SERBAKOV MÁRTON TIBOR

AZ ONLINE FELÜLETEK ÉS OKOSTELEFONOS ALKALMAZÁSOK MINT A TERRORCSELEKMÉNYEK ELŐREJELZŐ RENDSZEREI

1. Bevezetés

Jelen tanulmányban a különféle online felületeket és okostelefonos alkalmazásokat kívánom megvizsgálni, amelyek a terrorcselekmények tekintetében mint „korai figyelmeztető rendszerek”[1] funkcionálnak. Megvizsgálom, hogy korunk terroristái, főleg az Iszlám Állam terrorszervezet milyen online felületeken aktív, melyek felé mozdul el, miért, mire és milyen alkalmazásokat használ. Próbálok választ találni arra a kérdésre, hogy ezeken a felületeken való jelenlétükből hogyan kovácsolható előny a terrorizmus elleni harc során.

2. A terroristák internethasználata

Ahogy Bartkó Róbert rávilágít az egyes elhárítási eszközök a terrorista akciókkal együtt fejlődnek, így továbbra is alátámasztódni látszik a mára már „közhelynek” tekinthető állítás, miszerint a bűnözők egy lépéssel mindig a bűnüldöző hatóságok előtt járnak.[2] A bűnözők, köztük a terrorizmus finanszírozók és a terroristák is folyamatosan fejlesztik a technikáikat, szívesen használnak egyedi, vagy kísérleti jellegű szolgáltatásokat és termékeket, céljaik elérése érdekében.[3]

„*Az internet forradalmasította a terrorizmust*.”[4] A világhálót pszichológiai hadviselésre, publicitásra és propagandára, adatbányászásra, adománygyűjtésre, toborzásra és mobilizációra, kapcsolattartásra, információ megosztására, tervezésre és koordinációra használják.[5] Az okostelefonok és az egyéb hordozható készülékek megváltoztatták azt, ahogy a világ nagy része kommunikál egymással, és a terroristák is hamar átvették az ilyen

---

[1] Maura Conway: *Terrorist 'use' of the internet and fighting back.* Department of Political Science College Green Trinity College Dublin 2 Ireland, 22. o
Forrás: https://www.oii.ox.ac.uk/archive/downloads/research/cybersafety/papers/maura_conway.pdf (Letötlés ideje: 2019.07.29.)

[2] Bartkó Róbert: A terrorizmus elleni küzdelem kriminálpolitikai kérdései. UNIVERSITAS-GYŐR Nonprofit Kft., Győr 2011. 68.o

[3] Sean McCrossan: Combating the Proliferation of Mobile and Internet Payment Systems as Money Laundering Vehicles. CAMS-FCI, 15. o
Forrás: https://www.acams.org/wp-content/uploads/2015/08/Combating-the-Proliferation-of-Mobile-and-Internet-Payment-Systems-as-ML-Vehicles-S-McCrossan.pdf (Letötlés ideje: 2019.07.29.)

[4] Ariel Victoria Lieberman: Terrorism, the Internet, and Propaganda: A Deadly Combination. Journal of National Security Law and Policy, 2017, Volume 9, 122. o
Forrás: http://jnslp.com/wp-content/uploads/2017/04/Terrorism_the_Internet_and_Propaganda_FINAL.pdf (Letötlés ideje: 2019.07.29.)

[5] Gabriel Weimann: www.terror.net How Modern Terrorism Uses The Internet. United States Institute Of Peace, Special Reoprt, 2004. 5-10. o Forrás: https://www.usip.org/sites/default/files/sr116.pdf (2019.07.29.)

technológiák használatát. A mai terroristák erősen támaszkodnak az internet nyújtotta lehetőségekre, növekvő online jelenlétük új biztonsági kockázatokat hozott magával.[6]

Felmerülhet a kérdés, hogy 2019-ben egyáltalán veszélyes-e még az Iszlám Állam online tevékenysége, hiszen az ISIS elfoglalt területeit elveszítette.[7] Ennek ellenére a „virtuális Kalifátus" még nagyon is életben van, új tartalmakat generál, régieket hasznosít újra, az online kommunikáció és toborzás terén továbbra is aktív. Az ISIS online tevékenysége tehát továbbra is fenyegetést jelent. Több mint 150 közösségi média platformon van jelen az Iszlám Állam, az al-Kaida, és más extrémista csoportok.[8]

