*Ródler Norbert*

# TERRORIZMUS A KIBERTÉRBEN

## BEVEZETÉS

A történelmi tényt, hogy az ipari forradalmak mindig gyökeres változást hoztak az ipar 4.0 korában, saját magunk is megtapasztalhatjuk. Ugyanakkor természetesen ezek a forradalmak nemcsak a termelést érintették, hanem megváltoztatták az élet minden területét. Amellett, hogy a technológia fejlődése jelentősen megkönnyítette életünket, annak vívmányait ártó céllal ugyancsak fel lehet használni. Bár a terroristák mindig is törekedtek arra, hogy a legújabb technológiát alkalmazzák a pusztítás maximalizálására vagy pusztán tevékenységük konspirálására, a közvélemény számára az Iszlám Állam tevékenysége mutatta meg igazán a terrorizmus jelenlétét a kibertérben. A terrorista online tartalmak napi problémát okoznak nemcsak az ellenük küzdő szolgálatoknak és államoknak, de az IT-szolgáltatóknak egyaránt. Ahogy azt majd a későbbiekben kifejtem, a többségi vélemény szerint kiber-terrorcselekmény még nem valósult meg, ugyanakkor arra is rá kívánok világítani, hogy mindez csak értelmezés kérdése, és bármelyik pillanatban megvalósulhat egy olyan terrortámadás is, amelynek kiber mivoltát már senki sem fogja vitatni.

## FOGALMAK

Ahhoz, hogy érdemben vizsgáljuk a problémát, szükséges lenne meghatározni a kiberterrorizmus jelentését, amelyhez alapvetően annak fő elemein, a terrorizmus és a kibertér meghatározásán keresztül juthatunk el. Rövid kutatás, néhány tucat könyv és tanulmány elolvasása után azonban bárki ráébredhet arra, hogy pusztán a definíciók meghatározása, akár egyenként is, terjedelmes művek témája lehetne. Jelen tanulmányban – tekintve, hogy a kötet szerzői több ponton érintik – az összetett szó második elemével, a terrorizmus definíciójával nem kívánok részletesen foglalkozni, ugyanakkor a további gondolkodás megkönnyítése érdekében szeretném kiemelni a fogalommeghatározások legfontosabb közös elemeit, a politikai, ideológiai célt,



DOI: https://doi.org/10.36250/01259_15

és az attól elkülönülő erőszakos eszköz(bűn)cselekményt, amelynek sértettje nincs feltétlenül közvetlen kapcsolatban az általános céllal.

### *Kibertér*

Sajnos a kibertér tudományos fogalmának meghatározásakor sincs könnyebb dolgunk, mint amikor a terrorizmus egységesen elfogadott fogalmát keressük. Egy több tudományterületet érintő, egységes definíciót kellene megtalálni, hisz a matematika, informatika, fizika és egyéb mérnöki szaktudományok mellett a szociológia, a társadalomföldrajz, és negyedik vagy ötödik műveleti térként a hadtudomány is mélyrehatóan foglalkozik ezzel az új dimenzióval, amelyet az információk digitális tárolásának, továbbításának, feldolgozásának lehetősége nyitott meg számunkra.

A fogalom eredetét kutatók egyetértenek abban, hogy a görög kormányos (kübernétész) szóból származó kibernetika fogalom Norbert Wiener 1948-ban megjelent *Kibernetika*[1] című művében szerepelt először, míg a kibertér fogalmat William Gibson sci-fi író *Neurománc*[2] című regényében használta a valós világgal (metaspace) párhuzamosan létező környezetre. Aztán ha túllépünk a szavak eredetének keresésén, már egy sokkal differenciáltabb gondolkodással szembesülünk. A különböző szerzők kibertérfogalmainak tanulmányozása alapján helytállók Fang Binxing kibertér-szuverenitással foglalkozó művének[3] azon megállapításai, amelyek szerint a kibertér fogalma négy elem (1. információs és kommunikációs infrastruktúrák, 2. adatok, 3. felhasználók, 4. műveletek) ötféle kombinációjából tevődhet össze annak függvényében, hogy az egyes részelemeket az aktuális szerző a kibertér alapvető elemének tekinti-e.

Magyarország Nemzeti Kiberbiztonsági Stratégiája[4] szerint a kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint az ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti.

Nem kívánok állást foglalni a különböző definíciómegközelítések kapcsán, pusztán rávilágítanék arra, hogy bár a magyar stratégia látszólag csak a rendszert és az adatokat említi, de tekintve, hogy az adatokban, információkban manifesztálódó társadalmi és gazdasági folyamatoknak szükséges része az ember (felhasználó) és

[1] Wiener 1968.
[2] Gibson 1992.
[3] Fang 2018.
[4] 1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról.

a művelet is, amely a folyamatot elindítja, befolyásolja, így a kibertér mindenképpen többet kell hogy jelentsen az informatikai hálózatoknál és adatoknál.

## *Kiberterrorizmus*

Amikor a kiberterrorizmus meghatározását keressük, a két alapszóból kiindulva minimálisan az információs és kommunikációs infrastruktúrákon keresztül adatok, információk felhasználásával megvalósuló cselekményről kell beszélnünk, amely a terrorizmus ismérveit is magán hordozza.

Tekintve azonban, hogy a terrorizmus nem egy egyértelmű kategória, ezért annak kibertérben megvalósuló változata is rendkívül összetett kérdéseket vet fel. Ha a terrorizmus fogalmát nem szűkítjük annak büntetőjogi, konkrét támadás megvalósítására vonatkozó értelmezésre, hanem annak tágabb politikai, nemzetközi jogi dimenzióját vizsgáljuk, a kibertér eszköztára felhasználható a terrorizmus általános politikai, ideológiai céljának megvalósítása érdekében propagandára, tagok toborzására, azok radikalizálására, a szervezet kommunikációs, önfinanszírozási céljaira, művelet-előkészítésre stb. Ezt a kettősséget Kovács László *Az információs terrorizmus eszköztára*[5] című művében az információs rendszerek terroristák általi alkalmazásának *hard* és *soft* (kemény és lágy) felhasználásaként különbözteti meg. Jómagam a kiberterrorizmus kategóriáján belül az úgynevezett soft típusú eszközök terrorista célú felhasználását az információs műveletek fogalmából[6] kiindulva információs terrorizmusnak, míg a hard, azaz a konkrét támadó felhasználást pedig kiber-terrorcselekménynek nevezném.

Ha egyébiránt szűken egy támadás vagy támadások kivitelezését értjük a kiberterrorizmus alatt, akkor sem teljesen egyértelmű, hogy a fogalom mit takar. A kontinentális jogban, különösképpen az EU tagállamaiban, figyelemmel Az Európai Parlament és a Tanács (EU) 2017/541 irányelvére (2017. március 15.) a terrorizmus elleni küzdelemről, a 2002/475/IB tanácsi kerethatározat felváltásáról, valamint a 2005/671/IB tanácsi határozat módosításáról eredményeként az úgynevezett eszközcselekmény megvalósítható számítógépes bűncselekmények útján is, így például Magyarországon az információs rendszer felhasználásával elkövetett csalás

[5] Kovács 2006.

[6] „Az információs műveletek a döntéshozókat befolyásoló, politikai és katonai célkitűzések megvalósítását támogató tevékenységek, amelyek más felek információi, információs folyamatai, vezetési (C2), híradó és informatikai (CIS) rendszerei befolyásolására, ugyanakkor a saját információk és információs rendszerek felhasználására és védelmére irányulnak." NATO 2001.

[375. § (2)–(4) bekezdés], az információs rendszer vagy adat megsértése [423. § (1)–(4) bekezdés] elkövetésével a tényállásban meghatározott célzattal.

Az angolszász területeken ugyanakkor általánosabb fogalom, a kiberterrorizmus a kiberrendszerek elleni erőszak, zavarás vagy működésébe történő beavatkozás, vagy ezzel való fenyegetés, amikor valószínűsíthető, hogy ennek eredménye halál vagy sérülés, vagyontárgy súlyos károsodása, vagy a társadalmi rend megzavarása.[7] E harmadik kategória talán a legszűkebb kiberterrorizmus-fogalom, amely azt a szcenáriót foglalja magába, amelyben a jogellenes kibertertevékenység váltja ki a fizikai erőszakot a személyek vagy kiemelt vagyontárgyak ellen.

A következőkben e három kategóriával, az információs terrorizmussal és a kiberterrorcselekmény két típusával, azaz a jogi tényállás szerinti tágabb, és az angolszász definíció szerinti szűkebb értelmezésével külön foglalkozom.

## INFORMÁCIÓS TERRORIZMUS

A terrorizmusnak lényegi eleme az ideológia, eszme, vagy egyszerűen egy „ügy", amelynek mentén kitűzött cél elérése érdekében követik el a támadást, támadásokat. Az ideológiai háttér terjesztése, a szimpatizánsok megnyerése, az ellenség elrettentése, a tevékenységek összehangolása kommunikációt és az információk célzott, a tevékenység tiltott mivoltára figyelemmel konspirált használatát igényli.

