ÓBUDAI EGYETEM
ÓBUDA UNIVERSITY

DOKTORI (PHD) ÉRTEKEZÉS
TÉZISFÜZETE

GULYÁS ATTILA

Dzsihadista terrorszervezetek tevékenysége az interneten

Témavezető: **Prof. Dr. Besenyő János**

BIZTONSÁGTUDOMÁNYI DOKTORI ISKOLA

Budapest, 2024. június 30.

Tartalomjegyzék

1 Summary

The author examined the impact of today's digital and communication revolution on the activities of jihadist terrorist organizations, that is, how these organizations have adapted to the new technological and security environment. He formed his hypotheses so that their examination reveals the relationship of jihadist terrorist organizations to today's latest digital achievements. All three hypotheses refer to uncertainty regarding the relationship between jihadist groups and new technologies. This is partly due to the fact that these organizations try to keep their activities secret and do not make their methods and procedures public, so the extent of the applicability of new technologies and their usefulness for organizations is not known to many, or only partially.

The author first examined the relationship between jihadist terrorist organizations and the dark web and sought to answer the question of whether terrorist organizations have switched to the use of the dark web, which provides anonymity and censorship resistance, as a result of counter-activity from law enforcement agencies and social media stakeholders. The information collected using a wide range of OSINT tools and methods refuted the extensive use of the dark web by jihadist terrorist organizations.

In the remaining part of the research, he examined how jihadist terrorist organizations can ensure their continuous online presence despite widespread censorship. The data collected using a unique OSINT-based data collection system created by the author proved that jihadist terrorist organizations have the tools, methods, and procedures that enable them to ensure their continuous online presence on the World Wide Web.

Finally, the author examined the relationship between jihadist terrorist organizations and cryptocurrencies. He used three procedures to estimate the extent of use. First, he examined the online publications of the organizations in question for signs of cryptocurrency use, then examined the organizations' websites seeking cryptocurrency-based donation requests, and finally, he examined press reports related to cryptocurrency seizures. As a result of the research, he concluded that the use of cryptocurrency by terrorist organizations can be considered to be negligible.

Summarizing the results of the research, the author concluded that jihadist terrorist organizations are extremely susceptible to new technologies but do not give up their previously well-established, long-used methods and procedures just for the sake of technological change and novelty.

2 A kutatás előzményei

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, és 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 az X (korábban 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 is 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, valamint 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 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 és aktuálissá a dzsihadista terrorszervezetek online tevékenységének tudományos igényű kutatását.

3 Célkitűzések

A kutató munka során három olyan ellentmondásos kérdést azonosítottam, amelyek tisztázása elősegítheti a terrorszervezetek internetes tevékenységének jobb megértését ezzel javíthatva az ellenük folytatott harc hatékonyságát.

Elsődleges problémaként fogalmaztam meg a dark web és a dzsihadista terrorszervezetek 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 tevékenységüket 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 korábban 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 részkutatásokat 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 kívántam tisztázni. Kutatási területem és a terrorszervezetek pénzügyi műveleteinek egy része az online térben metszik egymást, így nem kerülhettem ki az internettől 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 ezen 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.

Értekezésemben megfogalmazott hipotézisek igazolása, illetve cáfolása keretében átfogó képet nyújtok a terrorszervezetek internetes tevékenységéről. Elsősorban tisztázom, hogy a tudományos életben elterjedt nézetnek megfelelően a terrorszervezetek online 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.

Harmadsorban 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.

Végül tekintettel arra, hogy a kutatásom során felderített terrorista vonatkozású tartalmak prezentálása, illetve terjesztése büntetőjogi következményekkel járna olyan kutatási modellt alkotok meg, amely lehetővé teszi a nyílt forrású információgyűjtés eszközeinek és módszereinek széleskörű alkalmazásával a hatékony adatgyűjtést és a kutatás megismételhetőségét.

A kutatásom célja, hogy a megfogalmazott problémák tisztázásával hozzájárulhassak a terrorizmus ellen folytatott online harc sikeréhez azzal, hogy feltárom és bemutatom a terrorszervezetek internetes tevékenységére napjainkban jellemző eszközöket, módszereket és eljárásokat.

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 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.

4 Vizsgálati módszerek

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 kutatás kezdetén telepítettem, majd folyamatosan használtam a dark webes alkalmazásokat és a Telegramot, annak érdekében, hogy működésüket, illetve a kutatásom szempontjából legjellemzőbb tulajdonságaikat megismerjem.

Tekintettel arra, hogy a 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 tartalmakat

felkutassam és az eredményekből saját adatbázist hozzak létre. Az adatgyűjtés során széles körben alkalmaztam a nyílt forrású információgyűjtés eszközeit és módszereit, amelyek hatékony felhasználása érdekében Python nyelvű scripteket fejlesztettem.

