

DR. SERBAKOV MÁRTON TIBOR*

Legújabb tendenciák a terroristák internet-használatát illetően

Bevezetés

Jelen tanulmányban a legújabb és legrelevánsabb tendenciákra mutatok rá a terroristák internethasználatát illetően. Megvizsgálom a szélsőjobboldali extrémisták és terroristák erősödő online jelenlétét és az azzal kapcsolatos trendeket. Górcső alá helyezem az Iszlám Állam (továbbiakban ISIS¹) online tevékenységét. Végül bemutatom a koronavírus-világjárvány hatását a terroristák internethasználatára és rávilágítok esetleges jövőbeli fenyegetésekre.

1. A terroristák internethasználatáról általánosságban

Az internet forradalmasította a terrorizmust.² A terroristák kezében a modern számítástechnológiai eszközök és az internet mint új „fegyver” jelent meg, akik céljaikra fel- (és ki)használják a modern technika lehetőségeit, élve ugyanazokkal a technika teremtette előnyökkel, amelyekkel bárki más is.³

Az információtechnológia terrorista célú felhasználásának Bócné Neparáczki két csoportját különíti el: „Az információtechnológia „hard” típusú alkalmazásakor a terroristák kifejezetten kibertámadást haj-

tanak végre (például kritikus infrastruktúrákat irányító információs rendszert bénítanak meg, tesznek működésképtelenné azzal, hogy terheléses támadást indítanak, férgek, vírusokat küldenek stb.). Másrészt 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 médialeként használják (például a célpont ellen végrehajtott

támadás felvételét megosztják, vagy közleményekben üzennek a világ számára), új terroristacsoport-tagokat vagy támogatókat toboroznak, terjesztik propagandájukat, az internet segítségével szereznek adatokat a lehetséges célpontokról (például épületalaprajzokat), a terroristák kiképzéséhez szükséges online kiadványokat tesznek közzé, vagy anyagi forrás szerzésére is igénybe veszik az internetet.”⁴ Bócné Neparáczki 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.”⁵

Jelen tanulmányban Bócné Neparáczki szavait kölcsönvéve, az információtechnológia terrorista célú felhasználásának „soft” típusú alkalmazására⁶ koncentrálok, ugyanis a kiberterrorizmust illetően egyetértek Dornfeld nézeteivel: „A kiberterrorizmusról szóló diskurzus kapcsán sokszor kevésbé 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 terro-

* Doktorandusz, Pécsi Tudományegyetem Állam- és Jogtudományi Kar.

¹ „A nyugati média az ISIL, vagy ISIS kifejezést használja, ezzel jelezni kívánják, hogy fegyveres szervezetről és nem államról van szó. Ez persze erősen vitatható, sőt nem igaz, mert a szervezet pont az állam létrehozását hangsúlyozza.” Kis-BENEDEK József: Katonai biztonság Marokkótól Iránig. Zrínyi Kiadó, Budapest 2018. 246. o.

² LIEBERMAN, Ariel Victoria: Terrorism, the Internet, and Propaganda: A Deadly Combination. Journal of National Security Law and Policy, 2017. 9. sz. 122. o.

³ NAGY Zoltán András: Tradicionális bűncselekmények számítógépes hálozatokon. JURA, 2007. 13. évf. 1. sz. 127.

⁴ BÓCNÉ NEPARÁCSKI Anna Viktória: A kiberterrorizmus büntető anyagi jogi megítélése. Ügyészek Lapja, 2020. 27. évf. 1. sz. 76–77. o.

⁵ Uo. 79–80. o.

⁶ Uo. 76–77. o.

risták internetes kommunikációja, az aktív dzsihadista propaganda és persze azok a pénzügyi támogatások, amelyeket a terrrorszervezetek az internet segítségével szereztek meg. Véleményem szerint ez egy olyan téma, amivel szemben a jövőben még keményebben kell fellépnie a nemzetközi közösségnek.⁷ Ugyanakkor nem vetem el annak a lehetőségét, hogy a jövőben a helyzet változhat, és az információtechnológia terroristák általi „hard” típusú alkalmazása⁸ a jelenleginél sokkal nagyobb veszélyt képvisel majd.

A terroristák a világhálót Weimann felosztásában pszichológiai hadviselésre, publicitásra és propagandára, adatbányászásra, adománygyűjtésre, toborzásra és mobilizációra, kapcsolattartásra, információ megosztására, tervezésre és koordinációra használják.⁹ Fishman felosztásában tartalom hosztolására (content hosting), közönségfejlesztésre, a brandkontrollra, biztonságos kommunikációra, a közösség fenntartására, finanszírozásra, információ gyűjtésre és gondozására.¹⁰ Tartalom hosztolása (content hosting): A terrrorszervezetek a propaganda széles skáláját termelik, képek, videók, audiófájlok formájában. Megjelenése után a tárolók az internetre kerültek, fájl-megosztó oldalakra. Bizonyos terrrorszervezetek, mint az ISIS, használnak felhő szolgáltatásokat is média tárolására és videóstreamelő szolgáltatásokat propaganda terjesztésére. Mások, mint a Hamász és az Atomwaffen Division, saját weboldallal rendelkeznek. Közönségfejlesztés (audience development): a terroristáknak több okból is szüksége van közönségre – hogy közvetlenül és indirekt módon elérjék azokat, akiket befolyásolni akarnak, hogy a média figyelmét magukra vonják, és hogy azonosítsák a potenciális újoncokat. Példa az ISIS Twitter-használata 2014 és 2015 között. Brandkontroll: A modern terrrorszervezetek használtak és használnak webfórumokat (pl.: al-Hesbah), hivatalos weboldalakokat (pl.: Atomwaffen, Hamász és Hezbollah), Twittert, és például Telegram csatornákat, hogy a célközönségük felé jelezhessék a közzétett anyagaik autentikus voltát. A brandkontroll következetességet kíván, ami a tech platformokra fontos szerepet ró a terrrorszervezetek ilyen tevékenysége elleni küzdelemben. A közösség fenntartására: Az online üzenetküldő alkalmazások és közösségi média platformok zárt csoportjai és a branddel ellátott online fórumok arra szolgálnak, hogy elválasszák a csoport tagjait a külsősöktől. Finanszírozás: A dítális térben a terroristák használhatnak tradicionális pénzügyi küldőket, mint a Western Union, elektronikus bankátutalásokat és online fizetési rendszereket (pl.:

Paypal vagy Venmo), adománygyűjtéseket rendezhetnek P2P tranzferekkel olyan platformokkal, mint a GoFundMe vagy Messenger Payments.¹¹ 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 rendszerellen elkövetett kibertámadásra, azonban a dark weben vásárolhatnak ilyen szolgáltatást.¹² Az internet már az extrémista csoportok propagandájának egyik legfontosabb médiuma. A propaganda terjesztésének egyik célja az új tagok megnyerése, a másik az ideológiájuk vagy ennek 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.¹³ Az internet jelentős és sokoldalú szerepet játszik korunk erőszakos extrémizmusában és terrorizmusában.¹⁴ Erőszakos extrémista csoportok visszaélnék az internet sebezhetőségeivel és nyíltságaival, azt felhasználva radikalizációra, toborzásra és a fiatalok felkészítésére. Fiatalok radikalizációjának médiumaként használnak chatszobákat, közösségi háló oldalakat, mint a Facebook, Twitter, YouTube, és online videójáték videókat is. Terrrorszervezetek, mint például a Boko Haram, az ISIS és az Al-Kaida, és más extrémista csoportok stratégiaileg 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 az anyagaik online terjesztésére. Apau szerint ezért fontos, hogy a kormányok felismerjék, hogy a fiatalok online radikalizációjának folyamata egy globális és sokoldalú jelenség, melyben a közösségi médiát egy eszközként használják 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 kellene vizsgálni.¹⁵ Piazza és Guler 2019-ben 6000 személyt vizsgált 6 arab országból, hogy kiderítsék, hogy azok a személyek, akik használják az internetet politikai hírek követésére vagy politikai nézetek kinyilvánítására, nagyobb valószínűséggel támogatják-e az ISIS-t.

¹¹ Uo. 84–86. o.

¹² BÁNYÁSZ Péter: Kiberbűnözés és közösségi média. Nemzetbiztonsági Szemle, 2017. 5. évf. 4. sz. 71. o.

¹³ NITSCH, Holger: Terrorismus und die Nutzung des Internet. In: Rüdiger, Thomas-Gabriel – Bayerl, Petra Saskia (Hrsg.): Cyberkriminologie: Kriminologie für das digitale Zeitalter. Springer VS, Wiesbaden 2020. 198. o.

¹⁴ CONWAY, Maura: Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research. Studies in Conflict & Terrorism, 2017. 40. évf. 11. sz. 91. o.

¹⁵ 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.

⁷ DORNFIELD László: Kiberterrorizmus – a jövő terrorizmusa? In: Mezei Kitti (szerk.): A büntügyi tudományok és az informatika. Pécsi Tudományegyetem Állam- és Jogtudományi Kar, MTA Társadalomtudományi Kutatóközpont, Budapest–Pécs 2019. 61. o.

⁸ BÓCZNÉ NEPARÁCZKI: i. m. 76–77. o.

⁹ WEIMANN, Gabriel: www.terror.net: How Modern Terrorism Uses The Internet. United States Institute Of Peace, Washington, D.C. 2004. 5–10. o. <https://www.usip.org/sites/default/files/sr116.pdf> (2019.12.10.)

¹⁰ Fishman, Brian: Crossroads: Counter-terrorism and the Internet. Texas National Security Review, 2019. Vol. 2. No. 2. 84–86. o.

Arra jutottak, hogy azok a válaszadók, akik a híreket online követik, jelentősen nagyobb valószínűséggel támogatják az ISIS-t, mint azok, akik azt a televízióban vagy a nyomtatott sajtóban követik. Továbbá arra, hogy akik online fórumokat használnak politikai nézetek kinyilvánítására, nagyobb valószínűséggel fejezik ki a támogatásukat az ISIS felé. Az online politikai diskusziókban részt vevők nagyobb valószínűséggel támogatják az ISIS-t, mint azok, akik hagyományos politikai tevékenységet folytatnak, bár kevésbé, mint azok, akik pörlekedő politikai magatartást tanúsítanak, mint a politikai tüntetésen való részvétel.¹⁶

Egyre több terrorizmusban részt vevő személy használta az internetet valamilyen módon az erőszak felé vezető útján. Reeve szerint az internet kétségtelenül egy a radikalizációt segítő eszköz, lehetővé téve a felhasználóknak, hogy egymással és akár terrorista csoportok tagjaival interaktáljanak, és kapcsolatokat képes létrehozni. A felhasználók találhatnak információt, köztük erőszakos extrémista ideológiát, propagandavideókat és publikációkat. Az internet eszközöket nyújt a logisztikához és felderítéshez. A terroristák az internetet használják virtuális interakcióra és virtuális tanulásra. A felhasználó internethasználata a radikalizáció során az igényei és érdekei szerint változik. Reeve szerint ezért a terroristák és leendő terroristák az internetet ügyintézésre (pl.: járatok lefoglalására) és kommunikációra használják. Néhányan amellet érvelnek,¹⁷ hogy a terrorista csoportokban történő tagság már a személyes megítélésen alapul, a terrorista ismeretek tömeges elterjedése miatt.¹⁸ Mind a dzsihádisták¹⁹ és jobboldali extrémista propaganda arra ösztönzi az egyéneket, hogy erőszakos cselekedeteket hajtsanak végre autonóm módon, és az elkövetőket „mártírként” és „szentként” dicsőíti.²⁰

A terrorista csoportok a műveleteik finanszírozásához szükséges bevételszerzési és pénzáttalalási módszerei tekintetében haladnak a modern technológia új trendjeivel (mint a kriptovaluták és a darkweb használata), de a tradicionális módszereket is használják (mint a zakat és hawala).²¹ Amikor csak külső anyagi forrásokra van szükségük, a terroristák különféle módszerekhez folyamodnak, melyek bonyolultságukban az egyszerűtől a rendkívül összetettig (Lásd például az al-Kasszám Brigádok, a Hamász katonai szárnyának felhívását bitcoinos közösségi finanszírozás-

ra.²²) terjednek.²³ Különösen riasztó a tény, hogy „... a terrorizmus finanszírozásával szemben a büntetőjogi eszközök hatékonysága a nullához konvergál.”²⁴ Az internetes pénzügyi tranzakciók száma növekszik. Újabb típusú fizetési eszközök, virtuális fizetőeszközök²⁵ jelennek meg, mint a Bitcoin és a Litecoin, melyek jogi státusza nem teljesen tiszta. Az információs technika fejlődése ugyan könnyebbé tette a pénzügyi szolgáltatások használatát, de a technológia a bűnözők számára egyre több lehetőséget nyújt az ezekkel történő visszaélésekre.²⁶

A terroristák más platformokon végzett tevékenységüket a dark web használatával egészítik ki, mivel annak titkosításokkal rendkívül erősen védett platformjai vannak, mely miatt a felhasználók IP címét a bűnüldöző szervek rendkívül nehezen tudják lekövetni, ezért nagyfokú anonimitást biztosít.²⁷ 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 okostelefonos propaganda applikációk.²⁸ További alternatív kommunikációs csatorna bűnözők,²⁹ terrorizmus finanszírozók, pénzmosók számára az online videójátékok, ún. MMORPG-k (Massively Multiplayer Online Role Playing Game), mint például a World of Warcraft és Second Life chatszobái és privát üzenetei.³⁰

²² FANUSIE, Yaya: Hamas Military Wing Crowdfunding Bitcoin. <https://www.forbes.com/sites/yayafanusie/2019/02/04/hamas-military-wing-crowdfunding-bitcoin/#306575c34d7f> (2020.08.18.)

