Who will be a lone wolf terrorist? Mechanisms of self-radicalisation and the possibility of detecting lone offender threats on the Internet. FOI, Swedish Defence Research Agency, Stockholm, 2012. 4. o.

COMMITTEE OF EXPERTS ON THE EVALUATION OF ANTI-MONEY LAUNDERING MEASURES AND THE FINANCING OF TERRORISM MONEYVAL: Money laundering and terrorism financing trends in MONEYVAL jurisdictions during the COVID-19 crisis. Council of Europe, Strasbourg, 2020. 5. o. https://rm.coe.int/moneyval-2020-18rev-covid19/16809f66c3 (2021.09.12.)

CONWAY, Maura: Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research. Studies in Conflict & Terrorism, 2017. Vol. 40. No. 11. 91. o.

CONWAY, Maura: Routing the Extreme Right. The RUSI Journal, 2020. Vol. 165. No. 1. 1. o.

CONWAY, Maura – SCRIVENS, Ryan – MACNAIR, Logan: Right-Wing Extremists' Persistent Online Presence: History and Contemporary Trends. ICCT, Hága, 2019. 2. o. https://icct.nl/app/uploads/2019/11/Right-Wing-Extremists-Persistent-Online-Presence.pdf (2021.07.21.)

CONWAY, Maura: Terrorist 'Use' Of The Internet And Fighting Back. Information & Security: An International Journal, 2006. Vol. 19. 21. o.

COTTEE, Simon: Incel (E)motives: Resentment, Shame and Revenge. Studies in Conflict & Terrorism, 2021. Vol. 44. No. 2. 93. o.

Covid 19 and E-commerce: Findings from a survey of online consumers in 9 Countries. United Nations UNCTAD, 2020. 4. o. https://unctad.org/system/files/official-document/dtlstictinf2020d1_en.pdf (2021.06.14.)

COVID-19-related Money Laundering and Terrorist Financing – Risks and Policy Responses. FATF, Párizs, 2020. 4. o. https://www.fatf-gafi.org/media/fatf/documents/COVID-19-AML-CFT.pdf (2021.09.12.)

COX, James: Canada and the Five Eyes Intelligence Community. Canadian Defence and Foreign Affairs Institute, Calgary, 2012. 4. o.

COX, Kate – MARCELLINO, William – BELLASIO, Jacopo – WARD, Antonia – GALAI, Katerina – MERANTO, Sofia – PAOLI, Giacomo Persi: Social Media in Africa: A Double-Edged Sword for Security and Development: Research report. United Nations Development Programme, Cambridge, 2018. 22. o. https://www.africa.undp.org/content/rba/en/home/library/reports/social-media-in-africa-.html (2021.06.14.)

CRAWFORD, Blyth – KEEN, Florence: The Hanau Terrorist Attack: How Race Hate and Conspiracy Theories Are Fueling Global Far-Right Violence. CTC Sentinel, 2020. Vol. 13. No. 3. 1. o.

Cryptocurrency Crime and Anti-Money Laundering Report. CipherTrace, 2020. 6. o. https://ciphertrace.com/wp-content/uploads/2020/06/spring-2020-cryptocurrency-anti-money-laundering-report.pdf (2021.09.09.)

CROTHERS, Charles – O'BRIEN, Thomas: The Contexts of the Christchurch terror attacks: social science perspectives. Kōtuitui: New Zealand Journal of Social Sciences Online, 2020. Vol. 15. No. 2. 248. o.

CSÁNYI Csaba: 9/11-re adott lehetséges válaszok az Egyesült Államok és Németország példáján keresztül. Acta Humana, 2016/5. 15. o.

CUNNINGHAM, Jr. William G.: Terrorism Definitions and Typologies. In: Moore, R. Scott (szerk.): Terrorism: Concepts, Causes, and Conflict Resolution. U.S. Defense Threat Reduction Agency, Fort Belvoir, 2003. 23. o.

DAASE, Christopher – CHRISTOPHER, Grant – DALNOKI-VERESS, Ferenc – POMPER,

Miles – SHAW, Robert: WMD Capabilities Enabled by Additive Manufacturing: NDS Report 1908. Negotiation Design and Strategy, Jupiter, FL/Monterey, CA, 2019. 10. o. http://www.nonproliferation.org/wp-content/uploads/2019/09/NDS_Report_1908_WMD_AM_2019.pdf (2021.08.30.)

DAFAURE, Maxime: The "Great Meme War:" the Alt-Right and its Multifarious Enemies. Angles, 2020. Vol. 10. No. 2. 1. o.

DALY, Angela – MANN, Monique – SQUIRES, Peter – WALTERS, Reece: 3D printing, policing and crime. Policing and Society, 2021. Vol. 31. No. 1. 42. o.

DAVEY, Jacob – EBNER, Julia: 'The Great Replacement': The Violent Consequences Of Mainstreamed Extremism. Institute for Strategic Dialogue, London, 2019. 7–8. o.

DAVIS, Jessica: New Technologies but Old Methods in Terrorism Financing. Royal United Services Institute for Defence and Security Studies, London, 2020. 1. o. https://static1.squarespace.com/static/5e399e8c6e9872149fc4a041/t/60b0ab3b05f173456658076b/1622190920308/New+Technologies+but+Old+Methods+in+TF.pdf (2021.09.12.)

DE CUIA, Chiara: Is (Islamic State) And The West: The Role Of Social Media. Libera Università Internazionale degli Studi Sociali Guido Carli, Róma, 2014/2015. 21–22. o.

DE', Rahul – PANDEY, Neena – PAL, Abhipsa: Impact of digital surge during Covid-19 pandemic: A viewpoint on research and practice. International Journal of Information Management, 2020. Vol. 55. No. 1. 1. o.

DE SMEDT, Tom – RUPAR, Verica – JAKI, Sylvia – CAUBERGHS, Olivier – VOUÉ, Pierre – CABALLERO, Joan: The QAnon superconspiracy - Analysis of tweets during the 2020 US presidential election. 2020. 2. o. https://www.researchgate.net/publication/348281072_The_QAnon_superconspiracy_-_Analysis_of_tweets_during_the_2020_US_presidential_election (2021.12.08.)

DIETZE, Carola: Introduction: Writing the History of Terrorism. In: DIETZE, Carola – VERHOEVEN, Claudia (szerk.): The Oxford Handbook of the History of Terrorism.

Oxford University Press, New York, 2022. 1. o.

DILIPRAJ, E.: Terror In The Deep And Dark Web. Air Power Journal, 2014. Vol. 9. No. 3. 126. o.

DION-SCHWARZ, Cynthia – MANHEIM, David – JOHNSTON, Patrick B.: Terrorist Use of Cryptocurrencies Technical and Organizational Barriers and Future Threats. RAND Corporation, Santa Monica, 2019. 23. o. https://www.rand.org/pubs/research_reports/RR3026.html (2021.09.08.)

DOBÁK Imre: OSINT – Gondolatok a kérdéskörhöz. Nemzetbiztonsági Szemle, 2019/2. 83–93. o.

DONNELLY, Denise – BURGESS, Elisabeth – ANDERSON, Sally – DAVIS, Regina – DILLARD, Joy: Involuntary Celibacy: A Life Course Analysis. The Journal of Sex Research, 2001. Vol. 38. No. 2. 159. o.

DOUGLAS, Karen M.: Are Conspiracy Theories Harmless? The Spanish Journal of Psychology, 2021. Vol. 24. 1–7. o.

DORNFELD László: A koronavírus-járvány hatása a kiberbűnözésre. In Medias Res, 2020/2. 204. o.

DORNFELD László: Kiberterrorizmus – a jövő terrorizmusa? In: MEZEI Kitti (szerk.): A bűnügyi tudományok és az informatika. Pécsi Tudományegyetem Állam- és Jogtudományi Kar, MTA Társadalomtudományi Kutatóközpont, Budapest-Pécs, 2019. 61. o.

DOYLE, Paula: Four Policy Actions Needed to Strengthen US and Coalition Efforts Against al-Qa'ida, ISIL, and Hizballah. In: BYRNE-DIAKUN, Robert Morgan (szerk.): Georgetown Security Studies Review: What the New Administration Needs to Know About Terrorism and Counterterrorism. Georgetown Security Studies Review, USA, 2017. 100. o.

ÉBERHARDT Gábor: Magyarország az újabb tömeges nemzetközi migráció kapujában.

Belügyi Szemle, 2021/3. 366. o.

ÉBERHARDT Gábor: Migráció és terrorizmus. Hadtudományi Szemle, 2019/3. 37–59. o.

ELDEN, Stuart: The geopolitics of Boko Haram and Nigeria's 'war on terror'. The Geographical Journal, 2014. Vol. 180. No. 4. 414–415. o.

ELLSWORTH, Jill H.: Education on the Internet. Sams Publishing, Indianapolis, 1994. 1–591. o.

ESZTERI Dániel: A World of Warcraft-tól a Bitcoin-ig: Az egyén, a gazdaság és a tulajdon helyzetének magán- és büntetőjogi elemzése a virtuális közösségekben. Doktori értekezés. Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola, Pécs, 2015. 231. o.

European Union Terrorism Situation And Trend Report 2018 (Tesat 2018). Europol, 2018. 64. o. https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-2018-tesat-2018 (2021.03.02.)

European Union Terrorism Situation and Trend Report (TE-SAT) 2019. Europol, 2019. 17. o. https://www.europol.europa.eu/activities-services/main-reports/terrorism-situation-and-trend-report-2019-te-sat (2021.07.15.)

European Union Terrorism Situation and Trend report (TE-SAT) 2020. Europol, 2020. 6. o. https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-te-sat-2020 (2021.07.15.)

European Union Terrorism Situation and Trend report (TE-SAT) 2021. Europol, 2021. 7. o. https://www.europol.europa.eu/activities-services/main-reports/european-union-terrorism-situation-and-trend-report-2021-tesat (2021.09.07.)

Éves jelentés 2016. év. Nemzeti Adó- és Vámhivatal Központi Irányítás Pénzmosás Elleni Információs Iroda, 2016. 14. o.

FARWELL, James P.: The Media Strategy of ISIS. Survival, 2014. Vol. 56. No. 6. 49–55.

o.

FATF REPORT 2019-2020. FATF, Párizs, 2020. 14. o. www.fatf-gafi.org/publications/fatfgeneral/documents/annual-report-2019-2020.html (2021.09.12.)

FATF REPORT: Emerging Terrorist Financing Risks. FATF, Párizs, 2015. 13–20. o. https://www.fatf-gafi.org/media/fatf/documents/reports/Emerging-Terrorist-Financing-Risks.pdf (2021.09.12.)

FATF REPORT: Financing of Recruitment for Terrorist Purposes. FATF, Párizs, 2018. 4. o. https://www.fatf-gafi.org/media/fatf/documents/reports/Financing-Recruitment-for-Terrorism.pdf (2021.09.12.)

FATF REPORT: Terrorist Financing Risk Assessment Guidance. FATF, Párizs, 2019. 30. o. http://www.fatf-gafi.org/media/fatf/documents/reports/Terrorist-Financing-Risk-Assessment-Guidance.pdf (2021.09.12.)

FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins. FATF, Párizs, 2020, 2. o. www.fatf-gafi.org/publications/virtualassets/documents/report-g20-so-called-stablecoins-june-2020.html (2021.09.12.)

FÁBIÁN Péter: A terrorcselekmény büntetőjogi szabályozásának jelene és aktuális kérdései. Büntetőjogi Szemle, 2018/2. 49–50. o.

FÁBIÁN Péter: Terrorcselekmények és a magánbiztonság kapcsolatának aktuális összefüggései. Magyar Rendészet, 2018/4. 99. o.

FENYVESI Csaba: A kriminalisztika válaszai a társadalmi kihívásokra – a bűnüldözés fejlesztési lehetőségei. In: GAÁL Gyula – HAUTZINGER Zoltán (szerk.): Pécsi Határőr Tudományos Közlemények XXII: A hadtudománytól a rendészettudományig−társadalmi kihívások a nemzeti összetartozás évében. Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport, Pécs, 2020. 221. o.

FERRARA, Emilio – CHANG, Herbert – CHEN, Emily – MURIC, Goran – PATEL, Jaimin: Characterizing Social Media Manipulation in the 2020 U.S. Presidential Election. First Monday, 2020. Vol. 25. No. 11.

FERWAGNER Péter Ákos – KOMÁR Krisztián – SZÉLINGER Balázs: Terrorista szervezetek lexikona: Gavrilo Principtől Oszama bin Ladenig. Maxim Könyvkiadó, Szeged, 2003. 14. o.

FEY, Marco: PRIF Report No. 144 3D Printing and International Security Risks and Challenges of an Emerging Technology. Peace Research Institute Frankfurt (PRIF), Frankfurt, 2017. 21. o.

FINKLEA, Kristin: Dark Web. Congressional Research Service, Washington DC, 2017. 1. o. https://www.fas.org/sgp/crs/misc/R44101.pdf (2021.08.02.)

FINSZTER Géza: Rendészettan. Dialóg Campus Kiadó, Budapest, 2018. 78. o

FINSZTER Géza: Szabályozott felderítés – titkosított büntetőeljárás. Miskolci Jogi Szemle, 2019/2. különsz. 280–281. o.

FISHMAN, Brian: Crossroads: Counter-terrorism and the Internet. Texas National Security Review, 2019. Vol. 2. No. 2. 84–86. o.

FREEMAN, Michael: The Sources of Terrorist Financing: Theory and Typology. Studies in Conflict and Terrorism, 2011. Vol. 34. No. 6. 462. o.

FRUEHAUF, Justin D. – HARTLE, Francis X. – AL-KHALIFA, Fahad: 2016 Proceedings of the Conference on Information Systems Applied Research. Las Vegas, 2016. 2. o.

FURNELL, Steve – WARREN, Matthew: Computer Hacking and Cyber Terrorism: The Real Threats in the New Millennium. Computers and Security, 1999. Vol. 18. No. 1. 28–34. o.

GALLAGHER, Aoife – DAVEY, Jacob – HART, Mackenzie: The Genesis of a Conspiracy Theory: Key trends in QAnon activity since 2017. Institute for Strategic Dialogue,

London/Washington DC/Beirut/Toronto, 2020. 3. o. https://www.isdglobal.org/wp-content/uploads/2020/07/The-Genesis-of-a-fganorConspiracy-Theory.pdf (2021.11.05.)

GANOR, Boaz: Defining Terrorism: Is One Man's Terrorist another Man's Freedom Fighter? Police Practice and Research: An International Journal, 2002. Vol. 3. No. 4. 304. o.

GÁL Bence – NÉMETH András: Additív gyártástechnológiák katonai alkalmazásának vizsgálata, különös tekintettel a katonai elektronika területére. Hadmérnök, 2019/1. 231–249. o.

GÁLIK Mihály: Visszhangkamrák és szűrőbuborékok. Médiakutató, 2020/1. 28. o.

GÁL István László: A XXI. század új bűncselekmény-típusa: a terrorizmus finanszírozása. Rendészeti Szemle: Az Igazságügyi És Rendészeti Minisztérium Szakmai, Tudományos Folyóirata, 2009/6. 61–90. o.

GÁL István László: A büntetőjog szerepe a gazdaságban, avagy megelőzhetők-e a brókerbotrányok büntetőjogi eszközökkel? 2017, 1. o. https://ujbtk.hu/prof-dr-gal-istvan-laszlo-a-buntetojog-szerepe-a-gazdasagban-avagy-megelozhetok-e-a-brokerbotranyok-buntetojogi-eszkozokkel/ (2021.09.01.)

GÁL István László: A koronavírus (COVID-19) és az általa okozott gazdasági világválság lehetséges hatásai a bűnözésre. Magyar Jog, 2020/5. 258. o.

GÁL István László: A terrorizmus finanszírozása. PTE Állam- és Jogtudományi Kar Gazdasági Büntetőjogi Kutatóintézet, Pécs, 2010. 3. o.

GÁL István László: A terrorizmus finanszírozásának fogalma és technikái a XXI. században. Szakmai Szemle, 2016/2. 91. o.

GÁL István László: A tőkepiac büntetőjogi védelme Magyarországon. Kódex Nyomda Kft, Pécs, 2019. 153. o.

GÁL István László: Bejelentés vagy feljelentés? : A pénzmosás és a terrorizmus

finanszírozása elleni küzdelemmel kapcsolatos feladatok és kötelezettségek. Penta Unió, Pécs, 2009. 169–171. o.