### *Az információs terrorizmus eszköztára*

#### Propaganda, toborzás, radikalizáció

A világháló felhasználása a terrorizmus, terroristák szempontjából a háttérideológia és az abból következő politikai, társadalmi cél terjesztésének legfontosabb eszközévé vált. Az online média háttérbe tudta szorítani a nyomtatott sajtó mellett a rádiót és a televíziót is, és ez az eszköz most bárkinek – így a terroristáknak is – a rendelkezésére áll multimédiás kommunikáció formájában ideológiai vagy gyakorlati útmutatás, magyarázat, igazolás közzétételére. Az eszközök tárháza végtelen: virtuális üzenetek, prezentációk, online hírügynökségek, magazinok, hitéleti vagy tudományosnak tűnő értekezések, audió- és videófájlok, videójátékok. Mindazonáltal az, hogy mi minősül terrorista propagandának, gyakran szubjektív értékelés

[7] Gillespie 2016.

arra is figyelemmel, hogy generálisan a propaganda terjesztése önmagában nem tiltott tevékenység. A nemzetközi jog egyik alaptétele az alapvető emberi jogok védelme, amely magában foglalja a véleménynyilvánítás szabadságához való jogot. Ez bizonyos kivételektől eltekintve garantálja az egyén számára a vélemény megosztásának vagy a mások által kifogásolhatónak tartott tartalom terjesztésének jogát is. Természetesen, mint ahogyan az emberi jogok többsége sem korlátlan és határtalan, a véleménynyilvánítás szabadságára való hivatkozás sem vezethet más ember alapvető jogának jelentős sérelmével járó cselekedethez. Így a véleménynyilvánítás szabadságának is megvannak a maga korlátai, amelyeket a nemzetek törvényeikben fogalmaznak meg. Ezen törvények védenek bizonyos kiszolgáltatott csoportokat azáltal, hogy tiltják a szexuális jellegű tartalom bizonyos kategóriáinak terjesztését, vagy a társadalom védelme érdekében korlátozzák az erőszakos vagy erőszakra felbujtó, vagy az államok nemzetbiztonságát súlyosan sértő tartalmakat. A fenti példák közül az erőszak népszerűsítése, legitimálása a terrorista propaganda egyik legfontosabb témája.

Az interneten keresztül terjesztett tartalom széles körű elérhetősége exponenciálisan növeli a propaganda közönségét, amire kiváló bizonyíték az Iszlám Állam „népszerűsége" és követőinek száma akár az al-Káidához viszonyítva is, amely leginkább az online felületek szisztematikus használatából eredt. A tartalmak közvetlen közzététele (feltöltése) pedig a hagyományos hírszolgáltatások olyan funkcióit zárja ki, mint az információk hitelességének független értékelése vagy a jogellenes tartalmak cenzúrázása. Az erőszakos cselekedetekre ösztönző szélsőséges retorikát, tartalmakat korábban viszonylag korlátozott közönségnek terjeszthették személyesen vagy fizikai adathordozókon, míg ma már az internetre feltöltve határtalan számú a célközönség. Az ilyen tartalmak az eszközök széles skálájával terjeszthetők, például célzott weboldalakon, dedikáltan létrehozott csevegőszobákban és fórumokon, online magazinok, közösségi hálózati platformok, például Twitter és Facebook, Telegram stb. formájában, valamint népszerű videó- és fájlmegosztó webhelyek útján. Az internetes keresőmotorok használata pedig megkönnyítette a téma iránt érdeklődőknek a terrorizmussal kapcsolatos tartalmak azonosítását és visszakeresését. Az internet közössége kimeríthetetlen bázist jelent a terrorista szervezeteknek potenciális tagok toborzására is. A propagandával gyakran a társadalom kiszolgáltatott és marginalizált csoportjait célozzák meg. A toborzás és a radikalizálódás folyamatában általában kihasználják a vélt vagy valós igazságtalanságokból, kirekesztettségből vagy megaláztatásból származó érzéseket.[8] A toborzás, a radikalizáció és a terrorizmusra való buzdítás egy jól megtervezett

[8] European Commission's Expert Group on Violent Radicalisation 2008.

folyamat. A radikalizálódás elsősorban a szélsőséges tanok tudatosítási folyamata, amely oda vezet, hogy az újonnan toborzott elfogadja az erőszak szükségességét, és leküzdi magában az erőszakkal szembeni gátlásokat.

Természetesen a propaganda célközönsége nemcsak a potenciális szimpatizánsok tábora, az szólhat a terrorcselekmények célpontjainak, vagy az ellenérdekelt szervezeteknek, társadalmaknak, politikai csoportoknak és a nemzetközi közösségnek is. Ugyanis a terrorista propaganda egyéb célkitűzései között szerepelhet a pszichológiai manipuláció alkalmazása az egyének kollektív társadalmi értékekbe, biztonságba vetett hitének aláásása érdekében, vagy a félelem és a pánik terjesztése.

## Finanszírozás

A terrorista tevékenység annak formájától, a szervezet vagy csoport méretétől függően eltérő finanszírozási szükségleteket igényel. Az elmúlt időszak hidegfegyverrel, gépjárművel, elsősorban magányos elkövető által végrehajtott támadásai nem igényelnek hatalmas forrásokat, így azok elkövetői nem kellett hogy komolyabb finanszírozási háttérműveleteket hajtsanak végre, forrásaikat legális jövedelemből vagy kisebb bűncselekményekből előteremthették. Azonban nagyobb szervezeteknek – legyenek azok tradicionális iszlám terrorszervezetek vagy szélsőjobboldali ideológiát követő, nagy létszámú nemzetközi csoportok – működésük finanszírozásához nagyobb összegeket kell előteremteniük, illetve mozgatniuk világszerte. Az ilyen nagyobb szervezetek a szükséges pénzösszegeket elsősorban adományokból, támogatásból, illetve bűncselekményekből tudták, tudják előteremteni, illetőleg preferálják a nem nyomon követhető készpénzes pénzmozgatást futárokon vagy hawalahálózatokon keresztül. Azonban az informatika fejlődése mindhárom területen új lehetőségeket nyitott számukra, amelyekkel élnek, visszaélnek.

A jótékonysági szervezetek és a nem kormányzati szervezetek folyamatosan komoly problémát jelentenek a terrorizmus finanszírozásában. A párizsi székhelyű Pénzügyi Akció Munkacsoport (FATF) már 2002-es jelentésében[9] szerepeltette, hogy „a nonprofit szervezetekkel a terrorizmus finanszírozása érdekében való visszaélést a globális küzdelem kulcsfontosságú gyenge pontjaként ismerik el az ilyen finanszírozás forrásnál történő leállítása érdekében", és természetesen azok internetes tevékenysége sem kivétel ez alól a problémás tendencia alól. Egyes jótékonysági szervezeteket létrehozhatnak kifejezetten a terrorizmus finanszírozásának céljával, míg lehetséges ilyen legális szervezetek terrorista célú kihasználása is, ugyanis komoly

[9] Financial Action Task Force 2002.

kihívás nemcsak a nonprofit szervezeteknek, de a professzionális bűnüldöző és hírszerző szolgálatoknak is hatékonyan nyomon követni a konfliktusövezetekben elosztott pénzeszközöket. A terrorizmus finanszírozására álcázottan létrehozott szervezetek jól felépített honlapjaival olyan személyek is a terrorizmus finanszírozójává válhatnak, akik pusztán segítséget szerettek volna nyújtani a bajbajutottaknak. Ugyanakkor az adománygyűjtés megvalósulhat oly módon is az interneten, hogy nem titkolt cél az adományok terrorista célra történő felhasználása. Természetesen ezekben az esetekben preferálják a kriptovaluták használatát a konspiráció fokozása érdekében.

2020. augusztus 13-án az Egyesült Államok igazságügy-minisztériuma három online terrorfinanszírozással kapcsolatos bűncselekmény felderítéséről számolt be.[10] Az egyik kiberalapú terrorfinanszírozási kampányt az al-Káida és a vele szövetséges terrorista csoportok üzemeltették. A szervezetek egy bitcoin pénzmosási hálózatot működtettek a Telegram-csatornák és más közösségimédia-platformok segítségével, hogy kriptovaluta-adományokat kérjenek terrorista céljaik elősegítése érdekében. Bizonyos esetekben jótékonysági szervezetként tüntették fel magukat, miközben valójában kifejezetten forrásokat kértek erőszakos támadásokhoz.

De természetesen ez a típusú adománygyűjtés nemcsak az iszlamista szervezetekre jellemző, hanem más szélsőséges szervezetek is alkalmazzák Európában. Példaként említhető például a Nordic Resistance Movement, amely ugyancsak bitcoin formájában való támogatásra buzdította tagjait.[11]

A kiberbűncselekmény útján történő finanszírozásra is természetesen rengeteg példát lehetne hozni. A marokkói származású brit állampolgár, Younis Tsouli például a dark weben megvásárolt hitelkártyaadatok felhasználásával finanszírozta az al-Káida érdekében kifejtett online propagandáját.[12]

Végül, de nem utolsósorban a kriptovaluták egy új, gyors lehetőséget kínálnak nemcsak a szervezett bűnözői csoportok, de a terroristák számára is a pénzeszközök mozgatására, elrejtésére.

[10] U.S. Department of Justice 2020.
[11] Europol 2020.
[12] Corera 2008.

## Művelet-előkészítés, hírszerzés, kommunikáció

Napjainkban reálisan legalább 60-70% az online elérhető információk, ezáltal az OSINT jelentősége a hírszerzésben.[13] A kibertér azonban nemcsak a szolgálatok hírigényeit képes kiszolgálni, hanem hasonlóan a terroristák, terrorszervezetek részére is az információk kimeríthetetlen tárházául szolgál. Ha az elmúlt időszak támadásait megvizsgáljuk, nagy számban találunk köztük olyat, amelyet az adódó alkalmat kihasználva hajtott végre az elkövető, ugyanakkor rengeteg olyat is, amely információkat, előkészületeket igényelt, amelyhez a világháló rengeteg segítséget tudott nyújtani. A célpont kiválasztásától kezdve az arról való információgyűjtésen, a szükséges kommunikáción, az eszközkiválasztáson, annak beszerzésén, elkészítésén keresztül akár a külön fejezetben tárgyalt támadásig az internet mindenben segítséget nyújthat.

