ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOKTORI (PHD) ÉRTEKEZÉSTERVEZET

GULYÁS ATTILA

Dzsihadista terrorszervezetek tevékenysége az interneten

Témavezető:

Prof. Dr. Besenyő János
egyetemi tanár

BIZTONSÁGTUDOMÁNYI DOKTORI ISKOLA

Budapest, 2024. június 30.

TARTALOM

BEVEZETÉS 6

Tudományos probléma megfogalmazása 6

Célkitűzés 8

A téma kutatásának hipotézisei 9

Kutatási módszerek, etikai kérdések 9

A kutatás módszerei 9

A kutatás korlátai 11

Büntetőjogi megfontolások 11

A kutatás során alkalmazott technikai környezet kialakítása 11

I. FEJEZET 12

A TERRORSZERVEZETEK JELENLÉTE A DARK WEBEN 12

1.1 Irodalmi áttekintés 12

1.2. A dzsihadista terrorszervezetekkel összefüggésbe hozható dark webes szolgáltatások felkutatása 15

1.2.1 A kutatás során vizsgált dark webes alkalmazások kiválasztása 15

1.2.2 A kutatás során alkalmazott keresőkifejezések kiválasztásának szempontjai 15

1.2.3 A közösségi médiában folytatott keresés eredménye 16

1.3 A TOR rendszerrel kapcsolatos kutatás 17

1.3.2 Kutatás dark webes tartalmak után a nyílt interneten 17

1.3.3 A TOR rendszerben használt keresőmotorok felhasználása 19

1.3.4 A TOR rendszerben található linkgyűjtemények átvizsgálása 19

1.3.5 A saját összeállítású TOR szolgáltatások gyűjteményének átvizsgálása 19

1.4 Az I2P rendszeren történő kutatás 20

I.4.1 Az I2P vonatkozású kutatás a nyílt interneten 20

1.4.3 I2P keresőmotorok használata 20

1.4.4 I2P linkgyűjtemények átvizsgálása 20

1.5 Freenet rendszer 21
1.5.1 Kutatás a nyílt interneten 21
1.5.2 Freenet keresőmotorok használata 21
1.5.3 Linkgyűjtemények átvizsgálása 21

1.6 Az alacsony szintű dark web használat okai 25

1.7 Összefoglalás 26

II. FEJEZET 28

CENZÚRA ELLENES TECHNIKÁK ÉS ELJÁRÁSOK AZ ONLINE TÉRBEN 28
Bevezetés 28

2.1 Szakirodalmi áttekintés 29
Az Iszlám Állam Internetes tevékenységével kapcsolatos szakirodalom áttekintése 29

2.2 A szélsőséges iszlám terrorszervezetek elleni online harc eszközei és célja 32
2.2.1 Deplatforming és deplatformization 32
2.2.2 Deamplification Deemphasizing (korlátozás, gyengítés) 35
2.2.3 Az önkéntesek szerepe a dzsihadista terrorszervezetek elleni harcban 36

2.3 Információgyűjtés, adatbázis építés 37

2.4 Dzsihadista szervezetek online jelenléte 37

2.5 Az Iszlám Állam által alkalmazott elkerülési technikák 39
2.5.1 Emberi tényezők 41
2.5.2 Technikai eljárások, módszerek 43
2.5.3 Kiberbiztonsági oktatás és továbbképzés 47
2.5.4 Tartalommanipuláció 52
2.5.5 Redundáns tartalomelosztás rendszere 55
2.5.6 Közösségi média szerepe a tartalommegosztás és kapcsolattartás rendszerében 63

2.6. Összefoglalás 66

III. FEJEZET 68

DZSIHADISTA TERRORSZERVEZETEK KRIPTOVALUTA HASZNÁLATA 68
Bevezetés 68

3.1 Szakirodalmi áttekintés 69
3.1.2 Szakértői csoportokhoz köthető irodalom.....71

3.2. A kriptovaluta.....73
3.2.1 A kriptovaluták előnyei, illetve hátrányai 74
3.2.2 Kriptovaluta elfogadottság 75
3.2.3 Kriptoháború, lefoglalás.....77

3.3 A dzsihadista terrorszervezetek kriptovaluta használata és az erre utaló jelek.....79

3.4 Dzsihadista terrorszerveztek online kiadványainak vizsgálata 81
3.4.1 A keresés eredménye 85

3.5 A vizsgált terrorszerezetek kriptovalutában történő online adománykérésének felmérése 88
3.5.1 Adatbázis kialakítása.....88
3.5.2 Az adatbázis kiértékelése 88
3.5.3 Az adatbázis elemzésének összegzése 92

3.6 A Jaysh al-Ummah bitcoin címéhez kapcsolódó tranzakciók elemzése (blokkláncelemzés) 92
3.6.1 Az elemzés lépései.....92
3.6.2 Megállapítások.....95
3.6.3 Figyelemre méltó tranzakciók: 95

3.7 Sajtóelemzés.....96
3.7.1 Kulcsszavak kiválasztása 96
3.7.2 Keresőmotorok: 97
3.7.3 A keresések eredményei.....97
3.7.4 A sajtó felmérés összefoglalása 98

3.8 Összefoglalás 98

3.9 Következtetés 101

ÚJ TUDOMÁNYOS EREDMÉNYEK/AJÁNLÁSOK 102

Tudományos eredmények 102

Ajánlások 103

HIVATKOZÁSOK 104

A HIPOTÉZISEKHEZ KAPCSOLÓDÓ TUDOMÁNYOS KÖZLEMÉNYEIM 114

TÁBLÁZATJEGYZÉK 116

ÁBRAJEGYZÉK 117

MELLÉKLETEK 119

1. számú Melléklet 119

A kutatás során alkalmazott OSINT eszközök és eljárások 119

Hivatalos források 119

A nyílt interneten alkalmazott módszerek 119

Dark webhez köthető módszerek 121

Bitcoin áramlásának nyomon követése 124

A Telegram, mint információforrás 124

2. számú melléklet 127

A dzsihadista online jelenlét felméréséhez szükséges adatbázis építés folyamata 127

Bevezetés 127

Az adatbázis építés folyamata 128

KÖSZÖNETNYILVÁNÍTÁS 130

BEVEZETÉS

Tudományos probléma megfogalmazása

Az Internet és a közösségi média térhódításával a kommunikációs lehetőségek eddig sosem látott tárháza tárult fel a 21. század embere előtt. A mindenütt jelenlévő és gyakorlatilag bárki számára elérhető internetes kapcsolattartási formákban rejlő lehetőségeket gyorsan felismerték a terrorszervezetek is, amelyek igyekeznek ezeket saját céljaik elérése érdekében kihasználni. Különösen a közösségi média nyújtotta lehetőségek nyújtanak kedvező lehetőségeket ahhoz, hogy terjesszék propagandájukat, tagokat toborozzanak, műveleteket tervezzenek, kiképezzenek, illetve koordináljanak, valamint anyagi támogatást szerezzenek.

A terrorszervezetek internetes tevékenységének bőséges szakirodalma van, azonban téma népszerűsége időben változó. Egy- egy nagyobb horderejű, főleg nyugati vonatkozású támadást követően fokozott érdeklődés tapasztalható a tudományos világ részéről. Megfigyelhető volt ez az Al Kaida vonatkozásában a hírhedt 09/11-es terrortámadást követően, majd az Iszlám Állam kikiáltását követő időszakban, illetve a véres párizsi terrortámadás után. Az online térben gyakorlatilag korlátozás nélkül terjedő terrorvonatkozású tartalmak bőséges kutatási lehetőséget szolgáltattak a tudományos világnak.

Törvényhozói és lakossági nyomásra a megfelelő törvényi környezet létrehozását követően a rendvédelmi szervek és a közösségi média érdekelt felei korlátozó és akadályozó tevékenységbe kezdtek, amely kezdetben jelentős eredményekkel járt, hiszen olyan platformokról, mint például a Twitter szinte teljesen sikerült eltávolítani a „toxikus” felhasználókat és tartalmakat. A hathatós intézkedések eredményeként a terrorista aktivitás visszaszorult, ami a témába vágó tudományos kutatások számának csökkenésével járt. Az ellentevékenység azonban bizonyos mértékig kontraproduktívvá vált, ugyanis a terrorszervezetek nem szüntették be a tevékenységüket, hanem alkalmazkodtak az új helyzethez. Folyamatosan keresték és keresik az új platformokat, alkalmazásokat fejlesztettek és a kommunikációjukban áttértek az végpontok közötti titkosítást alkalmazó üzenetküldő alkalmazásokra, alkalmazzák az anonimitást biztosító dark webes technológiákat, illetve a pénzügyi ellenintézkedések és szankciók hatásának kivédésre a kriptovaluták használatát is tanulmányozzák.

A terrorizmus elleni online harc kétségtelenül jelentős sikereket ért el ennek ellenére napjainkig nem sikerült felszámolni a terrorszervezetek online tevékenységét. Ehhez többek között

hozzájárul az elkövető és bűnüldöző közötti küzdelemből jól ismert mintázat, amely szerint az elkövetők igyekeznek új eljárásokat-módszereket alkalmazni, míg bűnüldözők általában egy lépéssel a bűnelkövetők mögött járnak.
Megítélésem szerint jelenleg az online dzsihadista terrortevékenység elleni harc kevésbé látványos szakaszában vagyunk. A sokrétű ellentevékenység következtében kevesebb felhasználó találkozik közvetlen „toxikus" tartalommal és ez azt a hamis benyomást keltheti, hogy a dzsihadista online tevékenységet sikerült visszaszorítani, azonban véleményem szerint ez nem felel meg a valóságnak, ugyanis a terrorszervezetek szervezetek folyamatosan keresik az új megoldásokat és ily módon képesek folyamatos online jelenlétüket és kapcsolati hálójukat fenntartani. Ez a részükről történő folyamatos törekvés az új eszközök és módszerek, valamint eljárások kidolgozásra és alkalmazására teszi indokolttá, a dzsihadista terrorszervezetek online tevékenységének tudományos igényű kutatását.

A négyéves időszakot felölelő kutatásom során a fundamentalista szélsőséges vallási indíttatású terrorszervezetek online tevékenységével összefüggésben elsődlegesen a nyílt internetes és dark webes tevékenységüket, valamint a kriptovalutákhoz való viszonyukat kutattam.
A kutató munka során ezzel kapcsolatban három olyan problémát azonosítottam, amelyek megoldása elősegítheti a terrorszervezetek tevékenységének jobb megértését ezzel elősegítve az ellenük folytatott harc hatékonyságát.

Elsődleges problémaként fogalmaztam meg a dark web és a vizsgált szervezetek viszonyát, ugyanis kutatásom során azzal szembesültem hogy a tudományos szakirodalomban elterjedt vélekedés és az általam tapasztaltak között ellentmondás van a szervezetek dark webes jelenlétét illetően. Tapasztalataim ellentmondtak annak a feltételezésnek miszerint a vizsgált szervezetek a tevekénységüket a rendvédelmi szervek és a közösségi média érdekelt felei által kifejtett nyomás hatására az anonimitást biztosító dark webre helyezték át.

A következő tisztázandó kérdésként jelöltem meg a terrorszervezetek folyamatos online jelenlétét lehetővé tevő körülmények tisztázását. Mint arra már a bevezetőben utaltam a koncentrált és kiterjedt online küzdelem sikerei ellenére azt tapasztaltam, hogy a vizsgált szervezetek továbbra is képesek a folyamatos online jelenlétüket, illetve a szimpatizánsaikkal a folyamatos kapcsolatot fenntartani. Feltevést fogalmaztam meg arra vonatkozóan, hogy a szervezetek rendelkeznek-e olyan eszközökkel, módszerekkel és eljárásokkal, amelyekkel képesek az ellenük kifejtett sokirányú ellentevékenységet kivédeni. A tudományos

szakirodalomban erre vonatkozóan csak részinformációkat találtam, amelyekből nem derült ki, hogy mi ezen szervezetek folyamatos online jelenlétének a titka.

Végül, a terrorszervezetek és a viszonylag új technológiának számító kriptovaluták viszonyát tanulmányoztam. Kutatási területem és a terrorszervezetek pénzügyi műveleteinek egy része az online térben metszik egymást, így nem kerülhettem ki a világhálótól elválaszthatatlan új pénzügyi eszköz szerepének tisztázását. Kutatásom során azt vizsgáltam, hogy a tanulmányozott szervezetek a számos nemzetközi pénzmosás elleni és terrorizmusfinanszírozást akadályozó szankció és rendelkezés hatására rákényszerültek-e a kriptovaluták használatára, vagy továbbra is a hagyományos módszereket és eljárásokat részesítik előnyben, ugyanis ezzel kapcsolatban is számos ellentmondásos feltételezés látott napvilágot, amelyek a komplex szemlélet helyett egy-egy tényező vizsgálatából levont következtetéseken alapultak.
Véleményem szerint, ami a terrorszervezetek finanszírozását illeti tisztázni kell, hogy megtörtént –e ez a váltás, illetve várható-e a közeljövőben ilyen változás. A terrorszervezetek pénzügyi forrásinak elvágása, illetve műveletinek felfedése és akadályozása rendkívüli fontossággal bír a terrorszervezetekkel szembeni harcban.

Célkitűzés

Értekezésemben megfogalmazott hipotézisek igazolása, illetve cáfolása keretében átfogó képet nyújtok a terrorszervezetek internetes tevékenységéről.
Elsősorban tisztázom, a tudományos életben elterjedt nézetnek megfelelően a terrorszervezetek tevékenységük folytatása érdekében valóban az anonimitást biztosító dark web felé fordultak-e.
Másodsorban feltárom, hogy léteznek-e olyan eszközök, módszerek és eljárások, amelyek a vizsgált terrorszervezetek számára lehetővé teszik, hogy folyamatosan jelen legyenek az online térben, illetve kapcsolatot tarthassanak szimpatizánsaikkal.

Végül a viszonylag új technológiának számító kriptovaluták és a terrorszervezetek viszonyának vizsgálatával tisztázni fogom, hogy a terrorszervezetek a nemzetközi pénzügyi korlátozó intézkedések hatására áttértek-e a kriptovaluták használatára és ehhez kapcsolódóan be fogom mutatni, hogy az új típusú valuta milyen helyet foglal el a terrorszervezetek pénzügyi rendszerében, különös tekintettel az online adománykérésekre.

A kutatásom célja az volt, hogy a megfogalmazott problémák tisztázásával hozzájárulhassak a terrorizmus ellen folytatott online harc sikeréhez azzal, hogy feltárom és bemutatom a terrorszervezetek internetes tevékenységére napjainkban jellemző azon eszközöket, módszereket és eljárásokat, amelyek lehetővé teszik számukra folyamatos online jelenlét fenntartását.

A téma kutatásának hipotézisei

1. Feltételezhető, hogy az utóbbi néhány évben a közösségi médiában bevezetett korlátozó és tartalomszűrő intézkedések következtében a terrorszervezetek lehetőségei beszűkültek, ezért tevékenységüket az anonimitást, illetve cenzúramentességet biztosító dark weben folytatják.
2. Feltételezhető, hogy a szélsőséges iszlám terrorszervezetek olyan technikákkal, taktikákkal és eljárásokkal rendelkeznek, amelyek segítségével a nyílt internet és a dark web előnyeit mesterien kihasználva a közösségi média tartalom szűrőit és a rendvédelmi szerveket kijátszva képesek biztosítani folyamatos jelenlétüket a világhálón
3. Feltételezhetően a szélsőséges Iszlám terrorszervezetek a nemzetközi pénzügyi korlátozó és szankciós intézkedések hatására pénzügyi műveleteik elrejtése érdekében a részleges anonimitást biztosító kriptovaluták felé fordultak.

Kutatási módszerek, etikai kérdések

A kutatás módszerei

Kutatásom megtervezésénél, illetve a hipotéziseim felállításánál felhasználtam a korábbi kutatásaimból származó szekunder adataimat, illetve célirányos és széleskörű kutatást folytattam az elérhető hazai és külföldi szakirodalomban, valamint internetes forrásokat tanulmányoztam annak érdekében, hogy beazonosíthassam azokat a kulcs elemeket, illetve ellentmondásokat, amelyek tisztázása elengedhetetlen a hipotéziseim igazolása, vagy cáfolása érdekében.

A primer kutatás szakaszának megtervezésénél felhasználtam a szekunder kutatás során összegyűjtött adatokat , illetve a már beazonosított hiányosságokat és ellentmondásokat.

Primer jellegű kutatás keretében telepítettem és használtam a dark webes alkalmazásokat és a Telegramot, annak érdekében, hogy működésüket, illetve a kutatásom szempontjából legjellemzőbb tulajdonságaikat megismerjem.

A dark webbel kapcsolatos adatgyűjtés során keletkezett nagy mennyiségű adatot adatbázisban tároltam, majd ezek feldolgozásának automatizálása érdekében célszoftvert fejlesztettem,

amelynek segítségével az összegyűjtött dark webes oldalak elérhetőségét és tartalmát automatizált módon ellenőriztem.
Tekintettel arra, hogy a szekunder kutatási módszer keretében tanulmányozott szakirodalomban szereplő terrorista jellegű tartalmakhoz a szerzők etikai és büntetőjogi megfontolásból elérhetőséget nem csatoltak, azonban kutatásom jellege megkövetelte, hogy ezeket eredetiben tanulmányozzam így kénytelen voltam eljárásokat kidolgozni arra vonatkozóan, hogy a szóban forgó tartalmakból saját adatbázist hozzak létre. Az adatgyűjtés során a terrorista vonatkozású tartalmak felkutatása érdekében széles körben alkalmaztam a nyílt forrású információgyűjtés (Open Source Intelligence röviden: OSINT) eszközeit és módszereit, illetve számos saját készítésű Python nyelvű scriptet fejlesztettem az adatok megszerzése, feldolgozása és adatbázisba rendezésének hatékonyabbá tétele érdekében.

Adatbázist építettem a dzsihadista terrorszervezetek online jelenlétével kapcsolatban annak érdekében, hogy felmérjem online jelenlétük mértékét, illetve első kézből tanulmányozhassam a rendvédelmi szervek és a közösségi média érdekelt felei által alkalmazott korlátozó intézkedések elleni technikáikat és eljárásaikat. Az adatbázis kialakításánál arra törekedtem, hogy több kutatási lépésnél is hasznosítható legyen így az összegyűjtött adatokat fel tudtam használni a vizsgált terrorszervezetek kriptovaluta-alapú online adománykéréseivel kapcsolatos felmérésemnél is.
A dzsihadista terrorszervezetek különböző nyelvű online magazinjaiból származó több mint 20 000 oldalt kitevő nyers adatok feldolgozását követően egységes angol nyelvű szöveges adatbázist hoztam létre, amely lehetővé tette a szervezetek kriptovalutával kapcsolatos viszonyának tanulmányozását.
Végül online sajtóelemzést végeztem annak érdekében, hogy megállapítsam hány esetben kaptak sajtónyilvánosságot dzsihadista terrorszervezetek kriptovalutához köthető visszaéléseivel kapcsolatos hatósági eljárások. Az adatok könnyebb áttekinthetősége érdekében a felmérés eredményét ebben az esetben is adatbázsiban tároltam.

A kutatás megtervezése során törekedtem arra, hogy a kidolgozott módszerek és felhasznált eszközök segítségével a kutatás megismételhető legyen. Az általam alkalmazott nyílt forrású információgyűjtés rendszerét az értekezés mellékletében tettem elérhetővé.

A primer kutatás keretében felvettem a kapcsolatot a Nemzeti Nyomozó Iroda illetékes osztályával azonban sem a dark webes kutatásommal, sem pedig a terrorszervezetek internetes

tevékenységével kapcsolatban érdemben segíteni nem tudtak. Hivatalosan, írásban tájékoztatást kértem a Terrorelhárítási Központtól abban a vonatkozásban, hogy hazánkban mi a rendje a terrorszervezetté nyilvánításnak, de időhiányra hivatkozva elutasítottak. Ennél fogva kutatásom során hivatalos szervek támogatására nem számíthattam.

A kutatás korlátai

Az adatgyűjtés során jellemzően szélsőséges iszlám terrorista tartalmakkal kerültem kapcsolatba, eközben azonban etikai megfontolásokból a terroristákkal mindennemű kommunikációt kerültem, ami a kutatás folytatásához szükséges információk, adatok beszerzését hátráltatta.

Büntetőjogi megfontolások

Az értekezésemben felhasznált terrorista tartalmak elérhetőségét szándékosan nem hoztam nyilvánosságra, mivel ez a 2012. évi C. törvény a Büntető Törvénykönyvről 331.§ (2) bekezdésében megfogalmazott törvényi tényállást valósította volna meg, amely szerint*:" (2) Az (1) bekezdés szerint büntetendő, ha súlyosabb bűncselekmény nem valósul meg, aki nagy nyilvánosság előtt a terrorizmus támogatására uszít, vagy egyébként a terrorizmust támogató hírverést folytat."* [83, 331.§ (2)]

Ennél fogva a releváns média tartalmakat képernyőfotóval az elérhetőségük nélkül, illetve szükség esetén a tartalom egy részének kitakarásával mutatom be.

Az adatgyűjtés során személyes adatokat nem kezeltem, természetes személyeket nem azonosítottam be.

A kutatás során alkalmazott technikai környezet kialakítása

A kutatási téma jellegéből adódóan olyan műszaki környezetet kellett kialakítanom, amely lehetővé tette a hatékony, ugyanakkor biztonságos kutatást. A többéves munka során nem lehetett szem elől veszíteni azt a körülményt, hogy a kutatási téma alapjául szolgáló tevékenységek bűncselekményt képeznek ennél fogva ezek előállítói, terjesztői olyan bűnözőknek minősülnek, akik az átlagos felhasználó szintjét jóval meghaladó informatikai tudással rendelkeznek. Mindezekre való tekintettel a technikai műszaki környezetnek biztosítania kellett az anonimitást és a földrajzi helyzetem névtelenségét, illetve a kutatás érdekében folytatott tevékenységem nyomon követésének akadályozását.

Doktori kutatásomat 2024. június 30-al zártam le.

I. FEJEZET

A TERRORSZERVEZETEK JELENLÉTE A DARK WEBEN

Feltételezhető, hogy az utóbbi néhány évben a közösségi médiában bevezetett korlátozó és tartalomszűrő intézkedések következtében a terrorszervezetek lehetőségei beszűkültek, ezért tevékenységüket az anonimitást, illetve cenzúramentességet biztosító dark weben folytatják

A dark web fogalmának és a kutatásomban vizsgált dark webes alkalmazások működésének valamint jellemzőinek bemutatásától értekezésemben terjedelmi okok miatt el kell tekintenem. Ezzel a témával kapcsolatban az alábbi publikációkat készítettem:

- Gulyás Attila:„The Dark Web” (Strategic Impact (Romania) 1841-5784 1824-9904, 77/2020/4.)
  Besorolás: nemzetközi „D”
- Besenyő János, Gulyás Attila: The effect of the dark web on the security (Journal of Security and Sustainability Issues 2029-7017 2029-7025 11/1).
  Hivatkozások száma: 12;
- Gulyás Attila: Vállatbiztonság és dark web (Biztonságtudományi Szemle, 3/3 2021)
  Besorolás: hazai „C”
- Gulyás Attila: Dark Web Investigation: edited by Babak Akhgar, Marco Gercke, Stefanos Vrochidis, and Helen Gibson, Switzerland AG, Springer Nature, 2021, ISBN 978-3-030-55342-5, $141.67(hardback), 305 pages’, Terrorism and Political Violence, 33(8), pp. 1807–1809. doi: 10.1080/09546553.2021.2000216.
  Besorolás: nemzetközi „Q2”
- Gulyás Attila: A dark web világos oldala (Ügyészségi Szemle 2559-8112, 8/1 2023)
  Besorolás: hazai „D”

1.1 Irodalmi áttekintés

A terrorszervezetek és a dark web közötti kapcsolat mélysége és lehetséges formái a témát kutató tudós társadalom körében heves viták melegágyát képezi. Egyes kutatók, mint Malik [1 pp. 17-23] és a témában széleskörű ismertségnek örvendő Weimann, [2 p. 133] azzal érvelnek, hogy a névtelenséget és földrajzi anonimitást, valamint cenzúra állóságot biztosító The Onion

Router nevű anonim számítógépes hálózat (a továbbiakban rövidítve: TOR) rendszer ideális közeget biztosít a terroristák számára tevékenységük zavartalan folytatására. Saltman a „Analysis of Online Extremism and How to Counter It” [3]. és Berton a “The dark side of the web: ISIL’s one-stop shop?”. [4 p. 1] azt állítják, hogy a szélsőséges iszlamista terrorszervezetek a rendvédelmi szervek és önkéntes hackerek ellentevékenységének hatására online tevékenységüket áttették a dark webre.

Malik és Weimann mindketten a 2015-ben bekövetkezett párizsi terrortámadást követően megjelenő Iszlám Államhoz kapcsolódó TOR rendszeren létrehozott weboldalt hozzák fel példaként. Az oldal elérhetőségének felfedezése Scot Terban kutatóhoz köthető, aki egy dzsihadista üzenőfalon bukkant rá az oldal hozzáférési adataira. [1 p. 18]

Úgy tűnik ebből az oldalból vonták le azt a következtetést, mely szerint a terrortámadást követő Iszlám Állam ellenes hacker kampány (Operation Paris (OpParis)) következményeként a terroristák kénytelenek voltak dark web felé fordulni.

Malik a már említett riportjának eredményeit úgy összegezte, hogy a terroristák többek között a közösségi média és a rendvédelmi szervek tartalomellenőrző rendszerének elkerülése érdekében használják a dark webet, illetve a toborzó tevékenységüket a nyílt internetes kapcsolatfelvételt követően a dark weben folytatják tovább. Megfigyelése szerint a terroristák a nyílt internetről eltávolított tartalmakat a dark weben, mint egyfajta biztonságos tárolóhelyen tárolják, ahol a rendvédelmi szervek a tárhelyhez nem férhetnek hozzá.

A dark web fogalmának meghatározása alapján megállapítható, hogy Malik [1 p.17] téved, amikor a tanulmányában összemossa a dark webet és a titkosított üzenetküldő alkalmazásokat, ezért a tanulmányában dark webes tevékenységéként azonosított hivatkozásai, amelyeket a terroristák az üzenetküldő alkalmazásokon (Telegram) folytattak nem vehetők a dark webes tevékenységek körébe. Ennek fényében a tanulmányában széleskörűnek nevezett dark webes tevékenység már jóval szerényebb méretűnek tűnik.

Weimann és Malik megállapításait és következtetéseit kétséggel fogadta Lakomy [5, pp. 2,5] arra hivatkozva, hogy a két kutató szinte semmilyen tényszerű bizonyítékkal sem tudja alátámasztani állításukat a terroristák dark web használatával kapcsolatban. Az ellentmondás feloldása érdekében Lakomy három időszakban: 2020. március és április, 2022. január és február, valamint 2022. május és június között megkísérelte feltérképezni a TOR rendszerben található szélsőséges iszlamista terrorszervezetek dark webes jelenlétét. Választ keresett arra, hogy a szélsőséges iszlám terrorszervezetek weboldalai hol helyezkednek el az adott szervezetek média ökoszisztémájában.

Lakomy kiterjedt keresést folytatatott a TOR népszerű keresőmotorjainak felhasználásával, a különböző nyílt internetes dzsihadista oldalakon történő TOR szolgáltatásra mutató linkek keresésével. A kutatása során megállapította, hogy a Weimann és Malik állításával szemben a dzsihadista szervezetek jelenléte a TOR rendszeren korántsem olyan széleskörű, mint azt a közösségi média és a rendvédelmi szervek tartalomszűrő tevékenysége indokolttá tenné. Megállapítása szerint a TOR szolgáltatások nem fő összetevői a dzsihadista médiaökoszisztémájának. Lakomy kutatása nagy bizonyossággal cáfolta azokat a feltételezéseket és elméleteket, amelyek szerint a terrorszervezetek átköltöztek volna a dark webre.

Lakomy kutatásának köszönhetően jelenleg két elmélet áll egymással szemben. A „nagy bizonyosság" kiegészítést nem véletlenül használtam, ugyanis Lakomy számos forrást, illetve olyan dark webes sajátosságot nem vett figyelembe a kutatása során, amelyek a képet árnyaltabbá tehetik és a bizonyosság valószínűségét megnövelik. A teljes bizonyosság megállapítása a dark web jellegéből adódóan lehetetlen, de legalább is kétséges. Azzal, hogy a kutatását csak a TOR rendszerre fókuszálta és nem vette figyelembe a rendszer sajátosságait, illetve a terroristák részéről azt a gyakorlatot, hogy a követőiket a nyílt webről vezetik a dark webre támadhatóvá tette a kutatásából levont következtetéseket. A jelzett hiányosságok mellett ugyanakkor nem vizsgálta az okokat sem, nem keresett magyarázatot arra, hogy amennyiben igaz a megállapítása, akkor az milyen okokra vezethető vissza. Milyen logikus magyarázattal indokolhatja megállapításait. Megítélésem szerint ezek hiányában a kép nem teljes és a megállapítása nem kellő mértékben megalapozott.

A hipotézisem igazolásának, vagy cáfolásának érdekében 2021. február 01-től 2024. június 30-ig terjedő időszakban folyamatosan kutattam a dark webet és napi szinten használtam a legnépszerűbb dark webes alkalmazásokat. Az 1. számú mellékletben található OSINT módszereknél leírt módon folyamatosan kutattam azokat a forrásokat, amelyek a dzsihadista terrorszervezetek dark webes jelenlétével kapcsolatba hozhatók lehettek, vagy erre vonatkozóan forrásként szolgálhattak. Lakomy kutatásának publikálását követően, megállapítottam azokat a hiányosságokat, amelyek miatt nem lehet kellő bizonyossággal kijelenteni az általa megfogalmazott állításokat. Ezt követően hipotézisem igazolása, vagy cáfolása, illetve a két nézőpont közötti ellentét feloldása érdekében kutatásomat olyan terv alapján folytattam, amelyben igyekeztem a jelzett hiányosságokat kiküszöbölni és a lehetőségekhez mérten objektív adatokat beszerezni.

1.2. A dzsihadista terrorszervezetekkel összefüggésbe hozható dark webes szolgáltatások felkutatása

1.2.1 A kutatás során vizsgált dark webes alkalmazások kiválasztása

A kutatásba bevont alkalmazások kiválasztását megelőzően 2020.október 01- és 2024. június 30. közötti időszakban folyamatosan használtam a TOR, az I2P, a Freenet és a Zeronet alkalmazásokat. A kutatásba bevont platformok kiválasztásánál a népszerűségüket, a felhasználótábor nagyságát, és az elérhető szolgáltatások számát vettem figyelembe[1]. Végül a Zeronetet[2] kihagytam a vizsgálatból, mivel a platform a fejlesztése 2021-ben megszűnt és bár a rendszer működik tovább, de biztonsági frissítések nem készültek és a rendszerben nyilvántartott szolgáltatások jelentős része már nem érhető el. A Zeronet hivatalos weboldalán nincs erre vonatkozó hivatalos közlés, azonban a programozói fórumok hozzászólásaiból arra lehet következtetni, hogy az egyébként magyar eredetű platform fejlesztője magára hagyta a projektet.

1.2.2 A kutatás során alkalmazott keresőkifejezések kiválasztásának szempontjai

A nyílt és a dark weben történő sikeres keresés végrehajtásának alapvető feltétele a megfelelő kereső kulcsszavak kiválasztása. A nem megfelelően kiválasztott kulcsszó használata vagy túl sok irreleváns, vagy túl kevés hasznosítható találatot eredményezhet. Ezért kerülni kell az olyan általános szavak kiválasztását, mint „islam", terror", „terrorist" és ehhez hasonlók. A jó kulcsszavak megtalálása elképzelhetetlen az adott szubkultúra nyelvezete, az általuk használt szófordulatok és slang kifejezések megismerése nélkül, ami feltételezte az idevágó szakirodalom tanulmányozását.

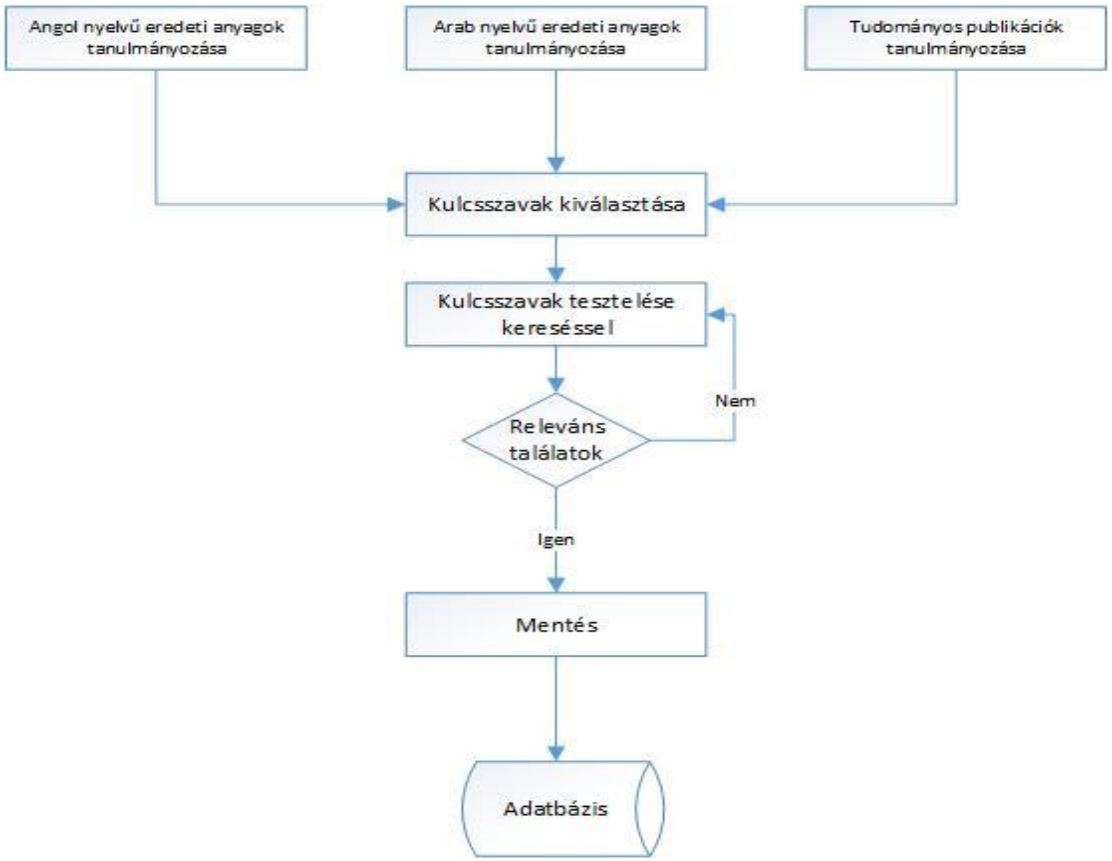
A vizsgált dzsihadista terrorszervezetek általában arab nyelven kommunikálnak, kiadványaik is leginkább az arab nyelvű közösséghez szólnak. A legismertebb ilyen kiadványok az „al Naba" (Iszlám Állam), vagy az „Ummah" (Al-Kaida), amelyeknek vannak ugyan idegen nyelvű fordításai is, de az eredeti kiadványok nyelve arab. Erre való tekintettel a kutatás során az angol mellett az arab nyelvű kulcsszavakat is gyűjtöttem.

A megfelelő keresőkifejezések kiválasztásának folyamata a 1. számú ábrán látható. A kutatás során fő forrásnak az arab és angol nyelvű eredeti tartalmakat, és a magyar valamint idegen

[1] 2023.11.30-án felhasználók száma: TOR: 4.300.000 fő, (https://metrics.torproject.org); I2P: 41623 fő (https://i2p-metrics.np-tokumei.net/network-size); Freenet: az elméletileg elérhető szolgáltatások száma 7.800. [14] Figueras M. E., Magán C. R., Boubeta P. J., "Drawing the web structure and content analysis beyond the Tor darknet: Freenet as a case of study," Journal of Information Security and Applications, vol. 68, p. 103229, 2022, doi: https://doi.org/10.1016/j.jisa.2022.103229

[2] https://www.reddit.com/r/zeronet/comments/xdsrlv/did_the_government_shut_this_project_down/?rdt=52156; https://github.com/HelloZeroNet/ZeroNet/issues/2749

nyelvű tudományos publikációkat választottam. A megfelelő kulcsszavak keresése nem egyszeri alkalom volt, hanem egy folyamat, amely magába foglalta a megszerzett információk és tartalmak elemzését és az ezekben esetlegesen található új kifejezések (valamint ezek esetleges kombinációjának) tesztelését, majd kedvező esetben az adatbázisba történő mentésüket. A vizsgált szervezetek weboldalai rendvédelmi szervek és a közösségi média korlátozó tevékenységének köszönhetően gyakran kénytelenek helyet változtatni és ezek újbóli megtalálása, vagy az esetleges új oldalak felderítése ugyancsak indokolttá teszi a keresés folyamat jellegének kialakítását.



1. ábra A keresőkifejezések kiválasztásának folyamata (a szerző szerkesztése)

1.2.3 A közösségi médiában folytatott keresés eredménye

Tekintettel arra, hogy a vizsgált szervezetek igyekeznek tartalmaikat minél szélesebb körben terjeszteni a hipotézis vizsgálatánál ezt a tényezőt is figyelembe kellett venni. Ennek megfelelően kiválasztottam azokat az alkalmazásokat, amelyek a legelterjedtebbek, legnépszerűbbek a felhasználók körében és a kutatásomat ezekre fókuszálva a már ismertetett módon kiválasztott kulcsszavak segítségével a kutatás időszakában rendszeresen hajtottam végre kereséseket a kutatásba bevont három dark webes alkalmazás vonatkozásában a

Facebook, Instagram, TikTok, és az „X” (korábban Twitter) alkalmazások felületein, illetve a Telegram nyílt webes csatornáin.

1.3 A TOR rendszerrel kapcsolatos kutatás

1.3.2 Kutatás dark webes tartalmak után a nyílt interneten

A vizsgált csoportok dark webes jelenlétének vizsgálata érdekében a kutatást a nyílt interneten kezdtem abból a feltételezésből kiindulva, hogy a szimpatizáns, vagy csak egyszerűen érdeklődő felhasználók is nagy valószínűséggel ebben a közegben kezdenek el az ilyen tartalmak után keresni. Ezt megalapozó másik feltételezésem szerint a vizsgált szervezetek is erről a platformról irányítják az érdeklődőket a számukra biztonságot nyújtó sötét web felé.

A terrorista tartalmak kutatásának sajátossága, hogy a felderített oldalak életciklusa gyakran változik. Az oldalak egyik napról a másikra elérhetetlenné válnak, ezért a Wayback Machine (Internet Archívum) használata elengedhetetlen. Ezt egyébként a terroristák követői, illetve szimpatizánsai is aktívan használják. A szolgáltatás üzemeltetője egy az Amerikai Egyesült Államokban működő non-profit alapítvány. A project létrehozásának célja egy olyan digitális „időgép” létrehozása, amely megmutatja, hogy a múlt adott időpontjában milyen volt az Internet. Az oldal a https://archive.org/web/ linket követve érhető el.

A legnépszerűbb keresőmotorok (Google, Bing, Yahoo, Yandex, DuckDuckGo, Yep, SwissCow, SearchEncrypt) és a Wayback Machine használatának kombinációjával összesen 61 Al-Kaidahoz, 71 Iszlám Államhoz, 15 Hezbollah-hoz, 16 palesztin dzsihadista szervezetekhez és 16 független dzsihadista szervezethez köthető weboldalt sikerült azonosítanom. A weboldalak elemzése során összesen négy különböző és működő dark webes oldalra történő hivatkozást találtam. Az oldalak valamennyien az Iszlám Államhoz köthetők.

Az első oldal az I’Lam alapítványhoz tartozik. Az oldal neve „Média mindenről, amit az Iszlám Állam adott ki több nyelven”. Az oldal a nevének megfelelően minden közlemény több nyelven történő megjelenítését tűzte ki céljául. Az értekezés készítésének időpontjában a weboldalon 23 nyelven voltak érhetők el a szervezet közleményei. A választék azonban folyamatosan bővül. Az olyan kevésbé elterjedt nyelvek, mint az albán, oromo, vagy kiswahili is megtalálható a gyűjteményben, hogy csak néhány példát említsek. Az oldal tökéletes másolata a https://I3lam.xxx linken megtalálható nyílt internetes weboldalnak.

A második weboldal az „Al Raud” média archívum, amely ugyancsak a tükörképe a https://rad.xxx linken található nyílt internetes oldalnak. Az oldal elsődlegesen arab nyelvű, de francia és angol nyelvű fordítások is találhatók rajta. A felhasználók megtalálhatják rajta az Iszlám Állam már megszűnt idegen nyelvű magazinjait, különböző hangfelvételeket,

ideológiai, vallási leckéket, előadásokat. Az Iszlám Állam központi könyvtárának elérhetőségét (al Himma).
A harmadik oldal neve „Muszlim hírek”, amely állítása szerint egy független híroldal, azonban főleg az Iszlám Állam kiadványai képezik a tartalom jelentős részét. Ennek az oldalnak a kutatásaim során nem találtam nyílt internetes megfelelőjét.
A negyedik oldal egy a hívőket támogató, segítő oldal, amely szintén arab nyelvű és a napi hírek, aktualitások mellett egyfajta kapcsolattartói csomópontként (hub) működik. A felhasználók az oldalról telegram csatornákat és nyílt internetes oldalakat érhetnek el azzal a figyelmeztetéssel, hogy a böngészés során használjanak virtuális magánhálózatot (VPN) a TOR rendszerrel kombinálva.
Az oldal a tükörképe a https://fahrxs.xxx linken található nyílt internetes weboldalnak.
A négy weboldallal kapcsolatban megállapítható, hogy naprakészek, folyamatosan új tartalmak jelennek meg rajtuk, amit alátámaszt az is, hogy az oldalakról elérhető az Iszlám Állam hivatalos kiadványának az „al Naba”-nak a legfrisseb száma.