GÁL István László: Korrelációs kapcsolat az illegális migráció és a terrorizmus finanszírozásának volumene között. In: GAÁL Gyula – HAUTZINGER Zoltán (szerk.): Pécsi Határőr Tudományos Közlemények XXI.: A bűnüldözés és a bűnmegelőzés rendészettudományi tényezői. Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoportja, Pécs, 2019. 217. o.

GÁL István László: Új biztonságpolitikai kihívás a XXI. században: a terrorizmus finanszírozása. Szakmai Szemle, 2012/1. 15. o.

GEARTY, Conor: Terror. Holnap Kiadó, Budapest, 1994. 31. o.

GING, Debbie: Alphas, Betas, and Incels: Theorizing the Masculinities of the Manosphere. Men and Masculinities, 2019. Vol. 22. No. 4. 638. o.

Global Terrorism Index 2015: Measuring and Understanding the Impact of Terrorism. Institute for Economics and Peace, Sydney, 2015. 4. o. https://www.visionofhumanity.org/wp-content/uploads/2020/10/2015-Global-Terrorism-Index-Report.pdf (2021.06.14.)

Global Terrorism Index 2017: Measuring and Understanding the Impact of Terrorism. Institute for Economics and Peace, Sydney, 2017. 6. o. https://reliefweb.int/sites/reliefweb.int/files/resources/Global%20Terrorism%20Index%202017%20%284%29.pdf (2021.11.01.)

Global Terrorism Index 2020: Measuring the Impact of Terrorism. Institute for Economics and Peace, Sydney, 2020. 2. o. https://www.visionofhumanity.org/wp-content/uploads/2020/11/GTI-2020-web-2.pdf (2021.06.24.)

GOLDMAN, Zachary K. –MARUYAMA, Ellie – ROSENBERG, Elizabeth –SARAVALLE, Edoardo – SOLOMON-STRAUSS, Julia: Terrorist Use Of Virtual Currencies: Containing the Potential Threat. CNAS, 2017. 19. o. https://www.lawandsecurity.org/wp-content/uploads/2017/05/CLSCNASReport-

TerroristFinancing-Final.pdf (2021.09.12.)

GRADOŃ, Kacper: Crime in the time of the plague: fake news pandemic and the challenges to law-enforcement and intelligence community. Society Register, 2020. Vol. 4. No. 2. 134. o.

GRAHAM, Robert: How Terrorists Use Encryption. CTC Sentinel, 2016. Vol. 9. No. 6. 25. o.

GUADAGNO, Rosanna E. – LANKFORD, Adam – MUSCANELL, Nicole L. – OKDIE, Bradley M. – MCCALLUM, Debra M.: Social Influence in the Online Recruitment of Terrorists and Terrorist Sympathizers: Implications for Social Psychology Research. Revue Internationale de Psychologie Sociale, 2010. Vol. 23. No. 1. 27. o.

GULYÁS Attila: Vállalatbiztonság és a dark web. Biztonságtudományi Szemle, 2021/3. 29–30. o.

HAIG Zsolt: Információs műveletek a kibertérben. Dialóg Campus Kiadó, Budapest, 2018. 301–302. o.

HAIG Zsolt: Internet terrorizmus. Nemzetvédelmi Egyetemi Közlemények, 2007/2. 84–85. o.

HAMMING, Tore Refslund: Global Jihadism after the Syria War. Perspectives On Terrorism, 2019. Vol. 13. No. 3. 11. o.

HANKISS Ágnes: A színfalak mögött - az al-Kaida médiastratégiája. ARC ÉS ÁLARC, 2018/3–4. 216. o.

HANKISS, Ágnes: Behind the Scenes of Al-Qa`ida's Media Strategy. Journal of Strategic Security, 2019. Vol. 12. No. 2. 67–68. o.

HANKISS Ágnes: Kihívások és ellentmondások a terrorizmus elleni harcban. In: DÁNOS Valér (szerk.): A terrorizmus Rubik-kockája, avagy a fenyegetések komplex megközelítése: Nemzetközi tudományos-szakmai konferencia: Rubik's cube of

terrorism or complex approach to the threats: International scientific and professional conference. BM Oktatási, Képzési és Tudományszervezési Főigazgatóság, Budapest, 2014. 98–99. o.

HASTINGS, Zoe – JONES, David – STOLTE, Laura: Involuntary Celibates: Background for Practitioners. Organization for the Prevention of Violence, Edmonton, 2020. 2. o.

HAUTZINGER Zoltán: A terrorizmus elleni küzdelem idegenjogi eszközei. In: GAÁL Gyula – HAUTZINGER Zoltán (szerk.): Pécsi Határőr Tudományos Közlemények XVI.: Modernkori veszélyek rendészeti aspektusai. Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoportja, Pécs. 2015. 203. o.

HAYS, G. – T., Ivan – JENZEN-JONES, N. R.: Desktop Firearms: Emergent Small Arms Craft Production Technologies. ARES Research Report No. 8. Armament Research Services (ARES), Perth, 2020. 13–16. o. http://armamentresearch.com/wp-content/uploads/2020/03/ARES-Research-Report-8-Desktop-Firearms.pdf (2021.08.30.)

HEGEMANN, Hendrik – KAHL, Martin: Was ist Terrorismus? Eine schwierige Begriffsbestimmung. In: HEGEMANN, Hendrik – KAHL, Martin (szerk.): Terrorismus und Terrorismusbekämpfung: Eine Einführung. Springer VS, Wiesbaden, 2018. 13. o.

HOFFMAN, Bruce – WARE, Jacob – SHAPIRO, Ezra: Assessing the Threat of Incel Violence. Studies in Conflict & Terrorism, 2020. Vol. 43. No. 7. 565. o.

HOLT, Chris – BRANIFF, William – SMITH, Jerry: In the Eye of the Storm: An Update: Managing Terrorism and Asymmetric Threats during Covid-19. CHC Global & START, 2020. 4. o. https://www.start.umd.edu/sites/default/files/publications/local_attachments/IntheEyeoftheStorm.pdf (2021.06.21.)

HOLT, Thomas J. – FREILICH, Joshua D. – CHERMAK, Steven M.: Examining the Online Expression of Ideology among Far-Right Extremist Forum Users. Terrorism and Political Violence, 2020. 2. o.

HONSBERGER, Hanna – WERNER, Denis – RHUMORBARBE, Damien – RIVA, Fabiano – GLARDON, Matthieu – GALLUSSER, Alain – DELÉMONT, Olivier: How to recognise the traces left on a crime scene by a 3D-printed Liberator? Part 2. Elements of ammunition, marks on the weapons and polymer fragments. Forensic Science International, 2019. Vol. 295. 144. o.

HONSBERGER, Hanna – RHUMORBARBE, Damien – WERNER, Denis – RIVA, Fabiano – GLARDON, Matthieu – GALLUSSER, Alain – DELÉMONT, Olivier: How to recognize the traces left on a crime scene by a 3D-printed Liberator? Part 1. Discharge, exterior ballistic and wounding potential. Forensic Science International, 2018. Vol. 286. 246. o.

HORNYÁK Szabolcs: A büntetőjog-tudomány és a bűnügyi tudományok rendszere. In: BALOGH Ágnes – TÓTH Mihály (szerk.): Magyar Büntetőjog. Általános Rész. Osiris Kiadó, Budapest, 2015. 31-34. o.

HORVÁTH Ádám – KURUCZ Attila: A 3D nyomtatás története és jövőbeli kérdései. In: REISINGER Adrienn – KECSKÉS Petra (szerk.): "Ifjúság - jövőképek": Kautz Gyula Emlékkonferencia 2016. június 15. elektronikus formában megjelenő kötete. Széchenyi István Egyetem, Győr, 2017. 9. o.

HORVÁTH Attila: A terrorizmus és a média kapcsolatáról. Acta Humana, 2016/5. 38. o.

HORVÁTH L. Attila: A terrorista csoportok toborzásáról. Belügyi Szemle, 2015/7–8. 116–117. o.

HORVÁTH L. Attila: A terrorizmus csapdájában. Zrínyi Kiadó, Budapest, 2014. 12. o.

HORVÁTH Orsolya – MARÓTI Péter: 3D nyomtatott fegyverek – vélt vagy valós veszélyek? In: GAÁL Gyula – HAUTZINGER Zoltán (szerk.): Pécsi Határőr Tudományos Közlemények XX.: A XXI. század biztonsági kihívásai. Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoportja, Pécs, 2018. 78. o.

HOUBEN, Robby – SNYERS, Alexander: Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion. Policy Department for Economic, Scientific and Quality of Life Policies (European

Parliament), Brüsszel, 2018. 53–56. o. http://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf (2021.09.12.)

Incels: A guide to symbols and terminology. Moonshot, 2020. 1–19. o. http://moonshotcve.com/incels-symbols-and-terminology/ (2021.06.19.)

Internet Organised Crime Threat Assesment (IOCTA) 2019. Europol, Hága, 2019. 48. o. https://www.europol.europa.eu/iocta-report (2021.07.21.)

Investigating the impact of global stablecoins. G7 Working Group on Stablecoins, 2019. 7. o. https://www.bis.org/cpmi/publ/d187.pdf (2021.09.03.)

IRWIN, Angela – SLAY, Jill: Detecting Money Laundering and Terrorism Financing Activity in Second Life and World of Warcraf. In: VALLI, Craig (szerk.): Proceedings of the 1st International Cyber Resilience Conference ICR2010. Edith Cowan University, Perth, 2010. 41. o.

IRWIN, Angela S. M. – SLAY, Jill – CHOO, Kim-Kwang Raymond – LIU, Lin: Money laundering and terrorism financing in virtual environments: a feasibility study. Journal of Money Laundering Control, 2014. Vol. 17. No. 1. 50–75. o.

JACOBS, James B. – HABERMAN, Alex: 3D-Printed Firearms, Do-It-Yourself Guns, & the Second Amendment. Law and Contemporary Problems, 2017. Vol. 80. No. 2. 141–144. o.

JARDINE, Eric: The Dark Web Dilemma: Tor, Anonymity and Online Policing. Centre for International Governance Innovation, London, 2015. 7. o. https://www.cigionline.org/sites/default/files/no.21.pdf (2021.08.09.)

JASENSZKY Nándor (szerk.): Mindennapi biztonság. Terrorelhárítási Központ, Budapest, 2019. 7. o.

JAVED, Bilal – SARWER, Abdullah – SOTO, Erik B. – MASHWANI, Zia-ur-Rehman: The coronavirus (COVID-19) pandemic's impact on mental health. International Journal of

Health Planning and Management, 2020. Vol. 35. No. 5. 993–996. o.

JOHNSTON, Patrick B. – ALAMI, Mona – CLARKE, Colin P. – SHATZ, Howard J.: Return and Expand? The Finances and Prospects of the Islamic State After the Caliphate. RAND Corporation, Santa Monica, 2019. IX. o. https://www.rand.org/content/dam/rand/pubs/research_reports/RR3000/RR3046/RAND_RR3046.pdf (2022.01.05.)

JÓZSA László: Globális terrorizmus – fogalmi keretek. In: TÁLAS Péter (szerk.): Válaszok a terrorizmusra avagy van-e út az afganisztáni „vadászattól" a fenntartható globalizációig. SVKH–CHARTAPRESS, Budapest, 2002. 93. o.

KASZNÁR Attila: Az európai terrorelhárítás jelene és jövője. In: DRUSZA Tamás (szerk.): A magyar elhárítás fejlődése: Tanulmányok a katonai és polgári nemzetbiztonsági elhárítás múltjáról, jelenéről, jövőjéről. Dialóg Campus Kiadó, Budapest, 2019. 191. o.

KASZNÁR Attila: Terroristák a közösségi hálón. In: LEZSÁK, Sándor (szerk.): Túlélési ösztön: Írások a Magyar Hírlapban megjelent Nemzeti Fórumos szerzőktől 2015-2021. Antológia Kiadó és Nyomda Kft., Lakitelek, 2021. 49–51. o.

KATONA László: A terrorizmus és a szervezett bűnözés elhatárolásának aktuális dilemmái. Felderítő Szemle, 2013/3. 70. o.

KATONA Tamás: Decentralizált pénzügy – A blokkláncon működő pénzlegó-rendszer lehetőségei. Hitelintézeti Szemle, 2021/1. 78. o.

KEATINGE, Tom – CARLISLE, David – KEEN, Florence: Virtual currencies and terrorist financing: assessing the risks and evaluating responses. Policy Department for Citizens' Rights and Constitutional Affairs, 2018. 9. o. https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf (2021.09.12.)

KEATINGE, Tom – DANNER, Kerstin: Assessing Innovation in Terrorist Financing. Studies in Conflict & Terrorism, 2021. Vol. 44. No. 6. 467. o.

KEATINGE, Tom – KEEN, Florence: Social Media and Terrorist Financing What are the Vulnerabilities and How Could Public and Private Sectors Collaborate Better? Global Research Network on Terrorism and Technology: Paper No. 10, Royal United Services Institute for Defence and Security Studies, 8. o.
https://rusi.org/sites/default/files/20190802_grntt_paper_10.pdf (2021.09.12.)

KIRBY, Aidan: The London Bombers as ‘ Self-Starters ’: A Case Study in Indigenous Radicalization and the Emergence of Autonomous Cliques. Studies in Conflict & Terrorism, 2007. Vol. 30. No. 5. 425. o.

KIS-BENEDEK József: Az Iraki és Levantei Iszlám Állam (ISIL) és az ellene folytatott küzdelem tendenciái. Hadtudomány, 2016/1–2. 33. o.

KIS-BENEDEK József: Dzsihadista fészkek, mint a terrorizmus lehetséges kiindulópontjai. Hadtudomány, 2017/1–2. 97. o.

KIS-BENEDEK József: Dzsihadizmus, radikalizmus, terrorizmus. Zrínyi Kiadó, Budapest, 2016. 195–196. o.

KIS-BENEDEK József: Katonai biztonság Marokkótól Iránig. Zrínyi Kiadó, Budapest, 2018. 246. o.

KIS-BENEDEK József – KENEDLI Tamás: A terrorfenyegetettség új tendenciái és lehetséges válaszlépések. Szakmai Szemle, 2015/1. 31. o.

KIS-BENEDEK József: The Islamic State and the intelligence. Nemzetbiztonsági Szemle, 2015/különsz. 47. o.

KISS Tibor: A terrorizmus arculatváltásának hatása a helyszíni reagálóerők felkészítésére. Honvédségi Szemle – Hungarian Defence Review, 2021/5. 17–34 o.

KISS Zoltán László: A terrorizmus elleni küzdelem szociológiai természetű kihívásai. Hadtudomány, 2005/4. 182–187. o.

KLEINBERG, Bennett – VAN DER VEGT, Isabelle – GILL, Paul: The temporal evolution

of a far-right forum. Journal of Computational Social Science, 2021. Vol. 4. No. 1. 1–2. o.

KOEHLER, Daniel: The Halle, Germany, Synagogue Attack and the Evolution of the Far-Right Terror Threat. CTC Sentinel, 2019. Vol. 12. No. 11. 14. o.

KOLONTÁRI Attila: Az afganisztáni szovjet beavatkozás külső és belső körülményei. In: DÁVID Ferenc – KOLONTÁRI Attila – LENGYEL Gábor (szerk.): Afganisztán – 1979-89-99-2009. Moszt, Pécs, 2010. 32–38. o.

KORINEK László: A terrorizmus. In: GÖNCZÖL Katalin – KEREZSI Klára – KORINEK László – LÉVAY Miklós (szerk.): Kriminológia-Szakkriminológia. CompLex Kiadó Jogi és Üzleti Tartalomszolgáltató Kft., Budapest, 2006. 451–452. o.

KORINEK László: A terrorizmus. Belügyi Szemle, 2015/7–8. 17–19. o.

KOUDELA Pál: Játékelmélet a kiberbiztonságban. Hadtudomány, 2019/4. 39. o.

KOU, Yubo – GUI, Xinning – CHEN, Yunan – PINE, Kathleen: Conspiracy Talk on Social Media. Proceedings of the ACM on Human-Computer Interaction, 2017. Vol. 1. No. 2. 1–21. o.

KOVÁCS István: Rendvédelmi ismeretek I. Magyar Rendészettudományi Társaság, Budapest, 2021. 32. o.

KOVÁCS Márk Károly: Az al-Káida céljai, szervezete és működése, módszerei és eljárásai a Nyugat ellen 1989 és 2015 között. Hadtudományi Szemle, 2021/1. 54. o.