²³ Europol's 2019 EU Terrorism Situation and Trend Report (TE-SAT) 17. o.

²⁴ GÁL István László: Új biztonságpolitikai kihívás a XXI. században: a terrorizmus finanszírozása. Szakmai Szemle: A Katonai Nemzetbiztonsági Szolgálat kiadványa, 2012. 8. évf 1. sz. 15. o.

²⁵ A virtuális pénzekkel kapcsolatos visszaélésekről bővebben: TÓTH Dávid: A virtuális pénzekkel kapcsolatos visszaélések. Rendészet-Tudomány-Aktualitások: A rendészettudomány a fiatal kutatók szemével, Szerkesztette: Baráth Noémi Emőke – Mezei József, Doktoranduszok Országos Szövetsége, Rendészettudományi Osztálya, Budapest 2019. 242–250. o.

²⁶ TÓTH, Dávid: Credit card fraud with a comparative law approach. In: 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, Bitola 2019. 232. o.

²⁷ ÖZKAYA, Erdal: The Use of Social Media for Terrorism. NATO Defence Against Terrorism Review, 2017. Vol. 9. 54. o.

²⁸ ALKHOURI, Laith – KASSIRER, Alex: Techforjihad: Dissecting Jihadists' Digital Toolbox. Flashpoint, USA 2016. 1. o. <https://www.flashpoint-intel.com/wp-content/uploads/2016/08/TechForjihad.pdf>. o. (2020.08.18.)

²⁹ Az internet egyre nagyobb szereppel bír nemcsak a terrorizmus, hanem az emberkereskedelem terén is. Lásd: Ripszám Dóra: Emberkereskedelem az interneten. KRE-DIT: A KRE-DOK ONLINE TUDOMÁNYOS FOLYÓIRATA, 2020. 3. évf. 1. sz.

³⁰ IRWIN, Angela – SLAY, Jill: Detecting Money Laundering and Terrorism Financing Activity in Second Life and World of Warcraft. In: Valli, Craig (szerk.): Proceedings of the 1st International Cyber Resilience Conference ICR2010. Edith Cowan University, Perth 2010. 41. o.

¹⁶ PIAZZA, James A. – GULER, Ahmet: The Online Caliphate: Internet Usage and ISIS Support in the Arab World, Terrorism and Political Violence, 2019. 1. o.

¹⁷ KIRBY, Aidan: The London Bombers as ‘Self-Starters’: A Case Study in Indigenous Radicalization and the Emergence of Autonomous Cliques. Studies in Conflict & Terrorism, 2017. 425. o. Idézi: Reeve, Zoey: Engaging with Online Extremist Material: Experimental Evidence, Terrorism and Political Violence, 2019. 2. o.

¹⁸ REEVE: i. m. 2. o.

¹⁹ A vallási indíttatású terrorizmusról lásd: KÓHALMI László: Gondolatok a vallási indíttatású terrorizmus ürügyén. Belügyi Szemle, 2015. 63. évf. 7–8. sz. 52–71. o.

²⁰ 6. o.

²¹ PASCA, Viorel – ORZA, Daniela Simona: Terrorism: between the need for funding and obtaining funding sources. Journal Of Eastern-European Criminal Law, 2019. No. 1. 227. o.

2. A szélsőjobb oldali terrorizmus online

2.1. A szélsőjobb oldali terrorizmus előretörése

Bartkó az Europol jelentéseiből³¹ kiindulva rögzíti, hogy az elmúlt években a terrorizmus dzsihadista szárnya erősödött meg az EU területén.³² A szélsőjobb oldali terrorizmus megerősödése is megfigyelhető: Az Europol's 2019 EU Terrorism Situation and Trend Report (TE-SAT) szerint a szélsőjobb oldali terrorizmushoz fűződő letartóztatások száma viszonylag alacsony maradt, de harmadik éve egyhuzamban növekedett. A jobb oldali extrémisták a társadalom iszlamizálódásától és a nemzeti identitás elvesztésétől való félelmeken élőködnek. A 2018-as terrorizmusoz fűződő büntetőügyek alapján a dzsihadista terrorista elítélések száma maradt a legmagasabb, de mind a baloldali és jobb oldali terrorista elítélésekben növekvés volt tapasztalható.³³ A trend folytatódni látszik: Az Europol's 2020 EU Terrorism Situation and Trend Report (TE-SAT) szerint 2019-ben 3 EU tagállam összesen hat jobb oldali terrorcselekményt jelentett (egy befejezett, egy sikertelen, négy megakadályozott), 2018-ban ez a szám egy volt. Továbbá két támadást jelentett Németország, melyek a nemzeti törvények szerint nem minősítettek terrorizmusnak, de azokat jobb oldali extrémisták követték el, és három ember életét oltották ki.³⁴

2.2. A szélsőjobb oldali terroristák internetes aktivitása és kutatásának nehézségei

A szélsőjobb internacionalizációjában kulcsfontosságú szerepet játszik a web. Az európai, és amerikai szélsőjobb oldali szervezetek egyre jobban támaszkodnak az internetre, a nemzeti törvények és a rendőrség nyomozásának megkerülésére. Az internet kommunikációs lehetőségei a transznacionális szolidaritást támogatják. Az izolált, egyéni „fogyasztók” közös identitást találhatnak a szélsőjobb oldali weboldalakon, mely meggyőzi őket, hogy nincsenek egyedül, hanem egy közösség részei, noha az virtuális. Az internet fon-

tos szerepet játszhat a mobilizáció folyamatainak megkönnyítésében is, csökkentve nagyszámú egyén között a kommunikáció költségeit, megoldja a vezetés és networking problémáit, és a szervezeteknek transznacionális és globális események szervezését teszi lehetővé. A kiberbűnözőkhöz hasonlóan a jobb oldali extrémisták is felhasználhatják illegális és szürke zónás tevékenységekre, pl. hackelésre, tömeges fenyegető e-mailekre, és csalásra. Végül, az internet hatékony eszköz lehet a „fantomsejtek” hálózatán alapuló, egyes amerikai radikális jobb oldali aktivisták által támogatott „vezető nélküli ellenállás” koncepciójának hatékony megvalósításában.³⁵ Mind a tradicionális média és mind az internet szerepe egyre elismertebb, mint fontos tényező a radikális jobb oldali mobilizáció megértésében.³⁶

Globális szinten egy szélsőjobb oldali extrémisták általi terrorhullám volt tapasztalható az utóbbi években: Pittsburgh, Christchurch, Poway, El Paso, Halle (továbbá Barum és Haunau).³⁷ 2018. október 27-én Robert G. Bowers a Tree of Life pittsburghi zsinagógában megölt 11 embert és támadása során 6 ember megsérült.³⁸ 2019. március 15-én Brenton Tarrant az új-zélandi Christchurch két mecsetében 50 embert megölt és sokakat megsebesített (egy személy később belehalt a sérüléseibe). Tarrant röviddel a támadás előtt manifesztumát e-mailben elküldte politikusoknak és sajtóorgánumoknak, és az elkövetés egy részét Facebookon livestreamelte (élőben közvetítette).³⁹

A christchurchi terrortámadás során az internet terrorista célokra való felhasználásának eddig példátlan elemei voltak tapasztalhatóak. A terrorcselekményről készült livestreamelt videó és az elkövető manifesztuma az interneten gyorsan elterjedt, ami az online terrorista tartalmak elleni harc új kihívásaira mutatott rá.⁴⁰ 2019. április 27-én John Timothy Earnest egy powayi zsinagógában egy személyt megölt, és hármat megsebesített. A támadás előtt egy manifesztumot töltött fel az internetre. Earnest azt állította, hogy az új-zélandi terrortámadás volt a saját támadásának a katalizátora.⁴¹ 2019. augusztus 10-én a norvég Barumban az Al-Noor Islamic Centre mecsetében egy

³⁵ 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.

³⁶ RYDGREN, Jens: The Radical Right: An Introduction. In: Rydgren, Jens (ed.): *The Oxford Handbook of the Radical Right*. Oxford University Press, New York 2018. 9. o.

³⁷ MACKLIN, Graham: The El Paso Terrorist Attack: The Chain Reaction of Global Right-Wing Terror, *CTC Sentinel*, 2019. 12. évf. 11. sz. 1. o.

³⁸ AMEND, Alex: Analyzing a terrorist's social media manifesto: the Pittsburgh synagogue shooter's posts on Gab. <https://www.splcenter.org/hatewatch/2018/10/28/analyzing-terrorists-social-media-manifesto-pittsburgh-synagogue-shooters-posts-gab> (2020.08.18.)

³⁹ CHARLES CROTHERS – THOMAS O'BRIEN: The Contexts of the Christchurch terror attacks: social science perspectives, *Kōtuitui: New Zealand Journal of Social Sciences Online*, 2020. 15. évf. 2. sz. 248. o.

⁴⁰ Europol The Internet Organised Crime Threat Assessment, Europol, Hága, 2019. 48. o. <https://www.europol.europa.eu/iocta-report> (2020.08.18.)

⁴¹ 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. 17. o.

³¹ Europol's 2015 EU Terrorism Situation and Trend Report (TE-SAT); Europol's 2016 EU Terrorism Situation and Trend Report (TE-SAT); Europol's 2017 EU Terrorism Situation and Trend Report (TE-SAT); Europol's 2018 EU Terrorism Situation and Trend Report (TE-SAT)

³² 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.

³³ Europol's 2019 EU Terrorism Situation and Trend Report (TE-SAT). 6–7. o.

³⁴ Europol's 2020 EU Terrorism Situation and Trend Report (TE-SAT) 6. o.

fegyveres nyitott tüzet. Egy ember megsérült.⁴² Az elkövetőnek, Philip Manhausnak a rendőrség szerint szélsőjobboldali és bevándolásellenes nézetei voltak. A támadása előtt egy Tarrantra utaló üzenetet posztolt az EndChan fórumra. Annak moderátorai eltávolították a posztot és a fő domain is offline került az elkövetés után.⁴³

2019. október 9-én, jom kippur ünnepe idején Stephan Balliet erőszakkal próbált behatolni a zsinagógába, a németországi Halle/Saale-ben, hogy online közvetített vérfürdőt rendezzen. Az épületbe bejutnia nem sikerült, ezért véletlenszerűen lelőtt egy arra járórt és egy török étteremhez ment, ahol lelőtt még egy embert. Balliet egy sisakra szerelt okostelefont használt a Twitch nevű platformon történő livestreamhez. Az internetre manifesztumot is töltött fel.⁴⁴ 2019. augusztus 3-án Patrick Wood Crusius egy El Paso-i Walmartban nyitott tüzet, 20 ember életét kioltva. Később 2 személy belehalt a sérüléseibe, így áldozatok száma 22-re emelkedett. A támadás során 26 ember sérült meg.⁴⁵ Az elkövető a fegyverét és hozzá 1000 darab lőszert az internetről vásárolta. Létrehozott egy „The Inconvenient Truth” (A kellemetlen igazság) című dokumentumot, amit az elkövetés előtt feltöltött az internetre.⁴⁶ 2020. február 19-én Tobias Rathjen a németországi Haunau Midnight vízipipabárjában megölt 3 embert. Azután az Arena Bér & Cafera nyitott tüzet, további 5 ember életét kioltva. Ez után hazament, és lelőtte az anyját és önmagát is. Órákkal a támadás után kiderült, hogy az internetre töltött anyagai alapján Rathjenre hatott a tradicionális szélsőjobb, a faji alapú és a bevándorlásellenes narratívák kombinációja és több obskúrus összeesküvés elmélet. Az ügy a további kutatás szükségességét jelzi ezen ideák kereszteződésének és az online ökoszisztémának tekintetében, ahol ezek virágznak, és ahol az olyan elképzelések, mint a „Great Replacement” elmélet hevesen propagáltak, melynek aspektusai megjelennek Rathjen manifesztumában. Crawford és Keen szerint ez az idea köti össze a látszólag különböző terrortámadásokat egy ideológiailag analóg terrorcselekmények globális hálózatában.⁴⁷

Macklin szerint egy a jobboldali extrémisták erőszakos online szubkulturális milióiban ösztönzött láncreakcióról van szó. Ez a digitális ökoszisztéma egy az abban részt vevők erőszak iránti ingerküszöbét csökkenteni szolgáló kumulatív lendületet táplál. Egyik terrorcselekmény ösztönzi és inspirálja a másikat, „szentek” és „mártírok” növekvő kánonját létre-

hozva.⁴⁸ Az Europol's 2020 EU Terrorism Situation and Trend Report (TE-SAT) is megerősíti, hogy 2019 a jobboldali támadások Christchurchben, Powayban, El Pasoban, Barumban és Halléban egy világszintű erőszakos incidensek hullámának része voltak, és azok elkövetői hasonló transznacionális online közösségeknek voltak részei és egymástól merítettek inspirációt.⁴⁹ A 8chan /polján sok névtelen felhasználó (anon) úgy utalt Tarrantra, a christchurchi elkövetőre, mint „Saint Tarrant” („szent Tarrant”) középkori inspirált-ságú ikonográfiával együtt.⁵⁰

2014 és 2017 között az ISIS közösségimédia-platformok széles skáláján tartott fenn virágzó közösségeket. A fő platformok agresszív felhasználóifóók és tartalom-eltávolító politikájának köszönhetően a látható közösségek már majdnem eltűntek. A christchurchi terrortámadás után többször felmerült a kérdés, hogy a fő platformok miért nem tudják az extrém jobboldalt ugyanúgy kiűzni.⁵¹

Conway rávilágít, hogy az extrém jobboldal nem hasonlítható az ISIS-hez, az inkább egy gyorsan változó „szcena”, mint egy csoport, és miközben e szcénába 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 szövegeket támogatnak. Ugyan ez nem teljesen akadályozza meg az online platformokat a tartalmak eltávolításában, mivel azoknak nem kell terrorista természetűnek lenniük, hogy eltávolíthatóak legyenek, de komplikálja a helyzetet. Hatalommal bíró szereplők – államfők, fő politikai pártok, néhány tradicionális médiaorgánum és a nyugati közvélemény jelentős része azonosulnak ezzel a tartalommal. Ez a közösségimédia-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 közösségimédia-platformjaikat. Ez kifejezetten igaz az extrém jobboldali aktivistákra az USA-ban, akik hivatkozhatnak az Első Alkotmánymódosításra. A fő közösségimédia-cégek az utóbbi években lépéseket tettek a gyűlölet visszafogására a platformjaikon. Nagyobb rajtuk a nyomás a christchurchi terrortámadás és az azt követő más jobboldali extrémista támadások óta.⁵² A „The Christchurch Call” egy ‘kormányok és tech cégek általi elköteleződés online terrorista és erőszakos extrémista tartalmak eltávolítására.’⁵³ 2019-

⁴² <https://www.bbc.com/news/world-europe-49308016> (2020.08.18.)