A kutatás második fázisában a Wayback Machine (archiv.org) archívumában folytattam a kutatást, amely a dzsihadista terroristák egyfajta tartalomarchiváló és kapcsolattartó helyének számít. A kutatás során a már ismert kulcsszavak felhasználásával elsődlegesen 86 találatot vizsgáltam meg, a melyek további 72 találathoz vezettek. A különböző kulcsszavak használatának és a tartalomelemzésnek köszönhetően az összesen megvizsgált 158 oldalon az eddig megismert dark webes tartalmakhoz képest további két új oldalt sikerült felderíteni. Azonban ezek a kutatás ideje alatt nem működtek, így ezekkel kapcsolatban meta adatok hiányában további információkat beszerezni nem tudtam. Az archívum vizsgálata során figyelembe vettem azt a tényt, hogy a TOR jelenlegi címzési protokollja 2021. október 01-től érvényes így, a korábbi címek feltalálása esetén azokat már nem lehetett volna az ellenőrzés körébe bevonni, mivel a jelenlegi eszközökkel ezek már nem elérhetők, ezért korábbi időre történő visszatekintés érdemi eredménnyel nem járt volna. Másrészt figyelembe vettem, hogy a tapasztalataim alapján éppen a tartalommegőrzés és a folyamatos kapcsolat fenntarthatóságának érdekében a dzsihadista szimpatizáns felhasználók jelentős része egyfajta tartalomsokszorozó szerepet tölt be, tehát az új tartalmak helyett a meglevőket sokszorosítja és másolja. Erre a szerepkörre a későbbiekben a második hipotézis vizsgálatánál még részletesen visszatérek.

1.3.3 A TOR rendszerben használt keresőmotorok felhasználása

A kutatás következő fázisában a TOR rendszeren megtalálható legnépszerűbb, illetve leghatékonyabb keresőszolgáltatásokat vettem igénybe. A már korábban kiválasztott keresőkifejezésekkel a Torch", „Haystak", „Onion Search", "SearX", „TorDex" és az „Ahmia.fi" keresőmotorokat használtam. A felsorolt szolgáltatások közül az „Ahmia.fi" generált releváns találatokat, amelyek egy kivételével megegyeztek a nyílt internetes keresés eredményével. Az előző találatokhoz képest egyetlen új találatot kaptam, amely egy Al-Kaida szimpatizáns által létrehozott és üzemeltetett túlnyomórészt kiberbiztonsággal foglalkozó weboldal, azonban ennek tartalma már elavult, ugyanis a tartalmát 2020- óta nem frissítették. A „Kiberneti___" nevű webhely túlnyomórészt német nyelven készült, de arab nyelvű cikkek, is találhatók rajta. Az Iszlám Állammal kapcsolatba hozható többi dark webes webhellyel szemben ennek nyílt internetes megfelelője nincs.

1.3.4 A TOR rendszerben található linkgyűjtemények átvizsgálása

A keresőmotorok alkalmazását követően a TOR rendszerben található linkgyűjteményeket, illetve a legnépszerűbb nyilvános fórumokat kutattam át a dzsihadista TOR szolgáltatások után.

A linkgyűjtemények az egyik legfontosabb navigációs és tájékozódási pontok a világhálónak ebben a szegmensében. A legismertebbek és legátfogóbbak a „Hidden Wiki", „Uncensored Hidden Wiki", „Another Hidden Wiki", „Onion Links", „OnionLinks v3", „Tor Links", „Daniel — all the dark web links you're looking for", „Shadow Wiki", hogy csak néhányat említsek. A linkgyűjteményeket követően a szélsőséges szubkultúrában ismert népszerű úgynevezett „image chan" -eket, vagy „image board"-okat vettem sorra. Az „endchan", „8chan", „4chan", „nanochan", „picochan", „256 chan", majd az anonim „kérdezz- felelek" oldalak következtek, mint a „hidden anwers" és a „dread". A két kategória tanulmányozása során egyetlen alkalommal sem találtam dzsihadista dark webes tartalmat. A felsorolt linkgyűjtemények, illetve fórumok szabályzatát tanulmányozva megállapítható, hogy a nem tolerálják a gyermekpornográfiával, illetve a szélsőséges iszlám nézetekkel kapcsolatos tartalmakat, annak ellenére, hogy érdekes módon a felsoroltak kivételével az oldalakon folytatott tevékenységek a bűncselekmények gyakorlatilag teljes spektrumát lefedik.

1.3.5 A saját összeállítású TOR szolgáltatások gyűjteményének átvizsgálása

A kutató munkám során folyamatosan végzett gyűjtőmunka eredményeként sikerült egy több ezer linkből álló gyűjteményt összeállítanom, amelynek teljes körű tanulmányozására a gyűjtés időszakában nem volt lehetőségem. A nagy mennyiségű adat ellenőrzése emberi erővel –

figyelembe véve a TOR rendszer sebességét – nem kivitelezhető, ezért a Python nyelven scriptet készítettem, amely automatikusan ellenőrizte a linkek működőképességét, a linkeken található weboldalak tartalmát és amennyiben a valamely releváns kulcsszóval kapcsolatos oldalt talált, azt külön elmentette. Ettől függetlenül az oldalon előforduló leggyakoribb 10 szót (nem számítva a kötőszavakat, segédigéket) szintén elmentette a későbbi felülvizsgálat megkönnyítése érdekében. Ezzel a módszerrel ki lehetett szűrni az olyan trükköket, ahol egyes weboldal üzemeltetők például gyermekpornót tárolnak és a terrorizmussal kapcsolatos keresésekre is az ő oldaluk jelenik meg találatként. Ilyen módon el tudtam kerülni, hogy személyesen keressek fel illegális tartalmat a dark weben. A nagy volumenű keresés ellenére ez a módszer releváns találatot nem eredményezett.

1.4 Az I2P rendszeren történő kutatás

I.4.1 Az I2P vonatkozású kutatás a nyílt interneten

A TOR rendszerrel kapcsolatos nyílt internetes kutatást az Az Invisible Internet Project (a továbbiakban röviden: I2P) rendszer vonatkozásában is több alkalommal is megismételtem. A közösségi médiaalkalmazásokban, illetve a népszerű nyílt internetes keresőkben a már korábban kiválasztott keresőkifejezésekkel végrehajtott keresések az I2P rendszerben létrehozott „eepsites” szolgáltatások vonatkozásában releváns találatot egyik alkalommal sem eredményezett.

1.4.3 I2P keresőmotorok használata

Az I2P rendszerben hasonlóan a TOR rendszerhez nincsenek a nyílt interneten megszokott hatékonyságú keresőmotorok, így már ismertetett módon kiválasztott kulcsszavakkal a legnépszerűbb keresőmotorokat használtam „I2P Search Engine”-t (https://i2pengine.com/), I2PFind (http://i2pfind.i2p/), legwork (http://legwork.i2p), Seeker (http://seeker.i2p), azonban releváns találat nem keletkezett.

1.4.4 I2P linkgyűjtemények átvizsgálása

A legfőbb tájékozódási alap ezen a területen a linkgyűjtemények átvizsgálása a tanulmány szempontjából releváns tartalmak felkutatására. Tekintettel arra, hogy ez a rendszer jóval kisebb népszerűségnek örvend, mint a TOR így a felhasználók és a szolgáltatások száma is jóval szerényebb méretű. A keresés első részében a beépített címjegyzék mintegy 7090 bejegyzését ellenőriztem, majd a rendszeren a legjelentősebb linkgyűjtemény a „Not Bob Lives here” (http://notbob.i2p/) és a reg.i2p (http://reg.i2p/all) következett, amelyek egyben egyfajta címjegyzék referenciák is, ahol az egyes oldalak tematikusan, illetve státuszuk szerint kerültek csoportosításra. Az oldalak volatalitását mutatja, hogy a kutatás időtartama alatt az

adatbázisban összegyűjtött mintegy 7300 oldalból mindössze átlagban 750 volt elérhető, ebből átlagban körülbelül 600 oldal minősül stabilnak, ami azt jelenti, hogy legalább 24 órája online van. A felhasználók körében népszerű további linkgyűjtemény az „eepstatus" (http://eepsites.i2p/) automatikusan karbantartott gyűjtemény, amely átlagban közel 360 oldalt tárol. Az oldalak a tulajdonosaik bejelentése alapján kerülnek az adatbázisba. A webszolgáltatás csak az oldalak elérhetőségét vizsgálja, a tartalmukat nem ellenőrzi.

A keresések és a linkgyűjtemények ellenőrzését követően a különböző imageboard-ok és fórumok témáját vizsgáltam át. Ezek sorban: 3ch (3ch), 9chan (http://9ch.i2p), Riot (http://riot.I2P), Discuss.i2p (http://discuss.i2p), Coffechan (coffeechan.i2p)

A közösségi oldalak I2P klónjai közül az X (régi nevén Twitter) megfelelőjén a Natteren (http://natter.i2p), a Facebook megfelelőjén a visibility (http://visiblity.i2p) oldalon a keresés eredménytelenül zárult.

A felsorolt eljárások alkalmazásával végrehajtott keresések egyetlen releváns találatot sem eredményeztek.

1.5 Freenet rendszer

A Freenet rendszerben, akárcsak a többi vizsgált dark webes közegben a hagyományos keresőmotorok nem érhetők el. Hasonlóan a TOR és az I2P környezethez a felhasználónak magának kell gondoskodni az általa létrehozott tartalom elérhetőségének terjesztéséről. Önkéntesek által létrehozott listák, hivatkozásgyűjtemények szolgáltatják az alapját a Freeneten történő tájékozódásnak.

1.5.1 Kutatás a nyílt interneten

A kutatás ebben az esetben is a nyílt interneten és a közösségi médiában történő kereséssel kezdődött. A már ismertetett módon a korábban kiválasztott kulcsszavak és keresőkifejezések használata a kutatás szempontjából releváns eredménnyel nem járt.

1.5.2 Freenet keresőmotorok használata

A Freenet rendszerben végzett kutatás során először a beépített Search Freenet (Library 36) nevű keresőmotor használatával kezdtem, azonban ez teljes mértékben használhatatlannak bizonyult, mivel a legegyszerűbb általános keresőszavakra sem adott releváns találat-gyakorlatilag nem működik, a rendszerben más kereső motor nem üzemel.

1.5.3 Linkgyűjtemények átvizsgálása

A keresőmotor után a következő linkgyűjteményekhez fordultam:

- Spider Freefiles list (uncensored list)

- Freefiles Graveyard (kulcs nélküli fájlok gyűjteménye, helyreállításuk lehetősége kétséges)
- „The Ultimate Freenet Index”
- YAFI (Yet Another Freenet Index) gyűjtemény
- saját linkgyűjtemény, amely 12917 linkből álló SQL alapú adatbázis

A fenti teljes állomány ellenőrzése úgy tűnik, hogy lefedte az elérhető oldalak számát tekintve, hogy Figueras et al 2020-as kutatása során 7150 élő oldalt tudott azonosítani. [6]

A linkgyűjteményekben folytatott kutatás alkalmával rábukkantam az Al Kaida in Arabian Peninsula (AQAP) 2010 és 2013 között kiadott, azóta már megszűnt „Inspire” magazinjainak tárhelyére. Ezzel kapcsolatban meg kell jegyeznem, hogy a tárhely melletti szövegkörnyezetből valószínűsíthető, hogy nem terrorista propaganda célzattal töltötte fel az ismeretlen, hanem inkább érdekesség, különlegességként. A feltöltő figyelmezteti a felhasználókat, hogy a szóban forgó kiadványok birtoklása az Egyesült Királyság törvényei szerint bűncselekménynek minősül. A tárhelyről készült képernyőfotó az 2. számú ábrán látható.

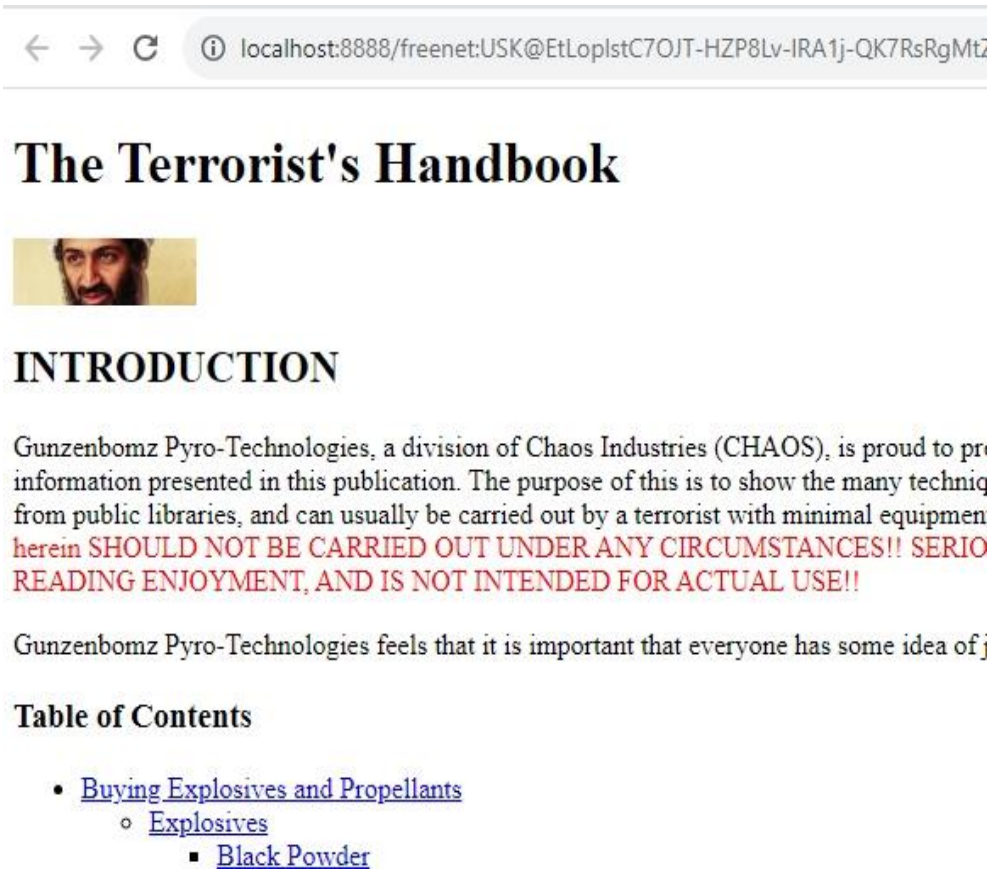
2. ábra Az Al-Kaida "Inspire" maganzinjának elérhetősége a Freeneten. Forrás: A szerző képernyőfotója

A másik releváns találat az Abdel –Aziz által jegyzett „The Mudjahideen Poison Handbook” című kiadvány. A 3. ábrán látható a könyvben receptek találhatók az emberi élet kioltására alkalmas különféle szerves és szervetlen mérgek előállítására, illetve ezek legcélszerűbb felhasználási módjára vonatkozóan. A webhely csak és kizárólag ezt a kiadványt tartalmazza, ezen túl semmilyen más közlés, ideológiai utalás nem található. Szigorúan véve nem lehetünk biztosak abban, hogy valamilyen terrorszervezethez köthető személy töltette fel, hiszen történhetett ez pusztán az érdekessége miatti megosztás céljából is. Hasonló a helyzet „Terrorist’s handbook” esetében is, amelyet a „Gunzenbomz Pyro-Technologies, a division of a Chaos Industry (CHAOS)” jegyez. A kiadvány mellé fűzött megjegyzés szerint céljuk a könyv

elkészítésével annak bizonyítása, hogy nem szükséges szofisztikált eszköz és háttér ahhoz, hogy az itt leírt eszközöket és módszereket bárki politikai vagy vallási célja érdekében alkalmazhassa. Állításuk szerint ezek az információk nyilvánosan közkönyvtárakban elérhetők, ők mindössze egy kötetbe rendezték azokat. A felhasználók figyelmét felhívják azonban arra, hogy ez csak ismeretterjesztő célból készült az információkkal való visszaélésért semmilyen

3. ábra The Mujahideen Poisons Handbook a Freenet hálózaton forrás: a szerző képernyőfotója

felelősséget nem vállalnak. A weboldalról készített képernyőfotó a 4. számú ábrán látható.



4. ábra Terrorist handbook a Freeneten forrás: A szerző képernyőfotója

A kutatás során egyértelműen dzsihadista tartalomként azonosítottam a „Military Studies in Jihad Against the Tyrants" című könyvet, amely az Al Kaida harcszabályzataként értelmezhető. A könyv sorra veszi azokat a képességeket, amelyek szükségesek ahhoz, hogy valaki egy terrorszervezet tagjává váljon, majd tizennyolc leckén keresztül végig vezeti az olvasót a terroristává váláshoz szükséges ismeretek átadásával. A weboldal környezete és a könyv tartalma egyértelműen arra utal, hogy a webhely tulajdonosa az Al Kaida aktivistája. Az oldalról készült képernyőfotó a 5. számú ábrán látható.

5. ábra Al Kaida Military Studies a Freenet hálózaton forrás: a szerző képernyőfotója

A felsorolt tartalmakkal kapcsolatban sajnos nem állapítható meg a feltöltés ideje, illetve a feltöltőkkel kapcsolatos további információk beszerzésére sem volt mód.

A Freenet tekintetében mindösszesen az Al Kaidával kapcsolatba hozható oldal azonosítható egyértelműen szélsőséges dzsihadista tartalomnak, a többiek megítélése legalább is kétséges. Az előtalált tartalmakkal kapcsolatban konkrét látogatási adatokat a Freenet természetéből adódóan nem nyerhetünk ki, azonban az a tény, hogy napjainkban is elérhetőek arra enged következtetni, hogy a felhasználók közelebbről meg nem határozható számban rendszeresen felkeresik ezeket az oldalakat, ugyanis ha nem így lenne, akkor a hálózat természetéből adódóan néhány hónap múlva már elérhetetlenek lennének.

1.6 Az alacsony szintű dark web használat okai

Felmerül a kérdés, hogy a terrorszervezetek miért csak ilyen alacsony mértékben használják ki a dark web anonimitásával és cenzúraállóságával járó előnyöket?

A válasz elsősorban a dark web nyújtotta alacsony sávszélességben rejlik. A néhány százkilobájtos átviteli sebesség szinte lehetetlenné teszi terrorszervezetek számára oly fontos videó összeállítások megtekintését, nagyméretű fájlok letöltését. A dark webes alkalmazások az adatok védelme érdekében többszörös titkosítási eljárásokat alkalmaznak és a forgalmat platformtól függően több számítógépen (útválasztón) keresztül továbbítják, ami lényeges sávszélesség csökkenéssel jár.

A másik tényező a felhasználók részéről elvárt magasabb számítástechnikai ismeret. Ezeknek a rendszereknek a kezelése, kiváltképpen a dark webhelyek üzemeltetői részéről az átlagot jóval meghaladó felhasználói ismereteket követel, különösen igaz ez az I2P és a Freenet rendszerek esetében.

A felhasználóik számára az anyagi lehetőségeiktől és a fenyegetési modelljüktől függően az alábbi alternatívákat javasolják:

- A felhasználó anonim VPN előfizetés nélkül használja a TOR rendszert a nyílt weboldalak megtekintésére (ez esetben az internetszolgáltató látja a hálózaton a TOR forgalmat, bár annak címzettjét és tartalmát nem ismerheti meg).
- Anonim VPN előfizetés hiányában a TOR rendszeren keresztül felkeresheti a dark webes oldalakat (ebben az esetben csak úgy, mint az első esetben a TOR használat kimutatható, de a kommunikáció többi része rejtett marad).
- Amennyiben rendelkezik anonim VPN előfizetéssel akkor azon keresztül keresheti fel a nyílt weboldalakat (az internetszolgáltató nem ismerheti meg a kommunikáció tartalmát és címzettjét).
- Anonim VPN előfizetés esetén a TOR rendszeren keresztül felkeresheti a nyílt weboldalakat (az internetszolgáltató elöl továbbra is rejtve marad a kommunikáció tartalma és címzettje, valamint a TOR rendszer használatának ténye).
- A legbiztonságosabb esetben az anonim VPN használatával a TOR rendszeren keresztül a dark webes weboldal felkeresése (ebben az esetben rejtve marad a TOR rendszer használata, a kommunikáció tartalma, címzettje).

A felsorolt esetekben közös vonásnak tekinthetjük, hogy a szolgáltatás (weboldal) üzemeltetője számára a felhasználó IP címe ismeretlen marad.

1.7 Összefoglalás

A hipotézisem megerősítése, vagy megcáfolása és a tudományos életben létrejött ellentmondás feloldása érdekében megítélésem szerint az elérhető eszközök lehető legteljesebb spektrumának felhasználást követően sikerült átfogó képet kapni dzsihadista terrorszervezeteinek dark webes jelenlétéről. A kutatás gerincét a kutatásetikai és törvényi előírások betartása mellett a nyílt forrású információgyűjtés eszközeinek és módszereinek célirányos és feladatorientált alkalmazása képezte. A széleskörben lefolytatott kutatás eredményeként mindössze néhány olyan weboldalt sikerült felderíteni, amelyek a dark weben működnek, ezek közül is mindössze négyről állapítható meg, hogy az üzemeltetőik napi rendszerességgel karbantartják, tartalmukat frissítik. Ezek az oldalak az Iszlám Államhoz kötődnek, míg a két Al Kaidához köthető oldal esetében nincs nyoma a napi karbantartásnak, tartalomfrissítésnek. A kutatás során más, egyértelműen szélsőséges iszlám terrorszervezethez köthető weboldalt nem sikerült felderíteni.

A felderített és napi szinten aktualizált és karbantartott dark webes oldalak tartalmának elemzését követően megállapítható, hogy ezek a nyílt weben található oldalaik tükörképei. Valószínűsíthetően az oldalak létrehozásának többszörös célja van. Egyrészt lehetőséget biztosítanak a jelentős fenyegetési modellel rendelkező szimpatizánsoknak a biztonságos tartalomeléréshez, másrészt tartalékul szolgálnak arra az esetre, ha a hatóság lefoglalná a nyílt internetes oldalakat. A dark webes tartalékok segítségével könnyen, tartalomvesztés nélkül egy másik címen újra éleszthetik a nyílt internetes szolgáltatásukat. Harmadrészt biztosítják a nyílt webes oldalak elérhetőségének folyamatosságát azáltal, hogy feltüntetik az oldalak új elérhetőségét segítve ezzel követőik tájékozódását.

A fentiek alapján a kutatásom során összegyűjtött adatok elemzését követően hipotézisemet, mely szerint

"Feltételezhető, hogy az utóbbi néhány évben a közösségi médiában bevezetett korlátozó és tartalomszűrő intézkedések következtében a terrorszervezetek lehetőségei beszűkültek, ezért tevékenységüket az anonimitást, illetve cenzúramentességet biztosító dark weben folytatják."

cáfolom

A széles körben végzett dark webes és nyílt internetes kutatás alapján megállapítható, hogy téves az a feltételezés, amely szerint a dzsihadista szélsőséges iszlám terrorszervezetek a nyílt interneten tapasztalható fokozódó rendészeti nyomás és tartalomszűrő intézkedések hatására internetes tevékenységüket áttették a dark webre. Azzal, hogy a kutatásom körébe a nyílt interneten található weboldalakat, a legkedveltebb közösségi média platformokat, és a legnépszerűbb dark webes alkalmazásokat is bevontam a Lakomy által tett megállapításokat sikerült megerősítenem és megalapozottabban sikerült igazolnom, egyúttal Weinman és Malik állításait pedig cáfolnom.

II. FEJEZET

CENZÚRA ELLENES TECHNIKÁK ÉS ELJÁRÁSOK AZ ONLINE TÉRBEN

Feltételezhető, hogy a szélsőséges iszlám terrorszervezetek olyan technikákkal, taktikákkal és eljárásokkal rendelkeznek, amelyek segítségével a nyílt internet és a dark web előnyeit mesterien kihasználva a közösségi média tartalom szűrőit és a rendvédelmi szerveket kijátszva képesek biztosítani folyamatos jelenlétüket a világhálón

A hipotézis igazolásával kapcsolatos kutatáshoz szükséges nyílt forrású információgyűjtéssel és annak automatizációs lehetőségeivel, valamint konkrétan a kutató munka során tett megállapításaimmal kapcsolatban az alábbi cikkeket publikáltam:

- Gulyás Attila: A nyílt forrásból származó adatgyűjtés automatizálásának lehetőségei
  Belügyi Szemle: A Belügyminisztérium Szakmai Tudományos Folyóirata (2010-) 71 : 7 pp. 1237-1269. , 33 p. (2023)
  Besorolás: hazai „A”

- Gulyás, Attila ; Demeter, Márton ; Besenyő, Janos:
  The Lernaean Hydra on the internet: Deplatformization-resistant media ecosystem of the Islamic State, Media War and Conflict 16 : 4 p. 9 Paper: OnlineFirst (2023) DOI WoS Scopus
  Besorolás: külföldi „Q1”

- Besenyő, János; Gulyás, Attila ; Trifunovic, Darko:
  Hezbollah and the Internet in the Twenty-First Century
  International Journal Of Intelligence And Counterintelligence online pp. 1-17. , 17 p. (2022) DOI WoS Scopus.
  Besorolás: nemzetközi „Q3”
  Hivatkozások száma: 9

Bevezetés

Az utóbbi három évtizedben lezajlott technológiai fejlődés eredményeit a szélsőséges iszlám terrorszervezetek is felismerték és az új lehetőségekhez alkalmazkodva folyamatosan fejlesztették és fejlesztik ma is képességeiket és hatékonyságukat. Az új technológiák és alkalmazások felhasználásával egyszerre nagyszámú felhasználót érhetnek el és szólíthatnak meg, illetve egymással is egyszerűbben és biztonságosabban tarthatnak kapcsolatot. A terrorszervezetek tevékenysége az interneten a United Nations Office on Drugs and Crime

(röviden: UNODC) [7] jelentése szerint hat egymástól szorosan el nem választható kategóriára terjed ki. Ezek nem fontossági sorrendben az alábbiak:

- a propaganda, amely magába foglalja a toborzást és radikalizácót,
- a pénzügyi alapok megteremtése,
- a kiképzés,
- titkos kommunikáció,
- a tervezés,
- a végrehajtás,

A szervezet a hatodik kategóriába sorolja a kibertámadásokat is, azonban ezek megítélésem szerint ez idáig nem jellemzők a terrorszervezetekre, bár kétségtelen, hogy elméletben fennáll az ilyen támadások lehetősége. [8 p.71]

A terrorszervezetek internetes tevékenysége bűncselekménynek minősül, ezért a rendvédelmi szervek egyik kiemelt feladata az ilyen tevékenységek, korlátozása, illetve megszűntetése. Ilyen körülmények között nem lehet vitatni Weinmann megállapítását miszerint a közösségi média vált a terrorizmus elleni harc egyik legfőbb színterévé. [9] Figyelembe véve, hogy a terrorszervezetek megítélése számos esetben a szervezettől és az adott országtól függően változhat, igyekeztem úgy megfogalmazni a hipotézisemet, hogy abban a vizsgált szervezetek megítélése ne számíthasson bizonytalansági tényezőnek és hazánkban egyértelmű legyen a megítélése. Úgy véltem továbbá, hogy a számos szélsőséges, esetenként szétforgácsolt, iszlamista terrorszervezetek tevékenységének egyenkénti felméréséből nem származna teljes értékű megoldás, mivel ezek nincsenek olyan nyomás alatt, mint a szélsőséges iszlamista terrorszervezetek médiatevékenységének mintaképe az Iszlám Állam és bizonyos vonatkozásokban az Al Kaida, valamint ezek társult szervezetei. Az előbbi szervezetek a kisebb nyomás miatt nem is kényszerülnek az elkerülési technikák és eljárások széles skálájának alkalmazására. [10, p. 3.] A felsorolt szempontok, illetve a értekezés terjedelmi korlátai miatt döntöttem úgy, hogy elsősorban az Iszlám Állam internetes tevékenységét vizsgálom.

2.1 Szakirodalmi áttekintés

Az Iszlám Állam Internetes tevékenységével kapcsolatos szakirodalom áttekintése

Az Iszlám Állam 2014-2015. között fejtette ki a legaktívabb tevékenységet az interneten. Gyakorlatilag uralta az statikus weboldalaktól kezdve a fórumokon át a közösségi médiát és a Twittert. A szakértők ezt az- időszakot a Virtuális Kalifátus létrehozásának és virágkorának tekintik. [11] A hatékony tevékenység egyik mérhető paramétere a toborzás hatékonysága. A Virtuális Kalifátus több mint nyolcvan országból harmincezernél is több harcost, illetve szimpatizánst beleértve nőket és gyerekeket toborzott túlnyomórészt a világhálón keresztül [12 p. 2.],[13 p. 2] Az Iszlám Állam hatalma csúcsán elárasztotta az online médiát az üzeneteivel.

Naponta ezrével posztolt a Twitteren, illetve a Facebookon, Instagramon. Számos kutató, így többek között a nemzetközi hírnévnek örvendő Winter [14], [15] ebben az időszakban a szervezet narratívájának megértésére koncentrált és sikerének titkát kutatta, mivel korábban ilyen méretű és sikeres propagandagépezet működtetésére nem volt példa.
Egy tanulmány szerint a 2014. szeptember és december közötti időszakban több mint 46.000 Iszlám Államhoz köthető Twitter felhasználói fiók volt aktív. [16 pp.2-3] Az olyan közösségi média platformok, mint a Facebook, Twitter, Instagram szerepe a közönség összegyűjtése volt. Winter, Berger és Morgan tanulmányaikban rámutattak arra, hogy terroristák közel egy évtizeden keresztül ezeken a platformokon gyűjtötték és irányították az érdeklődőket offline és online toborzó helyekhez azzal, hogy elérhetőséget adtak és utat mutattak a radikalizálódáshoz vezető további tartalmakhoz.[16], [17],[18]

Tagadhatatlan, hogy az Iszlám Állam 2019-ben bekövetkezett területi vesztesége és a média személyiségei ellen indított fizikai megsemmisítő csapások csökkentették a rendelkezésre álló lehetőségeiket és forrásaikat, ugyanakkor ez nem jelentette a tevékenységük beszüntetését. Lakomy a „The virtual "Caliphate" strikes back? Mapping the Islamic State's information ecosystem on the surface web” című tanulmányában rámutat arra, hogy a területi veszteségekkel párhuzamosan az Iszlám Állam online jelenléte csökkent, ami együtt járt azzal, hogy a tudományos élet és a kutatók érdeklődése is csökkent a szervezet internetes tevékenysége iránt, holott az még mindig jelentős kockázatot hordozott magában, mint ahogy erre az Európában bekövetkezett terrorcselekmények is rávilágítottak. [19 p.2] A korábbi népszerű platformok elhagyását követően a rendvédelmi szervek igyekeztek a titkosított csatornák üzemeltetőinél is elérni a szélsőséges iszlamista tartalmak kiszűrését, kitiltását így aztán az addig menedékhelynek számító Telegram is meghajolt akaratuk előtt és az Europollal együttműködve 2019-ben két hullámban is nagy tisztogatást végzett, amelynek keretében több ezer nyilvános szélsőséges dzsihadista csatornát számolt fel. [20]

Az Iszlám Állam média és internetes tevékenysége megalakulásától kezdve folyamatosan változik, fejlődik. Kadivar a „Daesh and the Power of Media and Message” című tanulmányában rávilágít, hogy a szervezet hatalmának egyik fő forrása a média, amelyre a vezetése nagy hangsúlyt fektet. Kadivar [21 p. 65], valamint Singer és Brooking, [13 pp. 213-215] szerint az Iszlám Állam kiadványai tartalmukban és megjelenésükben a nyugati média filmes eszközeinek széles tárházát alkalmazzák. A kiadványok alapvetően két nagy csoportra oszthatók úgymint hivatalos és nem hivatalos kiadványok. Az Iszlám Államnak vannak

hivatalos és nem hivatalos médiaügynökségei is, amelyek kiegészülnek az önkéntes médiaharcosok tartalomsokszorzó és esetenként önálló tartalmakat előállító tevékenységével. [21]. Kadivar média stratégiával kapcsolatos megállapításait megerősíti a „Salafi-jihadism and digital media" című tanulmányában Weimann et al [22 pp.132-157], akik szerint a szervezet felismerte, hogy a különböző felhasználói elvárások és a média formátumnak legjobban megfelelő platformok kiválasztása lényeges eleme a tartalmaik minél hatékonyabb terjesztésének.
A tartalomterjesztésre a közösségi média tökéletes közegnek minősül, hiszen a lájkolás és megosztás funkció segítségével az alany is a propaganda részévé válik. Winter a „Media Jihad" [14] című tanulmányában és a Saltmannal közösen írt cikkében [75] a szervezet információs hadviselésének sikerét jelentős részben az önkéntes médiaharcosokban látja, akiket az Iszlám Állam vezetése ugyan olyan fontosnak ítél meg, mint a fegyveres harcban résztvevő katonái.

Az Iszlám Állam lehetséges média stratégiáját Meili Criezis vizsgálta a „Create, Connect, and Deceive: Islamic State Supporters' Maintenance of the Virtual Caliphate Through Adaptation and Innovation" című tanulmányában. A tanulmányban azt vizsgálta, hogy a szervezet hivatalos és nem hivatalos tagjai, illetve szimpatizánsai milyen módon igyekeznek kapcsolatban maradni, hogyan próbálják kijátszani a különböző tartalomkorlátozó intézkedéseket. [23]

Lakomy tanulmányaiban [19] és [24 pp. 6-9] valamint Fisher és társai [25] feltérképezték az Iszlám Állam nyílt és dark webes ökoszisztémáját, azonban megítélésem szerint ezzel csak az Iszlám Állam cenzúraellenes törekvéseinek csak egy részét fedték fel. Az általuk megállapítottak – bár kétségtelenül rendkívül hasznosak – nem elegendőek ahhoz, hogy az Iszlám Állam internetes tevékenységének teljes spektrumát feltárják és magyarázatot adjanak arra, hogy hogyan képes a szervezet ilyen fokú ellentevékenység mellett is a folyamatos, jó minőségű online jelenlétét biztosítani. Pusztán a weboldalak, Telegram fiókok felsorolása és a közöttük lévő esetleges kapcsolatok bemutatása valójában csak egy szelete az Iszlám Állam által létrehozott és működtetett rendszernek.
Tekintettel arra, hogy az előzőekben hivatkozott kutatók által használt eredeti tartalmak elérhetőségei büntetőjogi és erkölcsi megfontolásokból nem publikusak, ezért ahogy már korábban utaltam rá kénytelen voltam saját adatbázist létrehozni, amely lehetővé tette, hogy a rendszert egészében vizsgálhassam.

2.2 A szélsőséges iszlám terrorszervezetek elleni online harc eszközei és célja

Az elmúlt évtized utolsó harmadára az online térben a szélsőséges iszlám terrorszervezetek tevékenysége olyan mértéket öltött, amely már az Egyesült Államok kongresszusában is egyre többször került szóba firtatva a rendvédelmi szervek és a közösségi média érdekelt szereplőinek szerepét és felelősségét. A Facebook és a Twitter többször is a kongresszusi képviselők kereszttüzében állt a nyíltan elérhető és terjedő szélsőséges iszlamista ideológia és propaganda elleni nem kellően hatékony ellenintézkedések miatt. [26] A küzdelem nehézségét jól érzékelteti, hogy 2019-ben a felhasználók **percenként** 474.000 Twitter üzenetet, 510.000 Facebook hozzászólást posztoltak és közel 300 óra videót töltöttek fel egyedül csak a YouTube-ra. [27] Egyedül a Twitteren 2015 közepe és 2016. eleje között több mint 125.000 Iszlám Államhoz köthető felhasználói fiókot blokkoltak. [16 p. 4] A számok alapján könnyen belátható, hogy milyen nagyságrendű feladattal néztek és néznek napjainkban is szembe, mikor a szélsőséges iszlamista terrorszervezetek tevékenységét szándékoznak korlátozni, illetve megakadályozni. Az ilyen mennyiségű információ feldolgozása, kiszűrése meghaladja az emberi teljesítőképesség és a szolgáltatók erőforrásainak határát, ezért kihasználva a gépi tanulásban rejlő lehetőségeket napjainkra egyre inkább jellemző a mesterséges intelligencia bevonása a közösségi média tartalom szűrésébe annak minden előnyével és hátrányával egyetemben. Tartalomszűrő robotok pásztázzák a platformok tartalmait, azonban ezek még nem érték el azt a fejlettségi fokot, hogy teljesen önállóan működjenek, és megnyugtató hatékonysággal kiszűrjék a káros tartalmakat. A „szoftveres cenzorok” viszonylag könnyen megtéveszthetők, hiszen nem tudják kezelni az úgynevezett ”virágnyelvű” beszélgetéseket az emojikat, vagy akár az úgynevezett homoglifák (amikor a betűt egy hasonló karakterrel helyettesítik) használatát. A mesterséges intelligencia kijátszási lehetőségeire a későbbiekben még részleteiben kitérek. A káros tartalmak tömeges megjelenésének kezelésére a nagy technológiai cégeknek (Microsoft, Google, Meta, stb.) két módszer áll a rendelkezésére.

2.2.1 Deplatforming és deplatformization

Mielőtt tisztáznám a két fogalom a jelentését, először látni kell, hogy mi is az a platformization, amely magyarul talán ebben az összefüggésben jobb szó híján az online infrastruktúra létrehozásának fordítható. Ez a jelenség arra utal, hogy az öt nagy technológiai óriás a Google, Apple, Facebook, Amazon, Microsoft röviden GAFAM gyakorlatilag megkerülhetetlenné vált azáltal, hogy egy a világot átszövő többszörösen összetett információs és technológia ökoszisztémát hozott létre. Az operációs rendszereik, a felhőszolgálatatásaik,

infokommunikációs eszközeik, kommunikációs platformjaik markáns részét képezik az online térnek. Ebben a környezetben kell különbséget tennünk a deplatforming az eltávolítás, kizárás, kiszorítás és a deplatformization között, ahogy azt José Van Dijck et. al. javasolja. [28]
A deplatforming fogalom mögött tulajdonképpen az a folyamat áll, amikor a radikális tartalmakat, illetve ezek terjesztőit kitiltják a platformról, vagyis megtagadják tőlük az online működéshez szükséges erőforrásokhoz való hozzáférést. Esetenként a szabályszegés súlyosságától, illetve gyakoriságától függően a felhasználói hozzáférés bizonyos időre történő korlátozása is szóba jöhet. Ennek médiumonként különböző módjai és fokozatai vannak, hiszen adott esetben csak a tartalmat törlik, vagy törlik és figyelmeztetik a felhasználót, esetleg felfüggesztik a felhasználói profilját egy bizonyos időszakra, vagy szélsőséges esetben ki is tilthatják a közösségből. Egyes platformokon kisebb nagyobb eredményességgel, de lehetőség van felülvizsgálat kérésére. Példaként a Facebookot hozhatnánk, ahol bevezették a felülvizsgálati lehetőséget és az első kilenc hónapban összesen több mint 524 ezer felülvizsgálati kérelmet kaptak. A társaságok 2016 előtt főleg a kalóz, illetve a terror jellegű tartalmak eltávolítására fókuszáltak, azonban ez ma már kiegészült a társadalomra „veszélyes", közösségellenes egyéb megnyilvánulások eltávolításával. Napjainkban egyre inkább jellemző, hogy a GAFAM tagjai igyekeznek a tartalmakat a saját értékrendjüknek megfelelően szabályozni és ami ettől eltér az gyakran a cenzorok áldozatává válik.

A TikTok egy igazán jó példa az önkényes tartalomcenzúrára. A platformon szabadon lehet buzdítani a magyar határ ostromára, csempész járatokat lehet szervezni, gyalázni a pedagógusokat ugyanakkor, ha valamely felhasználó hozzászólásában, akár csak egy smiley-val, nemtetszését fejezi ki, azt a hozzászólást a közösségi élet tisztaságára hivatkozva azonnal törlik. A panasz lehetőség mindössze egy felülvizsgálati kérés, minden egyéb megjegyzés lehetősége nélkül. A válasz egy ismételt elutasító válasz, ami ellen nem lehet fellebbezni.
Számos országban, így többek között Törökországban például a szolgáltatókat törvény kötelezi a tiltott tartalmak eltávolítására, illetve megsemmisítésére. A helyi szabályozásoknak megfelelően egy időablakot adnak a szolgáltatónak arra, hogy a törvénytelen tartalmat eltávolítsák, terjesztését megakadályozzák.

Az Európai Unió vonatkozásában például az Európa Tanács 2021. április 29-én rendeletet fogadott el az online terrorista tartalom terjesztésével szembeni fellépésről. A rendelet értelmében a tagállamok illetékes hatóságainak végzésben kell felszólítani a

tárhelyszolgáltatókat a terrorista tartalom eltávolítására, vagy tagállami szinten történő elérhetetlenné tételére. A szolgáltatóknak egy óra áll rendelkezésükre a végzés végrehajtására. A nyilvánvaló bűncselekményt tükröző tartalmak és a szólásszabadság, illetve a véleményszabadság közötti szürke zóna nagy mozgásteret biztosít a platformok tulajdonosi körének. A közösségi média tartalomszűrő politikája és a szólásszabadság közötti kölcsönhatás vizsgálata azonban kívül esik e tanulmány keretein.[74 pp. 20-27] Esetünkben a szélsőséges iszlám terrorista online tevékenység viszonylag könnyen behatárolható kategória, így nem kell a közösségi média szereplők más vonatkozású tartalomszűrő tevékenységét vizsgálnunk. A szóban forgó platformok jelenlegi kialakítása lehetővé teszi a kitiltott személyek számára, hogy másik profilt hozzanak létre, esetleg több álprofillal is rendelkezzenek, így ebben a formában ez a megoldás önmagában csak időleges, illetve részleges eredményt hozhat és magában rejti a probléma újra generálódását.