KOVÁCS Zoltán András: A polgári elhárítás negyedszázada (1990–2016). In: DRUSZA Tamás (szerk.): A magyar elhárítás fejlődése: Tanulmányok a katonai és polgári nemzetbiztonsági elhárítás múltjáról, jelenéről, jövőjéről. Dialóg Campus Kiadó, Budapest, 2019. 169–170. o.

KOVÁCS Zoltán András: Adalékok az információszerzés történetéhez. In: BODA József – REGÉNYI Kund (szerk.): A hírszerzés története az ókortól napjainkig. Dialóg Campus

Kiadó, Budapest, 2019. 11. o.

KŐHALMI László: A migráció és a kriminalitás néhány összefüggése. Jura, 2016/1. 94–99. o.

KŐHALMI László: A vallási terrorizmus útjai. JURA, 2021/2. 32–33. o.

KŐHALMI László: Gondolatok a vallási indíttatású terrorizmus ürügyén. Belügyi Szemle, 2015/7–8. 53–54. o

KŐVÁGÓ Paulina: Az AQIM és a Boko Haram támadásainak okai és trendjének alakulása. In: MARSAI Viktor – VOGEL Dávid (szerk.): Közel Afrikához: A válságkezelés és a stabilizáció lehetőségei és kihívásai a fekete kontinensen. Dialóg Campus Kiadó, Budapest, 2017. 181. o.

KŐVÁRI László: Az északi regionális biztonsági komplexum és az Északi-sarkvidéki Tanács. Felderítő Szemle, 2019/1. 20. o.

KRAUT, Andrea – KŐHALMI, László – TÓTH, Dávid: Digital dangers of smartphones. Journal of Eastern-European Criminal Law, 2020. Vol. 7. No. 1. 36–49. o.

KULUNGU, Mustapha: Does Boko Haram Pose a Threat to the US? Counter Terrorist Trends and Analyses, 2019. Vol. 11. No. 2. 9. o.

KWON, Sang Jib – PARK, Eunil, – KIM, Ki Joon: What drives successful social networking services? A comparative analysis of user acceptance of Facebook and Twitter. The Social Science Journal, 2014. Vol. 51 No. 4. 534–544. o.

LABBAF, Farshad: United by Rage, Self-Loathing, and Male Supremacy: The Rise of the Incel Community. Invoke, 2019. Vol. 5. 17-18. o.

LAKOMY, Miron: Between the "Camp of Falsehood" and the "Camp of Truth": Exploitation of Propaganda Devices in the "Dabiq" Online Magazine. Studies in Conflict & Terrorism, 2020. 1. o.

LAKOMY, Miron: Islamic State's Online Propaganda: A Comparative Analysis. Routledge, London, 2021. 1. o.

LEWANDOWSKY, Stephan – COOK, John: Az összeesküvés-elméletek kézikönyve. Center for Climate Change Communication, Fairfax, 2020. 3. o.

LIEBERMAN, Ariel Victoria: Terrorism, the Internet, and Propaganda: A Deadly Combination. Journal of National Security Law and Policy, 2017. Vol. 9. No. 1. 101. o.

LIV, Nadine: Jihadists' Use of Virtual Currency. ICT, Herzliya, 2019. 6. o. https://www.ict.org.il/images/Jihadists%20use%20of%20virtual%20currency%202.pdf (2021.09.12.)

LOCK, Etienne: Nigeria: Understanding Boko Haram. Conflict Studies Quarterly, 2020. No. 30. 80–81. o.

LUYTEN, Katrien: Addressing the dissemination of terrorist content online. European Parliamentary Research Service, 2020. 2–3. o. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/649326/EPRS_BRI(2020)649326_EN.pdf (2021.07.29.)

MACDONALD, Stuart: Terrorist Narratives & Communicative Devices: Findings from a Study of Online Terrorist Magazines. In: ZEIGER, Sara (szerk.): Expanding Research on Countering Violent Extremism. Hedayah and Edith Cowan University, Perth, 2016. 128. o.

MACKLIN, Graham: The El Paso Terrorist Attack: The Chain Reaction of Global Right-Wing Terror. CTC Sentinel, 2019. Vol. 12. No. 11. 1. o.

MAHMOOD, Omar S.: More than propaganda A review of Boko Haram's public messages. Instutute for Security Studies, Pretoria, 2017. 24–25. o. https://www.ecoi.net/en/file/local/1426834/1226_1521122538_war20.pdf (2021.06.14.)

MALEFAKIS, Medinat Abdulazeez: Social Media Dynamics in Boko Haram's Terrorist Insurgence. Policy Brief No. 50. Toda Peace Institute, Tokyo, 2019. 5–6. o.

https://toda.org/assets/files/resources/policy-briefs/t-pb-50_medinat-a.-malefakis_social-media-dynamics-and-boko-harams-terrorist-insurgence.pdf (2021.06.14.)

MALIK, Nikita: Terror in The Dark: How Terrorists use Encryption, the Darknet and Cryptocurrencies. The Henry Jackson Society. London, 2018. iv. o. https://henryjacksonsociety.org/wp-content/uploads/2018/04/Terror-in-the-Dark.pdf (2021.08.09.)

MARAS, Marie Helen: A terrorizmus elmélete és gyakorlata. Antall József Tudásközpont, Budapest, 2016. 244–245. o.

MARSAI Viktor – TRESZKAI Ákos: Radikális iszlamista csoportok az afrikai kontinensen. In: MARSAI Viktor (szerk.): Afrika a globalizált világban: Lehetőségek és kihívások. Dialóg Campus, Budapest, 2019. 268. o.

MATUS János: A Trump elnökség tanulságai: Karakter és vezetés. Hadtudomány, 2020/4. 73. o.

MAZA, Kangdim Dingji – KOLDAS, Umut – AKSIT, Sait: Challenges of Countering Terrorist Recruitment in the Lake Chad Region: The Case of Boko Haram. Religions, 2020. Vol. 11. No. 2. 14–15. o.

MÁTÉ István Zsolt: A digitális bűnfelderítés gyakorlata, avagy az igazságügyi informatikai szakértő a büntetőeljárásban. In: GAÁL Gyula – HAUTZINGER Zoltán (szerk.): Pécsi Határőr Tudományos Közlemények XIV.: Tanulmányok „A változó rendészet aktuális kihívásai" című tudományos konferenciáról. Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoportja, Pécs, 2013. 365. o.

MÁTÉ István Zsolt: Informatikai rendszerek elleni támadások szakértői vizsgálata – a digitális nyomok rögzítésének szerepe. Belügyi Szemle, 2018/7–8. 38. o.

MC 0472/1 MILITARY COMMITTEE CONCEPT FOR COUNTER – TERRORISM. North Atlantic Military Committee, 2016. 5. o. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_01/20160817_160106-mc0472-1-final.pdf (2021.10.28.)

MCBRIDE, Megan – GOLD, Zack – SCHRODEN, Jonathan – FREY, Lauren: Cryptocurrency: Implications for Special Operations Forces. CNA, Arlington, 2019. 5. o. https://www.cna.org/CNA_files/PDF/CRM-2019-U-020186-Final.pdf (2021.09.12.)

MCCROSSAN, Sean: Combating the Proliferation of Mobile and Internet Payment Systems as Money Laundering Vehicles. ACAMS CAMS-FCI, USA, 2015. 15. o. https://www.acams.org/wp-content/uploads/2015/08/Combating-the-Proliferation-of-Mobile-and-Internet-Payment-Systems-as-ML-Vehicles-S-McCrossan.pdf (2021.09.12.)

MELIÁ, Manuel Cancio: Terrorism and Criminal Law: The Dream of Prevention, the Nightmare of the Rule of Law. New Criminal Law Review, 2011. Vol. 14. No. 1. 122. o.

MELOY, J. Reid – O'TOOLE, Mary Ellen: The Concept of Leakage in Threat Assessment. Behavioral Sciences and the Law, 2011. Vol. 29. No. 4. 513–527. o.

MIHÁLY Laura Dominika: Az Európai Unió válasza az új globális kihívásokra, avagy a médiamegosztóplatform-szolgáltatások terrorista tartalmaival szembeni fellépés jogi eszköztára. In: TAMÁS Csaba Gergely (szerk.): Magyarország és a közép-európai térség az Európai Unióban: Díjnyertes pályázatok 2020. Országgyűlés Hivatala, Budapest, 2021. 120–121. o.

MILTON, Daniel: Down, but Not Out: An Updated Examination of the Islamic State's Visual Propaganda. Combating Terrorism Center at West Point, United States Military Academy, West Point, 2018. 51. o

MIREA, Mihnea – WANG, Victoria – JUNG, Jeyong: The not so dark side of the darknet: a qualitative study. Security Journal, 2019. Vol. 32. 107. o.

MISIAK, Błażej – SAMOCHOWIEC, Jerzy – BHUI, Kamaldeep – SCHOULER-OCAK, Merryam – DEMUNTER, Hella – KUEY, Levent – RABALLO, Andrea – GORWOOD, Philip – FRYDECKA, Dorota – DOM, Geert: A systematic review on the relationship between mental health, radicalization and mass violence. European Psychiatry, 2018. Vol. 56. No. 1. 57. o.

MOHAMEDOU, Mohammad-Mahmoud Ould: A Theory of ISIS: Political Violence and the Transformation of the Global Order. Pluto Press, London, 2018. 205. o.

MOISEIENKO, Anton – IZENMAN, Kayla: Gaming the System: Money Laundering Through Online Games. RUSI Newsbrief, 2019. Vol. 39. No. 9. 1. o.

MOLNÁR István Jenő: A bűnmegelőzés értelmezése és magyarországi fejlődése. In: GAÁL Gyula – HAUTZINGER Zoltán (szerk.): Pécsi Határőr Tudományos Közlemények XXI.: A bűnüldözés és a bűnmegelőzés rendészettudományi tényezői. Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoportja, Pécs, 2019. 89. o.

MOORE, Daniel – RID, Thomas: Cryptopolitik and the Darknet. Survival: Global Politics and Strategy, 2016. Vol. 58. No. 1. 24. o.

MORING, Tom: Terrorism, Media and the State: An Incestuous Spiral. In: HUSBAND, Charles (szerk.): Social Cohesion, Securitization and Counter-terrorism. Vol. 11. No. 11. University of Helsinki, COLLeGIUM: Studies across Disciplines in the Humanities and Social Sciences, Helsingfors, 2012. 80. o.

MUDDE, Cas: The Ideology of the Extreme Right. Manchester University Press, Manchester/New York, 2000. 11. o.

MUELLER, John – STEWART, Mark G.: Terrorism, counterterrorism, and the internet: The American cases. Dynamics of Asymmetric Conflict, 2015. Vol. 8. No. 2. 176–190. o.

NAGY Henriett: A pénzmosás magyarországi jogi szabályozásának vázlata. Magyar Rendészet, 2020/1. 97. o.

NAGY Katalin – MEZEI József: A biztonságtudatosítás megjelenése a terrorelhárítás területén. Nemzetbiztonsági Szemle, 2019/4. 106. o.

NAGY Melánia: A női terrorizmus. Pécsi Tudományegyetem Állam-és Jogtudományi Kar, Pécs, 2021.

NAGY Zoltán András: A joghatóság problémája a kiberbűncselekmények nyomozásában. In: HOMOKI-NAGY Mária – KARSAI Krisztina – FANTOLY Zsanett – JUHÁSZ Zsuzsanna –

SZOMORA Zsolt – GÁL Andor (szerk.): Ünnepi Kötet Dr. Nagy Ferenc Egyetemi Tanár 70. Születésnapjára. Szegedi Tudományegyetem Állam- és Jogtudományi Kar, Szeged, 2018. 755. o.

NAGY Zoltán András: A kiber-háború új dimenzió – a veszélyeztett állambiztonság (Stuxnet, DuQu, Flame – a Police malware). In: GAÁL Gyula – HAUTZINGER Zoltán (szerk.): Pécsi Határőr Tudományos Közlemények XIII: Tanulmányok „A Biztonság Rendészettudományi Dimenziói – Változások És Hatások" Című Tudományos Konferenciáról. Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport, Pécs, 2012. 221. o.

NAGY Zoltán András: A 3D nyomtatás, mint a jogrendszert érintő új kihívás. Magyar Jog, 2017/10. 613 – 621. o.

NAGY Zoltán András: Tradicionális bűncselekmények számítógépes hálózatokon. JURA, 2007/1. 127. o.

National Terrorist Financing Risk Assessment. 2018. 3. o. https://home.treasury.gov/system/files/136/2018ntfra_12182018.pdf (2021.09.12.)

NEPARÁCZKI Anna Viktória: A terrorizmus finanszírozása bűntettének szabályozása a nemzetközi elvárásokra figyelemmel. Ügyészségi Szemle, 2017/2. 7. o.

NESZMÉLYI György Iván: Őrségváltás Afrika óriásánál: Nigéria gazdasági és társadalmi kihívásai. In: VÁGÁNY Judit – FENYVESI Éva (szerk.): Multidiszciplináris kihívások, sokszínű válaszok: Tanulmánykötet. Budapesti Gazdasági Egyetem, Kereskedelmi, Vendéglátóipari és Idegenforgalmi Kar, Közgazdasági Intézeti Tanszéki Osztály, Budapest, 2016. 133. o.

NESZMÉLYI György: Nigéria perspektívái: kibontakozás vagy káosz és terrorizmus? Nemzet és Biztonság, 2012/2. 69. o.

NISSEN, Thomas Elkjer: Terror.com – IS's Social Media Warfare in Syria and Iraq. Contemporary Conflicts, 2014. Vol. 2. No. 2. 1–8. o.

NITSCH, Holger: Terrorismus und die Nutzung des Internet. In: RÜDIGER, Thomas-Gabriel – BAYERL, Petra Saskia (szerk.): Cyberkriminologie: Kriminologie für das digitale Zeitalter. Springer VS, Wiesbaden, 2020. 198. o.

NSA: Games: A Look at Emerging Trends, Uses, Threats and Opportunities in Influence Activities. 2007. http://www.propublica.org/documents/item/889134-games (2021.09.12.)

NYESTE Péter – SZENDREI Ferenc: Nyílt forrású információszerzés a bűnüldözésben. Nemzetbiztonsági Szemle, 2019/2. 66. o.

OGUNLANA, Sunday O.: Halting Boko Haram / Islamic State's West Africa Province Propaganda in Cyberspace with Cybersecurity Technologies. Journal of Strategic Security, 2019. Vol. 12. No. 1. 91. o.

OLAYOKU, Philip: Boko Haram and the Covid-19 Propaganda Dynamics. Spoor Africa, 2020. 9. o. https://spoorafrica.org/storage/data/spoorafrica.org/6b7b0ab7-c49d-49ae-98ca-30febb4a61cf.pdf (2021.06.14.)

OLOFINBIYI, Sogo Angel: The Intractable Malaise: Understanding the Patterns That Maintain the Terrorist Stronghold in Nigeria. SAGE Open, 2021. No. 2. 8. o.

O'MALLEY, Roberta Liggett – HOLT, Karen – HOLT, Thomas J.: An Exploration of the Involuntary Celibate (Incel) Subculture Online. Journal of Interpersonal Violence, 2020. 1. o.

OMENMA, J. Tochukwu – HENDRICKS, Cheryl – AJAEBILI, Nnamdi C.: al-Shabaab and Boko Haram: Recruitment Strategies. Peace and Conflict Studies, 2020. Vol. 27. No. 1. 14. o.

Online Harms White Paper.
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/973939/Online_Harms_White_Paper_V2.pdf (2021.06.21.)

ONUOHA, Freedom: Boko Haram and the evolving Salafi Jihadist threat in Nigeria. In:

PÉROUSE DE MONTCLOS, Marc-Antoine (szerk.): Boko Haram: Islamism, politics, security and the state in Nigeria. African Studies Centre, Leiden, 2014. 163. o.

ONYIA, Chukwuma: Understanding the ISIS Threat in the Lake Chad Basin. African Journal on Terrorism, 2020. Vol. 9. No. 1. 65. o.

ÖZKAYA, Erdal: The Use of Social Media for Terrorism. NATO Defence Against Terrorisim Review, 2017. Vol. 9. 47–59. o.

PAOLI, Giacomo Persi: The Trade in Small Arms And Light Weapons on the Dark Web: A Study. UNODA Occasional Papers, Number 32. United Nations Office for Disarmament Affairs (UNODA), New York, 2018. 59–60. o.