3. Elmozdulás az alternatív kommunikációs csatornák irányába

A terroristák közösségi médián való jelenléte ellen bizonyos platformok ellenlépéseket tettek. A Twitter kifejezetten erélyesen lépett fel az ISIS-t támogató felhasználói fiókokkal szemben.[9] A terroristák alkalmazkodóképességükről téve tanúbizonyságot, céljaik előbbre vitele és a kommunikáció biztosítása érdekében folyamatosan alternatív lehetőségek után kutatnak.[10] Kénytelenek biztonságosabb és rejtettebb alternatívákat keresni a felszíni web és a közösségi média platformjai helyett.[11] Miközben a fő platformok, mint a Facebook, Twitter, YouTube és Telegram egyre „barátságtalanabbak" az ISIS-szel szemben, a terrorszervezet egyre csak terjeszkedik a vállalkozások és játékosok számára tervezett, kevésbé ismert üzenetküldő alkalmazásokon. Iraki és szíriai területvesztései után az ISIS újratervezi a technológia használatának stratégiáját a toborzás és koordináció terén.[12] A terroristák továbbá az ún. dark web felé fordulnak, kiegészítve más platformokon végzett tevékenységüket, mivel annak titkosításokkal rendkívül védett platformjai vannak, melyeknek köszönhetően a felhasználók IP címeit a bűnüldöző szervek rendkívül nehezen tudják lekövetni, ezért nagyfokú anonimitást biztosít. A dark web ezért rengeteg illegális tevékenységnek ad otthont.[13] Az internet felső rétege, a felszíni web könnyen hozzáférhető a keresőmotorok által, vagy a böngészőbe az ismert weboldal címének beírásával. A „mélyebb rétegek", a deep web/mély web tartalmai nem indexeltek a tradicionális keresőmotorok által. A deep web legmélyebb rétegei, a dark web, szándékosan rejtett tartalmakat rejt, az egy olyan része a deep web-nek, ami csak specializált böngészők által érhető el. A felszíni web használata kockázatosabb a terroristák számára: ott felügyelhetőek, lekövethetőek, megtalálhatóak.

---

[6] Laith Alkhouri, Alex Kassirer: Tech for Jihad: Dissecting Jihadists' Digital Toolbox, Flashpoint, 2016. július, 1. o Forrás: https://www.flashpoint-intel.com/wp-content/uploads/2016/08/TechForJihad.pdf (Letötlés ideje: 2019.07.29.)

[7] Islamic State group defeated as final territory lost, US-backed forces say Vö. https://www.bbc.com/news/world-middle-east-47678157 (Letötlés ideje: 2019.07.29.)

[8] Anne Speckhard, Ardian Shajkovci: Is ISIS Still Alive and Well on the Internet? Forrás: https://www.hstoday.us/subject-matter-areas/terrorism-study/is-isis-still-alive-and-well-on-the-internet/ (Letöltés ideje: 2019.07.29.)

[9] Alkhouri, Kassirer: i.m. 1. o

[10] Uo

[11] Erdal Ozkaya: The Use of Social Media for Terrorism. NATO Defence Against Terrorisim Review. 9. 47. 2017. 8-9. o

[12] Rita Katz: A growning frontier for terrorist groups unsuspecting chat apps Forrás: https://www.wired.com/story/terrorist-groups-prey-on-unsuspecting-chat-apps/?fbclid=IwAR0rzGUvrw5SoMJy1_XGd-wHuTF6cgTGUrQlsWkpQr8_eZq_l6vSK0YKWcQ (Letöltés ideje: 2019.07.29.)