2020 egyik legnagyobb visszhangot keltő támadása a 47 éves franciaországi tanár, Samuel Paty lefejezése volt. A nyomozás során nyilvánosságra hozott adatok alapján is egyértelműen kijelenthető, hogy a gyilkossághoz vezető utat a tanár elleni szociálismédia-kampány kövezte ki. Egyértelműen az interneten jelentették meg az információt a támadást kiváltó tanóráról, amelyen a Mohamed-karikatúrákat bemutatta a tanár, illetve ott alakult ki az a gyűlöletkampány – amelyben többek között egy radikális imám is részt vett –, amely a csecsen származású Abdullakh Anzorov számára a triggert jelentette. Továbbá segítséget jelentett számára a világháló a tanár azonosításában is. A tett fizikai végrehajtója mellett több mint tíz fő ellen folyt eljárás, akik többsége „csak" az online térben követett el bűncselekményt. Úgy gondolom, hogy tettüket nyugodt szívvel minősíthetjük kiberterrorizmusnak, hisz mindenképpen hozzájárultak a végeredményhez, az erőszakhoz.

Az online elérhető műholdas felvételek, utcaképek, a közösségi hálózatokon közzétett információk maximális támogatást nyújtanak a célpont teljes körű feltérképezéséhez. Ezek az információk aztán megalapozhatják a támadáshoz használt eszköz kiválasztását is, amelyhez ugyancsak segítséget nyújtanak az online információk is. Bizonyosan kijelenthető, hogy egy támadásról közzétett videófelvétel komoly hatásokat tud kiváltani. A christchurchi támadás egyértelműen mintaként szolgált a hallei terrorcselekményhez, a 2016-os berlini karácsonyi vásár elleni teherautóval

[13] A becslések rendkívül differenciáltak attól is függően, hogy mit értünk az OSINT és a nyílt információ fogalma alatt. A modern digitális OSINT-eszközök, -technológiák ugyanis ötvözik több hírszerzési ág elemeit, és hozzáférést biztosítanak nemcsak a szó szűkebb értelmében nyílt, hanem a tulajdonos által nem nyíltnak szánt információkhoz is. A különböző szerzők, szervezetek az OSINT hírszerzésben betöltött jelentőségét 60-70%-tól akár 95-98%-ig becsülik (lásd például: Ünver 2018 vagy Gibson 2014).

elkövetett támadást pedig bizonyosan inspirálta a fél évvel korábbi, júliusi nizzai cselekmény. A know-how és az alapanyagok beszerzése, valamint a kibertér közötti kapcsolat demonstrálására magyar példát is meg tudunk említeni. A jogerősen többek között terrorcselekmény előkészülete miatt is elítélt P. László, a 2016-os Teréz körúti robbantás elkövetője ugyancsak az interneten talált információk alapján, az interneten megrendelt eszközök felhasználásával készítette el távirányítással működésbe hozható robbanószerkezetét. Egyértelműen megállapítható, hogy rövid keresés után részletes információk találhatók házi készítésű robbanóeszközök elkészítéséről, alapanyagairól, de akár „szofisztikáltabb" kémiai, biológiai támadás eszközeinek megalkotásához is.

Elvétve lehet olyan terrortámadást találni, amelyben az elektronikus kommunikációnak ne lett volna valamilyen szerepe. Nemcsak a bűnözők, de a terrorszervezetek is amellett, hogy lehetőséget láttak a különböző elektronikus kommunikációs csatornákban, azokat egyúttal fenntartásokkal is kezelték. Az 1990-es években Bin Láden állítólag abbahagyta műholdas telefonjának használatát, miután egy médiajelentésből kiderült, hogy az amerikai kormány ezen keresztül kísérelte meg nyomon követni. Ehelyett Bin Láden belső köre nagyban támaszkodott a futárokra – akik közül az egyik ironikus módon végül az Egyesült Államok szolgálatait elvezette pakisztáni rejtekhelyére.

Amellett, hogy a terrorszervezetek, bűnözők félelmeit igazolta Edward Snowdennek, a Nemzetbiztonsági Ügynökség (National Security Agency – NSA) alkalmazottjának 2013-as kiszivárogtatása, az esemény új távlatokat is nyitott mindenkinek, akinek a továbbított információk bizalmassága fontos volt. A nyilvánosság megdöbbent, amikor megtudta, hogy az Egyesült Államok kormánya milyen mélységben fér hozzá kommunikációs adatokhoz, illetve a technológiai vállalatok rendszereihez, ugyanakkor az érintett vállalatok is komoly bizalomvesztéssel szembesültek a gyanú miatt, miszerint bűnrészesek voltak a kormányzati felügyeletben. A szektor vállalkozásai erre reagálva gyorsan fejleszteni kezdtek, hogy bizonyítsák függetlenségüket a kormányoktól, és megnyugtassák a felhasználókat, hogy adataik titkosak. Ilyen válasz volt az erős titkosítás kiterjesztése, amelyet a Google, majd az Apple is bevezetett a termékein oly módon, hogy a kulcsot a felhasználó birtokolta, a felhasználó jelentette, ezért az eszközökön tárolt adatokhoz annak gyártója sem fért hozzá. Az Apple iMessage és a népszerű WhatsApp üzenetküldő szolgáltatás „végpontok közötti" (end-to-end) titkosítást vezetett be, ami azt jelenti, hogy az üzenet titkosítatlan szövege csak a küldő és a fogadó számára látható, az a kommunikációs csatornán elfogva nem visszafejthető még a szolgáltató számára sem. Természetesen további szolgáltatók is megpróbálták kihasználni a nagyok hírnevén esett csorbát, és kielégíteni a felhasználók levéltitok és privát szféra iránti igényét, így egymás után

jelentek meg és terjedtek ugrásszerűen további titkosított üzenetküldő alkalmazások, mint például a Viber, a Telegram vagy a Signal. A Snowden-botrány tanulságai, illetve az általa gerjesztett fejlődés a titkosított kommunikációban a bűnözőket és a terroristákat is ezekhez az új biztonságos platformokhoz vezették, amelyek közül hosszú ideig a Telegram volt a legnépszerűbb, tekintve, hogy az titkosított üzenetküldést kínált célzott címzettnek és csoportokban, ezáltal kiszolgálta a kommunikációs igény mellett a propagandacélokat is. A titkosított üzenetküldés lehetőségének az elmúlt években kiemelkedő szerepe volt számos nagy horderejű támadásban. A 2015–2016-os franciaországi és brüsszeli támadások elkövetőinek összehangolt tevékenységében azok Európába jutásától, a rejtőzködésen és a logisztikán keresztül egészen a végzetes támadásokig, sőt az azt követő bujkálásig hatalmas szerepe volt a különböző platformok által nyújtott titkosított kommunikációnak, amelynek részleteit sajnálatos módon a hatóságok még a támadásokat követően lefoglalt eszközökből sem tudták maradéktalanul megismerni.

Amellett, hogy a titkosítás fontos eszköz a kiberbiztonság és az alapvető jogok, így a magánélet és személyes adatok védelme szempontjából, az elkövetők azt biztonságos csatornaként is használhatják, amelyen keresztül elrejthetik cselekedeteiket a bűnüldöző szervek és az igazságszolgáltatás elől. Mivel annak alkalmazása könnyen és gyakran ingyenesen hozzáférhetővé vált, így a bűnözők, terroristák igénybe vehetik e jogvédelmi célokra kidolgozott eszközt. Ez természetesen kihívást jelent a nemzetbiztonsági, bűnüldöző és az igazságszolgáltatási szervek számára, mivel szinte minden bűncselekmény vagy nemzetbiztonságot sértő esemény kapcsán szükséges lehet ilyen kommunikációs adatokhoz való hozzáférés. A téma globális aktualitását mutatja, hogy az Öt Szem Szövetség[14] országai 2019 júliusában nyílt levélben hívták fel a közösségi üzenetküldő szolgáltatásokat működtető vállalatokat, hogy biztosítsák a bűnüldöző hatóságok hozzáférését az end-to-end titkosítási technológiával védett online kommunikációhoz, illetve 2020 második félévében az EU tanácsának német elnöksége is kifejezte a 2016-os szlovák elnökség által megkezdett, a titkosítással kapcsolatos munka folytatása iránti szándékát, és 2020 végére össze is állt a titkosítással kapcsolatos tanácsi állásfoglalás tervezete,[15] amely elismeri a titkosítás kettős jellegét, és megoldási javaslatokat keres azok egyensúlyba hozására. Rögzíti, hogy a titkosítási technikák alkalmazása egyrészről szükséges a kormányok, vállalatok, kritikus infrastruktúrák, állampolgárok, a média és az újságírók digitális biztonságához, valamint az alapjogok, magánélet és személyes adatok védelméhez, ugyanakkor meg kell őrizni a nemzetbiztonsági, bűnüldöző és igazságügyi hatóságok

[14] Ausztráliát, Kanadát, Új-Zélandot, az Egyesült Királyságot és az Egyesült Államokat magába foglaló hírszerző szövetség.

[15] Council of The European Union 2020.

képességét, ami a törvények által garantált hatáskörük gyakorlásához és az adatok bűnüldözési célú megismeréséhez szükséges. Az állásfoglalás legfontosabb megállapítása, hogy a törvényesség, a szükségesség és az arányosság elvére épülő szabályozási kereten nyugvó műszaki és operatív megoldásokat a szolgáltatókkal és a releváns illetékes hatóságokkal szoros együttműködésben kell kidolgozni.