PAPASAVVA, Antonis – BLACKBURN, Jeremy – STRINGHINI, Gianluca – ZANNETTOU, Savvas – DE CRISTOFARO, Emiliano: "Is it a Qoincidence?": A First Step Towards Understanding and Characterizing the QAnon Movement on Voat.co. In: LESKOVEC, Jure – GROBELNIK, Marko – NAJORK, Marc – TANG, Jie – ZIA, Leila (szerk.): WWW '21: Proceedings of the Web Conference 2021. Association for Computing Machinery, New York, 2021. 460. o.

PARDY Balázs: Az első 3D nyomtatott lőfegyverrel kapcsolatban felmerült alkotmányjogi kérdések az Amerikai Egyesült Államokban. Iustum Aequum Salutare, 2018/3. 185–202. o.

PASCA, Viorel - ORZA, Daniela Simona: Terrorism: between the need for funding and obtaining funding sources. Journal Of Eastern-European Criminal Law, 2019. Vol. 6. No. 1. 227. o.

PASHENTSEV, Evgeny N. – BAZARKINA, Darya Yu: ISIS Propaganda on the Internet, and Effective Counteraction. Journal of Political Marketing, 2021. Vol. 20. No. 1. 19. o.

PEARSON, Elizabeth – ZENN, Jacob: Boko Haram, the Islamic State, and the Surge in Female Abductions in Southeastern Niger. ICCT, Hága, 2021. 3. o. https://icct.nl/app/uploads/2021/02/Pearson-And-Zenn-research-paper.pdf (2021.06.14.)

PERRY, Nicholas J.: The Numerous Federal Legal Definitions of Terrorism: The Problem of too Many Grails. Journal of Legislation, 2004. Vol. 30. No. 2. 249. o.

PIAZZA, James A. – GULER, Ahmet: The Online Caliphate: Internet Usage and ISIS Support in the Arab World, Terrorism and Political Violence, 2019. 1. o.

PÓCZIK Szilveszter – SÁRIK Eszter – VASS Péter – BOLYKY Orsolya: A COVID-19 pandémia egyes kriminológiai aspektusai. Belügyi Szemle, 2021/3. 376. o.

PRANTNER Zoltán: Iszlám Állam - A világ legvéresebb terrorszervezete. Pannon-Literatúra Kft., Kisújszállás, 2016. 104. o.

RADA Mátyás – VAJDA Viktor: A terrorizmus elleni küzdelem, avagy a 22-es csapdája. Külügyi Szemle, 2010/1. 148. o.

RAMSAY, Gilbert: Why terrorism can, but should not be defined. Critical Studies on Terrorism, 2015. Vol. 8. No. 2. 211-228. o.

RAPOPORT, David C.: Fear and Trembling: Terrorism in Three Religious Traditions. The American Political Science Review, 1984. Vol. 78. No. 3. 664–665. o.

RAPOPORT, David C.: The Four Waves of Modern Terrorism. In: CRONIN, Audrey Kurth – LUDES, James M. (szerk.): Attacking Terrorism: Elements of a Grand Strategy. Georgetown University Press, Washington, D.C., 2004. 47.o

RAPOPORT, David C.: The Four Waves of Rebel Terror and September 11. Anthropoetics, 2002. Vol. 8. No. 1. 3. o.

RATHOD, Digvijaysinh: Darknet Forensics. International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), 2017. Vol. 6. No. 4. 78. o.

RAZALI, Nuruddin Bin – SURADI, Nur Razia binti Mohd: A Nest for Cyber Criminals: The Dark Web. IEEE, 2019. 2. o.
https://www.academia.edu/40783401/A_nest_for_cyber_criminals_-the_dark_web (2021.08.03.)

REEVE, Zoey: Engaging with Online Extremist Material: Experimental Evidence. Terrorism and Political Violence, 2019. 2. o.

Report of the Attorney General's Cyber Digital Task Force: Cryptocurrency Enforcement Framework. United States Department of Justice, Washington, D.C., 2020. 11. o. https://www.justice.gov/archives/ag/page/file/1326061/download (2021.09.07.)

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

RESPERGER István: A nemzetbiztonsági szolgálatok tevékenysége – biztonsági kihívások, kockázatok és fenyegetések. In: RESPERGER István (szerk.): Nemzetbiztonsági alapismeretek. Dialóg Campus Kiadó, Budapest, 2018. 86. o.

RESPERGER István: Terrorista szervezetek, módszerek, eljárások. Szakmai Szemle, 2018/2. 18. o.

RÉPÁSI Krisztián: Az új-zélandi terrortámadást követő szélsőjobboldali merénylethullám. Szakmai Szemle, 2021/2. 59. o.

Risk Analysis for 2018. FRONTEX, Varsó, 2018. 8. o. https://frontex.europa.eu/assets/Publications/Risk_Analysis/Risk_Analysis/Risk_Analysis_for_2018.pdf (2021.10.07.)

Risk Analysis for 2020. FRONTEX, Varsó, 2020. 22. o. https://euagenda.eu/upload/publications/untitled-301445-ea.pdf (2021.10.07.)

RITECZ György: A terrorizmus és a migráció viszonya a számok alapján. Acta Humana, 2016/5. 103. o.

RITECZ György: Az Európába irányuló tömeges irreguláris migráció felfutásának és

megszűnésének okai. Hadtudomány, 2018/3–4. 66. o.

ROSE, Miss Menna – MORRISON, John: An exploratory analysis of leakage warning behavior in lone-actor terrorists. Behavioral Sciences of Terrorism and Political Aggression, 2021. 1–36. o.

ROTH, John – GREENBURG, Douglas – WILLE, Serena: National Commission on Terrorist Attacks Upon the United States: Monograph on Terrorist Financing: Staff Report to the Commission. National Commission on Terrorist Attacks upon the United States, Washington D.C., 2004. 19. o.

ROTTWEILER, Bettina – GILL, Paul: Conspiracy Beliefs and Violent Extremist Intentions: The Contingent Effects of Self-efficacy, Self-control and Law-related Morality. Terrorism and Political Violence, 2020. 14. o.

RUBASUNDRAM, Geetha A.: The Dark Web and Digital Currencies: A Potent Money Laundering and Terrorism Opportunity. International Journal of Recent Technology and Engineering (IJRTE), 2019. Vol 7. No. 5. 481. o.

RUDESILL, Dakota S. – CAVERLEE, James – SUI, Daniel: The Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box. Woodrow Wilson International Center for Scholars, Washington, DC, 2015. 4. o. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2676615 (2021.07.31.)

RYDGREN, Jens: The Radical Right: An Introduction. In: RYDGREN, Jens (szerk.): The Oxford Handbook of the Radical Right. Oxford University Press, New York, 2018. 9. o.

SACCO, Lisa N.: Domestic Terrorism and the Attack on the U.S. Capitol. Congressional Research Service, 2021. 1. o. https://crsreports.congress.gov/product/pdf/IN/IN11573 (2021.11.03.)

SALEH, Saad – QADIR, Junaid – ILYAS, Muhammad U.: Shedding Light on the Dark Corners of the Internet: A Survey of Tor Research. Journal of Network and Computer Applications, 2018. Vol. 114. 1. o.

SALIFU, Uyo – EWI, Martin: Boko Haram and violent extremism: Perspectives from peacebuilders. Institute for Security Studies, Pretoria, 2017. 7–8. o. https://media.africaportal.org/documents/policybrief97_1.pdf (2021.06.14.)

SCHÄFER, Matthias – STROHMEIER, Martin – LIECHTI, Marc – FUCHS, Markus –ENGEL, Markus – LENDERS, Vincent: BlackWidow: Monitoring the Dark Web for Cyber Security Information. In: Minárik, T. –Alatalu, S. – Biondi, S. – Signoretti, M. – Tolga, I. – Visky, G. (szerk.): 2019 11th International Conference on Cyber Conflict: Silent Battle. NATO CCD COE Publications, Tallinn, 2019. 3. o.

SCHMID, Alex: Terrorism - The Definitional Problem. Case Western Reserve Journal of International Law, 2004. Vol. 36. No. 2. 376. o.

SCHMID, Alex P. – JONGMAN, Albert J.: Political Terrorism: A New Guide to Actors, Concepts, Data Bases, Theories & Literature. Transaction Publishers, New Brunswick, 2008. 4–5. o.

SCHMID, Alex P.: Towards Joint Political Strategies for De-legitimising the Use of Terrorism. In: SCHMID, Alex P.: (szerk.): Countering Terrorism through International Cooperation. ISPAC, Milánó, 2001. 266–273. o.

SCRIVENS, Ryan – DAVIES, Garth – FRANK, Richard: Measuring the Evolution of Radical Right-Wing Posting Behaviors Online, Deviant Behavior, 2018. 1. o.

SCRIVENS, Ryan: Exploring Radical Right-Wing Posting Behaviors Online. Deviant Behavior, 2020. 3. o.

SCHWARTZ, Craig: 3D Printing: The Potential Implications and Challenges for Law Enforcement. The Police Chief, 2015. Vol. 82. No. 3. 65. o.

SIEBER, Ulrich – VOGEL, Benjamin: Terrorismusfinanzierung: Prävention im Spannungsfeld von internationalen Vorgaben und nationalem Tatstrafrecht. Duncker & Humblot, Berlin, 2015. 10. o.

SILBER, Mitchell D. – BHATT, Arvin: Radicalization in the West: The Homegrown

Threat. New York Police Department, New York, 2007. 8. o.

SILKE, Andrew: COVID-19 and terrorism: assessing the short-and long-term impacts. Cranfield: Pool Re Solutions, 2020. 2. o. https://www.poolre.co.uk/wp-content/uploads/2020/05/COVID-19-and-Terrorsim-report-V1.pdf (2021.09.30.)

SIMON Béla: A kriptovaluták és a kapcsolódó rendészeti kihívások. In: MEZEI Kitti (szerk.): A bűnügyi tudományok és az informatika. Pécsi Tudományegyetem Állam- és Jogtudományi Kar – MTA Társadalomtudományi Kutatóközpont, Budapest – Pécs, 2019. 169–186. o.

SINKÓ, Gábor: Shifting the Battle to Social Media: The Effectiveness of Boko Haram's Online Strategy in Terms of its Recruitment. Belügyi Szemle, 2021/1. különsz. 137. o.

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 (2021.09.12.)

SOHN, Werner: „Radikalisierung" Ein Hilfsmittel zur rhetorischen Bewältigung der aktuellen Sicherheitslage. Kriminalistik, 2017. No. 2. 67–72. o.

SOMKUTI Bálint – MAJOR Csaba: A terrorizmus modern kori megjelenési formái. In: BEBESI Zoltán (szerk.): Terrorelhárítási alapismeretek. Dialóg Campus, Budapest, 2016. 113–129. o.

Stablecoin: Taxonomy and Key Considerations. Global Digital Finance, 2019. https://www.gdf.io/wp-content/uploads/2019/05/GDF-Stablecoin-Key-Considerations_9-MAY-SUMMIT-DISCUSSION.pdf (2021.09.03.)

STERNISKO, Anni – CICHOCKA, Aleksandra – VAN BAVEL, Jay J.: The dark side of social movements: social identity, non-conformity, and the lure of conspiracy theories. Current Opinion in Psychology, 2020. Vol. 35. 1. o.

STEVENSON, John A. – PATE, Amy – ASIAMA, Elvis: Effective counter-terrorism against Boko Haram: empirical assessments of coercion, delegitimization, incentivization and

denial strategies in Nigeria (2009-2014). In: HENTZ, James J. – SOLOMON, Hussein (szerk.): Understanding Boko Haram: Terrorism and Insurgency in Africa. (Contemporary Terrorism Studies). Routledge, Abingdon, 2017. 192–193. o.

SZABOLCS Ottó (szerk.): Nemzetközi küzdelem a terrorizmus ellen: (A 2004. november 6-án rendezett országos konferencia előadásai). A Történelemtanári továbbképzés kiskönyvtára XXXVI. ELTE BTK – MTTTT, Budapest, 2005. 22–23. o.

SZABÓ, András László: Criminal Policy Approach to Lone Offenders and a Possible Model for their Identification. Nemzetbiztonsági Szemle, 2020/2. 76. o.

SZABÓ Csaba: A 3D nyomtatási technológiával előállított tűzfegyverek biztonságpolitikai kihívásainak vizsgálata a fegyverrendészet aspektusából I. Nemzetbiztonsági Szemle, 2017/4. 100. o.

SZABÓ Csaba: A 3D nyomtatási technológiával előállított tűzfegyverek biztonságpolitikai kihívásainak vizsgálata a fegyverrendészet aspektusából II. Nemzetbiztonsági Szemle, 2017/4. 123. o.

SZALAI Máté – WAGNER Péter: A terrorizmus fogalmának kiterjesztése? Értelmezési lehetőségek Orlando kapcsán. KKI-elemzések, 2016/19. 3. o.

SZÁSZ Antónia: A kiberbűnözés társadalmi kontextusa. In: KOVÁCS Janka – KÖKÉNYESSY Zsófia – LÁSZLÓFI Viola (szerk.): A normán innen és túl: Tanulmányok a Történeti Kollégium konferenciájának előadásaiból. ELTE BTK Történeti Kollégium, Budapest, 2017. 105. o.

SZŰCS László: Szíria és az Iszlám Államnak nevezett terrorszervezet egyedi vonásai 2018-ig. Szakmai Szemle, 2019/1. 8–9. o.

TANGHERLINI, Timothy R. – SHAHSAVARI, Shadi – SHAHBAZI, Behnam – EBRAHIMZADEH, Ehsan – ROYCHOWDHURY, Vwani: An automated pipeline for the discovery of conspiracy and conspiracy theory narrative frameworks: Bridgegate, Pizzagate and storytelling on the web. PLOS One, 2020. Vol. 15. No. 6. 34. o.

TARRANT, Brenton: The Great Replacement. https://www.ilfoglio.it/userUpload/The_Great_Replacementconvertito.pdf (2020.05.14.)

TAYLOR, Helen: Domestic terrorism and hate crimes: legal definitions and media framing of mass shootings in the United States. Journal of Policing, Intelligence and Counter Terrorism, Vol. 14. No. 3. 2019. 227. o.

TÁLAS Péter: A nemzetközi terrorizmus és a szervezett bűnözés hatása a nemzetközi biztonságra és Magyarország biztonságára. ZMNE Stratégiai Védelmi Kutatóintézet Elemzések, Budapest, 2007. 5–6. o.

TÁLAS Péter: A terrorizmusról hét évvel 9/11 után. Nemzet és Biztonság, 2008/9. 75. o.

TÁLAS Péter: Kelet-Közép-Európa és az új típusú terrorizmus. In: TÁLAS Péter (szerk.): A terrorizmus anatómiája. Zrínyi Kiadó, Budapest, 2006. 19–20. o.

TÁLAS Péter – PÓTI László – TAKÁCS Judit: A terrorizmus elleni küzdelem fogalmi és tartalmi keretei, különös tekintettel annak katonai dimenziójára. ZMNE Stratégiai Védelmi Kutató Központ Elemzések, 2004/3. 3. o.

TÁLAS Péter – RÁCZ András – AMBRUS Andrea: Az új-zélandi muszlimellenes terrortámadás és tanulságai. Nemzet és Biztonság – Biztonságpolitikai Szemle, 2019/3. 52–61. o.

TEICHMANN, Fabian Maximilian Johannes: Financing terrorism through cryptocurrencies – a danger for Europe? Journal of Money Laundering Control, 2018. Vol. 21. No. 4. 517. o.

Terrorism Report - 2002-2005. V. o. https://www.fbi.gov/file-repository/stats-services-publications-terrorism-2002-2005-terror02_05.pdf/view (2021.03.02.)

Texas Domestic Terrorism Threat Assessment. Texas Fusion Center Intelligence & Counterterrorism Division Texas Department of Public Safety, Texas, 2020. 3. o. https://www.dps.texas.gov/sites/default/files/documents/director_staff/media_and_communications/2020/txterrorthreatassessment.pdf (2021.06.19.)

The impact of the COVID-19 pandemic on terrorism, counter-terrorism and counering violent extremism. CTED, 2020. 2–3. o. https://www.un.org/sc/ctc/wp-content/uploads/2020/06/CTED-Paper%E2%80%93-The-impact-of-the-COVID-19-pandemic-on-counter-terrorism-and-countering-violent-extremism.pdf (2020.07.30.)

THOMAS, Timothy L.: Al Qaeda and the Internet: The Danger of "Cyberplanning." Parameters, 2003. Vol. 33. No. 1. 112–122. o.