Másrészről a tapasztalatok azt mutatják, hogy a platformokról kitiltott közösségek nem bomlanak fel, vagy gyengülnek el, hanem ellenkezőleg. Megtalálják azokat az online felületeket, ahol tevékenységüket folytathatják, esetleg a „közös büntetés" még közelebb hozza őket, zártabbak, óvatosabbak lesznek tehát a módszer hatásossága legalább is kétséges. Mert igaz ugyan, hogy a Facebook, vagy Twitter tisztább lesz, de a probléma maga nem szűnik meg. Elég, ha arra gondolunk, hogy a 2020-as Fehérházi zavargásokat követően a QAnont és más szélsőjobboldali szervezeteket kitiltották a Twitterről, és a Facebookról, azonban szinte rögtön átköltöztek a Gab-ra, BitChute-ra, Telegramra, ahol a korábbi méretű közösséget újból képesek voltak kiépíteni. [29]

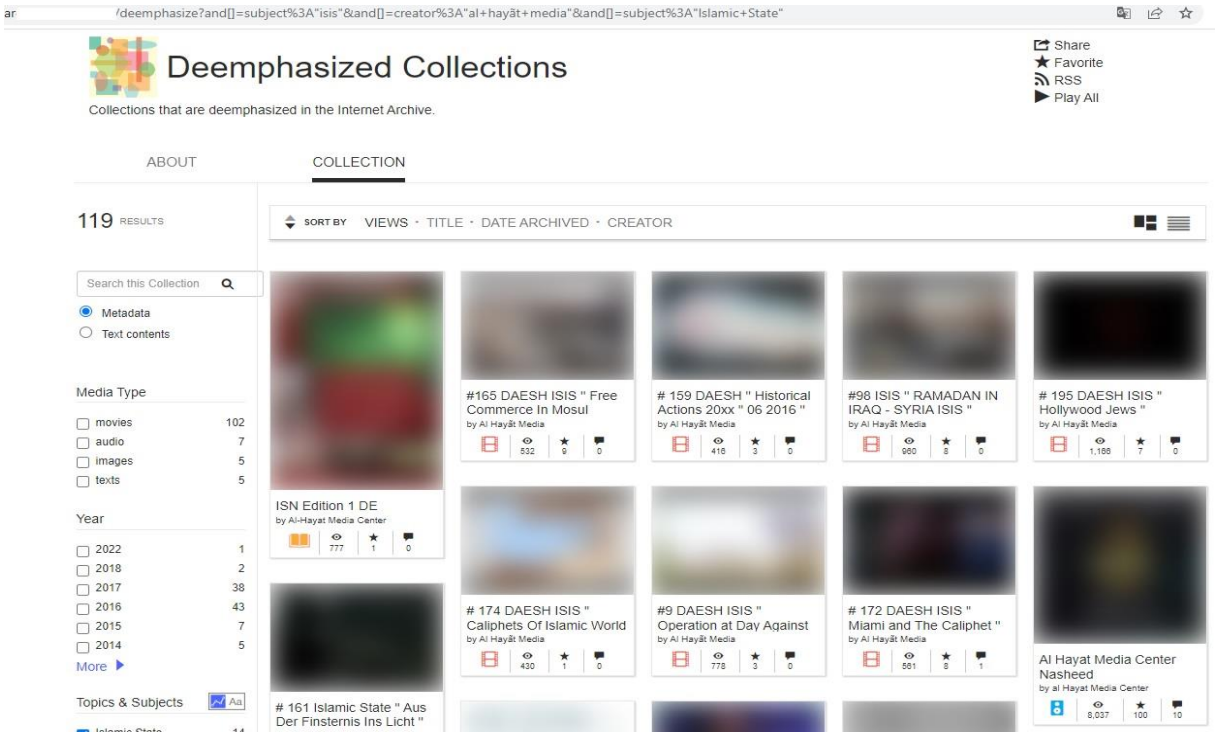
A deplatformization fogalma szélesebb és súlyosabb következményeket von maga után szemben a deplatforming intézményével, ugyanis ezt a GAFAM tagjai a szóban forgó nem kívánatos közösséghez köthető alkalmazások, szolgáltatások, vagy más néven platformok ellehetetlenítése érdekében végzik. Tudnunk kell, hogy a legtöbb ilyen platform támaszkodik valamilyen formában a GAFAM tagjai által nyújtott szolgálatatásra. Gondoljunk az Amazon Web Services (AWS) szolgáltatásaira, amelynek keretében többek között virtuális szervereket árusít, vagy a Google, illetve az Apple alkalmazásboltjaira. Ha ezekről kitiltják az adott platformot, akkor nagyon nehéz helyzetbe kerül, hiszen olyan funkciókat veszíthet el, mint a például Google play service, amelynek hiányában az alkalmazás használhatatlanná válhat, vagy elveszítheti felhasználói jelentős részét is.

2.2.2 Deamplification Deemphasizing (korlátozás, gyengítés)

A káros tartalmak terjesztésének akadályozását célzó intézkedések másik járható útja a tartalmak platformon belüli terjesztésének korlátozása. Például a YouTube azt a technikát alkalmazza, hogy az általa „szürkének", nem egyértelműen károsnak, tartott tartalmat nem törli, hanem csak a feltöltő csatornájának feliratkozói számára teszi elérhetővé. A feltöltés kereshető marad, de mások számára az ajánló sávon nem jelenhet meg. A feltöltőt nem tájékoztatják erről a korlátozásról, így nem tudhatja, hogy csak korlátozott számú felhasználó szerzett tudomást a feltöltéséről. Ezzel a technikával szándékoznak korlátozni a nem káros, hanem a terminológiájuk szerinti „toxikus" tartalmak terjedését.

Más platformok is hasonló technikát alkalmaznak. [28] A Wayback Machine (archive.org) hasonlóan a YouTube-hoz blokkolja a tiltott tartalomhoz és korlátozza a „szürke" tartalomhoz történő hozzáférést. Az 6. számú ábrán az Iszlám Államhoz köthető tartalmak egy részét a Wayback Machine aggályosnak ítélte meg, ezért azokat a „korlátozott" tartalom kategóriában sorolta.

A közösségi média érdekelt felei a tartalomszűrés során az úgynevezett „tényellenőrök" munkájára, hiteles adatbázisokra, a Global Internet Forum to Counter Terrorism (A továbbiakban: GIFCT) által károsnak ítélt tartalmak adatbázisára (a szervezet tevékenységére a későbbiekben még kitérek), a felhasználói bejelentésekre, a mesterséges intelligenciára, valamint a saját cenzoraikra támaszkodnak. Mindezen információk mellett is az alkalmazott tartalomszűrési módszerek és technikák részleteikben nem nyilvánosak, így a felhasználók számára nem átlátható a folyamat. A módszereik és moderálási elveik technikai részletei érthető módon üzleti titkot képeznek, hiszen ezek ismeretében a szabályszegők könnyebben játszhatnák ki a tartalomszűrési rendszereket.



6. ábra Az Iszlám Állammal kapcsolatos "hangsúlyozatlan" tartalom a webarchivumban forrás: szerző képernyőfotója

2.2.3 Az önkéntesek szerepe a dzsihadista terrorszervezetek elleni harcban

A rendvédelmi szervek és a közösségi média érdekelt felein kívül nem szabad figyelmen kívül hagyni az önszerveződő felhasználói közösségeket sem, mint a szélsőséges iszlám terrorszervezetek online tevékenysége elleni harc fontos szereplőit. Igaz az eszközeik palettája korántsem olyan széles, mint az előbbi két kategóriáé, de van egy kétségtelen előnyük. Sokan vannak és felismerhetik az álcázott tartalmakat is, amire a robotizált tartalomszűrők nem minden esetben képesek. Például az Iszlám Állam jelentőségét és az általa jelentett veszélyt jól érzékelteti az a tény, hogy olyan önkéntes csoportok alakultak, amelyek az online térben felvették a harcot a szervezet propaganda tevékenységével. Ezek a szervezetek alapvetően két kategóriára oszthatók:

- közösségi média felhasználói,
- hacker közösségek.

Mindkét csoport a maga sajátságos eszközeivel igyekezett és igyekszik ma is harcolni az Iszlám Állam, vagy az Al Kaida ellen.

A közösségi megmozdulásoknak olyan események adtak lökést, mint például a 2015-os párizsi Bataclan merénylet, amely világszerte nagy felzúdulást keltett. Ennek az események a hatására önkéntesek száma megsokszorozódott és megszervezték a szervezethez tartozó online tartalmak szolgáltatónak történő jelentését. A módszereik közé tartozott például, hogy az ilyen tartalmakat olyan egyezményes hashtag-ekkel látták el, amely megkönnyítette azok kiszűrését.

Iszlám Állam ellenes csoportok ma is működnek a közösségi médiában. Hogy csak néhány példát említsek a Facebook-on például „anti DAESH” (az Iszlám állam nevének rövidítése arabul, amit a szervezet egyébként sértőnek ítél) néven lehet rátalálni, a Telegramon „ISIShunter” csatorna működik, ahol az illegális tartalmakat összegyűjtik és intézkednek azok eltávolítására.

A hacker csoportok ezek közül a magát „Anonymous” hacker csoportként azonosító szervezet járt az élen, amely november 16-án nyilvánosan hadat üzent az Iszlám Államnak és ígéretet tett az online jelenlétének a felszámolására. A csoport kezdetben valóban hatékonyan lépett fel és számos weboldalt, dark webes oldalt felszámolt, azonban a kezdeményezés egy idő után elhalt. Ennek azonban két hatása is volt. Egyrészt egy időre a szervezet online jelenléte valóban megingott, teret veszett, azonban ezzel párhuzamosan meg is erősödött és képességeit fejlesztve továbbra is jelen tud lenni az online térben. A szervezet támadásából adódó evolúciós kockázatra egyébként szakemberek is felhívták a nyilvánosságon keresztül a hacker csoport figyelmét.[30], [73]

2.3 Információgyűjtés, adatbázis építés

A vizsgált terrorszervezetek internetes tevékenységének eredményes kutatása érdekében elengedhetetlen volt egy saját adatbázis létrehozása, amely lehetővé tette az általuk alkalmazott eszközök, módszerek és eljárások első kézből történő tanulmányozását.

Az anyaggyűjtést a tanulmányaim megkezdésével párhuzamosan kezdtem el, hiszen az ilyen jellegű kutató munka egyrészt technikai, illetve informatikai, információbiztonsági továbbá nemzetbiztonsági ismereteket is igényel a nyilvánvalóan elengedhetetlen kulturális háttérismeretek mellett. A kutatás technikai részleteit, korlátait, büntetőjogi és etikai megfontolásait már korábban ismertettem.

Az adatgyűjtés megismételhetőségének érdekében a kutatás alapját képező adatbáziséptés folyamatát a 2. számú mellékletben helyeztem el.

2.4 Dzsihadista szervezetek online jelenléte

A mellékletben ismertetett módon létrehozott adatbázis objektív okokból nem tükrözheti a valós számokat, hiszen egyrészt a keresőmotorok indexelő tevékenységének tehetetlensége (nem tudnak azonnal reagálni az új oldalakra) és az ebből származó pontatlan találatok miatt nem kaphatunk teljes mértékben valós képet, másrészt az online térben különösen ebben a kategóriában rendkívül magas az oldalak illékonysága. Oldalak jönnek létre és szűnnek meg, illetve ideglenesen deaktiválódnak.

Ezen felül, egyes esetekben a keresőmotorok üzemeltetői részéről is tapasztalható esetenként egyfajta szűrő tevékenység.

Mindezen korlátok mellett az eredmények jól közelítik a valós arányokat, ami az egyes szervezetek online jelenlétét illeti. Az 1. számú táblázat az általam létrehozott adatbázisban szereplő dzsihadista terrorszervezetek weboldalainak a számát ábrázolja. Fontosnak tartom megjegyezni, hogy ezek az oldalak egyenként ellenőrzött találatokat tartalmaznak szemben az interneten található egyéb forrásokkal, amelyek jórészt robotok által kulcsszavak alapján gyűjtött oldalak listáit tartalmazzák. A robotok esetenként a kulcsszavak átfedéséből adódóan nem tudnak különbséget tenni például egy anti- dzsihadista vagy Iszlám Állam ellenes weboldal és egy valódi Iszlám Államhoz köthető weboldal között.

Ssz.	Szervezet	Weboldalak száma
1.	**Abu Ali Mustapha Brigades**	1
2.	**Al Kaida**	**34**
3.	**AL Qassam Brigades**	2
4.	**Al Shabaab**	8
5.	**Ansar al-Din Front**	1
6.	**HAMASZ**	7
7.	**Hay'at Tahrir al-Sham (HTS)**	2
8.	**Független dzsihadista weboldalak**	12
9.	**Iszlám Állam**	**71**
10.	**Jaish al-Udl**	1
11.	**Jamiat Ulema-e-Hind**	1
12.	**Jaysh al-Ummah (Gaza)**	1
13.	**Mujahideen Brigades**	1
14.	**Palestinian Islamic Jihad**	1
15.	**Talibán Afganisztán**	10
16.	**Tehreek-e-Taliban**	3
17.	**Turkestan Islamic Party**	3
18.	**Palestinian Mujahideen Movement**	1
19.	**Al Quds**	1
	Összesen:	**161**

1. táblázat A kutatás során felépített adatbázisban szereplő szélsőséges iszlám terrorszervezetek weboldalainak száma forrás: a szerző szerkesztése

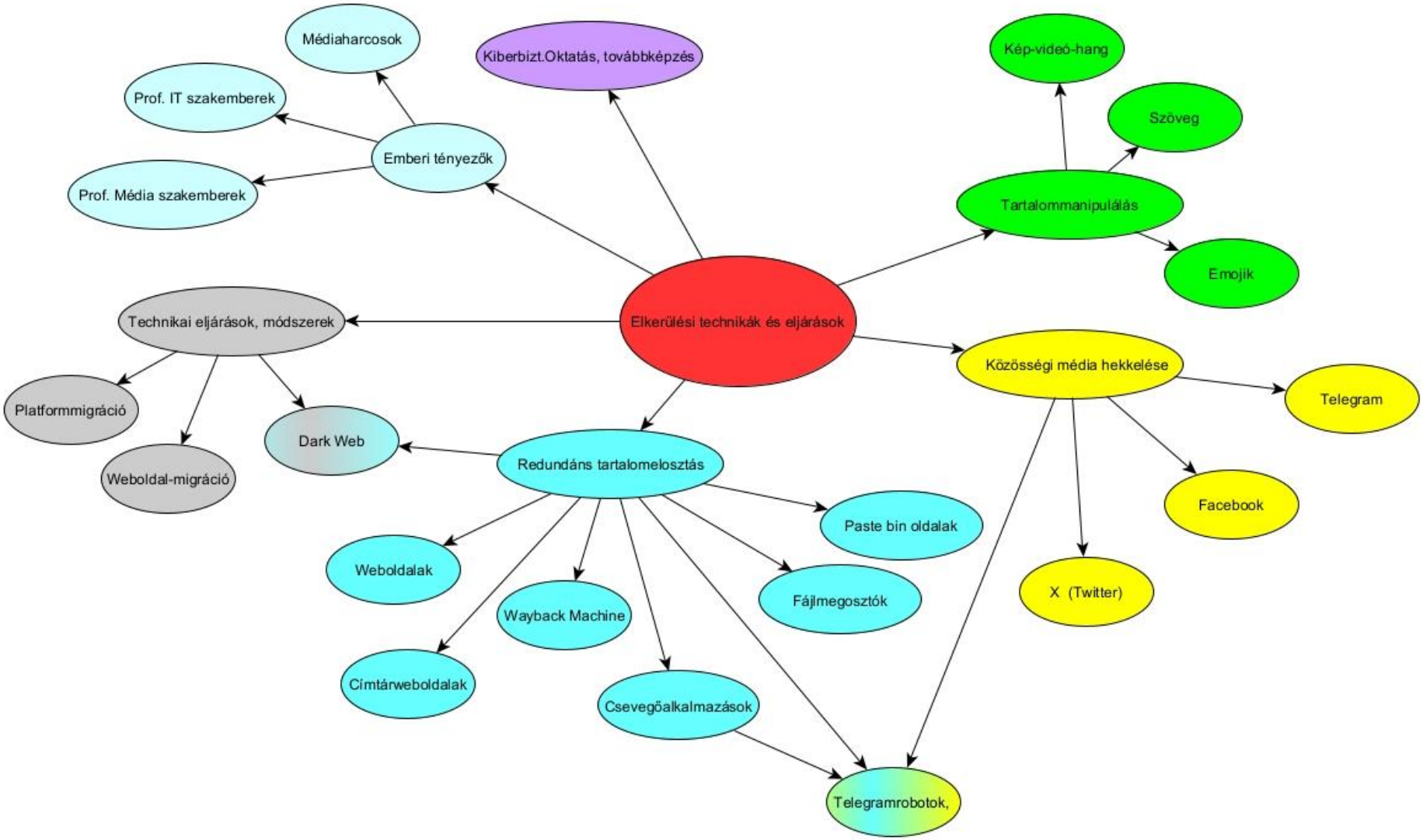
A táblázat adatai alapján a legjelentősebb online jelenléttel az Iszlám Állam rendelkezik. Ezt követően a második helyen áll az Al Kaida, amelyhez hozzávetőleg fele annyi weboldal köthető. A többi szervezet mindössze néhány oldallal képviselteti magát. Ettől függetlenül láthatóan jelen vannak az online térben. A független terrorszervezetkhez köthető kategóriába azokat az odalakat soroltam, amelyek nem köthetők egyetlen terrorszervezethez, hanem jellemzően a dzsihadizmus szellemét hirdetik, így egyaránt jelenítenek meg Iszlám Államhoz, vagy Al Kaidához, vagy más terrorszervezetekhez kapcsolható híreket. Ilyen például a kavkaz____ (elnevezés szándékosan csonkolva) weboldal. Ez a táblázat ugyanakkor érthetővé teszi azt is, hogy eltekintve az offline térben folyatatott tevékenységétől miért az Iszlám Államra irányul a rendvédelmi szervek és a közösségi média érdekelt feleinek fő erőkifejtése.

2.5 Az Iszlám Állam által alkalmazott elkerülési technikák

Az Iszlám Állam a cenzúra elleni harcban az erők és eszközök valamint eljárások széles spektrumát vonultatja fel. A kutatásom során azt tapasztaltam, hogy ezek általában nem önállóan, hanem sok esetben együtt, egymással kombinálva kerülnek alkalmazásra. Az Iszlám Állam cenzúra elleni harcának tanulmányozását követően az összegyűjtött elemeket, eddig egyedülálló módon, egyfajta logikai rendszerbe szerveztem és ennek eredményét 7. számú ábrán látható módon ábrázoltam. Terjedelmi okok miatt az ábrán a fő kategóriákat jelöltem be néhány példával kiegészítve. Hiszen például a közösségi média esetében a platformok ismertetése szétfeszítené az értekezés kereteit.

A továbbiakban kategóriánként felbontva ismertetem az egyes elemeket törekedve arra, hogy ismét a terjedelmi megkötésekre hivatkozva csak az egyedi megoldásokat, vagy érdekességeket hangsúlyozzam.

Az ábrán is látható, hogy egyes területek között átfedés van, azonban a könnyebb áttekinthetőség megőrzése érdekében kerültem valamennyi lehetséges kapcsolat ábrázolását.



7. ábra Az Iszlám Állam cenzúra elleni harcának erői, eszközei és módszerei forrás: a szerző szerkesztése

2.5.1 Emberi tényezők

Az emberi tényezők vizsgálatánál a hangsúlyt nem az IT vagy média szakemberekre fektetem, hiszen ezek megléte evidenciának számít. A kutatás szempontjából sokkal inkább érdekes megoldásnak tartom a médiaharcosok intézményét.

Médiaharcosok

> *Törölj, amit akarsz, Isten támogat minket veled szemben, és amikor törölsz egyet, 50-et hozunk létre a helyére - áthelyezve egy másik csatornára.*
>
> *(ismeretlen Iszlám Állam médiaharcos)*
> *arabról fordítva*
> *forrás:* https://archive.org/details/photo_2021-07-08_23-24-07_202107

Az Iszlám Állam sikeres média harcának egyik, ha nem a legfontosabb összetevője a médiaharcosok (média mudzsahedek) intézménye. A világ minden táján élnek és működnek a terrorszervezet szimpatizánsai, illetve aktivistái, akik megosztják, fordítják és terjesztik a szervezet hivatalos és nem hivatalos kiadványait, illetve ők maguk is készítenek és terjesztenek a szervezet tevékenységéhez kapcsolódó helyi vonatkozású kiadványokat.

Az Iszlám Állam 2016-ben megjelentetett egy 55 oldalas online elérhető arab nyelvű kiadványt, amelynek címe „média dzsihád” (angolul: Media Jihad). Ebben a műben az ismeretlen szerző ismerteti az szervezet információs és propaganda hadviselésének elveit. Felsorolja a különböző médiaharcosok kategóriát és külön kitér az önkéntesek szerepére hangsúlyozva, hogy munkájuk egyenértékű a fizikai dzsihaddal.[14]

Az Iszlám Állam médiaharcosai alapvetően négy csoportot alkotnak:

- az Iszlám Állam hivatalos munkatársai,
- a különböző vilajetek (provinciák) aktivistái, akik saját kiadványokat készítenek,
- önszerveződő kisebb közösségek, sejtek,
- egyéni szimpatizánsok, magányos farkasok (önkéntes médiaharcosok),

Az Iszlám Állam hivatalos, illetve a félhivatalos vagy önkéntes médiaharcosainak számára vonatkozóan nincsenek hiteles adatok. A szervezetnek egy viszonylag zárt, de dinamikusan változó média ökoszisztémája van, amelyet nem lehetséges külső eszközökkel feltérképezni. [31 p. 24] Ugyanakkor az Interneten elérhető propagandaanyagok mennyisége és sokfélesége arra enged következtetni, hogy a számuk akár a több ezret is meghaladhatja. Felmerül a kérdés, hogy mi az oka annak, hogy az Iszlám Állam jóval nagyobb mennyiségű és kiterjedtebb és ellenállóbb propagandát tud folyatni, mint az Al Kaida vagy akár más szélsőséges iszlamista

szervezetek. A magyarázat a már említett információs hadviselésük doktrínájában található. Az Iszlám Állam jóval nagyobb szerepet tulajdonít a médiának, illetve a médiaharcosoknak, mint a többi terrorszervezet, ahogy a mű egyik elemzője [14] többször is rámutat a szerzők a média dzsihadot egyenrangúnak tartják a fizikai harccal, ezért bíztatnak mindenkit, hogy terjesszék a szervezet propaganda anyagait, igyekezzenek másokat is megnyerni az ügynek, hiszen így ők is dzsihadistává válnak. Felszólítják az olvasókat, hogy vegyenek részt az események tudósításában, közvetítésében offline és online módon egyaránt. Véleményük szerint a „szóbeli dzsihád", vagyis tágabban értelmezve a nem fegyveres harc sokszor fontosabb lehet, mint a fegyveres küzdelem ezért Allah névtelen katonáiként hivatkoznak az önkéntes médiaharcosokra, akik az „ellenség" fészkében vállalva a hitetlenek börtöneiben való sínylődést tudósítanak és részt vesznek a propagandaanyagok terjesztésében. Ezzel a technikával szimpatizánsok ezreit tudták, illetve tudják megnyerni bevonva őket a „dzsihád" dicsőséges küzdelmébe.[14 p. 14] A megszólított szimpatizánsok a számítógép képernyője előtt ülve mudzsahednek érezhetik magukat, úgy érzik, hogy egy nagy közösség hasznos tagjaivá válhatnak, és ez motiválja őket arra, hogy nem kevés időt áldozzanak a propaganda terjesztésére még akkor is, ha vallási meggyőződésük nem különösebben erős. Ennél fogva az Iszlám Állam online jelenléte nagyságrendekkel meghaladja más szervezetékét, ideértve a korábban jelentős internetes jelenléttel büszkélkedő Al Kaidát is.[32] Ezzel a fogással egy olyan tartalomsokszorozó kapcsolati rendszer alakul ki, amely rendkívül ellenállóvá válik a külső akadályozó tényezőkkel szemben, hiszen egy csomópont kiesése nem okoz különösebb fennakadást a terjesztésben [31 p. 30].

Az Iszlám Állam hivatalos kiadványának az al Naba magazin 325-ös számának szerkesztői rovatában olvasható az alábbi részlet, amely gyakorlatilag összefoglalja mindazt, ami a média mudzsahed intézmény lényege. Az angol nyelvű szöveg magyarul így hangzik:

„A média dzsihád katonáinak tudniuk kell, hogy az iszlám ellen harcoló hatalmas számú média platformokkal szembeni harc felelőssége az ő vállukon nyugszik. Sikerüket csak az őszinteség, a felelősségteljes munka, a kitartás és a bizonyosság útján érhetik el. A médiaháború győzelme összhangban van a csatatér győzelmével; mindkettő hatalmas áldozatokat igényel, hogy legyőzzék a kuffar tömegeit és tehetetlenné tegyék varázslóikat. Egy varázsló soha nem lesz sikeres, mert Allah uralkodik ügyén, de a legtöbb ember nem tudja ezt." forrás: [al-Nabaa, Vol. 325 magazin] (A szerző fordítása)

2.5.2 Technikai eljárások, módszerek

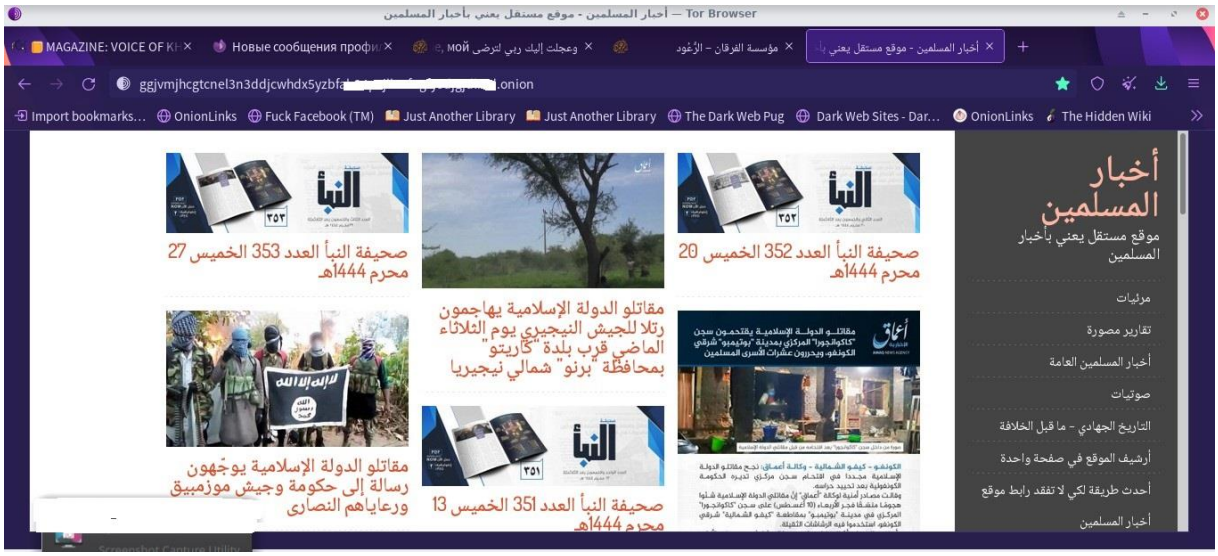
Platformmigráció

Az Iszlám Állam tagjai, illetve követői a platform egyszerűségét és alacsony erőforrás szükségletét kihasználva 2013-2014-ben a Twitteren csoportosultak. A túlnyomórészt Szíriában és Irakban élő tagok jellemzően propagandaterjesztésre, toborzásra, koordinációra és belső kommunikációra használták az alkalmazást. J.M. Berger és Jonathon Morgan által végzett célirányos kutatás szerint 2014. szeptember és december között mintegy 46.000 Iszlám Államhoz köthető profil volt elérhető a Twitteren [16 p. 2] A BBC 2016 elején arról tudósított, hogy a platform a rendvédelmi szervek és az Egyesült Államok kormányának nyomására 2015 közepétől számított 4 hónap alatt több mint 125 ezer Iszlám Államhoz köthető profilt függesztett fel. [33] Noha a támogatói jelenlétet azóta sem sikerült felszámolni ez a lépés jelentős csapást mért a szervezet kommunikációs gépezetére, ezért azonnal új platformok felkutatásába kezdtek.

Céljaiknak leginkább a felhőalapú, a már korábban ismertetett titkosított Telegram nevű alkalmazás felelt meg a legjobban. Emlékeztetőül, ezen az alkalmazáson belül lehetőség van úgynevezett csatornák létrehozására, amelyeken egyszerre akár több ezer felhasználóval is megoszthatók a tartalmak beleértve, képeket, videókat és más formátumú fájlokat is. A Telegram üzemeltetői együttműködve az Europollal 2018. októberében az „Action Day" keretében több ezer nyilvános Iszlám Állam szimpatizáns csatornát és felhasználót töröltek, illetve tiltottak ki az alkalmazásból. A következő év novemberében az úgynevezett „Second Action Day" keretében további csatornák és felhasználók ezreit távolították el. A tisztogatás azonban nem volt sikeres, ugyanis a terroristák továbbra is aktívak a platformon. Ezt a Telegram végpontok közötti titkosítást alkalmazó, tehát kívülállók számára elérhetetlen, kommunikációs funkciói teszik lehetővé. Ezek használatával ugyan nem lehetséges nagyszámú hallgatóság elérése, azonban a tartalmak elosztása a további megosztók között viszont megoldható.

Felhívom az olvasó figyelmét arra, hogy mielőtt elítélné a Telegram vezetését a terrorista tartalmak megtűrése miatt vegye figyelembe, hogy a vezetőik igyekeznek minden tőlük telhetőt megtenni az ilyen jellegű tartalmak és felhasználók eltávolítása érdekében. Az alkalmazásban ugyanis működik egy csatorna, amelyen naponta beszámolnak arról, hogy hány szélsőséges dzsihadista tartalmat, illetve felhasználót távolítottak el a felhasználók jelzései alapján. Az „ISIS WATCH" (https://t.me/ISISwatch) csatorna adatai szerint csak 2024. január 04-én 443 botot és csatornát távolítottak és addig az adott hónapban (tehát négy nap alatt) összesen 1329-et. E mellett például napi rendszerességgel blokkolják a HAMASZ és más, az Izraeli támadásban érintett dzsihadista szervezetek csatornáit.

A platform létjogosultságát és küldetését veszélyeztetnék, ha valamilyen formában ellenőriznék a titkosított magán beszélgetések tartalmát, erre egyébként a rendszer speciális infrastruktúrájának és a végpontok közötti titkosításnak köszönhetően nincs lehetőségük
Mindent figyelembe véve az Europol akciók időlegesen jelentősen gyengítették a terrorszervezet kommunikációs ökoszisztémáját és arra kényszerítették a vezetőséget, illetve a szimpatizánsokat, hogy diverzifikálják médiaforrásaikat és új platformokat vonjanak be az információs hadviselésbe.
A Telegramon történt tisztogatást követően az Iszlám Állam szakemberi kipróbálták az akkor népszerű és biztonságosnak mondott alkalmazásokat, azonban ezek vagy a technikai megoldások alkalmatlansága, vagy pedig az üzemeltetők ellenállása miatt csak részben sikerültek. Számos próbálkozást követően jutottak el a jelenlegi állapothoz, amelyben a továbbra is a Telegram, illetve a Rocket.Chat, Elements, valamint az XMPP alapú (Jabber) végpontok közötti titkosítást alkalmazó megoldások a legfontosabbak. Ez utóbbiak viszont alkalmasak a nagyszámú hallgatóság elérésére, egyeztetésre, napi események megvitatására, kiberbiztonsági továbbképzésekre. Ezen felül ezek a kommunikációs lehetőségek is biztosítják az úgynevezett elosztó központok (angolul hub-ok) tartalommal való ellátását. A kutatást ezeken a platformokon nem folytathattam, mivel ez kimerítette volna a terroristákkal való kommunikáció fogalmát.
A források diverzifikálásából megnövekedett stabilitás és ellenállóság adódott, így a hálózat szövevényesebbé vált. A jelenleg használt alkalmazásokon keresztül lehetőség van titkosított video, hang, illetve szöveges üzenetek továbbítására, valamint fájlok és linkek megosztására.
A deplatformizációs törekvések a kétségtelen eredményeik mellett bizonyos értelemben kontraproduktívak voltak és hozzájárultak a terrorszervezet online ellenállóképességének fejlesztéséhez. A különböző nyílt és titkosított kommunikációs lehetőségek megismerése, valamint az alkalmazások feladat specifikus kiválasztása olyan technológiai előnyhöz juttatta a szervezetet, amelynek birtokában az képes volt egy diverzifikált, több lábon álló, virtuális média ökoszisztéma kialakítására. Ennek a folyamatnak az eredménye többek között az Iszlám Állam dark webes jelenléte is, amely kihasználva az új médium által biztosított földrajzi és felhasználói anonimitást elrejti a bűnüldöző szervek elől a szervezet tevékenységét. A 8. számú ábrán egy Iszlám Állammal szimpatizáló dark webes weboldal képernyőfotója látható.



***8**. ábra Az Iszlám Állammal szimpatizáló Muszlim hírekkel foglalkozó független dark webes weboldal képernyőfotója (a weboldal elérhetőségét a szerző csonkolta) forrás: a szerző képernyőfotója*

Weboldalak migrálása

A szélsőséges Iszlám terrorista szervezetek megalakulásuktól fogva sokat tanultak a nyugati társadalmakban nagyobb múltra visszatekintő szélsőjobboldali, illetve anarchista szervezetekről. Az Iszlám Állam és az Al Kaida oktatóvideói között, amelyeken házi robbanóanyagkészítést, vagy méregkészítést lehet tanulni szép számmal találhatók amerikai anarchisták, vagy szélsőjobboldali aktivisták által készített oktatófilmek. De nem voltak válogatósak akkor sem, amikor az internetes megjelenésük kezdetén a korszerű kommunikációs technológiák használatának terén átvették az extrémista mozgalmak olyan hatóságok kijátszását célzó taktikai fogásait, mint a webhelyek anonimizálása, vagy a viszonylag laza adatvédelmi törvényekkel rendelkező országok felsőszintű tartományneveinek (top level domain) alkalmazása.

Az évek során a rendvédelmi szervek fokozódó nyomásának hatására Iszlám Állam ezeket a módszereket tovább fejlesztette. Az új webcímek feltehetően a pontos és előrelátó tervezésnek köszönhetően állandó készenlétben vannak arra az esetre, ha egyik weboldalukat a szolgáltató lekapcsolja, ugyanis a weboldal tartalma előre be van készítve egy másik webtárhelyre, illetve ugyan azon a néven, de másik felső szintű tartománynéven regisztrált elérhetőség csak aktiválására vár.[23 p. 12]

Kutatásaim során rábukkantam egy olyan Iszlám Államhoz köthető webhelyre, amelyen több mint 20 GB propaganda és kiképzési anyagot tároltak. Ezen a tárhelyen találtam egy olyan oktató cd-t, amely a felhasználót végig vezeti a mudzsaheddé válás minden területén az ideológiai felkészüléstől a lőkiképzésen keresztül egészen addig, hogy hogyan kell a

„hitetlenek” fogságában a kihallgatásokon viselkedni. A CD-ROM címe: „Hogyan válj igazi mudzsaheddé”.

A weboldal elérhetőségét jelentettem a Terrorelhárítási Központnak (TEK), akik együttműködő partnerszolgálataik útján intézkedtek a weboldal blokkolására. Megfigyeltem, hogy néhány órával a weboldal lekapcsolását követően ugyan ez a tartalom felső szintű tartománynevet váltva (esetünkben „.com”-ról „.co-ra” változtatva) ismét elérhető lett és a kutatás lezárásának idején még zavartalanul működött. A gyors váltás arra enged következtetni, hogy a domain név már regisztrálva volt és csak aktiválásra várt. A felső szintű tartománynév változtatására és néhány karakter módosítására kiváló példa az Iszlám Állam korábbi központi honlapja elérhetőségének változása. A következő felsorolás bemutatja ennek a módszernek a gyakorlatban történő alkalmazását. Az utóbbi néhány évben a szervezet honlapját a következő címeken lehetett elérni (ma már egyik sem aktív): elokab.com.ng; elokab.de; elokab.es; elokab.eu; elokab.fun; elokab.icu; elokab.in; elokab.nl; elokab.pm; elokab.pw; elokab.ro; elokabe.de; elokabe.org; elokabe.ro; elukab.org.

Hasonló módszert figyelhettünk meg az Al Qassam Brigades terrorszervezet esetében is, ahol az „alqassam.net”- ről az Egyesült Államok hatóságai tiltását követően „alqassam.__”-re (szándékosan torzítva) váltottak. Érdekesség, hogy az első oldal 2004-es bezárását követően rövid idő elteltével megjelent az új elérhetőségen ugyan az oldal, ami viszont most már több mint 18 éve működik megszakítás nélkül.

Egy másik esetben az előző két példával ellentétben egy dzsihadista szervezet zavartalanul jelen van az online térben. Az albán „Xhemati Alban” dzsihadista terrorszervezet, amely a szíriai Idlib-ben tevékenykedik a Hayat Tahrir Al-Sham (röviden: HTS) katonai irányítása alatt 2019-től folyamatosan üzemeltet egy weboldalt, amelyen taktikai tanácsokat, fegyverátalakítással kapcsolatos tapasztalatokat oszt meg és rendszeresen beszámol a sikeres akciókról. Ez a két példa jól mutatja, hogy a szervezetekre eső nyomás mennyire eltérő lehet egyes esetekben. Láthatóan a szervezetek nem egyformán vannak a rendvédelmi szervezetek látókörében, ennél fogva ezeknek nincs szükségük arra, hogy egy bonyolult rendszert hozzanak létre. Esetenként elegendő, ha egy tiltás esetén felső szintű tartomány nevet váltanak és zavartalanul folytathatják tevékenységüket.

Ennek a technikának az alkalmazására számos egyéb példát lehet találni. Ennek az az oka, hogy ez a technikai viszonylag egyszerűen kivitelezhető megoldás a blokkolás ellen, hiszen ennek végrehajtása nem igényel magas szintű felhasználói tudást.

A domain nevek regisztrációja alkalmával nem valós neveket használnak, illetve olyan címeket adnak meg, amelyek háborús övezetekben találhatók, így ezek ellenőrzése gyakorlatilag

lehetetlen. A nemzetközi adatbázisban a tartománynév név tulajdonosát különböző anonimizáló szolgáltatások igénybevételével rejtik el a nyilvánosság elől. Ilyen például a „GoDaddy", vagy a „Anonymize, Inc." amelyek a nyilvános adatbázisokban, mint tulajdonos jelennek meg és biztosítják a szolgáltatás igénybe vevőjének, hogy amennyiben hatósági megkeresés érkezik a domainnel kapcsolatban, úgy mielőtt teljesítenék a hatósági kérést értesítik a tulajdonost. A 9. számú ábrán egy Iszlám Államhoz köthető weboldal WhoIs rekordja látható, ahol a „GoDaddy" szerepel regisztrálóként és kontaktként a „Domains by Proxy LLC" (amely egyébként a GoDaddy csoporthoz tartozik). Az oldalaikat gyakran a „CloudFlare" szolgáltatással védik, amely egyrészt gyorsabb és stabilabb elérhetőséget biztosít a világ bármely tájáról, másrészt védelmi célból egyfajta virtuális fal mögé rejti a webhelyet a külső támadások megnehezítése érdekében. Érdekes módon az vizsgált weboldalak védelmét nyugati vállalkozások biztosítják.

9. ábra Iszlám Államhoz köthető weboldal WhoIs rekordja (az oldal elérhetősége biztonsági okokból csonkolva) forrás: a szerzők képernyőfotója

2.5.3 Kiberbiztonsági oktatás és továbbképzés

Az Iszlám Állam hozzáállása az internethez és a digitális technológiákhoz eléggé sajátságos, hiszen egyik oldalról igyekszik kihasználni az új technológiákban rejlő lehetőségeket, ugyanakkor ezeket a vívmányokat az ellenség fegyverének is tekinti. Éppen ezért, minden lehető módon igyekezett és igyekszik korlátozni a területén az internethozzáférést, ennek érdekében rombolta a mobiltelefon tornyokat, blokkolta az internetes kapcsolatokat, valamint katonái és tagjai számára tiltotta a közösségi média használatát. Az okostelefonokat az ellenség

kémeszközeinek tekintik, hiszen rájöttek, hogy ezeket követve az ellenségeik nyomon követhetik a tevékenységüket és megállapíthatják a tartózkodási helyüket, esetleg lehallgathatják őket. Az új technológia lehetővé teszi a „kémek" számára, hogy kapcsolatba lépjenek tartóikkal. Ezzel a témával több alkalommal is foglalkozott az Al Naba és a francia nyelvű Dar al Islam magazin [34 pp. 8-9], [35 pp. 14-15],[36 pp.30-33],[37 pp. 39-53]

A közösségi média és rendfenntartó szervek részéről fokozó deplatformizációs törekvések, valamint az egyre gyakoribb hackertámadások hatására felmerült az igény egy kiberbiztonsági szakértőkből álló szervezet létrehozására. Ez a szervezet az Electronic Horizons Foundation (arab rövidítése AFAQ), amelynek logója a 10. számú ábrán látható. Az alapítvánnyal kapcsolatban végzett saját kutatásaim és Dr. Azani valamint Haberfeld „The end of Islamic State's Cyber Security Unit Afaq?" címen publikált kutatásai alapján a következő kép rajzolódik ki a szervezetről:

10. ábra Az Electronic Horizons foundation logója forras: képernyőfotó a biztonság és alkalmazás engedélyek mobil telefonokon című oktató filmből

Az alapítvány 2016-ban kezdte meg a működését azzal a céllal, az Iszlám Állam és a támogatói kiberbiztonsági tudatosságát fejlessze, valamint elősegítse a biztonságos kommunikációt és a tartalomterjesztés korlátozásoktól mentes lehetőségét.

Ennek keretében az alapítvány két fő feladatot tűzött maga elé:

- A biztonságos kommunikáció kialakítására történő oktatás (Tor, Virtuális magán hálózatok használata (VPN)
- A különböző alkalmazások biztonságos használatának oktatása, illetve a hardver eszközök átalakítással történő biztonságossá tétele

Az alapítvány az évek során számtalan különböző webhely létrehozására kényszerült, ez azonban nem gyakorolt jelentős hatást a kiadványaik terjesztésére, ugyanis egyszerre több platformon is párhuzamosan, megszakítás nélkül posztolták a különböző témájú tananyagokat. Többek között előszeretettel használták a különböző „PasteBin" típusú és más anonim

fájlmegosztó webhelyeket, illetve a web archívumokat. A kiadványaik túlnyomórészt arab nyelven jelentek meg, de előfordultak angol és francia nyelvű kiadások is. Ezekben a kiadványokban az anonim kapcsolat kialakítására, illetve a különböző alkalmazások biztonsági beállításaira vagy a felhasználó után kémkedő alkalmazások listájára talált útmutatót az olvasó. Számos oktatóanyag készült a felhasználók biztonságának fokozása érdekében a mobil telefonok (okostelefonok) olyan hardveres átalakítására, mint a kamerák kiszerelése, vagy a mikrofonok eltávolítása. Ezzel kapcsolatos a 11. számú ábrán látható képernyőfotó.