⁴³ <https://www.bbc.com/news/world-europe-49318001> (2020.08.18.)

⁴⁴ KOEHLER, Daniel: The Halle, Germany, Synagogue Attack and the Evolution of the Far-Right Terror Threat. CTC Sentinel, 2019. 12. évf. 11. sz. 14. o.

⁴⁵ MACKLIN: i. m. 1.

⁴⁶ United States of America v. Patrick Wood Crusius, Case 3:20-cr-00389-DCG 02/06/20 1–2. o.

⁴⁷ CRAWFORD, Blyth – KEEN, Florence: The Hanau Terrorist Attack: How Race Hate and Conspiracy Theories Are Fueling Global Far-Right Violence. CTC Sentinel, 2020. 13. évf. 3. sz. 1. o.

⁴⁸ MACKLIN: i. m. 1.

⁴⁹ Europol's 2020 EU Terrorism Situation and Trend Report (TE-SAT)

⁵⁰ EVANS, Robert: Ignore The Poway Synagogue Shooter's Manifesto: Pay Attention To 8chan's /pol/ Board. <https://www.bellingcat.com/news/americas/2019/04/28/ignore-the-poway-synagogue-shooters-manifesto-pay-attention-to-8chan-pol-board/> (2020.08.18.)

⁵¹ CONWAY, Maura: Routing the Extreme Right. The RUSI Journal, 2020. 1. o.

⁵² Uo. 6. o.

⁵³ <https://www.christchurchcall.com/> (2020.08.18.). Idézi: Conway, Maura: Routing the Extreme Right. The RUSI Journal, 2020. 6. o.

ben a christchurchi támadás internetes hatásai után az állam és kormányfők, és az internetipar képviselői találkoztak Párizsban és aláírták a Emmanuel Macron francia elnök és Jacinda Ardern új-zélandi miniszterelnök által indított Christchurch Callt. 2017-ben a Facebook, Microsoft, Twitter és YouTube létrehozta a Global Internet Forum to Counter Terrorismot. 2019-ben csatlakozott a Dropbox, Amazon és WhatsApp. A fórum a 2015 decemberében létrehozott EU Internet Forumra építkezik és jelenleg a Christchurch Call inspirálja.⁵⁴ A főbb, és sok kisebb közösségimédia-cégek által közös lépések történtek a támadáshoz közvetlenül kötődő tartalmak platformjaikról való eltávolítására. Végső soron a probléma nem az extrém jobboldali terrorista tartalmak fő közösségimédia-platformokra való feltöltése és terjedése, mert ezek hasonlóan kezelhetők, mint az ISIS tartalmak. A probléma árnyaltabb és vitásabb, az az extrém jobboldali tartalom fő platformokról történő eltávolításának helyénvalóságára vonatkozik.⁵⁵

A szélsőjobboldali extrémizmus elleni küzdelem egyik kihívása, hogy nincs egy csoportokat összekötő egyesítő ideológiai rendszer. Több alapul szolgáló hitrendszert vizsgáltak már szélsőjobboldali szereplők-nél, köztük kormányellenes, antiglobalista, bevándorlásellenes, szuverén polgár mozgalmakat (sovereign citizen movements), paramilitáris csoportokat, neonácikat, odinistákat és faji ideológiai alapú csoportokat.⁵⁶

A jobboldali extrémizmus összetett ideológiáinak részletes⁵⁷ ismertetése szétfeszítené a jelen tanulmány kereteit.

Mudde a jobboldali extrémizmus 26 szakirodalmi definíciójának vizsgálata alapján a jobboldali extrémizmus 58 különböző jellemzőjét azonosítja, és arra mutat rá, hogy ezek közül csak öt jelenik meg valamilyen formában legalább a vizsgált szerzők felénél: nacionalizmus, rasszizmus, xenofóbia, antidemokrácia és erős állam.⁵⁸

A szélsőjobboldali terrorizmus témájának kutatása során kihívást jelent még, hogy sokszor komoly nehézséget okoz a tömeggyilkosság (mass shooting) és a terrortámadás elhatárolása.⁵⁹ Egy adott eset tekintetében vitás lehet, hogy melyik kategóriáról is van szó. Ez többek közt annak is köszönhető, hogy Townshend szerint egyfajta címkézésről van szó a terrorista szó

használata esetén. Ezt a megnevezést rendszerint mások, elsősorban a megtámadott államok kormányai aggatják a támadóikra, mert a terrorizmus fogalma súlyos mellékjelentéseket, azaz erőteljes kriminalitást, embertelenséget és a tényleges politikai támogatás hiányát foglalja magában.⁶⁰ A terrorizmus tipizálását illetően Korinek megkülönböztet állami és nem állami terrorizmust; nemzeti és nemzetközi terrorizmust. Ideológiai indítást tekintve szélsőjobboldali és szélsőbalos szervezeteket, etnikai, faji, vallási okokra visszavezethető, vagy ilyen célok 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”.⁶¹

Véleményem szerint adott elkövetéseknél ugyan lehet vitatkozni, hogy annak esetében tömeggyilkosságról (ún. mass shooting) vagy pedig terrorizmusról beszélünk-e, de a határvonal sokszor nagyon vékony és az áldozat számára mindegy, hogy ún. mass shooter vagy pedig terrorista veszi el értelmetlen módon az életét. Mindkét elkövető cselekményét ugyanolyan fontos megakadályozni. A különbségtétel külön tanulmány érdemel.

2.3. A 8chan fórum és a terror „videójátékosítása”

A 8chan online fórumot Fredrick Brennan indította 2013-ban, a „szólásszaszabadság utópiájaként”. A fórum erőszakos extrémisták gyülekezőhelyévé, megafonjává és toborzóplatformjává vált.⁶²

8chant a christchurchi, a powayi és az El Pasó-i terrortámadások elkövetői is használták. Az oldal különböző témájú társalgócsoportok széles skáláját tartalmazta, az animéken és kriptovalutákon át a politikáig és videójátékokig. Az oldal/pol/ boardja szélsőjobboldali extrémisták találkozóhelye volt, anonim tagokat erőszakos cselekedetek elkövetésére radikalizálás céljával. A christchurchi elkövető egy manifesztumot tett fel a 8chan-ra, „The Great Replacement” címmel, továbbá egy linket a Facebook Live-on livestreamelt támadásáról. A videót kevesebb mint 200-an nézték meg a Facebookon, mielőtt azt az oldal eltávolította volna, de a 8chan lehetővé tette, hogy a videó milliókhoz jusson el. Az El Pasó-i támadás elkövetője is töltött fel manifesztumot az oldalra, melyben Tarrantot dicsőítette. A powayi támadás elkövetője is használta a 8chant.⁶³ Az

⁵⁴ François THÉRON: Terrorist content online: Tackling online terrorist propaganda. 2020. 2–3. o. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/649326/EPRS_BRI\(2020\)649326_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/649326/EPRS_BRI(2020)649326_EN.pdf) (2020.08.18.)

⁵⁵ CONWAY, Maura: Routing the Extreme Right. The RUSI Journal, 2020. 6. o.

⁵⁶ 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.

⁵⁷ A jobboldali extrémizmus összetett ideológiájáról bővebben: Boross Zsigmond Attila: A jobboldali extrémizmus összetett ideológiája – mint a terrorizmus potenciális hivatkozása – TERROR & ELHÁRÍTÁS, 2017. 4. sz. 23–48. o.

⁵⁸ MUDDÉ, Cas: The Ideology of the Extreme Right. Manchester University Press, Manchester/New York 2000. 11. o.

⁵⁹ 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, 2019. 1. o.

⁶⁰ TOWNSHEND, Charles: A terrorizmus. Magyar Világ Kiadó, Budapest 2003. 9. o.

⁶¹ KORINEK László: A terrorizmus. Belügyi Szemle, 2015. 7–8. sz. 17–19. o.

⁶² ROOSE, Kevin: 8chan Is a Megaphone for Gunmen. ‘Shut the Site Down,’ Says Its Creator. <https://archive.is/JrNGc> (2020.08.18.)

⁶³ ÇELIKSOY, Ergül – OUMA, Smith: Terrorist Use Of The Internet. Bilişim Hukuku Dergisi, 2019. Vol. 1. No. 2. 250–252. o.

El Paso-i lövöldözés elkövetője, Crusius az elkövetés kezdetét a 8chan /pol boardján jelentette be és egy négyoldalas manifesztumot csatolt a poszthoz, és egy dokumentumot az, amelyben szerepelt a neve. A poszt archivált változata megtalálható, 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 threadet (komment-szekciót) szinte azonnal eltávolították az oldal moderátorai, akiknek már gyakorlata volt az ilyen threadek eltávolításában. A poszt archivált változatára csak három válasz érkezett. Az első egy névtelen (8chan szóhasználatnál anon), aki azt állítja, hogy a 8chan egy „board of peace” (a béke fóruma), ami nem fogadja el az erőszakot. Ez a szóhasználat mém a névtelenek között, gúnyosan utalva az állításokra, hogy az iszlám a „béke vallása”. A következő posztoló azt írta, hogy: „Every shabbat” („minden sabbat”), a reményét kifejezve, hogy ilyen támadások minden hétfőjén történjenek. Az eredeti thread gyorsan eltávolításra került, de más névtelenek újra kipsztozták a poszt másolatait és a manifesztumhoz vezető linket. Körülbelül két órával az elkövetés után került fel egy következő poszt, melyben az azt posztoló és mások szidták a lövöldözőt a „shitty” („silány”) és „0 effort manifesto” („0 erőfeszítéses manifesztum”) miatt. Az elkövető szavaiban nincs semmi új. Ugyanarról a fehér emberek „felcsereléséről” fejt ki a félelmeit, mint ami Tarrantot motiválta és leírja, hogy erősen motiválta őt Tarrant manifesztuma. A 8chan használói sok időt szenteltek Tarrant manifesztumának terjesztésére, hogy több elkövetést inspiráljanak.⁶⁴ Azt több nyelvre is lefordították.⁶⁵ Az El Paso-i események is bizonyítják, hogy ez a stratégia működik. Evans szerint a két legfontosabb tanulság az El Paso-i lövöldözésből a következő: 1. A 8chan /pol boardja továbbra is szándékosan radikalizálja a tömeggyilkosokat. 2. Az ártatlanok lemészárlása „videójátékosítva” („gamified”) lett. Az utóbbit világosan illusztrálja néhány komment, amiket Evans az El Paso-i események után fedezett fel online. Ebben a threadben miután egy névtelen képernyőképet posztol az El Paso-i elkövető threadjéről, azt kérdezi: „Is nobody going to check these incredible digits?” („Senki nem nézi meg ezeket az elképesztő számokat?”) Az állítás valószínűleg az elkövető magas emberáldozatainak számára utal. (Vagy esetleg az ismétlődő „14-re” egy poszt ID-ben, vagy más hasonlóan). A Christchurch után a 8chan használói gyakran kommentelték Tarrant áldozatainak magas számát és utaltak a szándékukra, hogy „beat his high score”⁶⁶ („megverjék a high score-ját”). Gyakran került fel egy

⁶⁴ EVANS, Robert: The El Paso Shooting and the Gamification of Terror. <https://www.bellingcat.com/news/americas/2019/08/04/the-el-paso-shooting-and-the-gamification-of-terror/> (2020.08.18.)

⁶⁵ EVANS, Robert: Ignore The Poway Synagogue Shooter's Manifesto: Pay Attention To 8chan's /pol/ Board. <https://www.bellingcat.com/news/americas/2019/04/28/ignore-the-poway-synagogue-shooters-manifesto-pay-attention-to-8chans-pol-board/> (2020.08.18.)