TRIANDAFYLLIDOU, Anna – MAROUKIS, Thanos: Migrant smuggling: Irregular migration from Asia and Africa to Europe. Palgrave Macmillan, London. 2012. 1. o.

TOBIAS, Adam Z. – ROTH, Ronald N. – WEISS, Leonard S. – MURRAY, Keith – YEALY, Donald M.: Tree of Life Synagogue Shooting in Pittsburgh: Preparedness, Prehospital Care, and Lessons Learned. Western Journal of Emergency Medicine, 2020. Vol. 21. No. 2. 374. o.

TORMA Adrienne – BENDES Ákos László: A cybercrime és a gyermekpornográfia összeolvadása. In: BENDES Ákos – NAGY Melánia – TÓTH Dávid (szerk.): Lépést tud-e tartani a jog a XXI. század kihívásaival? Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola, Pécs, 2019. 20. o.

TOWNSHEND, Charles: A terrorizmus. Magyar Világ Kiadó, Budapest, 2003. 45. o.

TOWNSHEND, Charles: Terrorism: A Very Short Introduction, Third Edition. Oxford University Press, Oxford, 2018. 4. o.

TÓTH Dávid: A terrorizmus típusai és a kiberterrorizmus. In: RAB Virág (szerk.): XII. Országos Grastyán Konferencia előadásai. PTE Grastyán Endre Szakkollégium, Pécs, 2014. 286–296. o.

TÓTH Dávid: A virtuális pénzekkel kapcsolatos visszaélések. In: BARÁTH Noémi Emőke – MEZEI József (szerk.): Rendészet-Tudomány-Aktualitások: A rendészettudomány a fiatal kutatók szemével. Doktoranduszok Országos Szövetsége, Rendészettudományi

Osztálya, Budapest, 2019. 242–250. o.

TÓTH, Dávid: Credit card fraud with a comparative law approach. In: GORAN, Ilik – ANGELINA, Stanojoska (szerk.): International Scientific Conference "Towards a Better Future: Democracy, EU Integration and Criminal Justice", Conference Proceedings, Volume I. Faculty of Law - Kicevo, University "St. Kliment Ohridski", Bitola, 2019. 232. o.

TÓTH Mihály: A terrorcselekmény büntetőjogi szabályozásának és gyakorlatának változásai. Hadtudomány, 2013/1-2. 30–31. o.

TRIMBUR, Margot – AMAD, Ali – HORN, Mathilde – THOMAS, Pierre – FOVET, Thomas: Are radicalization and terrorism associated with psychiatric disorders? A systematic review. Journal of Psychiatric Research, 2021. Vol. 141. 214. o.

ULLAH, Rahman: The Coronavirus, the War on Terrorism, and the Taliban in Afghanistan. Review Of Human Rights, 2020. Vol. 6. No. 1. 43. o.

United Nations Office On Drugs And Crime: Education For Justiceuniversity Module Series: Counter-Terrorism: Module 1: Introduction To International Terrorism. United Nations, Bécs, 2018. 1. o. https://www.unodc.org/documents/e4j/18-04932_CT_Mod_01_ebook_FINALpdf.pdf (2021.10.28.)

Update on the impact of the COVID-19 pandemic on terrorism, counter-terrorism and countering violent extremism. United Nations Security Council Counter-Terrorism Committee Executive Directorate, 2021. 7. o. https://www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jun/cted_covid_paper_15june2021_1.pdf (2021.09.30.)

URBÁNYI András: Nemzetbiztonsági vs. Bűnügyi felderítés – a megszerzett információkkal való gazdálkodás kérdései. Szakmai Szemle, 2019/4. 28. o.

VADAI Ágnes: A terrorizmus a nemzetközi jogban. Egyetemi disszertáció. Budapesti Közgazdaságtudományi Egyetem, Budapest, 1997, 60. o.

VAN BRUNT, Brian – TAYLOR, Chris: Understanding and Treating Incels: Case Studies, Guidance, and Treatment of Violence Risk in the Involuntary Celibate Community. Routledge, New York, 2020.

VAN PROOIJEN, Jan-Willem – DOUGLAS, Karen M.: Belief in conspiracy theories: Basic principles of an emerging research domain. European Journal of Social Psychology, 2018. Vol. 48. No. 7. 897. o.

VARGA Ákos: Textuális és állóképtartalmak: online megjelenés. In: GÁLIK Mihály – CSORDÁS Tamás (szerk.): A média gazdaságtanának kézikönyve. Nemzeti Média- és Hírközlési Hatóság Médiatanács Médiatudományi Intézete, Budapest, 2020. 178. o.

VARGA Árpád: Az informatikai bűnözés fogalmi meghatározása, csoportosítása és helye a hazai jogfejlődésben. In Medias Res, 2019/1. 151. o.

VARGA Márton: Társadalmi biztonság a terrorizmus árnyékában. Hadtudomány, 2017/1–2. 134. o.

VASS György: A terrorizmus finanszírozása elleni küzdelem nemzetközi aspektusai. PhD Értekezés. Nemzeti Közszolgálati Egyetem, Budapest, 2016. 46.o

VASS György: Egységes meghatározás a terrorizmusra. Hadtudományi Szemle, 2009/4. 10. o.

VITO, Christopher – ADMIRE, Amanda – HUGHES, Elizabeth: Masculinity, aggrieved entitlement, and violence: considering the Isla Vista mass shooting. International Journal for Masculinity Studies, 2018. Vol. 13. No. 2. 97-98. o.

VOGT, Sophia Dastagir: The Digital Underworld: Combating Crime on the Dark Web in the Modern Era. Santa Clara Journal of International Law, 2017. Vol. 15. No. 1. 114–115. o.

VU, Anh V.: Cambridge Cybercrime Centre COVID Briefing Paper # 5: The Pandemic as Incels see it. University of Cambridge, Cambridge, 2020.

WAGNER Péter: Az al-Káida metamorfózisa. MKI-tanulmányok, 2011/30. 3. o.

WALDRON, Jeremy: Terrorism and the Uses of Terror. The Journal of Ethics, 2004. Vol. 8. No. 1. 35. o.

WALKER, Andrew: What Is Boko Haram? United States Institute Of Peace, Washington D.C., 2012. 7. o. https://www.usip.org/publications/2012/05/what-boko-haram (2021.06.14.)

WANG, Tao – ZHUANG, Jun: The True Meaning of Terrorism and Response to Terrorism. Social Sciences, 2017. Vol. 6. No. 6. 161. o.

WARE, Jacob: Testament to Murder: The Violent Far-Right's Increasing Use of Terrorist Manifestos. ICCT Policy Brief, Hága 2020. 1. o. https://icct.nl/app/uploads/2020/03/Jaocb-Ware-Terrorist-Manifestos2.pdf (2021.07.21.)

WEIMANN, Gabriel: Going Darker? The Challenge Of Dark Net Terrorism. Wilson Center, Washington, D.C., 2018. 8. o. https://cyber.haifa.ac.il/images/Publications/darkweb_Gabriel%20Weimann.pdf (2021.08.03.)

WEIMANN, Gabriel – MASRI, Natalie: The Virus of Hate: Far Right in Cyberspace. International Institute for Counter Terrorism, Herzliya, 2020, 12. o. https://www.ict.org.il/images/Dark%20Hate.pdf (2021.10.05.)

WEIMANN, Gabriel: Terrorist Migration to the Dark Web. Perspectives on Terrorism, 2016. Vol. 10. No. 3. 42. o.

WEIMANN, Gabriel: www.terror.net: How Modern Terrorism Uses The Internet. Special Report. United States Institute Of Peace, Washington D.C., 2004. 5–10. o. https://www.usip.org/sites/default/files/sr116.pdf (2021.07.13.)

WEISS, Michael – HASSAN, Hassan: Az Iszlám Állam: A terror hadserege belülről. HVG Kiadó Zrt., Budapest, 2015. 205–206. o.

WEISS, Peter: Terrorism, Counterterrorism and International Law. Arab Studies Quarterly, 2002. Vol. 24. No. 2–3. 11. o.

WILKINSON, Paul: Terrorism versus Democracy: The Liberal State Response. Routledge, London and New York, 2006. 90–91. o.

WILKINSON, Paul: The Media and Terrorism: A Reassessment. Terrorism and Political Violence, 1997. Vol. 9. No. 2.

WITHER, James K.: The COVID-19 Pandemic: A Preliminary Assessment of the Impact on Terrorism in Western States. Occasional Paper Series, 2020. No. 33. 3–4. o. https://www.marshallcenter.org/en/publications/occasional-papers/covid-19-pandemic-preliminary-assessment (2021.10.05.)

WITT, Taisto: 'If i cannot have it, i will do everything i can to destroy it.' the canonization of Elliot Rodger: 'Incel' masculinities, secular sainthood, and justifications of ideological violence. Journal for the Study of Race, Nation and Culture, 2020. Vol. 26. No. 5. 675. o.

YAMPOLSKIY, Mark – SKJELLUM, Anthony – KRETZSCHMAR, Michael – OVERFELT, Ruel A. – SLOAN, Kenneth R. – YASINSAC, Alec: Using 3D printers as weapons. International Journal of Critical Infrastructure Protection, 2016. Vol. 14. No. 3. 58. o.

YOUNG, Reuven: Defining Terrorism: The Evolution of Terrorism as a Legal Concept in International Law and Its Influence on Definitions in Domestic Legislation. Boston College International and Comparative Law Review, 2006. Vol. 29. No. 1. 27. o.

ZEIGER, Sara – GYTE, Joseph: Prevention of Radicalization on Social Media and the Internet. In: SCHMID, Alex P. (szerk.): Handbook of Terrorism Prevention and Preparedness. International Centre for Counter-Terrorism, Hága, 2021. 360. o.

ZEMAN, Tomáš – BŘEŇ, Jan – URBAN, Rudolf: Role of internet in Lone Wolf Terrorism. Journal of Security & Sustainability Issues, 2017. Vol. 7. No. 2. 185. o.

ZENN, Jacob: Is the 'Bakura Faction' Boko Haram's New Force Enhancer Around Lake

Chad? Terrorism Monitor, 2020. Vol. 18. No. 2. 5. o.

ZUCKERMAN, Ethan: QAnon and the Emergence of the Unreal. Journal of Design and Science, 2019. No. 6. 3–4. o.

ZSIGOVITS László: A Z generáció paradigmái a bűnüldözés és a bűnmegelőzés platformján. In: GAÁL Gyula – HAUTZINGER Zoltán (szerk.): Pécsi Határőr Tudományos Közlemények XXI.: A bűnüldözés és a bűnmegelőzés rendészettudományi tényezői. Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoportja, Pécs, 2019. 113. o.

Internetes források

3D-nyomtatott fegyverei lehettek a szerbiai magyar bérgyilkosnak. HVG. (2019. március 21.). https://hvg.hu/vilag/20190321_3d_nyomtatas_fegyver_d_csaba_bergyilkos (2021.08.31.)

ABDULLAHI, Murtala – ADEBAJO, Kunle: Boko Haram Strongman, Shekau, Dead As ISWAP Fighters Capture Sambisa Forest. HumAngle. (2021, May 20). https://humangle.ng/boko-haram-strongman-shekau-dead-as-iswap-fighters-capture-sambisa-forest/ (2021.06.14.)

Aki megfújja a sípot. Nyelv és Tudomány. (2013. augusztus 21.) https://www.nyest.hu/hirek/aki-megfujja-a-sipot (2021.08.02.)

ALBERT Fruzsina – DÁVID Beáta – HUSZTI Éva: Magyar kutatók figyelmeztetnek: vigyázzunk, nehogy a távolságtartás elszigetelődéshez vezessen! Qubit. (2020. március 26.) https://qubit.hu/2020/03/26/magyar-kutatok-figyelmeztetnek-vigyazzunk-nehogy-a-tavolsagtartas-elszigetelodeshez-vezessen?fbclid=IwAR1oEzqUq_g0DZZ-XYQSQYX1gTM87IXIzE2SidLsQ9QspXRg5nxE3Wga7VU (2021.10.05.)

ALEXANDER, Dean C. – LESNIEWSKI, Dominic: The violent fringe of the incel

movement. Police 1. (2019, September 19). https://www.police1.com/mass-casualty/articles/the-violent-fringe-of-the-incel-movement-M2E5rlB5BYTDesoL/ (2021.06.21.)

AMARASINGAM, Amarnath: Telegram Deplatforming ISIS Has Given Them Something to Fight For. VOX-Pol. (2020, January 1). https://www.voxpol.eu/telegram-deplatforming-isis-has-given-them-something-to-fight-for/ (2022.01.07.)

AMEND, Alex: Analyzing a terrorist's social media manifesto: the Pittsburgh synagogue shooter's posts on Gab. Southern Poverty Law Center. (2018, October 28). https://www.splcenter.org/hatewatch/2018/10/28/analyzing-terrorists-social-media-manifesto-pittsburgh-synagogue-shooters-posts-gab (2022.01.27.)

Apache Tika - a content analysis toolkit. https://tika.apache.org/ (2021.08.06.)

ARGENTINO, Marc-André: QAnon and the storm of the US Capitol: The offline effect of online conspiracy theories. Quartz. (2021, January 7). https://qz.com/1954265/the-attack-on-the-us-capitol-shows-the-real-danger-of-qanon/ (2021.12.09.)

BAGCHI, Indrani: Terrorists used app to hide digital footprint. The Times of India. (2016, July 6). https://timesofindia.indiatimes.com/world/Terrorists-used-app-to-hide-digital-footprint/articleshow/53070343.cms (2021.07.06.)

BARONE, Daniele Maria: Cyber Jihad and Terrorism Financing: New Methods – Old Rules. ITSTIME. (2018, August 16). https://www.itstime.it/w/cyber-jihad-and-terrorism-financing-new-methods-old-rules-by-daniele-maria-barone/ (2021.09.12.)

BARRY, Dan – MCINTIRE, Mike – ROSENBERG, Matthew: 'Our President Wants Us Here': The Mob That Stormed the Capitol. The New York Times. (2021, January 9). https://www.nytimes.com/2021/01/09/us/capitol-rioters.html (2021.12.13.)

BAUMGÄRTNER, Maik – HÖFNER, Roman – LEHBERGER, Roman: RechtsterrorismusMitgründer der "Feuerkrieg Division" gefasst. Der Spiegel. (2020,

April 9). https://www.spiegel.de/politik/deutschland/rechtsterrorismus-mitgruender-der-feuerkrieg-division-gefasst-a-d88e6b8f-7a96-4c56-8904-85bb72653663?utm_source=dlvr.it&utm_medium=[facebook]&utm_campaign=[sponto p]&fbclid=IwAR01kQfV5avns0voCiI1SCFXe_FipiYntLxMhRqg6hTJ3rTlOLI6NVNQ p3A#ref=rss (2021.07.29.)

BECKETT, Lois: Pittsburgh shooting: suspect railed against Jews and Muslims on site used by 'alt-right'. The Guardian. (2018, October 27). https://www.theguardian.com/us-news/2018/oct/27/pittsburgh-shooting-suspect-antisemitism (2021.10.11.)

Behind the Jihadist Attack in Chad. International Crisis Group. (2020, April 6). https://www.crisisgroup.org/africa/central-africa/chad/derriere-lattaque-jihadiste-au-tchad (2021.06.14.)

BELL, Stewart – RUSSELL, Andrew – MCDONALD, Catherine: Deadly attack at Toronto erotic spa was incel terrorism, police allege. Global News. (2020, May 19). https://globalnews.ca/news/6910670/toronto-spa-terrorism-incel/ (2021.06.18.).

BELLINGER, Nisha – KATTELMAN, Kyle: How the coronavirus increases terrorism threats in the developing world. The Conversation. (2020, May 26). https://theconversation.com/how-the-coronavirus-increases-terrorism-threats-in-the-developing-world-137466 (2021.08.31.)

BERGER, J. M.: How ISIS Games Twitter. The Atlantic. (2014, June 16). ttps://www.theatlantic.com/international/archive/2014/06/isis-iraq-twitter-social-media-strategy/372856/ (2021.11.29.)

BERMAN, Mark: Prosecutors say Dylann Roof ‘self-radicalized’ online, wrote another manifesto in jail. The Washington Post. (2016, August 22). https://www.washingtonpost.com/news/post-nation/wp/2016/08/22/prosecutors-say-accused-charleston-church-gunman-self-radicalized-online/ (2021.10.14.)