### *Iszlám Állam / Kiberkalifátus*

Amellett, hogy az Iszlám Állam (IS/ISIS/Daesh)[16] is alkalmazta a korábban tárgyalt online lehetőségeket, tevékenysége mégis alapvetően különbözött az egyéb terrorszervezetek aktivitásától mind szervezettségében, mind intenzitásában. Az alapvető különbség talán az IS pszeudoállamként való működéséből adódhatott. Míg a legtöbb iszlamista terrorszervezet naptárában a nyugati hatalmak felett aratott végső győzelmet követően szerepelt a közel-keleti iszlám kalifátus megalapítása, addig az IS ezt a kezdet kezdetén megtette az általa uralt területen. Míg a többi szervezet kvázi felkelőként illegalitásban működött, addig az IS minisztériumokat alapított és közigazgatást szervezett, hogy biztosítsa hatalmát. Az államiság elérése érdekében ugyancsak használnia kellett az ún. *soft power*[17] eszköztárát annak érdekében, hogy megszólítsa híveit, és egyben félelmet keltsen ellenségeiben. Céljait nem érhette volna el, és meg sem közelíthette volna ennyire a kifinomult médiainfrastruktúrája és online kommunikációs stratégiája nélkül, amelynek eredménye a szervezet és tettei példátlan láthatósága lett. A terrorszervezetek között elsőként tudott kínálni egyszerre online és offline alternatívát azoknak, akik nem találták a helyüket saját közösségükben. Sikeresen toborozta az új harcosokat a konfliktusövezetbe, illetve radikalizálta és buzdította támadásra az „otthon" maradottakat online csatornákon keresztül. 2017 után, amikor mind online, mind offline fokozatosan a háttérbe kellett vonulnia, rugalmasan változtatta meg mind kommunikációs, mind harcászati taktikáját. Miután fel kellett adnia a jól strukturált online információs rendszert, a széles támogatói hátterére hagyatkozva maradt látható és hallható továbbra is

[16] Islamic State (IS): Iszlám Állam; Islamic State of Iraq and Syria (ISIS): Iraki és Szíriai Iszlám Állam; al-Dawla al-Islamiya fi al-Iraq wa al-Sham (Daesh): Iraki és Levantei Iszlám Állam.

[17] „A puha hatalom azon képesség, hogy kényszer vagy kifizetések helyett inkább a vonzódás kialakításával érjük el céljainkat. Amikor rábírsz másokat arra, hogy azt akarják, amit magad is akarsz, nem kell annyit költened jutalmakra és büntetésekre annak érdekében, hogy mások irányodba elmozduljanak. A kemény hatalom egy ország katonai és gazdasági erejéből fakadó kényszerítő ereje. A puha hatalom egy ország kultúrája, politikai eszméi és stratégiáiból fakadó vonzó mivolta." Joseph S. Nye.

a kibertérben. Saját weboldalak hálózata helyett elsősorban a titkosított üzenetküldő alkalmazásokra és fájlmegosztó szolgáltatásokra hagyatkozva, szükség esetén egyikről a másikra vándorolva továbbra is képes megszólítani híveit.

Mindezen eredményeket egy rendkívül szerteágazó médiabirodalom érte el, amely a százas nagyságrendű általános és tartományi szintű hírügynökség, online híroldal, magazin mellett saját rádiócsatornát is felölelt. Ebből a szerteágazó birodalomból ki kell emelni néhány jelentős vállalkozást.

Az Amaq hírügynökség és tevékenysége állt a pszeudoállamiság éveiben a médiastratégia középpontjában. Amennyiben a terrorszervezet által alapított állam elismerésre került volna, annak kommunikációs tevékenységét egyértelműen információs műveletnek lehetett volna minősíteni. A hírügynökség tevékenységén keresztül motiválta a követőket, újabb és újabb támadásra buzdította őket, igazolta tevékenységük szükségességét, dicsőítette a mártírokat, lejáratta az ellenséget, és tette ezt oly módon, hogy híreit, közleményeit ellátta az ügynökség logójával, amelyet sokszor a nyugati hírügynökségek is változtatás nélkül közöltek, erősítve a hírügynökség és a hírek hitelességét. Elsődleges eszközévé vált a támadások iránti felelősség elismerésének is. Fenntartotta és üzemeltette az IS weboldalait, híreit hat nyelven közvetítette, és saját mobilapplikációval is támogatta a legszélesebb hallgatóság elérését. Az IS online eszköztára elleni összehangolt 2018-as akcióig meghatározó szereplője volt a terrorista ideológia terjesztésének.[18]

A Nashir hírügynökség ellentétben az Amaqkal nem próbált klasszikus legális hírügynökségként működni, nem készített saját tartalmakat, illetve a híreket nem kommentálta, hanem inkább egyfajta gyűjtőhelye lett az IS publikációknak, és jelentősége a hírek hatékony, széles körű terjesztésében manifesztálódott, amely által a dzsihádista online szubkultúra meghatározó elemévé vált. 2017-ben és 2018-ban saját weboldalt is üzemeltetett, amely nemcsak közzétette a legfrissebb híreket, de egyfajta IS-tárhelyként elérhetővé tette az al-Naba magazin példányait visszamenőleg, illetőleg hozzáférést biztosított al-Hayat-tartalmakhoz és az al-Bayan rádió műsoraihoz is. Ugyancsak a Nashir volt, amelynek webinfrastruktúráján keresztül minden héten csütörtökön hatalmas közönséghez juthatott el az al-Naba magazin legfrissebb száma.

A 2018-as nemzetközi akcióig az IS egy rendkívül összetett online infrastruktúrára hagyatkozhatott, azonban azt követően elsősorban a különböző üzenetküldő alkalmazások és fájlmegosztó szolgáltatások maradtak a bástyái, és miután a Twitter és egyéb mainstream szolgáltatások felléptek a terrorista tartalmak ellen, ezek közül kiemelkedett a Telegram, amelyet természetesen nemcsak ekkor kezdtek el

[18] Europol 2018.

alkalmazni. A Nashir ügynökség 2015. szeptember 26-án, mindösszesen négy nappal azt követően megjelent a felületen, hogy a Telegram elindította a csatorna (channel) szolgáltatását,[19] és 2017 novemberében az ügynökség azt állította, hogy több mint 600 csatornát, csoportot üzemeltet.[20] Természetesen a Telegram nem biztosíthatott olyan láthatóságot, mint a Twitter, ugyanakkor az általa nyújtott anonimitás és stabilitás rengeteget jelentett a szervezetnek. A legnagyobb hangsúly talán az anonimitáson volt, hisz a Telegram többször hangsúlyozta, hogy a felhasználók jogainak védelme érdekében nem működik együtt a hatóságokkal, továbbá a platformon továbbított közlemények nem visszafejthetők. Külön előnyt jelentett a szervezet számára, hogy lehetőséget biztosított arra is, hogy nagy méretű fájlok (fotók, videók) kerüljenek feltöltésre a csatornákra, ezáltal, ha esetlegesen a továbbküldött link mögötti tartalom elérhetetlenné válik, a követők azt továbbra is megtalálják az alkalmazásban. Előnyt és hátrányt jelentett a szervezet szempontjából a zárt kommunikációs tér, mivel a tartalmakat a keresőmotorok nem indexálták, emiatt nem lehetett ezeken keresztül elérni azokat, akik még nem kezdték el valamilyen mértékben követni a terrorista ideológiát. Ugyanakkor tökéletes menedéket jelentett az előkészületekhez, megbeszélésekhez, a radikalizáció elmélyítéséhez, akár a képzéshez is. Az egyirányú kommunikáció elsődleges eszközévé vált, az elhivatott követőket folyamatosan ellátta időszerű tartalmakkal, mi több, a követőknek a dzsihádista közösséghez való tartozás érzését is biztosította.

2019 novemberében aztán a Telegram biztosította menedék megszűnt, miután a szolgáltató együttműködött az európai hatóságokkal, és az Europol által koordinált akció keretében több mint 2000 terrorizmushoz köthető felhasználói fiók, illetve bot került törlésre.[21] Majd a szolgáltató következetesen napi szinten lépett fel a csatornák újraalkotása ellen. Természetesen minden erőfeszítés és automatizmus ellenére sem lesz egyetlen platform sem mentes minden terrorista tartalomtól, ugyanakkor az akciónapot megelőző méretű hálózatot a logók használata nélkül, duplikált fiókok létrehozásával sem sikerült újjáépíteni. Ehelyett egy multiplatform környezet alakult ki, amelyben az online aktivisták olyan felületeken próbálkoztak, mint a Riot, Rocket.Chat, Tam-Tam, Hoop, BCM vagy Nandbox.[22] Ebben az összetett, decentralizált világban azonban ez idáig nem sikerült újraalkotni egy olyan méretű és annyi embert elérő hálózatot, mint amely a 2018 előtti időszakban a weblapokon és a Telegramon párhuzamosan, egymást erősítve létezett. A hatóságok és a szolgáltatók részére pedig fontos tanulság, hogy automatizmusok beépítésével,

19 *IS exploits Telegram mobile app to spread propaganda*. 2015.

20 Al-Lami 2018.

21 Europol 2019; *Europol disrupts Islamic State propaganda machine* 2019.

22 Clifford 2020.

a különböző médiavállalkozások logóinak, brandelemeinek módszeres keresésével gyorsan azonosíthatók a tartalmak, azok törlésére szinte azonnal lehetőség van, illetve a márkaelemek hiányában pedig a tartalom közel sem olyan egyszerűen megtalálható, és megjelenésében sem váltja ki ugyanazt a hatást.

Példa azonban arra, hogy a propagandagépezet továbbra is aktív, és rendkívül gyorsan reagál, a Netflix *Moszul* című produkciójára megjelent gyors és nemzetközi visszhangot keltő IS-válasz. A filmet 2020. november 26-án mutatták be, és hatalmas nézettséget ért el a platformon. 2020. november 28-án, mindösszesen két nappal a premier után az ISIS a filmre válaszul közzétett egy videót, amely egyértelműen a terrorszervezet propagandaüzeneteit és elbeszélését tartalmazta. Még ha az anyag minősége kívánnivalót is hagy maga után, a megjelentetés gyorsasága és a közvetített üzenet azt sugallja, hogy a professzionális online propagandagépezet továbbra is eltökélten segíti a terrorszervezet céljainak elérését.