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 értekezésemben elérhetővé tettem.

Hivatalos támogatás megszerzése érdekében szóban 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 értekezésemben 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.

5 Új tudományos eredmények

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.

A dark web a nyílt internettel szemben számos olyan technikai sajátossággal rendelkezik, amelyek befolyásolják a kutató lehetőségeit, ezért a technológia megismerése nélkül hatékony és eredményes kutatás ezen a domainen nem lehetséges. A dark webes platformok működését, sajátosságaikat és a dark web használati lehetőségeinek kettősségét, valamint ezek hatását a biztonságra az N1-N5-ig számozott publikációimban dolgoztam fel. Újszerű megközelítést tükröz, hogy hipotézisem vizsgálatánál 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 felderítenem 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. Dark webes tartalmaik jellemzően a nyílt internetes tartalmaik egyfajta biztonsági másolataiként szolgálnak. Az első hipotézis vizsgálatával kapcsolatban a dark web használatát mindössze az Iszlám Államhoz köthető két alapítvány esetében sikerült egyértelműen kimutatni.

Tézis 1:

A dzsihadista terrorszervezetek a rendvédelmi szervek és a közösségi média érdekelt felei részéről kifejtett ellentevékenység ellenére sem tértek át a dark web használatára

A dzsihadista terrorszervezetek cenzúra elkerülési technikáinak vizsgálatát illetően az eddigi kutatókkal szemben nem egyenként vizsgáltam az Iszlám állam cenzúraelkerülési technikáit, hanem egységes szerkezetben rendszerszemlélettel közelítettem meg végig követve annak evolúcióját. Megállapítottam, hogy az evolúciós folyamat során a terrorszervezet minden ellenintézkedésre olyan hatásos ellenlépésekkel tudott válaszolni, amelyek lehetővé teszik az online jelenlétének folyamatos 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. A dzsihadista terrorszervezetek cenzúraelkerülési technikának elsőkézből történő vizsgálata érdekében széles körben alkalmaztam nyílt információgyűjtés eszközeit és módszereit, amelyeknek automatizált felhasználásával kapcsolatban összegyűjtött tapasztalataimat N6-os számú publikációmban ismertettem. A szélsőséges iszlamista terrorszervezetek internethasználatával és cenzúraelkerülési technikáival kapcsolatban az N7-N8 sorszámon található publikációimban számoltam be.

Tézis 2:

A dzsihadista terrorszervezetek rendelkeznek azokkal az eszközökkel, módszerekkel és eljárásokkal, amelyekkel a korlátozó, illetve akadályozó intézkedések ellenére biztosítani tudják folyamatos online jelenlétüket a világhálón.

A szakirodalomban egymásnak szögesen ellentmondó nyilatkozatok, publikációk jelentek meg a szélsőséges iszlamista terrorszervezetek kriptovaluta-használatát illetően. Ennek az ellentmondásnak a feloldása érdekében a dzsihadista terrorszervezetek kriptovaluta használatának mértékét egyszerre több megközelítésből is vizsgáltam. Felmértem, hogy a terrorszervezetek online kiadványaiban szerepet kap-e a kriptovaluta-használattal kapcsolatos oktatás, majd megvizsgáltam, hogy a második hipotézisnél felállított adatbázisban milyen számban történt kriptovalutában történő adománykérés, és végül összegyűjtöttem az elmúlt öt

évben milyen számban fordultak elő a világsajtóban terrorszervezetekhez köthető kriptovaluta lefoglalásokkal kapcsolatos tudósítások. A kriptovalutában történő adománygyűjtéssel kapcsolatban az N9-es számú publikációmban számoltam be.

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.

Tézis 3:

A dzsihadista terrorszervezetek az ellenük bevezetett nemzetközi pénzügyi korlátozó és szankciós intézkedések ellenére nem tértek át a kriptovaluták használatára

6 Az eredmények hasznosítási lehetősége

Az általam megalkotott egyedi kutatási, illetve adatfeldolgozási modell más kutatási területeken is alkalmazható, ezért ajánlom mindazoknak a kutatóknak, akik kutatásuk során nagy mennyiségű internetes OSINT alapú adatot gyűjtenek, illetve dolgoznak fel.

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 ennél fogva hozzájárulnak a dzsihadista terrorszervezetek internetes tevékenységének valóságot jobban megközelítő megismeréséhez.

7 Irodalmi hivatkozások listája/ Irodalomjegyzék

[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

[84] "Performance – Tor Metrics," *metrics.torproject.org*, 2024. https://metrics.torproject.org/torperf.html (letöltve: 2024. 06.28).