BINDING, Lucia: Coronavirus: IS could exploit COVID-19 pandemic to carry out terror attacks, EU warns. Sky News. (2020, May 13). https://news.sky.com/story/coronavirus-is-could-exploit-covid-19-pandemic-to-carry-out-terror-attacks-eu-warns-11987706

(2021.09.29.)

Boko Haram. Britannica. https://www.britannica.com/topic/Boko-Haram (2021.06.14.)

Boko Haram: How di insurgents dey get internet to post videos, make calls from inside bush? BBC News. (2020, December 7) https://www.bbc.com/pidgin/tori-55212200 (2021.06.14.)

Boko Haram leader 'is dead,' jihadist rivals claim. Deutsche Welle. (2020, June 6). https://www.dw.com/en/boko-haram-leader-is-dead-jihadist-rivals-claim/a-57795611 (2021.06.14.)

BRITTON, Bianca – HAYES, Mike – ROCHA, Veronica – WAGNER, Meg: Baghdadi's death: More details emerge from US raid: Defense secretary: Baghdadi's death "marks a devastating blow for the remnants of ISIS". CNN. (2019, October 29). https://edition.cnn.com/politics/live-news/baghdadi-monday-dle-intl/index.html (2022.01.06.)

BURKE, Jason: Rise of Isis means Boko Haram's decline is no cause for celebration. The Guardian. (2021, May 22). https://www.theguardian.com/world/2021/may/22/rise-isis-means-boko-haram-decline-no-cause-celebration (2021.06.14.)

CASCAIS, Antonio: 10 years of radicalization: Boko Haram. Deutsche Welle. (2019, July 29). https://www.dw.com/en/10-years-of-radicalization-boko-haram/a-49781704 (2021.06.14.)

Christchurch Call. https://www.christchurchcall.com/ (2021.06.21.)

CILLIZZA, Chris: How coronavirus has sent gun and ammo sales through the roof. CNN. (2020, March 25). https://edition.cnn.com/2020/03/25/politics/guns-ammo-coronavirus/index.html (2021.08.11.)

CLARKE, Colin P.: Trends in Terrorism: What's On the Horizon in 2020. Foreign Policy Research Institute. (2020, January 2). https://www.fpri.org/article/2020/01/trends-in-terrorism-whats-on-the-horizon-in-2020/

(2021.07.15.)

CLARKE, Colin P.: Trends in Terrorism: What's on the Horizon in 2021? Foreign Policy Research Institute. (2021, January 5). https://www.fpri.org/article/2021/01/trends-in-terrorism-whats-on-the-horizon-in-2021/ (2021.06.19.)

COHEN, Zachary: Inside the dramatic US military raid that killed ISIS leader Baghdadi. CNN. (2019, October 28). https://edition.cnn.com/2019/10/27/politics/bagdhadi-inside-the-raid-timeline/index.html (2022.01.06.)

COLLINS, Ben – ZADROZNY, Brandy: The far right is struggling to contain Qanon after giving it life. NBC News. (2018, August 11). https://www.nbcnews.com/tech/tech-news/far-right-struggling-contain-qanon-after-giving-it-life-n899741 (2021.12.08.)

CONSTINE, Josh: ISIS Has Its Own Encrypted Chat App. TechCrunch. (2016, January 16). https://techcrunch.com/2016/01/16/isis-app/?guccounter=2 (2021.07.07.)

Coronavirus: Man planning to bomb Missouri hospital killed, FBI says. BBC. (2020, March 26). https://www.bbc.com/news/world-us-canada-52045958 (2021.10.05.)

Coronavirus triggers panic-buying of guns in Hungary. Al Jazeera. (2020, March 24). https://www.aljazeera.com/news/2020/3/24/coronavirus-triggers-panic-buying-of-guns-in-hungary (2021.08.11.)

Counter-terrorists win: Financial crime through video games is on the rise. The Economist. (2019, November 7). https://www.economist.com/finance-and-economics/2019/11/07/financial-crime-through-video-games-is-on-the-rise (2021.09.12.)

COURTY, Audrey: QAnon believers will likely outlast and outsmart Twitter's bans. The Conversation. (2020, July 24). https://theconversation.com/qanon-believers-will-likely-outlast-and-outsmart-twitters-bans-143192 (2021.10.21.)

COX, Joseph: 7 Ways the Cops Will Bust You on the Dark Web. Vice. (2016, June 26). https://www.vice.com/en/article/vv73pj/7-ways-the-cops-will-bust-you-on-the-dark-web

(2021.08.05.)

CRAWFORD, Blyth: Chan Culture and Violent Extremism. Global Network on Extremism & Technology. (2019, December 31). https://gnet-research.org/2019/12/31/chan-culture-and-violent-extremism-past-present-and-future/ (2021.07.29.)

CRONIN, Cat: Don't Forget About Boko Haram: A 2019 Update. American Security Project. (2019, June 24). https://www.americansecurityproject.org/dont-forget-about-boko-haram-a-2019-update/ (2021.06.14.)

CRUMP, Justin: Terrorism and security threat trends in 2021. Security Magazine. (2020, December 22). https://www.securitymagazine.com/articles/94219-terrorism-and-security-threat-trends-in-2021 (2021.06.21.)

CUEN, Leigh: In Palestine, Civilians Are Using Bitcoin More Than Hamas. CoinDesk. (2019, August 22). https://www.coindesk.com/palestinian-civilians-are-using-bitcoin-more-than-terrorists (2021.09.12.)

Current Efforts by the FATF to Monitor and Take Action against Terrorist Financing. FATF. (2019, February 22). https://www.fatf-gafi.org/publications/methodsandtrends/documents/fatf-action-against-terrorist-financing-feb-2019.html (2021.09.12.)

DAVIS, Aaron C. – LEONNIg, Carol D. – DEMIRJIAN, Karoun – HERMANN, Peter: Backup was denied, former Capitol Police chief says. The Seattle Times. (2021, January 10). https://www.seattletimes.com/nation-world/backup-was-denied-former-capitol-police-chief-says/ (2021.12.14.)

Deep Fakes and National Security. https://fas.org/sgp/crs/natsec/IF11333.pdf (2021.07.19.)

DENHAM, Hannah – TRAN, Andrew Ba: Fearing violence and political uncertainty, Americans are buying millions more firearms. The Washington Post. (2021, February 4). https://www.washingtonpost.com/business/2021/02/03/gun-sales-january-

background-checks/ (2021.08.11.)

DE SIMONE, Daniel – SOSHNIKOV, Andrei – WINSTON, Ali: Neo-Nazi Rinaldo Nazzaro running US militant group The Base from Russia. BBC. (2020, January 24). https://www.bbc.com/news/world-51236915 (2021.07.29.)

DEVECSAI János: Kábítószerek és bérgyilkosok a netről. DigitalHungary. (2017. október 11.). https://www.digitalhungary.hu/konferenciak/evolution/Kabitoszerek-es-bergyilkosok-a-netrol/5056/ (2021.08.02.)

DICKSON, E. J.: QAnon Believers Struggle With the Two Hardest Words: 'President Biden'. Rolling Stone. (2021, January 20). https://www.rollingstone.com/culture/culture-news/qanon-joe-biden-inauguration-donald-trump-1116733/ (2021.12.09.)

DUFF, Michelle: Gaming culture and the alt-right: The weaponisation of hate. Stuff. (2019, March 24). https://www.stuff.co.nz/national/christchurch-shooting/111468129/gaming-culture-and-the-alt-right-the-weaponisation-of-hate?cid=app-iPhone (2021.07.22.)

EAS Special Report, COVID-19 Disinformation. EUvsDisinfo. (2020, March 19). https://euvsdisinfo.eu/eeas-special-report-disinformation-on-the-coronavirus-short-assessment-of-the-information-environment/?highlight=special-report-%20disinformation-on-the-coronavirus-short-assessment-of-the-information-environment%2F (2021.10.05.) Idézi: WITHER: i.m. 3–4. o.

Elfogtak több feltételezett szélsőjobboldali terroristát Németországban. Honvédelem.hu (2020. február 16.) https://honvedelem.hu/cikk/elfogtak-tobb-feltetelezett-szelsojobboldali-terroristat-nemetorszagban/ (2021.07.29.)

Europol and Telegram Take On Terrorist Propaganda Online. Europol. (2019, November 25). https://www.europol.europa.eu/newsroom/news/europol-and-telegram-take-terrorist-propaganda-online (2021.07.07.)

EVANS, Robert: The El Paso Shooting and the Gamification of Terror. Bellingcat. (2019, August 4). https://www.bellingcat.com/news/americas/2019/08/04/the-el-paso-shooting-and-the-gamification-of-terror/ (2022.02.09.)

EVANS, Robert: Ignore The Poway Synagogue Shooter's Manifesto: Pay Attention To 8chan's /pol/ Board. Bellingcat. (2019, April 28). https://www.bellingcat.com/news/americas/2019/04/28/ignore-the-poway-synagogue-shooters-manifesto-pay-attention-to-8chans-pol-board/ (2021.07.27.)

Extremist Content Online: Extremists Plot Anti-Semitic Harassment Campaign Targeting Philadelphia Jewish Day School. Counter Extremism Project. (2020, April 6). https://www.counterextremism.com/press/extremist-content-online-extremists-plot-anti-semitic-harassment-campaign-targeting (2021.08.31.)

Facing the Challenge of the Islamic State in West Africa Province. International Crisis Group. (2019, May 16). https://www.crisisgroup.org/africa/west-africa/nigeria/273-facing-challenge-islamic-state-west-africa-province (2021.06.14.)

FATF Members and Observers. FATF. https://www.fatf-gafi.org/about/membersandobservers/ (2021.09.12.)

FAGHIHI, Rohollah: Iran's conservatives return to Telegram after failed ban. Al-Monitor. (2018, November 28). https://www.al-monitor.com/pulse/originals/2018/11/iran-telegram-ban-conservative-media-rejoin-tasnim-fars.html (2021.07.07.)

FANUSIE, Yaya: Hamas Military Wing Crowdfunding Bitcoin. Forbes. (2019, February 4).
https://www.forbes.com/sites/yayafanusie/2019/02/04/hamas-military-wing-crowdfunding-bitcoin/#306575c34d7f (2021.07.15.)

FANUSIE, Yaya: The New Frontier in Terror Fundraising: Bitcoin. The Cipher Brief. (2016, August 24).
https://www.thecipherbrief.com/column_article/the-new-frontier-in-terror-fundraising-bitcoin (2021.09.12.)

FELDEN, Esther – WILDON, Jordan – HÖHN, Anne – SANDERS, Lewis: As Donald Trump exits, QAnon takes hold in Germany. Deutsche Welle. (2021, January 19). https://www.dw.com/en/as-donald-trump-exits-qanon-takes-hold-in-germany/a-56277928 (2021.12.09.)

FERNÁNDEZ, Stacy: Trump administration sets into motion return of online 3D gun blueprints. The Texas Tribune. (2020, January 14). https://www.texastribune.org/2020/01/14/3d-printed-gun-blueprints-could-soon-go-back-online/ (2021.08.31.)

FRANCESCANI, Chris: The men behind QAnon. ABC News. (2020, September 22). https://abcnews.go.com/Politics/men-qanon/story?id=73046374 (2021.11.05.)

FRANEY, James: US Capitol storming: What you need to know. Deutsche Welle. (2021, January 7). https://www.dw.com/en/us-capitol-storming-what-you-need-to-know/a-56154560 (2021.11.02.)

GAULT, Matthew: 3-D Printers Could Help Spread Weapons of Mass Destruction. Scientific American. (2019, September 10). https://www.scientificamerican.com/article/3-d-printers-could-help-spread-weapons-of-mass-destruction/ (2021.08.30.)

GEHL, Robert W.: Illuminating the 'dark web'. The Conversation. (2018, October 30). https://theconversation.com/illuminating-the-dark-web-105542 (2021.08.03.)

German police criticised over Halle synagogue shootings. Financial Times. https://www.ft.com/content/d22459c8-eb42-11e9-a240-3b065ef5fc55 (2021.10.11.)

GHOSHAL, Abhimanyu: Telegram's updated privacy terms make it unsafe for terrorists – but what about the rest of us? TNW. (2018, August 30). https://thenextweb.com/insider/2018/08/30/telegrams-updated-privacy-terms-make-it-unsafe-for-terrorists-but-what-about-the-rest-of-us/?fbclid=IwAR1Zw6___iJIO82DQpA6U75Pg-

OPzmdvWfEOK1G04zSor_WxFs0ZNOd6-Ko (2021.07.07.)

GILBERT, David: Islamic State Can't Find an Online Home — So They Might Build Their Own App. Vice. (2019, December 3). https://www.vice.com/en_ca/article/d3ane7/islamic-state-cant-find-an-online-home-so-they-might-build-their-own-app (2022.01.07.)

GLASER, April: Where 8channers Went After 8chan. Slate. (2019, November 11). https://slate.com/technology/2019/11/8chan-8kun-white-supremacists-telegram-discord-facebook.html (2021.07.29.)

Global Terrorism Database. https://www.start.umd.edu/gtd/ (2021.12.16.)

GONIMAH, Diana: What is 8chan and Why Was it Banned? Storyful. (2019, November 12). https://storyful.com/resources/blog/what-is-8chan/ (2021.07.29.)

GREENSPAN, Rachel E. – ORECCHIO-EGRESITZ, Haven: A well-known QAnon influencer dubbed the 'Q Shaman' has been arrested after playing a highly visible role in the Capitol siege. Business Insider. (2021, January 9). https://www.businessinsider.com/q-shaman-qanon-influencer-capitol-siege-washington-dc-protest-riot-2021-1 (2021.11.03.)

GRÜN, Gianna: Tweets as weapons: How 'Islamic State' is fighting its battles... digitally. Deutsche Welle. (2015, June 03). https://www.dw.com/en/tweets-as-weapons-how-islamic-state-is-fighting-its-battles-digitally/a-18493604 (2021.12.17.)

GUCCIONE, Darren: What is the dark web? How to access it and what you'll find. CSO Online. (2021, July 1). https://www.csoonline.com/article/3249765/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html (2021.08.09.)

HAN, Yufei: Deepfakes: A Terror in the era of AI? NortonLifeLock. (2020, May 11). https://www.nortonlifelock.com/blogs/research-group/deepfakes-terror-era-ai (2021.07.19.)

HANNA, Andrew: What Islamists Are Doing and Saying on COVID-19 Crisis. Wilson

Center. (2020, May 14). https://www.wilsoncenter.org/article/what-islamists-are-doing-and-saying-covid-19-crisis (2021.10.04.)

HARPER, Ivy: Dark Web Red Rooms: Urban Legend or Worst Content on the Deep Web? The Dark Web Journal. https://darkwebjournal.com/dark-web-red-rooms/ (2021.08.02.)

HAUSLOHNER, Abigail – OHLHEISER, Abby: Some neo-Nazis lament the Pittsburgh massacre: It derails their efforts to be mainstream. The Washington Post. (2018, October 30). https://www.washingtonpost.com/national/some-neo-nazis-lament-the-pittsburgh-massacre-it-derails-their-efforts-to-be-mainstream/2018/10/30/3163fd9c-dc5f-11e8-85df-7a6b4d25cfbb_story.html (2022.01.26.)

HAYDEN, Michael Edison: Far-Right Extremists Are Calling for Terrorism on the Messaging App Telegram. Southern Poverty Law Center. (2019, June 27). https://www.splcenter.org/hatewatch/2019/06/27/far-right-extremists-are-calling-terrorism-messaging-app-telegram (2021.07.06.)

History of the FATF. FATF. https://www.fatf-gafi.org/about/historyofthefatf/ (2021.09.12.)

HOFFMAN, Bruce – WARE, Jacob: Incels: America's Newest Domestic Terrorism Threat. Lawfare. (2020, January 12). https://www.lawfareblog.com/incels-americas-newest-domestic-terrorism-threat (2021.06.18.)

HOFFMAN, Bruce – WARE, Jacob: Is 3-D Printing the Future of Terrorism? The Wall Street Journal. (2019, October 25). https://www.wsj.com/articles/is-3-d-printing-the-future-of-terrorism-11572019769 (2021.08.31.)

How to Make 3D Printed Gun Parts – Step by Step Guide. Pick 3D Printer. (2021, July 12). https://pick3dprinter.com/3d-printed-gun-parts/ (2021.08.11.)