⁶⁶ A high score videójátékokban az elért legmagasabb eredmény/érték/pont.

kép Christchurchöt 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 egyetlen igazi innovációt, amit a 8chan a globális terrorizmusba hozott: a tömeges erőszak videójátékosítását, mely nem csak a „high score-okra” való utalásokban látható, hanem abban is, ahogy Tarrant elkövette a támadását – élőben közvetítette úgy, hogy a lövöldözése majdnem teljesen úgy nézett ki, mint egy FPS videójáték. Ez tudatos volt, és az is, hogy ehhez szórakoztató és inspiráló aláfestő zenét választott. A powayi zsinagógai lövöldöző Tarrantot próbálta utánozni ezekben a taktikákban, zenei playlistet posztolva a lövöldözése mellé. Jelenleg nem ismert, hogy az El Paso-i elkövető megpróbálta-e livestreamelni a mészárlását, de a 8chanen található posztok azt sugallják, hogy a névtelenek őt „ourguyként” („mi fickónk”) vállalják fel és az eseményről szóló hírek live chat-jeit megpróbálták elárasztani.⁶⁷ 2019. augusztus 19-én a 8chan, más néven Infinitychan offline került, amikor a Cloudflare megvonta a támogatást az oldaltól, ejtve azt, de csak az augusztus 3-i El Paso-i lövöldözés után.⁶⁸ Sok 8chan-használó a Discordra migrált át.⁶⁹ A 8chan örökségének továbbvitelére a legjelentősebb példa a „8kun”, mely legtöbbször megbízhatóan csak a dark weben érhető el.⁷⁰

2.4. Der harte Kern (The Hard Core)

2020. február 15-én öt németországi tartományban tartottak házkutatásokat és elfogtak 12 embert szélsőjobboldali terrorista szervezkedés gyanúja miatt. A szervezet célja Németország állami és társadalmi rendjének, demokratikus berendezkedésének megdöntése volt.⁷¹ A „The Hard Core” elnevezésű új terrorista sejt polgárháború indításának szándékával mecseteket tervezett megtámadni. A csoport 10 koordinált támadást tervezett végrehajtani, melyeket az új-zélandi Christchurch támadás inspirált. A tagok a WhatsAppon találkoztak és a kutatók által „hive terrorism”-nek nevezett jelenség jegyeit mutatták, mely során szervezett extrémista szcénákhoz kevés korábbi kötődéssel rendelkező személyek hálózatait mobilizálják erőszakos cselekedetek megtervezésére. A felfedezést megnehezíti a csoportformáció többé-kevésbé spontán természetű. A csoport 2019 nyarán nagyon gyorsan alakult meg és radikalizálódott, melybe tartoztak régóta tevékenykedő neonácik, és olyanok is, akik korábban ismeretlenek voltak a hatóságok előtt. A razzia során

⁶⁷ EVANS, Robert: The El Paso Shooting and the Gamification of Terror. <https://www.bellingcat.com/news/americas/2019/08/04/the-el-paso-shooting-and-the-gamification-of-terror/> (2020.08.18.)

⁶⁸ <https://storyful.com/resources/blog/what-is-8chan/> (2020.08.18.)

⁶⁹ GLASER, April: Where 8channers Went After 8chan. <https://slate.com/technology/2019/11/8chan-8kun-white-supremacists-telegram-discord-facebook.html> (2020.08.18.)

⁷⁰ CRAWFORD, Blyth: Chan Culture and Violent Extremism. <https://gnet-research.org/2019/12/31/chan-culture-and-violent-extremism-past-present-and-future/> (2020.08.18.)

⁷¹ <https://honvedelem.hu/cikk/elfogtak-tobb-feltetelezett-szelojobboldali-terroristat-nemetorszagban/> (2020.08.18.)

egy házi készítésű fegyvert (amelyet először a német hallei támadás során dokumentáltak) is felfedeztek, mely azért volt aggodalmat keltő, mert így nincs szükség harmadik személyekre a fegyverek beszerzéséhez, és ez nehezíti a felfedezést. A csoportnak nemzetközi kapcsolatai is voltak: a szélsőjobboldali extrémista finn Soldiers of Odin csoporttal.⁷²

2.5. Feuerkrieg Division

A német nyomozók figyelmét a szélsőjobboldali „Feuerkrieg Division” (FKD) nevű terrorszervezet keltezte 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” az új tagok toborzásáért és a felvételükről való döntésért volt felelős. Bombagyártási instrukciókat osztott, szeretett volna Londonban terrortámadást, és katonai kiképző táborok szervezését javasolta februárra, az NSDAP „100. születésnapjára.” Mivel 14 év alatti, Észtországban nem lehet büntetőeljárás alá vonni. A „Parancsnok” által 2018. októberében társalapított FKD propagandáját videók, képek és írások formájában terjesztette közösségi hálózatokon és a Telegram alkalmazáson. Az FKD a jobboldali terroristákat „szenteknek” tartja, és tagjaikat a követésükre szólítja fel. Az FKD február 8-án jelentette be felszámolását. A belső chatekben azonban az látszik, hogy a nyilatkozat csak a nyilvánosságnak szól, és a szervezet új névvel működik tovább.⁷³

2.6. The Base

Rinaldo Nazzaro aki a „Norman Spear” és „Roman Wolf” fedőneveket használja, 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 fajlag motivált erőszakos extrémista csoportot, ami meg akarja gyorsítani az Egyesült Államok kormányának bukását és egy fehér etnoállamot akar létrehozni. A 2018 júliusában alapított szervezet online szerez követőket, titkosított üzenetküldő alkalmazásokkal kommunikál és a tagokat paramilitáris képzésben való részvételre buzdítja.⁷⁴ A propagandája nagy fenyegetést jelent, mivel az az egyéneket a ma-

gányos farkas és terroristasejt-orientált mentalitás felé tereli.⁷⁵

3. ISIS az interneten

3.1. Az ISIS online útja

Mennyiség és minőség tekintetében az ISIS úttörő volt az online terjesztésben. A terrorszervezet az online jelenlétét ugyanolyan fontosnak tartja, mint a csatatéren végzett műveleteit.⁷⁶ A közösségi médiás jelenlétük ellen számos platform ellenlépéseket tett. A Például a Twitter kifejezetten keményen lépett fel az ISIS-szimpatizáns felhasználói fiókokkal szemben, de a terroristák alkalmazkodóképesek, céljaik elérése és a kommunikáció biztosítása érdekében folyamatosan alternatív lehetőségeket keresnek.⁷⁷ Az internet felszíni része és a közösségi média helyett kénytelenek biztonságosabb és rejtettebb alternatívákat keresni.⁷⁸ Amiért a fő platformok, mint a Facebook, Twitter, YouTube és a Telegram egyre „barátságatlanabbak” voltak az ISIS-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.⁷⁹ Az Europol Szervezett bűnözés internetes fenyegetettségét (IOCTA) vizsgáló 2019-es éves jelentése szerint 2018 végén az ISIS-támogatók a Telegramon alternatív platformok és szoftverek használatát kezdték javasolni. Az ISIS ez után kiépítette a jelenlétét számos nyílt forráskódú (open source) decentralizált platformon. Főleg hivatalos ISIS-propagandát terjesztő felhasználói fiókokat és oldalakat hoztak létre a Mastodon, Nextcloud, Rocket.Chat and ZeroNet felületeken. Ezek a platformoknak az ellenálló volta, névtelensége és a sok felhasználási lehetőség előnyére válnak a terrorista csoportoknak az online kommunikáció és disztribúciós stratégia szempontjából. Ezek a platformokon a dzsihádisták aktivitás viszont 2018-ban nem tudott hűzóerővé válni, valószínűleg az alternatív platformok kisebb felhasználói bázisa és ezéért gyengébb tájékoztató képessége miatt. A Telegram maradt a terrorista szimpatizáló platformja.⁸⁰

Az ISIS-t 2019 márciusában a Szíriai Arab Köztársas-

⁷⁵ https://www.vice.com/en_us/article/a3mexp/neo-nazis-are-organizing-secretive-paramilitary-training-across-america (2020.08.18.)

⁷⁶ HAMMING, Tore Refslund: Global Jihadism after the Syria War. Perspectives On Terrorism, 2019. Vol. 13. No. 3. 11. o.

⁷⁷ ALKHOURI, Laith – KASSIRER, Alex: Tech for Jihad: Dissecting Jihadists’ Digital Toolbox. Flashpoint, USA 2016. 1. o.

⁷⁸ ÖZKAYA: i. m. 53. o.

⁷⁹ KATZ, Rita: A Growing Frontier For Terrorist Groups: Unsuspecting Chat Apps. https://www.wired.com/story/terrorist-groups-prey-on-unsuspecting-chat-apps/?fbclid=IwAR0rzGUvrw5SoMjy1_XGd-wHuTF6cgTGUrQlsWkpQr8_eZq_l6vSK0YKwCQ (2020.08.18.)

⁸⁰ Europol The Internet Organised Crime Threat Assessment. Europol, Hága, 2019. 49. o. <https://www.europol.europa.eu/iocta-report> (2020.08.18.)

⁷² https://www.vice.com/en_us/article/z3byxm/new-german-terror-cell-the-hard-core-wanted-to-attack-mosques-to-start-a-civil-war (2020.08.18.)

⁷³ BAUMGÄRTNER, Maik – HÖFNER, Roman – LEHBERGER, Roman: RechtsterrorismusMitgründer der „Feuerkrieg Division” gefasst. [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=\[sponsored\]&fbclid=IwAR01kQFV5avns0voCi1SCFXe_FipiYntLxMhRqg6hTJ3rTlO16NVNQP3A#ref=rss](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=[sponsored]&fbclid=IwAR01kQFV5avns0voCi1SCFXe_FipiYntLxMhRqg6hTJ3rTlO16NVNQP3A#ref=rss) (2020.08.18.)

⁷⁴ <https://www.bbc.com/news/world-51236915> (2020.08.18.)

ságban katonailag legyőzték.⁸¹ Bagúz elestével a földrajzi értelemben vett „kalifátusa” megszűnt létezni, és a terrorszervezet folytatta a főleg rejtett hálózatokba történő átalakulását.⁸²

Abu Bakr al-Baghdadi, az ISIS vezetője, 2019. október 26-án „felrobbantotta magát”, mikor az amerikai erők egy éjjeli rajtaütés során sarokba szorították Idlibben, Szíria északi részén.⁸³ Az USA védelmi minisztere szerint Baghdadi halála „egy pusztító csapást jelent az ISIS maradványai számára”.⁸⁴ Egy nappal később Abu Hassan al-Muhajirt, az ISIS szóvivőjét, akit Abu Bakr al-Baghdadi valószínű utódjának tartottak, egy amerikai légitámadás ölte meg.⁸⁵ Speckhard szerint a harcos dzsihadisták azt fogják gondolni, hogy Trump elnök leírásával szemben a vezetőjük „Allahu Akbar!” felkiáltással halt mártírhálál, és a paradicsomba jutott. Baghdadi a követőit ugyanerre szólította fel. „Mártírhálála” sok követőt fog inspirálni, és az nem jelenti az ISIS végét.⁸⁶

Telegram alternatívájaként az ISIS később is új és kisebb platformokkal kísérletezett. 2019. április 14-én a Nashir News Agency propagandaterjesztő csoport az új közösségimédia-oldalát promotálta a Koonecti nevű közösségimédia-platformon. 13 órán belül az oldal 28 lájkot kapott és ugyan megkapta a hitelesített státuszt, de pár órával később eltávolításra került. A Go Like platformot az ISIS hasonlóan sikertelenül tesztelte. A korábbi próbálkozásokat vizsgálva, egy minta ismerhető fel, mégpedig a kis és közepes méretű applikációk, platformok és szolgáltatások használata. Korábbi példák közé tartozik a Baaz, Viber, Kik, Ask, fm, Discord és más, köztük egy személy által működtetett mikroplatformok. Úgy tűnik a Telegram és bizonyos esetekben a kisebb platformok stabil alternatívájának bizonyult a decentralizált internet (decentralised web, DWeb), a jelenlegi world wide web alternatívája. Az ISIS DWeb platformokkal és applikációkkal is kísérletezik.

Bármely Telegram-alternatívának, beleértve a decentralizált internetszolgáltatásokat, specifikus jellemzőkkel kell bírnia, hogy azokat a terroristák széles körben adoptálják. A kisebb platformokkal való visszaélés sikere a következő tényezőkön múlik: 1. Biztonság: magas biztonsági standard (pl.: végpontok közötti titkosítás) az ISIS médiafelelősök és végfelhasz-

nálók műveleti biztonsága (operational security, OPSEC) növelése érdekében. 2. Stabilitás: milyen mértékben védettek az ISIS médiafelelősök és támogatói a platform tulajdonosa és/vagy harmadik személyek beavatkozásától (pl.: tartalom- és felhasználófiók-eltávolítás vagy D/Dos támadások). 3. Felhasználhatóság: mennyire könnyű az alkalmazásokat telepíteni, feliratkozni a platformokra és mennyire használhatók napi szinten. 4. Közönség elérésére való képesség: hány használó érhető el a platformmal vagy szolgáltatással. Amikor egy tech vagy közösségimédia-cég felméri a terroristák általi visszaéléssel való lehetőséget, ezeket a tényezőket számba kell venni. Az ISIS médiaszakértőinek megfigyelése elengedhetetlen fontosságú a támogatást igénylő platformok azonosításában. A megfigyelésbe bele kell tartoznia a szélesebb propagandaelosztó ökoszisztémának és a nagyobb és kisebb platformok közötti dinamikus és komplex interakciónak. A kutatás fókuszának inkább az elosztó-ökoszisztémára 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 diszkusszióknak ki kell terjednie a Dwebre és annak terroristák általi használatára. Egy sikeres fellépési műveletnek a rendszerelméletől tanuló bizonyítékokon alapuló kutatáson kell alapulnia. Bármilyen fellépésnek nem kívánt következményei is lehetnek, mint tömeges migráció a decentralizált internetre, amit nehezebb megérteni, befolyásolni és bomlasztani.⁸⁷

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 ISIS 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.⁸⁸ Az összehangolt akció fókuszában az online terrorista tartalmak terjesztése volt, különös tekintettel a propagandavideókra, publikációkra, valamint terrorizmust és erőszakos extrémizmust támogató közösségimédia-felhasználói fiókokra. 2015 júliusa óta az Europol szélsőséges internetes tartalmakkal foglalkozó egysége együttműködik a bűnüldöző szervekkel és az online szolgáltatást nyújtókkal a terroristák internettel való visszaélésének az EU Internet Forum keretirányelvben történő kezelése érdekében. Az elmúlt években az Europol együttműködött a Telegrammal a terroristák online aktivitása elleni fellépés érdekében. A Telegram komoly erőfeszítéseket tett a rossz szándékú tartalmak elleni fellépésre irányuló technikai képességeinek megerősíté-

⁸¹ S/2019/570 Twenty-fourth report of the Analytical Support and Sanctions Monitoring Team submitted pursuant to resolution 2368 (2017) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities. United Nations Security Council, 2019. 5. o.