A 12. számú ábrán az alapítvány egy kiberhadviseléssel kapcsolatos oktatófilmjének nyitóképéről készült képernyőfotó látható. A film címe nem egészen pontos, mert inkább azzal foglalkozik, hogy az Egyesült Államok nemzetbiztonsági szolgálatai azon belül is a Nemzetbiztonsági Ügynökség (National Security Agency, röviden: NSA) milyen adatokat gyűjt és tárol a lakosságról.

Kutatásaim során azt tapasztaltam, hogy működése során az alapítvány többszáz oldalnyi és több órányi oktatóvideót készített és osztott meg a felhasználókkal. Erre jellemzően a stabil platformnak számító anonim fájlmegosztókat (JustPaste.it és a Pastethis.to), valamint az archive.org felülete mellett a folyamatosan költözésre kényszerített weboldalukat használták. A tartalomkészítők figyelmet fordítottak arra, hogy közzé tegyék állandó elérhetőségüket, amelyek végpontok közötti titkosítással biztosított üzenetküldő alkalmazásokon létrehozott felhasználói fiókok voltak (Telegram, Threema, Jabber, chatwith.___).

Az évek során az alapítvány munkatársai a biztonságos és anonim fájlmegosztás, valamint a végpontok közötti titkosított kommunikáció biztosítása céljából számos alkalmazást fejlesztettek. Működése során szorosan együttműködtek egy másik kiberbiztonsággal foglalkozó alapítvánnyal, a Bank al-Ansar-al, amely csak a felhasználók közösségi média használatának oktatására fókuszált.

11. ábra Az Electronic Horizons foundation forras: képernyőfotó a biztonság és alkalmazás engedélyek mobil telefonokon című oktató filmből

12. ábra Az Afaq Electronic Foundation honlapján található oktatóanyag a kiberhadviselésről forrás: a szerző képernyőfotója

A szervezet olyan hatékonynak bizonyult az ismeretterjesztő és oktató tevékenységben, hogy az ellenséges hackerek, valamint a rendvédelmi szervek számára a „belső maghoz” tartozók elleni akciók egyre nehezebbé váltak, ezért a támadások súlypontját áthelyezték magának az alapítványnak az erőforrásaira.

Ennek eredményeként az „Elements” platformon 2021. júliusában „Coffespot” néven létrehozott szerverüket 2022 márciusában ismeretlen hackerek sikeresen feltörték, de az eddigiekkel ellentétben hagyták tovább működni, viszont a szervezet Rocket.Chat csatornájára

feltöltöttek egy infografikát, amely leleplezi az alapítvány vezetőségének személyazonosságát és azt állítja, hogy a támogatóktól kapott pénzen autókat, ingatlanokat vásároltak és informatikai cégeket alapítottak.

Az alapítvány közleményt adott ki, amelyben egyrészt cáfolja a „rágalmakat”, másrészt felhívja a felhasználók figyelmét arra, hogy a szervereiket több alkalommal is támadás érte, ezért a felhasználóik biztonsága érdekében az alapítvány ideiglenesen beszünteti a tevékenységét. Az alapítvány közleménye ellenére a hívőkben a bizalom megingott, hiszen a sebezhetetlenségüket övező mítosz szertefoszlott, illetve a tisztességük is megkérdőjeleződött. Az alapítvány jelenleg nem működik, azonban nem zárható ki, hogy a későbbiekben valamilyen formában ismét életre kel. Az alapítvány weboldala arról tájékoztatja a felhasználókat, ahogy az a 13.számú ábrán látható, hogy az ellenük irányuló támadások miatt működésüket felfüggesztik, mert nem akarják kockáztatni, hogy egy sikeres támadás esetén a felhasználóik adatai az ellenség kezébe kerüljenek.

13. ábra Az AFAQ alapítvány weboldalán a sorozatos hacker támadásokra hivatkozva a tevékenységük felfüggesztéséről tájékoztatják a felhasználókat. forrás: a szerző képernyőfotója

Az Iszlám Állam ugyanakkor nem maradt kiberbiztonsági szakértők nélkül, ugyanis korábban is létező, de eddig háttérbe szorult al-Qiam Electronic Foundation (Qef) alapítvány egyre inkább az előtérbe kerül és igyekszik az Afaq által hátrahagyott űrt betölteni. Mindazonáltal az belépő alapítvány képességei ez idáig nem tisztázottak [38] Nem mehetünk el ugyanakkor a mellett a lehetőség mellett sem, hogy az online mudzsahedek közül a megfelelő képzettséggel rendelkező és megbízható szakembereket bevonhatják a szervezet IT biztonságának

fejlesztésébe, ideértve a szoftverfejlesztést és szimpatizánsok, illetve követők részére történő műveleti biztonsággal kapcsolatos tanácsadást.

2.5.4 Tartalommanipuláció

A megtévesztés az egyik leghatékonyabb és leggyakrabban alkalmazott eszköz az Iszlám Állam médiaharcosainak fegyvertárában. Mint ahogy már a deplatformizációról szóló fejezetben arra kitértem a közösségi média üzemeltetői az eszközök széles spektrumát felhasználják a nemkívánatos tartalmak eltávolítása érdekében. A nagymennyiségű adatforgalom kezelése napjainkban már megoldhatatlan feladat lenne a mesterséges intelligencia alkalmazása nélkül. Az 2-es és 3-as számú táblázatokban a META Transparency Center adatai alapján látható, hogy milyen mennyiségű adattal kellett megbirkózniuk 2022. első három negyedévében. A kimutatás sajnos nem tartalmazza terrorszervezet szintjére lebontva az adatokat, de az egyértelműen látható, hogy a közösségi média terrorfertőzöttsége rendkívül magas.

Facebook

Időszak	Tiltás	Panasz	Panasz nélkül helyreállítva	Panaszra helyreállítva	Tiltva maradt
2022Q1	16 100 000	33 800	408 300	5 400	15 652 500
2022Q2	13 600 000	531 000	24 400	61 900	12 982 700
2022Q3	16700000	332 000	4 000 000	60 300	12 307 700

2. táblázat A Facebook 2022 első 3 negyedévében tiltott tartalmak számbeli alakulása Forrás: META Transparency Center

Instagram

Időszak	Tiltás	Panasz	Panasz nélkül helyreállítva	Panaszra helyreállítva	Tiltva maradt
2022Q1	1 500 000	0	84 900	0	1 415 100
2022Q2	1 900 000	99 400	4 600	18 000	1 778 000
2022Q3	2 200 000	56 700	915 500	12 700	1 215 100

3. táblázat Az Instagram 2023 első 3 negyedévében tiltott tartalmak számbeli alakulása Forrás: META Transparency Center

Mint arra már a deplatformizációról szóló fejezetben szó esett a közösségi médiaszolgáltatók több eszközt is igénybe vesznek a nemkívánatos tartalmak kiszűrése érdekében. Ezekkel kapcsolatban két fő probléma merül fel. A humán erőforrások által végzett szűrés ugyan hatékony, ugyanakkor rendkívül szűk a keresztmetszete, míg az automatizált gépi tanuláson alapuló mesterséges intelligencia megoldások rendkívül nagy mennyiségű adat ellenőrzésére alkalmasak, azonban tudásuk korlátozott, csak bizonyos feladatokat képesek pontosan

végrehajtani. Ezeket a gyengeségeket használják ki többek között az Iszlám Állam média szakemberei, illetve a szimpatizánsaik.

A mesterséges intelligencián alapuló tartalom ellenőrzés kijátszása alapvetően három nagy kategóriára bontható:

A szöveges tartalom manipulációja

A szöveges tartalom ellenőrzése ellen bevált módszer az úgynevezett virágnyelv alkalmazása, amelyben például az al Naba magazint csak „A muszlim újság”-ként jelölik. A robotok nyelvi képességei elsősorban az angol nyelvre fókuszálnak és arabul, vagy akár afrikai törzsi nyelveken kevésbé hatékonyak, ezért gyakori trükk a szavak szándékos helytelen betűzése, betűk és számok kombinálása (KH4LIF4H, I3lam). Elterjedt módszer az egymásközötti azonosításra a közösségi médiában oly népszerű „hashtag” rendszert. Olyan „hashtag”-ekkel (#hashtag) jelölik a tartalmaikat, amelyek egymás közötti megállapodásban a közösségükhöz való tartozás ellenőrzésére alkalmasak.

A kapcsolattartás érdekében olyan rendkívül összetett rendszert fejlesztettek ki, amely lehetővé teszi számukra, hogy a különböző platformokon teljesen semleges neveket használjanak, amelyek a kívülállók számára semmilyen formában sem utalnak a csatornák, vagy a webhelyek valódi tartalmára. Ilyenek például a „linkshare”, „National Geographic”, „Ilam” stb… (A kapcsolattartás rendszerére a későbbiekben még részletesen kitérek.)

A hangulat ikonok (emojik) használata

Szólnom kell az továbbá úgynevezett emoji kódkönyvről. A rajzos hangulatjelek segítségével egyszerűen kijátszható az ellenőrző szoftver. Ezt a módszert használták az oltástagadók a Facebookos kommunikációjuk során, ahol az oltás, vagy a vakcina szót egy fecskendő emojijával helyettesítették, de hasonló módszert alkalmaztak fiatalok az Egyesült Államokban a kábítószerrel kapcsolatos beszélgetéseikben a különböző kábítószerek nevének helyettesítésére is. Ez utóbbival kapcsolatban további információk érhetőek el a https://www.dea.gov/sites/default/files/2021-12/Emoji%20Decoded.pdf címről letölthető dokumentumban.

A médiatartalmak (kép, videó, hang) manipulálása

A közösségi média szolgáltatókra nehezedő nyomás hatására jött létre 2017-ben a GIFCT azzal a céllal, hogy az egyes platformokon beazonosított káros tartalmak digitális ujjlenyomatait egymás között megosztva csökkentsék az ezekkel kapcsolatos reakció idejüket. A GIFCT nem kormányzati szervezet, hanem a Facebook, Twitter, YouTube és Microsoft által létrehozott fórum, amelyhez megalakulása óta már több mint egy tucat platform csatlakozott. A

szervezettel kapcsolatos további információk a https://gifct.org címen érhetők el. A fórum tagjai a beazonosított káros tartalmakról készített digitális ujjlenyomatokat (hash-t) megosztják egymással így a többieknek csak a saját tartalmaik digitális ujjlenyomatait kell összehasonlítaniuk a káros mintával jelentősen lecsökkentve a reakció időt, hiszen egyezés esetén azonnal el lehet a káros tartalmat távolítani. A digitális ujjlenyomat egy olyan eljáráson alapul, amelyben az adott tetszőleges hosszúságú fájlt egy matematikai eljárással számok és betűk meghatározott hosszúságú sorával (hash) helyettesítik oly módon, hogy abból semmilyen formában sem lehet az eredeti tartalomra visszakövetkeztetni, ugyanakkor a fájl legkisebb megváltoztatása esetén a „hash" is megváltozik. A technológia előnye, hogy az egész fájl helyett elegendő a „hash"-en elvégezni bizonyos műveleteket így erőforrást és időt lehet megtakarítani, tovább a fájl integritása is könnyen ellenőrizhető.

A „hash" technológia erőssége egyúttal annak gyengesége is. Az Iszlám Állam szakértői felismerték, hogy a publikált, illetve megosztott tartalmak legkisebb módosítása is lehetetlenné teszi a digitális ujjlenyomat alapján történő szűrést. Ehhez elegendő egy betűt megváltoztatni, vagy a képeken illetve videókon egy apró módosítást végezni és a „hash" technológián alapuló szűrés használhatatlanná válik. Az aktivistáik természetesen tisztában vannak ezzel és élnek is a lehetőségekkel.

A kategórián belül maradva a következő fogás módszerét tekintve ugyan hasonló az előzőekben bemutatott tartalommanipulációval, de ez a megtévesztés ebben az esetben a tartalmat elemző mesterséges intelligencia kijátszását célozza. Az arcfelismerésre, vagy a geolokációs beazonosításra használt mesterséges intelligencia megtévesztése érdekében elterjedt módszer a fényképek hátterének, vagy a képen szereplő személyek arcának, esetleg felszerelésének elmosása, elhomályosítása. A 14. ábrán képernyőfotó látható az Iszlám Állam egyik videójáról, amelyen jól érzékelhető, hogy a geolokációs beazonosítás, illetve az arcfelismerés akadályozása érdekében a képen szereplők arcát és a háttérben található jellegzetes tereptárgyakat szándékosan elhomályosították.

14. ábra A felvételek az Iszlám Állam egyik propaganda vieójából készített képernyő fotó forrás: szerzők képernyőfotója

2.5.5 Redundáns tartalomelosztás rendszere

A tartalommegosztás és kapcsolattartás redundáns rendszere

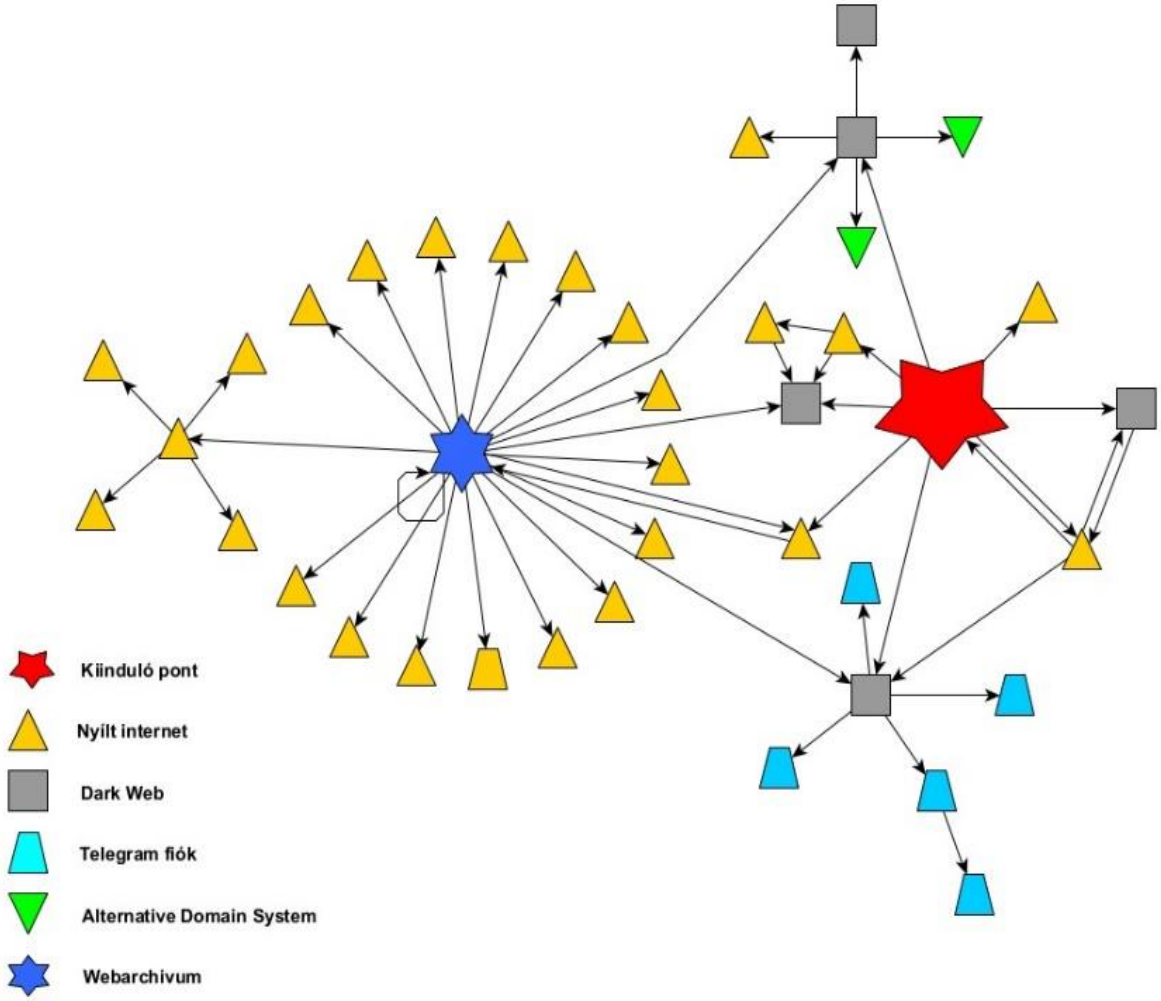
Az Iszlám Állam sikeres internetes tevékenységének kulcsa az általuk készített tartalmak folyamatos online elérhetőségének biztosítása. A korábban bemutatott technikák mellett, illetve ezekkel párhuzamosan létrehoztak egy olyan tartalommegosztó redundáns kapcsolati hálózatot, amely alaposan feladja a leckét az illetékes rendvédelmi szerveknek és a közösségi média érdekelt feleinek azzal, hogy biztosítja a szervezet folyamatos online jelenlétét az interneten. Ennek a rendszernek egyrészről az a lényege, hogy a központ által kibocsájtott propagandaanyagot a Telegram privát csatornákon, a Rocket. chat és a többi végpontok közötti titkosítást alkalmazó üzenetküldő alkalmazásokon keresztül először egy szűk mag kapja meg, a bizalmi kör, majd ezek különböző egyéb csatornákon osztják tovább a követőikkel. Ezek szintén tovább osztják, azzal a feladattal, hogy minden felhasználónak (média mudzsahednek) feladata a tartalom minél több helyen történő megosztása, úgy, hogy az egyes megosztásokkal együtt más megosztásokhoz is mutassanak elérhetőségek. Összességében ez a tevékenység eredményezi azt, hogy a tartalmak gyakorlatilag kiirthatatlanok az online térből és ha egy forrás kiesik (letiltják) a tartalom továbbra is elérhető marad máshol, amit aztán a média mudzsahed további helyeken ismét megoszt. Ez a magyarázata annak, hogy ma is elérhetők az Iszlám Állam olyan videói, amelyeket tíz évvel korábban töltöttek fel az internetre.

Ez az elmélet könnyen ellenőrizhető, ha megvizsgáljuk, hogy a például az Iszlám Állam hivatalos kiadványának az Al Naba magazinnak mekkora a terjedési sebessége. A magazin legújabb számának megjelenését követően néhány órán, vagy esetleg egy-két napon belül számos egymástól függetlennek tűnő webhelyen válik elérhetővé. Az ellenőrzés eszközeként olyan OSINT eszközt használhatunk mint a „Tinyeye”, vagy „Image Search” képkeresők,

amely segítségével a magazin egy jellegzetes képét felhasználva rábukkanhatunk a többi feltöltött példány elérhetőségére.

Másrészről a redundáns hálózatban az egyes csomópontok (tartalmak, elérhetőségei) kölcsönösen elérhetők egymás felületein. Az oldalak és platformok összekapcsoltságára vonatkozó feltevésem bizonyítása érdekében végeztem el, egy olyan kísérletet, amelynek keretében egy adott (fah____.r_, az elérhetőség szándékosan csonkolva) weboldalról elindulva a linkeket és felhasználói fiókokat követve egy diagrammot rajzoltam fel, amely az egyes webhelyek, közösségi médiaplatformok, névtelen megosztó tartalommegosztó oldalaknak, azonnali üzenetküldő alkalmazások robotjainak, illetve felhasználói fiókjainak elérhetőségét kapcsolja össze. A linkek és a kapcsolatokat, ahol lehetett maximálisan három szint mélységig követtem. Az olyan felhasználói fiókoknál, robotoknál, ahol a továbbjutás a terroristákkal való kommunikációval járt volna a nyomon követést megszűntettem. A Telegram robotokat például a nap 24 órájában arra használják, hogy a „védett" csatornákba a felhasználó bejutását bizonyos kulcsszavak megadása mellett lehetővé tegyék, tehát egyes esetekben egyfajta kapuőrökként szolgálnak.

A felderített forrásokat adatbázisba foglaltam és a yED 3.23.2 vizualizációs szoftver segítségével hálózati diagrammot készítettem, amely 15. számú ábrán látható.



15. ábra Egy kiválasztott weboldalról követett linkek kapcsolódásának ábrázolása forrás: a szerző munkája

Az ábrán a piros csillag a kiindulópontot jelöli, ahonnan a linkeket követve a fenti ábra rajzolódott ki. A sárga háromszögek a nyílt weboldalakra mutató linkeket jelölik, a zöld színű háromszöveg az alternatív tartományi rendszereken található tartalmakhoz vezetnek, míg a szürke négyszögek a dark weben található oldalakra mutatnak. A kék trapézok Telegram felhasználói fiókokat, vagy botokat takarnak. A sötétkék csillag a webarchívumon tárolt egyetlen oldalt mutat, ahonnan számos nyílt webes oldalra mutatnak tovább a linkek. Az ábrában 40 db csomópont és 50 db él (kapcsolat) található. Néhány ponton a linkek kölcsönösen egymásra hivatkoznak. Ilyet lehet látni például az ábra jobb oldalán, ahol a dark webes és a nyílt webes oldalak oda-vissza hivatkozzák egymást. A webarchívumban látható önmagába mutató nyíl azt jelenti, hogy az adott oldal egy másik webarchívumos oldalra is hivatkozott.
Természetesen egyrészt terjedelmi, másrészt kutatás etikai és bűntetőjogi megfontolásokból a bemutatott felmérés csak egy kis szeletét villantja fel a többszörösen összetett hálózatnak, azonban megítélésem szerint alkalmas arra, hogy demonstráljam hogyan is néz ki a gyakorlatban az általam említett redundáns tartalommegosztó és kapcsolattartó rendszer.

A redundáns tartalommegosztó és kapcsolatfenntartó rendszer elemei:

A Wayback Machine mint tartalomelosztó központ

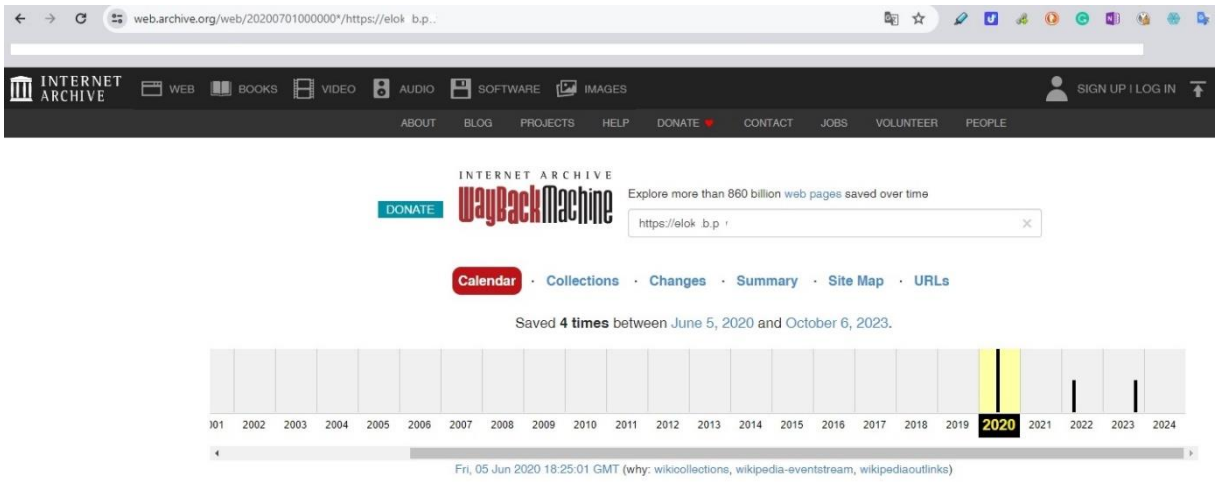
A Wayback Machine az Amerikai Egyesült Államokban Internet Archive néven bejegyzett non-profit szervezet által alapított és üzemeltetett szolgáltatás azzal a céllal jött létre, hogy megőrizze az Internet múltját és ingyenesen kutathatóvá tegye a nagyközönség számára. Az archive.org webhelyen digitális könyvtár, film és kép archívum található párosítva azzal a különleges lehetőséggel, hogy gyakorlatilag az online tér valamennyi webhelyének megtalálható rajta az időközönkénti mentése. Röviden: a felhasználónak lehetősége van egy adott webhely adott időpontban létezett állapotának megtekintésére.[3] Ez a képesség nagyon jó lehetőséget biztosít a kutatóknak. Sajnos vagy szerencsére bizonyos terrorvonatkozású anyagok blokkolva vannak, ezekhez a felhasználók nem férhetnek hozzá, azonban ennek a tiltásnak a logikájára nem sikerült rájönnöm, ugyanis más esetekben nagyon komoly propagandaértékkel és elrettentő erővel bíró anyagok a regisztrált felhasználók számára korlátozás nélkül elérhetők. Az egyes weboldalak mentéseit egy idősíkon ábrázolja a rendszer és a megfelelő dátumra kattintva a felhasználó hozzáfér a kérdéses weboldalhoz. Az Iszlám Állam honlapjai esetében

[3] A szolgáltatással kapcsolatban további információk érhetők el a https://archive.org/about/ oldalon

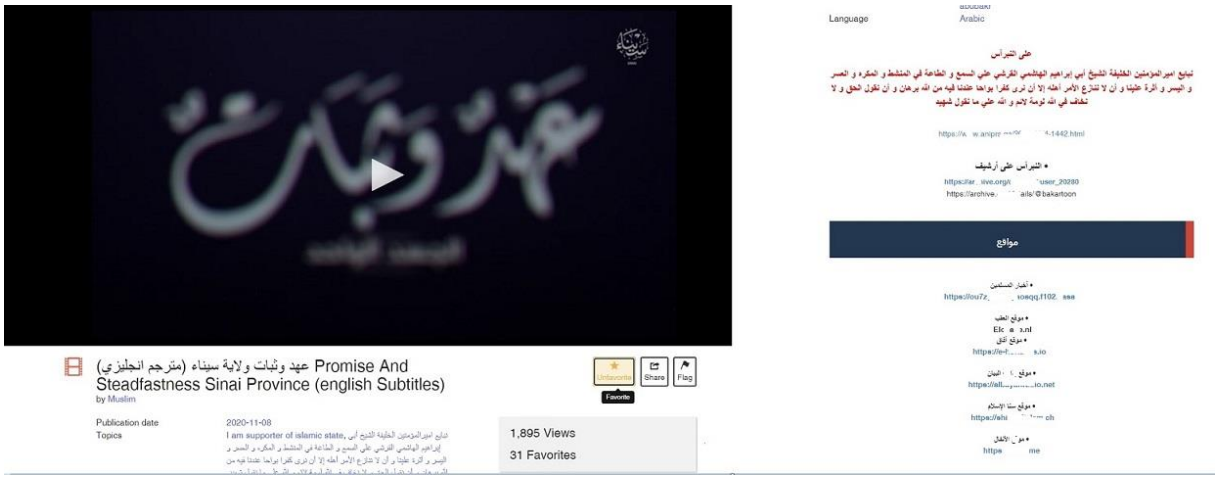
a mentések száma viszonylag kevés, ahogy az a 16. számú ábrán is látható, hiszen az aktiválásukat követően az oldalakat a hatóságok rövid időn belül lekapcsolták.

Az archívum másik rendkívül népszerű szolgáltatása a felhasználók saját archívumának létrehozási lehetősége. Ennek értelmében egy adott felhasználó digitalizált szöveg, kép, hang és videó archívumot hozhat létre, amelyhez a többi felhasználó is hozzáférhet. Ez az a képesség, amelyet a terrorista vonatkozású tartalmak megosztására használnak fel a média mudzsahedek. A kutatásom során találtam például olyan felhasználót, aki egymaga több mint háromszáz Iszlám Állam vonatkozású videót oszt meg. Jellemzően ezekhez az oldalakhoz üzeneteket további linkeket csatolhatnak, további elérhetőségeket adhatnak meg, ahogy az 17. számú ábrán is látható, ahol egy Iszlám Állammal szimpatizáló felhasználó videót és további linkeket oszt meg más felhasználókkal.

Összességében megállapítható, hogy az archívum jelentős szerepet tölt be jellemzően az Iszlám Állam tartalommegosztó rendszerében.



16. ábra a webarchivum időközönként mentést készít a weboldalak pillanatnyi állapotáról. Forrás: a szerző képernyőfotója az Iszlám Állam egyik honlapjának mentéseiről.



17. ábra Egy Iszlám Állammal szimpatizáló felhasználó oldala, ahol videót és további linkeket oszt meg. forrás: a szerző képernyőfotója (a linkeket szándékosan csonkoltam)

Telegram robotok

A Telegramon a robotok általában a következő kulcsfontosságú funkciók egyikét látják el: tartalomelosztás, beszélgetések moderálása, kapuőrség és archívumszolgáltatás.

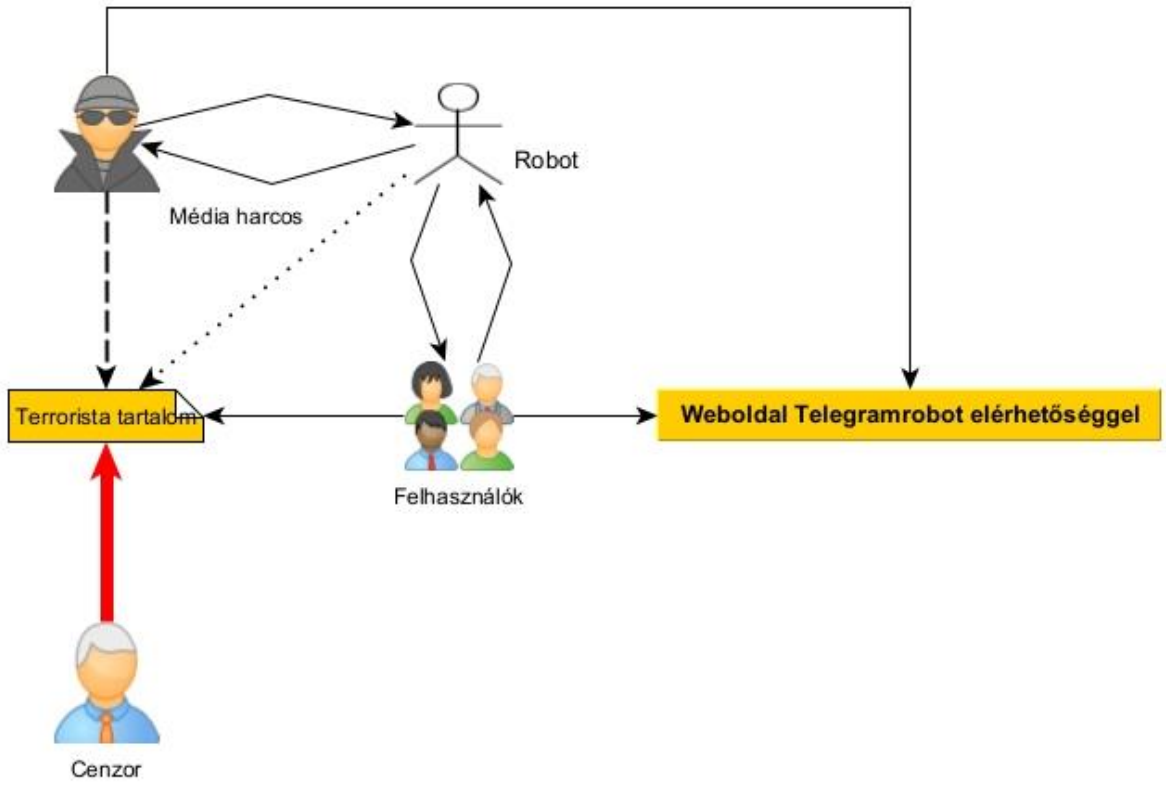
A robotok tehát fontos szerepet játszanak a szervezet Telegram ökoszisztémájának fenntartásában, hiszen számos vonatkozásban képesek az élőerő helyettesítésére, illetve tehermentesítésére. Ezek a szoftverkomponensek képesek a tartalom megosztására így részt vesznek az ideológia felerősítésében. Ezen túl a nyilvános, illetve zárt csoportokban folytatott beszélgetések moderálására, illetve egyfajta tartalomszűrő feladatokra is használják őket, valamint képesek fizetések fogadására is. A Telegram alkalmazás számos nemzetközi pénzügyi szolgáltatóval van szerződésben és így az ezeken keresztül történő pénzküldésre és fogadására is van lehetőség.

Az Iszlám Állam tagjai (aktivistái) a robotok és az élőerő kombinált alkalmazásával egy hibrid rendszert hoztak létre, amely hatékonyabbá teszi a szervezet tevékenységét az online térben. Ez a hibrid rendszer és a Telegram titokvédelmi és információbiztonsági politikája lehet az oka annak, hogy a szervezet már évek óta komolyan támaszkodik erre a platformra.

A felhasználó általában egy weboldal, vagy közösségi média hivatkozás révén jut el egy telegram robothoz. A robot a kapcsolatfelvételt követően funkciójától függően viselkedik. Működhet egyfajta hídként a felhasználói fiókok között elrejtve ezzel egy fontosabb felhasználót a külvilág elől, vagy csak rögzíti a jelentkezés tényét és majd az adminisztrátora dönt a jelentkező felvételéről a csoportba, de adott esetben kérdésekre adott válaszoktól, vagy

jelszótól függően automatikusan is adhat hozzáférést a meglátogatni tervezett csatornához. Ez utóbbi funkció folyamata jól nyomon követhető a 18. számú ábrán.

Esetünkben a médiaharcos létrehoz egy telegramrobotot, amelynek az elérhetőségét megadja a közösségi médiában, vagy más weboldalakon. Létrehozza a publikálásra tervezett tartalmat, amelynek elérhetőségét megadja a robotnak, ami majd automatikusan, vagy valamilyen feltételhez kötve, átadja azt a felhasználónak, aki ez alapján felkeresheti a tartalmat. Amint egy cenzor elérhetetlenné teszi az inkriminált anyagot a médiaharcos a robotja útján, vagy pedig saját rendszeres ellenőrzése által tudomást szerez erről és haladéktalanul új elérhetőséget készít, amit ismét átad a robotnak, ami már az új elérhetőséget fogja továbbítani. A robotok alkalmazásának kétségtelen előnye, a médiaharcos kilétének titokban tartása, és a tartalomkezelés leegyszerűsítése. [10 p. 1,2]



18. ábra A Telegramrobotok szerepe a tartalommegosztásban (a szerző szerkesztése)

A weboldalak

Az Iszlám Államhoz köthető weboldalak a propaganda tevékenységen túl nagyon fontos szerepet töltenek be a tartalommegosztás és a kapcsolattartás folyamatosságának biztosításában, mivel mindig tartalmaznak tovább mutató linkeket a szervezet más weboldalaira, online archívumaira, Telegram robotokra, illetve kapcsolattartó e-mailekre, vagy Jabber elérhetőségekre.

A Paste.bin jellegű és fájlmegosztó oldalak

A Paste.bin jellegű oldalak eredetileg programozói fórumoknak indultak, hiszen azzal a céllal hozták létre őket, hogy a programozók szabadon, anonim módon oszthassák meg kódjaikat másokkal. Ez a rendeltetés hamarosan kinőtte magát és alapvetően az ilyen oldalak illegális tartalmak megosztásának melegágyaivá váltak. A névtelen tartalommegosztás lehetővé tette különböző feltört felhasználói fiókok adatainak, illetve digitális szolgáltatásokhoz való illegális hozzáférések terjesztését. Ezt a lehetőséget a terrorszervezetek szimpatizánsai is felismerték és az illegális tartalmak, vagy azok elérhetőségeinek terjesztésére használják ezeket. Az Al Kaida például többek között a NOTE.share platformon osztja meg tartalmait.

Csevegőalkalmazások

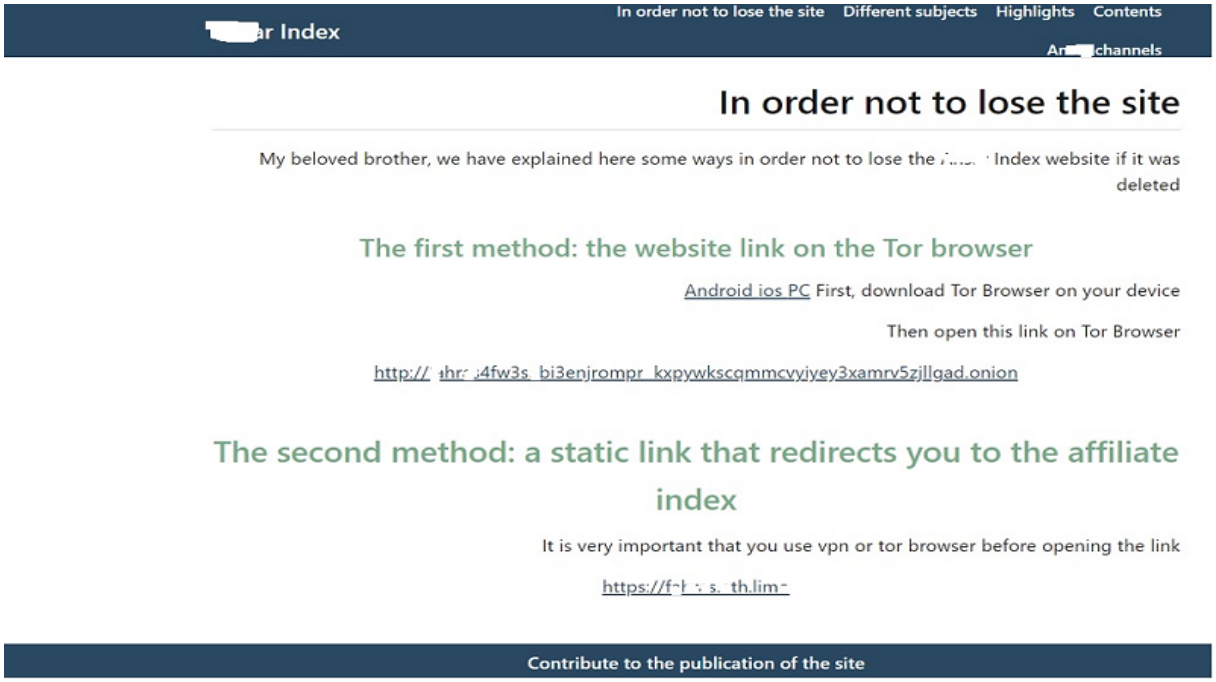
Az Iszlám Állam szimpatizánsai jellemzően a Telegramot, a Rocket.Chat, valamint az Elements platformokat és a JabberIM-et használják. Ezek a platformok biztosítják a számukra megfelelő anonimitást és titkosságot. A kutatás témájának szempontjából vizsgálva a platformok szerepe a tartalmak elérhetőségének megosztása és a kapcsolattartás folyamatosságának biztosítása. Ez annál is célszerűbb számukra, mivel a végpontok között titkosított kommunikációból adódóan a szolgáltatók, illetve a rendvédelmi szervek nem tudnak kontrollt gyakorolni a platformok felett.

A dark web szerepe

Az első hipotézissel kapcsolatos kutatás eredményeként bizonyítottam, hogy a dark web nem tekinthető az Iszlám Állam és más dzsihadista terrorszervezetek online tevékenységének kiemelt működési területeként, hiszen ezen szervezetek tevékenysége jellemzően a nyílt interneten zajlik. Ugyanakkor a dark web jelentőségét különösen az Iszlám Állam esetében nem szabad alul értékelni, hiszen a szervezethez köthető dark webes oldalak rendkívül fontos szerepet töltenek be, mint a legfontosabb nyílt webes tartalmak tükörképei, egyfajta tartalékai, másrészt ezek az oldalak magasfokú cenzúraállóképességük okán fontos szerepet játszanak a követőikkel kialakított folyamatos kapcsolat fenntartásában. Ezeken az oldalakon megtalálhatók a nyílt webes tartalmak legújabb elérhetőségei, kapcsolatfelvételi email címek, közösségi médiafiókok, Telegram csatornák, robotok elérhetőségei. Ilyen oldal képernyőfotója látható a 19. számú ábrán. A képen látható színes szöveg a tartalomhoz vezető linket rejti. A linkek naprakészek, követik a nyílt weben található oldalak elérhetőségét. A linkek sorban fentről lefelé: Egy független muszlim híroldal a TOR rendszeren, I'lam Foundation

weboldalának legújabb nyílt webes elérhetősége, majd ugyanennek a szervezetnek a dark webes oldala következik, lejjebb pedig az Al Raud Media Archive nyílt és dark webes elérhetőségei láthatók.

Összességében tehát kijelenthető, hogy a dark web fontos összetevője az Iszlám Állam médiaökoszisztémájának.