How To Use Tor Browser: Everything You MUST Know in 2021. vpnMentor. (2021, July 12). https://www.vpnmentor.com/blog/tor-browser-work-relate-using-vpn/ (2021.08.02.)

HUBBARD, Ben – SHOUMALI, Karam: Likely Successor to Dead ISIS Leader Also Reported Killed. The New York Times. (2019, October 30). https://www.nytimes.com/2019/10/27/world/middleeast/al-baghdadi-successor-reported-killed.html (2022.01.06.)

HUME, Tim: Gunman Kills 9 in Hookah Bars in Suspected Far-Right Terror Attack in Germany. Vice. (2020, February 20). https://www.vice.com/en/article/z3byd9/gunman-kills-9-in-hookah-bars-in-suspected-far-right-terror-attack-in-germany (2021.07.22.)

HUME, Tim: New German Terror Cell 'The Hard Core' Planned to Attack Mosques to Start a Civil War. Vice. (2020, February 17). https://www.vice.com/en/article/z3bymx/new-german-terror-cell-the-hard-core-wanted-to-attack-mosques-to-start-a-civil-war (2021.07.29.)

https://defcad.com/library/ (2021.03.12.)

https://thepiratebay.org/description.php?id=28522986 (2021.08.31.)

https://www.youtube.com/channel/UCKdzJMxUSGJzNJ95ppd-ohg (2021.12.30.)

Incels (Involuntary celibates). https://www.adl.org/resources/backgrounders/incels-involuntary-celibates (2021.06.18.)

InfoWars. https://www.infowars.com/ (2021.10.21.)

Iraq accuses US of state terrorism. BBC News. (2002, February 20). http://news.bbc.co.uk/2/hi/middle_east/1830640.stm (2021.11.03.)

ISIS Mario. https://www.youtube.com/watch?v=Ih_V45B5uEo (2021.12.30.)

ISIS Use of Smaller Platforms and the DWeb to Share Terrorist Content. VOX-Pol. (2019, July 3). https://www.voxpol.eu/isis-use-of-smaller-platforms-and-the-dweb-to-share-terrorist-content/ (2022.01.06.)

JACKSON, Beau: Interview with the ICSR: A 3D printed gun was not used in the Halle terror attack. 3D Printing Industry. (2019, October 18). https://3dprintingindustry.com/news/interview-with-the-icsr-a-3d-printed-gun-was-not-used-in-the-halle-terror-attack-163643/ (2021.08.31.)

Joe Biden orders review of US domestic extremism threat. Deutsche Welle. (2021, January 23). https://www.dw.com/en/joe-biden-orders-review-of-us-domestic-extremism-threat/a-56321162 (2021.11.05.)

Joe Biden slams pro-Trump mob as 'domestic terrorists'. Deutsche Welle. (2021, January 7). https://www.dw.com/en/joe-biden-slams-pro-trump-mob-as-domestic-terrorists/a-56163969 (2021.11.03.)

JOHNSON, Bridget: ISIS: Cities Distracted by Coronavirus Should be Hit with Attacks Like Paris, London, Brussels. Homeland Security Today. (2020, March 24). https://www.hstoday.us/subject-matter-areas/counterterrorism/isis-cities-distracted-by-coronavirus-should-be-hit-with-attacks-like-paris-london-brussels/ (2021.08.09.)

KAPLAN, Eben: Tracking Down Terrorist Financing. Council On Foreign Relations. (2006, April 4). https://www.cfr.org/backgrounder/tracking-down-terrorist-financing (2021.09.17.)

KARASZ, Palko: What Is Telegram, and Why Are Iran and Russia Trying to Ban It? The New York Times. (2018, May 2). https://www.nytimes.com/2018/05/02/world/europe/telegram-iran-russia.html (2021.07.07.)

KATZ, Rita: A Growing Frontier for Terrorist Groups: Unsuspecting Chat Apps. Wired. (2019, September 1). https://www.wired.com/story/terrorist-groups-prey-on-unsuspecting-chat-apps/?fbclid=IwAR0rzGUvrw5SoMJy1_XGd-wHuTF6cgTGUrQlsWkpQr8_eZq_l6vSK0YKWcQ (2020.07.05.)

KATZ, Rita: Almost Any Messaging App Will Do—If You're ISIS. Vice. (2016, July 14). https://www.vice.com/en/article/kb7n4a/isis-messaging-apps (2021.07.07.)

KATZ, Rita: ISIS Is Now Harder to Track Online—but That's Good News. Wired. (2019, December 16). https://www.wired.com/story/opinion-isis-is-now-harder-to-track-onlinebut-thats-good-news/ (2022.01.07.)

KATZ, Rita: ISIS's Mobile App Developers Are in Crisis Mode. Vice. (2016, June 3). https://www.vice.com/en/article/qkj34q/isis-mobile-app-developers-are-in-crisis-mode (2021.07.07.)

KATZ, Rita: Tales of Crypto-Currency: Bitcoin Jihad in Syria and Beyond. The Daily Beast. (2019, October 13). https://www.thedailybeast.com/the-bitcoin-jihad-in-syria-and-beyond-tales-of-crypto-currency (2021.08.09.)

KATZ, Rita: The Far-Right's Online Discourse on COVID-19 Pandemic. SITE Intelligence Group. https://ent.siteintelgroup.com/index.php?option=com_acymailing&ctrl=archive&task=view&mailid=20576&key=4lfGcEyn&subid=1472-t9ir9gm3ghmVr7&tmpl=component (2021.10.05.)

KEHOE, Shawn R.: The Digital Alleyway: Why the Dark Web Cannot Be Ignored. Police Chief Magazine. (2018, June 12). https://www.policechiefmagazine.org/the-digital-alleyway/ (2021.08.05.)

KELLY, Kim: The Rise of the 3D-Printed Gun. The Soapbox. (2020, May 21). https://newrepublic.com/article/157753/rise-3d-printed-gun (2021.08.11.)

Kiberbűnözés és a virtuális tér veszélyei – interjú az Internet Világnapja alkalmából. Birosag.hu. (2018. május 18.) https://birosag.hu/hirek/kategoria/magazin/kiberbunozes-es-virtualis-ter-veszelyei-interju-az-internet-vilagnapja (2021.08.02.)

KOHN, Isabelle: Inside the World of 'Femcels'. MEL Magazine. https://melmagazine.com/en-us/story/femcels-vs-incels-meaning-reddit-discord (2021.06.18.)

KOLOMYCHENKO, Maria: Russia tries more precise technology to block Telegram messenger. Reuters. (2018, August 30). https://www.reuters.com/article/us-russia-telegram/russia-tries-more-precise-technology-to-block-telegram-messenger-idUSKCN1LF1ZZ (2021.07.07.)

KUMAR, Ruchi: Taliban launches campaign to help Afghanistan fight coronavirus. Al Jazeera. (2020, April 6). https://www.aljazeera.com/news/2020/04/taliban-launches-campaign-afghanistan-fight-coronavirus-200406055113086.html (2021.10.05.)

LANDLER, Mark: Obama Calls Blasts an 'Act of Terrorism'. The New York Times. (2013, April 16). https://www.nytimes.com/2013/04/17/us/politics/obama-calls-marathon-bombings-an-act-of-terrorism.html (2021.11.03.)

Lelepleződött egy durva izraeli kémfegyver, az Orbán-kormány kritikusait és magyar újságírókat is célba vettek vele. Telex. (2021. július 18.) https://telex.hu/direkt36/2021/07/18/leleplezodott-egy-durva-izraeli-kemfegyver-az-orban-kormany-kritikusait-es-magyar-ujsagirokat-is-celba-vettek-vele (2021.07.20.)

LEONNIG, Carol D. – DAVIS, Aaron C. – HERMANN, Peter – DEMIRJIAN, Karoun: Outgoing Capitol Police chief: House, Senate security officials hamstrung efforts to call in National Guard. The Washington Post (2021, January 10). https://www.washingtonpost.com/politics/sund-riot-national-guard/2021/01/10/fc2ce7d4-5384-11eb-a817-e5e7f8a406d6_story.html (2021.12.15.)

LETSCH, Constanze: Laughing at Isis: Syrian video artists go beyond fear to ridicule jihadis. The Guardian. (2015, March 12). https://www.theguardian.com/world/2015/mar/12/laughing-at-isis-syrian-video-artists-jihadis-refugee-islamic-state (2021.12.30.)

LORENZ, Taylor: The Shooter's Manifesto Was Designed to Troll The violent rhetoric was written for an audience. The Atlantic. (2019, March 15). https://www.theatlantic.com/technology/archive/2019/03/the-shooters-manifesto-was-designed-to-troll/585058/ (2021.07.22.)

M., Aysha: 3D printed guns: where are we now? 3D Natives. (2020, September 2).

https://www.3dnatives.com/en/3d-printed-gun-020920205/#! (2021.08.30.)

MAKUCH, Ben – LAMOUREUX, Mack: Neo-Nazis Are Organizing Secretive Paramilitary Training Across America. Vice. (2018, November 20). https://www.vice.com/en/article/a3mexp/neo-nazis-are-organizing-secretive-paramilitary-training-across-america (2021.07.29.)

MALIK, Nikita: Self-Isolation Might Stop Coronavirus, but It Will Speed the Spread of Extremism. Foreign Policy. (2020, March 26). https://foreignpolicy.com/2020/03/26/self-isolation-might-stop-coronavirus-but-spread-extremism/ (2021.06.21.)

Man jailed after found with 3D-printed gun and 'lawmaker hit list'. BBC. (2019, February 14). https://www.bbc.com/news/world-us-canada-47243007 (2021.08.31.)

MATTMANN, Christian: Searching deep and dark: Building a Google for the less visible parts of the web. The Conversation. (2017, January 9). https://theconversation.com/searching-deep-and-dark-building-a-google-for-the-less-visible-parts-of-the-web-58472 (2021.08.05.)

MCHUGH, David – RISING, David – JORDANS, Frank: German gunman calling for genocide kills 9 people. Associated Press. (2020, February 20). https://apnews.com/b5736c3dba1d677e89ef947bcf5ab213 (2021.07.22.)

MCINTIRE, Mike – ROOSE, Kevin: What Happens When QAnon Seeps From the Web to the Offline World. The New York Times. (2020, February 9). https://www.nytimes.com/2020/02/09/us/politics/qanon-trump-conspiracy-theory.html (2021.12.09.)

MEISENZAHL, Mary: ISIS is reportedly using popular Gen Z app TikTok as its newest recruitment tool. Business Insider. (2019, October 21). https://www.businessinsider.com/isis-using-tiktok-to-target-teens-report-2019-10 (2021.07.07.)

Mi az a Stablecoin? Virtuális Cash. (2019. július 29.). https://www.virtualis.cash/mi-az-a-stablecoin/ (2021.09.12.)

Mire jó a VPN? Valóban anonim böngészést nyújt! VPN szerver. (2021. március 8.). https://www.vpnszerver.hu/mire-jo-a-vpn/ (2021.08.03.)

mkeh.gov.hu/haditechnika/kettos_felhasznalasu (2021.08.15.)

Mobile internet user penetration in Nigeria from 2015 to 2025. Statista. https://www.statista.com/statistics/972900/internet-user-reach-nigeria/ (2021.06.14.)

MOUTOT, Michel: Smartphones: a double-edged sword for terrorists. Phys.org. (2018, November 13).
https://phys.org/news/2018-11-smartphones-double-edged-sword-terrorists.html (2021.07.07.)

NAGY Zoltán: Visszaélés a 3D nyomtatással. Ars Boni. (2019. július 3.). https://arsboni.hu/visszaeles-a-3d-nyomtatassal/ (2021.08.31.)

NEIWERT, David: Conspiracy meta-theory 'The Storm' pushes the 'alternative' envelope yet again. Southern Poverty Law Center. (2018, January 17). https://www.splcenter.org/hatewatch/2018/01/17/conspiracy-meta-theory-storm-pushes-alternative-envelope-yet-again (2021.10.25.)

Nigeria: Seven years since Chibok, the government fails to protect children. Amnesty International. (2021, April 14).
https://www.amnesty.org/en/latest/news/2021/04/nigeria-seven-years-since-chibok-the-government-fails-to-protect-children/ (2021.06.14.)

Nigerian army investigates reports of Boko Haram leader’s death. Al Jazeera. (2021, May 21).
https://www.aljazeera.com/news/2021/5/21/nigeria-investigates-reports-of-boko-haram-leaders-death (2021.06.14.)

Nigeria's Boko Haram behind schoolboys' abduction - audio message. Reuters. (2020,

December 15). https://www.reuters.com/article/nigeria-security-kidnappings-idUSKBN28P2DL (2021.06.14.)

Norway mosque shooting: Man opens fire on Al-Noor Islamic Centre. BBC. (2019, August 10). https://www.bbc.com/news/world-europe-49308016 (2021.07.27.)

Norway mosque attack: Bruised suspect Manshaus appears in court. BBC. (2019, August 12). https://www.bbc.com/news/world-europe-49318001 (2021.07.29.)

PAGANINI, Pierluigi: Islamic State launches the Kybernetiq magazine for cyber jihadists. Security Affairs. (2016, January 9). http://securityaffairs.co/wordpress/43435/hacking/kybernetiq-magazine-cyber-jihad.html (2019.12.10.)

PALIY, George: What Is The Dark Web? Business 2 Community. (2017, November 27). https://www.business2community.com/cybersecurity/what-is-the-dark-web-01961365 (2021.08.09.)

PALMER, Danny: VPN use surges as coronavirus outbreak prompts huge rise in remote working. ZDNet. (2020, March 23). https://www.zdnet.com/article/vpn-use-surges-as-coronavirus-outbreak-prompts-huge-rise-in-remote-working/ (2021.08.05.)

PARDY Balázs: Lőfegyvert otthon műanyagból? Ars Boni. (2019. január 7.). https://arsboni.hu/lofegyvert-otthon-muanyagbol/ (2021.08.12.)

PÁL Tamás: Edward Snowden a Pegasus-ügyről: Ez túlmutat a kémkedés azon szintjén, amit eddig ismertünk. Telex. (2021. július 20.). https://telex.hu/kulfold/2021/07/20/edward-snowden-interju-die-zeit-pegasus-ugy-nso (2021.07.20.)

PEREZ, Yessi Bello: The differences between cryptocurrencies, virtual, and digital currencies. The Next Web. (2019, February 19). https://thenextweb.com/hardfork/2019/02/19/the-differences-between-cryptocurrencies-virtual-and-digital-currencies/ (2020.09.12.)

POE, Ted: Time to silence terrorists on social media. CNN. (2015, February 26). http://edition.cnn.com/2015/02/25/opinion/poe-terrorism-social-media/ (2021.12.17.)

Polizei war jüdischer Feiertag Jom Kippur nicht bekannt. Spiegel. (2020, Juni 10). https://www.spiegel.de/panorama/justiz/halle-anschlag-auf-synagoge-polizei-war-juedischer-feiertag-nicht-bekannt-a-7ef5bd6e-c38b-40ea-80d1-ac005a322338?fbclid=IwAR3wi7DOh10WstBd_muQ_peQxHla0To5kHmRqeWbccAmvSU1iKyOrK-qtqQ (2021.10.11.)

PRINS, Nico: An Analysis of the Russian Social Media Landscape in 2019. Linkfluence. https://www.linkfluence.com/blog/russian-social-media-landscape (2021.07.07.)

RATNESAR, Romesh: Islamic State Is Dying on the Battlefield—and Winning on the Internet. Bloomberg. (2017. July 20). https://www.bloomberg.com/news/articles/2017-07-20/islamic-state-is-dying-on-the-battlefield-and-winning-on-the-internet (2022.01.05.)

RAZEEK, Thameenah: 'Threema' app used by 21/4 terrorists Encryption, a barrier against war on terror? Ceylon Today. (2019, September 29). https://ceylontoday.lk/print-more/41446 (2021.07.06.)

Referral Action Day Against Islamic State Online Terrorist Propaganda. Europol. (2019, November 22). https://www.europol.europa.eu/newsroom/news/referral-action-day-against-islamic-state-online-terrorist-propaganda (2021.07.07.)

REISINGER, Don: ISIS Has Launched A Mobile App—For Children. Fortune. (2016, May 11). http://fortune.com/2016/05/11/isis-mobile-app-children/ (2021.07.07.)

Remarks On Financial Aspects of Terrorism at Office of Financial Crimes Enforcement Network. U.S. Department of State Archive. https://2001-2009.state.gov/secretary/former/powell/remarks/2001/5979.htm (2021.09.12.)