Végül mindenképpen szeretnék szót ejteni a propagandán és a kapcsolattartáson túlmenően az ISIS kiberműveleteiről, különös tekintettel a szervezet emblematikus hackeréről, Junaid Husszeinről – hackernevén TriCk, majd harci nevén Abu Husszein al-Britani –, aki kiberterroristaként került fel az Egyesült Államok körözési listájára, és végül 2015-ben egy célzott rakétatámadás végzett vele. Az emblematikus kiberterroristáról talán a legrészletesebb kutatást Nafees Hamid és kutatócsoportja készítette, amelynek eredményét a *CTC* (Combating Terrorism Center) *Sentinel*-ben tették közzé.[23] Az 1994-ben született Junaid Husszein, hasonlóan több európai terrortámadás elkövetőjéhez, második generációs európai (brit) állampolgár volt, akinek családja Pakisztánból származott. Korai gyermekkorát Birmingham bűnözéssel sújtott, szegényebb környékén töltötte, majd a továbbiakban a város egy kifejezetten élhető, jó környékén nevelkedett. Apja a brit pakisztáni közösség elismert, a közösség számára nyitott tagja volt, Junaid Husszeint ezzel ellentétben rendkívül zárkózottnak jellemezték, akivel csak a számára fontos témákról lehetett érdemben társalogni. Saját bevallása szerint 11 évesen indult meg az úton, hogy hackerré váljon, amikor bosszút akart állni azon, aki ellopta felhasználói fiókját egy online játékhoz. A kibertérben aztán kiteljesedett, ott társakra, barátokra lelt. Hackerkészségének fejlődésével a politikai témák iránt is növekedett az érdeklődése, amely során több összeesküvés-elmélet is megérintette, és a muszlimok jogainak védelme, az őket ért igazságtalanságok feltárása, megtorlása lett a célja. Mindezek ellenére érdekes módon a vallás nem igazán érdekelte. Az általa bűnösnek, korruptnak minősített szervezeteket kezdte el támadni, és ehhez hasonló gondolkodású hacktivisták csoportját hozta össze TeaMpoisoN néven. Hatalmas energiákat fektettek a brit szélsőjobboldali

[23] Hamid 2018.

csoportok oldalai elleni támadásokba, illetve az onnan megszerzett adatok nyilvánosságra hozásába. 2011-ben a TeaMpoisoN online közzétette Tony Blair volt brit miniszterelnök címjegyzékét, megtámadta a BlackBerryt, Horvátország NATO[24] weboldalát, egy ENSZ (Egyesült Nemzetek Szervezete) szervert, és még rengeteg további célpontot. A TeaMpoison egyik legelhíresültebb támadása 2012 áprilisában történt, amikor telefonos szolgáltatásmegtagadási támadást indítottak az Egyesült Királyság Terrorizmusellenes Parancsnokság forródrótja ellen. A támadás következtében az iroda telefonvonalait egy robothang bombázta, amely a „Team Poison" szót ismételte. Közvetlenül a támadások után TriCk név alatt közleményt adott ki, amelyben kifejtette, hogy tettét az motiválta, hogy az Egyesült Királyság terrorvád miatt kiadott több muszlimot az Egyesült Államoknak, amely pedig globális terror elleni háború címén valójában az iszlám ellen indított támadást. 2012 áprilisában aztán elfogták, és korábbi cselekményeiért – ügyvédjének köszönhetően – 2012. július 27-én csak összességében hat hónapos börtönbüntetésre ítélték, amelyből végül beszámítva az előzetes fogvatartást és a kedvezményeket, csak másfél hónapot töltött börtönben. Azonban feltehetőleg ez a másfél hónap volt az, ami gyökeresen megváltoztatta a rácsok mögött megismert radikális iszlamista csoportnak köszönhetően. Szabadulását követően látszólag felhagyott a hackertevékenységgel, ellenben egyre erőteljesebb iszlamista online propagandatevékenységet folytatott, illetve utcai megmozdulásokon vett részt, ahol le is tartóztatták. Végül 2013 végén Szíriába utazott, csatlakozott az Iszlám Államhoz, és felvette az Abu Husszein al-Britani szólítónevet.

Szíriában online dzsihádpropagandista és toborzó szerepet töltött be, és alapító tagja lett az Iszlám Államon belül egy angol nyelvű online toborzócsoportnak, amely egy tucat tagból állt, akiket az FBI „A légiónak" és a „Raqqa 12"-nek nevezett el. Husszein – köszönhetően a médiában róla megjelent rengeteg cikknek – rendkívül népszerűvé vált a dzsihádista online szubkultúrában. Bizonyítottan több sikeres és meghiúsított támadást is ő motivált, és ugyan az Iszlám Állam Hacker Osztályának (Islamic State Hacker Division – ISHD) vezetőjeként tartották számon, nem bizonyított, hogy közvetlenül valós hackertevékenységet végzett-e a konfliktusövezetből, ugyanakkor hackelésre buzdította kapcsolatait, akik által a megszerzett adatokat az Iszlám Állam érdekében használta fel.

Végül propaganda- és toborzási tevékenysége, a támadások megtervezése és azokra való felbujtás, valamint az érzékeny információk kiszivárogtatása a koalíciós erők nagy értékű célpontjává tette, és 2015. augusztus 24-én egy amerikai dróncsapás

[24] North Atlantic Treaty Organisation: Észak-atlanti Szerződés Szervezete.

végzett vele. Bár párhuzamosan a „légió" több tagjával végeztek, mégis ő volt az első, aki online tevékenység miatt lett egy rakétacsapás elsődleges célpontja.

### *Az online terrorista tartalmak elleni nemzetközi fellépés*

A terrorista tartalmak nagymérvű elterjedése arra késztette mind az államokat, mind a szolgáltató szektort, hogy fel-, illetve elismerjék, hogy összehangoltan fel kell lépniük ellenük. A kormányok a terrorizmus elleni küzdelem jegyében, míg a szolgáltatók az általuk teremtett brandek reputációjának védelme érdekében össze kellett hogy fogjanak, annak ellenére, hogy a két érdekcsoport viszonya nem volt felhőtlen, elsősorban a felhasználói adatok és kommunikációs tartalmak állami ellenőrizhetősége mentén kialakult viták miatt.

Az EU Internet Forum[25] létrehozását 2015 decemberében Dimitris Avramopoulos, az EU migrációs, belügyi és állampolgársági biztosa kezdeményezte az internet terrorista célú felhasználása ellen, tárgyalóasztalhoz ültetve az EU-tagállamok belügyminisztereit, az internetipart, tartalom- és tárhelyszolgáltatókat, és minden érdekelt felet, akinek szerepe lehet a probléma kezelésében. 2016-ban a szolgáltatóipar bejelentette egy „hash adatbázis" létrehozását a terrorista tartalmakról, elkerülendő azt, hogy az egyik szolgáltatónál törölt tartalmat másik platformon tegyenek elérhetővé, és hogy ezáltal az eltávolítások állandók és visszafordíthatatlanok legyenek.

2017 júniusában megalakult a terrorizmus elleni globális internetes fórum[26] is (Global Internet Forum to Counter Terrorism) ugyancsak azzal a céllal, hogy összefogja a technológiai ágazatot, a kormányokat, a civil társadalmat és az egyetemeket annak érdekében, hogy elősegítse az együttműködést és az információmegosztást a terrorista és az erőszakos extremizmus elleni küzdelemben.

A következő lökést a transznacionális és interszektorális együttműködés fokozására meglepő módon nem az iszlamista propaganda, nem egy Európában elkövetett dzsihádista indíttatású terrorcselekmény adta, hanem a christchurchi mészárlás. 2019. március 15-én az akkor 29 éves Brenton Harrison Tarrant ausztrál állampolgár terrortámadást hajtott végre az új-zélandi Christchurch két mecsetje, illetőleg az ott tartózkodók ellen, amely során megölt 51 és megsebesített 50 embert. A valós térben elkövetett terrortámadás mellett saját véleményem szerint a kibertérben is elkövetett egy terrorcselekményt, amely kijelentést valószínűleg a többség vitatná, tekintve, hogy online aktivitása nem járt közvetlen erőszakkal civilek ellen.

[25] European Union Internet Forum (EUIF).
[26] Global Internet Forum to Counter Terrorism (GIFCT).

De mi is történt a kibertérben? Az 8chan alkalmazáson jelenik meg elsőként egy poszt, amelyben megtalálható egy link az elkövető – fehér felsőbbrendűséget és neonáci ideológiát követő – kiáltványához, illetve a Facebook-link a cselekmény online közvetítéséhez. Majd a cselekménnyel egy időben felkerül a világhálóra egy 17 perces videó, amely a mai napig jelen van, közvetlen pszichikai befolyással a Tarrant által hirdetett ideológiára fogékony, potenciális magányos elkövetőkre, illetőleg hergelve – nemcsak a radikális – iszlám hívőket. Ugyan a Facebook „gyorsan" reagált az eseményre, de az eredeti videó törléséig azt több mint négyezren megtekintették, és másolatban – de legalább komment szintjén – megjelent a közösségi média minden platformján. Amellett, hogy természetesen az internet minden rétegén megtalálható a felvétel, ha csak annak Facebook-közzétételét vizsgáljuk is, arra a következtetésre jutunk, hogy a felvétel apró módosításaival folyamatosan kijátszhatók a szolgáltató ellenintézkedései. A Facebook közleménye szerint az első 24 órában a videó 1,5 millió másolatát távolították el a közösségi oldalról, illetve későbbi nyilatkozatuk szerint a támadáshoz kapcsolódóan 4,5 millió tartalmat tiltottak le. Két hónappal az esemény után az új-zélandi miniszterelnök és a francia elnök meghirdette a Christchurch Call[27] kiáltványt, amelyhez 53 ország, illetve nemzetközi szervezet mellett tíz online szolgáltató is csatlakozott, és köteleződött el az online terrorista tartalmak elleni fellépés iránt. Erősödött azon algoritmusoknak a fejlesztése, amelyek már az online közvetítés közben azonosíthatják a tartalmat, ezáltal lehetővé téve az időszerű cselekvést.