[85] United Nations Secuity Council (UNSC Report S/2017/97

[86] Weimann G., "Going Darker: Challenge of Dark Net Terrorism," 2018. https://www.scribd.com/document/380971367/Going-Darker-Challenge-of-Dark-Net-Terrorism #from_embed (letöltve: 2023.10.20).

8 Publikációk

8.1 A tézispontokhoz kapcsolódó tudományos közlemények

N1. Gulyás Attila: The Dark Web (Strategic Impact (Romania) 1841-5784 1824-9904, 77/2020/4.) Besorolás: nemzetközi „D”

N2. 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;

N3. Gulyás Attila: Vállatbiztonság és dark web (Biztonságtudományi Szemle, 3/3 2021) Besorolás: hazai „C2”

N4. 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”

N5. Gulyás Attila: A dark web világos oldala (Ügyészségi Szemle 2559-8112, 8/1 2023) Besorolás: hazai „D”

N6. 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”

N7. 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”

N8. 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

N9. 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.

8.2 További tudományos közlemények (opcionális)

N10. 32790735 Folyóiratcikk Konferenciaközlemény (Folyóiratcikk) Gulyás, Attila [Gulyás, Attila (hadtudomány), szerző] Biztonságtudományi Doktori Iskola (ÓE) "LAZARUS" THE NORTH KOREAN HACKER GROUP 2022 DOI: 10.53477/2668-6511-22-08; Egyéb URL: https://revista.unap.ro/index.php/XXI_CSSAS/article/view/1354

N11. 33107149 Folyóiratcikk Ismertetés (Folyóiratcikk) Gulyás, Attila [Gulyás, Attila (hadtudomány), szerző] Biztonságtudományi Doktori Iskola (ÓE) Könyvismertető; Book review 2022 Review about the book Amy B. Zegart: Spies, Lies, and Algorithms: Teljes dokumentum: https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/243/209

N12. 32790756 Folyóiratcikk Szakcikk (Folyóiratcikk) Gulyás, Attila [Gulyás, Attila (hadtudomány), szerző] Biztonságtudományi Doktori Iskola (ÓE) The Role of the Civilian Joint Task Force in the Improvement of Security in Borno State, Nigeria 2021 Teljes dokumentum: https://jceeas.bdi.uni-obuda.hu/index.php/jceeas/article/view/28/30

N13. 32790776 Folyóiratcikk Recenzió/kritika (Folyóiratcikk) Gulyás, Attila [Gulyás, Attila (hadtudomány), szerző] Biztonságtudományi Doktori Iskola (ÓE) A Review of: "Bitskrieg: The New Challenge of Cyberwarfare"by John Arquilla 2021

N14. 33664490 Folyóiratcikk Szakcikk (Folyóiratcikk) Gulyás, Attila [Gulyás, Attila (hadtudomány), szerző] Biztonságtudományi Doktori Iskola (ÓE) KIBERHADVISELÉS ÉSZAK-KOREAI MÓDRA I. 2017

N15. 33664491 Folyóiratcikk Szakcikk (Folyóiratcikk) Gulyás, Attila [Gulyás, Attila (hadtudomány), szerző] Biztonságtudományi Doktori Iskola (ÓE) KIBERHADVISELÉS ÉSZAK-KOREAI MÓDRA I. 2017

N16. 33664530 Folyóiratcikk Szakcikk (Folyóiratcikk) Gulyás, Attila [Gulyás, Attila (hadtudomány), szerző] Biztonságtudományi Doktori Iskola (ÓE) Kína informatikai hadviseléséről 2015

N17. 33664508 Folyóiratcikk Szakcikk (Folyóiratcikk) Gulyás, Attila [Gulyás, Attila (hadtudomány), szerző] Biztonságtudományi Doktori Iskola (ÓE) Árulód lehet a nyomtatód 2009

N18. 33664524 Folyóiratcikk Szakcikk (Folyóiratcikk) Gulyás, Attila [Gulyás, Attila (hadtudomány), szerző] Biztonságtudományi Doktori Iskola (ÓE) Amit a Google Chrome -ról tudni érdemes 2009

N19. 33666874 Folyóiratcikk Összefoglaló cikk (Folyóiratcikk) Besenyő, János [Besenyő, János (Történelemtudomány), szerző] Bánki Donát Gépész és Biztonságtechnikai Mérnök. (ÓE);Barten, Dennis G.;De Cauwer, Harald G.;Tin, Derrick;Gulyás, Attila [Gulyás, Attila (hadtudomány), szerző] Biztonságtudományi Doktori Iskola (ÓE) A Review of Ambulance Terrorism on the African Continent 2023 DOI:10.1017/S1049023X23000213;WoS:000940261800001; Scopus: 85150665947;Egyéb URL: https://www.cambridge.org/core/product/identifier/S1049023X23000213/type/journal_article10