REUTERS: Crypto terror financing: Hamas shifts tactics in bitcoin fundraising. The Jerusalem Post. (2019, April 26). https://www.jpost.com/middle-east/crypto-terror-

financing-hamas-shifts-tactics-in-bitcoin-fundraising-587930 (2021.09.09.)

Rolling updates on coronavirus disease (COVID-19). World Health Organization. https://www.who.int/emergencies/diseases/novel-coronavirus-2019/events-as-they-happen (2021.09.28.)

ROOSE, Kevin: 8chan Is a Megaphone for Gunmen. 'Shut the Site Down,' Says Its Creator. The New York Times. (2019, August 4). https://archive.is/JrNGc (2021.07.29.)

SCHAPIRO, Rich – KOSNAR, Michael: Capitol rioter in horned hat gloats as feds work to identify suspects. NBC News. (2021, January 8). https://www.nbcnews.com/news/us-news/capitol-rioter-horned-hat-gloats-feds-work-identify-suspects-n1253392 (2021.11.03.)

SCHNEIDER, Ari: 3D-Printed Guns Are Getting More Capable and Accessible. Slate. (2021, February 16). https://slate.com/technology/2021/02/3d-printed-semi-automatic-rifle-fgc-9.html (2021.08.11.)

SCHULTE, Sarah: FBI warns America about domestic terrorism following attack on US Capitol. ABC 7 Chicago. (2021, January 14). https://abc7chicago.com/domestic-terrorism-fbi-us-capitol-building-the-internet/9634442/ (2021.12.28.)

Secretary-General's remarks to the Security Council on the COVID-19 Pandemic [as delivered]. United Nations. (2020, April 9). https://www.un.org/sg/en/content/sg/statement/2020-04-09/secretary-generals-remarks-the-security-council-the-covid-19-pandemic-delivered (2021.09.29.)

SHER, Davide: Study shows 3D printed weapons face similar issues as any AM segment. 3D Printing Media Network. (2018, August 7). https://www.3dprintingmedia.network/arms-trade-study-reports-3d-printable-gun-files-widely-available-on-dark-web/ (2021.08.31.)

SILBERGLITT, Richard – CHOW, Brian G. – HOLLYWOOD, John S. – WOODS, Dulani – ZAYDMAN, Mikhail – JACKSON, Brian A.: Visions of Law Enforcement Technology in the Period 2024-2034. Rand Corporation, Santa Monica, 2015. https://www.ojp.gov/pdffiles1/nij/grants/248718.pdf (2021.08.15.)

SIMONS, Greg – BIANCA, Cristina: The Specter of Terrorism During the Coronavirus Pandemic. E-International Relations. (2020. May 8). https://www.e-ir.info/2020/05/08/the-specter-of-terrorism-during-the-coronavirus-pandemic/ (2021.06.14.)

SITE Intelligence Group Launches "Bioterrorism and Public Health" Service to Support Healthcare Efforts amid Global Threats. SITE Intelligence Group. https://ent.siteintelgroup.com/Press-Release/site-intelligence-group-launches-public-health-and-bioterrorism-service-to-support-healthcare-efforts-amid-global-threats.html (2021.09.30.)

Somerset County Man Charged With Attempts To Provide Material Support To Hamas, Making False Statements, And Making Threat Against Pro-Israel Supporters. United States Department of Justice. (2019, May 22). https://www.justice.gov/usao-nj/pr/somerset-county-man-charged-attempts-provide-material-support-hamas-making-false (2021.09.12.)

SPECKHARD, Anne: Baghdadi Just Confirmed ISIS 'Martyrdom' Narrative, Ensuring ISIS Will Live. The International Center for the Study of Violent Extremism (ICSVE). (2019, October 30). https://www.icsve.org/baghdadi-just-confirmed-isis-martyrdom-narrative-ensuring-isis-will-live/ (2022.01.06.)

SPECKHARD, Anne – ELLENBERG, Molly – MORTON, Jesse – ASH, Alexander: Involuntary Celibates' Experiences of and Grievance Over Sexual Exclusion and the Potential Threat of Violence Among Those Active in an Online Incel Forum. International Center for the Study of Violent Extremism. (2021, February 3). https://www.icsve.org/involuntary-celibates-experiences-of-and-grievance-over-sexual-exclusion-and-the-potential-threat-of-violence-among-those-active-in-an-online-incel-forum/ (2021.06.18.)

SPECKHARD, Anne: Is ISIS Still Alive and Well on the Internet? Homeland Security Today. (2019, January 14). https://www.hstoday.us/subject-matter-areas/terrorism-study/is-isis-still-alive-and-well-on-the-internet/ (2022.01.07.)

Student jailed for making 3D printed gun. BBC. (2019, September 19). https://www.bbc.com/news/uk-england-london-49761290 (2021.08.31.)

SQUIRREL, Tim: A definitive guide to Incels part one: Incelocalypse. https://www.timsquirrell.com/blog/2018/5/30/a-definitive-guide-to-incels-part-one-incelocalypse (2021.06.19.)

Still don't know Vkontakte, the Russian Facebook with 70 Million active users? E-commerce Nation. (2019, January 2). https://www.ecommerce-nation.com/still-dont-know-vkontakte-the-russian-facebook-with-70-million-active-users/ (2021.07.06.)

STRAUB, Jeremy: 3D-printed guns may be more dangerous to their users than targets. The Conversation. (2019, January 7). https://theconversation.com/3d-printed-guns-may-be-more-dangerous-to-their-users-than-targets-103724 (2021.09.01.)

SYMANOVICH, Steve: How to safely access the deep and dark webs. Norton. (2020, July 23). https://us.norton.com/internetsecurity-how-to-how-can-i-access-the-deep-web.html (2021.08.09.)

TAN, Rebecca: Terrorists' love for Telegram, explained. It's become ISIS's "app of choice." Vox. (2017, June 30). https://www.vox.com/world/2017/6/30/15886506/terrorism-isis-telegram-social-media-russia-pavel-durov-twitter (2021.07.06.)

Terrorists on Telegram. https://www.counterextremism.com/terrorists-on-telegram (2021.07.06.)

The Risks of 3D Printing. http://www.sciroccogroup.com/the-risks-of-3d-printing/ (2021.08.12.)

Tor And The Deep Web: Everything You Secretly Wanted To Know.

https://www.whoishostingthis.com/blog/2017/03/07/tor-deep-web/ (2020.03.28.)

Total number of active social media users in Nigeria from 2017 to 2021. Statista. https://www.statista.com/statistics/1176096/number-of-social-media-users-nigeria/ (2021.06.14.)

Total number of Websites. Internet Live Stats. https://www.internetlivestats.com./total-number-of-websites/ (2022.01.18.)

Több mint háromszáz diákot rabolt el a Boko Haram. Honvedelem.hu. (2020. december 16.). https://honvedelem.hu/hirek/tobb-mint-haromszaz-diakot-rabolt-el-a-boko-haram.html (2021.06.14.)

TUCKER, Patrick: If You Do This, the NSA Will Spy on You. Defense One. (2014, July 7). https://www.defenseone.com/technology/2014/07/if-you-do-nsa-will-spy-you/88054/ (2021.08.03.)

Tunisia arrests 2 over 'coronavirus cough attack plot' on police station. The New Arab. (2020, April 17). https://english.alaraby.co.uk/english/news/2020/4/16/tunisia-foils-extremist-plot-to-infect-police-with-coronavirus (2021.09.30.)

UBERTI, David: The Christchurch Terror Attack Video Is Still Spreading on Facebook. Vice. (2019, November 13). https://www.vice.com/en/article/wjw93n/the-christchurch-terror-attack-video-is-still-spreading-on-facebook (2021.07.22.)

UBERTI, David: The German Synagogue Shooter's Twitch Video Didn't Go Viral. Here's Why. Vice. (2019, October 11). https://www.vice.com/en/article/zmjgzw/the-german-synagogue-shooters-twitch-video-didnt-go-viral-heres-why (2021.07.22.)

VALAHOVITS Szilvia Éva: Magyar találmány: cenzúrázhatatlan internet. Válasz.hu. (2017. április 21.). http://valasz.hu/techvilag/egy-magyar-fiatalember-feltalalta-a-cenzurazhatatlan-internetet-123507 (2021.08.04.)

VALENTI, Jessica: When Misogynists Become Terrorists. The New York Times. (2018, April 26.). https://www.nytimes.com/2018/04/26/opinion/when-misogynists-become-

terrorists.html (2021.06.19.)

VAN DER VEER, Renske: Terrorism in the age of technology. https://www.clingendael.org/pub/2019/strategic-monitor-2019-2020/terrorism-in-the-age-of-technology/ (2021.08.30.)

VÁRADI Bendegúz: Önreprezentáció az inceloszférában? https://eltedszk.org/2020/08/28/onreprezentacio-az-inceloszferaban/ (2021.06.19.)

WARD, Antonia: ISIS's Use of Social Media Still Poses a Threat to Stability in the Middle East and Africa. RAND Corporation. (2018, December 11). https://www.rand.org/blog/2018/12/isiss-use-of-social-media-still-poses-a-threat-to-stability.html (2021.11.15.)

WARE, Jacob – HOFFMAN, Bruce – SHAPIRO, Ezra: Remembering Toronto: Two Years Later, Incel Terrorism Threat Lingers. Global Network on Extremism & Technology. (2020, May 6). https://gnet-research.org/2020/05/06/remembering-toronto-two-years-later-incel-terrorism-threat-lingers/ (2021.06.21.)

Webinar: Finding the Next Incel Killer. Homeland Security Today. (2020, September 16). https://www.hstoday.us/subject-matter-areas/counterterrorism/webinar-finding-the-next-incel-killer/ (2021.06.21.)

WEIMANN, Gabriel: Social Media's Appeal to Terrorists. Insite Blog on Terrorism & Extremism. (2014, October 3). https://news.siteintelgroup.com/blog/index.php/entry/295-social-media's-appeal-to-terrorists (2021.06.14.)

What is the Deep Web? The Definitive Guide [2020]. https://www.thedarkweblinks.com/what-is-the-deep-web/ (2021.08.02.)

WINTER, Charlie: Inside the collapse of Islamic State's propaganda machine. Wired. (2017, December 20). https://www.wired.co.uk/article/isis-islamic-state-propaganda-content-strategy (2022.01.05.)

WINTER, Jana: Exclusive: FBI document warns conspiracy theories are a new domestic terrorism threat. Yahoo! News. (2019, August 1). https://news.yahoo.com/fbi-documents-conspiracy-theories-terrorism-160000507.html (2021.12.08.)

YUEN, Stacey: It's not just Russia — terror financiers are also using social media propaganda. CNBC. (2018, January 1). https://www.cnbc.com/2017/12/18/social-media-propaganda-terror-financiers-operate-on-internet.html (2021.09.12.)

YUNIAR, Resty Woro: Bitcoin, PayPal Used to Finance Terrorism, Indonesian Agency Says. The Wall Street Journal. (2017, January 10). https://www.wsj.com/articles/bitcoin-paypal-used-to-finance-terrorism-indonesian-agency-says-1483964198 (2021.09.12.)

Zero-day (0day) exploit. https://www.imperva.com/learn/application-security/zero-day-exploit/ (2021.07.07.)

ZETTER, Kim: Use privacy services? The NSA is probably tracking you. Wired. (2014, April 7). https://www.wired.co.uk/article/nsa-targeting-tor-users (2021.08.03.)

Felhasznált jogszabályok

AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2017/541 IRÁNYELVE (2017. március 15.) a terrorizmus elleni küzdelemről, a 2002/475/IB tanácsi kerethatározat felváltásáról, valamint a 2005/671/IB tanácsi határozat módosításáról.

Code of Laws of the United States of America Title 18 §2331(5) https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title18-section2331&num=0&edition=prelim

United States Code of Federal Regulations Title 28 §0.85(l)
Uniting And Strengthening America By Providing Appropriate Tools Required To Intercept And Obstruct Terrorism (USA Patriot Act) Act of 2001, PUBLIC LAW 107–56—OCT. 26, 2001.

Felhasznált bírósági döntések

United States of America v. Patrick Wood Crusius, Case 3:20-cr-00389-DCG 02/06/20 1–2. o.
https://www.justice.gov/usao-wdtx/file/1245756/download (2021.07.22.)

A munka témaköréből készült saját publikációk jegyzéke

GÁL, István László – SERBAKOV, Márton Tibor: How Acts of Terrorism are Financed and Orchestrated in Secrecy Today: Criminal Offenses, Donations, Legal Businesses and Smartphone Applications. Journal Of Eastern-European Criminal Law, 2019. Vol. 6. No. 1. 66–76. o.

SERBAKOV Márton Tibor: A Boko Haram internethasználatának evolúciója. In: KŐHALMI László (szerk.): PhD Tanulmányok 15. Pécsi Tudományegyetem Állam- és Jogtudományi Kar, Pécs, 2021. 137–153. o.

SERBAKOV Márton Tibor: A Dohány utcai zsinagógánál történt két merénylet a korabeli jogszabályok és antiszemita szervezetek tükrében. Jogtörténeti Szemle, 2021/2. 32–40. o.

SERBAKOV Márton Tibor: A koronavírus (COVID-19) pandémia hatása a globális terrorizmus és extrémizmus fenyegetésére. In: GAÁL Gyula – HAUTZINGER Zoltán (szerk.): Pécsi Határőr Tudományos Közlemények XXII.: A Hadtudománytól A Rendészettudományig – Társadalmi Kihívások A Nemzeti Összetartozás Évében. Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport, Pécs, 2020. 323–330. o.

SERBAKOV Márton Tibor: A terroristák drónhasználata. Nemzetbiztonsági Szemle, 2019/4. 30–43. o.

SERBAKOV Márton Tibor: A terroristák internethasználata. Büntetőjogi Szemle, 2018/2. 85–93. o.
SERBAKOV Márton Tibor: A terrorizmus definíciójának kérdése. Büntetőjogi Szemle, 2019/2. 87–100. o.

SERBAKOV Márton Tibor: Az Iszlám Állam finanszírozási forrásai. In: TÓTH Dávid – BENDES Ákos László – DIÓSI Szabolcs – GÁSPÁR Zsolt – PROJICS Nárcisz – SERBAKOV Márton Tibor – SZÍVÓS Alexander Roland (szerk.): I-II. Konferenciakötet. Pécsi Tudományegyetem Állam- és Jogtudományi Kar Doktori Iskola, Pécs, 2021. 137–149. o.

SERBAKOV Márton Tibor: Az online felületek és okostelefonos alkalmazások mint a terrorcselekmények előrejelző rendszerei. In: GAÁL Gyula – HAUTZINGER Zoltán (szerk.). Pécsi Határőr Tudományos Közlemények XXI.: A bűnüldözés és a bűnmegelőzés rendészettudományi tényezői. Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoportja, Pécs, 2019. 119–124. o.

SERBAKOV Márton Tibor: Az utóbbi évek jelentős nemzetközi szélsőjobboldali terrorcselekmények elkövetőinek internethasználata és globális összefüggései. Jogelméleti Szemle, 2020/3. 60–69. o.

SERBAKOV Márton Tibor: Gondolatok a terrorizmus elleni küzdelem és a terrorcselekmények megelőzésének elméleti kérdéseiről, különös tekintettel az internethez kötődő megelőzési módszerekről. KRE-DIT: A KRE-DOK ONLINE TUDOMÁNYOS FOLYÓIRATA, 2020/1.

SERBAKOV Márton Tibor: Kriminalitás a dark weben: illegális piacok, pedofil oldalak, terroristák és az ellenük való küzdelem. Büntetőjogi Szemle, 2020/1. 91–107. o.

SERBAKOV Márton Tibor: Legújabb tendenciák a terroristák internethasználatát illetően. Büntetőjogi Szemle, 2020/2. 122–139. o.

SERBAKOV Márton Tibor: Okostelefonos alkalmazások a terroristák szolgálatában. JURA, 2020/2. 143–155. o.

SERBAKOV, Márton Tibor: The attack on the U.S. Capitol and the security threat posed by the QAnon conspiracy theory. Jogelméleti Szemle, 2021/2.106–124. o.
SERBAKOV, Márton Tibor: The latest techniques and sources of terrorist financing. KRE-DIT: A KRE-DOK ONLINE TUDOMÁNYOS FOLYÓIRATA, 2020/2.

SERBAKOV, Márton Tibor: Trends in terrorism in 2021. Büntetőjogi Szemle, 2021. Vol. 10. No. különsz. 68–75. o.