[13] Ozkaya: i.m. 8-9. o

Ezzel szemben a dark web-en decentralizált és anonim hálózatok használatával a lebukás elkerülhető és a terrorista platformok zártak maradhatnak.[14]

További alternatív kommunikációs csatornák a bűnözők, terrorizmus finanszírozók, pénzmosók számára az online videojátékok, ún. MMORPG-k, mint például a World of Warcraft és Second Life chat szobái és privát üzenetei.[15]

4. A terroristák által használt okostelefonos alkalmazások csoportosítása

Laith Alkhouri és Alex Kassirer a terroristák digitális „szerszámosládájában" a következő eszközöket sorolja fel: a biztonságos böngészők, a VPN-ek és proxy szolgáltatások, védett e-mai szolgáltatások, okostelefonos biztonsági alkalmazások, titkosítással ellátott üzenetküldő alkalmazások, és okostelefonos propaganda applikációk.[16] A terroristák által használt alkalmazások közül a jelen tanulmány szempontjából relevánsabb titkosítással ellátott üzenetküldő alkalmazásokat vizsgálom részletesebben, a biztonsági és propaganda alkalmazásokat csupán érintőlegesen tárgyalom.

4.1. Biztonsági alkalmazások

Az okostelefonos alkalmazások használata kockázatokkal is jár a terroristák számára, ezért a biztonsági kockázatok csökkentése érdekében további alkalmazásokat használnak. A következő biztonsági applikációk kedveltek a terroristák körében: Locker, FAKE GPS, D-Vasive Pro, AMC Security, ESET Mobile Security, Battery Saver, Call/SMS Blocker, Privasy Locker, APP Manager, iSHREDDER PRO, Override DNS, DNSCrypt, Net Guard, AFWall, F-Secure Freedome, Hide.me, Tutanota.[17]

4.2. Titkosítással ellátott üzenetküldő alkalmazások

A terroristák szívesen használnak ún. end-to-end encryptionnel, azaz végpontok közötti titkosítással ellátott mobiltelefonos alkalmazásokat, hogy lebukást elkerüljék.[18] Ilyen applikációkat a terroristák már évek óta használnak diszkrét kommunikációra, melyek általában okostelefonról és számítógépről is elérhetőek. A svájci Threema-t szívesen használják, mivel az nem gyűjt és igényel személyes adatokat, és minden szempontból (pl. fájlok, audiók etc. tekintetében) erős titkosítással rendelkezik.

A terroristák kedvenc alkalmazásának az orosz VKOntakte alapító Pavel Durov által fejlesztett Telegram tűnik.[19] Az ISIS a Telegramot használta például a 2016-os berlini karácsonyi vásáron elkövetett merénylethez is: azon keresztül toborozták a terrortámadás elkövetőit. A 2017-es, 15 emberéletet követelő szentpétervári terrortámadást is az

[14] Gabriel Weimann: Terrorist Migration to the Dark Web. Perspectives on Terrorism, Vol. 10, No. 3 (June 2016), 40-41.o

[15] Angela Irwin, Jill Slay: Detecting Money Laundering and Terrorism Financing Activity in Second Life and World of Warcraf. In C. Valli (Ed.), Proceedings of the 2010 International Cyber Resilience Conference *ICR2010* (pp. 41-51). Perth: Edith Cowan University. 41.o

[16] Alkhouri, Kassirer: i.m. 1.o

[17] Alkhouri, Kassirer: i.m. 5-6.o

[18] Pierluigi Paganini: The Role of Technology in Modern Terrorism. Forrás: https://resources.infosecinstitute.com/the-role-of-technology-in-modern-terrorism/#gref (Letötlés ideje: 2019.07.29.)

[19] Alkhouri, Kassirer: i.m. 7-8. o

alkalmazás használatával tervezték meg. A Telegram rendkívül magas fokú titkosítással, privát chat szobákkal, és önmegsemmisítő üzenetekkel rendelkezik, könnyű hozzá csatlakozni és új felhasználói fiókokat létrehozni.[20] A Telegramon megtalálható többek közt az ISIS, az Al-Kaida, az *al-Nuszra Front, a Hamasz, a Hezbollah és a tálibok.*[21] *Egy újabb jelenség a Telegramon a szélsőjobboldali terrorizmust támogató tartalmak fokozott megjelenése.*[22]