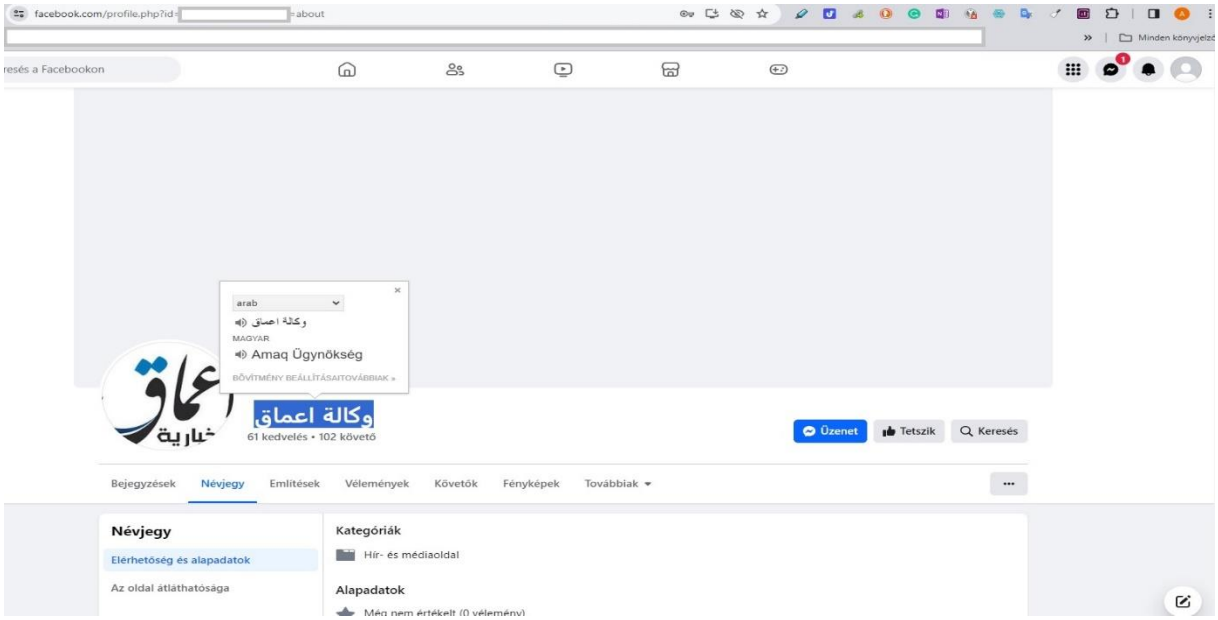
19. ábra Az Iszlám Állam tartalomelosztó és kapcsolat fenntartó dark webes oldaláról készült képernyőfotó. forrás: a szerző képernyőfotója (az elérhetőség szándékosan csonkolásra került)

2.5.6 Közösségi média szerepe a tartalommegosztás és kapcsolattartás rendszerében

Kapcsolattartás a Facebookon

A Facebook a népszerűségét olyan integrált szolgálatatásoknak köszönheti, ismerősök gyűjtésének lehetősége, a tetszésnyilvánítás (like), a tartalommegosztás, a hírfolyam, az idővonal és az élőközvetítés lehetősége és nem utolsó sorban a jelölő címkék (#hastag) alkalmazása. Ugyanakkor a platformon szigorú tartalomellenőrzést folytatnak, amelynek a pártatlanságáról ugyan lehet vitatkozni, azonban a terrorista tartalmakkal szemben vitán felül igyekeznek következetesen eljárni. Ennél fogva napjainkban már korántsem olyan egyszerű nyíltan terrorista tartalmat találni a platformon. A már korábban ismertetett kulcsszavakkal végrehajtott keresés eredményeként Iszlám Állam vonatkozású oldalt egyet találtam. Ahogy az a 20.számú ábrán látható az Amaq hírügynökség oldala jelentkezett találatként, azonban az oldal privát így nyilvános tartalom vagy az ismerősök listája nem érhető el. Természetesen semmi garancia sincs arra, hogy ez valóban a hírügynökség oldala, hiszen lehetséges, hogy csak

egy aktivista üzemelteti. Mindenesetre érdekes, hogy az oldal a Facebook tartalomszűrőjén átcsúszott pedig az ügynökség logója is szerepel az oldalon.



20. ábra Állítólagos Amaq hírügynökségi oldal a Facebookon forrás: a szerző képernyőfotója

Iszlám Államhoz köthető tartalomhoz kerülő úton, úgynevezett vezető aktivisták (connector nodes) segítségével áttételesen lehet hozzá jutni, azonban ehhez az illető ismerősévé kell válni. Jellemzően az ilyen személyeknek több tucat Facebook ismerősük van. A saját profiljaikat is klónozzák, így, ha az adott fiókot a szolgáltató blokkolja, szinte azonnal tudja folytatni a tevékenységét, miközben újabb klónokat generál. Ezt a módszert követik a felhasználók is, és így gyakorlatilag egy kiirthatatlan hálózat veti meg a lábát a platformon. A biztonság kedvéért természetesen egymásnak más platformon létrehozott elérhetőségüket is megadják, így még egy sikeres Facebook művelet sem tudná a hálózatot felbomlasztani. [23]

Ezek a hálózatok napjainkban már nem terjesztenek a korábbihoz mérhető brutalitású célirányos propagandát, hanem helyette egyfajta bújtatott (suttogó) propagandát folytatnak a Facebookhoz hasonlóan szigorú kontrol alatt tartott platformokon. Példaként említhető, hogy amikor a 2023 tavaszán Etiópiában mecsetrombolási hullám kezdődött (https://www.akem.org.tr/post/mosques-demolished-in-ethiopia), akkor az Iszlám Állam propagandistái felhasználva az etióp muszlim közösség felháborodását, ezt úgy tálalták a közösségi médiában, hogy az ilyen cselekedetek ellen keményen fel kell lépni. De a korábbiaktól eltérően nem hangzott el a konkrétan a szervezet neve, azonban a felvételen látható jelképek és a nyelvezet azt sugallták, hogy a felhívás mögött az Iszlám Állam áll, ami

szembeszáll ezzel a „barbár” cselekedettel és aki igazhívő az csatlakozik az ügyükhöz. Arra vonatkozóan, hogy ez egy új taktika kezdete, vagy csak egy kísérlet volt nincs további információm.

Az úgynevezett vezető aktivistáknak több tucat Facebook-ismerősük van. Ezek az emberek megjelölik az Iszlám Állam szimpatizánsait vagy a tartalom támogatóit, hogy az új vagy visszatérő személyek könnyebben azonosíthassák őket a kitiltásuk után. Ez egyrészt csoportépítésre szolgál másrészt, ha nem tiltják le a biztonsági beállításoknál, akkor a tartalom megjelenik az idővonalon, és az ismerősök is láthatják. Baráti láncon keresztül a tartalom rövid időn belül széles körben elterjed. Az ilyen típusú tartalmak gyakran tartalmaznak más platformokra mutató hivatkozásokat. Az aktivistáknak általában több felhasználói profiljuk is van, amelyek egymás barátai, így az egyik profil kitiltása után nem különösebben nehéz újra kapcsolatba lépni a csoport többi tagjával.

A közösségi média „meghekkelése”

A közösségi média szerepe nem elhanyagolható az Iszlám Állam online propagandagépezetében, bár tagadhatatlanul az utóbbi időben a közösségi média érdekelt feleinek együttműködésével kialakított védelmi hálónak köszönhetően ez a tevékenység évről évre visszaszorul és amint az a Twitter esetében is megfigyelhető volt platformot vált. Mégis a küzdelem még nem ért véget, és mint ahogy az a 21. számú ábrán is a Bank al Ansar alapítvány Telegram csatornáján terjesztett videóban látható ezres nagyságrendben képesek létrehozni felhasználói fiókokat az egyes közösségi média platformokon. A módszerekről nem esik szó a videóban, azonban feltételezhető, hogy ehhez a munkához is, ügyelve az anonimitás fenntartására, a média mudzsahedek segítségét veszik igénybe. [39]

21. ábra Bank al Ansar alapítvány telegram csatornáján terjesztett videó szerint a képen látható számú felhasználói fiókot hoztak létre a közösségi médiában.

2.6. Összefoglalás

A hipotézis igazolásának vagy cáfolásának érdekében a kutatás során azért esett a választás az Iszlám Állam tevékenységének részletes bemutatására, mert egyrészt a többi szervezetnél jóval nagyobb online jelenléttel rendelkezik és ebből adódóan jóval inkább a hatóságok látókörében van, ami azt eredményezi, hogy nagyobb nyomás nehezedik rá. Ez ellen a fokozott nyomás ellen hatékonyabban kell küzdenie ennél fogva a technikák és módszerek szélesebb körű alkalmazására kényszerül. A kisebb jelenléttel rendelkező szervezetek is alkalmazzák ugyan a rendszer egy- egy elemét, azonban célravezetőbbnek tartottam egy szervezeten keresztül a komplex egész bemutatását, amely a lehetséges technikák és eljárások teljes spektrumát feltárja az olvasó előtt és lehetővé teszi a deplatformizáció elleni harc rendszerszintű megközelítésének bemutatását.

Az értekezés első részében ismertettem, hogy milyen lehetőségek állnak az úgynevezett Tech óriások és a közösségi média érdekelt feleinek rendelkezésére, amelyekkel korlátozhatják, illetve akadályozhatják a nemkívánatos közösségek, térnyerését, illetve propagandájuk terjesztését.

A kutatás további szakaszában adatbázist építettem, amelyben dzsihadista weboldalakat gyűjtöttem össze. Az oldalakat szervezetenként csoportosítottam, ezzel igazoltam, hogy a szélsőséges iszlám terrorszervezetek képviselik magukat az online térben, mi több néhányan hosszú évek óta zavartalanul lehetnek jelen a világhálón. Ezt az adatbázist használtam fel arra, hogy tanulmányozzam a dzsihadista terrorszervezetek ún. kikerülési technikáit, illetve az Iszlám Állam redundáns tartalommegosztó és kapcsolattartó hálózatát.

A könnyebb áttekinthetőség érdekében logikai rendbe szedtem az egyes technikákat és eljárásokat, amelyeket az Iszlám Állam az online térben alkalmaz annak érdekében, hogy a folyamatos jelenlétét biztosítsa.

Az ellenintézkedéseik rendszere meglátásom szerint két külön összetevőre választható szét. Az első a technikai megoldások rendszere. Én ide sorolom például sok más egyéb mellett a különböző platformok közötti migrálását, illetve a webhelyek felső szintű tartományneveivel való trükközést stb. A második csoportba azok az eljárások tartoznak, amelyek nélkül az előbbi technikai fogások nem lennének ennyire hatékonyak. Ebbe a csoportba sorolom a kiberbiztonsági oktatást és a kétségtelenül legeredetibb ötletet, a médiaharcos intézményének alkalmazását, amelyet az Iszlám Állam mester szintre fejlesztett.

Az előző két összetevőhöz szorosan kapcsolódik a következő innováció, amely a tartalomelosztás és a kapcsolattartás folyamatosságát biztosító redundáns kapcsolatokból felépített hálózat, amely így rendszerbe foglalva az Iszlám Állam innovációja.

A valós képhez hozzátartozik, hogy az Iszlám Állam a 2019-es területi veszteségeit követően az online térben is időről időre teret veszít. A rendvédelmi szerveknek és a közösségi média érdekelt feleinek erélyes fellépésének hatására a szervezet lehetőségei érezhetően szűkültek, de ez igaz egyébként más terrorszervezetekre is. A 2018-ig tapasztalható nyílt propaganda terjesztés helyét online kapcsolati pontok, és a media mudzsahedek által működtetett online tartalomelosztó, tartalomsokszorzó központok vették át.
Ezek az intézkedések azonban káros mellékhatásokkal is jártak, hiszen mint a fizikában úgy az online térben is egy adott hatás azonos mértékű ellenhatást eredményez. Az Iszlám Állam ellen irányuló intézkedések és korlátozások azzal jártak, hogy a szervezet áthelyezte tevékenységét az eddig viszonylag könnyen ellenőrizhető platformokról olyanokra, amelyeknek az ellenőrzése nagyságrendekkel nagyobb kihívást jelent. Ebből adódóan nehezebben azonosíthatók be az aktivisták, a szimpatizánsok és a platformokon folyó tevékenység. Technikai oldalról a végpontok közötti titkosított kommunikáció, míg humán oldalról a fórumokon, a csetszobákban, a kapcsolati központok működtetői között megnövekedett bizalmatlanság okán biztonsági intézkedéseket vezetnek be a belső konspiráció megtartása érdekében, ami jelentősen nehezíti a hatóságok felderítő munkáját. Ez a terrorszervezetek online tevékenysége elleni harc dilemmája.

Következtetés

A kutatásom során összegyűjtött adatok elemzését követően hipotézisemet, mely szerint:

„Feltételezhető, hogy a szélsőséges iszlám terrorszervezetek olyan technikákkal, taktikákkal és eljárásokkal rendelkeznek, amelyek segítségével a nyílt internet és a dark web előnyeit mesterien kihasználva a közösségi média tartalom szűrőit és a rendvédelmi szerveket kijátszva képesek biztosítani folyamatos jelenlétüket a világhálón ”

igazolom.

A kutatás során létrehozott adatbázis igazolja, hogy a rendvédelmi szervek és a közösségi média érdekelt feleleinek korlátozó- akadályozó intézkedési ellenére nyíltan mindenki számára elérhető módon jelen vannak a szélsőséges iszlám terrorszervezetek az online térben. Az esetleges korlátozó akadályozó intézkedésekre képesek reagálni és rövid időn online jelenlétüket helyreállítani.

III. FEJEZET

DZSIHADISTA TERRORSZERVEZETEK KRIPTOVALUTA HASZNÁLATA

Feltételezhetően a szélsőséges Iszlám terrorszervezetek a nemzetközi pénzügyi korlátozó és szankciós intézkedések hatására pénzügyi műveleteik elrejtése érdekében a részleges anonimitást biztosító kriptovaluták felé fordultak.

A terrorszervezetek kriptovaluta-alapú online adománygyűjtésével kapcsolatban az alábbi publikációt készítettem:

- Gulyás Attila: „Dzsihadista terrorszervezetek kriptovaluta alapú online adománygyűjtése", *Honvédségi Szemle – Hungarian Defence Review*, 152(5), o. 60–78. doi: 10.35926/HSZ.2024.5.4.
  Besorolás: Hazai „A"

Bevezetés

A terrorszervezeteknek ideológiai és földrajzi elhelyezkedésüktől függetlenül van egy közös vonásuk, mégpedig a működésükhöz szükséges anyagi eszközök előteremtésének kényszere. A szervezetek költségvetése alapvetően két fő kategóriára osztható: a fenntartással kapcsolatos és a műveletek finanszírozását biztosító műveleti költségekre. Egyes terrorszervezetek esetén ez kiegészül a szociális költségekkel, amelyek a mártírok, sebesültek, illetve rokkantak, valamint szociális létesítmények (iskola, kórház) fenntartását szolgálják. Az ilyen összetett gazdálkodás elengedhetetlenné teszi a költségvetés készítését, amelyhez az anyagi alapokat alapvetően legális és illegális úton teremtik elő. A megszerzett pénzt azonban tárolni kell valamilyen formában, szükség esetén mozgatni kell, akár határokon túl is, illetve valahogyan és valahol fel is kell használni. Ezek az elemek alkotják a terrorszervezetek pénzügyi műveleteit. [76 pp. 38-66]

A terrorizmus elleni harc egyik legfontosabb összetevője a terrorszervezetek pénzügyi műveleteinek megakadályozása érdekében a hagyományos banki pénzmozgások (fiat valuták áramlása) ellenőrzése és figyelemmel kísérése, valamint a pénzmosás elleni nemzetközi szintű intézkedések kidolgozása és alkalmazása.

Az összehangolt és egyre hatékonyabb nemzetközi szintű terrorizmusfinanszírozás (Counter-Terrorist Financing a továbbiakban: CTF) és pénzmosás ellenes (Anti-Money Laundering a továbbiakban AML) intézkedések hatására a terrorszervezetek lépéskényszerbe kerülnek és kénytelenek olyan módszereket és technikákat kifejleszteni, amelyek segítségével ezeket az intézkedéseket kijátszhatják, illetve megkerülhetik.

Tekintettel arra, hogy a terrorszervezetek rendkívüli gyorsasággal képesek az új technológiákat befogadni és alkalmazni [78] a rendvédelmi szervek és a politikai döntéshozók részéről felmerült annak a lehetősége, hogy a korlátozó intézkedések kijátszása érdekében a részleges anonimitást és központi irányítást nélkülöző kriptovaluták felé fordulnak. [79] Amennyiben ez megtörténik a terrorszervezetek ismét lépéselőnybe kerülnek, hiszen a rendvédelmi szerveknek hosszabb időt vesz igénybe, hogy felkészüljenek az ilyen jellegű műveletekkel kapcsolatos nyomozati technikák kidolgozására és az elkövetők igazságszolgáltatás elé történő állítására. Tovább nehezíti ezt a feladatot, hogy szinte naponta jelennek meg új kriptovaluták, amelyek közül számos olyan lehetőségeket kínál, amellyel a felhasználók gyakorlatilag a rendvédelmi szervek elől rejtetten bonyolíthatják pénzügyi műveleteiket. Természetesen a helyzet nem egyszerű a terrorszervezetek számára sem, hiszen a kriptovalutáknak is vannak hátrányai, hogy csak egyet említsek ezeket valahol vagy el kell költeni, vagy át kell váltani hagyományos valutákra. Az elfogadó helyek korlátozott száma, illetve a valutaváltás infrastrukturális nehézségei a kriptovaluta használat ellen szólnak. Ebből a néhány kiragadott példából látható, hogy a kérdés rendkívül összetett. Ez okozhatja azt, hogy a terrorszervezetek kriptovaluta használatával kapcsolatban számos egymásnak részben vagy teljesen ellentmondó publikáció, illetve médiatudósítás lát napvilágot, amelyek között nehéz eligazodni. Kutatásom célja, hogy a nyílt információgyűjtés eszközeinek és módszereinek felhasználásával összegyűjtött adatok feldolgozását és elemzését követően állást foglalhassak abban a kérdésben, hogy a dzsihadista terrorszervezetek a nemzetközi pénzügyi korlátozó intézkedések hatására pénzügyi műveleteik folytatása, illetve elrejtése érdekében valóban áttértek-e a kriptovaluták használatára.

3.1 Szakirodalmi áttekintés

A szakirodalom áttekintése során azzal a nehézséggel kellet szembe néznem, hogy az idevágó publikációk jelentős része 2016 és 2020 időszakában íródott, amikor a kriptovaluták igazán kezdtek népszerűvé válni, ugyanakkor a blokkláncelemzésben rejlő lehetőségek különösen a bitcoin esetében nem voltak közismertek. Napjainkra kiderült, hogy a blokkláncelemzési technikák fejlődése következtében a kriptovaluták névtelenségébe vetett hit jórészt tévesnek bizonyult. A jelzett időben készült tudományos publikációk jelentős részükben idejét múltak,

vagy az akkori feltételezéseket az idő meghaladta. Ebben a dinamikusan fejlődő technikai és műveleti környezetben célszerűbb a napi eseményekre és a témára specializált vállalatok, illetve ThinkTank-ek (agytrösztök) jelentéseire támaszkodni.

A következőkben a terrorszervezetek kriptovaluta használatára vonatkozó egymásnak ellentmondó megállapítások és beszámolók segítségével érzékeltetném a témában kialakult bizonytalanságot.

A Reuters az elmúlt év októberében ENSZ szakértőkre [40] hivatkozva arról tudósít, hogy senki sem tudja biztosan a terrorszervezetek kriptovaluta-használatának mértékét, csak valószínűsíteni tudják, hogy az nem jelentős.[40]

Az ENSZ Biztonsági Tanácsának Terrorizmusellenes Bizottsága 2022. 10. 28-29. között Mumbaiban ülésezett, ahol Svetlana Martynova a terrorizmus finanszírozása elleni küzdelem koordinátora interjút adott, amelyben újságírói kérdésre elmondta, hogy az elmúlt néhány évben a terrorizmusfinanszírozásban a kriptovaluták aránya 5%-ról 20%-ra emelkedett és további emelkedés várható. [41]

A Chainanalysis (világszerte elismert blokkláncelemző vállalat) jelentése szerint az összes illegális kriptovaluta forgalom mindössze egy százaléka köthető terrorizmusfinanszírozáshoz. [42]

Az Elliptic kriptovaluta blokkláncelemző cég jelentése szerint a terrorszervezetek kriptovaluta használata meredeken nő. [43] Whang és Zhu tanulmányukban arról számolnak be, hogy a terrorszervezetek kriptovalutahasználata fontos része a szervezetek pénzügyi rendszerének, ennek ellenére aránya mégsem számít számottevőnek. [44 pp. 1]

A Coindesk (kriptovalutára specializálódott szaklap) cikke szerint az Egyesült Államok pénzügy minisztere Janet Yellen a Szenátus Pénzügyi bizottsági meghallgatásán úgy nyilatkozott, hogy a kriptovaluták használata a terrorizmusfinanszírozásában különösen komoly aggályokat vet fel.[45] Az ENSZ Biztonsági Tanácsának Szankciómonitorozási Bizottságának 2021-ben írott levele szerint az Iszlám Állam és az Al Kaida kriptovaluta használata növekszik. A francia rendőrség szerint 29 személy szerte az országban kis összegű kriptovaluta kuponokat vásárolt, amelynek a felhasználási kódját titkos csatornán keresztül elküldték a szíriai HTS terrorszervezet tagjainak, akik felhasználták a kuponokat.

Az Egyesült Államok 2020 augusztusában arról tájékoztatta a bizottságot, hogy felszámoltak egy Telegramon folytatott online adománygyűjtési kampányt, amely kriptovalutát gyűjtött az Al Kaida részére.[46]

Az Európai Unió Emberjogi és Alkotmányügyi bizottsága által támogatott jelentés szerint a terrorszervezetek kriptovaluta használatát nehéz megbecsülni, de a szervezetek keresik az útját

a minél szélesebb körű használatnak. A jelentés szerint a kriptovalutát közösségi médiában folytatott adománygyűjtésre, illetve illegális javak dark weben történő beszerzésére fogják fordítani, valamint a nemzetközi banki átutalások helyettesítése is lehetséges ezen a módon. A jelentésben lehetőségként felmerül a kiberbűnözés és a terrorizmusfinanszírozás összefonódása is. [47 p. 9]

A New York Times 2019 augusztusában megjelent cikkében az Egyesült Államok pénzügyminiszterére és a CIA egykori elemzőjére hivatkozva arra hívja fel a figyelmet, hogy a terrorszervezetek egyre inkább a kriptovaluták felé fordulnak azok viszonylagos névtelensége és központi szabályozottságának hiánya miatt. [48]

Wiwoho és társai arról számolnak be tanulmányukban, amelyben iszlám terrorszervezetek kriptovaluta-használatát vizsgálták, hogy az Al Kaida és az Iszlám Állam társult szervezetei előszeretettel használnak kriptovalutát akcióik finanszírozásához. Véleményük szerint a terrorszervezetek kihasználva a szabályozás hiányát várhatóan nagyobb mértékben fordulnak a kriptovaluták felé. [49 p. 19]

A CNAS (Center for a New American Security) 2020-ban készült jelentése szerint a terrorista csoportok egyre inkább a kriptovaluta-alapú adománygyűjtés felé fordulnak, amelynek során előnyben részesítik a közösségi média nyújtotta lehetőségeket. A jelentés szerint a terrorista csoportok hozzáértő digitális szereplőkké válnak. [50]

3.1.2 Szakértői csoportokhoz köthető irodalom

Az Al Kaida vonatkozásában az Egyesült Államok Igazságügy Minisztériuma az Al Kaida finanszírozásának megakadályozását célzó kampányában számos Telegram csatornát fedett fel, amelyek a szervezet részére bitcoinban gyűjtöttek támogatást. A hatóságok munkájának megnehezítése érdekében minden adomány részére szoftveresen új egyedi címet generáltak. Annak ellenére, hogy a címek nyilvánosak voltak különböző műveletekkel sikerült a hatóságokat kijátszaniuk és sikeresen tisztára mosni a kapott kriptovalutát.

A szakértők ezzel kapcsolatban megjegyezték, hogy bár terrorszervezetek kriptovaluta használata veszélyt rejt magában, de a szervezetek pénzmosási és kriptovalutával kapcsolatos műveleti tudásszintje jelentősen elmarad az észak- koreai kiberbűnözők képességeitől. [50]

A blokklánc elemzéssel foglalkozó Chainanalisys jelentése szerint az Al Kaida Szíriában több kisebb terrorszervezettel együtt kriptovalutaalapú adománygyűjtő kampányt indított. A műveletiket több rétegű tranzakciókkal fedték el, majd elosztották egymás között. A blokkláncelemzés a nyomozókat egy a szíriai Idlibben található BitCoinTransfer Office-hoz,

mint csomóponthoz vezettek. Az irodán 2018-as megnyitása óta mintegy 280 ezer dollár ment át, amelynek egy része terrorizmusfinanszírozáshoz köthető. [51],

Az Iszlám Államot illetően a TRM labs adati szerint az Iszlám Állam társult szervezete az Afganisztánban működő Korazán tartomány (Islamic State Khorasan Province röviden: ISKP) média ügynöksége az Al Azazim Médiaügynökség kriptovalutában fogad el adományokat. A TRM labs Bitcoin, Ethereum és Tron címet azonosított. A címeket megvizsgálva megállapították, hogy a Tron cím egyenlege kevesebb mint ezer dollár volt, míg a másik kettőt nem használták. [52] Az ISKP kriptovaluta használatával kapcsolatban az Egyesült Államok Államkincstára arra hívja fel a figyelmet, hogy az Iszlám Állam dél-ázsiai szervezetei egyelőre még kis mértékben, de próbálkoznak a kriptovaluta alkalmazásával. [53] Az ISKP pénzügyi kapcsolatokkal rendelkezik Szíriában és Törökországban. Szíriában kriptovaluta tőzsde működik, ahol válthatnak a kriptovaluták között, míg Törökországban lehetőség van a kriptovaluta elköltésére, vagy készpénzre váltására, amit aztán a hawala[4] rendszeren keresztül tudnak továbbítani.

A Hezbollah finanszírozását illetően az Izraeli Védelmi Minisztérium 2023 júniusában nyilatkozatot adott ki arról, hogy hírszerzési információik szerint az Iráni Iszlám Forradalmi Gárda Katonai Hírszerző Egysége 1,7 millió dollár értékű kriptovalutát (Tron valutanemben) utalt át a Hezbollah részére. Az izraeli szakértők szerint az összeg csak egy töredéke annak a több százmillió dollárnak, amit a szervezet kap mégis ezt az akciót úttörő jellegűnek tekintik, ami igazolja, hogy kriptovaluta nyomon követő képességük szintet lépett.[54]

A HAMASZ a terrorizmus finanszírozás elleni rendszabályok kijátszása érdekében fordult a kriptovalutákhoz. A szervezet bitcoin és különböző stable coin-okat használt a pénzeszközök tárolására, illetve mozgatására. Becslések szerint 2021 és 2023 között kriptovalutában mintegy 41 millió dollár támogatást kapott. A 2023-as esztendőben azonban számos komoly csapás érte a kriptovaluta-rendszerüket. A thether kriptovaluta kibocsájtó a honlapján olvasható tájékoztatás szerint az izraeli Terrorfinanszírozási Irodával együttműködve 32 virtuális – részben HAMASZ-hoz köthető – pénztárcát fagyasztott be. Ezen túl az izraeli szolgálatok több alkalommal foglaltak le terrorszervezethez köthető nagy összegű kriptovalutát. Ezeknek a

[4] A Hawala egy arab szó, amely szó szerint fordításban „transzfer".A Hawala egy informális pénzátutalási rendszer, amelyben a pénzt brókerek hálózatán keresztül továbbítják (akiket hawaladaroknak hívnak) a készpénz tényleges / fizikai mozgása nélkül. A pénzátutalás a szokásos banki útvonalaktól eltérő módon történik, ezért néha földalatti banknak hívják. forrás https://hu.know-base.net/7577219-hawala

csapásoknak a hatására a HAMASZ 2023 áprilisában közleményt adott ki, amelyben kijelentette, hogy megszűnteti a kriptovaluta portfólióját, a továbbiakban hagyományos valutákat használ.

A kijelentés elsőre komolytalannak tűnhet, azonban ezzel a szervezet a támogatóit védi, akik innentől tudják, hogy, aki a HAMASZ nevében kriptovalutában kér támogatást az vagy csaló, vagy a hatóság embere. [55], [56]

A Palestine Islamic Dzsihad (PIJ) a pénzeszközök mozgatására igénybe veszi a Gázában és Ciszjordániában, valamint Törökországban működő, illegális, vagy legalább is szürke kategóriába tartozó pénzügyi szolgáltatókat, mint például a Herzallah Exchange vagy a General Trading Company LLC. A PIJ alkalmankénti kriptovaluta használatát igazolják azok a sajtónyilatkozatok, amelyek szerint a hatóságok több alkalommal sikeresen foglaltak tőlük kriptovalutát, legutóbb például 2023. július 4-én, 94 millió dollár értékű tron került a hatóságok kezére. [57]

A PIJ az anyagi eszközei eredetének és pénzügyi műveleteinek elrejtése érdekében számos módszert alkalmaz. Többek között törekednek törvényesen bejegyzett jótékonysági szervezetek álcájával pénzre szert tenni, illetve tranzakcióik elrejtése érdekében előnyben részesítik a kriptovaluta mixereket és e mellett igénybe veszik az orosz Grantex tőzsdét is, amely nem veszi figyelembe a nyugati eredetű pénzügyi szankciós és korlátozó intézkedéseket. A mártírok családjainak járó támogatást a Muhjat al Qds alapítványon keresztül juttatják el a rászorulóknak. Esetenként az ideológiai ellentétek ellenére pénzügyi kérdésekben együttműködnek a HAMASZ-al. [58]

A továbbiakban a kutatás eredményeinek jobb értékelhetősége érdekében szükségesnek tartom, ha csak röviden is, bemutatni a kriptovaluta lényegét és azt, hogy milyen tényezők befolyásolhatják annak elfogadottságát, vagy másként fogalmazva használhatóságát, illetve a rendvédelmi szervek lehetőségeit kriptovalutákkal kapcsolatos visszaélések esetében.

3.2. A kriptovaluta

A kriptovaluta korunk digitális technológiájának terméke. Annak ellenére, hogy csak alig több mint egy évtizede létezik máris világméretű ismertségre tett szert pedig még a benne rejlő lehetőségek csak töredékét használjuk ki. Arra kérdésre, hogy mi a kriptovaluta (crypto currency) más választ adhat egy kriptovaluta fejlesztő, egy bankár, vagy egy befektető. A szoftvermérnök számára algoritmus és adatstruktúra, a bankár számára egy olyan új technológia, amely bizonyos mértékben veszélyezteti a pozícióit és óvatossággal kell kezelni,

míg egy felhasználó számára fizetési eszköz, vagy befektetési lehetőség. Visszatérve a kérdésre, hogy mi a kriptovaluta a válasz egy olyan virtuális fizető eszköz, amely azért létezik, mert az emberek fizetnek érte, hogy birtokolhassák. A megszerzett kriptovalutáért szolgáltatásokat, árukat lehet vásárolni, vagy beváltható hagyományos (fiat) pénzekre. Az emberek a kriptovalutát vagy online tőzsdén vásárolják, vagy eladott áruért cserébe kapják, illetve néhányan azért kapnak kriptovalutát, mert hitelesítik a tranzakciókat (bányásznak). [59 p. 1], [60 p. 1], [80]

Az első kriptovalutát egy Satoshi Nakamoto álnevű személy hozta létre bitcoin néven 2009-ben. Satosi valódi kiléte a mai napig nem ismert. A bitcoin létrehozásakor az alkotója 21 millió darabban határozta meg a korlátot, amelyből még kb. 2,3 millió maradt hátra napjainkban.

A kriptovaluták függetlenek a hagyományos pénzügyi intézményrendszerektől, nincs központi hatóságuk. A kriptovaluta értéke mögött nincs aranyfedezet vagy kormányzati jótállás. A valuta árát a hálózaton belül határozzák meg, tehát a programkódtól, vagyis az előállítás nehézségétől, a hálózaton belüli megegyezéstől és a külső hatásoktól függ. A kriptovalutákból mindig egy meghatározott mennyiséget hoznak létre. Ennek következtében az adott valuta értéke lehet kereslet-kínálatfüggő, vagy pedig egy penny, vagy egy rúpia, esetleg egy kilowatt villamos áram ára. Ez utóbbit „stable coin”- nak nevezik. A stable coin ára tehát egy referencia eszköz árához van kötve.

3.2.1 A kriptovaluták előnyei, illetve hátrányai

Az előnyök:

- a tranzakciók köztes fél közreműködése nélkül történnek;
- a kétszeri költés nem lehetséges;
- a tranzakciók díja minimális;
- a főkönyv hitelessége biztosított;
- a főkönyv megsemmisülésének esélye rendkívül kicsi;
- a rendszer működése kormányzati befolyástól mentes;
- a rendszer egyfajta anonimitást biztosít;
- az anonimitás lehetővé teszi az elnyomott rendszerekben az ellenzékiek és felkelők támogatását;
- a kriptovaluták piaci árai a központi bankoktól függetlenek, mivel a kereslet kínálaton alapulnak.

A hátrányok:

- az anonimitásból kifolyólag lehetővé teszi a pénzügyi jellegű bűncselekmények elkövetését és a bűnelkövetők kedvelt fizetőeszköze ennél fogva számos bűncselekmény kapcsolatba hozható a kriptovalutákkal;
- a kriptovaluták kereskedelme határokon átnyúló, nagy volumenű így ennek hatósági ellenőrzése rendkívül nehéz;
- a kriptovaluták hatóságok általi lefoglalása nehézkes, esetenként megvalósíthatatlan;
- a kriptovaluták egy részének működtetése magas energiafelhasználással jár;
- egyes kriptovalutákkal lebonyolított ügyletek nyomon követese egyelőre korlátozottan lehetséges. [81]

3.2.2 Kriptovaluta elfogadottság

Egy terrorszervezet esetében, amely a kriptovaluta használatra való áttérést tervezi kiemelt fontossággal bír, hogy a működési területén, vagy a tervezett felhasználás helyén milyen mértékű a kriptovauta elfogadottság. Mielőtt tovább haladnánk célszerű megvizsgálnunk, hogy milyen körülmények befolyásolhatják a felhasználók és a kriptovaluták viszonyát, vagyis milyen tényezők befolyásolják a kriptovaluták elfogadottságát, illetve használhatóságát. Könnyen belátható, hogy olyan környezetben, ahol az új fizetőeszköz széleskörben elterjedt a terrorszervezetek nagyobb valószínűséggel alkalmazhatják ezt az új technológiát, mint a digitálisan elmaradott térségekben.

A kriptovaluta elfogadását a következő tényezők eredői befolyásolják:

Személyi tényezők

A kriptovaluta használatot, befogadást befolyásoló személyes tényezők között első helyre kell tennünk az alapfokú iskolázottságot, illetve digitális tudást. Ajánlatos, hogy a felhasználó értse a kriptovaluták lényegét, belássa azok hasznosságát, de legyen tisztában a kockázatokkal is. A kriptovaluták felhasználói környezetének egyszerűnek kell lennie. Abban az esetben, ha a felhasználó el akarja rejteni kilétét, vagy a tranzakciók egyéb részleteit az átlagosat jóval meghaladó felhasználói ismeretek szükségesek, különösen az olyan nyílt blokkláncok esetében, mint a bitcoin. A személyek kriptovaluta használatát befolyásoló további tényező a fogyasztói bizalom. A napi hírekben szereplő tőzsdeösszeomlások, hackerek által kifosztott tőzsdék, a dark webbel összefüggésbe hozható bűncselekmények kapcsán felmerülő kriptovaluta műveletek megingathatják a felhasználók bizalmát a kriptovaluták iránt. [61 pp.1-2], [63 pp.1-14]

Törvényi szabályozottság, gazdasági környezet

A törvényi szabályozottság, illetve az állami garancia hiánya olyan tényezők, amelyek elrettenthetik a felhasználókat az új technológia alkalmazásától, ugyanakkor azokban az országokban, ahol a gazdasági élet egyébként is szabályozatlan ott még a kriptovalutával kapcsolatos aggodalmak is eltörpülhetnek az egyébként bizonytalan gazdasági környezetből adódó biztonsági kockázatok mellett. A szabályozottság hiánya ösztönzőleg hathat az új fizetőeszközzel kapcsolatos bűncselekmények elkövetőire, különös tekintettel a szervezett bűnözői körökre, a pénzmosásra, a terrorizmus finanszírozására és más egyéb illegális pénzügyi tevékenységekre. Ami a gazdasági környezetet illeti itt egy érdekes kettősséget egy látszólagos ellentmondást kell megvizsgálnunk. Kik vásárolnak kriptovalutát? A gazdag országok és a szegény országok állampolgárai. Egyrészt a jó gazdasági állapotban lévő országok felhasználói azért vásárolnak kriptovalutát, hogy befektessenek és nyereséget szerezzenek. A tartalékképzés, vagy megtakarítás nem a megfelelő választás, hiszen az árfolyamkockázat azzal jár, hogy elveszíthetik a megtakarításuk jelentős részét. Másrészt, egyes felhasználók vállalva a kriptovaluták esetében fennálló árfolyamkockázatot azért vásárolnak kriptovalutát, mert nem bíznak országuk hagyományos fizetőeszközében. A válság sújtotta országokban, ahol a bizonytalan politikai berendezkedés, vagy a rossz közbiztonság miatt a tulajdonukat nem érzik biztonságban az új valuta vásárlása mellett döntenek fenntartva ezzel a vagyonuk feletti önrendelkezésüket. Ez igaz még akkor is, ha az ország infrastruktúrája egyébként nem kedvező a kriptovaluta elköltéséhez.[61 pp. 1-2], [62],[63 pp. 1-14]

Infrastrukturális körülmények

A felsorolt összetevők mellett van még egy fontos tényező, amely nélkül minden optimális körülmény ellenére nem valósul meg a kriptovaluta elfogadottsága. Ez a tényező az infrastrukturális környezet, amelybe olyan komponensek tartoznak mint a megbízható elektromos áram ellátottság, a megfelelő telekommunikációs lefedettség, amely lehet mobil internet vagy vezetékes internet elérhetőség, vagyis az internetpenetráció. Triviálisnak tűnhet, de mindezeken túl szükség van olyan eszközökre, amelyek képesek biztosítani a szükséges sávszélességet, illetve alkalmasak a szükséges alkalmazások futtatására. A kriptovaluta elfogadóhelyek és automaták száma ugyancsak fontos tényező lehet, ha a kriptovaluták elterjedésének tényezőit vizsgáljuk. Az afrikai kontinensen mindössze néhány kriptovaluta automata akad és az elfogadóhelyek száma sem magas, míg például Pakisztánban automata nincs, az elfogadó helyek száma pedig húsz alatt van. Mégis Afrikában viszonylag magas a kriptovaluta vásárlók száma, amire a már korábban említett ingatag pénzügyi infrastruktúrák miatti bizonytalanság lehet a magyarázat.

Vallási, ideológiai nézőpont

Az értekezésnek nem célja a vallási kérdések értelmezése, de elkerülhetetlen, hogy megemlítsem a kriptovaluta megítélésével kapcsolatos vallási megközelítési aggályokat és ellentmondásokat. A muszlim hívők körében a kriptovaluták megítélése ugyanis nem egyértelmű. Egyes vallási iskolák a dínárral, vagy a dirhammal szemben a kriptovalutát nem tartják valódi fizetőeszköznek („haram" vagyis tiltott), mivel nincs mögötte megfogható érték. [64] Véleményük szerint a digitális fizetőeszközök a csalás és manipuláció eszközei, ezért a sharia szempontjából nem tekinthetők elfogadhatónak. Ugyanakkor, más iskolák szerint a kriptovaluta megfelel a sharia előírásainak („halal" vagyis engedélyezett), mert a tranzakciók végén előbb-utóbb fizikai javakká konvertálódik. [65]

A kétségek komolyságát alátámasztja, hogy az Egyesült Arab Emírségekben elismert vallási vezetőkből és iszlám jogtudósokból, valamint pénzügyi-befektetési és informatikai szakemberekből álló csoport létrehozott egy úgynevezett „Islam Coin" nevű kriptovalutát, amely teljes mértékben megfelel a sharia előírásinak. Az új valuta mentes a spekulációtól, a forgalomból származó hasznot teljes mértékben jótékonysági célokra fordítják. Ezzel sikerült kivédeniük a spekulációs és jogtalan haszonszerzéssel kapcsolatos aggodalmakat. [66]

Mindazonáltal az alig egy éve forgalomba került új valuta súlya a piacon egyelőre nem jelentős. A vallási vezetők kriptovalutákkal kapcsolatos megosztó véleménye hatással lehet a hívők kriptovaluta-adományozási hajlandóságára, ami befolyásolhatja a dzsihadista terrorszervezetek kriptovaluta-alapú online adománygyűjtési kampányainak eredményességét. A jelenség mögött összetett vallási és ideológiai értelmezésbeli ellentétek húzódnak meg, amelyek vizsgálata értekezésem keretein kívül esik.

3.2.3 Kriptoháború, lefoglalás

A terrorszervezeteknek mielőtt a kriptovaluták használata, illetve alkalmazása mellett döntenek mérlegelniük kell, hogy a hatóságok milyen eszközökkel és lehetőségekkel rendelkeznek a tranzakciók felderítésére, illetve a kriptovalutájuk lefoglalására.

A bűnüldöző szolgálatok lehetőségei, eszközei

A bűnüldöző és biztonsági szervek valamint a bűnelkövetők között egyfajta fegyverkezési versenynek lehetünk szemtanúi, amely a digitális térben zajlik. A kriptovaluták bevezetésének kezdetén a bűnelkövetők előnyben voltak, hiszen az egy teljesen új területnek minősült, amelyre fel kellett készülniük a bűnüldöző szerveknek. Azóta sikerült némileg behozni a lemaradásukat, amit számos sikeres akció is igazol, azonban csakúgy, mint a való világban a bűnözők még mindig egy lépéssel előrébb járnak. A bűnelkövetők olyan technikákat alkalmaznak, mint a

tranzakciónkénti egyedi cím generálása, virtuális magánhálózatok és, vagy a TOR rendszer, illetve a titkosított kriptovaluták használata (Monero, Tron, stb.).

A rendvédelmi szerveknek a kriptovalutával kapcsolatos bűncselekmények nyomozásánál hibrid módszereket kell alkalmazniuk. A hagyományos nyomozási technikák és az új eljárások összehangolt alkalmazásával számos esetben sikeresen deríthetik fel az elkövetőket. A kriptovalutával összefüggő bűncselekmények esetén sok esetben megnehezíti a nyomozást, hogy nincs azonosítható személy a digitális pénztárcák mögött. Az ilyen bűncselekmények esetében a blokkláncelemzés bizonyul a leghatékonyabb nyomozási módszernek. A főkönyv (blokklánc) és a tranzakciók egyes kriptovaluták esetében nyilvánosak így lehetőség lehet az érintett elkövető(k) beazonosítására. Célszoftverek segítségével a pénz útja nyomon követhető, felismerhetők a pénzügyi műveletek mintázatai. A pénz útját követve a tőzsdékkel együttműködésben esély lehet az elkövető beazonosítására, amikor a kriptovalutát hagyományos (fiat) pénzre váltja. A folyamat elképzelhetetlen nemzetközi együttműködés, nyílt forrásból származó információgyűjtés és a hagyományos nyomozati eljárások és technikák alkalmazása nélkül. A nyílt forrásból származó információgyűjtés fontos elemei azok az önkéntesek által működtetett nyilvános internetes adatbázisok, amelyeket azok a felhasználók töltenek fel adatokkal, akik például ransomware támadások, vagy online csalások áldozatai lettek és az ügyükben érintett címeket megosztják másokkal.