Az Európai Unióban az EU Internet Forum keretében 2019 októberében elfogadták az EU krízisprotokollt az online terrorista tartalmak virális terjedésének megakadályozására, oly módon, hogy a protokoll első tesztjét már szeptemberben végrehajtották. A 2019 októberében elfogadott dokumentumban a Bizottság, a tagállamok és az online szolgáltatók, köztük a Facebook, a Twitter, a Google, a Microsoft, a Dropbox, a JustPaste.it és a Snap elkötelezte magát az önkéntes együttműködésre.[28] A protokoll azóta több esetben került aktiválásra, mint például Samuel Paty már említett brutális meggyilkolása kapcsán.

Az is látszik azonban a bemutatott fórumok kapcsán, hogy azok eredményei a szolgáltató szektor önkéntes, aktív együttműködésén alapszanak. Ez azonban egy olyan iparágban, ahol a világ bármely pontjáról (egymástól gyökeresen különböző jogi környezetből) lényegében bárki kormányzati aktív ellenintézkedések nélkül a világ egészére tud szolgáltatást nyújtani, nem lehet elégséges. Nem véletlen tehát, hogy a tagállamok önállóan jogszabályalkotásba kezdtek, és az európai közösség is

[27] *Christchurch Call to eliminate terrorist and violent extremist online content adopted* 2019.
[28] European ComissionCommission 2019.

párhuzamosan elkezdett gondolkodni a terrorista tartalmak elleni egységes fellépésről és végső soron a tárhelyszolgáltatók együttműködésre kényszerítéséről, szükség esetén szankcionálásáról. Az EU-n belüli sorozatos terrortámadások és az interneten terjedő terrorista propaganda miatt az Európai Parlament 2017. június 15-én, majd 2017. június 22–23-án az Európai Tanács is állásfoglalásaikban a szolgáltatókat szólította meg a fellépés érdekében, majd a következő évben elfogadták a Bizottság (EU) 2018/334 ajánlását az illegális online tartalom hatékony kezelésére irányuló intézkedésekről, amelyben megfogalmazta a szükséges intézkedéseket mind a tagállamok, a szolgáltatók és az uniós intézmények (Europol) felé. 2018. szeptember 12-én aztán a Bizottság rendeletjavaslatot terjesztett a Tanács elé az online terrorista tartalom terjesztésének megelőzésére (Terrorism Content Online – TCO) irányulóan, amely az EU híresen lassú és nehézkes jogszabályalkotási mechanizmusán alig több mint két és fél év alatt keresztülverekedte magát, és megszületett Az Európai Parlament és a Tanács 2021. április 29-i (EU) 2021/784 rendelete az online terrorista tartalom terjesztésével szembeni fellépésről.[29] A rendelet kiemelt célja, hogy amikor terrorista tartalmat azonosítanak a hatóságok, a lehető leggyorsabban történjen meg azok eltávolítása, illetve hogy az online platformok intézkedéseket hozzanak abból a célból, hogy szolgáltatásaikkal ne lehessen visszaélni, és az eltávolított tartalmakat máshol ne lehessen ismét feltölteni. Kiemelt szempont, hogy mindez úgy történjen meg, hogy párhuzamosan teljes körű védelmet biztosítsanak a polgároknak a véleménynyilvánítás és a tájékozódás szabadságához fűződő alapvető jogai számára. A rendelet 2022 nyarán lépett hatályba, így annak eredményeit korai lenne még e sorok írásakor értékelni.

## KIBER-TERRORCSELEKMÉNYEK

Korábban utaltam arra, hogy a szakértők többsége elsősorban az angolszász fogalommeghatározásra hagyatkozva úgy tartja, hogy még nem került sor ilyen eseményre. Véleményem szerint, ha pusztán a bűncselekmény magyar büntető törvénykönyvben szereplő jogi definícióját vesszük figyelembe, akkor nagy valószínűséggel bármikor megtörténhet, sőt úgy gondolom, már meg is történt – csak nem került sor annak terrorcselekménnyé minősítésére – egy olyan terrorcselekmény, amelyben az eszközcselekmény egy, a számítástechnikai bűnözés kategóriájába tartozó deliktum.

[29] Az Európai Parlament és a Tanács (EU) 2021/784 rendelete az online terrorista tartalom terjesztésével szembeni fellépésről.

*Potenciális kiber-terrorcselekmény jogi értelemben Magyarországon*

Ha megvizsgáljuk a Btk. vonatkozó szakaszai alapján a Magyarországon terrorizmus szempontjából releváns ítéleteket, akkor arra a megállapításra juthatunk, hogy azok többségében a Btk. 316. §-ba ütköző terrorcselekmény elkövetésével fenyegetés bűntettében születtek, és a tényállás alapján az elkövető valamely hatóságot, legtöbbször igazságügyi hatóságot, rendőrséget fenyegetett meg erőszakos cselekmény elkövetésével, ha a hatóságok az elkövetőnek fontos eljárásban nem teljesítik a neki megfelelő intézkedést, vagy nem hoznak neki megfelelő döntést.

Ha egy olyan közelmúltban született ítéletet kívánunk megvizsgálni magyarországi elkövetés kapcsán, ahol az elkövető a fenyegetésen túllépve annál többet tett, a 2016-os Teréz körúti robbantás kapcsán 2019-ben megszületett jogerős döntés vizsgálata kézenfekvő. Az ítélet részletes tanulmányozása nélkül, pusztán a fővárosi ítélőtábla sajtóközleményét[30] elolvasva látszik, hogy az emberölés kísérlete és a robbanóanyaggal visszaélés mellett a terrorcselekmény kísérlete, majd jogerősen előkészülete azért került megállapításra, mert az elkövető a Belügyminisztérium részére elküldött, illetve előkészített levelében pénzkövetelés teljesítésétől tette függővé, hogy további robbantásokat nem hajt végre.

A fentiek alapján a kiber-terrorcselekmény elkövetése esetén is legnagyobb valószínűsége annak van, hogy az információs rendszer felhasználásával elkövetett csalást, vagy az információs rendszer vagy adat megsértése eszközbűncselekményt a törvényi tényállásban szereplő célzatok közül azért követik el, hogy az állami szervet arra kényszerítsék, hogy valamit tegyen (fizessen), ne tegyen, vagy eltűrjön. A két eszközbűncselekmény közül ha a legegyszerűbb forgatókönyvet keressük, egyértelműen az információs rendszer vagy adat megsértését kell alapul vennünk, tekintve, hogy a törvényi tényállások vizsgálata során megállapítható, hogy ez a bűncselekmény szükségszerű eszközcselekménye az információs rendszer felhasználásával elkövetett csalásnak, amelynek megvalósulásához szükségszerű a kár bekövetkezése is. Az információs rendszer vagy adat megsértésének törvényi tényállása alapján megállapítható, hogy a bűncselekmény elkövethető az információs rendszerbe belépéssel, az információs rendszer működésének akadályozásával vagy információs rendszerben lévő adat megváltoztatásával, törlésével vagy hozzáférhetetlenné tételével, természetesen akkor, ha az adott cselekmény jogosulatlanul, vagy a jogosultság kereteit túllépve történik. Nincs szükség ahhoz mélyebb informatikai ismeretre, hogy eljussunk arra a következtetésre, hogy az információs rendszerek és a bennük tárolt adatok elleni fenti cselekményekre a legalkalmasabb eszközök

[30] Fővárosi Ítélőtábla 2019.

a különböző kártékony szoftverek. Ezek főbb típusait ha számba vesszük, a terrorcselekmény elkövetéséhez szükséges fenti cél és eszközcselekmény ismeretében arra a megállapításra juthatunk, hogy egy zsarolóvírus[31] állami szervhez történő célba juttatása megvalósíthatja a terrorcselekmény törvényi tényállását. Tekintve, hogy a vonatkozó bírói gyakorlat – ahogy az egyébként a Btk. nagykommentárjában is megjelenik – állami szervnek tekinti az alaptörvényben felsorolt intézményeket, a jogszabály alapján közhatalmi, államigazgatási és önkormányzati igazgatási feladatokat ellátó szerveket, az állami gazdasági és költségvetési szerveket és az állam által alapított alapítványokat, ezért rendkívül nagy azon információs rendszerek száma, amelyek ransomware-rel történő támadása terrorcselekménynek minősülhet.

Ha a fentiek mellett figyelembe vesszük azt is, hogy a darkneten lehet vásárolni ransomware-készítő eszközöket, így azok megalkotására kezdő „hackereknek" is van lehetőségük, megállapíthatjuk, hogy megtaláltuk a jogi értelemben vett kiber-terrortámadás legegyszerűbb és legvalószínűbb forgatókönyvét. Mindezek ismeretében ugyanakkor joggal vetődik fel a kérdés mindenkiben, hogy az állami szerveket ért ilyen típusú támadásokról szóló sajtóhírek mellett miért nem hallunk a terrorcselekmény elkövetése miatt megindult eljárásokról, letartóztatásokról. Talán mindennek oka az is, hogy ugyancsak nincs információ Magyarországon befejezett, eredményesen lezárt olyan büntetőeljárásról sem, amely olyan információs rendszer vagy adat megsértése bűncselekmény volt, amelyet ransomware felhasználásával követtek volna el. Ahogy Gyaraki Réka *A számítógépes bűnözés nyomozásának problémái* című PhD-értekezésében kifejti, az ilyen támadások kapcsán a legnagyobb problémát az jelenti, hogy „önmagában ennek a deliktumnak a nyomozása sokkal inkább másodlagos, mint a jogellenes cselekmény bekövetkezésének felismerése és a helyzet kezelése".[32] Mindezek ellenére álláspontom szerint egy állami szerv ellen intézett célzott zsarolóvírus-támadás esetén annak helyes minősítése minden esetben terrorcselekmény kell hogy legyen, ugyanakkor egy, a WannaCryhoz hasonló, féreg típusú ransomware esetében értelemszerűnek tűnik a hatóságok azon hozzáállása, hogy az esetlegesen meginduló büntetőeljárásban a cselekmény minősítése az információs rendszer vagy adat megsértése, tekintve, hogy az elkövető azonosítását követően – arra tekintettel, hogy a terrorcselekmény szándékos bűncselekmény – a bizonyításnak arra is ki kell terjednie, hogy az elkövetőnek legalább eshetőleges szándékában állt állami szerveket is megtámadni.