⁸² Uo. 3. o.

⁸³ COHEN, Zachary: Inside the dramatic US military raid that killed ISIS leader Baghdadi. <https://edition.cnn.com/2019/10/27/politics/baghdadi-inside-the-raid-timeline/index.html> (2020.08.18.)

⁸⁴ BRITTON, Bianca: Baghdadi's death: More details emerge from US raid: Defense secretary: Baghdadi's death „marks a devastating blow for the remnants of ISIS”. <https://edition.cnn.com/politics/live-news/baghdadi-monday-dle-intl/index.html> (2020.08.18.)

⁸⁵ HUBBARD, Ben – SHOUMALI, Karam: Likely Successor to Dead ISIS Leader Also Reported Killed. <https://www.nytimes.com/2019/10/27/world/middleeast/al-baghdadi-successor-reported-killed.html> (2020.08.18.)

⁸⁶ SPECKHARD, Anne: Baghdadi Just Confirmed ISIS 'Martyrdom' Narrative, Ensuring ISIS Will Live. <https://www.icsve.org/baghdadi-just-confirmed-isis-martyrdom-narrative-ensuring-isis-will-live/> (2020.08.18.)

⁸⁷ <https://www.voxpol.eu/isis-use-of-smaller-platforms-and-the-dweb-to-share-terrorist-content/> (2020.08.18.)

⁸⁸ Referral Action Day against Islamic State online terrorist propaganda. <https://www.europol.europa.eu/newsroom/news/referral-action-day-against-islamic-state-online-terrorist-propaganda> (2020.08.18.)

sével, és azzal, hogy szoros partnerséget ápol nemzetközi szervezetekkel, mint az Europol.⁸⁹

Katz arra világít rá, hogy az ISIS-nek a Telegramról való eltávolítása után nincs fő otthona a weben. Így nehezebb online megtalálni, de a tagjainak is nehezebb egyesülni és toborozni. A Telegram eltávolító algoritmusa sokkal célzottabb volt, mint korábban bármikor. A korábbi eltávolító kampányok az ISIS-es felhasználók által használt csatornákra és chatcsoportokra fókuszáltak. Ezek után az ISIS számtalanszor visszatért, de most a platform a „felégetett föld” taktikát alkalmazva nemcsak a csatornákat, hanem a csatornák létrehozóit és használóit is törölte, támogatóktól a top médiafelelősökig. Sok tartalom 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 ISIS-t. A tagok elvesztették egymással a kapcsolatot, miközben az egész médiainfrastruktúra, amely olyan csoportok köré épült, mint a Nashir News, Fursan al-Rafa, és Invasion Brigades gyorsan szétesett. Az ISIS Telegramos jelenléte darabokra hullott, és a szervezet az interneten új otthon után nézett. Az ISIS első állomása a Riot, egy nyílt forráskódú üzenetküldő kliens volt, ahonnan egyszer már 2017 őszén gyorsan eltávolításra kerültek. Az ISIS által használt üzenetküldő platformok közül a Riot-hoz a legkönnyebb csatlakozni, ahhoz elég egy felhasználónév és jelszó. Csatlakozni lehet chatcsoportokhoz URL vagy meghívó nélkül is, ami sokkal hozzáférhetőbbé teszi a Telegramnál. Az ISIS hálózat részei hamarosan ellepték a Riotot chatszobákkal. Napokkal az után, hogy a Telegram elkezdte a tisztítást, az ISIS Riot fiókjai törlésre kerültek. Az ISIS-hez köthető csoportok ezután még hetekig hirdették a Riot szobáikat, de eltávolításuk folytatódott. Még mindig lehet találni sok ISIS-hez köthető szobát a Rioton, de a terroriszervezet hálózata, mint egész, más otthonra kerekedett és gyorsan talált is a TamTamot, ami a Telegramhoz hasonló üzenetküldő platform. A TamTamot is sikertelenül próbálta kihasználni 2018 tavaszán az ISIS. A platformon egyértelművé vált a friss jelenléte, mikor azon vállalta magára először a 2019. november 29-i London Bridge-nél történt késelést. December 1-re több száz nyilvános és privát ISIS-csatorna, -csoportok és -fiók lepte el a TamTamot, köztük a fő ISIS-hez köthető médiaegységek, mint a Halummu és Mutarjim. Az ISIS innen is hamarosan eltávolításra került. Egy nap alatt a fiókjainak a fele eltűnt. Az ISIS így járt más platformokon is. Ezek közé tartozik a kanadai Hoop Messenger, ami azonnal elkezdte a fiókok és csatornák eltávolítását (de úgy tűnik, az ISIS újakat hozott létre). Az ISIS megpróbált sikertelenül megtelepedni még kevésbé ismert közösségimédia-plat-

⁸⁹ Europol and Telegram take on terrorist propaganda online. <https://www.europol.europa.eu/newsroom/news/europol-and-telegram-take-terrorist-propaganda-online> (2020.08.18.)

formokon, mint az egyesült államokbeli MeWen, és egy nyílt forráskódú Twitter alternatíván, a német fejlesztésű Mastodonon. Ugyan az ISIS még mindig képes átcsúszni a Telegram néhány részén, mint jelöletlen csatornák és diszkrét felhasználói nevek használatával, de két számjegyű platformon szóródott szét, mely tendencia folytatódni fog a felkészült platformokon, melynek nagy jelentősége van. Katz szerint a széles körben használt platformokon lévő centralizált online menedékek az egyik legfontosabb változó volt az ISIS növekedésében és fenntartásában. Egy ilyen központ stabilitást ad az olyan szervezeteknek, mint az ISIS, a propaganda megbízható áramlását biztosítva, a hamis propaganda megjelölését lehetővé téve és a leendő regrutáknak a kapcsolatfelvételhez kijelölt helyszínt nyújtva. Korábban a terroriszervezet nyílt színen toborzott olyan platformokon, mint a Twitter. Ahogy a Twitter egyre keményebben lépett fel ellenük, 2015-ben a Telegramra váltottak, kihasználva annak lehetőségeit, a csatornákat, chatcsoportokat, médiaarchiválást és a végpontok közötti titkosítást. Katz szerint ugyan az olyan technológiákról, mint a dark web, gyakran azt gondolják, megfelelnek az ISIS biztonsági igényeinek, azok nagyrészt alkalmatlanok a közönség eléréséhez, mivel az ISIS-nek ott kell lennie, ahol a felhasználók már jelen vannak, különben csak „magához beszél egy üres szobában”. A kutatók feladatát nehezíti az ISIS platformról platformra való ugrálása, de a leendő újoncoknak is nehezebb annak online tartózkodási helyét megtalálni. Az ISIS sokáig nem fog eltűnni, de Katz szerint kritikus csapás érte, mely tendenciának folytatódnia kell.⁹⁰ Egy ISIS támogató egy kutatók által, a Hoop és TamTam platformokról a tartalmaik eltávolításáról közzétett tweetet osztott meg a Twitteren, 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.”) Más szavakkal, miközben a kutatók a bomlasztásukról beszélnek, ők mulatnak rajta, hogy bizonytalanságban tartják az ellenük küzdőket.⁹¹ Mivel az ISIS nem talál online otthonra, erre a célra létrehozhat egy saját alkalmazást.⁹²

3.2. Az ISIS Facebookon használt eltávolítást megkerülő taktikái

Az utóbbi két évben a Facebook átláthatósági jelentése (transparency reporting) azt mutatja, hogy a cég a terrorizmushoz kötődő posztok 99%-át, kb. 26 millió tar-

⁹⁰ KATZ, Rita: ISIS Is Now Harder to Track Online – but That's Good News. <https://www.wired.com/story/opinion-isis-is-now-harder-to-track-online-but-thats-good-news/> (2020.08.18.)

⁹¹ <https://www.voxpol.eu/telegram-deplatforming-isis-has-given-them-something-to-fight-for/> (2020.08.18.)

⁹² GILBERT, David: Islamic State Can't Find an Online Home – So They Might Build Their Own App. https://www.vice.com/en_ca/article/d3ane7/islamic-state-cant-find-an-online-home-so-they-might-build-their-own-app (2020.08.18.)

talimat felfedez és eltávolítja, még mielőtt azokat jelenéne. Az Institute for Strategic Dialogue (ISD) a The Propaganda Pipeline: The ISIS Fuouaris Upload Network on Facebook című publikációban egy ISIS-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 célja terrorista tartalom terjesztése a platformon. Az ISD kvalitatív kutatása ennek az ökoszisztémának csak a felszínét kaparta, példát nyújtva arról, milyen betekintés nyerhető manuális nyomozás során. Hogy érthető legyen a kihívás valódi mértéke és természete, egy ilyen analízist automatizáltan kell végezni. Az ISD kutatása 2020. április 7-től július 30-ig, azaz 87 napon át tartott, mely során a platformon egy magát Fuouaris Uploadnak nevező ISIS-támogató Facebook fiókok hálózatát követte, analizálta és elemezte annak viselkedését. A megfigyelés során 288 ISIS-támogatói 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 SoundCloudon jelenleg 18 branddel ellátott fiókot kontrollál, melyek 91 ISIS audiotartalmat tettek közzé. Ugyan a Fuouaris Upload fiókok 70%-a a megfigyelési időtartam alatt eltávolításra került, ezek a decentralizált hálózatok komoly szívósságról tettek tanúbizonyságot. 62 fiók került eltávolításra a fő fiókok közül, de 28 ugyanilyen fiók megmaradt, mely a moderáció egyenetlenségét mutatja. Ahogy az egyes fiókok eltávolításra kerültek, az ISIS-es felhasználók gúnyolták a Facebook moderátorait azért, mert nem értik a platformon való jelenlétük mértékét.⁹³ A kutatás az ISIS-támogatók által használt elkerülésre szolgáló új taktikákra mutat rá, melyek az automatizált vagy manuális felfedezés és a terrorista tartalmak és felhasználói fiókok moderálásának akadályozását célozzák. A kutatás 6 fő taktikát azonosított: 1. Felhasználói fiók eltérítése: Az ISIS-támogatók a Facebook egyik fő kiskapujával visszaélve két alkalmazással eltérítik más felhasználók fiókjait. A két alkalmazás lehetővé teszi a platform által küldött jelszó-helyreállítási üzenet elfogását. Több felhasználói fiók oktatóvideókat gyártott és osztott meg a módszerről. 2. Tartalom elfedése: A Facebookon az ISIS-tartalmak túlélése kozmetikai módosításokra támaszkodik. Ezek közé tartoznak videóeffektek, melyek népszerű hírcsatornák (pl.: France24 és BBC) megjelölését helyezik hivatalos ISIS-propagandára, és a nyilvánvaló ISIS-ikonográfiát homályosítják el. Az ilyen tartalmak megkerülnek a Facebook terrorista anyagok automatizált felfedezésére szolgáló hashing technológiáját, ami úgy

látszik, nem képes az enyhén szerkesztett hivatalos terrorista média felismerésére. 3. Linkmegosztás: Az ISIS támogatók decentralizált hálózatai kommentszekciókat használnak ismert dzsihádista oldalakhoz vezető linkek megosztására. 4. Koordinált ún. „raid-ek” (rajtaütés, továbbiakban raid): Az ISIS támogatók hálózatai a Facebookon szervezett raideket terveznek, készítenek elő és hajtanak végre más Facebook-oldalak, köztük a US Department of Defence, US Army, a US Air Force Academy és Trump elnök 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 polarizáció generálása. ISIS-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 ISIS-támogató fiókok taktikájára emlékeztet, akik a megosztó társadalmi problémák körüli online dikszurzus eltérítését célozták és propagandát terjesztettek népszerű hashtagek használatával. 6. Szöveganalízis kijátszása/Gaming Text Analysis: Szöveganalízis moderálás megkerülése ún. „broken text” (szándékosan hibás szöveg) formátum vagy specializált betűtípus használatával a posztokban.⁹⁴

4. A koronavírus pandémia hatása a terrorizmusra és a terroristák internethasználatára

4.1. Erősödő online aktivitás és fokozott sebezhetőség a radikalizációval szemben

Ambrus rámutat arra, hogy amíg nem lesz vakcina a WHO által 2020. március 11-én pandémiának/világjárványnak nyilvánított⁹⁵ koronavírus (COVID-19) szemben, a rendkívüli helyzet tovább fog tartani, mely várhatóan gazdasági recessziót jelent, ami például számos munkahely megszűnése miatt kriminogén hatással is járhat, ezért nem kizárható, hogy az egész világot érintő válság miatt fokozódni fog a bűncselekmények száma.⁹⁶ Gál a koronavírus nyomán kibontakozó gazdasági világválsággal kapcsolatban a következő megállapításokat teszi: „1. a koronavírus feltételezhetően több halálos áldozatot fog követelni világszerte, mint a nemzetközi terrorizmus eddig összesen a világtör-

⁹³ 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>) (2020.08.18.)