A fenti nyomozati eljárásoknak köszönhetően, amíg 2016-ban kriptovaluta lefoglalások 97%-a bitcoin volt, addig 2022-ben ez már csak 19%. Ez a szám egyrészt bizonyítja az eljárások használhatóságát, másrészt ne legyenek illúzióink, ez a csökkenés nem azt jelenti, hogy ennyivel kevesebb kriptovalutával kapcsolatos bűncselekmény történt, hanem azt, hogy a bűnelkövetők más kriptovaluták használatára tértek át. Ezek olyanok, amelyek nagyobb titkosságot és jobb értékállóságot biztosítanak. [67] Sajnos a titkosított kriptovaluták esetében jelenleg a rendvédelmi és biztonsági szervek, valamint a pénzügyi intézményrendszer szereplői közös erőfeszítésük ellenére egyelőre nem képesek a blokkláncok elemzésére. Az Egyesült Államok Adóhivatala (Internal Revenue service, röviden IRS) 625 ezer dollár jutalmat ajánlott fel annak, aki fel tudja törni a monero rendszerét. A feladat nehézségéről sokat elárul, hogy a pénz még az államkasszában hever. [82]

Kriptovaluták lefoglalása

A kriptovalutával kapcsolatos nyomozások esetén sor kerülhet az ügyben érintett kriptovaluta lefoglalására, illetve amennyiben ez nem lehetséges az ügyben érintett címek jelzéssel történő

ellátásra, ami azt jelenti, hogy a címeket tiltólistára teszik, és erről értesítik a tőzsdéket, kereskedőket, akik nem fogadhatnak el sem onnan sem oda irányuló ügyleteket. Sajnos ez a módszer jelenleg korlátozottan működik, mivel számos ország politikai vagy egyéb megfontolásból nem veszi figyelembe az ilyen irányú jelzéseket. A kriptovalutát vagy a tőzsdén vezetett számláról, vagy pedig abban az esetben tudják lefoglalni, ha az eljárás során sikerül megszerezni a pénztárcához tartozó privát kulcsot, amennyiben nem sikerül, úgy a jelzéssel történő megjelölés a járható út.

Összességében látható, hogy kriptovaluta elfogadottság és a hatósági lehetőségek mérlegelése együttesen egy meglehetősen komplex problémakört alkotnak. A terrorszervezeteknek tehát számos tényezőt figyelembe kell venniük mielőtt a kriptovaluta használat mellett döntenek.

3.3 A dzsihadista terrorszervezetek kriptovaluta használata és az erre utaló jelek

A terrorista sejtek igyekeznek vagyonukat a megbízható és mindig elérhető készpénzben, vagy legfeljebb olyan értékes vagyontárgyakban tárolni, amelyek szükség esetén gyorsan pénzzé tehetők. A szervezetek arra törekszenek, hogy megakadályozzák pénzeszközeik eredetének és mozgásának felderítését, igyekeznek vásárlásaikat titokban tartani, illetve az ellenük hozott szankciókat kijátszani, valamint pénzvagyonukat elrejteni. A titkos pénzügyi műveletek ezen felül azt a célt szolgálják, hogy költségvetésüket és irányítási struktúrájukat a rendvédelmi szervek elől elrejtsék.

Vizsgáljuk meg milyen feltételek esetén lehet vonzó a készpénz kriptovalutában történő tárolása:

- Nincs más egyszerűbb elérhető alternatíva.
- Pénzmosás elleni és terrorista finanszírozási előírások kijátszásának szükségessége.
- Hozzáférés lehetősége olyan tőzsdéhez, vagy pénzügyi szolgáltatóhoz, ami lehetővé teszi tetszőleges időben a kriptovaluta készpénzzé történő konvertálását.
- A pénzeszközök lefoglalásának megakadályozása.
- Feltűnés nélküli pénzmozgatás szükségessége.

- A rögzített árfolyamú kriptovaluták (stable coins) használatával járó esetleges inflációs veszteség bevállalása. [68]

A szempontokat összegezve a kriptovalutában történő értéktárolás azoknak a terrorszervezetknek lehet előnyös, akik nagymennyiségű pénzt akarnak határokon keresztül mozgatni, illetve tartanak attól, hogy a pénzük rejtekhelyét felfedik és lefoglalják, vagy pedig a viszonylag kis költségvetési szervezeteknek, amelyek pénzügyi alapjaikat főleg adománygyűjtés útján külföldről jellemzően ellenséges pénzügyi környezetből várják. Ilyen téren a Hezbollah, illetve az Iszlám Állam vehető számításba. Mindkettő gazdag szervezet, azonban míg a Hezbollah egy centralizált költségvetésű csoport addig az utóbbi provinciái egymástól és a központtól való távolságuk miatt inkább önálló forrás előteremtésre kényszerülnek. A határokon keresztül történő mozgatás esetén elég az offline pénztárcához (cold wallet) tartozó jelszót megjegyezni, vagy átadni. Előnyös lehet még olyan országokban a használata, ahol a pénzmosás elleni törvények szigorúak, azonban a kriptovalutákkal kapcsolatos szabályozás laza.[69 p. 9]

A nagy összegű pénzek kriptovalutában történő tárolása az árfolyam ingadozás veszélyével jár, ezért ha élnek ezzel a módszerrel, akkor olyan rögzített árfolyamú kriptovalutákat kell választaniuk, mint a tron, vagy a tether és társaik, amelyek használata esetén ugyan nem számíthatnak nyereségre, mi több inflációs veszteségeik lehetnek, azonban a pénzük biztonságban marad és állandóan elérhető lesz. Valószínűleg olyan rögzített árfolyamú kriptovalutát fognak választani, amelynek nagy a forgalma így a nagyobb összegű, vagy a nagyszámú tranzakciók nem keltik fel a hatóságok érdeklődését.

A felsorolt szempontok miatt a látókörből kiesik az egyébként népszerű bitcoin, amelynek nagy az árfolyamingadozása és a pénzügyi műveletek is bárki számára nyomon követhetők ezen túl a tranzakciók hatóság elöl történő elrejtése nehézkes, kockázatos és magasabb szintű felhasználói ismereteket igényel.

A terrorszervezetek kriptovaluta használatával kapcsolatos eddig nyilvánosságra került ügyekben a kriptovaluta a továbbítás fázisában volt. Nagy összegű tárolásra vonatkozó információ eddig nem került nyilvánosságra.

Ha megvizsgáljuk, hogy milyen jelek utalnának arra, hogy a terrorszervezetek nagy összegeket terveznek kriptovalutában tárolni, úgy a következő jeleket észlelnénk:

- A terrorszervezetek prominens tagjai kriptovalutával kapcsolatos kereséseket hajtanának végre, olyan személyeket toboroznának, illetve helyeznének fontos pozícióba, akik mesteri szinten ismerik a kriptovalutákat és a kriptopiacot.

- Kapcsolatot keresnének olyan személyekkel (szervezetekkel), amelyek képesek nagy összegű kriptovalutát készpénzre, vagy más értéktárgyra cserélni. Ezek jellemzően hawaladárok, illetve illegális, de legalábbis szürkezónás pénzügyi szolgáltatók lehetnek.

- A hatóságok a készpénzfutárok számának csökkenését tapasztalhatnák, ha helyüket a kriptovaluta műveletek vennék át.

Azonban a felsorolt jelekkel kapcsolatos információk ez idáig nem kerültek a rendvédelmi szervek birtokába. [68]

3.4 Dzsihadista terrorszerveztek online kiadványainak vizsgálata

A terrorszervezetek az online térben számos módon érhetik el közönségüket. A közösségi média posztok és a weboldalak fontos szerepet töltenek be a propaganda terjesztésben, azonban ezek közül is kiemelkednek az online magazinok. Ezek a kiadványok képi világukkal, struktúrájukkal és tartalmukkal magukon viselik a professzionista propagandamunkások kézjegyeit. A szerzők az aktualitásokon túl helyet szentelnek az olvasóközönség ideológia és esetenként biztonságtudatossági nevelésére is.

Ez utóbbi alapozta meg azt a feltételezésemet, hogy megvizsgáljam a terrorszervezetek tematikájában szerepel-e a kriptovaluták használatával kapcsolatos tájékoztatás, felkészítés, illetve ösztönzik-e olvasóközönségüket a kriptovaluták használatára illetve, az abban történő adakozásra.

Feltételezésem ellenőrzése érdekében a második hipotézisnél már alkalmazott OSINT módszerek felhasználásával 2024. június 01. és 2024. június 30. közötti időszakban dzsihadista terrorszervezetek online magazinjait gyűjtöttem adatbázisba. Az adatbázisban szereplő magazinok listája a 4. számú táblázatban látható.

	Kiadvány címe	Intervallum	Példány-szám	Nyelv	Kiadó	Szervezet
1.	Al Naba	2015-2024	441	arab	Central Media Office	IS[5]
2.	Dabiq Magazine	2013-2016	15	angol	Al-Hayat Media Center	IS
3.	Dar Al Islam	2014-2016	10	francia	Al-Hayat Media Center	IS
4.	Nawai-Afghan-Jihad-Magazine (Voice of Afghan Dzsihad)	2010-2020	87	Arab/Dari		AQIS[6]
5.	Nawai-Ghazwat-al-Hind Magazine	2020-2024	30	urdu	As-Sahab Media Subcontinent	AQIS[7]
6.	Arkan	2020-2022	3	angol	Ar-Rukn Media Center	IS
7.	Khalifatullah Mahdi	2021	1	angol	Ar-Rukn Media Center	IS
8.	Ictok	2015-2016	4	orosz	Al-Hayat Media Center	IS
10.	Inspire Magazine	2010-2017	16	arab/angol	Al-Malahem Media	AQAP[8]
11.	Inspire Guide Magazine	2016-2017	5	angol	Al-Malahem Media	AQAP
12.	The Voice of Khurasan	2020-2024	34	angol/pastu	Al-Azaim Foundation	IS
13.	Rumiyah Magazine	2016-2017	13	angol	Al-Hayat Media Center	IS
14.	Sada_al_Malahim	2008-2010	18	arab	Al-Malahem Media	AQ
15.	Gaidi-Mtaani	2012-2016	9	Szuaheli/ Swahili/ angol	al Kataib Media Agency	AQ/Al Shabaab
16.	Sawt Al-Hind (Voice of Hind)	2021-2022	27	angol	Al-Qitaal Media	IS
17.	Wolves of Manhattan	2019-2021.	3	angol, arab	al-Malahem Electronic Army	AQ

4. táblázat A tanulmányozott dzsihadista magazinok listája Forrás: a szerző szerkesztése

[5]Islamic State Iszlám Állam
[6] Al Kaida: AQ (Al Kaida)
[7] Al Kaida: Al Qaeada in the Indian Subcontinent-AQIS(Al Kaida az indiai szubkontinensen)
[8] Al Kaida: Al-Qaeda in the Arabian Peninsula-AQAP (Al Kaida az Arab-félszigeten)

A táblázatot tanulmányozva megállapítható, hogy a kiadványok az Al Kaida és az Iszlám Állam, valamint ezek társult szervezeteihez köthetők. A szervezeti eloszlásnak megfelelően a kiadványok nyelve is széles skálán mozog. A hatékony feldolgozás érdekében úgy döntöttem, hogy valamennyi kiadványt egy közös adatbázisba rendezem, majd ezen hajtom végre a keresést. Az adatbázis létrehozása közben számos kihívással kerültem szembe. A nagymennyiségű (22 980 oldalt kitevő) feldolgozandó oldalszám, az eltérő nyelv, a pdf formátum, illetve a kiadványok jellegéből adódóan feliratozott képek nagy száma lehetetlenné tette az egyszerű keresések végrehajtását, ezért úgy döntöttem, hogy a kiadványokat egy szöveges adatbázisba mentem, amelynek a nyelve egységesen angol. A tervezett adatbázis létrehozása érdekében a következő feladatsort dolgoztam ki:

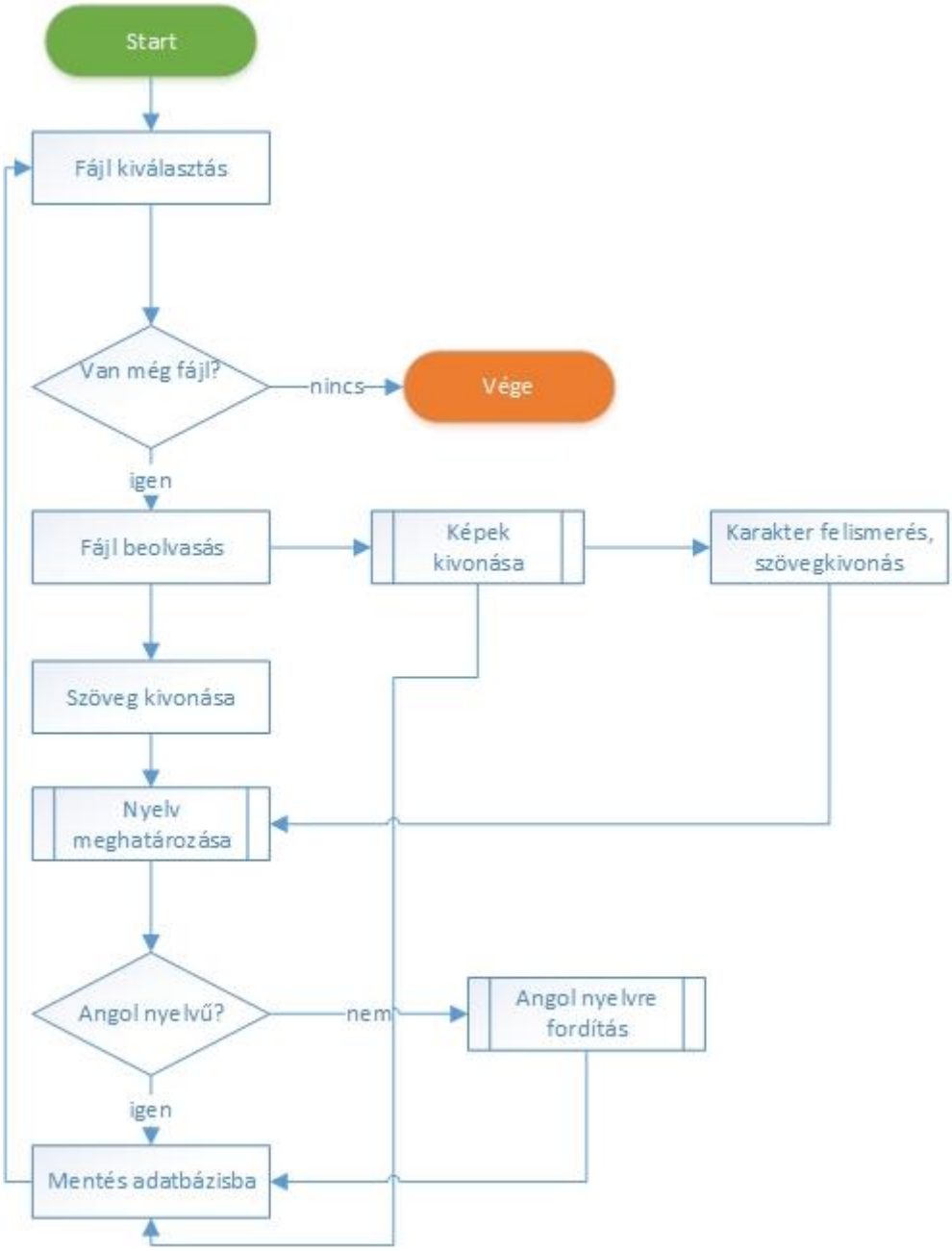
1. pdf formátumból a szöveg kinyerése;
2. a szöveg fordítása angol nyelvre és a kiadvány nevével valamint az oldalszámokkal együtt adatbázisba történő mentése;
3. a képek kivonása és adatbázisba mentése;
4. A képeken található feliratok (amennyiben van ilyen) kivonása és fordítása angol nyelvre, majd adatbázisba mentése;

A fenti feladatok végrehajtásának folyamatábrája a 22. számú ábrán látható.

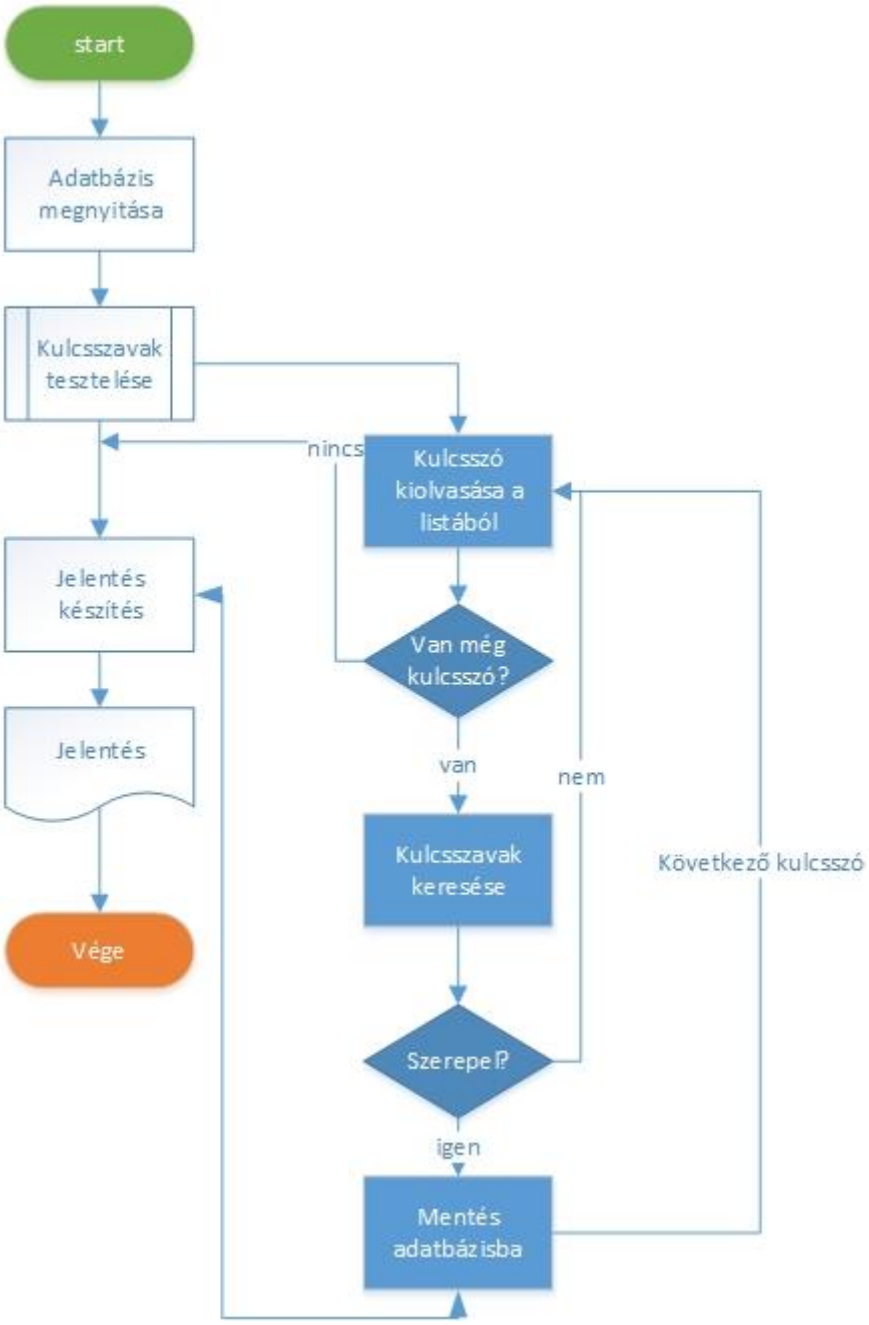
A feladat elvégzéséhez szabadon elérhető, vagy kereskedelmi forgalomban kapható szoftvert nem találtam, ezért magam készítettem Python nyelven scripteket, melyek segítségével a tervezett feladatott végrehajtottam.

Az adatbázis létrehozását követően a megfelelő kulcsszavak kijelölése után a 23.számú ábrán látható módon végrehajtottam a kriptovalutával kapcsolatos keresést.

A kutatás megtervezésénél a következő kulcsszavakat jelöltem ki: crypto currency, Bitcoin, Monero, BTC, XMR, Tether, Tron, USD, TRX, coin, $,



22. ábra A kiadványok feldolgozásának munkafolyamata Forrás: a szerző szerkesztése



23. ábra Kulcsszavak keresése az adatbázisban forrás: a szerző szerkesztése

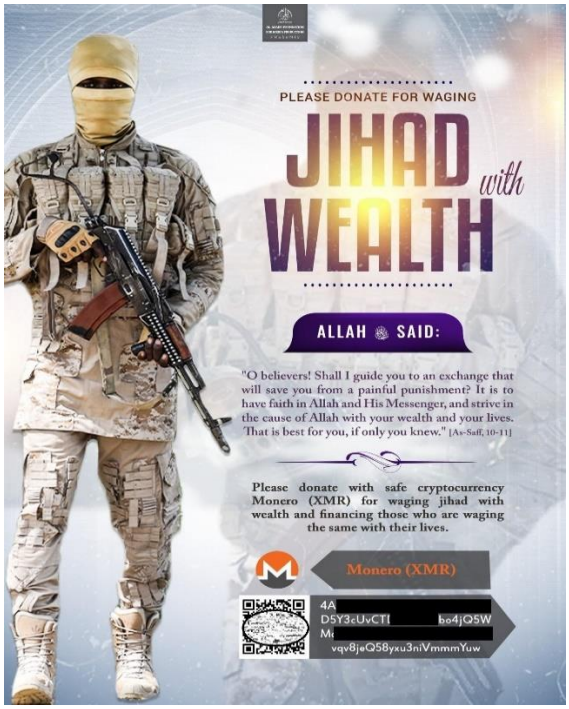
3.4.1 A keresés eredménye

A keresés során három kiadvány esetében keletkezett releváns találat:

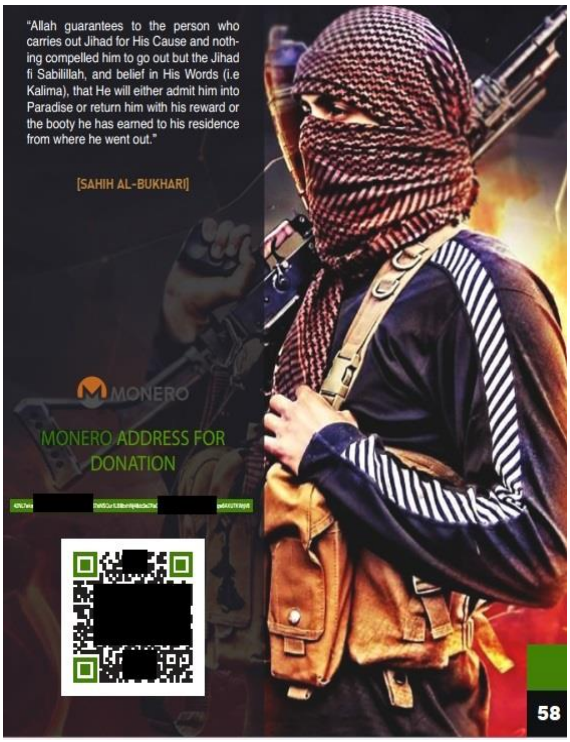
1. Az Iszlám Államhoz köthető Al Azaim Foundation által jegyzett „Voice of Khorasan” című angol nyelvű magazin 31,33 és 34-es számaiban található felhívás a moneroban történő adományozásra (24. számú ábra), illetve

2. Az Iszlám Állammal szövetséges Katiba Al-Mahdi fi Bilad Al-Arakan néven ismert mianmari dzsdihadista csoporthoz tartozó Ar-Rukn Media Center gondozásában megjelentetett „Arkan” című angol nyelvű magazin második kiadásának (2021) 58. oldalán jelent meg felhívás moneroban történő adakozásra (25. számú ábra)

3. Az Al Kaidához köthető „Wolves of Manhattan” magazinban az első kiadástól kezdődően több számon átívelő, a kriptovaluták használatával kapcsolatos oktató anyag jelent meg. A magazin 2021. április 14-én megjelent számában a terrorszervezet felhívást tett közzé, amelyben azt ígérte, hogy 60 000 USD értékű bitcoint ad annak, aki meggyilkol egy keresztény rendőrt. Nincs ellenőrzött információ arra vonatkozóan, hogy ennek a felhívásnak a hatására, vagy ettől függetlenül, de kilenc nappal később Jamel Gorchene, tunéziai bevándorló, „Allahu Akbar”-t kiáltva halálra késelte Stéphanie Monfermé rendőrnőt a rambouilleti (Franciaország) rendőrkapitányság bejáratánál. A merénylőt a helyszínen lelőtték. A rendőri tudósítások szerint az elkövető a merényletet megelőzően dzsihadista videókat nézett. [70]



24. ábra Felhívás a dzsihad kriptovalutával történő támogatására forrás: a szerző képernyőfotója a Voice of Khorasan magazin 33. szám 91.oldal, megjelent: 2024. február 16-i



25. ábra Felhívás Moneroban történő adakozásra az "Arkan" című magazin 58. oldalán (a szerző képernyőfotója)

Az Iszlám Államot illetően a felmérés mindössze két tartomány esetében tárt fel kriptovalutában történő adománykérést. Úgy tűnik, hogy amíg a szervezet magazinjaiban nagy hangsúlyt fektet követői kiberbiztonsági oktatására addig a kriptovalutákkal kapcsolatos ismereteket nem tekinti súlyponti kérdésnek. Valószínűsíthetően pénzügyi ökoszisztémájukban egyelőre nem szánnak kiemelt szerepet az új fizetőeszköz alkalmazásának.

Az adománykérésben szereplő monero titkosított jellegéből adódóan nem lehetséges a begyűjtött adományok nagyságát még megbecsülni sem. Ez a kriptovaluta típus egyelőre hozzáférhetetlen a rendvédelmi és pénzügyi ellenőrző szervek számára is szerte a világon.

Az Al Kaida esetében adakozásra történő felhívással kapcsolatos találat nem keletkezett, ugyanakkor kétségtelen, hogy a szervezet arra törekszik, hogy az olvasók alapvető ismereteket szerezzenek a kriptovaluták mibenlétéről és használatáról. Ennek fényében mégis érdekes, hogy a rendőrökre kitűzött vérdíjat bitcoinban hirdették meg, amelyről köztudott, hogy a tranzakciók adatainak elrejtéséhez az átlagos felhasználói tudást jóval meghaladó tudás szükséges. A közleményben érzek némi cinizmust is, hiszen a tapasztalatok azt mutatják, hogy a magányos merénylőket a rendfenntartó szervek még a támadás során megsemmisítik, így a vérdíj kitűzői tisztában kellett, hogy legyenek azzal, hogy a szóban forgó összeget nagy valószínűséggel nem kell majd kifizetniük senkinek. Véleményem szerint a vérdíj kitűzése egyszerű progagandafogás volt a részükről, amelynek anyagi vonatkozásaival nem kellett reálisan számolniuk.

3.5 A vizsgált terrorszerezetek kriptovalutában történő online adománykérésének felmérése

3.5.1 Adatbázis kialakítása

A felmérés során a második hipotézisnél ismertetett módon létrehozott adatbázist használtam. Az adatbázis adatokkal való feltöltése alkalmával minden weboldalt megvizsgáltam abból a szempontból, hogy szerepel-e rajta kriptovalutában történő adománykérés és ha igen, akkor azt milyen valutanemben kérik. A vizsgálat teljessége érdekében a kutatást az első hipotézis vizsgálata alkalmával felderített dark webes oldalakra is kiterjesztettem.

3.5.2 Az adatbázis kiértékelése

Az adatbázisban található weboldalak szervezetenkénti megoszlása az 5. számú táblázatban látható.

Ssz.	Szervezet megnevezése	Archív	Élő	Összesen
1.	Iszlám Állam	**52**	**12**	**64**
2	Al Kaida	**21**	**13**	**34**
3.	Abu Ali Mustapha Brigades		**1**	**1**
4.	Al Shabaab	**4**	**3**	**7**
5	Hezbollah	**8**	**2**	**10**
6.	Hay'at Tahrir al-Sham (HTS)	**1**	**1**	**2**
7.	Taliban	**8**	**2**	**10**
8.	Kataib Hezbollah	**4**	**1**	**5**
9.	Islamic Revolution Guard	**1**	**1**	**2**
10.	Harakat Hezbollah	**1**	**1**	**2**
11.	Al Qassam Brigades	**1**	**1**	**2**
12.	Független/beazonosíthatatlan	**9**	**7**	**16**
13.	HAMASZ	**1**	**3**	**4**

Ssz.	Szervezet megnevezése	Archív	Élő	Összesen
14.	Mujahideen Brigades	**0**	**1**	**1**
15.	Al Quds Brigades	**1**	**2**	**3**
16.	Islam Emirate	**1**	**0**	**1**
17.	Tehreek-e-Taliban	**2**	**1**	**3**
18.	Ansar al-Din Front	**1**	**0**	**1**
19.	Palestinian Islamic Jihad	**0**	**1**	**1**
20.	Jaysh al-Ummah	**0**	**1**	**1**
21.	Turkistan Islamic Party TIP	**0**	**1**	**1**
22.	Al Qaeda in the Islamic Maghreb	**1**	**0**	**1**
23.	Houthi	**0**	**3**	**3**
	Összesen	**117**	**58**	**175**

5. táblázat Az összegyűjtött webolalak szervezetenkénti felbontásban forrás: A szerző szerkesztése

A következő 6-es, 7-es és 8-as számú táblázatokban látható a kriptovalutában történő adomány kérés megoszlása szervezet, weboldalak aktivitása és jellege szerint valutanemenként csoportosítva.

Szervezet megnevezése	Archív weboldal	
	Bitcoin	**Monero**
Iszlám Állam	0	3
Jaysh al-Ummah	0	0
Független	0	0
Összesen	**0**	**3**

6. táblázat A szervezetekhez tartozó archív webolalak és az azokon kért adományok kriptovaluta nemenkénti megoszlása forrás: a szerző szerkesztése, rögzítés időpontja:2024.02.15.

Szervezet megnevezése	Aktív weboldal	
	Bitcoin	**Monero**
Iszlám Állam	0	3
Jaysh al-Ummah	1	0
Független	1	0
Összesen	**2**	**3**

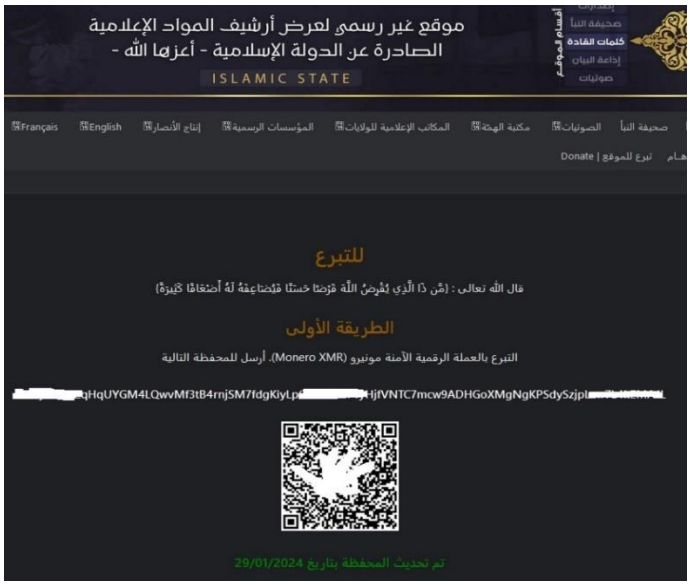
7. táblázat A szervezetekhez tartozó aktív webolalak és az azokon kért adományok kriptovaluta nemenkénti megoszlása forrás: a szerző szerkesztése, rögzítés időpontja: 2024. 02.15.

Szervezet megnevezése	Dark web	
	Bitcoin	**Monero**
Iszlám Állam	0	2
Jaysh al-Ummah	0	0
Független	0	0
Összesen	**0**	**2**

***8**. táblázat A szervezetekhez tartozó dark webes weboldalak és az azokon kért adományok kriptovaluta nemenkénti megoszlása forrás: a szerző szerkesztése rögzítés időpontja: 2024. 02.15.*

A táblázatokban szerepelő adatok alapján megállapítható, hogy a vizsgált terrorszervezetekre nem jellemző a kriptovalutában történő nyilvános adománykérés. Az Iszlám Államhoz köthető I'lam foundation és az Al Raud Media Archive a névtelenséget biztosító monero-t részesíti előnyben a nyílt webes és a dark webes felületein egyaránt. Az Al Raud dark webes adománykéréséről készült képernyőfotó a 26. számú ábrán látható. Összevetettem az adománykérések címeit, és megállapítottam, hogy az alapítványok nyílt és dark webes monero címei egyeznek, de a két alapítvány címei azonban egymástól eltérnek.

Az Iszlám Állam egykori központi archív weboldalain megjelenő adakozásra történő felkérések nem jelölték meg a kért adomány nemét, hanem arra kérték a híveket, hogy adakozás előtt vegyék fel a kapcsolatot a weboldalon megadott email címmel, annak érdekében, hogy az adakozás részleteit megismerhessék.



26. ábra Az al Raud Media Archive dark webes oldalán található adakozásra történő felszólítás forrás: http://xxxxxcv2uv2h3fay3cpopxuug6fxyp2reykt7lg67hnuonhm4xxxxx.onion/ (2024.02.15.)

A kavka##cen### nevű kaukázusi eseményekkel foglalkozó, orosz nyelvű, független, főleg csecsen és orosz vonatkozású dzsihadista hírportál bitcoinban kér adományt. Az adománygyűjtő felület az 27. számú ábrán látható.

27. ábra A kaukázusi független dzsihadista weboldal adománykérő felülete forrás: a szerző képernyőfotója (2024.02.15.)

A kavka##cen### -hez tartozó bitcoin cím ellenőrzése során megállapítottam, hogy az adományozásra szolgáló bitcoin címhez tartozó egyenleg 0.00180353BTC (93.55USD), amelyet egy a 3JkkXiEnagdURDFV4xetevU4YHm5kaB9vL címről küldtek 2018. 01.12-én 17 órakor. A címen ez volt az egyetlen tranzakció, az egyenleg azóta nem változott. A három szint mélységéig végrehajtott blokkláncelemzés érdemi eredményt nem hozott.

Az Al Kaidával kapcsolatban álló Jays al-Ummah palesztin terrorszervezet a weboldalán bitcoinban történő adományozásra szólít fel. A szervezet a weboldalán többek között árlistát is közöl az egyes fegyverek beszerzési áráról annak érdekében, hogy a támogatókat adakozásra ösztönözze. Az adakozásra történő felszólításról készült kép a 28. számú számú ábrán látható.

***28**. ábra A Jaysh-al-ummah-weboldalán található adakozásra történő felszólítás forrás: https://alraxxxx.nex/en/category/ (2024.02.15)*

3.5.3 Az adatbázis elemzésének összegzése

1. Az adatbázisban található weboldalak elemzését követően megállapítható, hogy a kriptovalutában történő online adománykérés nem jellemző a vizsgált dzsihadista terrorszervezetekre.

2. Az 58 aktív weboldalból mindössze 5 oldalon szerepel felhívás kriptovalutában történő támogatásra, ami a vizsgált oldalak mindössze 8,6% -a.

3. Ugyanakkor megfigyelhető a hatóságok kijátszására, illetve munkájuknak akadályozására vonatkozó törekvés. Az Iszlám Államhoz köthető alapítványok adománygyűjtési célra a névtelenséget biztosító monero-t használják.

4. Úgy tűnik, hogy a HAMASZ betartja az új típusú fizetőeszközzel kapcsolatos moratóriumát és weboldalain nem folytat kriptovaluta-alapú adománygyűjtést.

5. A Jaysh al-Ummah és a kavka##cen### látszólag semmilyen intézkedést nem alkalmaznak a hatóságok kijátszásra. A szervezetek fenntartását biztosító kriptovaluta műveletek szabadon megtekinthetők a bitcoin blokkláncán. Ezt a lehetőséget kihasználva a blokkláncelemzés technikáját és nyílt forrású információkat felhasználva megvizsgáltam a Jays al- Ummah bitcoin címéhez tartozó tranzakciókat.

3.6 A Jaysh al-Ummah bitcoin címéhez kapcsolódó tranzakciók elemzése (blokkláncelemzés)

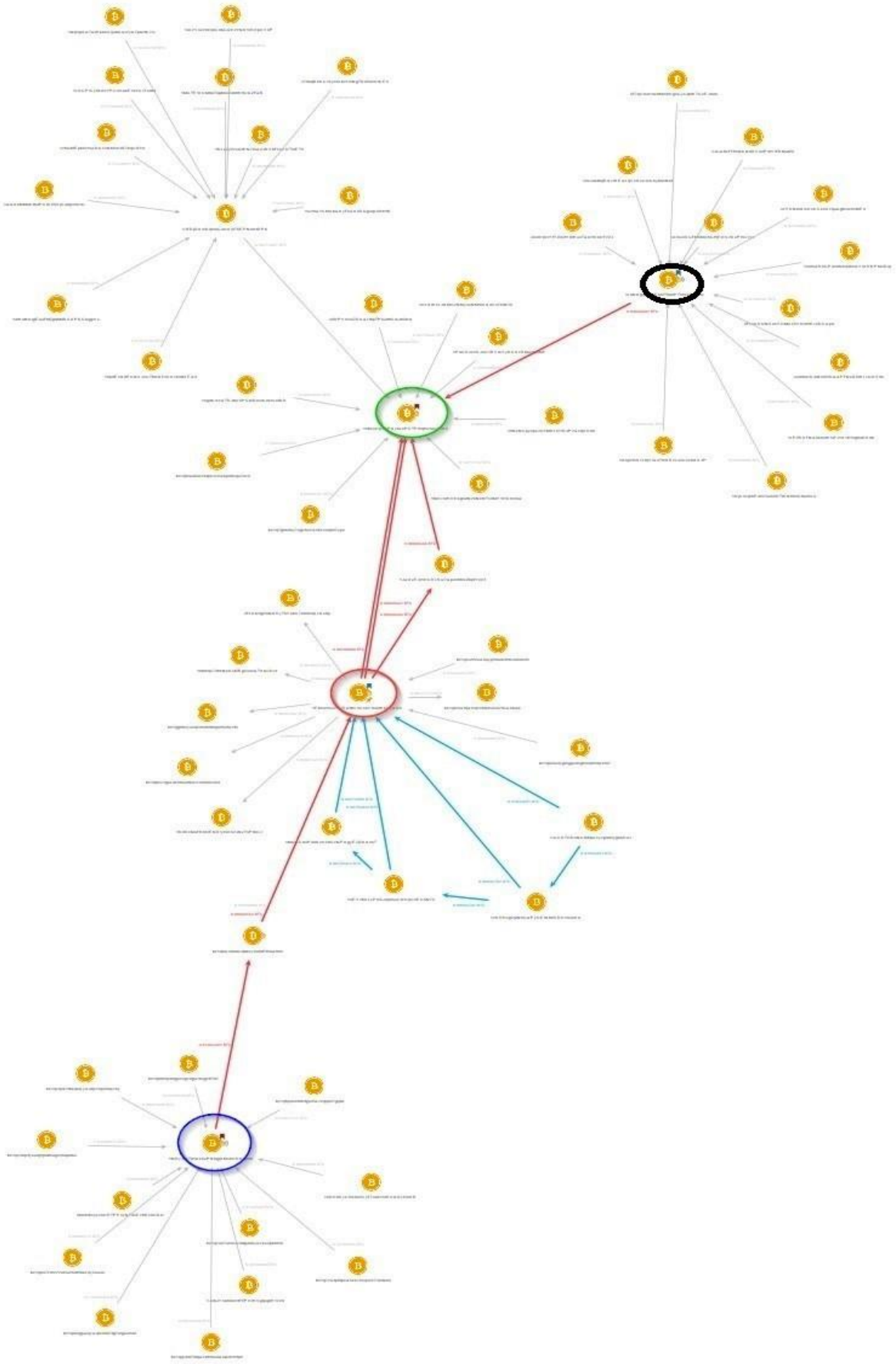
3.6.1 Az elemzés lépései

1. A Jaysh al –Ummah támogatásra irányuló felszólításában szereplő bitcoin címre vonatkozóan összegyűjtöttem a kapcsolódó tranzakciókat, majd minden partnerre vonatkozóan hasonló módon egyenként elvégeztem a tranzakciók kigyűjtését. A nagy mennyiségű adatra való tekintettel háromszintű kapcsolatmélységig végeztem el a kutatást.

2. Az elemzés során felmerült bitcoin címeket egyenként ellenőriztem az olyan nyilvános adatbázisokba, mint a „bitcoin who is who” (https://www.bitcoinwhoswho.com/) és a „crypto scam” (https://cryptscam.com), amelyek a felhasználók önkéntes adatszolgáltatásán alapuló adatbázisok, ahol a csalásokkal, pénzmosással, terrorizmusfinanszírozással kapcsolatos bitcoin címek listája található.

3. A felderített címeket internetes kereséssel is ellenőriztem annak érdekében, hogy ellenőrizzem szerepelnek-e más weboldalakon.

4. A felderített adatokat a vizsgálat szempontjából nem releváns adatok eltávolítását követően a könnyebb áttekinthetőség érdekében a Maltego (4.7.0.) alkalmazás segítségével vizuálisan brázoltam. A tranzakciók hálózata a 29. számú ábrán látható.



29. ábra A Jays al-Ummah nyilvános bitcoin címéhez kapcsolódó tranzakciók grafikus ábrázolása forrás: a szerző szerkesztése

3.6.2 Megállapítások

1. A kiindulási pont a piros körrel jelölt cím:

1EM4e8eu2S2RQrbS8C6aYnunWpkAwQ8GtG

Egyenlege: 0 BTC

Fogadott: 0.00896503 =468,55USD (7 tranzakció)

Küldött: 0.00896503 =468,55 USD (7 tranzakció)

Tranzakciók száma: 14

Első tranzakció: 2020.07.08.