A szkeptikus dzsihádista egyik alkalmazásban sem bízik meg teljesen, mivel a többségük nyugati fejlesztés. 2013 februárjában a Global Islamic Media Front (GIMF) kifejlesztette az Asrar al-Darshah (Secrets of Chatting) alkalmazást, mely egy titkosító plugin, ami élő beszélgetések titkosítását teszi lehetővé üzenetküldő platformokon, mint a Paltalk, Google Chat, Yahoo, MSN és Pidgin.[23] Az Iszlám Állam saját fejlesztésű titkosítottással ellátott chat alkalmazása az Alrawi. [24]

A TrueCrypt egy biztonságos kommunikációs alkalmazás, melyet 2004-ben indított útjára a programozó és bűnöző Paul Le Roux. Az ISIS titkosított kommunikációra és fájlmegosztásra használja.[25]

A RocketChat egy nyílt-forrású üzenetküldő szolgáltatás, elérhető okostelefonról és PC-ről is, 2018. december közepe óta ISIS csatornákkal. A Nashir News Agency és sok más ISIS-hez köthető média csoporta támogatókat sürgette az app-hoz való csatlakozásra.

A Yahoo Together egy mobilos üzenetküldő alkalmazás, terroristák által kedvelt. A Vibert az utóbbi időkben a terroristák fokozottan használják. A Discord egy üzenetküldő applikáció videojátékosoknak, több mint 130 millió regisztrált felhasználóval, a platform a chat közösségeit szerverekre osztja, ISIS barát szerverek is találhatók rajta, pl.: „Al Bagdadi" vagy "dawlatulislambiqiyah". Korábban az ISIS próbálkozott a Riot és TamTam platformokkal is, de ezek a cégek gyorsan reagáltak ellenük, ezért a terroristák felhagytak a használatukkal.

Az üzenetküldő cégek gyors reakciója vagy közömbössége dönt, hogy hova „migrálnak" a terrorista csoportok.[26]

Al-Khabir al-Taqni, egy dzsihádista-támogató és önjelölt biztonsági szakértő a Twitteren 33 okostelefonos üzenetküldő alkalmazást kategorizált biztonságosság szempontjából, mint nem biztonságos, a mérsékelten biztonságos, biztonságos és legbiztonságosabb.[27]

---

[20] Rebecca Tan: Terrorists' love for Telegram, explained. It's become ISIS's "app of choice." https://www.vox.com/world/2017/6/30/15886506/terrorism-isis-telegram-social-media-russia-pavel-durov-twitter (Letötlés ideje: 2019.07.29.)

[21] Terrorists on Telegram. Forrás: https://www.counterextremism.com/terrorists-on-telegram (Letöltés ideje: 2019.07.29.)

[22] Michael Edison Hayden: Far-Right Extremists Are Calling for Terrorism on the Messaging App Telegram. Forrás: https://www.splcenter.org/hatewatch/2019/06/27/far-right-extremists-are-calling-terrorism-messaging-app-telegram (Letötlés ideje: 2019.07.29.)

[23] Alkhouri, Kassirer: i.m. 7-8. o

[24] Josh Constine: ISIS Has Its Own Encrypted Chat App. Forrás: https://techcrunch.com/2016/01/16/isis-app/?guccounter=2 (Letöltés ideje: 2019.07.29.)

[25] Gabriel Weimann: Terrorist Migration to the Dark Web. Perspectives on Terrorism, Vol. 10, No. 3 (June 2016), 42. o

[26] Rita Katz: A Growing Frontier for Terrorist Groups: Unsuspecting Chat Apps https://www.wired.com/story/terrorist-groups-prey-on-unsuspecting-chat-apps/?fbclid=IwAR3d9byhbjIhYKMka_7bSRRF2FmXhLamDuQhSOV_2XC3cQnvSZmOYqF0_Xo (Letötlés ideje: 2019.07.29.)

[27] Rita Katz: Almost Any Messaging App Will Do—If You're ISIS https://motherboard.vice.com/en_us/article/kb7n4a/isis-messaging-apps (Letötlés ideje: 2019.07.29.)