---

[31] „Zsarolóvírus (angolul: ransomware) alatt olyan kártékony szoftvert értünk, amelynek célja valamilyen módon »túszul ejteni« a felhasználók informatikai eszközein tárolt adatokat, amelyeket csak váltságdíj megfizetése esetén tesz újra elérhetővé." Nemzeti Kibervédelmi Intézet 2019. Online: https://nki.gov.hu/it-biztonsag/tudastar/zsarolovirus-ransomware-v2/

[32] Gyaraki 2018.

## *Egy erőszakot is megvalósító kiber-terrortámadás lehetséges forgatókönyvei*

Amellett, hogy azonosítottam, hogy a terrorcselekmény törvényi tényállása hogyan meríthető ki legegyszerűbben a kibertér eszköztárával, szükségesnek tartom annak a vizsgálatát is, hogy egy, az angolszász definíciónak is megfelelő, a fizikai térben erőszakot, halált, rombolást is megvalósító kiberterrorista cselekmény mely módon valósulhatna meg. Kézenfekvő megoldást jelentenek a célpont keresésénél – már csak elnevezésük alapján is – a létfontosságú rendszerek, rendszerelemek,[33] amelyek informatikai rendszereiken keresztül történt megtámadása vitán kívül súlyos következményekkel járhat. Ugyanakkor pont kiemelkedő fontosságuk miatt mind nemzeti, mind nemzetközi szinten prioritást képez ezen infrastruktúrák védelme.

Nem célom kiragadni egy példát, és szimulálni az eseményeket. Álláspontom szerint egy potenciális támadó – aki véleményem szerint leginkább egy, a magányos elkövető kategóriájába tartozó, feltehetőleg mentális betegséggel is küzdő hacker – leginkább az ipari irányítórendszerekben, illetve azok sérülékenységeiben találhatja meg azt a célpontot, amelynek saját eszközeivel történő megtámadásával személyes sérelmeit megbosszulhatja, illetőleg az általa befogadott szélsőséges, erőszakos eszmében megfogalmazott célokat előmozdíthatja. Ma, a negyedik ipari forradalom korszakában ezek az egymással is összekapcsolt, a gyártást és az ipari folyamatokat irányító, automatizáló rendszerek jelen vannak a gazdaság minden ágazatában, irányítva hatalmas – kétségtelenül az emberre és a környezetre is veszélyes – gépsorokat, kontrollálnak robbanásveszélyes vagy mérgező anyagokat, és természetesen a kritikus infrastruktúrák üzemeltetésében is jelentős szerepük van. Túllépve az ipari szektor korlátait, a dolgok internete (Internet of Things, IoT)[34]

[33] „Létfontosságú rendszerelem: az 1. mellékletben meghatározott ágazatok (Energia, Közlekedés, Agrárgazdaság, Egészségügy, Társadalombiztos, Pénzügy, Infokommunikációs technológiák, Víz, Honvédelem, Közbiztonság-védelem) valamelyikébe tartozó szolgáltatás, eszköz, létesítmény vagy rendszer olyan rendszereleme, továbbá azok által nyújtott szolgáltatások, amelyek elengedhetetlenek a létfontosságú társadalmi feladatok ellátásához – így különösen az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához, az ország honvédelméhez –, és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna." 2012. évi CLXVI. tv. a létfontosságú rendszerek és létesítmények azonosításáról kijelöléséről és védelméről, 1. § j) pont.

[34] „Egy társadalmi-technológiai keretkoncepció, ami azt írja le, hogy termékek, tárgyak, eszközök online összekapcsolódnak, egymással kommunikálnak, feladatokat hajtanak végre, anélkül, hogy ehhez feltétlenül felhasználói kezelőfelület csatlakozna. Technikailag olyan természetes, vagy ember által megalkotott objektumok sokaságát írjuk így le, amik IP-címmel rendelkeznek

megjelenésével és elterjedésével életünk minden területén, ma már hétköznapjainkban, otthonainkban is komoly hatással bírnak.

Az Önkéntes Kibervédelmi Összefogás[35] égisze alatt indított, ipari és folyamatirányítási informatikai rendszerek biztonsági kérdéseivel foglalkozó ICS Cyber Security blog[36] szakmai bejegyzéseit megvizsgálva a különböző vezérlőrendszerek sérülékenységei mellett több, a közműszektort is érintő kibertámadást vizsgálhatunk meg, köztük az egyébként a hazai sajtóban is szinte minden fórumon megjelent incidenst, amelyben a floridai Oldsmar város vízművében a támadó több mint százszorosra emelte a vízhez adagolt marólúg mennyiségét. A behatoló a rendszer több, egyenként is súlyos sérülékenységét használta ki, amihez még magas fokú tudásra sem volt szükség. Bár a hatóságok azzal nyugtatták a lakosságot, hogy a vízminőség megváltozásához több napra lett volna szükség, és a rendszer biztonsági mechanizmusai időben jeleztek volna, szakértők szerint egy szofisztikált támadás esetén egy képzett hacker azok kiiktatásáról is gondoskodhatott volna. Az ivóvíz mint egyik legfontosabb éltető elemünk hadászati vagy terrorista célú támadása nem új keletű jelenség, arra a történelem minden korszakában lehet példát találni, ezért a 21. században, amikor informatikai rendszerek biztosítják számunkra annak a minőségét, mint ahogy a példa is mutatja, akár egy kiberterrorista támadás célpontja is lehet. Nem véletlen, hogy a Nemzeti Közszolgálati Egyetem hallgatói a Belügyi Tudományos Tanács pályázatára is kidolgoztak egy szcenáriót, amely során kibertámadást intéznek a Fővárosi Vízművek rendszerei ellen.[37] Bár a forgatókönyv véleményem szerint sokkal inkább egy kiber-terrortámadásnak álcázott kiberművelet, ugyanakkor elméleti alapon bemutatja a floridai példával gyakorlatban igazolt támadás működőképességét. Túllépve a közműágazaton, az is könnyen felismerhető, hogy a különböző ágazatok által használt veszélyes technológiák, anyagok egy terrorista által könnyedén fegyverként is használhatók.

A kérdés már csak az, hogy ezen irányítórendszerekkel való visszaélésnek mekkora realitása van például Magyarországon. A BlackCell magyar kiberbiztonsági cég 2019. december 10. és 29. között lefolytatott kutatása[38] eredményeként megállapította,

és képesek az internetes hálózaton keresztül adatot forgalmazni…" Informatikai, Távközlési és Elektronikai Vállalkozások Szövetsége 2014–2015.

35 2011-ben civil informatikai-biztonsági, kibervédelmi szakemberek által létrehozott társadalmi szervezet, amelynek célja többek között, hogy a szakemberek egymással összefogva és a szükséges információkat megosztva a lehető legmagasabb szintű védelmet tudják megvalósítani, felajánlva az állam számára tagjainak szaktudását és tettrekészségét azért, hogy az a haza kiberterének védelmét szolgálja. Önkéntes Kibervédelmi Összefogás. Online: https://www.kibev.hu/.

36 ICS Cyber Security blog. Online: https://icscybersec.blog.hu

37 Almási et al. 2018.

38 Kocsis 2019.

hogy a vizsgált időszakban 2013 olyan szélesebb értelemben vett ipari vezérlőeszköz érhető el szabadon az interneten, amelyek nagy része sebezhető is, és legalább 364 darabot már korábban meg is hackeltek. Természetesen az bizton kijelenthető, hogy nincs minden eszköz mögött ember vagy anyagi javak támadására alkalmas rendszer, ugyanakkor ha csak egy darab is megtalálható, az is időzített bomba lehet Magyarország és a magyar állampolgárok ellen.

Hangsúlyozni szeretném, hogy az elemzés az érintett eszközök vonatkozásában a „külsős" által könnyedén támadható, sérülékeny eszközöket vette számba. Ugyanakkor ne felejtsük el, hogy a támadó belsős is lehet, akár az adott létfontosságú információs rendszerelem „gazdája", annak biztonságáért felelős személy is, akik ugyan többségükben nemzetbiztonsági ellenőrzésre is kötelezettek, de mivel az érintett szolgálatok sem ellenőrizhetnek folyamatosan mindenkit, ezeknél a kritikus rendszereknél különösen fontos a több szem elvének alkalmazása a biztonság érdekében.

Az informatika életünk minden részét behálózó rendszerében bizonyosan képtelenség számba venni minden olyan metódust, amellyel az egyébként az életünket megkönnyítő technológia az életünk ellen fordítható. Persze a kijelentés igaz a fizikai térben kivitelezhető terrortámadásokra is, hisz az elkövetők folyamatosan keresik azokat a megoldásokat, amelyekkel a lehető legkisebb ráfordítás mellett az áldozatok száma maximalizálható. A 2016. július 14-i, 84 áldozatot követelő nizzai terrortámadásig – amelyben az elkövető egy bérelt teherautóval hajtott az ünneplők közé – a hatóságok a nyilvános terek és a tömegrendezvények biztosítása során sokkal kisebb hangsúlyt fektettek a helyszínek gépjárművektől való védelmére, holott jelenleg már az önvezető járművek kapcsán azzal is számolnunk kell, hogy a gépjárművet az elkövető távolról is fegyverré változtathatja.

## ÖSSZEGZÉS

Az informatika, a kibertér vívmányai életünk, mindennapjaink szerves részévé váltak, ugyanakkor, ahogy minden éremnek két oldala van, napról napra tapasztalhatjuk meg a fejlődés életünket és biztonságunkat veszélyeztető oldalát is. Persze a jelenség nem a számítástechnikai rendszerekből ered, hanem belőlünk, emberekből, akik az első primitív eszközök feltalálása vagy a tűz felfedezése óta a rendelkezésünkre álló eszközökkel, erőforrásokkal nemcsak élni, de visszaélni is tudunk.