⁹⁴ Uo. 2–4. o.

⁹⁵ <https://www.who.int/emergencies/diseases/novel-coronavirus-2019/events-as-they-happen> (2020.08.18.)

⁹⁶ AMBRUS István: A koronavírus-járvány és a büntetőjog MTA Law Working Papers 2020/5, Budapest, 2020. 22. o.

tételemben, 2. de az is előfordulhat, 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.”⁹⁷ Gál hipotézise alapján 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 az, hogyan lassítható és mérsékelhető.⁹⁸ A legfrissebb adatok Gált⁹⁹ igazolják: 2020-ban jelentősen nőtt az emberölések száma Magyarországon.¹⁰⁰ A koronavírus egyik hatásaként fokozódik a cyber-enabled crime (kapcsolódó kibercselekmények¹⁰¹ vagy kibertér által elősegített bűnözés¹⁰²), a terrorizmus és az információs hadviselés (például dezinformációs kampányok és álhírek terjesztése).¹⁰³ Rövid távon a zárlati (lockdown) intézkedések visszafogják a terrortámadásokat, de az azok elkövetésére felhívó propaganda ösztönözni fog néhány incidenst. Sok – kifejezetten szélsőjobboldali extrémista – propaganda a koronavírushoz kapcsolódó összeesküvés-elméletekre fókuszál, és ezek már inspiráltak terveket és elkövetéseket. Az iszlamista extrémista propaganda inkább a pandémiával elfoglalt ellenséges kormányok sebezhetőségére koncentrálnak, és arra, hogy ez lehetőséget ad terrortámadásokra. Az online extrémista aktivitást illetően jelentős fokozódás tapasztalható, ami a rövid és középtávon a radikalizáció kockázatát növeli. Hosszú távon erősen aggasztó, hogy a pandémia gazdasági következményei miatt meggyengült államok sebezhetőbbek lesznek a terrorista csoportokkal szemben.¹⁰⁴ A terroristák tudják, hogy emberek milliói otthon kényszerülnek maradni, ezért több időt töltenek online és a közösségi médián. Dzsihadisták szokása, hogy bármely ellenségüket érintő természeti csapásról azt állítják, hogy Isten akarata és hogy az lehetőség támadások elkövetésére. Az al-Kaida és az ISIS is fokozta a propagandáját, köztük apokaliptikus YouTube-videókkal, melyek a zsidókat vagy Amerikát okolják a COVID-19 miatt. Miközben mindkét terror-szervezet szerint a COVID-19 Isten haragja a nyugat ellen, az üzeneteik eltérnek. Az al-Kaida propaganda

szárnya, az As-Sahab rávilágított az amerikai gazdaságra gyakorolt káros hatásokra, ami hosszú távú kampánycél, de a nyugatiakat arra sűrgette, hogy használják ki az időt az iszlam tanulmányozására és térjenek át. Néhány más iszlamista csoporttal együtt az al-Kaida ténylegesen promotált módokat a vírus terjedésének visszafogására. Az ISIS médiacsoportjai, mint a Ribat és Murhafat erősebbek és hajthatatlanok voltak, támadásokra felszólítva.¹⁰⁵

Az ISIS a hivatalos al-Naba hírlevelében egész oldalas infografikát közölt a COVID-19 fertőzés megakadályozásáról. Az ISIS a hírleveleiben január óta figyelemmel kísérte a koronavírus, rendszeresen tájékoztatva róla. „Egy új vírus terjeszt halált és rettegést Kínában”, írta az al-Naba januárban. Ahogy a vírus terjedt, az ISIS egyre jobban kritizálta a kínai kormányt, amiért titkolta a járvány valódi mértékét. Az ISIS szerint a járvány Isten büntetése, amiért Kína sanyargatja az ujur népeket. Az ISIS azt tanácsolja, hogy „helyezték a hitet Istenbe és keressetek Benne menedéket a betegségektől” és „az egészségesek ne lépjenek a járvány földjére, és az az által sújtottak ne távozzanak onnan”. (Az ISIS ehhez képest hajt végre műveleteket Algériában, Egyiptomban, Irakban, Afganisztánban, Indiában, a Fülöp-szigeteken és Indonéziában, ahol vannak igazolt esetek.) Az ISIS szorgalmazza a kézmosást, és azt tanácsolja, hogy „ásításkor és tüsszentéskor takard el a szádát”. Az al-Naba szerint a koronavírus „további nyomást és terhet” ró a kormányokra, csökkenti azok együttműködési képességeit a terrorizmus elleni harc terén és biztonsági szempontból olyan részt jelent, amit szerinte ki kell használni „a párizsi, londoni, brüsszeli és más csapásokhoz hasonló” terrorcselekmények elkövetéséhez, a foglyok kiszabadításához.¹⁰⁶

A szélsőjobboldali csoportok aktívak online az összeesküvés-elméletek, a dezinformáció, kisebbségek, kritikus infrastruktúra és Szövetségi Válságkezelési Ügynökség elleni erőszak promotálása terén. Betiltott csoportok a rendőrség és a zsidó közösség elleni támadásokra szólítottak fel. A célpontok és támadási módszerek azonosítása terén a szélsőjobboldali chatcsoportok még tovább is mentek a szalafista dzsihadista csoportoknál. Technikáik közé tartozik a testnedvekkel teli spray, a vírus terjesztése köhögéssel, vagy felületek érintése üzletekben, tömegközlekedésen. A szélsőjobboldali extrémisták kifejezetten aktívak a közösségi médián, élükön az „akcelerationistákkal” („accelerationists”) akik úgy vélik, az erőszakos cselekedetek felgyorsíthatják az általuk globálisan összekapcsoltnak és degeneráltnak tartott társadalom el-

⁹⁷ GÁL István László: A koronavírus (COVID-19) és az általa okozott gazdasági világválság lehetséges hatásai a bűnözésre. Magyar Jog, 2020. 45. évf. 5. sz. 258. o.

⁹⁸ Uo. 258. o.

⁹⁹ Lásd továbbá: Gál István László: A spanyolnátha, a koronavírus és a büntetőjog. Büntetőjogi Szemle, 2020. 9. évf. 1. sz. 57–64. o.

¹⁰⁰ https://qubit.hu/2020/07/22/2020-ban-jelentosen-megnott-az-emberolek-szama-magyarorszagon?_ga=2.90202842.1187097502.1593935711-1665391435.1543668993&fbclid=IwAR1xyR4C2eMUqgh-zUX6gqR0wPxDiYqHDjive3Xp5kHPDVpUEwhQ8ra_7Sk (2020.08.18.)

¹⁰¹ MÁTÉ István Zsolt: Informatikai rendszerek elleni támadások szakértői vizsgálata – a digitális nyomok rögzítésének szerepe. Belügyi Szemle, 2018. 66. évf. 7–8. sz. 38. o.

¹⁰² VARGA Árpád: Az informatikai bűnözés fogalmi meghatározása, csoportosítása és helye a hazai jogfejlődésben. In Medias Res, 2019. 8. évf. 1. sz. 151. o.

¹⁰³ GRADOŃ, Kacper. Crime in the time of the plague: fake news pandemic and the challenges to law-enforcement and intelligence community. Society Register, 2020. 4. évf. 2. sz. 134. o.

¹⁰⁴ SILKE, Andrew: COVID-19 and terrorism: assessing the short-and long-term impacts. Cranfield: Pool Re Solutions, 2020. 2. o.

¹⁰⁵ WITHER, James K.: The COVID-19 Pandemic: A Preliminary Assessment of the Impact on Terrorism in Western States. Occasional Paper Series, 2020. 33. sz. 3–4. o. <https://www.marshallcenter.org/en/publications/occasional-papers/covid-19-pandemic-preliminary-assessment> (2020.08.18.) 2–3. o.

¹⁰⁶ JOHNSON, Bridget: ISIS: Cities Distracted by Coronavirus Should be Hit with Attacks Like Paris, London, Brussels. <https://www.hstoday.us/subject-matter-areas/counterterrorism/isis-cities-distracted-by-coronavirus-should-be-hit-with-attacks-like-paris-london-brussels/> (2020.08.18.)

kerülhetetlen összeomlását.¹⁰⁷ A Telegramon, Gabon, és chan fórumokon, továbbá a mainstreamebb platformokon, mint az Instagram, a Facebook és a Twitter szélsőjobboldali csoportok és egyének öszeesküvés-elméleteket terjesztenek, dezinformációval fokozzák a pánikot és az elégedetlenséget, és támadásokra szólítanak fel – közvetlen erőszakra, vagy a vírus biológiai fegyverként való használatára.¹⁰⁸ 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 kisebbségre.” Egy másik kritikus infrastruktúra elleni támadásra buzdít: „Köhögj a helyi tömegközlekedéseden.”¹⁰⁹ A mainstream közösségimédia-cégek már gyakorlatilag az egyértelműen terrorizmushoz fűződő tartalmak eltávolításában, és jelenleg együtt dolgoznak a pandémiához fűződő dezinformáció elleni harcon,¹¹⁰ de az extrémisták kihasználják a közegészségügyi dezinformáció szűrkezőnáját, amit nem fednek le a közösségi média korlátozásai.¹¹¹

2020. április 1-én egy oldal felhasználói egy philadelphiai zsidó iskola tanulóinak Zoom órát antiszemita zaklatásért tervezték, Zoom linkeket és az online órák órarendjét feltöltve, és másokat az ebben való részvételre bátorítottak. Ahogy több a virtuális meeting, a szélsőjobboldali extrémisták alkalmazkodnak a megfélemlítő és zaklató kampányaikkal azok környezetéhez.

2020. március 30-án egy akceleracionista/accelerationist Telegram csatorna linkeket osztott meg, instrukciókhoz arról, hogyan kell pisztolyt készíteni 3D nyomtatással létrehozott alkatrészekkel.¹¹²

A koronavírus pandémia alatti „social distancing” során az izolált embereknek sokkal több a szabadideje, és sebezhetőbbek a radikalizációval szemben, mikor a félelem idején válaszokat keresnek és eközben extrémista és terrorista csoportok online anyagaihoz fordulhatnak.¹¹³ A „Self-Isolation” gyorsítja az extrémizmus terjedését. Otthon rekedt milliók fordulnak

közösségi média felé. Egy megoldás lehetne egy „misinformation flag” a YouTube-on és Facebookon, amivel a helytelen vagy káros tartalmak megjelölhetőek lennének, továbbá ellennarratívák is használhatóak extrémista tartalmak ellen. Csak a közösségimédia-cégek általi meggondolt, koordinált és proaktív válasszal lehet a dezinformációval szemben fellépni.¹¹⁴

4.2. A koronavírus hatása a terrorizmus finanszírozására és annak online aspektusaira

A FATF a következő megállapításokat teszi: A COVID-19-hez fűződő olyan bűncselekmények növekedése, mint a csalás, kiberbűnözés, állami támogatások vagy nemzetközi pénzügyi támogatás hűtlen kezelése vagy elsikkasztása, a bűnözők számára új bevételi forrásokat generál. A COVID-19 megfékezésére szolgáló intézkedések a bűnözői gazdaságra hatással vannak és változtatják a bűnözői viselkedést, úgy, hogy a profitorientált bűnözők más illegális cselekedetek felé fordulhatnak. A COVID-19 pandémia a kormányok és a magánszektor pénzmosás¹¹⁵ és terrorizmus finanszírozás¹¹⁶ elleni (AML/CFT) kötelezettségeinek¹¹⁷ végrehajtási képességére is hatással van: a felügyeletre, szabályozásra, eljárási reformokra, a gyanús tranzakciók jelentésére és a nemzetközi kooperációra. Ezek a fenyegetések és sebezhetőségek fokozódó pénzmosási és terrorizmusfinanszírozási kockázatot képviselnek. Ezek a kockázatok a következő eredményekkel járhatnak: A bűnözők megtalálhatják az ügyfél-átvilágítási eljárások megkerülésének módjait. Fokozódhat a visszaélés az online pénzügyi szolgáltatásokkal és virtuális eszközökkel illegális összegek mozgatására és elrejtésére. Előfordulhat visszaélés a gazdasági stimulus intézkedésekkel és csődbűncselekmény, mint módok a természetes és jogi személyek számára, illegális jövedelmek elrejtésére és mosására. Növekedhet a nem szabályozott pénzügyi szektor használata, további lehetőséget adva bűnözőknek az illegális összegek mosására. Előfordulhat a hazai és nemzetközi pénzügyi támogatások és rendkívüli segélylappal való visszaélés és annak hűtlen kezelése. Bűnözők és terroristák kihasználják a COVID-19-et és az ahhoz kapcsolódó gazdasági recessziót, hogy új készpénzintenzív és magas likviditású üzletágak felé mozdul-

¹⁰⁷ WITHER: i. m. 3–4. o.

¹⁰⁸ KATZ, Rita: The Far-Right's Online Discourse on COVID-19 Pandemic. https://ent.siteintelgroup.com/index.php?option=com_acymailing&ctrl=archive&task=view&mailid=20576&key=4lfGcEyn&subid=1472-t9ir9gm3ghmVr7&tmpl=component (2020.08.18.)