Utolsó tranzakció: 2024. 01.04

A terrorizmussal, illetve a kiberbűnözéssel kapcsolatos nyilvános adatbázisokban a vizsgált cím nem szerepel.

3.6.3 Figyelemre méltó tranzakciók:

a) a kiindulási pont mellett zöld nyíllal jelölt tranzakciók mintázata arra enged következtetni, hogy a küldő igyekezett az összeg feldarabolásával, és a címekkel való játékkal az általa utalt összeg eredetének elrejtésére, és a nyomon követhetőség megnehezítésére.

b) a bc1qnw3n6l6vqrlkcy0uhrr7r89wr0mhgpmlsle6yn címen keresztül 20 USD-t kapott a 1NDyJtNTjmwk5xPNhjgAMu4HDHigtobu1s címről (kék körrel jelölve), amely kriptovalutával kapcsolatos csalások és bitcoin mixer tevékenység miatt szerepel a „bitcoinwhoiswho" és a „cryptscam" adatbázisában. A bc1-es kezdetű cím feltehetően a valódi küldő elrejtése miatt mindössze csak ehhez az egy tranzakcióhoz köthető. A csalás miatt megjelölt cím további tranzakcióit terjedelmi okok miatt nem vizsgáltam. A cím jelentőségét jól mutatja, hogy 1,191,638 db tranzakcióban összesen 15654676,01811631 bitcoint fogadott, (ami napi árfolyamon 809,117,409,132 USD-nak felel meg) és küldött tovább az elmúlt hat évben. Jelenlegi egyenlege: 0,318 bitcoin. Feltehetően a címet már nem használják.

c) Az 1EM4e8eu2S2RQrbS8C6aYnunWpkAwQ8GtG kimenő tranzakciói között figyelemre méltó a 18MJ9vje3yPAytwePSTPmqmzaayB8LCQ7n (zöld kör) ugyanis ide két alkalommal közvetlenül és egy esetben közvetítőn keresztül is küldött kis összegeteket. Ezek a tranzakciók piros nyíllal vannak jelölve az ábrán. Ez a cím nem szerepel egyik adatbázisban sem, ugyanakkor figyelemre méltó kapcsolatai közé tartozik a 1LaNXgq2ctDEa4fTha6PTo8sucqzieQctq cím, amelyről 0,9665092 bitcoint kapott. Az 1LaNXgq2ctDEa4fTha6PTo8sucqzieQctq (fekete kör) cím viszont 2019. február 09-óta szerepel a scamalert adatbázisában, mint a HAMASZ-hoz köthető cím, amelyet terrorizmusfinanszírozásra használnak fel. A szóban forgó címre 3370,01580508 bitcoin érkezett és innen 3370,01462506 bitcoint küldtek el összesen 9054 tranzakcióban.

Internetes keresés feltárta, hogy a szóban forgó cím egy Cash4ps nevű palesztin pénzügyi szolgáltatóhoz tartozik, amelynek valóban vannak terrorizmusfinanszírozáshoz köthető kapcsolatai. A Chainalysis szerint a címen megforduló összegből körülbelül 1 millió dollárnyi kriptovaluta köthető terrorista csoporthoz.[71]

3.7 Sajtóelemzés

A dzsihadista terrorszervezetekkel kapcsolatos kriptovaluta lefoglalások véleményem szerint hitelesen jeleznék az egyes szervezetek elköteleződését az új típusú fizetőeszközök iránt, azonban erre vonatkozó kimutatást, listát nyílt forrásból nem sikerült találnom, ezért úgy döntöttem, hogy a valós felhasználás méréséhez szükségem van egy viszonylag megfogható mérőszámra, ezért az internetes tudósításokban szereplő hatósági intézkedés alapján lefoglalt, vagy elkobzott kriptovaluta felhasználói fiókokkal kapcsolatos tudósításokra esett a választásom. Szempontként vettem figyelembe továbbá, hogy ez a terület aránylag rövid múltra tekint vissza különösen, ami az ilyen lefoglalásokat illeti, ezért feltételeztem, hogy az ilyen esetek nagy valószínűséggel megjelennek a nemzetközi sajtóban. A módszer helyességét alátámasztja, hogy a nemzetközileg elismert RAND Corporation a „Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats," című jelentésének elkészítésekor többek között ugyancsak ezt a módszert alkalmazta.[69 p.10]

Önmagukban természetesen az ilyen módon gyűjtött adatok sem vehetők abszolút pontos mérőszámnak, hiszen bűnüldözési szempontból lehetnek olyan esetek, amelyek nem kerülnek nyilvánosságra mégis, a számok nagysága/nagyságrendje utalhat a jelenség gyakoriságára, és a szervezetek kriptovaluták iránti elkötelezettségére. A felmérés nyelveként az angolt választottam, ugyanis véleményem szerint, ha valahol releváns esemény történt az nagy valószínűséggel megjelent az angol nyelvű világsajtóban. A vizsgálat a következő lépésekből állt:

- Megfelelő kulcsszavak kiválasztása.
- Keresések végrehajtása.
- Keresések eredményeinek személyes ellenőrzése.
- Összegzés, értékelés.

3.7.1 Kulcsszavak kiválasztása

A kereséshez legrelevánsabb találatok elérése érdekében több alkalommal különböző keresőszavakkal próbálkoztam. Végül többszöri próbálkozást követően a következő kereső kifejezések mellett döntöttam:

1. „forfeit", „crypto", „currency", „terrorism", „islamic"

2. „seized”, „crypto”, „currency”, „accounts”, terrorism, jihad”

A találatok szűrése érdekében az elmúlt öt év eseményeit vizsgáltam, ezért a keresési intervallumot 2019. február 01 és 2024. február 28. közé állítottam be egyidejűleg a „Hírek” szűrőt is aktiváltam.

3.7.2 Keresőmotorok:

Az internetes keresések során az alábbi keresőmotorok szolgáltatásait vettem igénybe: DuckDuckGo, Google, Yahoo, Yandex, Yep, SearchEncrypt, SwissCow;

3.7.3 A keresések eredményei

A két különböző keresőkifejezéssel végrehajtott keresések eredményi a következőképpen alakultak:

Az első esetben 30 találat keletkezett, míg a második esetben 70 találatot kaptam vissza, amelyekből a leválogatást követően 5, illetve 8 releváns találat maradt. A találatok egyenkénti leválogatása, majd kiértékelés rávilágított arra, hogy a sajtóközlések első pillantásra nagynak tűnő száma valójában más cikkek hiányos átvétele. A cikkek adathiányának másik oka a hatósági közlések adathiányából fakad. A szervezetenkénti megoszlás az 9. számú táblázatban látható.

Ssz.	**Szervezet megnevezése**	**Esetek száma**	**Kriptovaluta**
1.	Al-Kaida	2	bitcoin
2.	Iszlám Állam	1	bitcoin
3.	HAMASZ, Al Kasszam Brigádok	6	bitcoin, tron, dogecoin, tether,ether
4.	Hezbollah	2	tether
5.	Palesztin Iszlám Dzsihád (PIJ)	3	tron
6.	Katibat al Tawhid wal Jihad (KTJ)	1	bitcoin
7.	Palesztin Népi Ellenállás Bizottság	1	bitcoin
8.	Al Malhama	1	bitcoin

9. táblázat A sajtótudósításokban szereplő kriptovaluta lefoglalásban érintett terrorszervezetek listája 2019 február 01. és 2024. február 28 között. A szerző szerkesztése

A táblázatból látható, hogy a Hezbollah, a HAMASZ és a Palestine Islamic Jihad a legaktívabb kriptovaluta felhasználó terrorcsoportok. Ezek a csoportok a bitcoinon kívül más kriptovalutákkal is kísérleteztek. Az egyes lefoglalások értékének megállapítására, vagy a lefoglalások szervezetenkénti lebontására a hiányos adatközlések, illetve esetek összevonása

miatt, nem volt minden esetben lehetőség. A lefoglalt pénzösszegek 20 USD és 94 millió USD között ingadoztak.

3.7.4 A sajtó felmérés összefoglalása

Összegezve a sajtófelmérés eredményét megállapítható, hogy az elmúlt öt évben mindössze néhány szervezettől foglaltak le kriptovalutát. A Hezbollah és a HAMASZ, illetve a Palesztin Iszlám Dzsihad terrorszervezetek érintettek leginkább a kriptovaluta használatban. A hagyományosan nagy terrorszervezetek mint az Al Kaida, vagy az Iszlám Állam kisebb mértékben érintettek a kriptovaluta lefoglalásokban.

Természetesen ez nem azt jelenti, hogy ezek a csoportok nem foglalkoznak kriptovalutával, nyilván valamekkora látencia van a valódi használat és a nyilvánosságra került esetek között, azonban tekintettel, hogy ezek a szervezetek jobban a rendvédelmi szervek látókörében vannak, mint a kisebb csoportok valószínűsíthető, hogy nagyobb eséllyel derítenének fel ilyen eseteket, ha ez nagyobb mértékben lenne jellemző rájuk.

A terrorszervezetek kriptovaluta iránti elkötelezettségét illetően megállapítható, hogy a bitcoinon kívül igyekeznek más valutákkal is kísérletezni, úgy tűnik, hogy többnyire azokkal próbálkoznak, amelyek árfolyama kevésbé ingadozik, illetve rögzített. Összességében megállapítható, hogy a lefoglalt összegek a nyilvánvaló veszteségeken kívül nem veszélyezették a terrorszervezetek költségvetését, illetve működését.

3.8 Összefoglalás

Az szakirodalmi áttekintés rávilágított arra, hogy nincs egységes álláspont arra vonatkozóan, hogy a terrorszervezetek pénzügyi műveletikben milyen mértékben használnak kriptovalutákat. Ugyanakkor a szakirodalmi adatgyűjtés feltárt néhány esetet, amelyben dzsihadista terrorszervezetek kriptovalutával kapcsolatos illegális ügyleteket bonyolítottak, azonban ezek volumene összevetve a szóban forgó szervezetek becsült vagyonával, illetve költségvetésével gyakorlatilag jelentéktelennek mondható.

Kutatásomban megvizsgáltam a kriptovaluta elfogadottságának legfontosabb tényezőit, egészen pontosan azokat, amelyek véleményem szerint befolyásolhatják a terrorszervezetek vezetőit abban a kérdésben, hogy hol és hogyan, valamint milyen mértékben használják ki a digitális fizetőeszköz nyújtotta lehetőségeket. Ebben a fejezetben, eddig egyedülálló módon, a tényezők közé soroltam a vallási szempontú megközelítésben rejlő ellentmondásokat, amelyek véleményem szerint befolyásolhatják a támogatók kriptovalutában végrehajtott adakozási hajlandóságát.

Megvizsgáltam, hogy a kriptovalutával kapcsolatos visszaélések esetén milyen lehetőségei vannak a rendvédelmi szerveknek, hiszen ez fontos abból a szempontból, hogy mekkora visszatartó erőt jelenthet azoknak, akik a kriptovalutákat bűnös célokra kívánják felhasználni. Összességében megállapítható, hogy a rendvédelmi szervek egyelőre lemaradásban vannak, különösen az anonimitást biztosító kriptovaluták vonatkozásában, bár kétségtelen, hogy a blokkláncelemzés területén jelentős előrehaladás történt az utóbbi néhány évben.

A kriptovaluta felhasználás felmérése érdekében meghatároztam, hogy milyen jelei lehetnek annak, ha egy dzsihadista terrorszervezet nagyobb mértékben akarna a kriptovaluták használatára áttérni, azonban a kutatás során ilyen jelekre utaló információk nem keletkeztek.

A kutatásom megtervezése során arra a következtetésre jutottam, hogy a terrorszervezetek kriptovaluta-használatával kapcsolatban egzakt, közvetlen bizonyítékokat beszerezni a szervezetek működésének, és tevékenységének jellege, valamint a kriptovaluták tulajdonságai miatt nyílt forrásból nem lehetséges. Azonban több oldalról, közvetett bizonyítékok, és adatok összegyűjtését követően lehetőség van egyfajta kép kialakítására a kriptovaluta használat beágyazottságáról, így megbecsülhető, hogy a szervezetek milyen mértékben tértek át az új típusú fizetőeszköz használatára. Az idevágó irodalom tanulmányozásán túl a közvetett bizonyítékok és adatok beszerzése érdekében végrehajtott kutatási lépések eredményét a könnyebb áttekinthetőség érdekében a 10. számú táblázatban foglaltam össze.

		Előfordulás		
ssz.	Szervezet megnevezése	**Magazinban**	**Weboldalon**	**Sajtóban**
1.	Iszlám Állam	2	5	1
2.	Al Kaida	2		2
3.	Hamasz			6
4.	Hezbollah			2
5.	Jays al- Ummah		1	
6.	Palesztin Iszlám Dzsihád (PIJ)			3
7.	Katibat al Tawhid wal Jihad (KTJ)			1
8.	Palesztin Népi Ellenállás Bizottság			1
9.	Al Malhama			1
10.	Független		1	
	Összesen:	4	7	17

10. táblázat A kutatás ereményinek összegzése (a szerző szerkesztése)

A táblázatból látható, hogy az egyes kutatási lépések eredményeként mindössze néhány releváns találat keletkezett.
Az online magazinok elemzése során két Iszlám Államhoz köthető kriptovalutával kapcsolatos adománykérést sikerült azonosítani, míg az Al Kaida kriptovalutákkal kapcsolatos tananyagot és egy bitcoinban kitűzött vérdíjat publikált az online magazinok lapjain.
A weboldalak elemzése is csekély számú értékes találatot adott. Az Iszlám Államhoz köthető két alapítványon kívül a Jays al -Ummah és egy kaukázusi független dzsihadista oldalon sikerült kriptovalutában történő adománykérést rögzíteni. Az Iszlám Állam alapítványai a teljes mértékben anonim monerot használják így itt további kutatásra nem volt lehetőség, míg a másik két szervezet bitcoint kért, ami lehetővé tette, hogy megvizsgáljam a kampányaik sikerét. A blokkláncelemzés felfedte, hogy adománygyűjtési akcióik eredménye mindössze néhány száz dollárt tesz ki és egyben igazolta, hogy a palesztin terrorszervezet kapcsolatban áll más palesztin terrorszervezetekkel és online csalásokban érintett kiberbűnözőkkel.
A harmadik lépésben végrehajtott sajtóelemzés sem hozott átütő eredményt. A nyilvánosságra került esetek száma elenyésző és a hatóságok által lefoglalt kriptovaluta mennyisége sem tekinthető jelentősnek, ha az egyes szervezetek becsült vagyonához, illetve költségvetésükhöz viszonyítjuk.
Ugyanakkor a kriptovaluta használatban észlelhető volt a szervezetek érdeklődésének eltolódása a bitcointól más, állandó árfolyamú valuták irányába. A lefoglalások alapján a legaktívabb kriptovaluta használók az olyan palesztin terrorcsoportok mint a HAMASZ, a Palestine Islamic Jihad, illetve még ide számít a libanoni Hezbollah. Meglepetésre az Al Kaida és az Iszlám Állam ezekhez képest jelentéktelen számban szerepelt a tudósításokban.

A felmérések eredménye a téma sajátosságaiból adódóan nem tükrözheti a valós számokat, azonban a tendenciák jelzésére megfelelő. Ennek alapján kijelenthető, hogy a dzsihadista terrorszervezetek nem fordultak a kriptovaluta használat felé. A kutatás során a kriptovaluta használattal összefüggésben keletkezett információk csak sporadikus használatra utalnak, azonban ez nem azt jelenti, hogy a jövőben ez a tendencia nem fog változni. Jelenleg úgy tűnik, hogy ehhez valamilyen szélsőséges fordulatra van szükség, amely lehet egy rendkívül hatékony nemzetközi terrorizmusfinanszírozás elleni művelet eredménye, vagy pedig egy olyan forradalmi technikai áttörés, amely a jelenleginél egyszerűbbé és biztonságosabbá teszi a kriptovaluták használatát.

Következtetés

A kutatásom során összegyűjtött adatok elemzését követően hipotézisemet, mely szerint

Feltételezhetően a szélsőséges Iszlám terrorszervezetek a nemzetközi pénzügyi korlátozó és szankciós intézkedések hatására pénzügyi műveleteik elrejtése érdekében a részleges anonimitást biztosító kriptovaluták felé fordultak.

cáfolom

A nemzetközi pénzügyi korlátozó intézkedések hatására a terrorszervezetek hagyományos pénzügyi műveletei nem szenvedtek végzetes csapást, ezért nem fordultak a kriptovaluták felé. A terrorcsoportok továbbra is képesek a hagyományos módon megteremteni pénzügyi alapjaikat, illetve a szükséges pénzügyi műveleteket végrehajtani. Ugyanakkor kétségtelen, hogy a jelenlegi kriptovaluta használatuk már most is nyomást helyez a nemzetközi pénzügyi és terrorista ellenes szervezetekre. Egyelőre úgy tűnik, hogy a terrorszervezetek kriptovaluta használata kísérleti stádiumban van, próbálkoznak olyan területeket találni, ahol minél jobban ki tudják aknázni az új technológiában rejlő lehetőségeket, de működésük egyelőre nem függ a kriptovalutáktól.

A kriptovaluta használat jövőbeli mértéke egyelőre nem meghatározható, mivel számos tényező befolyásolhatja úgy, mint például a változások a pénzügyi szabályozásban, a technológia evolúciója, illetve a hagyományos pénzügyi rendszerben bekövetkező esetleges változások. Mindenesetre azt látni kell, hogy a kriptovaluta technológia ilyen mértékű fejlődése indokolttá teszi a pénzügyi szabályozó szervek, a hírszerző szolgálatok és a rendvédelmi szervek nemzetközi szintű együttműködését a terrorizmus elleni harc sikere érdekében.

ÚJ TUDOMÁNYOS EREDMÉNYEK/AJÁNLÁSOK

Tudományos eredmények

A hipotéziseimmel kapcsolatos kutatásom során azt vizsgáltam, hogy az utóbbi néhány évben megjelent és elterjedté vált új technológiák és a rendvédelmi szervek részéről tapasztalható nyomás erősödése milyen hatást gyakorolt a dzsihadista terrorszervezetek internetes tevékenységére.

1.Az első hipotézisemmel kapcsolatban értékként tekintem, hogy az eddigi kutatásokkal szemben kiszélesítettem a kutatások területét és megvizsgáltam a három legismertebb és leginkább használt dark webes területeket. Kutatásom során sikerült a TOR rendszeren kívül egy eddig nem publikált Al Kaidához köthető tartalmat felderíteni a Freeneten. A széleskörű kutatás eredményeként felderített dark webes dzsihadista tartalmak mennyisége nem számottevő így a vizsgált platformok sajátosságait figyelembe véve nagyobb biztonsággal jelenthetjük ki, hogy a dzsihadista terrorszervezetek nem fordultak a cenzúraállóságot és anonimitást biztosító dark web felé. A dark web használatát mindössze az Iszlám Államhoz köthető két alapítvány esetében sikerült egyértelműen kimutatni.

2.A második hipotézisemmel kapcsolatos kutatásom legfőbb eredményeként azt tekintem, hogy az eddigi kutatókkal szemben nem egyenként vizsgáltam az Iszlám állam cenzúraelkerülési technikáit, hanem egységesen szerkezetben rendszerszemlélettel közelítettem meg végig követve annak evolúcióját. A rendszert vizsgálva megállapítható, hogy az evolúciós folyamat során a terrorszervezet minden ellenintézkedésre olyan hatásos ellenlépésekkel tudott válaszolni, amelyek lehetővé teszik az online jelenlétének fenntartását. Ez az új szemléletű megközelítés rávilágított arra, hogy az ilyen összetett rendszerrel szemben csak hasonló komplexitású rendszerszemléletű ellenintézkedésekkel van esély az eredményes küzdelemre. Ugyanakkor véleményem szerint a rendszer egyik legfontosabb eleme a redundáns tartalommegosztó és kapcsolati rendszer lehet az ökoszisztéma Achilles sarka is egyben azzal, hogy lehetővé teszi a rendvédelmi szervek számára, hogy folyamatosan nyomon kövessék a hálózat változásait megteremtve a lehetőséget az azonnali intézkedések megtételére és az Iszlám Állam folyamatos nyomás alatt tartására.

3.A harmadik hipotézissel kapcsolatban hozzáadott értéknek tekintem, hogy a dzsihadista terrorszervezetek kriptovaluta használatának mértékét egyszerre több megközelítésből is vizsgáltam. Eddig egyedülálló módon a kriptovaluta használatot befolyásoló tényezők számbavételénél figyelembe vettem a kriptovaluták vallási megítélésében kialakult kettősséget, amely véleményem szerint befolyásolhatja a támogatók egy részének virtuális valutában történő támogatási hajlandóságát. A három megközelítéssel kapcsolatos egyidejű kutatás, a nyilvánvaló látencia ellenére véleményem szerint hitelesebben alátámasztja a következtetésemet miszerint a terrorcsoportok továbbra is képesek a hagyományos módon megteremteni pénzügyi alapjaikat, illetve a szükséges pénzügyi műveleteket végrehajtani.

Tagadhatatlan ugyanakkor, hogy a dzsihadista terrorszervezetek kriptovaluta használata – még a jelenlegi szinten is – nyomás alatt tartja a nemzetközi terrorizmusellenes szervezeteket és az ebben a harcban érintett pénzügyi intézményeket. Egyelőre az látszik, hogy a vizsgált szervezetek kriptovaluta használata a kísérletezés szakaszában van, de ez nem jelenti azt, hogy valamely olyan körülmény, mint jelentős változás a hagyományos pénzügyi rendszerben, vagy a kriptovaluta technológiában bekövetkező markáns fejlődés hatására ez nem fog gyökeresen megváltozni.

A terrorizmus elleni harc sikeres megvívásának érdekében célszerűnek tartanám a rendvédelmi szervek, titkosszolgálatok és a politikai döntéshozó szervek, valamint a pénzügyi szabályozó szervek nemzetközi szintű információcseréjének, illetve együttműködésének kialakítását.

Ajánlások

Kutatásom az informatikai vonzatai mellett is elsősorban a rendvédelmi területen és azon belül is terrorizmus elleni harcban érintett állomány képzése, illetve továbbképzése során hasznosítható. A kutatás a nagy mennyiségű szakirodalom feldolgozásán túl több oldalról megközelítve gyakorlati úton vizsgálta, hogy a dzsihadista terrorszervezetek napjainkban hogyan viszonyulnak az olyan újnak számító technológiákhoz, mint a dark web, vagy a kriptovaluták és választ adott arra, hogy ezek a szervezetek hogyan tudják folyamatos online jelenlétüket biztosítani. A kutatás során keletkezett adatok cáfolnak olyan divatos nézeteket, mint a dzsihadista terrorszervezetek aktív dark webes tevékenysége, vagy a kriptovaluták elterjedt használata körükben ennél fogva hozzájárulnak a dzsihadista terrorszervezetek internetes tevékenységének valóságot jobban megközelítő megismeréséhez.

HIVATKOZÁSOK

[1] Malik N., “Terror in The Dark: How Terrorists use Encryption, the Darknet and Cryptocurrencies - Henry Jackson Society,” *Henry Jackson Society*, 2018. https://web.archive.org/web/20220126185013/http://henryjacksonsociety.org/wp-content/uploads/2018/04/Terror-in-the-Dark.pdf (letöltve: 2023.06.21.).

[2] Weimann G., “Terrorist Migration to the Dark Web on JSTOR,” *Jstor.org*, 2016. https://www.jstor.org/stable/26297596 (letöltve: 2023.07.20.).

[3] Saltman E.M., “Jihad trending: Analysis of online extremism and how to counter it,” *Index on Censorship*, 2014. https://www.indexoncensorship.org/2014/05/jihad-trending-comprehensive-analysis-online-extremism-counter/ (letöltve: 2023.07.18.).

[4] Berton B., “The dark side of the web: ISIL’s one-stop shop?,” *European Union Institute for Security Studies*, 2015. https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert_30_The_Dark_Web.pdf

(letöltve: 2023.09.10.).

[5] Lakomy M., “Dark web *jihad*: exploring the militant Islamist information ecosystem on The Onion Router,” *Behavioral Sciences of Terrorism and Political Aggression*, pp. 1–20, 2023, doi: https://doi.org/10.1080/19434472.2022.2164326.

[6] Figueras M. E., Magán C. R., Boubeta P. J., “Drawing the web structure and content analysis beyond the Tor darknet: Freenet as a case of study,” *Journal of Information Security and Applications*, vol. 68, p. 103229, 2022, doi: https://doi.org/10.1016/j.jisa.2022.103229.

[7] United Nations Office on Drugs and Crime, “The use of the Internet for terrorist purposes In collaboration with the UnITed naTIons CoUnTer-TerrorIsm ImplemenTaTIon Task ForCe,” 2012.

[8] Bányász P., “Közösségi média és kiberbűnözés,” *Nemzetbiztonsági Szemle*, vol. 2017/4, p. 71, 2017.

[9] Weimann G., “Terrorist Migration to Social Media,” *Georgetown Journal of International Affairs*, vol. 16, no. 1, pp. 180–187, 2015, http://www.jstor.org/stable/43773679, (letöltve: 2023.08.17.).

[10] Alrhmoun A., Winter C., Kertész J., “Automating Terror: The Role and Impact of Telegram Bots in the Islamic State’s Online Ecosystem,” *Terrorism and Political Violence*, pp. 1–16, 2023, doi: https://doi.org/10.1080/09546553.2023.2169141.

[11] Winter C., “Documenting the Virtual ‘Caliphate,’” Quilliam Foundation, 2015, https://core.ac.uk/download/pdf/30670971.pdf, (letöltve: 2023.09.01.)

[12] Cook J. and Vale G., “From Daesh to ‘Diaspora’: Tracing the Women and Minors of Islamic State,” *The International Centre for the Study of Radicalisation (ICSR)*, 2018.

[13] Singer P.W. and Brooking E.T, *Likewar : the weaponization of social media*. Boston: Houghton Mifflin Harcourt, An Eamon Dolan Book. Copyright, 2018.

[14] Winter C., “Media Jihad: The Islamic State’s Doctrine for Information Warfare,” The International Centre for the Study of Radiacalisation and Political Violence , London, 2017.

[15] Winter C., “ ‘Totalitarian Insurgency: Evaluating the Islamic State’s In-Theater Propaganda Operations,’” CIWAG Case Studies. 15, 2017.

[16] Berger J.M., Morgan J., “The ISIS Twitter Census Defining and describing the population of ISIS supporters on Twitter,” The Center for Middle East Policy, Washington, D.C., 2015.

[17] Berger J.M., “How terrorists recruit online (and how to stop it),” *Brookings*, 2015. https://www.brookings.edu/articles/how-terrorists-recruit-online-and-how-to-stop-it/ (letöltve: 2023.06.20.).

[18] Klausen J., “Tweeting the Jihad: Social Media Networks of Western Foreign Fighters in Syria and Iraq,” *Studies in Conflict & Terrorism*, vol. 38, no. 1, pp. 1–22, 2014, doi: https://doi.org/10.1080/1057610x.2014.974948.

[19] Lakomy M, “The virtual ‘Caliphate’ strikes back? Mapping the Islamic State’s information ecosystem on the surface web,” *Security Journal*, vol. 36, Dec. 2022, doi: https://doi.org/10.1057/s41284-022-00364-z.

[20] Europol, “Europol and Telegram take on terrorist propaganda online,” *Europol*. https://www.europol.europa.eu/media-press/newsroom/news/europol-and-telegram-take-terrorist-propaganda-online (letöltve: 2023. 06. 21).

[21] Kadivar J., “Daesh and the Power of Media and Message,” *Arab Media & Society*, 2021. https://www.arabmediasociety.com/daesh-and-the-power-of-media-and-message (letöltve: 2023.05.15.).

[22] Weimann G., Berton B., and Samouris A., “IS’s global digital arenas,” in *Salafi-Jihadism and Digital Media*, Ahlerup L. and Ahlin F., Eds., New York: Routledge, 2022,

[23] Criezis M., “““Create, Connect, and Deceive: Islamic State Supporters’ Maintenance of the Virtual Caliphate Through Adaptation and Innovation,” George Washington University, Washington D.C., 2022. https://extremism.gwu.edu/create-connect-deceive (letöltve: 2023.02.10.)

[24] Lakomy M., “‘Why Do Online Countering Violent Extremism Strategies Not Work? The Case of Digital Jihad,’ ,” *Terrorism and Political Violence*, vol. 35, no. 6, pp. 1–38, 2022, doi: https://doi.org/10.1080/09546553.2022.2038575.

[25] Fisher A., Prucha N., and Winterbotham E., “Mapping the Jihadist Information Ecosystem: Towards the Next Generation of Disruption Capability,” *www.rusi.org*, 2019. https://www.rusi.org/explore-our-research/publications/special-resources/mapping-jihadist-information-ecosystem-towards-next-generation-disruption-capability (letöltve: 2023.05.10.).

[26] Reichert C., “Facebook, Twitter and Google will testify to Congress on terrorist content,” *CNET*, 2019. https://www.cnet.com/tech/mobile/facebook-twitter-and-google-will-testify-on-terrorist-content/ (letöltve: 2024. 03. 17.).

[27] Lackey D., “How Much Data Do We Create Every Day? The Mind-Blowing Stats Everyone Should Read – Content For marketers,” *Blazon*, 2019. https://blazon.online/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read (letöltve: May 20, 2023).

[28] Möller J., “What is deplatformization and how does it work?,” *Israel Public Policy Institute (IPPI)*, 2022. https://www.ippi.org.il/what-is-deplatformization-and-how-does-it-work/ (letöltve: 2023. 03. 17.).

[29] Van Dijck J., de Winkel T., and Schäfer M.T:, “Deplatformization and the governance of the platform ecosystem,” *New Media & Society*, vol. 25, no. 12, p. 146144482110456, 2021, doi: https://doi.org/10.1177/14614448211045662.

[30] BBC, “Anonymous hackers ‘declare war’ on jihadists after France attacks,” *BBC News*, 2015. https://www.bbc.com/news/newsbeat-30755975, (letöltve: 2023.05.20.).

[31] Cohen K. and Kaati L., “Digital Jihad Propaganda from the Islamic State,” Totalförsvarets forskningsinstitut, Stockholm, 2018, https://www.foi.se/rest-api/report/FOI-R--4645--SE (letöltve: 2022.10.22.)

[32] Malsin J., “Understanding the ISIS vs. al-Qaeda Rivalry,” *TIME*, Nov. 24, 2015. https://time.com/4124810/isis-al-qaeda-rivalry-terror-attacks-mali-paris/ (letöltve: 2024.03. 17, 2024).

[33] BBC, “Twitter shuts 125,000 ‘terror’ accounts,” *BBC News*, 2016. https://www.bbc.com/news/world-us-canada-35505996 (letöltve: 2023. 08.20.)

[34] IS Central Media Diwan, “ Al-Hatif al-Jawwal ... al-Ma’asiyat al-Musta’siyah (A Mobil Telefon katasztrófa),” *Al Naba*, no. 56, pp. 8–9, 2016.

[35] IS Media Diwan, “Al-Hatif fi Khidmatik wa fi Khidmat A’ada’ek (A telefon az Ön szolgálatában áll, és a szolgálata az ellensége),” *Al Naba*, no. 56, pp. 14–15, 2016.

[36] Dar al Islam magazin 2015. numero 5. Les règles de sécurité du musulman (Muszlim biztonsági szabályok) (pp. 30-33.)

[37] Dar al Islam 2016. numero 9. Sécurité Informatique (Informatikai biztonság) (pp.39-53.)

[38] Azani E., Haberfeld D., “The end of Islamic State 's cyber security unit Afaq?,” Reichman Uiversity, International Institute for Counter-Terrorism., Herzliya, Israel, 2022.

[39] MEMRI, “Bank Al-Ansar - The ‘Supporters Bank’ - Supplies Jihadis With Ready-To-Use Face-book, Twitter Accounts,” *The Middle East Media Research Institute (MEMRI)*, 2016. https://www.memri.org/cjlab/bank-al-ansar-the-supporters-bank-supplies-jihadis-with-ready-to-use-facebook-twitter-accounts (letöltve: 2023.10.05.).

[40] ENSZ Közgyűlés, “The United Nations Global Counter-Terrorism Strategy : 8th review : resolution /: adopted by the General Assembly,” *digitallibrary.un.org*, vol. 41, no. 60, 2023, http://digitallibrary.un.org/record/4013935 (letöltve: 2023.11.20.).

[41] Bloomberg, “UN says crypto use in terror financing likely soaring,” *Mint*, 2022. https://www.livemint.com/market/cryptocurrency/un-says-crypto-use-in-terror-financing-likely-soaring-11667220010748.html (letöltve: 2023. 11. 08.).

[42] Chainalysis Team, “2023 Crypto Crime: Illicit Crypto Volumes Reach All-Time Highs,” *Chainalysis*, 2023. https://www.chainalysis.com/blog/2023-crypto-crime-report-introduction (letöltve: 2023. 03. 17.).

[43] Elliptic, “Terrorist Financing Through Cryptoassets in 2023,” *www.elliptic.co*. https://www.elliptic.co/resources/terrorist-financing-and-cryptoassets-in-2023 (letöltve: Dec. 15, 2023).

[44] Wang S., Zhu X., “Evaluation of Potential Cryptocurrency Development Ability in Terrorist Financing,” *Policing: A Journal of Policy and Practice*, vol. 15, no. 4, 2021, doi: https://doi.org/10.1093/police/paab059.

[45] ENSZ Biztonsági Tanács, “Letter dated 21 January 2021 from the Chair of the Security Council Committee pursuant to resolutions 1267 (1999), 1989 (2011) and 2253 (2015) concerning Islamic State in Iraq and the Levant (Da’esh), Al-Qaida and associated individuals, groups, undertakings and entities addressed to the President of the Security Council,” *documents.un.org*, 2021. https://documents.un.org/doc/undoc/gen/n21/000/98/pdf/n2100098.pdf? (letöltve: 2023. 10. 20.).

[45] De N., “Crypto Use in Terrorism ‘a Growing Problem,’ Yellen Says,” *www.coindesk.com*, 2021. https://www.coindesk.com/policy/2021/02/11/crypto-use-in-terrorism-a-growing-problem-yellen-says (letöltve: 2023. 11. 17.).

[46] ENSZ Biztonsági Tanács, “Letter dated 21 January 2021 from the Chair of the Security Council Committee pursuant to resolutions 1267 (1999), 1989 (2011) and 2253 (2015) concerning Islamic State in Iraq and the Levant (Da’esh), Al-Qaida and associated individuals, groups, undertakings and entities addressed to the President of the Security Council,” *documents.un.org*, 2021. https://documents.un.org/doc/undoc/gen/n21/000/98/pdf/n2100098.pdf? (letöltve: 2023. 10. 20.).

[47] Policy Department for Citizens' Rights and Constitutional Affairs, "Virtual Currencies and terrorist financing: assessing the risks and evaluating responses," *European Parliament*, 2018. https://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf (letöltve: 2023. 12. 02.).

[48] Popper N., "Terrorists Turn to Bitcoin for Funding, and They're Learning Fast," *The New York Times*, 2019. https://www.nytimes.com/2019/08/18/technology/terrorists-bitcoin.html (letöltve: 2023. 12. 22.).

[49] J. Wiwoho J., Pratama A.M., Pati U.K., Tejomurti K., "Examining Cryptocurrency Use among Muslim Affiliated Terrorists: Case Typology and Regulatory Challenges in Southeast Asian Countries," *Al-Ihkam: Jurnal Hukum dan Pranata Sosial*, vol. 18, no. 1, pp. 102–124, 2023, doi: https://doi.org/10.19105/al-lhkam.v18i1.7147.

[50] Dorshimer S., "The New Era in Cyber-Enabled Terrorist Financing," *Center for a New American Security (CNAS)*, 2020. https://www.cnas.org/publications/commentary/the-new-era-in-cyber-enabled-terrorist-financing (letöltve: 2023. 11. 28.).

[51] Chainalysis Team, "DOJ Takedowns Terrorism Financing with Blockchain Analysis," *Chainalysis*, 2020. https://www.chainalysis.com/blog/cryptocurrency-terrorism-financing-al-qaeda-al-qassam-brigades-bitcointransfer (letöltve: 2023. 12. 12.).

[52] Davis J., "ISIL-KP Financing," *Insight Monitor*, 2023. https://newsletter.insightthreatintel.com/p/isil-kp-financing (letöltve: 2024. 03. 17.).

[53] TRM Labs, "New Evidence Confirms ISIS Affiliate in Afghanistan Accepting Cryptocurrency Donations | TRM Insights," *TRM Labs*, 2022. https://www.trmlabs.com/post/new-evidence-confirms-isis-affiliate-in-afghanistan-accepting-cryptocurrency-donations (letöltve: 2024. 03. 17.).

[54] Chainalysis Team, "Terrorism Financing: Israel Seizes $1.7M in Crypto from Hezbollah," *Chainalysis*, 2023. https://www.chainalysis.com/blog/israel-nbctf-hezbollah-iran-quds-crypto-seizure/ (letöltve: 2023. 12. 12.).

[55] TRM Labs, "In Wake of Attack on Israel, Understanding How Hamas Uses Crypto | TRM Insights," *TRM Labs*, 2023. https://www.trmlabs.com/post/in-wake-of-attack-on-israel-understanding-how-hamas-uses-crypto (letöltve: 2023. 12. 10.).

[56] Tether, “Tether Freezes 32 Addresses Linked to Terrorism and Warfare in Israel and Ukraine,” *Tether, Tether Gold,* 2023. https://tether.to/en/tether-freezes-32-addresses-linked-to-terrorism-and-warfare-in-israel-and-ukraine/ (letöltve: 2023. 11. 28.).

[57] Naprys E., “Palestinian militants didn’t need to smuggle cash – they used crypto,” *Cybernews,* 2023. https://cybernews.com/news/palestinian-militants-used-crypto-for-fundraising/ (letöltve: 2023. 11. 18.).

[58] Martynova E., “Inside Look: The Financial Network Underpinning the Palestinian Islamic Jihad,” *Insight Monitor,* 2024. https://newsletter.insightthreatintel.com/p/inside-look-the-financial-network (letöltve: 2024. 03. 18.).

[59] Varghese H.M., Nagoree D.A., Jayapandian N., Anshu, “Cryptocurrency Security and Privacy Issues: A Research Perspective,” *IEEE Xplore,* 2021. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9489254&casa_token=aAtWr2pXPWUAAAAA:8tzuvQFu_UUmZHIeKkNSlOjiumRRgHmMhB1ST83WGxkPBvCx9EKRoVKrlul8POhdPawMDfZy1g&tag=1 (letöltve: 2023. 12. 23.).

[60] Ferdous MD.S., Chowdhury M.J.M., Hoque M.A., “A survey of consensus algorithms in public blockchain systems for crypto-currencies,” *Journal of Network and Computer Applications,* vol. 182, p. 103035, 2021, doi: https://doi.org/10.1016/j.jnca.2021.103035.

[61] Sagheer N., Khan K.I., Fahd S., Mahmood S., Rashid T., Jamil H., “Factors Affecting Adaptability of Cryptocurrency: An Application of Technology Acceptance Model,” *Frontiers in Psychology,* vol. 13, Jun. 2022, doi: https://doi.org/10.3389/fpsyg.2022.903473.

[62] Chainalysis Team, “2022 Global Cryptocurrency Adoption Index,” *Chainalysis,* 2022. https://blog.chainalysis.com/reports/2022-global-crypto-adoption-index/ (letöltve: 2023. 12. 08.)

[63] Shahzad M.F., Xu S., Lim W.M., Hasnain F., Nusrat S., “Cryptocurrency awareness, acceptance, and adoption: the role of trust as a cornerstone,” *Humanities and Social Sciences Communications,* vol. 11, no. 1, pp. 1–14, 2024, doi: https://doi.org/10.1057/s41599-023-02528-7.

[64] Darul Istaa UK, “Shaykh Mufti Muhammad Taqi Usmani’s latest position on Crypto Currency.,” *X (formerly Twitter)*, 2021.május 14. https://x.com/DarulIftaa/status/1392988550233313282 (letöltve: 2023. 12. 20.)

[65] Anonym, “Is Bitcoin Halal? A Guide To Cryptocurrency For Muslims | Bloom Money,” *bloommoney.co*, 2023. https://bloommoney.co/learning-hub/is-bitcoin-halal-a-guide-to-cryptocurrency-for-muslims (letöltve: 2023. 12. 20.)

[66] “Islamic Coin,” *islamiccoin.net*, 2024. https://islamiccoin.net (letöltve: 2023. 11. 21.)

[67] Schwartz L., “Bitcoin recedes as illicit actors look to Tron, Ethereum, and Binance Smart Chain in the evolving blockchain wars against law enforcement,” *Fortune Crypto*, 2023. https://fortune.com/crypto/2023/06/28/bitcoin-illicit-actors-tron-ethereum-binance-blockchain-wars/ (letöltve: 2024. 03. 17.)

[68] Davis J, “Terrorists storing funds in cryptocurrency?,” *newsletter.insightthreatintel.com*, 2023. https://newsletter.insightthreatintel.com/p/terrorists-storing-funds-in-cryptocurrency (letöltve: 2023. 12. 15.)

[69] Dion-Schwarz C., Manheim D., Johnston P.B., “Terrorist Use of Cryptocurrencies: Technical and Organizational Barriers and Future Threats,” *RAND Corporation*, 2019. https://www.rand.org/pubs/research_reports/RR3026.html (letöltve: 2023. 12. 07.)

[70] “Jihadist magazine offered $60,000 bounty for the killing of Western police officer,” *The Arab Weekly*, 2021. https://thearabweekly.com/jihadist-magazine-offered-60000-bounty-killing-western-police-officer

[71] Chainalysis Team, “Fact Checking Recent Cryptocurrency Terrorism Financing Reports,” *Chainalysis*, May 20, 2020. https://www.chainalysis.com/blog/cryptocurrency-terrorism-financing-fact-check (letöltve: Feb. 05, 2024).