A terrorista, a terrorszervezet ugyanúgy a maximális teljesítményre, hatékonyságra törekszik, mint bármelyik legális emberi vállalkozás. Mindezek miatt nem meglepő, hogy a hatékonyságát növelő eszközöket, így a kibertérben rejlő potenciált is alkalmazza tevékenysége minden területén a propagandától és a toborzástól,

az arra fogékony és sérülékeny közönség radikalizációjától kezdve a szervezet működtetéséhez szükséges javak előteremtésén és a kommunikáción keresztül a műveletek előkészítéséig. Bár egyértelmű, az angolszász fogalommeghatározás szerinti közvetlen erőszakot megvalósító kiber-terrortámadásra ez idáig nem került sor, együtt kell élnünk a gondolattal, hogy bármelyik pillanatban megtörténhet, továbbá nehéz lenne összeszámolni azokat az áldozatokat, akik halálát az online radikalizált elkövetők cselekményei okozták.

A terrorizmus elhárításáért felelős szervezeteknek tehát folyamatosan képesnek kell lenniük a megújulásra, hisz abban kétségtelenül biztosak lehetünk, hogy a támadók minden elérhető lehetséges eszközt és módszert használni fognak. A jelen kihívásai mellett a jövőbe is kell tekinteni, elkerülendő, hogy áldozatok árán azonosítsuk az újabb fenyegetéseket. Amellett, hogy elismerjük a kibertérből bármikor érkezhető fenyegetéseket, szükséges azonosítanunk azok potenciális jövőjét is. Nem véletlen tehát, hogy az ENSZ Terrorellenes Központja[39] az ENSZ Terrorizmus Elleni Irodájával[40] és az ENSZ Interregionális Bűnügyi és Igazságügyi Kutatóintézetével[41] közösen a Terrorelhárítás a Mesterséges Intelligencia Korában címmel bejelentett kutatási kezdeményezésében[42] nemcsak a mesterséges intelligencia terrorelhárítású célú felhasználását említi például az online terrorista tartalmak gyors azonosításában potenciálisan betölthető szerepe miatt, de annak rosszindulatú, terroristák általi felhasználásának lehetőségét is. Ez utóbbi kapcsán talán nem én vagyok az egyetlen, akinek a fejében megfordul az a jelenleg még science fiction-forgatókönyv is, amikor adott esetben már egy emberi irányítás nélküli mesterséges intelligencia ellen kell küzdenie a szolgálatoknak.

## FELHASZNÁLT IRODALOM

Al-Lami, Mina (2018): Analysis: Wave of Telegram Suspensions Hits Jihadist Accounts. *BBC,* 2018. december 7. Online: https://monitoring.bbc.co.uk/product/c200h0s4

Almási Csaba Sándor et al. (2018): A főváros ivóvízellátó rendszere ellen intézett informatikai támadás potenciális következményei és azok felszámolásának megoldási lehetőségei. *Rendvédelem,* 7(1), 103–149. Online: https://bm-tt.hu/wp-content/uploads/2022/02/2018_1.pdf

*Christchurch Call to Eliminate Terrorist and Violent Extremist Online Content Adopted* (2019). Online: https://www.christchurchcall.com/media-and-resources/news-and-updates/christchurch-call-adopted

[39] UN Counter-Terrorism Centre (UNCCT).

[40] UN Office of Counter-Terrorism (UNOCT).

[41] UN Interregional Crime and Justice Research Institute (UNICRI).

[42] UN Counter-Terrorism Centre – UN Interregional Crime and Justice Research Institute 2020.

CLIFFORD, Bennett (2020): *Extremist Experimentation with Text-Based Instant Messaging Applications.* Global Network on Extremism & Technology. Online: https://gnet-research.org/2020/11/09/extremist-experimentation-with-text-based-instant-messaging-applications/

CORERA, Gordon (2008): The World's Most Wanted Cyber-Jihadist. *BBC,* 2008. január 16. Online: http://news.bbc.co.uk/2/hi/americas/7191248.stm

*Europol Disrupts Islamic State Propaganda Machine* (2019). *BBC,* 2019. november 25. Online: https://www.bbc.com/news/world-middle-east-50545816

FANG, Binxing (2018): *Cyberspace Sovereignty. Reflections on Building a Community of Common Future in Cyberspace.* Beijing: Springer. Online: https://doi.org/10.1007/978-981-13-0320-3

Financial Action Task Force (FATF) (2002): *International Best Practices Combating the Abuse of Non-Profit Organisations.* Online: https://www.fatf-gafi.org/media/fatf/documents/recommendations/11%20FATF%20SRIX%20BPP%20SRVIII%20October%202003%20-%20COVER%202012.pdf

GIBSON, Stevyn D. (2014): Exploring the Role and Value of Open Source Intelligence. In HOBBS, Christopher – MORAN, Matthew – SALISBURY, Daniel (szerk.): *Open Source Intelligence in the Twenty-First Century. New Security Challenges.* London: Palgrave Macmillan, 9–23. Online: https://doi.org/10.1057/9781137353320_2

GIBSON, William (1992): *Neurománc.* Budapest: Valhalla Páholy Kft.

GILLESPIE, Alisdair A. (2016): *Cybercrime – Key Issues and Debates.* London – New York: Routledge. Online: https://doi.org/10.4324/9781315884202

GYARAKI Réka Eszter (2018): *A számítógépes bűnözés nyomozásának problémái.* PhD-disszertáció. Pécs: Pécsi Tudományegyetem Állam- és Jogtudományi Karának Doktori Iskolája. https://ajk.pte.hu/files/file/doktori-iskola/gyaraki-reka/gyaraki-reka-muhelyvita-ertekezes.pdf

HAMID, Nafees (2018): The British Hacker Who Became the Islamic State's Chief Terror Cybercoach: A Profile of Junaid Hussain. *CTC Sentinel,* 11(4), 30–37. Online: https://ctc.usma.edu/wp-content/uploads/2018/04/CTC-SENTINEL-042018-3.pdf

*IS Exploits Telegram Mobile App to Spread Propaganda* (2015). *BBC,* 2015. október 7. Online: https://www.bbc.com/news/technology-34466287

KOCSIS Tamás (2019): *ICS/OT Snapshot 2019.* Black Cell Magyarország Kft.

KOVÁCS László (2006): Az információs terrorizmus eszköztára. *Hadmérnök,* 1(Különszám), 171–179. Online: http://www.hadmernok.hu/kulonszamok/robothadviseles6/kovacs_rw6.html

ÜNVER, H. Akın (2018): Digital Open Source Intelligence and International Security: A Primer. *Cyber Governance and Digital Democracy,* (8). Online: https://www.jstor.org/stable/resrep21048

UN Counter-Terrorism Centre – UN Interregional Crime and Justice Research Institute (2020): *UNCCT and UNICRI Jointly Launched a New Research Initiative: Counter-Terrorism in the Age of Artificial.* Online: https://www.un.org/counterterrorism/sites/www.un.org.counterterrorism/files/20200701_press_release_new_joint_ai_research_initiative.pdf

U.S. Department of Justice Office of Public Affairs (2020): *Global Disruption of Three Terror Finance Cyber-Enabled Campaigns.* Online: https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyber-enabled-campaigns

WIENER, Norbert (1968): *Cybernetics or Control and Communication in the Animal and the Machine.* Cambridge: The Massachusetts Institude of Technology. Online: https://uberty.org/wp-content/uploads/2015/07/Norbert_Wiener_Cybernetics.pdf

## *Egyéb források*

1139/2013. (III. 21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról.

2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról kijelöléséről és védelméről.

Az Európai Parlament és a Tanács (EU) 2021/784 rendelete az online terrorista tartalom terjesztésével szembeni fellépésről. 2021. április 29.

Council of the European Union (2020): Council Resolution on Encryption – Security through Encryption and Security Despite Encryption. Online: https://data.consilium.europa.eu/doc/document/ST-13084-2020-REV-1/en/pdf

European Comission (2019): *Fighting Terrorism* Online: *EU Internet Forum Committed to an EU-wide Crisis Protocol.* Online: https://ec.europa.eu/commission/presscorner/detail/en/ip_19_6009

European Commission's Expert Group on Violent Radicalisation (2008): *Radicalisation Processes Leading to Acts of Terrorism.* Online: https://www.clingendael.org/sites/default/files/pdfs/20080500_cscp_report_vries.pdf

European Union Internet Forum (EUIF). Online: https://home-affairs.ec.europa.eu/networks/european-union-internet-forum-euif_en

Europol (2018): *Islamic State Propaganda Machine Hit by Law Enforcement in Coordinated Takedown Action.* Online: https://www.europol.europa.eu/media-press/newsroom/news/islamic-state-propaganda-machine-hit-law-enforcement-in-coordinated-takedown-action

Europol (2019): *Referral Action Day against Islamic State online terrorist propaganda.* Online: https://www.europol.europa.eu/media-press/newsroom/news/referral-action-day-against-islamic-state-online-terrorist-propaganda

Europol (2020): *EU Terrorism Situation & Trend Report (TE-SAT).* Online: https://www.europol.europa.eu/activities-services/main-reports/eu-terrorism-situation-and-trend-report#fnd-tn-tabs-0-bottom-2.

Fővárosi Ítélőtábla (2019): *Sajtóközlemény: Súlyosította a Fővárosi Ítélőtábla a Teréz körúti robbantó büntetését.* Online: https://fovarosiitelotabla.birosag.hu/sites/default/files/field_attachment/p.l.g._sajtokozlemeny_0.pdf

Informatikai, Távközlési és Elektronikai Vállalkozások Szövetsége (2014–2015): *Előzetes Megvalósíthatósági Tanulmány „Az Internet of Things koordinált fejlesztése és alkalmazásának elterjesztése Magyarországon" tárgykörben.* Budapest.

NATO (2001): AJP-01(B) Allied Joint Doctrine. Ratification Draft 1. – 14-1.