4.3. Propaganda alkalmazások

Az Amaq médiaegységhez köthető The A'maq Agency az egyik első dzsihádista fejlesztésű okostelefonos alkalmazás, mely hírekkel és harctéri videókkal szolgál az ISIS támogatóknak. Az Al-Bayan Radio applikáció az ISIS hivatalos rádió állomása. A Voice of Jihad alkalmazás az afgán tálibokhoz köthető, azt 2016. április 1-én indították útjára, hírek, jelentések, bejelentések, cikkek és videók nézését tette lehetővé. Az ISIS dzsihádista témájú Ábécé alkalmazása gyerekeknek tanítja meg az arab betűket. [28]

Az ISIS 2013-ban indította útjára a Dawn of Glad Tidings nevű alkalmazását, mely a terroristák számára a résztvevő twitteres felhasználói fiókokból tweetek tízezreinek küldését teszi lehetővé, továbbá a twitteres közösségi média kampány magas szintű szervezését.[29]

5. Okostelefonos alkalmazások használatában rejlő kockázat a terroristák számára – egy beszivárgási lehetőség

Az ISIS okostelefonos applikáció-használata kockázatokat is hozott a terrorszervezet számára. Valamennyi terrorista alkalmazás kizárólag androidra készül. A fő különbség az iPhone és Android eszközök között, hogy az Android lehetővé teszi felhasználói számára a kijelölt app store-on kívüli alkalmazások készítését és telepítését. Android applikációkat lehet készíteni és installálni függtelenül APK (Andoid application package) fájlokként, anélkül hogy valaha is a Google Play Store-ba kerülne. Ezt a technikát „sideloading-nak" nevezik, mely megkönnyíti a hatóságok és önjelölt igazságosztók dolgát, mivel a Google Play-en és IOS store-on kívüli alkalmazásokba könnyebb álcázott malware-t helyezni és az ISIS támogatók közé beszivárogni. Gyakori védekezési módszer az ilyen megtévesztés ellen az egyénileg generált checksum file-ok által történő hitelesítés, amivel meg lehet állapítani, hogy az eredeti fájlon eszközöltek-e változtatást, de nem minden ISIS támogató él ezzel a biztonsági intézkedéssel.[30]

Mit lehet tenni az end-to-end encryption-nal szemben? A biztonsági ügynökségeknek a végpontoknál kell meghackelniük a szoftvert, főleg 0day[31] igénybe vételével. Az end-to-end encryption feltörésével próbálkozni nem járható út. Az ügynökségeknek továbbá a terroristák gyenge operációs biztonságát (opsec) kell kihasználni, például a terroristák nem elég erős jelszavainak kitalálásával.[32]

---

[28] Alkhouri, Kassirer: i.m. 7-9. o

[29] Mohammad-Mahmoud Ould Mohamedou: A Theory of ISIS: Political Violence and the Transformation of the Global Order. Pluto Press, 2018. 205. o

[30] Rita Katz: ISIS's Mobile App Developers Are in Crisis Mode https://motherboard.vice.com/en_us/article/qkj34q/isis-mobile-app-developers-are-in-crisis-mode (Letöltés ideje: 2019.07.29.)

[31] 0day egy a szoftver szolgáltatója és antivírus szolgáltatója előtt is ismeretlen sebezhetőséget megcélzó kibertámadás. A 0day sebezhetőségeknek piaca is van, szervezetek fizetnek kutatóknak, akik felfedeznek ilyen sebezhetőségeket. Van fehér, szürke és fekete piaca a 0day sebezhetőségeknek. Forrás: Zero-day (0day) exploit https://www.imperva.com/learn/application-security/zero-day-exploit/ (Letötlés ideje: 2019.07.29.)

[32] Robert Graham: How Terrorists Use Encryption. In: Combating Terrorism Center at West Point, JUNE 2016, VOLUME 9, ISSUE 6. 25.o Forrás: https://ctc.usma.edu/app/uploads/2016/06/CTC-SENTINEL_Vol9Iss614.pdf (Letöltés ideje: 2019.07.29.)