[72] Katte S., “Countries ignoring crypto AML rules risk placement on FATF’s ‘grey list:’ Report,” *Cointelegraph*. Cointelegraph, 2022. [Mp4]. Available: https://cointelegraph.com/news/countries-ignoring-crypto-aml-rules-risk-placement-on-fatf-s-grey-list-report (letölve:2023.12.08.)

[73] Hummel K., “Banning Encryption to Stop Terrorists: A Worse than Futile Exercise,” *Combating Terrorism Center at West Point*, 2017. https://ctc.westpoint.edu/banning-encryption-to-stop-terrorists-a-worse-than-futile-exercise/ (letöltve: 2023.08.14.).

[74] Kundnani A., Hayes B., “The globalisation of Countering Violent Extremism policies Undermining human rights, instrumentalising civil society,” Transnational Institute, Amsterdam, 2018, https://www.tni.org/files/publication-downloads/the_globalisation_of_countering_violent_extremism_policies.pdf. (letöltve: 2023.08.01.)

[75] Saltman E.M., Winter C., “Islamic State: The changing face of modern jihadism,” Quilliam Foundation, London, 2014. https://issuu.com/m.r.mohamed/docs/islamic-state-the-changing-face-of- (letöltve: 2023.09.10.)

[76] Ehrenfeld R., *Funding evil updated : how terrorism is financed and how to stop it.*, Updated Edition 2011. Bonus Books, 2004, p. 11.

[78] Berman I, “Technology is Making Terrorists More Effective—And Harder to Thwart,” *The National Interest*, 2019. https://nationalinterest.org/feature/technology-making-terrorists-more-effective%E2%80%94and-harder-thwart-45452 (letöltve: 2023.12.10.).

[79] Gilmer E.M., “Technology-Savvy Terrorist Groups Seen Embracing Cryptocurrency,” *BLaw*, 2021. https://news.bloomberglaw.com/privacy-and-data-security/technology-savvy-terrorist-groups-seen-embracing-cryptocurrency (letöltve: 2023.11.11.).

[80] The Investopedia Team, “Cryptocurrency Explained With Pros and Cons for Investment,” *Investopedia*, 2023. https://www.investopedia.com/terms/c/cryptocurrency.asp (letöltve: 2024.07.11.).

[81] Yasar K., “Pros and cons of cryptocurrency,” *WhatIs.com*,2023. https://www.techtarget.com/whatis/feature/Pros-and-cons-of-cryptocurrency (letöltve: 2023.10.10.).

[82] Mapperson J., “The IRS offers a $625,000 bounty to anyone who can break Monero and Lightning,” Cointelegraph, 2020. https://cointelegraph.com/news/the-irs-offers-a-625-000-bounty-to-anyone-who-can-break-monero-and-lightning (letöltve: 2023.10.14.).
[83] 2012. évi C. törvény a Büntető Törvénykönyvről

A HIPOTÉZISEKHEZ KAPCSOLÓDÓ TUDOMÁNYOS KÖZLEMÉNYEIM

1. Gulyás Attila: The Dark Web (Strategic Impact (Romania) 1841-5784 1824-9904, 77/2020/4.)
   Besorolás: nemzetközi „D”
2. Besenyő János,Gulyás Attila: The effect of the dark web on the security (Journal of Security and Sustainability Issues 2029-7017 2029-7025 11/1)
   Hivatkozások száma: 12;
3. Gulyás Attila: Vállatbiztonság és dark web (Biztonságtudományi Szemle, 3/3 2021)
   Besorolás: hazai „C2”
4. Gulyás Attila: Dark Web Investigation: edited by Babak Akhgar, Marco Gercke, Stefanos Vrochidis, and Helen Gibson, Switzerland AG, Springer Nature, 2021, ISBN 978-3-030-55342-5, $141.67(hardback), 305 pages', Terrorism and Political Violence, 33(8), pp. 1807–1809. doi: 10.1080/09546553.2021.2000216.
   Besorolás: nemzetközi „Q2”
5. Gulyás Attila: A dark web világos oldala (Ügyészségi Szemle 2559-8112, 8/1 2023)
   Besorolás: hazai „D”
6. Gulyás Attila: A nyílt forrásból származó adatgyűjtés automatizálásának lehetőségei Belügyi Szemle: A Belügyminisztérium Szakmai Tudományos Folyóirata (2010-) 71 : 7 pp. 1237-1269. , 33 p. (2023)
   Besorolás: hazai „A”
7. Gulyás, Attila ; Demeter Márton ; Besenyő János:
   The Lernaean Hydra on the internet: Deplatformization-resistant media ecosystem of the Islamic State, Media War and Conflict 16 : 4 p. 9 Paper: OnlineFirst (2023)
   DOI WoS Scopus
   Besorolás: külföldi „Q1”
8. Besenyő János; Gulyás Attila ; Trifunovic Darko:
   Hezbollah and the Internet in the Twenty-First Century
   International Journal Of Intelligence And Counterintelligence online pp. 1-17. , 17 p. (2022) DOI WoS Scopus.
   Besorolás: nemzetközi „Q3”
   Hivatkozások száma: 9

9. Gulyás Attila: Dzsihadista terrorszervezetek kriptovaluta alapú online adománygyűjtése, Honvédségi Szemle – Hungarian Defence Review, 152(5), o. 60–78. doi: 10.35926/HSZ.2024.5.4.
   Besorolás: Hazai „A”

TÁBLÁZATJEGYZÉK

1. táblázat A kutatás során felépített adatbázisban szereplő szélsőséges iszlám terrorszervezetek weboldalainak száma forrás: a szerző szerkesztése 38

2. táblázat A Facebook 2022 első 3 negyedévében tiltott tartalmak számbeli alakulása Forrás: META Transparency Center 52

3. táblázat Az Instagram 2023 első 3 negyedévében tiltott tartalmak számbeli alakulása Forrás: META Transparency Center 52

4. táblázat A tanulmányozott dzsihadista magazinok listája Forrás: a szerző szerkesztése 82

5. táblázat Az összegyűjtött webolalak szervezetenkénti felbontásban forrás: A szerző szerkesztése 89

6. táblázat A szervezetekhez tartozó archív webolalak és az azokon kért adományok kriptovaluta nemenkénti megoszlása forrás: a szerző szerkesztése, rögzítés időpontja:2024.02.15. 89

7. táblázat A szervezetekhez tartozó aktív webolalak és az azokon kért adományok kriptovaluta nemenkénti megoszlása forrás: a szerző szerkesztése, rögzítés időpontja: 2024. 02.15. 89

8. táblázat A szervezetekhez tartozó darkwebes webolalak és az azokon kért adományok kriptovaluta nemenkénti megoszlása forrás: a szerző szerkesztése rögzítés időpontja: 2024. 02.15. 90

9. táblázat A sajtótudósításokban szereplő kriptovaluta lefoglalásban érintett terrorszervezetek listája 2019 február 01. és 2024. február 28 között. A szerző szerkesztése 97

10. táblázat A kutatás ereményinek összegzése (a szerző szerkesztése) 99

11. táblázat Az adatbázis mezői és adattípusai forrás: a szerző szerkesztése 127

ÁBRAJEGYZÉK

1. ábra A keresőkifejezések kiválasztásának folyamata (a szerző szerkesztése) 16

2. ábra Az Al-Kaida "Inspire" maganzinjának elérhetősége a Freeneten. Forrás: A szerző képernyőfotója 22

3. ábra The Mujahideen Poisons Handbook a Freenet hálózaton forrás: a szerző képernyőfotója 23

4. ábra Terrorist handbook a Freeneten forrás: A szerző képernyőfotója 24

5. ábra Al Kaida Military studies a freenet hálózaton forrás: a szerző képernyőfotója 25

6. ábra Az Iszlám Állammal kapcsolatos "hangsúlyozatlan" tartalom a webarchivumban forrás: szerző képernyőfotója.....36

7. ábra Az Iszlám Állam cenzúra elleni harcának erői, eszközei és módszerei forrás: a szerző szerkesztése.....40

8. ábra Az Iszlám Állammal szimpatizáló Muszlim hírekkel foglalkozó független dark webes weboldal képernyőfotója (a weboldal elérhetőségét a szerző csonkolta) forrás: a szerző képernyőfotója.....45

9. ábra Iszlám Államhoz köthető weboldal WhoIs rekordja (az oldal elérhetősége biztonsági okokból csonkolva) forrás: a szerzők képernyőfotója.....47

10. ábra Az Electronic Horizons foundation logója forras: képernyőfotó a biztonság és alkalmazás engedélyek mobil telefonokon című oktató filmből 48

11. ábra Az Electronic Horizons foundation forras: képernyőfotó a biztonság és alkalmazás engedélyek mobil telefonokon című oktató filmből.....50

12. ábra Az Afaq Electronic Foundation honlapján található oktatóanyag a kiberhadviselésről forrás: a szerző képernyőfotója 50

13. ábra Az AFAQ alapítvány weboldalán a tevékenység felfüggesztéséről és annak okáról szóló közlemény olvasható forrás: a szerző képernyőfotója (gépi fordítás arab nyelvről) 51

14. ábra A felvételek az Iszlám Állam egyik propaganda vieójából készített képernyő fotó forrás: szerzők képernyőfotója.....55

15. ábra Egy kiválasztott weboldalról követet linkek kapcsolódásának ábrázolása forrás: a szerző munkája.....57

16. ábra a webarchivum időközönként mentést készít a weboldalak pillanatnyi állapotáról. Forrás: a szerző képernyőfotója az Iszlám Állam egyik honlapjának mentéseiről. 59

17. ábra Egy Iszlám Állammal szimpatizáló felhasználó oldala, ahol videót és további linkeket oszt meg. forrás: a szerző képernyőfotója (a linkeket szándékosan csonkoltam).....60

18. ábra A Telegramrobotok szerepe a tartalommegosztásban.....61

19. ábra Az Iszlám Állam tartalomelosztó és kapcsolat fenntartó dark webes oldaláról készült képernyőfotó. forrás: a szerző képernyőfotója (az elérhetőség szándékosan csonkolásra került) 63

20. ábra Állítólagos Amaq hírügynökségi oldal a Facebookon forrás: a szerző képernyőfotója 64

21. ábra Bank al Ansar alapítvány telegram csatornáján terjesztett videó szerint a képen látható számú felhasználói fiókot hoztak létre a közösségi médiában.....65

22. ábra A kiadványok feldolgozásának munkafolyamata Forrás: a szerző szerkesztése.....84

23. ábra Kulcsszavak keresése az adatbázisban forrás: a szerző szerkesztése 85

24. ábra Felhívás a dzsihad kriptovalutával történő támogatására forrás: a szerző képernyőfotója a Voice of Khorasan magazin 33. szám 91.oldal, megjelent: 2024. február 16-i 86

25. ábra Felhívás Moneroban történő adakozásra az "Arkan" című magazin 58. oldalán (a szerző képernyőfotója).....87

26. ábra Az al Raud Media Archive darkwebes oldalán található adakozára történő felszólítás forrás: http://xxxxxcv2uv2h3fay3cpopxuug6fxyp2reykt7lg67hnuonhm4xxxxx.onion/ (2024.02.15.).....90

27. ábra A kaukázusi független dzsihadista weboldal adománykérő felülete forrás: a szerző képernyőfotója (2024.02.15.).....91

28. ábra A Jaysh-al-ummah-weboldalán található adakozásra történő felszólítás forrás: https://alraxxxx.nex/en/category/ (2024.02.15) 91

29. ábra A Jays al-Ummah nyilvános bitcoin címéhez kapcsolódó tranzakciók grafikus ábrázolása forrás: a szerző szerkeztése.....94

30. ábra A dark webes környezetben folytatott kutatás folyamatábrája forrás: a szerző saját szerkesztése.....123

31. ábra A II. hipotézishez kapcsolódó nyílt forrású információgyűjtés folyamata forrás: a szerző szerkesztése 129

MELLÉKLETEK

1. számú Melléklet

A kutatás során alkalmazott OSINT eszközök és eljárások

Hivatalos források

A kutatás során a terrorszervezetté nyilvánítás hazai rendjével és gyakorlatával kapcsolatban állásfoglalást, illetve segítséget kértem a Terrorelhárítási Központtól, azonban rendkívül nagy leterheltségükre hivatkozva elutasítottak.

A Készenléti Rendőrség Nemzeti Nyomozó Iroda Kiberbűnözés Elleni Főosztályától kértem segítséget a terrorszervezetek dark webes jelenlétével kapcsolatos tapasztalataikról, de arról tájékoztattak, hogy csak a TOR rendszerrel foglalkoznak és a terrorvonatkozású információk nem tartoznak a hatáskörükbe, ilyeneket nem is vizsgálnak.

A nyílt interneten alkalmazott módszerek

Kulcsszó alapján történő keresés

A kulcsszó alapján történő keresés során az ismert kereső motorokon (DuckDuckGo, Bing stb..) angol és arab nyelvű kulcsszavak és ezek különböző variációi felhasználásával futtatott keresések eredményeinek egyenkénti ellenőrzését követően a hasznosítható találati eredmények egy erre a célra dedikált MS Excel táblába kerültek mentésre.

Hasonló módon történt keresés az egyes kulcsszavak szándékosan eltorzított változataival. Ilyen például az „Islam” helyett az „I3lam”. Tekintettel arra, hogy a terrorszervezetek a cenzúra kijátszása érdekében, többek között ilyen technikákat alkalmaznak. Ezekre a technikákra az értekezés későbbi részében még visszatérek. A találatok az ellenőrzést követően ugyancsak a már említett táblázatba kerültek mentésre.

Kép alapján történő keresés

A keresés alapjául szolgáló képek forrásaként a különböző tudományos publikációkban szereplő releváns képek, a kulcsszó alapján indított keresés eredményeként mentett weboldalakról származó képek szolgáltak. A képalapú kereséshez a Google, a Bing és a „1 Tinyeye” és az „image-search.org” kereső szolgáltatásai kerültek felhasználásra. A releváns találatok a korábbiakkal megegyező módon kerültek mentésre.

Top Level Domain swapping (TLD swapping technic)

A TLD swapping technológia lényege, hogy megadott domain név alapján az erre a célra készített szoftver (https://dnstwist.it) az összes TLD variációt („com”, „edu”, stb.) és a domain név betűinek kombinációját teszteli és megpróbál csatlakozni a különböző variációkhoz. A sikeres csatlakozás eredményét listázza. A visszaadott linkeket követve a felhasználó pedig meggyőződhet arról, hogy a találatok relevánsak-e a kutatásához.

Ezzel a módszerrel a már felderített domain nevek további variáció is megtalálhatók. A szélsőséges iszlám terrorszervezetek bevett gyakorlata a cenzúra kijátszására, hogy egyszerre ugyan azt a domain nevet regisztrálják de két vagy több Top Level Domain-el. Például „xyz.com” és „xyz.tk”, vagy „yzy.com”. A releváns találatok a már ismert módon mentésre kerültek.

IP alapú domain ellenőrzés (Reverse IP domain check)

Ezzel a módszerrel fel lehet deríteni a domain szerverén milyen más webhelyek kerültek kiszolgálásra. Egyes esetekben ilyen módszerrel meg lehet találni egy adott webhely klónját, vagy esetleg tartalmilag hasonló párját, amit feltehetően ugyan az a felhasználó vagy felhasználói kör üzemeltet. Ilyen szolgálatás található a következő webhelyen: https://www.yougetsignal.com/tools/web-sites-on-web-server/

Internet Archivum (Wayback Machine) mint forrás

A Wayback Machine az egyik leghasználhatóbb és leghatékonyabb forrás a szélsőséges iszlám terrorista tartalmak felkutatására. A szolgáltatás lehetővé teszi a már nem elérhető oldalak visszamenőleges tartalmának megismerhetőségét, illetve a kulcsszavas keresés lehetőségének hála számos olyan tartalom érhető el, amely már valamilyen okból kifolyólag nem hozzáférhető. A szolgáltatás által elérhetővé tett tartalmak segítséget nyújtanak a leghatékonyabb kulcsszavak, illetve keresendő képek kiválasztásához.

Keresés felhasználónév alapján

A közösségi médiában a különböző forrásokból kivont felhasználó nevek keresés abból a feltételezésből indult miszerint egy adott kapcsolattartó email cím több weboldalon is megjelenhet, hasonlóan egy felhasználónév is több platformon is ugyan azon személyhez tartozhat. Ezt a feltevést kiindulópontként felhasználva a CS Linuxon telepített SocMint szoftvercsomag került ilyen célból alkalmazásra. A szoftver képes a legnépszerűbb közösségi média platformokon adott felhasználónév, vagy email cím ellenőrzésére és találat esetén az

eredmények listázására. Az eredmények az Aware Online” (https://www.aware-online.com/en/osint-tools/username-search-tool/)szolgáltatás segítségével kerültek ellenőrzésre, illetve kiegészítésre.
Amennyiben a felhasználónévhez kapcsolódóan sikerült releváns eredményhez jutni úgy annak elérhetősége szintén bekerült az adatbázisba.

Webszolgáltatások mint adatforrások

A kutatás során számos esetben szükség volt különböző gazdasági és népesség vonatkozású statisztikák beszerzésére. Erre a célra a statista.com ingyenes lehetőségeit, illetve a World Bank Open Data szolgáltatásait használtam. A terrorizmussal kapcsolatos adatok beszerzése esetén a Global Terrorism Database és annak riportjai bizonyultak a leghasznosabb hiteles információforrásnak.
A webszolgáltatásokkal kapcsolatos forgalmi és egyéb statisztikai adatok beszerzésénél egyrészt a Google Trends szolgáltatásit, illetve a Semrush keresőoptimalizációs szolgáltatásait használtam.

Dark webhez köthető módszerek

A dark webes környezetben a nyílt internetes kutatásnál alkalmazott módszerek nem, vagy csak nagyon korlátozott mértékben alkalmazhatók. A dark webes tartalmak esetében alaphelyzetben nincs lehetőség a tartalmak indexelésére, jelen helyzet szerint nem lehetséges teljes körűen megállapítani, hogy milyen szolgáltatások léteznek, illetve ezek hol találhatók és ki üzemelteti őket. A dark weben folytatott kutatás sémája a 30. számú ábrán látható

Nyílt interneten történő keresés dark webes tartalomra

A nyílt interneten az népszerű kereső motorokban a már ismert kulcsszavak és az egyes dark webes szoftvermegoldások nevére illetve top level domainjeikre történt keresés. Ezt követően a releváns rendszerben a felderített cím felkeresésével a tartalom ellenőrzése. A releváns eredmények a már ismert módon kerültek mentésre az adatbázisban.

Linkgyűjtemények használata

A dark weben történő keresés alapját a különböző tematikus és leginkább a cenzúramentes linkgyűjteményekben történő keresés képezte. Az itt található linkek közül leginkább a különböző fórumok, illetve csevegőszobák tűntek a legígéretesebbnek, azonban ilyen módon releváns találatot elérni nem sikerült. Tekintettel arra, hogy az ilyen jellegű nyilvános

szolgáltatások esetében az üzemeltetők igyekeznek kiszűrni a terrorvonatkozású posztokat, mivel ez magára vonná a rendvédelmi szervek, illetve titkosszolgálatok figyelmét, ami hátrányosan befolyásolná az egyébként jellemzően illegális témákkal (drogfogyasztás, hitelkártyacsalás stb.) foglalkozó szolgáltatásaik biztonságát.

Dark webes kereső motorok használata

A dark weben nem léteznek a nyílt interneten megszokotthoz mérhető hatékonyságú keresőmotorok. A dark webes oldalak nincsnek indexelve. A kereső motorok leginkább csak azokat a webhelyeket indexelik, amelyeket hozzájuk bejelentenek. Történtek kísérletek a dark webes tartalmak felmérésére, azonban ezek inkább a weboldalak kapcsolati hálójára fókuszáltak a tartalmi összefüggések helyett. Mindazonáltal ezek a felmérések a weboldalak illékonysága miatt inkább a pillanatnyi helyzetet tükrözik mintsem, hogy napi használatra alkalmas linkgyűjteményként használhatók legyenek. A dark webes a szolgáltatás üzemeltetője, ha akarja, nem hozza nyilvánosságra szolgáltatás elérhetőségét úgy arról rajta kívül nincs senkinek sincs tudomása. Ennél fogva lehetetlen teljes bizonysággal kijelenti, hogy egy adott weboldal létezik, vagy sem, nem beszélve arról, hogy lehetetlen megjósolni a legközelebbi online jelentlét időpontját. Ebből adódóan a dark webes oldalak elérhetősége rendkívül hektikus. Az elérhetőség függ attól, hogy a felhasználó hol tárolja a weboldalt, hiszen lehetőség van a saját számítógépén is szolgáltatás létrehozására. Ebben az esetben a hálózatról való lecsatlakozás esetén az elérhetetlenné válik. Ilyen esetekben olyan tényezőket is figyelembe kellene venni, mint a tulajdonos időzónája, hiszen lehetséges, hogy az online jelenlét az illető időzónájától függ. Ezzel az információval viszont az anonim rendszer miatt nem rendelkezünk. A fenti korlátok mellett természetesen működnek keresőmotorok, különösen a TOR rendszeren található számos példány. Esetünkben sajnos hátrányként jelentkezik, hogy az üzemeltetők állítólag a legtöbb esetben a terrorvonatkozású tartalmakra mutató linkeket kiszűrik. Azt azonban nem tudjuk, hogy valóban találtak-e ilyen oldalakat és ki kellett szűrniük, vagy pedig nem is találtak ilyen tartalmakat. A kevés kivételhez tartozik az „ahmia” keresőmotor, amelyen több Iszlám Államhoz kapcsolható dark webes tartalmat is adott a találati listájában. A releváns találatok ebben az esetben is mentésre kerültek.

Saját dark webes linkgyűjtemény ellenőrzése

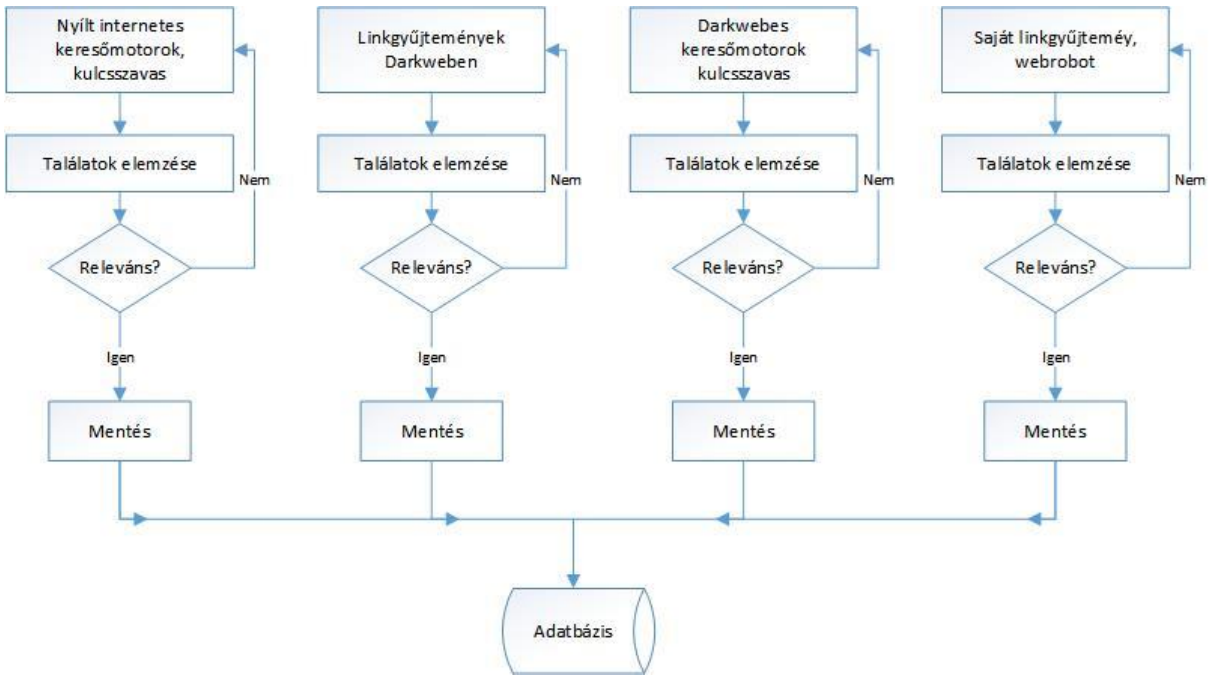
A kutató munka során felvettem a kapcsolatot két dark web kutatóval, akik rendelkezésemre bocsájtották saját linkgyűjteményüket. A saját gyűjteményemmel együtt az ellenőrzendő linkek száma meghaladta a harmincezer darabot. Ennek a mennyiségnek az ellenőrzése meghaladja az

emberi teljesítőképességet, ezért erre a célra egy Pythonalapú szoftvert készítettem, amely ellenőrizte az oldal elérhetőségét, illetve annak címe és az oldalon előforduló leggyakoribb szavak alapján az oldal tartalmát. A kapott eredményt „csv” formátumú szövegfájlba mentette, amelyet MS Excelben egyszerűen lehet kezelni. Sajnos az ellenőrzés nem talált terrorvonatkozású weboldalakat.

Webcrawler használata

A webcrawler olyan szoftver , amely egy adott webhelyről elindulva a meghatározott mélységig követi a linkeket ezáltal a külső linkek követésével újabb webkapcsolatok deríthetők fel.

A találati listában szereplő weboldalakon saját fejlesztésű Pythonalapú webcrawler került indításra a nyílt és a darkweben egyaránt két link mélységig történő beállítással. Ezzel a módszerrel mindkét domainen sikerült néhány új, eddig nem ismert weboldalt felderíteni. Ezek hasonlóan a korábbi releváns találatokhoz mentésre kerültek.



30. ábra A dark webes környezetben folytatott kutatás folyamatábrája forrás: a szerző saját szerkesztése

Az eredmények grafikus ábrázolása

Az adatgyűjtés során feltárt struktúrák és kapcsolatok ábrázolása az ingyenes Social Network Visualizer és Gephi alkalmazások felhasználásával történt. A szoftverek lehetőséget teremtettek a nagy mennyiségű adatban meghúzódó rejtett kapcsolatok, összefüggések felismerésére, majd ezek ábrázolására.

Bitcoin áramlásának nyomon követése

A terrorszervezetek kriptovalutával való kapcsolatának vizsgálatakor a felderített releváns weboldalakból a támogatás céljából meghirdetett Bitcoin pénztárca címek kigyűjtésre kerültek. A kriptopénztárcák közötti forgalom ellenőrzésére számos ingyenes webszolgáltatás vehető igénybe azonban ezek nyers adatokat szolgáltatnak és további feldolgozásuk manuálisan rendkívül időigényes. Ezt a feladatot a részben ingyenes Maltego szoftver Bitcoin követő funkciója automatikusan megoldja és a pénztárcák közötti kapcsolatokat a meta adatokkal együtt grafikusan is ábrázolja. Ezzel a módszerrel a kutatás szempontjából releváns adatokat sikerült kinyerni, amelyek a manuális módszerrel valószínűleg rejtve maradtak volna.
A kutatás során a felderített Bitcoin címek és az ezekkel kapcsolatban álló további Bitcoin címeket a kapcsolati hálózatuk hármas szintű mélységéig követtem. A kutatás során felmerült címeket olyan nyílt adatbázisokban ellenőriztem, amelyeket kiberbiztonsági cégek és non-profit szervezetek hoztak létre a bűncselekményekkel kapcsolatba hozható címek nyilvántartására. Néhány ilyen nyilvántartásba többek között az áldozatok és más felhasználók is tölthetnek fel olyan címeket, amelyek ransomware, vagy egyéb más bűncselekményekkel hozhatók összefüggésbe. Tapasztalatom szerint nincs olyan nyilvántartás, amely átfogná a teljes spektrumot, ezért célszerű volt egy adott címet több más nyilvántartásban is ellenőrizni. Az ellenőrzés eszközei az alábbi linken találhatók:. https://start.me/p/6rvdx4/cryptocurrency-intelligence

A Telegram, mint információforrás

A Telegram azonnal üzenetküldő alkalmazás kedvező tulajdonságai miatt rendkívüli népszerűségnek örvend a hétköznapi felhasználók és a különböző bűncselekmények elkövetőinek körében egyaránt. A kutatás szempontjából vizsgált szélsőséges iszlám terrorszervezetek közül leginkább az Iszlám Államra jellemző, hogy mesterien kihasználja az alkalmazás nyújtotta lehetőségeket. A nyílt csatornák mellett előszeretettel használják a zárt csevegőcsoportokat, mint tartalommegosztó központokat (hub), illetve széles körben alkalmazzák a robotokat (automata szoftverkomponenseket), mint kapuőröket, amelyek megfelelő feltételek teljesülése esetén a felhasználó részére megadják az adott zártkörű csoporthoz vezető linket. A felhasználó ennek a linknek a birtokában csatlakozhat a csoporthoz, azonban itt további ellenőrzéseken kell átesnie. A csatorna gazdája, illetve a csoport tagjai vallási, illetve ideológiai kérdéseket tehetnek fel, illetve felszólíthatják az új résztvevőt, hogy ossza meg a tiltott tartalmat és ezt igazolja is. Ilyen feltételek mellett a kutatónak meg kell

szakítania a kutatás további folytatását, mivel ez a terroristákkal való kommunikációval járna, ami egyrészt etikai kérdéseket vet fel, másrészt bűncselekmény elkövetésének számít.
A kutató számára a nyílt csatornákon található tartalmak felkutatása és elemzése az egyetlen etikailag helyes és törvényes út.
A nyílt csatornák szerepe sem elhanyagolható, hiszen sok esetben ezek azok a kiinduló pontok, ahol a terrorszervezetek a nyílt interneten bevált módszereiket alkalmazva igyekeznek a tartalmaikat, illetve propagandájukat a felhasználók széles köréhez eljuttatni. Az ilyen üzenetek elemzésével újabb elosztóközpontokat, illetve forrásokat, webhelyeket, kriptovaluta címeket lehet felderíteni.
A Telegram alkalmazáson belül a nyílt csatornákon a következő nyílt forrású információgyűjtő lehetőségek állnak a kutató rendelkezésére:

A Nyílt csatornák tartalmának elemzése

Számtalan olyan nyílt csatorna található a rendszerben, amely ugyan nem közvetlen terrorvonatkozású, azonban tartalmukat tekintve vannak átfedések. Ilyenek a különböző OSINT, Military, Security, Cyber Secirity tematikájú csatornák, amelyeken lehetséges olyan információk, képek, linkek kinyerése, amelyek további kutatómunka alapját képezhetik. Ezek alapján nyílt interneten képkeresését, vagy kulcsszóalapú keresést lehet indítani.

Kulcsszóalapú keresés

Az alkalmazásba beépített keresőfunkcióban a már korábban már ismertetett módszerrel a nyílt interneten bevált keresőkifejezések használata egyes esetekben eredménnyel járhat. Az alkalmazásban ezeket a kereséseket gyakrabban kell végrehajtani, mert a közvélekedéssel ellentétben a Telegram közösségi nyomásra cenzúrázza a nyílt csatornákon megjelenő terrorvonatkozású tartalmakat. A terrorizmus támogatásának vádját kikerülendő például létezik egy „ISIS_hunter” csoport, amely gyűjti a felhasználóktól származó bejelentéseket és folyamatosan távolítja el a kifogásolt tartalmakat.

Közösségi médiaelemzés

A Telegram tartalmakhoz a más forrásokból származó tartalmak elemzésével is hozzá lehet jutni. Tapasztalataim szerint a legtöbb általam felderített terrorvonatkozású weboldal elvezetett egy, vagy több telegram linkhez, amely mögött általában egy robot, vagy egy titkos csevegőcsoport húzódott meg.

Telegram specifikus keresőmotorok

A Google több olyan Telegram specifikus kereső szolgálatatást is üzemeltet, amelyek a nyílt csatornák tartalmát indexelik és kereshetővé teszik. Ilyen például a „Commentgram”, vagy a „Telegago”. Hasznos keresőeszköz a Lyzem és az OSINT ME által fejlesztett CSE keresőmotor, vagy a TGStat, amelyen a csatornák meta adatai érhetőek el látogatottsági statisztikákkal kiegészítve. A lista korántsem teljes számos más szolgálatatás is elérhető, ezek közül néhány kizárólag orosz nyelven.

A Telegramon történő kutatás során betartandó célszerű óvintézkedések

- A telegram alkalmazásba történő regisztráció feltétele egy SMS fogadására alkalmas telefonszám. Ha lehetséges célszerű erre a célra a saját telefonszám helyett egy SMS fogadására alkalmas szolgáltatást igénybe venni.
- A kutatásra használt telefont más célra ne használjuk tekintve, hogy a kutatás szempontjából vizsgált tartalmak olyan kártevőket tartalmazhatnak, amelyek felfedhetik a kutató kiléte és személyi adatait.
- Az alkalmazás használata során célszerű anonim VPN szolgálatatást használni, tekintve, hogy a vizsgált tartalomban gyakran találhatók linkek, amelyek követése felfedheti a felhasználó IP címét és más egyéb érzékeny adatokat az eszközéről.

A Telegram alkalmazás használata során egyébiránt nincs jelentősége a VPN használatnak, mivel a szerver és a kliens közötti kapcsolat nem IP cím alapú, hanem eszköz és szerver, tehát hiába a VPN a Telegram szerver egyértelműen tudja, hogy melyik eszközzel áll kapcsolatban.

2. számú melléklet

A dzsihadista online jelenlét felméréséhez szükséges adatbázis építés folyamata

Bevezetés

A dzsihadista online jelenlét kutatásához szükséges adatbázis építés érdekében a nyílt forrású információgyűjtés keretében célirányosan olyan eszközöket választottam ki, amelyek egyrészt alkalmasak voltak a kutatás szempontjából releváns weboldalak, felhasználói fiókok, posztok összegyűjtésére, ezek rendszerezésére, másrészt az egyes elemek közötti kapcsolatok ábrázolására. A hipotézis bizonyításához, illetve cáfolásához szükséges nyílt információgyűjtés keretében folytatott adatbázisépítés menete az 31. számú ábrán látható.

A kulcsszavak forrása, mint arra már utaltam a tudományos, munkákból, szakkönyvekből, ismeretterjesztő kiadványokból származik. Ezek kiválasztásának folyamatát az 1. hipotézis esetében már ismertettem. (1.2.2 fejezet)

A kutatás szempontjából hasznos linkeket MS Excel táblában gyűjtöttem. A táblázat az 11. számú táblázatban található mezőket és adattípusokat tartalmazza.

Mezőnév	Adattípus		Mezőnév	Adattípus
URL	szöveg		**Kezdete**	dátum
Év	szám		**Vége**	dátum
Különbség	szám		**Mentések**	szám
Élő?	bináris		**Arhiv?**	bináris
Jihad?	bináris		**Vallási?**	bináris
Napi	bináris		**Kérés**	bináris
Crypto	szöveg		**Nyelv**	szöveg
Ország	szöveg		**Szervezet**	szöveg
Társult	szöveg		**Tiltott**	szöveg
Link	szöveg		**Megjegyzés**	szöveg

11. táblázat Az adatbázis mezői és adattípusai forrás: a szerző szerkesztése

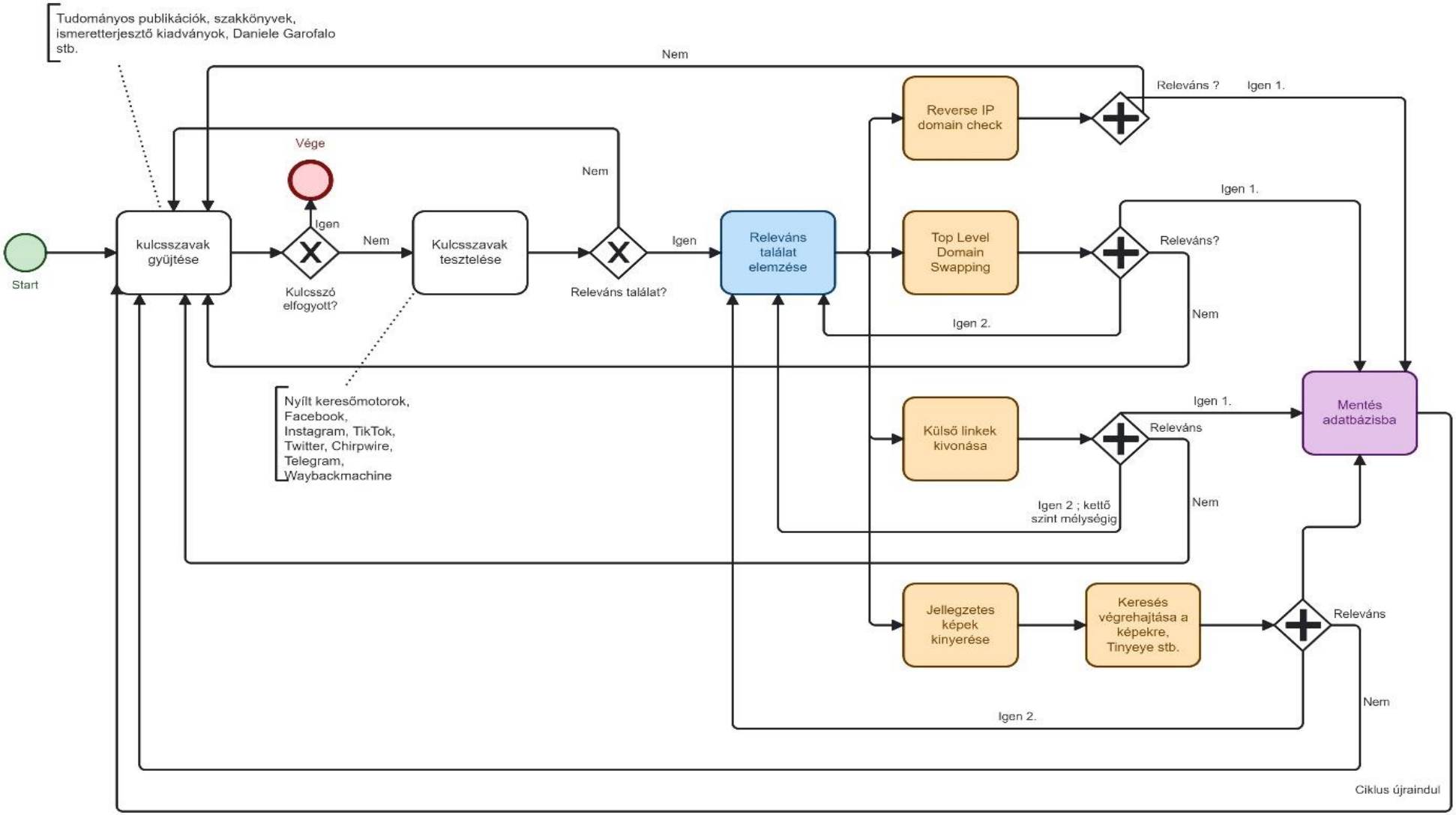
A hasznosnak ítélt weboldal esetében megvizsgáltam a megjelenésének idejét, az utolsó ismert online állapotát, amennyiben már nem működött. Ennél a pontnál fontosnak tartom megjegyezni, hogy az oldal első megjelenésénél nem a domain regisztráció idejét vettem figyelembe, hanem a Wayback Machine-ban történő első megjelenés idejét. Természetesen ezt sem lehet tökéletesen pontosnak számítani, de az weboldal élettartamának kiszámításához és

az arányos későbbi összevetéséhez ez tűnt a legmegfelelőbb megoldásnak. A jellegét tekintve vizsgáltam, hogy kifejezetten dzsihadista a tartalom, vagy vallási, esetleg napi információkat tárol. Vizsgáltam továbbá, hogy a van-e az oldalon adakozásra történő felszólítás, ha igen, akkor azt milyen kriptovalutában kéri. Rögzítettem, hogy milyen az oldal elsődleges nyelve, mely országhoz tartozik, ha ez megállapítható. Melyik „fő" terrorszervezethez köthető, ha a szóban forgó oldalt valamely társult terrorszervezet működteti, vagy ahhoz kapcsolható. Vizsgáltam azt is, hogy van-e nyoma annak, hogy az oldalt hivatalosan betiltotta-e valamelyik rendvédelmi szervezet, rögzítettem az elérhetőségét, illetve készítettem egy megjegyzés rovatot. A kutatás időszakában az adatbázis folyamatos karbantartásáról gondoskodtam.

Az adatbázis építés folyamata

- A különböző forrásokból származó kulcsszavakat teszteltem a felsorolt platformokon.
- Amennyiben releváns találat keletkezett azt elmentettem az adatbázisba, majd a tartalom jellegétől függően végrehajtottam az IP cím alapján történő ellenőrzését annak érdekében, hogy megtudjam, milyen más weboldalakat tárolnak az adott szerveren. Ha releváns weboldalt találtam, akkor azt elmentettem az adatbázisba, majd azt is elemeztem.
- A releváns weboldalakon végrehajtottam a Top Level Domain Swapping ellenőrzést, hogy megállapítsam az adott weboldalnak van –e olyan klónja, mely más TLD alatt fut.
- Az elemzett weboldalakból kivontam az olyan képeket, amelyek alkalmasak lehetnek más, esetleg klónozott webhelyek, kiadványok, posztok felderítésére
- A releváns weboldalakból kivontam a külső webhelyekre mutató linkeket és ezeken is végrehajtottam az elemzést és a fentebb felsorolt ellenőrzéseket két szint mélységéig

Az adatbázis építés során az I. számú hipotézis kapcsán végzett kutatás alkalmával felderített hasznos linkeket is felhasználtam.



31. ábra A II. hipotézishez kapcsolódó nyílt forrású információgyűjtés folyamata forrás: a szerző szerkesztése

KÖSZÖNETNYILVÁNÍTÁS

Köszönöm Prof. Dr. Besenyő Jánosnak témavezetőmnek, amiért támogatásával és személyes motivációjával sikerült befejeznem az értekezést.

Szeretném megköszönni Justin Seitz kanadai etikus hackernek, amiért megerősített abban, hogy dark webes kutatásomban jó irányba haladok.

A doktori iskola munkatársainak, akik segítettek, támogattak és hozzájárultak tanulmányaim sikeres befejezéséhez.

Végül, de nem utolsósorban köszönöm páromnak amiért türelemmel viselte, hogy gyakran a közös időtöltésre szánt időt is a kutatásomra fordítottam.