¹⁰⁹ WEIMANN, Gabriel – MASRI, Natalie: The Virus of Hate: Far Right in Cyberspace. International Institute for Counter Terrorism, 2020, 12. o. <https://www.ict.org.il/images/Dark%20Hate.pdf>. (2020.08.18.)

¹¹⁰ EAS Special Report, COVID-19 Disinformation. 2020. <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>. (2020.08.18.) Idézi: Wither: i. m. 3–4. o.

¹¹¹ MALIK, Nikita: Self-Isolation Might Stop Coronavirus, but It Will Speed the Spread of Extremism. <https://foreignpolicy.com/2020/03/26/self-isolation-might-stop-coronavirus-but-spread-extremism/>. (2020.08.18.) Idézi: Wither: i. m. 3–4. o.

¹¹² <https://www.counterextremism.com/press/extremist-content-online-extremists-plot-anti-semitic-harassment-campaign-targeting> (2020.08.18.)

¹¹³ SIMONS, Greg – BIANCA, Cristina: The Specter of Terrorism During the Coronavirus Pandemic. 2. o. <https://www.e-ir.info/2020/05/08/the-specter-of-terrorism-during-the-coronavirus-pandemic/> (2020.08.18.)

¹¹⁴ MALIK: i. m.

¹¹⁵ A pénzmosás szabályozásának irányairól bővebben: Gál István László: A pénzmosás szabályozásának régi és új irányai a nemzetközi jogban és az EU-jogban. Európai Jog: Az Európai Jogakadémia Folyóirata, 2007. 7. évf. 1. sz. 12–23. o.; A pénzmosás technikáról lásd: Gál István László: The Techniques of Money Laundering In: Gál István László – Köhalmi László (szerk.): Em-lékkönyv Losonczy István professzor halálának 25. évfordulójára. Pécsi Tudományegyetem, Állam- és Jogtudományi Kar, Pécs 2005. 129–138. o.

¹¹⁶ GÁL István László: A terrorizmus finanszírozása: Die Terrorismusfinanzierung. Pécs, PTE Állam- és Jogtudományi Kar Gazdasági Büntetőjogi Kutatóintézet, Pécs 2010.

¹¹⁷ A pénzmosásra vonatkozó regulációt soha nem volt egyszerű alkalmazni és analizálni. Lásd: Gál István László – Tóth Mihály: The Fight against Money Laundering in Hungary. JOURNAL OF MONEY LAUNDERING CONTROL, 2004. Vol. 8. No. 2. 190. o.

janak el fejlődő országokban. AML/CFT regulációs válszok segíthetnek a COVID-19 elleni intézkedések gyors és hatékony végrehajtásában. Ezek közé tartoznak: Hazai koordináció a COVID-19-nek az AML/CFT kockázatokra és rendszerekre való hatásának felmérése érdekében. Megerősített kommunikáció a privát szektorral. Az ügyfél-átvilágítási eljárások tekintetében ösztönzés a kockázatalapú megközelítés teljes használatára. Elektronikus és digitális fizetési lehetőségek támogatása.¹¹⁸

5. A jövő – terror deep fake használatával?

Clarke szerint ugyan a mesterséges intelligencia és a gépi tanulás a nem állami szereplők számára nehezebben megközelíthető, a dezinformáció és a „deep fake-ek” új és összetett kihívásokat állítanak a terrorizmus elleni harc szereplői elé.¹¹⁹ A deep fake kifejezés a „Deep Learning” és „Fake” szavak kombinációjából¹²⁰ 2017-ben jelent meg mesterséges intelligencia (MI) technológiákkal generált realiztikus fotó, audio, videó és más hamisítványok leírására.¹²¹ Ez a technika felhasználható a célszemély arcképeinek vagy arcmozgásainak egy forrásszemélyről készült videóra való ráhelyezésére, abból a célból, hogy olyan videót hozzanak létre, amiben a célszemély úgy viselkedik, ahogy a forrásszemély. A létrejött hamisítvány gyakran jóformán megkülönböztethetetlen az eredetitől.¹²² Ezen hamisítványok ártó szándékkal való használatának csak az emberi fantázia szab határt.

Caldwell, Andrews, Tanay és Griffin a mesterséges intelligencia és az ahhoz fűződő technológiák bűncselekmények elkövetésében való lehetséges alkalmazásait azonosították, és osztályozták a fenyegetési szintjük alapján.¹²³ 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 hírek.¹²⁴

¹¹⁸ 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> (2020.08.18.)

¹¹⁹ CLARKE, Colin P.: Trends in Terrorism: What's On the Horizon in 2020. <https://www.fpri.org/article/2020/01/trends-in-terrorism-whats-on-the-horizon-in-2020/> (2020.08.18.)

¹²⁰ HAN, Yufei: Deepfakes: A Terror in the era of AI? <https://www.nortonlifelock.com/blogs/research-group/deepfakes-terror-era-ai> (2020.08.18.)

¹²¹ Deep Fakes and National Security. <https://fas.org/sgp/crs/natsec/IF11333.pdf> (2020.08.18.)

¹²² HAN: i. m.

¹²³ CALDWELL, M. – ANDREWS, J. T. A. – TANAY, T. – GRIFFIN, L. D.: AI-enabled future crime. *Crime Science*, 2020. No. 9. 1. o.

¹²⁴ Uo. 6–9. o.

Összegzés

Egyetértek Boross-sal, hogy az extrémizmus elleni fellépés alapvető nemzetbiztonsági feladat.¹²⁵ Az internet használható kommunikációs csatornaként a rendvédelmi szervek számára is. A radikalizálódó hírportálok, fórumoldalakon rövid tanulmányokkal, hozzászólásokkal mintegy moderálni, a szélsőséges, befolyásoló propagandát, lejártni, kiszorítani is lehet, amihez képzett, motivált állomány szükséges.¹²⁶ Egyetértek Kis-Benedekkel és Kenedlivel, hogy a terrorizmus propagandájával szembeni fellépés fontos, különösen az online terjesztett tanok, toborzó videók felkutatása, az eredetük megállapítása és azok eltávolítása is szükséges, ezzel megóva azokat, akik magukban hordozzák a radikalizálódás lehetőségét.¹²⁷ Az interneten egyértelműen megfigyelhető a szélsőjobboldali terrorista és extrémista aktivitás megerősödése. Úgy vélem, a terroristák internetes tevékenységeinek vizsgálata során nem szabadna kizárólag a dzsihádistá terroristák tevékenységére koncentrálni, a kutatás során nagyobb hangsúlyt kellene fektetni minden más típusú, főleg a szélsőjobboldali terroristák internethasználatának vizsgálatára is.

A koronavírus pandémia miatt a sok otthon maradt egyén fokozott internethasználata és bizonytalansága, esetleg az államban meggyengült hite, és emiatt az extrémista ideákra való fokozott fogékonysága miatt nagyobb kockázatot jelent a terroristák online anyagainak radikalizáló képessége, mint valaha,¹²⁸ ami a terrorizmus elleni harc szereplőinek éber figyelmét igényli. Véleményem szerint ezért soha nem volt ennyire fontos a terroristák internetes aktivitásának és annak legfrissebb tendenciáinak megfigyelése és kutatása, mint napjainkban, melynek során a nyomozó hatóságokra és titkosszolgálatokra kitüntetett szerep hárul.

Irodalomjegyzék

- 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> (2020.08.18.)
- AMBRUS István: A koronavírus-járvány és a büntetőjog MTA Law Working Papers 2020/5, Budapest, 2020. 22. o.
- AMEND, Alex: Analyzing a terrorist's social media

¹²⁵ BOROSS Zsigmond Attila: Humán faktor (Az emberi tényező szerepe az extrémizmus-elhárítás kérdéskörében). *Nemzetbiztonsági Szemle*, 2014. 2. évf. 2. sz. 139. o.

¹²⁶ Uo. 156. o.

¹²⁷ KIS-BENEDEK József – KENEDLI Tamás: A terrorfenyegetettség új tendenciái és lehetséges válaszlelések. *Szakmai Szemle*, 2015. 1. sz. 31. o.

¹²⁸ SIMONS-BIANCA: i. m. 2. o.

- manifesto: the Pittsburgh synagogue shooter's posts on Gab. <https://www.splcenter.org/hatewatch/2018/10/28/analyzing-terrorists-social-media-manifesto-pittsburgh-synagogue-shooters-posts-gab> (2020.08.18.)
- 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.
 - 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. 17. o.
 - 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>) (2020.08.18.)
 - BÁNYÁSZ Péter: Kiberbűnözés és közösségi média. *Nemzetbiztonsági Szemle*, 2017. 5. évf. 4. sz. 71. 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.
 - BAUMGÄRTNER, Maik – HÖFNER, Roman – LEHBERGER, Roman: RechtsterrorismusMitgründer der „Feuerkrieg Division“ gefasst.
 - [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=IwAR01kQfV5avns0voCiIISCFXe_FipiYntLxMhRqg6hTJ3rTIOLI6NVNQp3A#ref=rss](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=IwAR01kQfV5avns0voCiIISCFXe_FipiYntLxMhRqg6hTJ3rTIOLI6NVNQp3A#ref=rss) (2020.08.18.)
 - BOROSS Zsigmond Attila: A jobboldali extrémizmus összetett ideológiája – mint a terrorizmus potenciális hivatkozása – *TERROR & ELHÁRÍTÁS*, 2017. 4. sz. 23–48. o.
 - BOROSS Zsigmond Attila: Humán faktor (Az emberi tényező szerepe az extrémizmus-elhárítás kérdéskörében). *Nemzetbiztonsági Szemle*. 2014. 2. évf. 2. sz. 139. o.
 - BÓCZNÉ NEPARÁCZKI Anna Viktória: A kiberterrorizmus büntető anyagi jogi megítélése. *Ügyészek Lapja*, 2020. 27. évf. 1. sz. 76–77. o.
 - BRITTON, Bianca: Baghdadi's death: More details emerge from US raid: Defense secretary: Baghdadi's death „marks a devastating blow for the remnants of ISIS”.
 - <https://edition.cnn.com/politics/live-news/baghdadi-monday-dle-intl/index.html> (2020.08.18.)
 - 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. No. 9. 1. o.
 - ÇELIKSOY, Ergül – OUMA, Smith: Terrorist Use Of The Internet. *Bilişim Hukuku Dergisi*, 2019. Vol. 1. No. 2. 250–252. o.
 - Charles CROTHERS – Thomas O'BRIEN: The Contexts of the Christchurch terror attacks: social science perspectives, *Kōtuitui: New Zealand Journal of Social Sciences Online*, 2020. 15. évf. 2. sz. 248. o.
 - CLARKE, Colin P.: Trends in Terrorism: What's On the Horizon in 2020.
 - <https://www.fpri.org/article/2020/01/trends-in-terrorism-whats-on-the-horizon-in-2020/> (2020.08.18.)
 - COHEN, Zachary: Inside the dramatic US military raid that killed ISIS leader Baghdadi. <https://edition.cnn.com/2019/10/27/politics/baghdadi-inside-the-raid-timeline/index.html> (2020.08.18.)
 - CONWAY, Maura: Determining the Role of the Internet in Violent Extremism and Terrorism: Six Suggestions for Progressing Research. *Studies in Conflict & Terrorism*, 2017. 40. évf. 11. sz. 91. o.
 - CONWAY, Maura: Routing the Extreme Right. *The RUSI Journal*, 2020. 1. o.
 - 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> (2020.08.18.)
 - CRAWFORD, Blyth: Chan Culture and Violent Extremism.
 - <https://gnet-research.org/2019/12/31/chan-culture-and-violent-extremism-past-present-and-future/> (2020.08.18.)
 - CRAWFORD, Blyth – KEEN, Florence: The Hanau Terrorist Attack: How Race Hate and Conspiracy Theories Are Fueling Global Far-Right Violence. *CTC Sentinel*, 2020. 13. évf. 3. sz. 1. o.
 - Deep Fakes and National Security. <https://fas.org/sgp/crs/natsec/IF11333.pdf> (2020.08.18.)
 - DORNFIELD 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.
 - EAS Special Report, COVID-19 Disinformation. 2020. <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>. (2020.08.18.)
 - Europol's 2015 EU Terrorism Situation and Trend Report (TE-SAT)
 - Europol's 2016 EU Terrorism Situation and Trend Report (TE-SAT)
 - Europol's 2017 EU Terrorism Situation and Trend Report (TE-SAT)
 - Europol's 2018 EU Terrorism Situation and Trend Report (TE-SAT)
 - Europol's 2019 EU Terrorism Situation and Trend Report (TE-SAT)