6. A megelőzés fontosságáról

Egyetértek Jonathan Barker-rel, aki szerint nem elegendő csupán a már elkövetett terrorcselekményekre adott reakció, hanem a megelőzéssel is foglakozni kell, és elengedhetetlen fontosságú a hírszerzés fejlesztése.[33]

Horváth L. Attila hangsúlyozza, hogy legideálisabb az alvó vagy szervezkedő terrorista csoportokat felderíteni, és a veszélyt semlegesíteni. A nemzetközi és nemzeti szervek és valamilyen formában a társadalom együttműködésére van szükség, hogy a titkosszolgálatok felvehessék a harcot a terrorizmus ellen.[34]

A hírszerzés számára a terrorelhárítás tekintetében a legnagyobb kihívást az jelenti, hogy olyan szervezkedések felfedése a feladat, amelyeket kis számú ember tervez és készít elő titokban, akik a műveleti biztonságot nagyon komolyan veszik.[35]

Az interneten a terroristák megfigyelhetők, ellenőrizhetők, a tevékenységük tanulmányozható; vannak elméletek, amik szerint ezek miatt a terroristák online jelenléte valójában ellenük dolgozik. A weboldalak és netes fórumok egy korai előrejelző *rendszerként működnek a terrorcselekményeket illetően.*[36] Michel Moutot szerint ugyan az okostelefon a terroristák egy komoly „fegyvere" lehet, viszont az a titkosszolgálatoknak egy eszköz is, hogy őket lekövethessék, így az „kétélű kard" a terroristák kezében.[37] Az internet biztosította anonimitás tehát nem csak a terroristáknak kedvez, hiszen az fedett ügynökök beépülésére is lehetőséget ad. Az USA-ban számos FBI-ügynököknek sikerült már terrorszervezetekbe beépülni, és ez által terrortámadásokat meghiúsítani.[38]

7. Javaslatok

A terroristák által frekventált online platformok, virtuális terek és okostelefonos applikációk olyan felületek, amelyek fokozott felügyelete, a terroristák platformról platforma történő vándorlásának nyomon követése a terrorcselekmények megelőzése szempontjából elengedhetetlen fontosságú. Ezeken a felületeken a terroristák tevékenységét lehetséges és szükséges is tanulmányozni. Továbbá ezek a platformok lehetőséget adnak fedett ügynökök terroristák közé történő beépülésére és ezáltal terrorcselekmények elkövetésének és toborzás megakadályozására. A terroristákhoz kötődő alkalmazásokat fel kell törni, továbbá megfigyelő malware-ekkel ellátott hamis terrorista alkalmazásokat szükséges fejleszteni,[39] ezek használatával a terroristák közé beszivárogni és ezáltal terrorcselekményeket megelőzni.

---

[33] Jonathan Barker: A terrorizmus. HVG Kiadói Rt., Budapest 2003. 145-146. o

[34] Horváth L. Attila: A terrorizmus csapdájában. Zrínyi Kiadó, Budapest 2014. 241-243. o

[35] Paul R. Pillar: Terrorism and Current Challenges for Intelligence. GSSR Special Issue: What the New Administration Needs to Know About Terrorism and Counterterrorism, February 2017., 108. o http://georgetownsecuritystudiesreview.org/wp-content/uploads/2017/02/GSSR-What-the-New-Administration-Needs-to-Know-About-Terrorism-and-Counterterrorism.pdf (Letöltés ideje: 2019.07.29.)

[36] Conway: i.m. *22. o*

[37] Moutot, Michel: Smartphones: a double-edged sword for terrorists. Forrás: https://phys.org/news/2018-11-smartphones-double-edged-sword-terrorists.html (Letöltés ideje: 2019.07.29.)

[38] Kis-Benedek József: Dzsihadizmus, radikalizmus, terrorizmus, Zrínyi Kiadó, 2016. 195-196. o

[39] Rita Katz: Almost Any Messaging App Will Do—If You're ISIS https://motherboard.vice.com/en_us/article/kb7n4a/isis-messaging-apps (Letöltés ideje: 2019.07.29.)