- Europol's 2020 EU Terrorism Situation and Trend Report (TE-SAT)
- Europol and Telegram take on terrorist propaganda online.
- <https://www.europol.europa.eu/newsroom/news/europol-and-telegram-take-terrorist-propaganda-online> (2020.08.18.)
- Europol The Internet Organised Crime Threat Assessment, Europol, Hága, 2019. 48. o. <https://www.europol.europa.eu/iocta-report> (2020.08.18.)
- EVANS, Robert: Ignore The Poway Synagogue Shooter's Manifesto: Pay Attention To 8chan's (pol) Board. <https://www.bellingcat.com/news/americas/2019/04/28/ignore-the-poway-synagogue-shooters-manifesto-pay-attention-to-8chans-pol-board/> (2020.08.18.)
- EVANS, Robert: The El Paso Shooting and the Gamification of Terror
- <https://www.bellingcat.com/news/americas/2019/08/04/the-el-paso-shooting-and-the-gamification-of-terror/> (2020.08.18.)
- FANUSIE, Yaya: Hamas Military Wing Crowdfunding Bitcoin.
- <https://www.forbes.com/sites/yayafanusie/2019/02/04/hamas-military-wing-crowdfunding-bitcoin/#306575c34d7f> (2020.08.18.)
- FISHMAN, Brian: Crossroads: Counter-terrorism and the Internet. Texas National Security Review, 2019. Vol. 2. No. 2. 84–86. o.
- François THÉRON: Terrorist content online: Tackling online terrorist propaganda. 2020. 2-3. o.
- [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/649326/EPRS_BRI\(2020\)_649326_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/649326/EPRS_BRI(2020)_649326_EN.pdf) (2020.08.18.)
- GÁL István László: A pénzmosás szabályozásának régi és új irányai a nemzetközi jogban és az EU-jogban. Európai Jog: Az Európai Jogakadémia Folyóirata, 2007. 7. évf. 1. sz. 12–23. o.
- GÁL István László: A terrorizmus finanszírozása: Die Terrorismusfinanzierung. Pécs, PTE Állam- és Jogtudományi Kar Gazdasági Büntetőjogi Kutatóintézet, Pécs, 2010.
- GÁL István László: Új biztonságpolitikai kihívás a XXI. században: a terrorizmus finanszírozása. Szakmai Szemle: A Katonai Nemzetbiztonsági Szolgálat kiadványa, 2012. 8. évf. 1. sz. 15. o.
- GÁL István László: The Techniques of Money Laundering In: Gál István László – Kóhalmi László (szerk.): Emlékkönyv Losonczy István professzor halálának 25. évfordulójára. Pécsi Tudományegyetem, Állam- és Jogtudományi Kar, Pécs 2005. 129–138. o.
- GÁL István László: A koronavírus (COVID-19) és az általa okozott gazdasági világválság lehetséges hatásai a bűnözésre. Magyar Jog, 2020. 45. évf. 5. sz. 258. o.
- GÁL István László: A spanyolnátha, a koronavírus és a büntetőjog. Büntetőjogi Szemle, 2020. 9. évf. 1. sz. 57–64. o.
- GÁL István László – Tóth Mihály: The Fight against Money Laundering in Hungary. JOURNAL OF MONEY LAUNDERING CONTROL, 2004. Vol. 8. No. 2. 190. o.
- GILBERT, David: Islamic State Can't Find an Online Home – So They Might Build Their Own App. https://www.vice.com/en_ca/article/d3ane7/islamic-state-cant-find-an-online-home-so-they-might-build-their-own-app (2020.08.18.)
- GLASER, April: Where 8channers Went After 8chan
- <https://slate.com/technology/2019/11/8chan-8kun-white-supremacists-telegram-discord-facebook.html> (2020.08.18.)
- GRADOŃ, Kacper. Crime in the time of the plague: fake news pandemic and the challenges to law-enforcement and intelligence community. Society Register, 2020. 4. évf. 2. sz. 134. o.
- HAMMING, Tore Refslund: Global Jihadism after the Syria War. Perspectives On Terrorism, 2019. Vol. 13. No. 3. 11. o.
- HAN, Yufei: Deepfakes: A Terror in the era of AI?
- <https://www.nortonlifelock.com/blogs/research-group/deepfakes-terror-era-ai> (2020.08.18.)
- 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.
- HUBBARD, Ben – SHOUMALI, Karam: Likely Successor to Dead ISIS Leader Also Reported Killed. <https://www.nytimes.com/2019/10/27/world/middleeast/al-baghdadi-successor-reported-killed.html> (2020.08.18.)
- IRWIN, Angela – SLAY, Jill: Detecting Money Laundering and Terrorism Financing Activity in Second Life and World of Warcraft. In: Valli, Craig (ed.): Proceedings of the 1st International Cyber Resilience Conference ICR2010. Edith Cowan University, Perth 2010. 41. o.
- JOHNSON, Bridget: ISIS: Cities Distracted by Coronavirus Should be Hit with Attacks Like Paris, London, Brussels.
- <https://www.hstoday.us/subject-matter-areas/counterterrorism/isis-cities-distracted-by-coronavirus-should-be-hit-with-attacks-like-paris-london-brussels/> (2020.08.18.)
- KATZ, Rita: A Growing Frontier For Terrorist Groups: Unsuspecting Chat Apps. https://www.wired.com/story/terrorist-groups-prey-on-unsuspecting-chat-apps/?fbclid=IwAR0rzGUvrw5SoMJy1_XGd-wHuTF6cgTGUrQlsWkpQr8_eZq_l6vSK0YKWcQ (2020.08.18.)
- KATZ, Rita: ISIS Is Now Harder to Track Online – but That's Good News <https://www.wired.com/story/opinion-isis-is-now-harder-to-track-online-but-thats-good-news/> (2020.08.18.)
- KATZ, Rita: The Far-Right's Online Discourse on COVID-19 Pandemic.
- https://ent.siteintelgroup.com/index.php?option=com_acymailing&ctrl=archive&task=view&mail

- id=20576&key=4lfGcEyn&subid=1472-t9ir9gm3ghmVr7&tmpl=component (2020.08.18.)
- KIS-BENEDEK József – KENEDLI Tamás: A terrorfenyegetettség új tendenciái és lehetséges válaszlépések. Szakmai Szemle, 2015. 1. sz. 31. o.
 - KIS-BENEDEK József: Katonai biztonság Marokkótól Iránig. Zrínyi Kiadó, Budapest 2018. 246. o.
 - KIRBY, Aidan: The London Bombers as „Self-Starters”: A Case Study in Indigenous Radicalization and the Emergence of Autonomous Cliques. *Studies in Conflict & Terrorism*, 2017. 425. o.
 - KOEHLER, Daniel: The Halle, Germany, Synagogue Attack and the Evolution of the Far-Right Terror Threat. *CTC Sentinel*, 2019. 12. évf. 11. sz. 14. o.
 - KORINEK László: A terrorizmus. *Belügyi Szemle*, 2015. 7–8. sz. 17–19. o.
 - KÓHALMI László: Gondolatok a vallási indíttatású terrorizmus ürügyén. *Belügyi Szemle*, 2015. 63. évf. 7–8. sz. 52–71. o.
 - LIEBERMAN, Ariel Victoria: Terrorism, the Internet, and Propaganda: A Deadly Combination. *Journal of National Security Law and Policy*, 2017. 9. sz. 122. o.
 - MACKLIN, Graham: The El Paso Terrorist Attack: The Chain Reaction of Global Right-Wing Terror, *CTC Sentinel*, 2019. 12. évf. 11. sz. 1. o.
 - MALIK, Nikita: Self-Isolation Might Stop Coronavirus, but It Will Speed the Spread of Extremism. <https://foreignpolicy.com/2020/03/26/self-isolation-might-stop-coronavirus-but-spread-extremism/>. (2020.08.18.)
 - MÁTÉ István Zsolt: Informatikai rendszerek elleni támadások szakértői vizsgálata – a digitális nyomok rögzítésének szerepe. *Belügyi Szemle*, 2018. 66. évf. 7–8. sz. 38. o.
 - MUDDE, Cas: The Ideology of the Extreme Right. Manchester University Press, Manchester/New York 2000. 11. o.
 - NAGY Zoltán András: Tradicionális bűncselekmények számítógépes hálózatokon. *JURA*, 2007. 13. évf. 1. sz. 127.
 - NITSCH, Holger: Terrorismus und die Nutzung des Internet. In: Rüdiger, Thomas-Gabriel – Bayerl, Petra Saskia (eds.): *Cyberkriminologie: Kriminologie für das digitale Zeitalter*. Springer VS, Wiesbaden 2020. 198. o.
 - ÖZKAYA, Erdal: The Use of Social Media for Terrorism. *NATO Defence Against Terrorism Review*, 2017. Vol. 9. 54.o.
 - PASCA, Viorel – ORZA, Daniela Simona: Terrorism: between the need for funding and obtaining funding sources. *Journal Of Eastern-European Criminal Law*, 2019. No. 1. 227. 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.
 - REEVE, Zoey: Engaging with Online Extremist Material: Experimental Evidence, *Terrorism and Political Violence*, 2019. 2. o.
 - Referral Action Day against Islamic State online terrorist propaganda. <https://www.europol.europa.eu/newsroom/news/referral-action-day-against-islamic-state-online-terrorist-propaganda> (2020.08.18.)
 - RIPSZÁM Dóra: Emberkereskedelem az interneten. *KRE-DIT: A KRE-DOK ONLINE TUDOMÁNYOS FOLYÓIRATA*, 2020. 3. évf. 1. sz.
 - ROOSE, Kevin: 8chan Is a Megaphone for Gunmen. „Shut the Site Down”, Says Its Creator. <https://archive.is/JrNGc> (2020.08.18.)
 - RYDGREN, Jens: The Radical Right: An Introduction. In: Rydgren, Jens (ed.): *The Oxford Handbook of the Radical Right*. Oxford University Press, New York 2018. 9. o.
 - S/2019/570 Twenty-fourth report of the Analytical Support and Sanctions Monitoring Team submitted pursuant to resolution 2368 (2017) concerning ISIL (Da'esh), Al-Qaida and associated individuals and entities. United Nations Security Council, 2019. 5. o.
 - SILKE, Andrew: COVID-19 and terrorism: assessing the short-and long-term impacts. Cranfield: Pool Re Solutions, 2020. 2. o.
 - SIMONS, Greg – BIANCA, Cristina: The Specter of Terrorism During the Coronavirus Pandemic. 2. o. <https://www.e-ir.info/2020/05/08/the-specter-of-terrorism-during-the-coronavirus-pandemic/> (2020.08.18.)
 - SPECKHARD, Anne: Baghdadi Just Confirmed ISIS „Martyrdom” Narrative, Ensuring ISIS Will Live. <https://www.icsve.org/baghdadi-just-confirmed-isis-martyrdom-narrative-ensuring-isis-will-live/> (2020.08.18.)
 - 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*, 2019. 1. o.
 - TÓTH Dávid: A virtuális pénzekkel kapcsolatos visszaélések. *Rendészet-Tudomány-Aktualitások: A rendészettudomány a fiatal kutatók szemével*. Szerkesztette: Baráth Noémi Emőke, Mezei József, Doktoranduszok Országos Szövetsége, Rendészettudományi Osztálya, Budapest 2019. 242–250. o.
 - TÓTH, Dávid: Credit card fraud with a comparative law approach. In: *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, Bitola 2019. 232. o.*
 - TOWNSHEND, Charles: A terrorizmus. Magyar Világ Kiadó, Budapest 2003. 9. o
 - United States of America v. Patrick Wood Crusius, Case 3:20-cr-00389-DCG 02/06/20 1–2. o.
 - VARGA Árpád: Az informatikai bűnözés fogalmi meghatározása, csoportosítása és helye a hazai jogfejlődésben. In *Medias Res*, 2019. 8. évf. 1. sz. 151. o.
 - WEIMANN, Gabriel – Masri, Natalie: The Virus of Hate: Far Right in Cyberspace. *International Institute for Counter Terrorism*, 2020, 12. o. <https://www.ict.org.il/images/Dark%20Hate.pdf>. (2020.08.18.)
 - WEIMANN, Gabriel: www.terror.net: How Modern

- Terrorism Uses The Internet. United States Institute Of Peace, Washington, D.C. 2004. 5–10. o.
- <https://www.usip.org/sites/default/files/sr116.pdf> (2019.12.10.)
 - WITHER, James K.: The COVID-19 Pandemic: A Preliminary Assessment of the Impact on Terrorism in Western States. Occasional Paper Series, 2020. 33. sz. 3–4. o.
 - <https://www.marshallcenter.org/en/publications/occasional-papers/covid-19-pandemic-preliminary-assessment> (2020.08.18.)
 - 2–3. o.
 - <https://honvedelem.hu/cikk/elfogtak-tobb-feltetelezett-szelojobboldali-terroristat-nemet-orzagban/> (2020.08.18.)
 - https://qubit.hu/2020/07/22/2020-ban-jelentosen-megnott-az-emberolesek-szama-magyarorszagon?_ga=2.90202842.1187097502.1593935711-1665391435.1543668993&fbclid=IwAR1xyR4C2eMUqgh-zUX6gqR0wPxDiYqHDJjve3Xp5kHPDVpUEwhQ8ra_7Sk (2020.08.18.)
 - <https://storyful.com/resources/blog/what-is-8chan/> (2020.08.18.)
 - <https://www.bbc.com/news/world-51236915> (2020.08.18.)
 - <https://www.bbc.com/news/world-europe-49308016> (2020.08.18.)
 - <https://www.bbc.com/news/world-europe-49318001> (2020.08.18.)
 - <https://www.christchurchcall.com/> (2020.08.18.)
 - <https://www.counterextremism.com/press/extremist-content-online-extremists-plot-anti-semitic-harassment-campaign-targeting> (2020.08.18.)
 - https://www.vice.com/en_us/article/a3mexp/neo-nazis-are-organizing-secretive-paramilitary-training-across-america (2020.08.18.)
 - https://www.vice.com/en_us/article/z3bymx/new-german-terror-cell-the-hard-core-wanted-to-attack-mosques-to-start-a-civil-war (2020.08.18.)
 - <https://www.voxpol.eu/isis-use-of-smaller-platforms-and-the-dweb-to-share-terrorist-content/> (2020.08.18.)
 - <https://www.voxpol.eu/telegram-deplatforming-isis-has-given-them-something-to-fight-for/> (2020.08.18.)
 - <https://www.who.int/emergencies/diseases/novel-coronavirus-2019/events-as-they-happen> (2020.08.18.)